bitdefender
INTERNET SECURITY 2011

Benutzerhandbuch

BitDefender Internet Security 2011
Benutzerhandbuch

Veröffentlicht 2010.09.08

Rechtlicher Hinweis


bitdefender

Inhaltsverzeichnis

Installation und Deinstallation

1. Systemanforderungen

Sie können BitDefender Internet Security 2011 nur auf Computern mit den folgenden Betriebssystemen installieren.

- Windows XP mit Service Pack 3 (32 bit) / Windows XP mit Service Pack 2 (64 bit)
- Windows Vista mit Service Pack 1 oder höher (32/64 bit)
- Windows 7 (32/64 bit)

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestanforderungen für Hardware und Software erfüllt.

Beachten Sie

Um Informationen über Ihr Betriebssystem und Ihre Hardware zu erhalten, klicken Sie mit der rechten Maustaste auf dem Desktop auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus dem Menü.

1.1. Mindestsystemanforderungen

- 1 GB verfügbarer Festplattenspeicher
- 800 MHz Prozessor
- Arbeitsspeicher:
  - 512 MB für Windows XP
  - 1 GB für Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (ist ebenfalls Bestandteil des Installationspakets)
- Adobe Flash Player 10.0.45.2

1.2. Empfohlene Systemanforderungen

- 1 GB verfügbarer Festplattenspeicher
- Intel CORE 2 Duo (1.66 GHz) oder gleichwertiger Prozessor
- Arbeitsspeicher:
  - 1 GB für Windows Vista/Windows 7
  - 1.5 GB für Windows Vista
- Internet Explorer 7
- .NET Framework 2 (ist ebenfalls Bestandteil des Installationspakets)
- Adobe Flash Player 10.0.45.2

1.3. Software-Anforderungen

Der Antiphishing-Schutz funktioniert nur für:

- Internet Explorer 6.0 (oder höher)
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Instant Messaging (IM) Verschlüsselung funktioniert nur für:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Der Antispam-Schutz steht für alle POP3/SMTP Email-Clients zur Verfügung.Die BitDefender Antispam-Toolbar wird integriert in:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

2. Vor der Installation

Bevor Sie BitDefender Internet Security 2011 installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass der Zielcomputer für die BitDefender-Installation die Systemvoraussetzungen erfüllt.Wenn Ihr Computer nicht die Mindest-Systemanforderungen erfüllt, kann BitDefender nicht installieren werden. Wird die Systemkonfiguration nachträglich verändert, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen.Eine vollständige Liste der Systemanforderungen finden Sie unter *„Systemanforderungen“ (S. 2)*.
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie andere Sicherheits-Software von Ihrem Computer.Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen.Windows Defender wird standardmäßig deaktiviert bevor die Installation startet.
- Deaktivieren oder entfernen Sie jegliche Firewall-Programme, die auf dem PC installiert sind.Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen.Die Windows Firewall wird standardmäßig deaktiviert, bevor die Installation startet.

3. Installation von BitDefender

Sie können BitDefender von einer BitDefender Installations-CD oder per Installations-Paket installieren, welches Sie von der BitDefender Webseite oder anderen BitDefender autorisierten Webseiten heruntergeladen haben, installieren.Sie können das Installationspaket von der BitDefender Webseite unter folgender Adresse herunterladen: http://www.bitdefender.com/site/Downloads/.

- Um BitDefender von CD zu installieren, legen Sie die CD ins Laufwerk ein. Ein Willkommens-Bildschirm sollte nach wenigen Augenblicken eingeblendet werden. Folgen Sie den Anweisungen um die Installation zu starten.

  Beachten Sie

  Auf der Willkommensseite haben Sie die Möglichkeit das Installationspaket von der CD auf einem USB Speicher zu kopieren. Dies ist nützlich, wenn Sie BitDefender auf einen Computer installieren möchten, der kein CD-ROM Laufwerk hat (bspw. ein Netbook).Verbinden Sie das Speichermedium mit einem USB Port und klicken Sie auf **Kopiere auf USB**.Danach gehen Sie zu dem Computer ohne CD-ROM-Laufwerk, verbinden das Speichermedium mit dem USB-Port und doppel-klicken in dem Verzeichnis, in dem Sie das Installationspaket gespeichert haben, auf `runsetup.exe`.

  Falls der Begrüßungsbildschirm nicht eingeblendet wird, gehen Sie in das Root-Verzeichnis Ihrer CDs und doppelklicken Sie auf `autorun.exe`.

- Um BitDefender anhand der auf ihrem Computer geladenen Installations-Datei zu installieren, führen Sie sie mit einem Doppelklick aus.

Der Installer wird zuerst Ihr System prüfen, um die Installation zu bestätigen.Wenn die Installation bestätigt ist, werden Sie aufgefordert, die gewünschte Sprache zu wählen, bevor der Setup-Assistent eingeblendet wird.

Der Assistent hilft Ihnen bei der Installation von BitDefender auf Ihrem Computer und ermöglicht Ihnen gleichzeitig, die wichtigsten Einstellungen und die Benutzeroberfläche zu konfigurieren.

3.1. Schritt 1 - Einführung

Bitte lesen Sie sich die Lizenzvereinbarung durch und wählen Sie **Durch Aktivierung dieses Kästchens stimme ich den Lizenzvereinbarungen von BitDefender zu**.Klicken Sie auf **Weiter**.

Wenn Sie diesen Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie verlassen den Setup-Vorgang.

3.2. Schritt 2 - Vorbereitung der Installation

BitDefender scannt Ihr System und überscannt, ob eine andere Sicherheitssoftware installiert ist.

Quick Scan

Ein Quick Scan der kritischen Bereiche Ihres Systems wird durchgeführt, um sicherzustellen, dass sich dort keine Malware verbirgt.

Der Scan sollte nicht länger als einige Minuten dauern. Sie können ihn jederzeit durch einen Klick auf die entsprechende Schaltfläche (Button) abbrechen.

Wichtig
Wir empfehlen dringend, den Scan abzuschließen.
Aktive Malware könnte die Installation stören oder sogar dazu führen, dass die Installation fehlschlägt.

Nachdem der Scan abgeschlossen wurde, werden die Ergebnisse angezeigt. Wurden Bedrohungen festgestellt, folgen Sie den Anweisungen, um diese zu entfernen, bevor Sie mit der Installation fortfahren.

Klicken Sie auf **Weiter**.

Entfernen existierender Sicherheitssoftware

BitDefender Internet Security 2011 informiert Sie, wenn weitere Antiviren-Programme auf Ihrem Computer installiert sind.Klicken Sie auf den entsprechenden Button, um den Installationsvorgang zu starten und den Anweisungen zu folgen, wie diese Produkte eventuell entfernt werden können.

Warnung
Es wird dringend empfohlen, andere Antiviren-Programme zuvor zu deinstallieren. Eine zeitgleiche Verwendung mehrerer Antiviren-Produkte kann Instabilität und Systemabstürze zur Folge haben.

BitDefender empfiehlt außerdem Aktionen, um die Windows Sicherheitsfunktionen zu aktivieren.

- **Windows-Firewall ausschalten** - Deaktivierung der Windows-eigenen Firewall.

Wichtig
Wir empfehlen die Windows-basierte Firewall zu deaktivieren. BitDefender Internet Security 2011 beinhaltet eine erweiterte Firewall. Der Gebrauch von zwei Firewalls auf einem Computer kann zu Problemen führen.

- **Windows Defender ausschalten** - Deaktivierung von Windows Defender.

Klicken Sie auf **Weiter**.

3.3. Schritt 3 - Registrierung

Der Registriervorgang von BitDefender umfasst eine Registrierung des Produkts mit einem Lizenzschlüssel und die Aktivierung der Online-Funktionen durch die Erstellung eines BitDefender-Benutzerkontos.

Registrieren Sie Ihr Produkt.

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

- **Ich habe BitDefender Internet Security 2011 online oder auf CD gekauft.**

  In diesem Fall müssen Sie das Produkt registrieren:

  1. Geben Sie den Lizenzschlüssel in das Bearbeiten-Feld ein.

     Beachten Sie

     Sie finden den Lizenzschlüssel:
     - Auf der Schnell-Start-Anleitung.
     - Auf der Produktregistrierkarte.
     - In der Email-Bestätigung des Online-Kaufs.

     Wenn Sie keinen BitDefender-Lizenzschlüssel besitzen, klicken Sie auf den angegebenen Link, um so zum BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu kaufen.

  2. Klicken Sie auf **Jetzt registrieren**.
  3. Klicken Sie auf **Weiter**.

- **Ich habe BitDefender Internet Security 2011 zum Testen heruntergeladen**

  In diesem Fall können Sie alle Produktfunktionen 30 Tage lang nutzen.Um die Testphase zu starten, wählen Sie **Ich möchte BitDefender Internet Security 2011 für 30 Tage testen** und klicken Sie auf **Weiter**.

Aktivierung Online-Funktionen

Sie müssen ein BitDefender Benutzerkonto registrieren, um die BitDefender Updates zu erhalten.Mit dem BitDefender-Benutzerkonto erhalten Sie zudem Zugriff auf die Online-Kindersicherung, den kostenfreien technischen Support und Sonderangebote und -Aktionen.Wenn Sie Ihren BitDefender-Lizenzschlüssel verlieren, können Sie sich unter http://myaccount.bitdefender.com in Ihr Konto einloggen, um ihn wieder zu erhalten.

Wenn Sie im Moment kein BitDefender-Benutzerkonto anlegen möchten, klicken Sie auf **Später registrieren** und dann auf **Beenden**.

Beachten Sie

Wenn Sie BitDefender Internet Security 2011 zum Testen installieren, müssen Sie jetzt ein BitDefender-Benutzerkonto erstellen.
Wenn Sie das Produkt gekauft haben, müssen Sie innerhalb von 30 Tagen nach der Installation ein Benutzerkonto einrichten.

Ansonsten wählen Sie:

- **Ich habe noch kein BitDefender-Benutzerkonto**

  Um ein BitDefender-Benutzerkonto anzulegen, gehen Sie folgendermaßen vor:

  1. Wählen Sie **Neues Benutzerkonto erstellen**.
  2. Geben Sie die Daten in die entsprechenden Felder ein.Die hier ingegebenen Daten bleiben vertraulich.
     - **Benutzername** - geben Sie Ihre Email-Adresse ein.
     - **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein.Das Passwort muss zwischen 6 und 16 Zeichen lang sein
     - **Passwort erneut eingeben** - geben Sie das vorher vergebene Passwort erneut ein.

       Sie müssen das Passwort nicht erneut eintippen, wenn Sie gewählt haben, dass das Passwort während des Eintippens unverschlüsselt dargestellt wird.

     Beachten Sie

     Wenn das Konto einmal aktiviert ist, können Sie unter http://myaccount.bitdefender.com die angegebene Email-Adresse und das Passwort für die Anmeldung an Ihrem Konto verwenden.

  3. Auf Wunsch wird BitDefender Sie über die Email-Adresse Ihres Benutzerkontos über Sonderangebote und Promotions informieren.Klicken Sie auf **Kontaktoptionen ansehen** und wählen Sie im eingeblendeten Fenster eine der verfügbaren Optionen.
     - **Alle Nachrichten senden**
     - **Wichtige Nachrichten senden**
     - **Ich möchte keine Nachrichten erhalten**
  4. Klicken Sie auf **Übermitteln**.
  5. Klicken Sie auf **Weiter**.

     Beachten Sie

     Sie müssen Ihr Benutzerkonto aktivieren bevor Sie es nutzen können.
     Sobald Sie die vom BitDefender Registrierung dienst gesendete Mail erhalten haben, folgen Sie den darin enthaltenen Anweisungen.

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

BitDefender weist Sie daraufhin, wenn bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert ist.In diesem Fall geben Sie das Passwort für Ihr Benutzerkonto ein und klicken Sie auf **Einloggen**.Klicken Sie auf **Weiter**.

Wenn Sie schon über ein aktives Konto verfügen, BitDefender dieses aber nicht findet, folgen Sie diesen Schritten, um Ihr Produkt zu registrieren.

1. Wählen Sie **Einloggen (Bestehendes Ben.konto)**.
2. Geben Sie die Email-Adresse und das Passwort Ihres Kontos in den entsprechenden Feldern ein.

   Beachten Sie
   Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Anweisungen.

3. Auf Wunsch wird BitDefender Sie über die Email-Adresse Ihres Benutzerkontos über Sonderangebote und Promotions informieren.Klicken Sie auf **Kontaktoptionen ansehen** und wählen Sie im eingeblendeten Fenster eine der verfügbaren Optionen.
   - **Alle Nachrichten senden**
   - **Wichtige Nachrichten senden**
   - **Ich möchte keine Nachrichten erhalten**
4. Klicken Sie auf **Übermitteln**.
5. Klicken Sie auf **Weiter**.

3.4. Schritt 4 - Ansicht wählen

Hier können Sie wählen, welche Installation svariante Sie durchführen möchten und sich den Ansichtsmodus der Benutzerfläche ansehen.

Wählen Sie die Setup-Art.

Folgende Setup-Buttons stehen zur Verfügung:

- **Einfacher Setup** - wählen Sie diese Option, wenn Sie eine schnelle Installation bevorzugen und die BitDefender-Einstellungen nicht im Detail konfigurieren möchten.
- **Benutzerdefinierter Setup** - wählen Sie diese Option, wenn Sie den Setup und die BitDefender-Einstellungen benutzerdefiniert anpassen möchten.

Um sich ein Video-Tutorial anzusehen, das Ihnen bei der Installation weiterhelfen kann, klicken Sie auf **Hilfestellung**.

Beachten Sie
Um BitDefender in der Voreinstellung zu installieren und gleich zum letzten Arbeitsschritt des Installations-Assistenten zu gehen, wählen Sie **Setup überspringen**.

Klicken Sie auf **Weiter**.

Setup-Ort wählen

Beachten Sie

Dieser Schritt steht nur zur Verfügung, wenn Sie die Variante **Benutzerdefinierter Setup** gewählt haben.

Als Voreinstellung wird BitDefender Internet Security 2011 in `C:\Programmdateien\BitDefender\` installiert.Falls Sie ein anderes Verzeichnis wählen möchten, klicken Sie auf **Durchsuchen** und wählen Sie das Verzeichnis in dem Sie BitDefender installieren möchten.

Sie können die Produktdateien und Signaturen mit anderen BitDefender-Anwendern teilen.So können BitDefender-Updates schneller durchgeführt werden.Falls Sie diese Funktion nicht aktivieren möchten, wählen Sie die entsprechende Option.

Beachten Sie

Wenn diese Funktion aktiviert ist, werden keinerlei persönlich identifizierbaren Informationen mitgeteilt.

Klicken Sie auf **Weiter**.

Wählen Sie Ihre Ansicht (Benutzeroberfläche)

Wählen Sie die für Sie am besten geeignete Ansicht der Benutzeroberfläche.BitDefender Internet Security 2011 bietet Ihnen die Auswahl zwischen drei Ansichten, jede von Ihnen zugeschnitten auf verschiedene Benutzertypen.

Basis-Ansicht

Geeignet für Anfänger und für diejenigen, die BitDefender ohne Aufwand zum Schutz des Computers und der Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits.

Sie müssen nur dann Probleme beheben, wenn BitDefender Sie dazu auffordert. Ein intuitiver Schritt-für-Schritt Assistent hilft Ihnen dabei.Zusätzlich können Sie normale Aufgaben, Vorgänge wie das Aktualisieren der BitDefender-Virensignaturen und Produktdateien oder den Scan Ihres Computers durchführen.

Standard-Ansicht

Sie können die Haupteinstellungen von BitDefender konfigurieren, Probleme separat beseitigen, die BitDefender-Produkte, die auf den Computern Ihres Haushaltes installiert sind, verwalten und wählen, welche Probleme überwacht werden sollen.Zudem können Sie über die Kindersicherung steuern, wie Ihre Kinder den PC und das Internet benutzen dürfen.

Experten-Ansicht

Gedacht für technisch fortgeschrittene Anwender, erlaubt diese Ansicht jede Funktion von BitDefender zu konfigurieren.Weiterhin können Sie zudem alle Funktionen nutzen, um Ihren Computer und Ihre Daten zu schützen.

Treffen Sie Ihre Auswahl und klicken Sie zum Fortfahren auf **Weiter**.

3.5. Schritt 5 - Konfiguration

Hier können Sie Ihr Produkt anpassen.

Einstellungen konfigurieren

Beachten Sie

Dieser Schritt wird nur eingeblendet, wenn Sie als Ansicht für BitDefender die **Experten-Ansicht** gewählt haben.

Hier können Sie die in zwei Kategorien eingeteilten BitDefender-Funktionen aktivieren/deaktivieren.Um den Status einer Einstellung zu ändern, klicken Sie auf den entsprechenden Regler.

- **Sicherheitseinstellungen**

  Hier können Sie die Einstellungen aktivieren bzw. deaktivieren, die die verschiedene Bereiche Ihres Computers und der Datensicherheit betreffen.

Einstellung	Beschreibung
Antivirus	Der Echtzeitschutz gewährleistet, dass alle Dateien gescannt werden, sobald auf sie zugegriffen wird, sei es durch Sie oder eine ausgeführte Anwendung.
Automatisches Update	Durch das Automatische Update werden die aktuellsten BitDefender Produktdateien und Signaturen regelmäßig und automatisch heruntergeladen und installiert.
Schwachstellenprüfung	Die automatische Schwachstellenprüfung gewährleistet, dass wichtige Software auf Ihrem PC stets auf dem neusten Stand ist.
Antispam	Antispam filtert die eingehenden Emails und markiert unerwünschte und Junk-Mails als SPAM.
Antiphishing	Antiphishing alarmiert Sie umgehend in Echtzeit, wenn es entdeckt dass eine Webseite dazu konfiguriert ist, persönliche Informationen zu stehlen.
Identitätskontrolle	Die Identitätskontrolle verhindert, dass persönliche Daten ohne Ihr Einverständnis ins Internet gelangen.

Einstellung	Beschreibung
	Sie blockiert IM-Nachrichten, Email oder Mails, in denen Daten an Dritte gesendet werden können, die Sie als privat kategorisiert haben.
Instant-Messaging-Verschlüsselung	Die IM-Verschlüsselung sichert Ihre Konversationen über Yahoo! Messenger und Windows Live Messenger, vorausgesetzt Ihr Chat-Partner verwendet ebenfalls ein BitDefender-kompatibles Produkt und IM-Software.
Kindersicherung	Die Kindersicherung begrenzt die Rechner- und Online-Aktivitäten Ihrer Kinder, basierend auf den von Ihnen definierten Regeln.Beschränkungen können das Blockieren von unangebrachten Webseiten sowie den Zugriff aus bestimmte Spiele beinhalten und das Internet zeitlich begrenzen.
Firewall	Die Firewall schützt Ihren Computer vor Hackern und schädlichen Angriffen.

- **Allgemeine Einstellungen**

  In diesem Bereich können Sie Einstellungen aktivieren bzw. deaktivieren, die das Produktverhalten und die Nutzung der Software beeinflussen.

Einstellung	Beschreibung
Spiele-Modus	Der Spiele-Modus verändert temporär die Einstellungen so, dass sie die Systemleistung während des Spielens so wenig wie möglich beeinträchtigen.
Laptop-Modus	Der Laptop-Modus verändert temporär die Sicherheitseinstellungen so, dass die Betriebsdauer des Laptop-Akkus so wenig wie möglich beeinträchtigt wird.
Passworteinstellungen	Dies gewährleistet, dass die Einstellungen von BitDefender nur von der Person verändert werden können, die das Passwort kennt. Wenn Sie diese Option aktivieren, werden Sie zur Eingabe des Passwortes aufgefordert.Geben Sie das Passwort in beide Felder ein und klicken Sie auf **OK** um das Passwort festzulegen.

Einstellung	Beschreibung
BitDefender Neuigkeiten	Wenn Sie diese Option aktivieren, erhalten Sie von BitDefender wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.
Produktbenachrichtigungen	Wenn Sie diese Option aktivieren, erhalten Sie Informationsnachrichten.
Scan-Aktivitätsanzeige	Die Aktivitätsanzeige ist ein kleines, transparentes Fenster in dem der Fortschritt der BitDefender Scan-Aktivitäten wird.Weitere Informationen finden Sie unter *„Scan-Aktivitätsanzeige“* (S. 21).
Virenberichte senden	Wenn Sie diese Option aktivieren, werden Virenberichte zur weiteren Analyse an das BitDefender-Team gesendet. Bitte bachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.
Outbreak-Erkennung	Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch an das BitDefender Labor zur weiteren Analysen weitergeleitet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten sollten und nicht für kommerzielle Zwecke verwendet werden.

Klicken Sie auf **Weiter**.

Konfiguration von Meine Werkzeuge

Beachten Sie

Dieser Schritt wird nur eingeblendet, wenn Sie als Ansicht für BitDefender die **Experten-Ansicht** oder **Standard-Ansicht**. gewählt haben.

In **Meine Werkzeuge** können Sie das Dashboard nach Ihren Wünschen anpassen, indem Sie den für Sie wichtigsten Werkzeugen Direktzugriffe zuweisen.So können Sie schnell und einfach auf sie zugreifen.

Von diesem Bildschirm aus können Sie Direktzugriffe für jedes der folgenden Werkzeuge hinzufügen:

- Kindersicherung - überwachen und kontrollieren Sie die Computer-Aktivitäten Ihrer Kinder

- Spiele-Modus - konfigurieren Sie BitDefender so, dass Ihre Spielerlebnis nicht beeinträchtigt wird.
- Der Laptop-Modus verändert temporär die Sicherheitseinstellungen so, dass die Betriebsdauer des Laptop-Akkus so wenig wie möglich beeinträchtigt wird.
- Heimnetzwerk-Verwaltung - verwalten Sie die auf Ihren Computern im Heimnetzwerk installierten BitDefender-Produkte von einem einzigen PC aus.

Wählen Sie die Werkzeuge, die Sie hinzufügen möchten aus, und klicken Sie zum Fortfahren auf **Weiter**.

Aktivierung der Kindersicherung

Beachten Sie

Dieser Schritt wird nur eingeblendet, wenn Sie die Kindersicherung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

Sie können aus drei Optionen auswählen:

- **Kindersicherung für Kinder-Benutzerkonten einrichten**

  Aktivieren Sie diese Option, um die Kindersicherung für die Benutzerkonten Ihrer Kinder zu aktivieren und diese von Ihrem Administrations-Benutzerkonto aus zu verwalten.

- **Kindersicherung für das aktuelle Benutzerkonto einrichten**

  Wählen Sie diese Option, um die Kindersicherungsfunktion für das aktuelle Benutzerkonto zu aktivieren. Dies bedeutet, dass Sie nicht für jedes Kind ein separates Benutzerkonto anlegen müssen, sondern dass die Kindersicherungsregeln für jeden angewendet werden, der dieses Benutzerkonto verwendet.

  In diesem Fall ist ein Passwort notwendig, um die Kindersicherungseinstellungen zu schützen.Sie können dieses jetzt oder zu einem späteren Zeitpunkt im BitDefender-Fenster festlegen.

- **Den Setup vorerst überspringen**

  Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem BitDefender-Fenster aus zu konfigurieren.

Klicken Sie auf **Weiter**.

Heimnetzwerk-Verwaltung

Beachten Sie

Dieser Schritt wird nur eingeblendet, wenn Sie die Heimnetzwerk-Verwaltung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

Sie können aus drei Optionen auswählen:

- **Dieses PC als Server festlegen**

  Aktivieren Sie diese Option, wenn Sie BitDefender-Produkte auf anderen Computern des Heimnetzwerks von diesem Rechner aus verwalten möchten.

  Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

- **Diesen PC als Client festlegen**

  Wählen Sie diese Option, wenn BitDefender von einem anderen Computer im Heimnetzwerk, auf dem BitDefender ebenfalls installiert ist, verwaltet werden soll.

  Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

- **Den Setup vorerst überspringen**

  Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem BitDefender-Fenster aus zu konfigurieren.

Klicken Sie auf **Weiter**.

3.6. Schritt 6 - Support-Optionen

Hier können Sie die Hilfe- und Support-Optionen anpassen:

- **Smart Tipps** aktivieren/deaktivieren.Smart Tipps sind personalisierte Nachrichten, die im BitDefender-Dashboard angezeigt werden und Ihnen helfen, die Leistung Ihres Computers zu verbessern.
- Bestätigen Sie die Email-Adresse, die Sie verwenden möchten, sollten Sie vom BitDefender-Kundendienst kontaktiert werden. Möchten Sie nicht via Email mit dem Kundendienst kommunizieren, wählen Sie die entsprechende Option.

3.7. Schritt 7 - Bestätigung

Hier können Sie die ausgewählten Konfigurationen noch einmal begutachten.

Als Voreinstellung sind zwei Aufgaben geplant:

- Sofort nachdem die Installation abgeschlossen ist, wird ein Vollsystem-Scan durchgeführt.

  Wir empfehlen, diesen umfassenden Scan durchzuführen, durch den jegliche Malware und andere Systembedrohungen festgestellt werden.

- Jeden Sonntag um 02:00 Uhr wird ein vollständiger Scan durchgeführt.

  Wir empfehlen dringend, Ihr System mindestens ein Mal pro Woche zu scannen.Wählen Sie einen anderen Tag und Zeit, falls Sie ein anderes als das

voreingestellte Datum wünschen.Falls der Computer im Moment der geplanten Aufgabe ausgeschaltet ist, wird die Aufgabe beim nächsten Computerstart gestartet.

Klicken Sie auf **Fertigstellen**.

3.8. Schritt 8 - Fertigstellung

Die Installation ist fast abgeschlossen. Die abschließenden Einstellungen werden nun angewandt und ein Update wird durchgeführt.

Der Assistent schließt sich automatisch, wenn die Installation abgeschlossen ist.Ein Vollsystem-Scan wird gestartet, wenn diese Option während des vorherigen Schrittes aktiviert wurde.

Dieser Setup-Assistent erkennt das Netzwerk, mit dem Sie verbunden sind und lässt Sie dieses als Zuhause/Büro oder Öffentlich klassifizieren.

Beachten Sie
Es kann ein Neustart nötig sein.

4. Update von einer älteren BitDefender-Version

Wenn Sie die BitDefender Internet Security 2011-Produktversionen 2011 beta, 2008, 2009 oder 2010 verwenden, können Sie einen Update auf BitDefender Internet Security 2011 durchführen.

Es gibt zwei Möglichkeiten, das Update durchzuführen:

- Installieren Sie BitDefender Internet Security 2011 direkt über die alte Version.Wenn Sie direkt über die 2010er Version installieren, wird die Freunde- und Spammerliste sowie die Quarantäne automatisch importiert.
- Deinstallieren Sie zunächst die Vorgängerversion. Starten Sie dann den Computer neu und installieren Sie die neue Version wie im Abschnitt *„Installation von BitDefender“ (S. 5)* beschrieben.Es werden keinerlei Produkteinstellungen gespeichert.Nutzen Sie diese Update-Methode falls, die andere fehlschlägt.

5. BitDefender reparieren oder entfernen

Wenn Sie BitDefender Internet Security 2011 reparieren oder deinstallieren möchten, öffnen Sie bitte das Windows Startmenü: **Start → Programme → BitDefender 2011 → Reparieren oder Deinstallieren**.

Ein Assistent wird eingeblendet, um Ihnen beim Abschluss der gewünschten Aufgaben zu helfen.

1. **Reparieren oder entfernen**

   Wählen Sie, welche Aktion Sie ausführen möchten:

   - **Reparieren** - um alle Programmkomponenten neu zu installieren.
   - **Entfernen** - dient zum Entfernen aller installierten Komponenten.

   Beachten Sie

   Wir empfehlen die Option **Entfernen**, um eine saubere Neuinstallation durchzuführen.

2. **Aktion bestätigen**

   Bitte lesen Sie sich die eingeblendeten Informationen sorgfältig durch, bevor Sie auf **Weiter** klicken, um so die Aktion zu bestätigen.

3. **Fortschritt**

   Warten Sie, bis BitDefender die von Ihnen ausgewählte Aktion abgeschlossen hat.Dies kann einige Minuten in Anspruch nehmen.

4. **Fertigstellen**

   Die Ergebnisse werden angezeigt.

   Sie müssen Ihren Computer neustarten, um diesen Vorgang abzuschließen. Klicken Sie auf **Neustart**, um Ihren Rechner sofort neuzustarten oder auf **Beenden**, um das Fenster zu schließen und den Neustart später durchzuführen.

Erste Schritte

6. Übersicht

Sobald Sie BitDefender Internet Security 2011 installiert haben, ist Ihr Computer gegen jede Art von Malware (wie beispielsweise Viren, Spyware und Trojaner) und andere Internetbedrohungen (wie Hacker, Phishing und Spam) geschützt.

Sie müssen neben den während der Installation konfigurierten Einstellungen keine weiteren BitDefender-Einstellungen konfigurieren.Sie können jedoch auch die BitDefender-Einstellungen für die Feineinstellung nutzen und Ihren Schutz verbessern.

Von Zeit zu Zeit sollten Sie BitDefender öffnen und existierende Probleme beheben.Es ist möglich, dass-Sie, um Ihren Computer und Ihre Daten zu schützen, bestimmte BitDefender-Komponenten konfigurieren oder vorbeugende Maßnahmen durchführen müssen.Wenn Sie möchten, können Sie BitDefender so konfigurieren, dass Sie bei bestimmten Problemen nicht alarmiert werden.

Falls Sie das Produkt nicht registriert haben (dies beinhaltet auch das Anlegen eines BitDefender Benutzerkontos), sollten Sie dies bis zum Ende der Testzeit tun.Sie müssen innerhalb von 15 Tagen nach der Installation von BitDefender ein Benutzerkonto anlegen (wenn Sie sich mit einem Lizenzschlüssel registriert haben, wird diese Zeit auf 30 Tage verlängert).Ansonsten erhält BitDefender keine automatischen Updates.Weitere Informationen bezüglich der Registrierung finden Sie unter *„Registrierung und My-Account“ (S. 52)*.

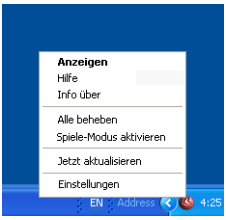
6.1. Öffnen Sie BitDefender

Zugriff auf die Hauptbenutzeroberfläche von BitDefender Internet Security 2011 erhalten Sie über das Windows-Startmenü: **Start → Alle Programme → BitDefender 2011 → BitDefender Internet Security 2011**oder schneller per Doppelklick auf das BitDefender-Symbol in der Systemleiste.

Weitere Informationen zum Haupt-Anwendungsfenster finden Sie unter *„Hauptanwendungs-Fenster“ (S. 25)*.

6.2. System Tray-Symbol

Um das gesamte Produkt schneller zu verwalten, können Sie das BitDefender-Symbol im System-Tray nutzen.Wenn Sie auf dieses Symbol doppelklicken öffnet sich BitDefender. Zudem öffnen Sie durch einen Rechtsklick ein Untermenü das Ihnen ein schnelles Verwalten des BitDefender-Produktes ermöglicht.



Tray Icon

- **Anzeigen** - öffnet die Hauptbedienoberfläche von BitDefender.
- **Hilfe** - öffnet die Hilfedatei, die erklärt, wie man BitDefender Internet Security 2011 konfiguriert und benutzt.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über BitDefender erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.
- **Alle Probleme beheben** - hilft bestehende Sicherheitsschwachstellen zu entfernen.Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme.Weitere Infos finden Sie unter *„Probleme beheben“* (S. 42).
- **Spiele-Modus An / Aus** - aktiviert / deaktiviert den Spiele-Modus.
- **Jetzt aktualisieren** - startet ein sofortiges Update.Ein neues Fenster wird eingeblendet, in dem Sie den Status des Updates sehen können.
- **Einstellungen** - öffnet ein Fenster, in dem Sie die Haupteinstellungen des Produkts aktivieren und deaktivieren oder das Benutzerprofil neu konfigurieren können.Weitere Informationen finden Sie unter *„Konfiguration der Grundeinstellungen“* (S. 45).

Das BitDefender-Symbol in der System Tray informiert Sie über spezielle Symbole, über mögliche Probleme:

Rotes Dreieck mit einem Ausrufezeichen: Kritische Sicherheitsprobleme beeinflussen die Systemsicherheit. Diese benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.
Buchstabe G: Das Produkt arbeitet im Spiele-Modus.

Wenn BitDefender nicht funktioniert, ist das Symbol grau hinterlegt.Dies passiert normalerweise, wenn die Lizenz abgelaufen ist, aber auch, wenn die BitDefender Dienste nicht reagieren oder andere Fehler die normale Funktionsweise von BitDefender einschränken.

6.3. Scan-Aktivitätsanzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung des Scan-Vorgangs.Dieses kleine Fenster steht in der Voreinstellung nur in der Experten-Ansicht zur Verfügung.

Die grauen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50.Die orangen Balken in der **Netz-Zone** zeigen die Anzahl der transferierten KBytes (gesendet und empfangen aus dem Internet) pro Sekunde auf einer Skala von 0 bis 100.

Scan-Aktivitätsanzeige

Beachten Sie
Die Aktivitätsanzeige informiert Sie mit einem roten „X“, wenn der Echtzeitschutz oder die Firewall deaktiviert sind (**Datei-Zone** oder **Netz-Zone**).

6.3.1. Dateien und Verzeichnisse scannen

Sie können die Aktivitätsanzeige verwenden, um schnell Dateien und Verzeichnisse zu scannen.Ziehen Sie die gewünschte Datei über die **Scan-Aktivitätsanzeige**, wie auf den folgenden Bildern dargestellt.

Herüberziehen der Datei

Ablegen der Datei

Der Antivirus Scan-Assistent wird eingeblendet werdenund Sie durch den Scan-Vorgang führen.

Scan-Optionen. Die Scan-Optionen sind für bestmögliche Entdeckungsraten vorkonfiguriert.Falls infizierte Dateien entdeckt werden, wird BitDefender versuchen diese zu desinfizieren (den Malware-Code entfernen). Sollte die Desinfizierung fehlschlagen, wird Ihnen der Antivirus Scan-Assistent andere Möglichkeiten vorschlagen, wie mit den infizierten Dateien verfahren werden kann.Die Scan-Optionen sind standardisiert, sie können daher nicht geändert werden.

6.3.2. Ein-/Ausblenden der Aktivitätsanzeige

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**.Um die Aktivitätsanzeige wiederherzustellen folgen Sie diesen Schritten:

1. Öffnen Sie BitDefender.
2. Klicken Sie in der oberen rechten Bildschirmecke auf **Optionen** und wählen Sie **Einstellungen**
3. Aktivieren Sie in der Kategorie "Allgemeine Einstellungen" das entsprechende Kästchen für die **Scan-Aktivitätsanzeige**.
4. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

6.4. Automatische Geräteerkennung

Wenn ein externes Speichergerät mit dem PC verbunden wird, erkennt BitDefender dies automatisch, und bietet an, es vor dem Zugriff zu zu überprüfen.Dies ist empfohlen, um die Infizierung Ihres Systems mit Viren und anderer Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, wie Flash Sticks und externe Festplatten
- Verbundene (remote) Netzlaufwerke

Wenn solch ein Gerät entdeckt wird, erscheint ein Hinweis.

Um das Speichergerät zu überprüfen, klicken Sie auf **Ja**.Der Antivirus Scan-Assistent wird eingeblendet werdenund Sie durch den Scan-Vorgang führen.

Falls Sie das Gerät nicht prüfen möchten, klicken Sie auf **Nein**. In diesem Fall könnte eine der folgenden Optionen sinnvoll sein:

- **Bei diesem Gerätetyp nicht mehr nachfragen** - BitDefender wird für diesen Gerätetyp keine Prüfung vorschlagen, wenn dieser mir dem PC verbunden wird.
- **Automatische Geräteerkennung deaktivieren** - Sie werden nicht länger aufgefordert, neue Speichergeräte zu prüfen, wenn diese mit dem PC verbunden werden.

Falls Sie die automatische Geräteerkennung versehentlich deaktivieren oder reaktivieren, oder die Einstellungen anpassen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Virus-Scan**.

3. Suchen Sie in der Liste der Scan-Aufgaben die Aufgabe **Geräte-Scan**.
4. Rechtsklicken Sie auf die Aufgabe und wählen Sie **Eigenschaften**.Ein neues Fenster wird geöffnet.
5. Im Reiter **Übersicht** können Sie die Scan-Optionen nach Bedarf konfigurieren.Weitere Informationen finden Sie unter *„Konfiguration der Scan-Einstellungen“* (S. 76).
6. Im Reiter **Erkennung**, wählen Sie, welche Art von Speichergerät erkannt werden soll.
7. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

7. Hauptanwendungs-Fenster

BitDefender Internet Security 2011 ist sowohl für Profis als auch für Computer-Neulinge geeignet. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Sie können die Benutzeroberfläche in einem von 3 Modi darstellen lassen, abhängig von Ihrer Computer Erfahrung und Ihrer Erfahrung mit BitDefender.

Basis-Ansicht

Geeignet für Anfänger und für diejenigen, die BitDefender ohne Aufwand zum Schutz des Computers und der Daten nutzen wollen. Diese Ansicht ist einfach in der Handhabung und verlangt minimalen Aufwand Ihrerseits.

Sie müssen nur dann Probleme beheben, wenn BitDefender Sie dazu auffordert. Ein intuitiver Schritt-für-Schritt Assistent hilft Ihnen dabei.Zusätzlich können Sie normale Aufgaben, Vorgänge wie das Aktualisieren der BitDefender-Virensignaturen und Produktdateien oder den Scan Ihres Computers durchführen.

Standard-Ansicht

Diese Ansicht ist für Benutzer mit durchschnittlichen Computer-Kenntnissen gedacht und erweitert Basis-Ansicht.

Sie können Probleme beheben und entscheiden welche Probleme überwacht werden sollen.Ferner können Sie die auf anderen Computern in Ihrem Haushaltinstallierten BitDefender-Produkte verwalten.

Experten-Ansicht

Gedacht für technisch fortgeschrittene Anwender, erlaubt diese Ansicht jede Funktion von BitDefender zu konfigurieren.Weiterhin können Sie zudem alle Funktionen nutzen, um Ihren Computer und Ihre Daten zu schützen.

Der Ansichtsmodus wird während der Installation gewählt.

Änderung des Ansichtsmodus:

1. Öffnen Sie BitDefender.
2. Klicken Sie in der oberen rechten Bildschirmecke auf den Button **Optionen**.
3. Wählen Sie die gewünschte Ansicht im Menü aus.

7.1. Basis-Ansicht

Wenn Sie ein Computer-Anfänger sind, ist die Basis-Ansicht der Benutzeroberfläche vermutlich die beste Wahl für Sie.Dieser Modus ist einfach zu handhaben und erfordert nur minimale Interaktion Ihrereseits.

Das Fenster ist aufgeteilt in drei Hauptbereiche:

Statusbereich
Die Statusinformation wird auf der linken Bildschirmseite angezeigt.

Der Bereich "Ihren PC schützen"
Hier können Sie die für die Verwaltung Ihres Schutzes notwendigen Aktionen durchführen.

Hilfebereich
Hier können Sie herausfinden, wie Sie BitDefender Internet Security 2011 benutzen und wie Sie Hilfe bekommen können.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters finden Sie einige nützliche Links.

Link	Beschreibung
Lizenzinfo	Öffnet ein Fenster, in dem die aktuellen Lizenzschlüsselinformationen angezeigt werden und in dem aus Sie einen neuen Lizenzschlüssel registrieren können.
Protokolle ansehen	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.
Hilfe und Support	Klicken Sie auf diesen Link, wenn Sie Hilfe zu BitDefender benötigen.
?	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von BitDefender unterstützt.

7.1.1. Statusbereich

Die Statusinformation wird auf der linken Bildschirmseite angezeigt.

- **Sicherheitsstatus** informiert Sie über die Risiken, die die Sicherheit Ihres Systems gefährden und hilft diese zu beheben.Durch Klicken auf **Alle Probleme beheben** wird ein Assistent eingeblendet, der Ihnen helfen wird, die Bedrohungen auf Ihrem PC zu entfernen.Weitere Infos finden Sie unter *„Probleme beheben“ (S. 42)*.
- **Lizenzstatus** zeigt an, wie viele Tage noch verbleiben, bis die Lizenz ausläuft.Wenn Sie eine Testversion verwenden oder Ihre Lizenz bald ausläuft, können Sie auf **Jetzt kaufen** klicken, um so einen Lizenzschlüssel zu erwerben.Weitere Infos finden Sie unter *„Registrierung und My-Account“ (S. 52)*.

7.1.2. Der Bereich "Ihren PC schützen"

Hier können Sie die für die Verwaltung Ihres Schutzes notwendigen Aktionen durchführen.

Drei Buttons stehen zur Verfügung:

- **Sicherheit** bietet Ihnen Verknüpfungen zu Sicherheitsaufgaben und Einstellungen.
- **Jetzt aktualisieren** hilft Ihnen, die Virensignaturen und Produktdateien von BitDefender upzudaten.Ein neues Fenster wird eingeblendet, in dem Sie den Status des Updates sehen können.Wenn neue Updates erkannt werden, werden sie automatisch auf Ihren PC heruntergeladen und installiert.
- In **Meine Werkzeuge** können Sie Verknüpfungen für Ihre favorisierten Aufgaben und Einstellungen definieren.

Um eine Aufgabe auszuführen oder Einstellungen zu konfigurieren, klicken Sie im Menü auf den entsprechenden Button für das gewünschte Werkzeug.Um Verknüpfungen hinzuzufügen oder zu entfernen, klicken Sie auf den entsprechenden Button und wählen Sie **Weitere Optionen**.Weitere Infos finden Sie unter *„Meine Werkzeuge“ (S. 33)*.

7.1.3. Hilfebereich

Hier können Sie herausfinden, wie Sie BitDefender Internet Security 2011 benutzen und wie Sie Hilfe bekommen können.

Smart Tipps sind ein einfacher und unterhaltsamer Weg, mehr über Computer-Sicherheitstechniken und wie BitDefender Internet Security 2011 diese anwendet, herauszufinden.

Falls Sie Hilfe benötigen, tippen Sie im Feld **Hilfe und Support** ein Schlagwort oder eine Frage ein und klicken Sie auf **Suchen**.

7.2. Standard-Ansicht

Die Standard-Ansicht ist für Benutzer mit durchschnittlich guten PC-Kenntnissen ausgelegt, die Oberfläche gibt Ihnen Zugriff auf alle grundlegenden Module. Sie müssen Warnungen und kritische Alarme nachverfolgen und unerwünschte Probleme beheben.

Die Standard-Ansicht ist in mehrere Bereiche unterteilt.

Dashboard
: Das Dashboard hilft Ihnen, Ihren Schutz einfach zu überwachen und zu verwalten.

Sicherheit
: Zeigt den Status der Sicherheitseinstellungen an und hilft Ihnen, festgestellte Probleme zu beheben.Sie können Sicherheitsaufgaben ausführen oder Sicherheitseinstellungen konfigurieren.

Netzwerk
: Zeigt die Struktur des BitDefender Heimnetzwerks an.Hier können Sie verschiedene Aktionen durchführen, um die in Ihrem Heimnetzwerk installierten

BitDefender Produkte, zu konfigurieren und zu verwalten.So können Sie die Sicherheit Ihres Heimnetzwerks von einem einzelnen Computer aus verwalten.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters finden Sie einige nützliche Links.

Link	Beschreibung
Lizenzinfo	Öffnet ein Fenster, in dem die aktuellen Lizenzschlüsselinformationen angezeigt werden und in dem aus Sie einen neuen Lizenzschlüssel registrieren können.
Protokolle ansehen	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.
Kaufen/Verlängern	Unterstützt Sie beim Kauf des Lizenzschlüssels für Ihr BitDefender Internet Security 2011-Produkt.
Hilfe und Support	Klicken Sie auf diesen Link, wenn Sie Hilfe zu BitDefender benötigen.
?	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von BitDefender unterstützt.

7.2.1. Dashboard

Das Dashboard hilft Ihnen, Ihren Schutz einfach zu überwachen und zu verwalten.

Das Dashboard besteht aus folgenden Bereichen:

- **Statusdetails** - zeigt den Status jedes Hauptmoduls, unter Verwendung eindeutiger Sätze und eines der folgenden Symbole:

  Grüner Kreis mit einem Häkchen: Keine Bedrohungen beeinflussen den Sicherheitsstatus.Ihr Rechner und Ihre Daten sind geschützt.

  Roter Kreis mit einem Ausrufezeichen: Bedrohungen beeinflussen die Sicherheit Ihres Systems.Kritische Bedrohungen erfordern Ihre unmittelbare Aufmerksamkeit. Auch die nicht-kritischen Bedrohungen sollte bald näher betrachtet werden.

  Grauer Kreis mit einem Ausrufezeichen: Die Aktivität dieser Modulkomponenten wird nicht überwacht. Daher liegen keine Informationen zum Sicherheitsstatus vor.Es könnten möglicherweise, spezifische Probleme mit diesem Modul existieren.

  Klicken Sie auf den Namen eines Moduls um Einzelheiten zum Status zu erhalten und die Statusüberwachung für diese Komponente zu konfigurieren.

- **Lizenzstatus** zeigt an, wie viele Tage noch verbleiben, bis die Lizenz ausläuft.Wenn Sie eine Testversion verwenden oder Ihre Lizenz bald ausläuft, können Sie auf **Jetzt kaufen** klicken, um so einen Lizenzschlüssel zu erwerben.Weitere Infos finden Sie unter *„Registrierung und My-Account“ (S. 52)*.
- In **Meine Werkzeuge** können Sie Verknüpfungen für Ihre favorisierten Aufgaben und Einstellungen definieren.Weitere Infos finden Sie unter *„Meine Werkzeuge“ (S. 33)*.
- **Smart Tipps** sind ein einfacher und unterhaltsamer Weg, mehr über Computer-Sicherheitstechniken und wie BitDefender Internet Security 2011 diese anwendet, herauszufinden.

7.2.2. Sicherheit

Über den Reiter "Sicherheit" können Sie die Sicherheit Ihres Computers und Ihrer Daten verwalten.

„Statusbereich“ (S. 29)
„Quick Tasks“ (S. 30)

Statusbereich

Im Statusbereich finden Sie die vollständige Liste der überwachten Sicherheitskomponenten und deren aktuellen Status sehen.Durch die Überwachung jedes Sicherheitsmoduls wird BitDefender Sie nicht nur darüber informieren, wenn Sie Einstellungen vornehmen, die die Sicherheit Ihres Computers beeinträchtigenkönnen. Sondern auch, wenn wichtige Aufgaben vergessen wurden.

Der aktuelle Status einer Komponente wird durch eindeutige Sätze und eines der folgenden Symbole angezeigt:

Grüner Kreis mit einem Häkchen: Keine Bedrohungen gefährden Ihren Computer.
Roter Kreis mit einem Ausrufezeichen: Bedrohungen gefährden Ihren Computer.

Klicken Sie auf **Beheben**, um das jeweilige Problem zu beheben.Sollte ein Problem nicht direkt behoben werden können, dann folgen Sie dem Assistent.

Um zu konfigurieren, welche Komponenten überwacht werden sollen:

1. Klicken Sie auf **Liste hinzufügen/bearbeiten**.
2. Um die Überwachung für einen bestimmten Eintrag ein- oder auszuschalten, verwenden Sie diesen Schalter.
3. Klicken Sie auf **Schließen**, um die Änderungen zu speichern und das Fenster zu schließen.

Wichtig
Um zu gewährleisten, dass Ihr System vollständig gesichert ist, aktivieren Sie bitte das Tracking „für alle Komponenten und alle gemeldeten Probleme reparieren“.

Quick Tasks

Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben:

- **Jetzt aktualisieren** - startet ein sofortiges Update.
- **Vollsystem-Scan** - startet einen Standard-Scan Ihres Systems (exklusive Archive). Weitere On-Demand-Scans finden Sie, wenn Sie auf den Pfeil dieses Buttons klicken und dann eine andere Scan-Aufgabe wählen.
- **Benutzerdefinierter Scan** - startet einen Assistenten, mit dem Sie einen individuellen Scan erstellen und starten können.
- **Schwachstellenprüfung** - startet einen Assistenten der Ihnen beim Finden und Beheben von Schwachstellen in Ihrem System behilflich ist.
- **Firewall konfigurieren** - öffnet ein Fenster, in dem Sie die Firewall-Einstellungen einsehen und konfigurieren können.Weitere Informationen finden Sie unter „*Firewall*“ (S. 132).

7.2.3. Netzwerk

Hier können Sie verschiedene Aktionen durchführen, um die in Ihrem Heimnetzwerk installierten BitDefender Produkte, zu konfigurieren und zu verwalten.So können Sie die Sicherheit Ihres Heimnetzwerks von einem einzelnen Computer aus verwalten.

Weitere Infos finden Sie unter „*Heimnetzwerk*“ (S. 156).

7.3. Experten-Ansicht

Die Experten-Ansicht gibt Ihnen Zugriff auf jede einzelne Komponente von BitDefender. Hier können Sie BitDefender im Einzelnen konfigurieren.

Beachten Sie
Die Experten-Ansicht ist für Anwender geeignet, die über sehr gute PC-Kenntnisse verfügen, die umfassende Kenntnisse über existierende PC-Bedrohungen haben und wissen, wie ein Sicherheitsprogramm arbeitet.

Auf der linken Seite des Fensters sehen Sie ein Menü, mit allen Sicherheitsmodulen.Jedes Modul verfügt über einen oder mehrere Reiter über die in Sie die dazugehörigen Sicherheitseinstellungen konfigurieren oder Sicherheits- und Administrativ aufgaben durchführen können.Die folgende Auflistung beschreibt in Kürze jedes Modul.Weitere Infos finden Sie unter „Konfiguration und Verwaltung“ (S. 56) diesen Teil des Benutzerhandbuchs.

Allgemein
Hier haben Sie Zugriff auf die allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen einsehen.

Antivirus
Bietet Ihnen die Möglichkeit, Ihren Virus-Schild und Scan-Vorgänge zu konfigurieren, Ausnahmen festzulegen und das Quarantäne-Modul zu konfigurieren.Hier können Sie auch die Funktionen Antiphishing-Schutz und Search Advisor konfigurieren.

Antispam
Bietet Ihnen die Möglichkeit, Ihr Postfach SPAM-frei zu halten und die Antispam-Einstellungen detailliert zu konfigurieren.

Kindersicherung
Bietet Ihnen die Möglichkeit, Ihre Kinder gegen jugendgefährdende Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

Einstellungen zur Privatsphäre
Bietet Ihnen die Möglichkeit Datendiebstahl von Ihrem Computer vorzubeugen und Ihre Privatsphäre zu schützen während Sie online sind.

Firewall
Erlaubt es Ihnen, Ihren Computer gegen unerlaubte Zugriffe von außen und innen zu schützen. Ähnlich einem Türsteher wird die Firewall ein wachsames Auge auf Ihre Internetverbindung haben und beobachten, wem der Zugriff auf das Internet erlaubt wird und wem nicht.

Schwachstellen
Bietet Ihnen die Möglichkeit wichtige Software auf Ihrem PC stets auf dem neusten Stand zu halten.

Verschlüsselung
Bietet Ihnen die Möglichkeit Unterhaltungen über Yahoo und Windows Live (MSN) Messenger zu verschlüsseln.

Spiele/Laptop-Modus
Bietet Ihnen die Möglichkeit, voreingestellte Scan BitDefender Aufgaben zu verschieben, wenn Ihr Laptop im Akkubetrieb ist. Zudem werden während des Spielbetriebs keine Pop-Up-Fenster und andere Benachrichtigungen eingeblendet.

Heimnetzwerk
Bietet Ihnen die Möglichkeit, mehrere Computer in Ihrem Haushalt zu verwalten und zu konfigurieren.

Update
Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.

Registrierung
Lässt Sie BitDefender Internet Security 2011 registrieren, den Lizenzschlüssel wechseln oder ein BitDefender Benutzerkonto erstellen.

Über den Button **Optionen** in der rechten oberen Bildschirmecke können Sie die Ansicht ändern und die Hauptprogramm-Einstellungen konfigurieren.

In der rechten unteren Ecke des Fensters finden Sie einige nützliche Links.

Link	Beschreibung
Lizenzinfo	Öffnet ein Fenster, in dem die aktuellen Lizenzschlüsselinformationen angezeigt werden und in dem aus Sie einen neuen Lizenzschlüssel registrieren können.
Protokolle ansehen	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.
Kaufen/Verlängern	Unterstützt Sie beim Kauf des Lizenzschlüssels für Ihr BitDefender Internet Security 2011-Produkt.
Hilfe und Support	Klicken Sie auf diesen Link, wenn Sie Hilfe zu BitDefender benötigen.
?	Gibt Ihnen Zugriff auf eine Hilfedatei, die Sie bei der Verwendung von BitDefender unterstützt.

8. Meine Werkzeuge

Wenn Sie BitDefender in der Basis- oder Standard-Ansicht verwenden, können Sie Ihr Dashboard anpassen, indem Sie wichtigen Aufgaben und Einstellungen Verknüpfungen zuweisen.Auf diese Weise erhalten Sie schnell Zugriff auf die Funktionen, die Sie regelmäßig nutzen und auf die Erweiterten Einstellungen, ohne dabei in eine andere Ansicht wechseln zu müssen.

Abhängig von der gewählten Ansicht stehen die dem Bereich "Meine Werkzeuge" hinzugefügten Verknüpfungen wie folgt zur Verfügung:

Basis-Ansicht
: Klicken Sie im Bereich "PC schützen" auf "Meine Werkzeuge".Ein neues Menü wird eingeblendet.Klicken Sie auf die Verknüpfung des entsprechenden Werkzeugs, um dieses aufzurufen.

Standard-Ansicht
: Die Verknüpfungen werden unter "Meine Werkzeuge" angezeigt.Klicken Sie auf die Verknüpfung des entsprechenden Werkzeugs, um dieses aufzurufen.

Um das Fenster zu öffnen, in dem Sie die Verknüpfungen auswählen können, die im Bereich "Meine Werkzeuge" angezeigt werden, gehen Sie folgendermaßen vor:

Basis-Ansicht
: Klicken Sie im Bereich "Ihren PC schützen" auf "Meine Werkzeuge" und dann auf **Weitere Optionen**.

Standard-Ansicht
: Klicken Sie im Bereich "Meine Werkzeuge" auf einen der Buttons oder auf den Link **Meine Werkzeuge konfigurieren**.

Über die Schalter können Sie wählen, welche Werkzeuge dem Bereich "Meine Werkzeuge" hinzugefügt werden sollen.Sie können jede der folgenden Werkzeugkategorien auswählen.

- **Scan-Aufgaben**

  Fügen Sie die Aufgaben, die Sie regelmäßig anwenden, um Ihr System auf Sicherheitsbedrohungen zu scannen, hinzu.

Prüfaufgabe	Beschreibung
Tiefensystem-Scan	Scannt das komplette System.In der Voreinstellung wird auf alle Arten von Bedrohungen gescannt, wie z.B. Viren, Spyware, Adware, Rootkits etc.
Vollsystem-Scan	Scannt alle Dateien mit Ausnahme von Archiven.In der Standardkonfiguration, wird nach allen Arten von Malware mit Ausnahme von Rootkits gescannt.

Prüfaufgabe	Beschreibung
Quick Scan	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 Virenscan in Anspruch nehmen würde.
Prüfung anpassen	Startet einen Assistenten, mit dem Sie eine benutzerdefinierte Aufgabe erstellen können.
Scan des Verzeichnisses „Meine Dokumente“	Verwenden Sie diese Aufgaben, um die folgenden für den jeweiligen Benutzer Verzeichnisse zu scannen: `Eigene Dateien`, `Desktop` und `Autostart`. Dadurch wird die sichergestellt, dass Ihre eigenen Daten, ein sicherer Arbeitsplatz sowie eine saubere Ausführung der Anwendungen beim Systemstart gewährleistet.
"Meine Aufgaben" planen	Leitet Sie in das Fenster mit den Antiviren-Einstellungen weiter, in dem Sie die On-Demand Scan-Aufgaben anpassen können.

Weitere Informationen über Scan-Aufgaben finden Sie unter *„Verwaltung der existierenden Scan-Aufgaben“* (S. 73).

- **Einstellungen**

  Weisen Sie den BitDefender-Einstellungen, die Sie konfigurieren möchten, Tastaturkürzel zu.

Einstellungen	Beschreibung
Antivirus Einstellungen	Konfigurieren Sie das Antiviren-Modul. Weitere Informationen finden Sie unter *„Antivirus-Schutz“* (S. 61).
Firewall konfigurieren	Konfigurieren Sie die Firewall-Modul. Weitere Informationen finden Sie unter *„Firewall“* (S. 132).
Kindersicherung	Konfigurieren Sie die Kindersicherung. Weitere Informationen finden Sie unter *„Kindersicherung“* (S. 104).
Spiele-Modus	Ein-/Ausschalten des Spiele-Modus. Weitere Informationen finden Sie unter *„Spiele-Modus“* (S. 150).

Einstellungen	Beschreibung
Laptop-Modus	Ein-/Ausschalten des Laptop-Modus. Weitere Informationen finden Sie unter „*Laptop-Modus*“ (S. 153).
Jetzt aktualisieren	Auslösen eines Updates von BitDefender. Weitere Informationen finden Sie unter „*Update*“ (S. 160).
Anzeigen & Alle Probleme beheben	Öffnen einen Assistenten, der Ihnen hilft, alle Sicherheitsprobleme, die Ihr System beeinträchtigen, zu beheben. Weitere Informationen finden Sie unter „*Probleme beheben*“ (S. 42).

- **Hilfe & Support**

  Betreten Sie den Support-Bereich. Weitere Informationen finden Sie unter „Kontaktieren Sie uns direkt aus Ihrem BitDefender-Produkt“ (S. 207).

9. Warnhinweise und Pop-Ups

BitDefender verwendet Pop-Ups-Fenster und Warnungen, um Sie über Aktionen oder besondere Vorkommnisse zu informieren und fordert Sie zu notwendigen Aktionen auf.In diesem Kapitel werden die BitDefender-Pop-Ups und Warnungen, die eingeblendet werden können, erläutert.

Pop-ups sind kleine Fenster, die hin und wieder auf dem Bildschirm erscheinen, um Sie über verschiedene BitDefender-Ereignisse zu informieren, so wie die Überprüfung von Emails, einen neuer Computer der sich in Ihr kabelloses Netzwerk einloggt, eine neue Firewall-Regel, usw.Wenn Pop-ups eingeblendet werden, werden Sie meistens aufgefordert, auf **OK** oder einen Link zu klicken.

Warnungen sind große Fenster, die Sie zu einer Handlung auffordern oder Sie über etwas Wichtiges (beispielsweise, dass ein Virus gefunden wurde) informieren.Neben Warnhinweisfenstern erhalten Sie unter Umständen Warnhinweise zu Emails, Instant Messages oder Internetseiten.

Die BitDefender Pop-Ups und Warnungen beinhalten:

- Antivirus-Warnhinweise
- Active Virus Control-Warnungen
- Geräte-Entdeckungsbenachrichtigung
- Firewall Pop-Ups und Warnhinweise
- Antiphishing Warn-seiten
- Warnhinweise Kindersicherung
- Warnhinweise Privatsphäre-Einstellungen

9.1. Antivirus-Warnhinweise

BitDefender schützt Sie vor allen Arten von Malware (wie Viren, Trojaner, Spyware, Rootkits usw.).Wenn BitDefender einen Virus oder andere Malware entdeckt, führt die Software mit der infizierten Datei spezifische Aktionen durch und informiert Sie darüber in einem Warnhinweisfenster.

Sie sehen den Namen des Virus, den Pfad der infizierten Datei und die Aktion, die BitDefender ausführt.

Klicken Sie auf **OK**, um dieses Fenster zu schließen.

Wichtig

Wenn ein Virus gefunden wurde, ist es am sinnvollsten, den gesamten Computer zu scannen, um sicherzugehen, dass keine weitere Viren vorhanden sind.Weitere Informationen finden Sie unter *„Wie kann ich Dateien und Verzeichnisse scannen?“* (S. 165).
Wurde der Virus nicht blockiert, siehe *„Malware von Ihrem System entfernen“* (S. 196).

9.2. Active Virus Control-Warnungen

Active Virus Control kann so konfiguriert werden, dass Sie informiert werden, wenn eine Anwendung versucht, eine möglicherweise schädliche Aktion durchzuführen.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, informiert Sie ein Pop-Up, wenn die Active Virus Control eine potentiell schädliche Anwendung blockiert hat.Wenn Sie die Experten-Ansicht nutzen, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine Anwendung Anzeichen einer Malware-Infektion zeigt.

Wenn Sie die entdeckte Anwendung kennen und ihr trauen, klicken Sie auf **Erlauben**.

Wenn Sie die Anwendung unverzüglich beenden möchten, klicken Sie auf **OK**.

Wählen Sie **Diese Aktion für diese Anwendung merken** aus, bevor Sie Ihre Wahl treffen, und BitDefender wird die gleiche Aktion für die entdeckte Anwendung auch in Zukunft ausführen.Die Regel, die erstellt wird, wird im Fenster der Active Virus Control gelistet.

9.3. Geräte-Entdeckungsbenachrichtigung

Wenn ein externes Speichergerät mit dem PC verbunden wird, erkennt BitDefender dies automatisch, und bietet an, es vor dem Zugriff zu zu überprüfen.Dies ist empfohlen, um die Infizierung Ihres Systems mit Viren und anderer Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, wie Flash Sticks und externe Festplatten
- Verbundene (remote) Netzlaufwerke

Wenn solch ein Gerät entdeckt wird, erscheint ein Hinweis.

Um das Speichergerät zu überprüfen, klicken Sie auf **Ja**.Der Antivirus Scan-Assistent wird eingeblendet werden und Sie durch den Scan-Vorgang führen.

Falls Sie das Gerät nicht prüfen möchten, klicken Sie auf **Nein**. In diesem Fall könnte eine der folgenden Optionen sinnvoll sein:

- **Bei diesem Gerätetyp nicht mehr nachfragen** - BitDefender wird für diesen Gerätetyp keine Prüfung vorschlagen, wenn dieser mir dem PC verbunden wird.
- **Automatische Geräteerkennung deaktivieren** - Sie werden nicht länger aufgefordert, neue Speichergeräte zu prüfen, wenn diese mit dem PC verbunden werden.

Falls Sie die automatische Geräteerkennung versehentlich deaktivieren oder reaktivieren, oder die Einstellungen anpassen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Virus-Scan**.
3. Suchen Sie in der Liste der Scan-Aufgaben die Aufgabe **Geräte-Scan**.
4. Rechtsklicken Sie auf die Aufgabe und wählen Sie **Eigenschaften**.Ein neues Fenster wird geöffnet.
5. Im Reiter **Übersicht** können Sie die Scan-Optionen nach Bedarf konfigurieren.Weitere Informationen finden Sie unter *„Konfiguration der Scan-Einstellungen“ (S. 76)*.
6. Im Reiter **Erkennung**, wählen Sie, welche Art von Speichergerät erkannt werden soll.
7. Klicken Sie **OK**, um die Änderungen zu speichern und zu übernehmen.

9.4. Firewall Pop-Ups und Warnhinweise

Die Firewall verwendet Pop-Ups, um Sie über die unterschiedlichen mit Ihrer Netzwerkverbindung zusammenhängenden Ereignisse zu informieren (beispielsweise, wenn sich ein neuer Computer in das WiFi-Netzwerk eingeloggt hat, wenn eine neue Anwendung auf das Internet zugreifen darf oder wenn ein Port-Scan blockiert ist).Diese Pop-Ups sind sehr nützlich, um Einbruchversuche aufzuspüren und sich gegen Netzwerkbedrohungen zu schützen.

Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Sie können folgendes sehen: die Anwendung, die versucht, auf das Internet zuzugreifen, den Anwendung spfad, den Zielort, das verwendete Protokoll und der Port, über den die Applikation versucht die Verbindung herzustellen.

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellte Protokoll zu erlauben (eingehend und ausgehend). Wenn Sie **Blockieren**wählen, wird der Zugriff entsprechend blockiert.

Wichtig
Erlauben Sie eingehende Verbindungen nur von IP-Adressen oder Internet-Domänen, denen Sie wirklich vertrauen.

Basierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen, wird die Regeln automatisch angewendet.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, wird der Verbindungsaufbau automatisch blockiert.

9.5. Antiphishing-Warnhinweise

Mit aktiviertem Antiphishing-Schutz alarmiert BitDefender Sie, wenn Sie versuchen, auf Webseiten zuzugreifen, die eingerichtet wurden, um persönliche Information zu stehlen.Bevor Sie auf solch eine Webseite zugreifen können, wird BitDefender diese Seite blockieren und ein allgemeines Webseiten-Alarmsignal zeigen:

Überprüfen Sie die Adresse der Webseite in der Adresszeile Ihres Browsers.Suchen Sie nach Hinweisen, die anzeigen könnten, dass die Webseite für Phishing verwendet wird.Wenn die Webseite verdächtigt ist, empfehlen wir diese nicht zu öffnen.

Anbei einige nützliche Tipps:

- Wenn Sie die Adresse einer legitimen Website eingetippt haben, überprüfen Sie, ob die Adresse richtig ist. Wenn die Adresse falsch ist, tippen Sie die Adresse erneut ein und greifen Sie erneut auf die Webseite zu.
- Wenn Sie auf einen Link in einer Email oder einer Instant Message geklickt haben, prüfen Sie nach, wer der Absender war. Wenn Ihnen der Absender unbekannt ist, handelt es sich möglicherweise um einen Phishing-Versuch. Wenn Sie den Absender kennen, sollten Sie überprüfen, ob diese Person Ihnen wirklich den Link gesendet hat.
- Falls Sie über eine Internetsuchanfragee Suche auf die Seite gelangt sind, überprüfen Sie die Webseite auf der Sie den Link gefunden haben (indem Sie im Browser auf „Zurück“ klicken).

Falls Sie sich die Webseite ansehen möchten, klicken Sie auf den entsprechenden Link, um eine dieser Aktion durchzuführen.

- **Internetseite einmalig betrachten.** Es existiert kein Risiko solange Sie auf der Webseite keine Informationen angeben.Falls die Seite seriös ist, können Sie diese der White List hinzufügen (klicken Sie auf die BitDefender Antiphishing-Symbolleiste und wählen Sie **Der White List hinzufügen**).
- **Fügen Sie die Internetseite der White List hinzu.** Die Seite wird sofort angezeigt und BitDefender wird sie nicht länger beanstanden.

Wichtig

Fügen Sie der White List ausschließlich Seiten hinzu, denen Sie vollkommen vertrauen (z.B.: der Homepage Ihrer Hausbank, Ihnen bekannte Online-shops, usw.)BitDefender wird die Seiten der White List nicht auf Phishing prüfen.

Der Antiphishing-Schutz und die White List können über die BitDefender-Toolbar Ihres Webbrowsers verwaltet werden.Weitere Informationen finden Sie unter *„Handhabung des BitDefender Antiphishing-Schutzes in Internet Explorer und Firefox“* (S. 87).

9.6. Warnhinweise Kindersicherung

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Der Internetzugang zu bestimmten Zeiten (beispielsweise während der Schule).
- Webseiten, Mails und Instant Messaging-Nachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat oder Filesharing-Programme.
- Instant Messages, die nicht von erlaubten IM-Kontakten gesendet werden.

Der Benutzer wird mittels einer Warnmeldung (z. B. einer Standardwarn-Webseite, Email oder Instant Message)informiert, wenn eine Aktivität blockiert wurde.Detaillierte Informationen begründen, wieso die Aktivität geblockt wurde.

9.7. Warnhinweise Privatsphäre-Einstellungen

Die Privatsphärekontrolle bietet erfahrenen Benutzern einige Extrafunktionen, um die Privatsphäre zu schützen.Anhand von spezifischen Warnhinweisfenstern werden Sie zu Aktionen aufgefordert, falls Sie eine der folgenden Komponenten aktivieren:

- Registry-Kontrolle - fragt immer um Erlaubnis, wenn ein Programm versucht die Registry zu ändern, um beim Windows Neustart ausgeführt zu werden.
- Cookie-Kontrolle - fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle - fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu aktivieren.

9.7.1. Registry-Alarme.

Wenn Sie die Registry Control aktivieren, werden Sie immer um Erlaubnis gefragt, wenn ein neues Programm versucht, einen Registry-Eintrag zu ändern, um beim Windows-Neustart ausgeführt zu werden.

Sie können das Programm sehen, das versucht die Windows-Registry zu modifizieren.

Beachten Sie

BitDefender wird Sie bei der Installation neuer Programme informieren, wenn ein automatisches Starten nach der Windows-Anmeldung erforderlich ist. In den meisten Fällen sind diese Programme legal und Sie können ihnen vertrauen.

Wenn Sie das Programm nicht kennen und es Ihnen verdächtig erscheint, klicken Sie auf **Blockieren** um es davon abzuhalten die Windows-Registry zu verändern.Klicken Sie anderenfalls auf **Erlauben** um die Veränderung zuzulassen.

Je nach Ihrer Auswahl wird eine Regel erstellt und in der Regeltabelle aufgelistet.Dieselbe Aktion wird immer ausgeführt wenn diese Anwendung versucht einen Registry-Eintrag zu ändern.

Weitere Informationen finden Sie unter *„Registry Control“ (S. 128)*.

9.7.2. Skript-Alarme

Wenn Sie die Funktion "Skript-Kontrolle" aktivieren, wird immer eine Anfrage an Sie gerichtet, wenn eine neue Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu verankern.

Der Namen der Quelle wird Ihnen angezeigt.

Klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Tabelle gelistet.Jedes Mal, wenn die entsprechende Seite versucht, aktive Inhalte auszuführen, wird automatisch dieselbe Aktion angewendet.

Beachten Sie
Einige Webseiten können nicht vollständig angezeigt werden, wenn Sie den aktiven Inhalt blockieren.

Weitere Informationen finden Sie unter *„Skript-Kontrolle“ (S. 130)*.

9.7.3. Cookie-Alarme

Wenn Sie die Cookie-Kontrolle aktivieren, werden Sie jedes Mal, wenn eine neue Webseite versucht, einen Cookie zu speichern oder diesen abzufragen, um Ihre Erlaubnis gebeten.

Der Name des Programms, das versucht einen Cookie zu senden, wird Ihnen angezeigt.

Klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Tabelle gelistet.Wenn Sie auf die entsprechende Webseite zugreifen, wird immer dieselbe Aktion automatisch ausgeführt.

Weitere Informationen finden Sie unter *„Cookie-Kontrolle“ (S. 128)*.

10. Probleme beheben

BitDefender verwendet ein Problem-Tracking-System, um sicherheitsgefährdende Probleme festzustellen und Sie über diese zu informieren. Standardmäßig werden nur die wichtigsten Bereiche überwacht. Sie können es jedoch so konfigurieren, dass Sie über die von Ihnen gewählten Probleme benachrichtigt werden.

So werden Sie über latente Bedrohungen benachrichtigt:

- Ein besonderes Symbol wird über dem BitDefender-Symbol in der Systemleiste angezeigt, um auf latente Probleme hinzuweisen.Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Problem existiert.
- Wenn Sie BitDefender öffnen, wird im Bereich Sicherheitsstatus die Anzahl der offenen Probleme angezeigt.
  - In der Basis-Ansicht wird der Sicherheitsstatus auf der linken Bildschirmseite angezeigt.
  - Gehen Sie in der Experten-Ansicht auf **Allgemein > Dashboard**, um den Sicherheitsstatus zu überprüfen.

10.1. Fehlersuche-Assistent

Der einfachste Weg existierende Probleme zu beseitigen, ist Schritt für Schritt dem **Problemlösungs-Assistent** zu folgen.Um den Assistenten zu öffnen, haben Sie folgende Möglichkeiten:

- Rechtsklicken Sie im System Tray auf das BitDefender-Symbol und wählen Sie **Basiseinstellungen**.
- Öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:
  - Klicken Sie in der Basis-Ansicht auf **Alle Probleme anzeigen**.
  - Gehen Sie in der Experten-Ansicht auf **Allgemein>Dashboard** und klicken Sie auf **Alle Probleme anzeigen**.

Beachten Sie
Im Bereich Meine Werkzeuge können Sie eine Verknüpfung hinzufügen.

Eine Liste von existierenden Sicherheitsbedrohungen wird angezeigt.

Alle aktuellen Probleme sind zum Beheben ausgewählt. Wenn es ein Problem gibt, dass nicht behoben werden soll, heben Sie einfach die entsprechende Markierung auf. Der Status wechselt dann auf **Überspringen**.

Beachten Sie

Falls Sie über bestimmte Probleme nicht benachrichtigt werden möchten, müssen Sie das Überwachungssystem wie im nächsten Abschnitt beschrieben, konfigurieren.

Um die ausgewählten Bedrohungen zu beheben, klicken Sie auf **Beheben**. Einige Bedrohungen werden sofort behoben bei anderen, hilft Ihnen ein Assistent bei der Lösung.

Die Risiken die Ihnen dieser Assistent hilft zu beheben, können in diese Hauptkategorien eingeordnet werden

- **Deaktivierte Sicherheitseinstellungen.** Diese Probleme werden sofort durch die entsprechenden Sicherheitseinstellungen behoben.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Ein Beispiel für eine solche Aufgabe ist der Scan Ihres PCs. Es ist empfohlen, diesen scan mindestens einmal wöchentlich durchzuführen. In den meisten Fällen erledigt BitDefender dies automatisch. Falls Sie die Scan-Planung verändert haben oder diese nicht vollständig ist, so werden Sie darüber informiert.

  Bei der Beseitigung dieser Probleme, hilft Ihnen ein Assistent.
- **Systemschwachstellen.** BitDefender überprüft Ihr System automatisch auf Schwachstellen und informiert Sie über diese.Zu den möglichen Systemschwachstellen gehören folgende:
  - Unsichere Passwörter für Windows Benutzerkonten.
  - Veraltete Software auf Ihrem PC.
  - Fehlende Windows-Updates.
  - Deaktivierung des Automatischen Windows Update.

  Wenn solche Probleme beseitigt werden sollen, wird der Schwachstellen Scan-Assistent geöffnet. Der Assistent hilft Ihnen bei der Beseitigung der entdeckten Schwachstellen.Weitere Infos finden Sie unter *„Auf Schwachstellen scannen“ (S. 145)*.

10.2. Status-Warnmeldungen konfigurieren

Das Statuswarnsystem ist so vorkonfiguriert, dass die wichtigsten Sicherheitsrisiken für Ihr Systems und Ihre Daten überwacht und Sie darüber informiert werden.Neben überwachten Standardproblemen, gibt es weitere, über die Sie sich informieren lassen können.

Sie können das Warnsystem ganz nach Ihren individuellen Ansprüchen konfigurieren, indem Sie wählen, über welche Ereignisse Sie informiert werden möchten.Sie können dies sowohl in der Standard- als auch der Experten-Ansicht tun.

- In der Standard-Ansicht kann das Warnsystem von verschiedenen Stellen aus konfiguriert werden.Gehen Sie folgendermaßen vor:

1. Gehen Sie auf den Reiter **Sicherheit**.
2. Klicken Sie im Statusbereich auf den Link **Liste hinzufügen/bearbeiten**.
3. Verwenden Sie den entsprechenden Schalter, um dessen Warnstatus zu ändern.

- In der Experten-Ansicht kann das Warnsystem zentral konfiguriert werden. Gehen Sie folgendermaßen vor:Gehen Sie folgendermaßen vor:
  1. Gehen Sie auf **Allgemein>Dashboard**.
  2. Klicken Sie auf **Warnungen hinzufügen/bearbeiten**.
  3. Verwenden Sie den entsprechenden Schalter, um dessen Warnstatus zu ändern.

11. Konfiguration der Grundeinstellungen

Sie können die Haupteinstellungen des Produkts (einschließlich der Benutzeransicht) im Fenster "Grundeinstellungen" konfigurieren. Um dieses zu öffnen, gehen Sie folgendermaßen vor:

- Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Präferenzen**.
- Rechtsklicken Sie in der Systemleiste auf das BitDefender-Symbol und wählen Sie **Präferenzen**.

Beachten Sie

Um die Produkteinstellungen im Detail zu konfigurieren, benutzen Sie die Experten-Ansicht.Weitere Infos finden Sie unter „Konfiguration und Verwaltung“ (S. 56) diesen Teil des Benutzerhandbuchs.

Die Einstellungen sind in drei Gruppen unterteilt:

- Sicherheitseinstellungen
- Alarmeinstellungen
- Allgemeine Einstellungen

Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

Um die Änderungen anzuwenden und zu sichern, klicken Sie **OK**. Um das Fenster zu schließen ohne die Änderungen zu übernehmen, wählen Sie **Abbrechen**.

Der Link **Neukonfiguration Benutzerprofil** in der linken oberen Bildschirmecke ermöglicht eine Neukonfiguration des Nutzungsprofils.Weitere Informationen finden Sie unter *„Neukonfiguration des Benutzerprofils“* (S. 49).

11.1. Sicherheitseinstellungen

Hier können Sie die Einstellungen aktivieren bzw. deaktivieren, die die verschiedene Bereiche Ihres Computers und der Datensicherheit betreffen.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

Warnung

Wir raten Ihnen zur Vorsicht wenn Sie den Echtzeitschutz, die Firewall oder das automatische Update deaktivieren.Diese Funktionen zu deaktivieren kann die Sicherheit Ihres Computers gefährden. Falls sie wirklich einmal deaktiviert werden müssen, vergessen Sie nicht sie so bald wie möglich wieder zu aktivieren.

Dieses sind die verfügbaren Einstellungen:

Antivirus
Der Echtzeitschutz gewährleistet, dass alle Dateien gescannt werden, sobald auf sie zugegriffen wird, sei es durch Sie oder eine ausgeführte Anwendung.

Automatisches Update
Durch das Automatische Update werden die aktuellsten BitDefender Produktdateien und Signaturen regelmäßig und automatisch heruntergeladen und installiert.Als Voreinstellungen werden die Updates stündlich durchgeführt.

Schwachstellen-Scan
Der Automatische Schwachstellen-Scan informiert Sie über eventuelleSystemschwachstellen und wie diese zu beheben sind. Zu solchen Schwachstellen gehören veraltete Software, unsichere Passwörter für Benutzerkonten oder fehlende Windows-Updates.

Antispam
Antispam filtert die eingehenden Emails und markiert unerwünschte und Junk-Mails als SPAM.

Antiphishing
Antiphishing alarmiert Sie umgehend in Echtzeit, wenn es entdeckt dass eine Webseite dazu konfiguriert ist, persönliche Informationen zu stehlen.

Search Advisor
Der Search Advisor scannt die Links Ihrer Suchergebnisse in Suchmaschinen und informiert Sie, welche Links sicher sind und welche nicht.

Identitätskontrolle
Die Identitätskontrolle verhindert, dass persönliche Daten ohne Ihr Einverständnis ins Internet gelangen. Sie blockiert IM-Nachrichten, Email oder Mails, in denen Daten an Dritte gesendet werden können, die Sie als privat kategorisiert haben.

Instant-Messaging-Verschlüsselung
Die IM-Verschlüsselung sichert Ihre Konversationen über Yahoo! Messenger und Windows Live Messenger, vorausgesetzt Ihr Chat-Partner verwendet ebenfalls ein BitDefender-kompatibles Produkt und IM-Software.

Kindersicherung (aktueller Benutzer)
Die Kindersicherung begrenzt die Rechner- und Online-Aktivitäten Ihrer Kinder, basierend auf den von Ihnen definierten Regeln.Beschränkungen können das Blockieren von unangebrachten Webseiten sowie den Zugriff aus bestimmte Spiele beinhalten und das Internet zeitlich begrenzen.

Firewall
Die Firewall schützt Ihren Computer vor Hackern und schädlichen Angriffen.

Der Status von einigen dieser Einstellungen kann durch das BitDefender Tracking-System überwacht werden.Wenn Sie eine überwachte Einstellung deaktivieren, zeigt BitDefender dieses als Risiko an, das Sie beheben müssen.

Wenn Sie nicht wollen, dass eine überwachte Einstellung als ein Problem angezeigt wird, müssen Sie das Tracking System entsprechend konfigurieren. Dies können Sie sowohl in der Standard- als auch der Experten-Ansicht vornehmen.Weitere Infos finden Sie unter *„Status-Warnmeldungen konfigurieren“* (S. 43).

11.2. Alarmeinstellungen

Hier können Sie die BitDefender-Pop-Ups und Warnungen deaktivieren.BitDefender verwendet Warnungen, um Sie zu einer Aktion aufzufordern und Pop-Ups, um Sie über bereits automatisch durchgeführte Aktionen oder andere Ereignisse zu informieren.Um eine Warnhinweiskategorie ein- oder auszuschalten, verwenden Sie den entsprechenden Schalter.

Wichtig

Die Einblendung der meisten Warnungen und Pop-Ups sollte aktiviert sein, um so potentielle Probleme zu vermeiden.

Dieses sind die verfügbaren Einstellungen:

Antivirus-Warnhinweise

Antivirus-Warnungen informieren Sie, wenn BitDefender einen Virus gefunden und blockiert hat.Wenn ein Virus gefunden wurde, ist es am sinnvollsten, den gesamten Computer zu scannen, um sicherzugehen, dass keine weitere Viren vorhanden sind.

Pop-Up Active Virus Control

Wenn Sie die Basis- oder Standard-Ansicht verwenden, informiert Sie ein Pop-Up, wenn die Active Virus Control eine potentiell schädliche Anwendung blockiert hat.Wenn Sie die Experten-Ansicht nutzen, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine Anwendung Anzeichen einer Malware-Infektion zeigt.

Pop-Up Email-Scan

Diese Pop-Ups werden angezeigt, um Sie darüber zu informieren, dass BitDefender Ihre Emails auf Malware scannt.

Warnungen Heim-Netzwerkverwaltung

Diese Warnungen informieren den Benutzer, wenn administrative Aktionen per Fernsteuerung durchgeführt werden.

Firewall Pop-Ups

Die Firewall verwendet Pop-Ups, um Sie über die unterschiedlichen mit Ihrer Netzwerkverbindung zusammenhängenden Ereignisse zu informieren (beispielsweise, wenn sich ein neuer Computer in das WiFi-Netzwerk eingeloggt hat, wenn eine neue Anwendung auf das Internet zugreifen darf oder wenn ein Port-Scan blockiert ist).Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Diese Pop-Ups sind sehr nützlich, um Einbruchversuche aufzuspüren und sich gegen Netzwerkbedrohungen zu schützen.

Quarantäne-Warnungen
Quarantäne-Warnungen informieren Sie, wenn alte Quarantänedateien gelöscht wurden.

Kindersicherungs-Warnungen
Wenn die Kindersicherung eine Aktivität blockiert, wird ein Warnhinweis eingeblendet, der Sie darüber informiert, wieso diese Aktivität blockiert wurde (z. B. wird eine Alarm-Webseite anstatt einer blockierten Webseite angezeigt).

Registrierungs-Pop-Ups
Registrierungs-Pop-Ups werden verwendet, um Sie daran zu erinnern, dass Sie BitDefender registrieren müssen oder um Sie zu informieren, dass der Lizenzschlüssel bald ablaufen wird oder schon abgelaufen ist.

11.3. Allgemeine Einstellungen

In diesem Bereich können Sie Einstellungen aktivieren bzw. deaktivieren, die das Produktverhalten und die Nutzung der Software beeinflussen.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

Dieses sind die verfügbaren Einstellungen:

Spiele-Modus
Der Spiele-Modus verändert temporär die Einstellungen so, dass sie die Systemleistung während des Spielens so wenig wie möglich beeinträchtigen.

Laptop-Modus
Der Laptop-Modus verändert temporär die Sicherheitseinstellungen so, dass die Betriebsdauer des Laptop-Akkus so wenig wie möglich beeinträchtigt wird.

Passworteinstellungen
Um zu verhindern, dass jemand anderes die BitDefender-Einstellungen ändert, können Sie diese durch ein Passwort schützen.Wenn Sie diese Option aktivieren, werden Sie zur Eingabe des Passwortes aufgefordert.Geben Sie das Passwort in beide Felder ein und klicken Sie auf **OK** um das Passwort festzulegen.

BitDefender Neuigkeiten
Wenn Sie diese Option aktivieren, erhalten Sie von BitDefender wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.

Produktbenachrichtigungen
Wenn Sie diese Option aktivieren, erhalten Sie Informationsnachrichten.

Scan-Aktivitätsanzeige
Die Aktivitätsanzeige ist ein kleines, transparentes Fenster in dem der Fortschritt der BitDefender Scan-Aktivitäten wird.

Virenberichte senden

Wenn Sie diese Option aktivieren, werden Virenberichte zur weiteren Analyse an das BitDefender-Team gesendet. Bitte bachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

Outbreak-Erkennung

Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch an das BitDefender Labor zur weiteren Analysen weitergeleitet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten sollten und nicht für kommerzielle Zwecke verwendet werden.

11.4. Neukonfiguration des Benutzerprofils

Während der Installation konnten Sie das Nutzungsprofil konfigurieren.Das Nutzungsprofil reflektiert die Hauptaktivitäten auf dem entsprechenden Computer. Basierend auf dem Nutzungsprofil, wird die Benutzeroberfläche organisiert, damit Sie bequem auf Ihre bevorzugten Aufgaben zugreifen können.

Klicken Sie zur Neukonfiguration des Benutzerprofils auf **Neukonfiguration des Benutzerprofils** und folgen Sie den Anweisungen des Konfigurations-Assistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Wählen Sie Ihre Ansicht.**

   Wählen Sie Ihre bevorzugte Ansicht.

2. **Konfiguration von Meine Werkzeuge**

   Falls Sie die Basis- oder Standard-Ansicht gewählt haben, wählen Sie die Funktionen, für die Sie Verknüpfungen erstellen möchten, auf dem Dashboard.

3. **Einstellungen konfigurieren**

   Wenn Sie die Experten-Ansicht gewählt haben, konfigurieren Sie die BitDefender-Einstellungen nach Bedarf.Um eine Einstellung zu aktivieren bzw. zu deaktivieren, nutzen Sie den entsprechenden Button.

4. **Aktivierung der Kindersicherung**

   Beachten Sie
   Dieser Schritt wird nur eingeblendet, wenn Sie die Kindersicherung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

   Sie können aus drei Optionen auswählen:

   - **Kindersicherung für Kinder-Benutzerkonten einrichten**

Aktivieren Sie diese Option, um die Kindersicherung für die Benutzerkonten Ihrer Kinder zu aktivieren und diese von Ihrem Administrations-Benutzerkonto aus zu verwalten.

- **Kindersicherung für das aktuelle Benutzerkonto einrichten**

  Wählen Sie diese Option, um die Kindersicherungsfunktion für das aktuelle Benutzerkonto zu aktivieren. Dies bedeutet, dass Sie nicht für jedes Kind ein separates Benutzerkonto anlegen müssen, sondern dass die Kindersicherungsregeln für jeden angewendet werden, der dieses Benutzerkonto verwendet.

  In diesem Fall ist ein Passwort notwendig, um die Kindersicherungseinstellungen zu schützen.Sie können dieses jetzt oder zu einem späteren Zeitpunkt im BitDefender-Fenster festlegen.

- **Den Setup vorerst überspringen**

  Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem BitDefender-Fenster aus zu konfigurieren.

5. **Heimnetzwerk-Verwaltung**

   Beachten Sie
   Dieser Schritt wird nur eingeblendet, wenn Sie die Heimnetzwerk-Verwaltung dem Bereich "Meine Werkzeuge" hinzugefügt haben.

   Sie können aus drei Optionen auswählen:

   - **Diesen PC als "Server" festlegen**

     Aktivieren Sie diese Option, wenn Sie BitDefender-Produkte auf anderen Computern des Heimnetzwerks von diesem Rechner aus verwalten möchten.

     Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

   - **Diesen PC als "Client" festlegen**

     Wählen Sie diese Option, wenn BitDefender von einem anderen Computer im Heimnetzwerk, auf dem BitDefender ebenfalls installiert ist, verwaltet werden soll.

     Für die Teilnahme am Netzwerk ist ein Passwort nötig.Geben Sie in der entsprechenden Textbox Ihr Passwort ein und klicken Sie auf **Übertragen**.

   - **Den Setup vorerst überspringen**

     Aktivieren Sie diese Option, um diese Funktion zu einem späteren Zeitpunkt von einem BitDefender-Fenster aus zu konfigurieren.

6. **Setup abgeschlossen**

   Klicken Sie auf **Fertigstellen**.

12. Verlauf und Ereignisse

Der **Protokolle einsehen** Link im unteren Bereich des BitDefender Sicherheitscenters öffnet ein weiteres Fenster mit den BitDefender-Ereignissen und dem Verlauf. Dieses Fenster gibt Ihnen einen Überblick über alle sicherheitsrelevanten Ereignissen.So können Sie beispielsweise einfach überprüfen, ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.

Für eine Filterung des Verlaufs und der Ereignisse BitDefender werden auf der linken Seite die folgenden Kategorien eingeblendet:

- **Dashboard**
- **Antivirus**
- **Antispam**
- **Kindersicherung**
- **Einstellungen zur Privatsphäre**
- **Firewall**
- **Schwachstellen**
- **Instant-Messaging-Verschlüsselung**
- **Spiele/Laptop-Modus**
- **Heimnetzwerk**
- **Update**
- **Registrierung**

Für jede Kategorie steht eine Liste von Ereignissen zu Verfügung. Jedes Ereignis enthält folgende Informationen: Eine Kurzbeschreibung, die von BitDefender durchgeführte Aktion sowie Datum und Zeitpunkt des Auftretens. Wenn Sie nähere Informationen zu einem Ereignis erhalten möchten, doppelklicken Sie auf das entsprechende Ereignis.

Hier finden Sie auch Detailinformationen und Statistiken zu den Ereignissen der Kindersicherung, wie z. B. besuchte Webseiten oder durch Ihre Kinder genutzte Anwendungen.

Klicken Sie auf **Alle Protokolle löschen** wenn Sie alte Protokolle entfernen möchten oder auf **Aktualisieren** um sicherzustellen, dass die angezeigten Protokolle aktuell sind.

13. Registrierung und My-Account

Die Registrierung erfolgt in zwei Schritten:

1. **Produktaktivierung (Registrierung eines BitDefender Benutzerkontos).** Um die Updates und den kostenlosen technischen Support zu erhalten, müssen Sie ein BitDefender Benutzerkonto anlegen.Falls Sie bereits über ein BitDefender-Benutzerkonto verfügen, registrieren Sie Ihr BitDefender-Produkt unter diesem Konto.BitDefender wird Sie darüber benachrichtigen, dass Sie Ihr Produkt zu aktivieren müssen und Ihnen helfen, dies zu bewerkstelligen.

   Wichtig

   Sie müssen innerhalb von 15 Tagen nach der Installation von BitDefender ein Benutzerkonto anlegen.Ansonsten erhält BitDefender keine automatischen Updates.

2. **Registrierung mit einem Lizenzschlüssel.** Der Lizenzschlüssel legt fest für wie lange Sie berechtigt sind das Produkt zu nutzen.Sobald der Lizenzschlüssel abgelaufen ist wird BitDefender alle Funktionen und somit den Schutz Ihres Computers einstellen.Sie sollten Ihre Lizenz einige Tage vor Ablauf verlängern oder eine neue Lizenz erwerben.

Wenn Sie BitDefender Internet Security 2011 auf CD/DVD oder online gekauft haben, werden Sie während der Installation zur Registrierung Ihres Produkts mit einem Lizenzschlüssel aufgefordert.

Wenn Sie BitDefender Internet Security 2011 zum Testen downloaden, müssen Sie das Produkt innerhalb von 30 Tagen mit einem Lizenzschlüssel registrieren, um auch nach der 30-Tages-Testphase BitDefender weiter nutzen zu können.Während der Testperiode ist das Produkt voll funktionsfähig, Sie können es testen um zu sehen ob es Ihre Erwartungen erfüllt.

13.1. BitDefender Internet Security 2011 registrieren

Wenn Sie das Produkt mit einem Lizenzschlüssel registrieren oder den aktuellen ändern möchten, klicken Sie auf den Link **Lizenzinformationen**, ganz unten im BitDefender-Fenster.Der Registrierungs-Assistent wird eingeblendet.

Sie sehen den Registrierungsstatus von BitDefender sehen, den aktuellen Lizenzschlüssel und wieviele Tage verbleiben, bis die Lizenz abläuft.

Um BitDefender Internet Security 2011 zu registrieren:

1. Geben Sie den Lizenzschlüssel in das Bearbeiten-Feld ein.

   Beachten Sie

   Sie finden den Lizenzschlüssel:

- Auf der Schnell-Start-Anleitung.
- Auf der Produktregistrierkarte.
- In der Email-Bestätigung des Online-Kaufs.

Wenn Sie keinen BitDefender-Lizenzschlüssel besitzen, klicken Sie auf den angegebenen Link, um den Assistenten zu öffnen, der Ihnen beim Kauf eines Lizenzschlüssels behilflich ist.

2. Klicken Sie auf **Jetzt registrieren**.
3. Klicken Sie auf **Fertigstellen**.

13.2. Aktivierung von BitDefender

Um Bitdefender zu aktivieren, müssen Sie einen BitDefender Benutzerkonto erstellen oder damit Anmelden.Wenn Sie im Rahmen des während der Installation noch kein BitDefender-Benutzerkonto registriert haben, können Sie Folgendes tun:

Basis-Ansicht
: Klicken Sie auf **Alle Probleme anzeigen**.Der Assistent hilft Ihnen alle latenten Bedrohungen zu beheben, einschließlich der Aktivierung des Produkts.

Standard-Ansicht
: Gehen Sie auf den Reiter **Sicherheit** und klicken Sie auf den Button **Ansicht& Beheben**, entsprechend dem aufgetretenen Update-Problem.Klicken Sie im Assistenten-Fenster auf **Start**, um das Produkt zu aktivieren.

Experten-Ansicht
: Gehen Sie auf **Registrierung** und klicken Sie auf den Button **Produkt aktivieren** .

Das Fenster Benutzerkonto-Registrierung wird geöffnet.Hier können Sie einen Benutzerkonto erstellen oder sich in ein bereits existierendes einloggen um das BitDefender zu aktivieren.

Wenn Sie im Moment kein BitDefender-Benutzerkonto anlegen möchten, klicken Sie auf **Benutzerkonto später erstellen** und dann auf **Beenden**.Ansonsten wählen Sie:

- „Ich habe noch kein BitDefender-Benutzerkonto“ (S. 53).
- „Ich habe bereits ein BitDefender Benutzerkonto.“ (S. 54).

Wichtig

Sie müssen innerhalb von 15 Tagen nach der Installation von BitDefender ein Benutzerkonto anlegen.Ansonsten erhält BitDefender keine automatischen Updates.

Ich habe noch kein BitDefender-Benutzerkonto

Um ein BitDefender-Benutzerkonto anzulegen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Neues Benutzerkonto erstellen**.
2. Geben Sie die Daten in die entsprechenden Felder ein.Die hier ingegebenen Daten bleiben vertraulich.
   - **Benutzername** - geben Sie Ihre Email-Adresse ein.
   - **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein.Das Passwort muss zwischen 6 und 16 Zeichen lang sein
   - **Passwort erneut eingeben** - geben Sie das vorher vergebene Passwort erneut ein.

     Sie müssen das Passwort nicht erneut eintippen, wenn Sie gewählt haben, dass das Passwort während des Eintippens unverschlüsselt dargestellt wird.
   - **Passworthinweis** - geben Sie ein Wort oder Schlagwort ein, das Ihnen hilft, sich an das vergessene Passwort zu erinnern.

   Beachten Sie
   Wenn das Konto einmal aktiviert ist, können Sie unter http://myaccount.bitdefender.com die angegebene Email-Adresse und das Passwort für die Anmeldung an Ihrem Konto verwenden.

3. Auf Wunsch wird BitDefender Sie über die Email-Adresse Ihres Benutzerkontos über Sonderangebote und Promotions informieren.Klicken Sie auf **Kontaktoptionen ansehen** und wählen Sie im eingeblendeten Fenster eine der verfügbaren Optionen.
   - **Alle Nachrichten senden**
   - **Wichtige Nachrichten senden**
   - **Ich möchte keine Nachrichten erhalten**
4. Klicken Sie auf **Übermitteln**.
5. Klicken Sie auf **Beenden**, um das Fenster zu schließen.

Beachten Sie
Sie müssen Ihr Benutzerkonto aktivieren bevor Sie es nutzen können.
Sobald Sie die vom BitDefender Registrierung dienst gesendete Mail erhalten haben, folgen Sie den darin enthaltenen Anweisungen.

Ich habe bereits ein BitDefender Benutzerkonto.

BitDefender weist Sie daraufhin, wenn bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert ist.In diesem Fall geben Sie das Passwort für Ihr Benutzerkonto ein und klicken Sie auf **Einloggen**.Klicken Sie auf **Beenden**, um das Fenster zu schließen.

Wenn Sie schon über ein aktives Konto verfügen, BitDefender dieses aber nicht findet, folgen Sie diesen Schritten, um Ihr Produkt zu registrieren.

1. Wählen Sie **Einloggen (Bestehendes Ben.konto)**.
2. Geben Sie die Email-Adresse und das Passwort Ihres Kontos in den entsprechenden Feldern ein.

   Beachten Sie
   Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Anweisungen.

3. Auf Wunsch wird BitDefender Sie über die Email-Adresse Ihres Benutzerkontos über Sonderangebote und Promotions informieren.Klicken Sie auf **Kontaktoptionen ansehen** und wählen Sie im eingeblendeten Fenster eine der verfügbaren Optionen.
   - **Alle Nachrichten senden**
   - **Wichtige Nachrichten senden**
   - **Ich möchte keine Nachrichten erhalten**
4. Klicken Sie auf **Übermitteln**.
5. Klicken Sie auf **Beenden**, um das Fenster zu schließen.

13.3. Kauf oder Erneuerung des Lizenzschlüssels

Wenn sich die Testperiode bald ausläuft, sollten Sie einen Lizenzschlüssel erwerben und Ihr Produkt registrieren.

Falls Ihr aktueller Lizenzschlüssel in Kürze abläuft, müssen Sie Ihre Lizenz verlängern.Als BitDefender Kunde erhalten Sie einen Nachlass, wenn Sie die Lizenz für Ihr BitDefender Produkt erneuern.

Um ein einfaches und sicheres Verfahren zu starten, über das Sie einen neuen Lizenzschlüssel kaufen oder einen bestehenden verlängern können, öffnen Sie BitDefender in der Standard- oder Experten-Ansicht und klicken Sie unten auf dem Bildschirm auf **Kaufen** / **Verlängern**.

Konfiguration und Verwaltung

14. Allgemeine Einstellungen

Das Allgemein-Modul bietet Informationen über die BitDefender-Aktivität und das System.Hier können Sie auch das allgemeine Verhalten von BitDefender ändern.

Konfiguration der allgemeinen Einstellungen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein> Einstellungen**.

- **Passwortschutz für Programm-Einstellung aktivieren** - aktiviert die Festlegung eines Passwortes, um Ihre BitDefender-Einstellungen zu schützen.

  Beachten Sie
  Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

  Geben Sie sowohl im **Passwort**-Feld als auch im **Wiederholung**-Feld ein Passwort ein und klicken Sie auf **OK**.

  Wenn Sie das Passwort festgelegt haben, werden Sie immer danach gefragt, wenn Sie die BitDefender-Einstellungen ändern möchten.Ein anderer Systemadministrator (falls vorhanden) muss dieses Passwort ebenfalls angeben, um BitDefender-Einstellungen ändern zu können.

  Wenn Sie nur während der Konfiguration der Kindersicherung nach dem Passwort gefragt werden möchten, so aktivieren Sie die Option **Passwortschutz nur für Kindersicherungseinstellungen anwenden**.Wenn ein Passwort nur für die Kindersicherung festgelegt wurde, Sie diese Option jedoch deaktiviert haben wird das entsprechende Passwort bei der Einstellung jeder BitDefender-Option abgefragt werden.

  Wichtig
  Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie das Produkt reparieren, um die BitDefender-Konfiguration zu ändern.

- **Bei Aktivierung der Kindersicherung fragen, ob ich ein Passwort konfigurieren möchte** - Sie werden bei Aktivierung der Kindersicherung aufgefordert, ein Passwort zu vergeben, falls dies noch nicht vergeben wurde.Wenn Sie ein Passwort festlegen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.
- **BitDefender-News anzeigen** (sicherheitsrelevante Benachrichtigungen) - von Zeit zu Zeit erhalten Sie Sicherheitsmeldungen über Virenausbrüche, die von BitDefender-Servern versendet werden.

- **Pop-Ups (Bildschirmbenachrichtigungen)** - Pop-Up-Fenster mit Informationen zum Produktstatus werden eingeblendet.Sie können BitDefender so konfigurieren, dass die Pop-Ups nur angezeigt werden, wenn Sie die Basis-, Standard- oder Experten-Ansicht gewählt haben.
- **Scan-Aktivitätsanzeige anzeigen (grafische Bildschirmanzeige der Produktaktivität)** - die Leiste mit der Scan-Aktivität wird eingeblendet wenn Sie sich in Windows einloggen.Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass die Scan-Aktivitätsleiste weiterhin angezeigt wird.

Beachten Sie

Diese Option kann nur für das aktuelle Windows Benutzerkonto konfiguriert werden.Die Aktivitätsanzeige ist nur in der Experten-Ansicht verfügbar.

Einstellungen Virenprotokoll

- **Virenprotokolle senden** - sendet auf Ihrem Computer gefundene Viren an das BitDefender-Virenlabor. Diese Meldung hilft uns, Virenausbrüche im Auge zu behalten.

  Das Protokoll beinhaltet keine persönlichen Daten - wie Ihren Namen, IP-Adresse oder ähnliches. Ihre Daten werden nicht für Werbezwecke verwendet. Die Informationen beinhalten nur den Virennamen und wird für die Erstellung von Statistiken verwendet.
- **BitDefender Outbreak-Erkennung aktivieren** - sendet Protokolle über mögliche Virenausbrüche an das BitDefender-Labor.

  Das Protokoll beinhaltet keine persönlichen Daten wie Ihren Namen,IP-Adresse oder ähnliches, Ihre Daten werden nicht für Werbezwecke verwendet. Die Informationen beinhalten nur den Virennamen und werden nur für die Erkennung von neuen Viren verwendet.

Verbindungseinstellungen

Für viele BitDefender-Komponenten (Firewall, LiveUpdate, Echtzeit-Virenprotokoll und Echtzeit-Spambericht) ist ein Internetzugang notwendig. BitDefender ist mit einem Proxy-Manager ausgestattet, der Ihnen von einer Stelle aus die Konfiguration der Proxy-Einstellungen erlaubt, die die BitDefender Komponenten nutzen, um auf das Internet zuzugreifen.

Falls Ihre Firma für die Internetverbindungen einen Proxy-Server verwendet, müssen Sie dessen Proxy-Einstellungen konfigurieren um sicherzustellen, dass sich BitDefender selbst updaten kann. Anderenfalls werden die Proxy-Einstellungen des Administrators, der das Produkt installiert hat oder die momentanen Proxy-Einstellungen des Standard-Browsers verwendet.Weitere Informationen finden Sie unter *„Wo finde ich "Meine Proxy-Einstellungen"?“* (S. 214).

Beachten Sie

Proxy-Einstellungen von Benutzer mit Administratorrechten oder sog. Power Usern (also Anwender, die die notwendigen Passwörter kennen) konfiguriert werden.

Um die Proxy-Einstellungen zu verwalten, klicken Sie auf **Proxy-Einstellungen**.

Es bestehen drei mögliche Proxy-Einstellungen:

- **Proxy während Installation entdeckt** - während der Installation wurden Proxy-Einstellungen für das Administrator-Benutzerkonto gefunden. Diese können nur von diesem Administratorkonto aus geändert werden. Sollten ein Benutzername und Passwort nötig sein, so geben Sie diese in den dafür vorgesehenen Feldern ein.
- **Standard Browser Proxy** - Proxy-Einstellungen des aktuellen Benutzers, extrahiert vom Standard-Browser. Falls der Proxy einen Benutzernamen und Passwort voraussetzt, geben Sie diese in den entsprechenden Feldern an.

  Beachten Sie

  Die unterstützen Browser sind hierbei Internet Explorer, Mozilla Firefox und Opera. Sollten Sie einen anderen Browser verwenden kann BitDefender dessen Einstellungen nicht übernehmen.

- **Benutzerdefinierte Proxy-Einstellungen** - Hier können Sie selbst, als Administrator angemeldet, Proxy-Einstellungen vornehmen.

  Die folgenden Einstellungen müssen eingegeben 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.

BitDefender wird die Proxy-Einstellungs-Sets in der folgenden Reihenfolge anwenden, bis der Verbindungsaufbau zum Internet gelingt:

1. die spezifizierten Proxy-Einstellungen.
2. die bei der Installation gefundenen Proxy-Einstellungen.
3. die Proxy-Einstellungen des aktuellen Benutzers.

Bei einem Updateversuch werden alle Proxyeinstellung nacheinander verwendet bis ein Update möglich ist.

Zuerst wird versucht, ein Update über die eigenen Proxy-Einstellungen vorzunehmen. Als nächstes werden die Proxy-Einstellungen des Administrators verwendet. Wenn auch dies nicht zum Erfolg führt, wird ein Update über die Einstellungen des momentanen Benutzers durchgeführt.

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

Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern. Wenn Sie auf **Voreingestellt** klicken, werden die Werkseinstellungen geladen.

Systeminformation

In BitDefender können Sie von einer Stelle aus alle Systemeinstellungen und die Programme, die beim Systemstart gestartet werden, einsehen. So können Sie die Aktivitäten des Systems und der installierten Anwendungen überwachen und mögliche Systeminfizierungen feststellen.

So finden Sie die Systeminformationen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein > Systeminfo**.

Die Liste enthält alle Einstellungen, die beim Systemstart geladen werden, sowie die geladenen Einträge für die unterschiedlichen Anwendungen.

Drei Buttons stehen zur Verfügung:

- **Wiederherstellen** - stellt die ursprüngliche Dateizuordnung wieder her.Nur für die Einstellungen der **Dateizuordnung** verfügbar!
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt (z.B. **Registry**).

Beachten Sie
Abhängig vom ausgewählten Eintrag wird den Button **Gehe zu** nicht eingeblendet.

- **Aktualisieren** - öffnet erneut den Bereich **Systeminfo**.

15. Antivirus-Schutz

BitDefender schützt Sie vor allen Arten von Malware (Viren, Trojaner, Spyware, Rootkits etc.).Der Virenschutz, den BitDefender bietet, lässt sich in zwei Kategorien einteilen:

- Echtzeitschutz - hält neue Malware-Bedrohungen davon ab, in Ihr System zu gelangen.BitDefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.

  Der Echtzeitschutz ist auch bekannt als On-Access -Scanning (Auf-Zugriff-Scan) - Dateien werden gescannt, sobald der Benutzer auf sie zugreift.

  Wichtig
  Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie den **Echtzeitvirenschutz** immer aktiviert.

- On-Demand-Scan - erkennt und entfernt Malware, 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.Die Scan-Aufgaben erlauben Ihnen, die Scan-Routinen an Ihre Bedürfnisse anzupassen und diese zu einem festgelegten Zeitpunkt zu starten.

Wenn BitDefender einen Virus oder andere Malware feststellt, versucht das Programm automatisch den Malware-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen.Diese Operation bezeichnet man als Desinfektion.Dateien, die nicht desinfiziert werden können, werden in das QuarantäneVerzeichnis verschoben, um so die Infizierung einzudämmen.Weitere Informationen finden Sie unter *„Quarantäne“ (S. 84)*.

Wenn Ihr Computer mit Malware infiziert ist, siehe *„Malware von Ihrem System entfernen“ (S. 196)*.

Fortgeschrittene Anwender können Scan-Ausschlüsse festlegen, falls bestimmte Dateien vom Scan ausgeschlossen werden sollen.Weitere Informationen finden Sie unter *„Konfiguration der Scan-Ausschlüsse“ (S. 80)*.

15.1. Echtzeitschutz

BitDefender bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie Email-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) gescannt werden.

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

können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Schutzstufen wählen.Wenn Sie ein erfahrener Anwender sind, können Sie die Scan-Einstellungen auch selbst im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe definieren.

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Anpassen der Sicherheitsstufe des Echtzeitschutzes“* (S. 62)
- *„Erstellen einer benutzerdefinierten Schutzeinstellung“* (S. 63)
- *„Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird“* (S. 64)
- *„Wiederherstellen der Voreinstellungen“* (S. 65)

Um Sie gegen unbekannte Malware-Anwendungen zu schützen, greift BitDefender auf eine fortschrittliche Heuristik-Technologie (Active Virus Control) und ein Intrusion Detection System, das Ihr System durchgehend überwacht, zurück.Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Konfiguration der Active Virus Control“* (S. 66)
- *„Konfiguration des Intrusion Detection Systems“* (S. 68)

15.1.1. Anpassen der Sicherheitsstufe des Echtzeitschutzes

Die Schutzstufe des Echzeitschutzes definiert die Scan-Einstellungen für den Echtzeitschutz.Sie können die Einstellungen zum Echtzeitschutz einfach Ihren Bedürfnissen anpassen, indem Sie eine der vordefinierten Schutzstufen wählen.

Um die Sicherheitsstufe für den Echtzeitschutz anzupassen:

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

   Standard-Ansicht

   Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

   Klicken Sie auf den Reiter **Schild**.

   Experten-Ansicht

   Gehen Sie zu **Antivirus > Schild**.

Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

3. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

15.1.2. Erstellen einer benutzerdefinierten Schutzeinstellung

Erfahrene Anwender möchten sich eventuell näher mit den Scan-Einstellungen von BitDefender beschäftigen. Der Scanner kann so eingestellt werden, dass nur spezielle Dateiendungen oder spezielle Malware-Bedrohungen gescannt oder Archive übersprungen werden. So werden die Scan-Zeit verringert und die Antwortzeiten Ihres Rechners während eines Scans verbessert.

Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe festlegen.Schutzstsufe zu erstellen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Benutzerdefinierte Einstufung**.
4. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.Um herauszufinden, was eine Option bewirkt, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Auch im Internet können Sie hilfreiche Informationen finden.
- **Scanne Dateien, auf die zugegriffen wird.** Sie können BitDefender so programmieren, dass alle Dateien, nur Anwendungen (Programmdateien) oder nur bestimmte Dateitypen, die Sie als gefährlich einstufen, gescannt werden sollen.Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger gegen Malware-Angriffe als andere Typen oder Dateien.Diese Kategorie beinhaltet die folgenden Dateierweiterungen:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Falls Sie sich für die Option **Anwenderdefinierte Erweiterungen scannen** entscheiden, empfehlen wir, dass Sie neben allen anderen Dateierweiterungen,

die Sie als potentiell gefährlich einstufen, auch alle Anwendungserweiterungen mit einschließen.

- **Nur neue und geänderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Archive scannen.** Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird.Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.
- **Aktionsoptionen.** Falls Sie die Aktionen, die auf verdächtige Dateien angewendet werden sollen, ändern möchten, finden Sie Tipps in *„Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird“* (S. 64).
- **Scan-Optionen für Email-,Internet- und Instant Messaging-Datenverkehr .** Um zu verhindern, dass Malware auf Ihren Computer geladen wird, scannt BitDefender automatisch die folgenden Malware Einfalltore:
  - eingehende Emails
  - Internet-Datenverkehr
  - über Yahoo! Messenger und Windows Live Messenger empfangene Dateien

  Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

  Obwohl wir dies nicht empfehlen, können Sie den Scan von Emails, Web- oder Instant Messaging deaktivieren, um die Systemleistung zu verbessern.Wenn Sie die entsprechenden Scan-Optionen deaktivieren, werden empfangene Emails und aus dem Internet geladene Dateien nicht gescannt. Dies bedeutet aber, dass infizierte Dateien auf Ihrem Computer gespeichert werden können.Dies ist keine bedeutende Bedrohung, da der Echtzeitschutz die Malware blockiert, wenn auf die infizierten Dateien zugegriffen wird (geöffnet, verschoben, kopiert oder ausgeführt).

15.1.3. Ändern der Aktion, die bei verdächtigen Dateien durchgeführt wird

Die vom Echtzeitschutz festgestellten Dateien werden in zwei Kategorien gruppiert:

- **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der BitDefender Malware-Signaturen-Datenbank überein.BitDefender kann im Normalfall Malware-Codes aus einer infizierten Datei entfernen und die Originaldatei wiederherstellen. Diese Aktion wird Desinfektion genannt.

Beachten Sie

Malware-Signaturen sind Code-Bruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.
Die BitDefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch BitDefender-Mitarbeiter upgedateten Malware-Signaturen.

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

Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:

- 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 in Schach zu halten.

Wichtig

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

- Wird eine verdächtige Datei gefunden, wird der Zugriff auf diese Datei verweigert, um so eine potentielle Infizierung auszuschließen.

Sie sollten die voreingestellten Aktionen für verdächtige Dateien nicht ändern, es sei denn, Sie haben einen guten Grund dafür.

Um die voreingestellten Aktionen für infizierte oder verdächtige Dateien zu ändern:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Benutzerdefinierte Einstufung**.
4. Konfigurieren Sie die Aktionen, die für jede Dateikategorie durchgeführt werden sollen.Die zweite Aktion wird ausgeführt, wenn die erste fehlschlägt (wenn beispielsweise die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben).

15.1.4. Wiederherstellen der Voreinstellungen

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

Um die vorgegebenen Echzeitschutz-Einstellungen wiederherzustellen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Voreingestellter Level**.

15.1.5. Konfiguration der Active Virus Control

Die BitDefender Active Virus Control kann potentiell gefährliche Anwendungen anhand ihrer speziellen Verhaltensweisen entdecken.

Die Active Virus Control überwacht kontinuierlich die auf Ihrem Computer laufenden Anwendungen auf Malware-ähnliche Aktionen. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird zudem eine Allgemeineinstufung erstellt.Wenn die Allgemeineinstufung für einen Prozess einen bestimmten Schwellenwert erreicht, wird der Prozess als schädlich eingestuft. Abhängig von den Programmeinstellungen wird der Prozess entweder automatisch blockiert oder Sie werden aufgefordert, die auszuführende Aktion zu spezifizieren.

Active Virus Control kann so konfiguriert werden, dass Sie informiert werden, wenn eine Anwendung versucht, eine möglicherweise schädliche Aktion durchzuführen.

Wenn Sie die entdeckte Anwendung kennen und ihr trauen, klicken Sie auf **Erlauben**.

Wenn Sie die Anwendung unverzüglich beenden möchten, klicken Sie auf **OK**.

Wählen Sie **Diese Aktion für diese Anwendung merken** aus, bevor Sie Ihre Wahl treffen, und BitDefender wird die gleiche Aktion für die entdeckte Anwendung auch in Zukunft ausführen.Die Regel, die erstellt wird, wird im Fenster der Active Virus Control gelistet.

Konfiguration der Active Virus Control:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Markieren Sie das dazugehörige Kästchen um die Active Virus Control zu aktivieren.
6. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

Anpassung des Schutzstufen-Levels

Konfiguration der Schutzstufe der Active Virus Control:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

Konfiguration der Reaktion auf Malware-typisches Verhalten

Falls eine Anwendung Anzeichen einer Malware-Infektion zeigt, erhalten Sie eine Abfrage, ob diese zugelassen oder blockiert werden soll.

Konfiguration der Antwort auf Malware-typisches Verhalten:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Möchten Sie zu einer Aktion aufgefordert werden, wenn Active Virus Controll eine potentiell schädliche Anwendung findet, aktivieren Sie die Option **Warnen, bevor eine Aktion durchgeführt wird**.Soll eine Anwendung, die Zeichen einer Malware-Infizierung zeigt automatisch blockiert werden (ohne ein Warnhinweisfenster einzublenden), aktivieren Sie diese Option.

Die Verwaltung von vertrauenswürdigen/fragwürdigen Anwendungen

Sie können Anwendungen die Sie kennen und denen Sie vertrauen, zur Liste der vertrauenswürdigen Anwendungen hinzufügen. Diese Anwendungen werden nicht länger von der BitDefender Active Virus Control gescannt, der Zugriff wird automatisch erlaubt.

Verwaltung der Anwendungen, die nicht von der Active Virus Control überwacht werden:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf den Reiter **AVC** (Active Virus Control).
5. Klicken Sie auf den Reiter **Ausschlüsse**.

Die Anwendungen für die eine Regel erstellt wurde, wird in der Tabelle **Ausschlüsse** angezeigt.Der Pfad der Anwendungen und die Aktion, die Sie dafür konfiguriert haben (erlaubt oder blockiert), wird für jede Regel angezeigt.

Um die Aktion für eine Anwendung zu ändern, klicken Sie die aktuelle Aktion und wählen Sie im Menü eine andere Aktion aus.

Um die Anwendungen zu verwalten, nutzen Sie die Buttons neben der Tabelle:

- **Hinzufügen** - eine neue Anwendung der Liste hinzufügen.
- **Entferne** - eine Anwendung aus der Liste entfernen.
- **Bearbeiten** - eine Anwendungsregel bearbeiten.

15.1.6. Konfiguration des Intrusion Detection Systems

Das Intrusion Detection System von BitDefender überwacht das Netzwerk und die Systemaktivitäten auf Malware-Aktivitäten oder Richtlinienverletzungen.

Konfiguration des Intrusion Detection Systems:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie auf den Reiter **IDS**.
5. Aktivieren Sie das entsprechende Kästchen, um das Intrusion Detection System zu aktivieren.
6. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die Schutzstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

15.2. Scan-Vorgang (Scannen)

Die Hauptaufgabe der BitDefender-Software ist es sicherzustellen, dass Ihr virenfrei ist. Dies wird in erster Linie dadurch erreicht, dass neue Viren von Ihrem Computer ferngehalten werden und indem Ihre Email-Anhänge und Downloads gescannt und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass sich bereits vor der Installation von BitDefender ein Virus in Ihrem System befand. Deshalb sollten Sie Ihren Computer nach der Installation von BitDefender auf residente Viren scannen. Und es ist definitiv eine gute Idee, auch in Zukunft Ihren Computer regelmäßig auf Viren zu scannen.

On-Demand-Scanning basiert auf Scan-Aufgaben, Scan-Aufgaben definieren die Scan-Optionen und die Objekte, die gescannt werden sollen.Sie können den Computer jederzeit scannen, indem Sie die voreingestellten oder die von Ihnen selbst definierten Aufgaben starten. Sie können auch festlegen, dass Scans regelmäßig

durchgeführt werden sollen oder wenn Ihr PC gerade nicht benutzt wird.Schnelle Hilfestellung finden Sie in folgenden Themenbereichen:

- *„Wie kann ich Dateien und Verzeichnisse scannen?“* (S. 165)
- *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 168)
- *„Wie plane ich einen Scan?“* (S. 170)

15.2.1. Dateien und Verzeichnis scannen

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 scannen**.Der Antivirus Scan-Assistent wird eingeblendet werdenund Sie durch den Scan-Vorgang führen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen möchten, könnenSie eine benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.Weitere Informationen finden Sie unter *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 168).

Um Ihren Computer oder Teile Ihres Computers zu scannen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben definieren.Um eine Scan-Aufgabe auszuführen, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Basis-Ansicht
: Klicken Sie auf den Button **Sicherheit** und wählen Sie eine der verfügbaren Scan-Aufgaben.

Standard-Ansicht
: Gehen Sie auf den Reiter **Sicherheit**.Klicken Sie im linken Quick Task-Bereich auf **Vollsystem-Scan** und wählen Sie eine der verfügbaren Scan-Aufgaben.

Experten-Ansicht
: Gehen Sie zu **Antivirus > Virusen-Scan**.Um eine System- oder Benutzerdefinierten-Scan auszuführen, klicken Sie auf den entsprechenden **Aufgabe Ausführen**-Button.

Dies sind die voreingestellten Aufgaben, die Sie für einen Scan Ihres Computers nutzen können:

Vollsystem-Scan
: Scannt alle Dateien mit Ausnahme von Archiven.In der Standardkonfiguration, wird nach allen Arten von Malware mit Ausnahme von Rootkits gescannt.

Quick Scan
: 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 Virenscan in Anspruch nehmen würde.

Tiefensystem-Scan

Scannt das komplette System.In der Voreinstellung wird auf alle Arten von Bedrohungen gescannt, wie z.B. Viren, Spyware, Adware, Rootkits etc.

Bevor Sie einen Scan starten sollten Sie sich vergewissern, dass BitDefender auf dem neuesten Stand der Malware-Signaturen ist. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu scannen, kann BitDefender daran hindern, neue seit dem letzten Update gefundene Malware zu erkennen.

Damit Sie einen vollständigen Scan mit BitDefender durchführen können, ist es wichtig, alle Programme zu beenden. Besonders wichtig ist, dass Sie Ihr Email Programm schließen (z. B. Outlook, Outlook Express oder Eudora).

Prüftips

Hier finden Sie noch einige Scan-Tipps, die Sie vielleicht nützlich finden:

- Je nach Festplattengröße kann das Durchführen einer umfassenden Systemprüfung (wie Systemprüfung oder Tiefe Systemprüfung) einige Zeit in Anspruch nehmen (bis zu einer Stunde oder mehr).Aus diesem Grund sollten Sie derartige Scans nur durchführen, wenn Sie den Computer für längere Zeit nicht nutzen (z.B. während der Nacht).

  Sie können einen Scan für einen günstigen Zeitpunkt terminieren.Stellen Sie sicher, dass der Computer weiterhin läuft.Wenn Sie mit Windows Vista arbeiten, stellen Sie sicher, dass sich Ihr Rechner nicht im Schlafmodus befindet, wenn eine geplante Aufgabe ansteht.

- Falls Sie regelmäßig Dateien aus dem Netz in ein bestimmtes Verzeichnis herunterladen, erstellen Sie eine neue Scan-Aufgabe und legen das Verzeichnis als Scan-Ziel fest.Terminieren Sie einen täglichen (oder auch häufigeren) Scan.

- Es gibt eine Art von Malware, die sich selbst so konfiguriert, dass bei einem Windows-Neustart die Windows-Einstellungen verändert werden.Um Ihren Computer vor derartiger Malware zu schützen, können Sie den **Autologon-Scan** beim Systemstart ausführen lassen.Bitte beachten Sie, dass diese Funktion die Systemleistung für kurze Zeit nach dem Start beeinflussen kann.

15.2.2. Antivirus Scan Assistent

Wann immer Sie einen On-Demand Scan starten (z.B. indem Sie auf ein Verzeichnis rechtsklicken und dann **Mit BitDefender 2011 scannen wählen**), wird der BitDefender Antivirus Scan-Assistent eingeblendet.Befolgen Sie die dreistufige Anleitung um den Scan-Vorgang durchzuführen.

Beachten Sie

Falls der Scan-Assistent nicht eingeblendet wird, ist der Scan möglicherweise so konfiguriert, dass er still im Hintergrund durchgeführt wird.Sehen Sie nach dem

Scan-Fortschrittssymbol in der Systemleiste.Sie können dieses Symbol anklicken, um so das Scan-Fenster zu öffnen und den Scan-Fortschritt zu beobachten.

Schritt 1/3 - Scannen

BitDefender startet den Scan der aus gewählten Dateien und Verzeichnisse.

Der Scan-Status und die Statistiken (Scan-Geschwindigkeit, vergangene Zeit, Anzahl der gescannten/infizierten/verdächtigen/versteckten Objekte) werden eingeblendet.

Bitte warten Sie, bis BitDefender den Scan beendet hat.

Beachten Sie
Der Scan-Vorgang kann, abhängig von der Komplexität des Scan, einen Moment dauern.

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

- **Ich möchte für dieses Objekt das Passwort eingeben.** Wenn Sie möchten das 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.
- **Ich möchte für dieses Objekt kein Passwort angeben (dieses Objekt überspringen).** Wählen Sie diese Option, um den Scan diesen Archivs zu überspringen.
- **Ich möchte für kein Objekt ein Passwort angeben (alle passwortgeschützten Objekte 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.

Klicken Sie auf **OK** um fortzufahren.

Stoppen oder Anhalten des Scans. Sie können den Scan jederzeit durch einen Klick auf **Stopp&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.Um den Scan vorrübergehend anzuhalten, klicken Sie einfach auf **Pause**. Um den Scan fortzusetzen klicken Sie auf **Fortsetzen**.

Schritt 2/3 - Aktionsauswahl

Wenn der Scan abgeschlossen ist, werden in einem neuen Fenster angezeigt die Scan-Ergebnisse angezeigt.

Sind keine ungelösten Probleme vorhanden, klicken Sie auf **Weiter**.Andernfalls müssen Sie neue Aktionen konfigurieren, die auf die nicht beseitigten Bedrohungen angewandt werden sollen. Nur so ist Ihr System weiterhin geschützt.

Die infizierten Objekte werden in Gruppen angezeigt, kategorisiert nach der Malware, mit der sie infiziert sind.Klicken Sie auf den der Bedrohung entsprechenden Link, Informationen über die infizierten Objekte zu erhalten.

Sie können eine allgemeine Aktion für alle Probleme definieren oder einzelne Aktionen für Problemgruppen definieren.Eine oder mehrere der folgenden Optionen können im Menü erscheinen:

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

Desinfizieren
Der Malware-Code wird aus den infizierten Dateien entfernt.

Löschen
Infizierte Dateien werden von der Festplatte entfernt.

In Quarantäne verschieben
Verschiebt die entdeckten Dateien in die Quarantäne.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht ein nur geringes Infektionsrisiko.Weitere Informationen finden Sie unter *„Quarantäne“ (S. 84)*.

Dateien umbenennen
Benennt verborgene Dateien durch Anhängen von `.bd.ren` an Ihren Namen um.Als Ergebnis können Sie solche Dateien (falls vorhanden) auf Ihrem Computer suchen und finden.

Bitte beachten Sie, dass es sich bei den verborgenen Dateien nicht um absichtlich von Windows verborgenen Dateien handelt. In diesem Fall handelt es um versteckte Dateien, die von speziellen Programmen versteckten werden und als sog Rootkits bekannt sind.Rootkits sind nicht grundsätzlich schädlich. JSie werden jedochhäufig verwendet, um Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

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

Schritt 3/3 - 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
Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

BitDefender konnte einige Probleme nicht lösen

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.Weitere Informationen und Anweisungen, wie Sie Malware manuell entfernen können, finden Sie unter *„Malware von Ihrem System entfernen“* (S. 196).

BitDefender hat verdächtige Dateien gefunden

Verdächtige Dateien sind Dateien, die von der heuristischen Analyse als potentiell infiziert erkannt werden, und deren Signaturen noch nicht bekannt sind.

Falls verdächtige Dateien während des Scanes erkannt werden, werden Sie aufgefordert, diese Dateien an das BitDefender-Labor zu senden.Klicken Sie auf **OK**, um diese Dateien zum BitDefender-Lab für weitere Analysen zu senden.

15.2.3. Anzeige der Scan-Protokolle

Für jeden Scan wird ein Protokoll erstellt.Dieser Bericht enthält detaillierte Informationen über den Scan-Vorgang, wie beispielsweise die 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.

Um die Scan-Protokolle später anzusehen:

1. Öffnen Sie BitDefender.
2. Klicken Sie unten rechts im Fenster auf den Link **Protokolle ansehen**.
3. Klicken Sie imMenü auf der linken Seite auf **Antivirus**.
4. Im Bereich **On-Demand-Aufgaben** können Sie überprüfen, welche Scans kürzlich durchgeführt wurden.Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um das Scan-Protokoll zu öffnen, klicken Sie auf **Scan-Protokoll ansehen**.Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

15.2.4. Verwaltung der existierenden Scan-Aufgaben

BitDefender verfügt über mehrere vordefinierte Aufgaben, die für die gängigsten Sicherheitsprobleme angewandt werden können.Weitere Informationen finden Sie unter *„Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?“* (S. 168).

Verwaltung der existierenden Scan-Aufgaben:

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

Standard-Ansicht

Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

Klicken Sie auf den Reiter **Virenscan**

Experten-Ansicht

Gehen Sie zu **Antivirus > Virusen-Scan**.

Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

Es gibt drei verschiedene Kategorien der Scan-Optionen:

- **Systemaufgaben** - Enthält die Liste der Standard-Systemaufgaben. Die folgenden Aufgaben stehen zur Verfügung:

  Vollsystem-Scan

  Scannt alle Dateien mit Ausnahme von Archiven.In der Standardkonfiguration, wird nach allen Arten von Malware mit Ausnahme von Rootkits gescannt.

  Quick Scan

  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 Virenscan in Anspruch nehmen würde.

  Auto-logon Scan

  Scannt die Einträge, die ausgeführt werden, wenn ein Benutzer sich in Windows anmeldet.In der Voreinstellung ist der Auto-logon Scan deaktiviert.

  Um die Aufgabe zu benutzen, klicken Sie mit der rechten Maustaste auf die Aufgabe, wählen Sie **Terminplaner** und legen Sie fest, dass Aufgabe **beim Systemstart** durchgeführt wird.Sie können festlegen, wie lange nach dem Systemstart die Aufgabe gestartet werden soll (in Minuten).

  Tiefensystem-Scan

  Scannt das komplette System.In der Voreinstellung wird auf alle Arten von Bedrohungen gescannt, wie z.B. Viren, Spyware, Adware, Rootkits etc.

Beachten Sie

Bei den Scans **Tiefensystem-Scan** und **Vollsystem-Scan** werden alle Dateien gescannt, deshalb kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir, diese Aufgaben mit niedriger Priorität durchzuführen oder besser wenn Sie den Computer nicht verwenden.

- **Benutzerdefinierte Aufgaben** - enthält die benutzerdefinierten Aufgaben.

  Eine Aufgabe, die sog `Meine Dokumente` steht zur Verfügung.Verwenden Sie diese Aufgaben, um die folgenden für den jeweiligen Benutzer Verzeichnisse zu scannen: `Eigene Dateien`, `Desktop` und `Autostart`. Dadurch wird die sichergestellt, dass Ihre eigenen Daten, ein sicherer Arbeitsplatz sowie eine saubere Ausführung der Anwendungen beim Systemstart gewährleistet.

- **Verschiedene Aufgaben** - enthält eine Liste verschiedener Scan-Aufgaben. Diese Scan-Aufgaben weisen auf alternative Scan-Aufgaben hin, die nicht aus diesem Fenster heraus ausgeführt werden können. Hier können Sie nur die Einstellungen ändern oder sich die Scan-Berichte ansehen.Folgende Aufgaben stehen zur Verfügung:

  Geräte-Scan
  BitDefender stellt automatisch fest, wenn ein neues Speichergerät an den Computer geschlossen wird und scannt dieses.Nutzen Sie diese Aufgabe, um die Optionen der automatischen Erkennung und der Prüfung von Speichergeräten (CDs/DVDs, USB-Speicher oder Netzlaufwerke) zu konfigurieren.

  Kontext-Scan
  Diese Aufgabe wird ausgeführt, wenn über das Kontextmenü von Windows oder über die Scan-Aktivitätsleiste gescannt wird.Sie können die Scan-Optionen an Ihre Situation anpassen.

Sie können die Scan-Aufgaben über die Buttons oder das Verknüpfungs-Menü verwalten.

Um eine System- oder Benutzerdefinierten-Scan auszuführen, klicken Sie auf den entsprechenden **Aufgabe Ausführen**-Button.Der Antivirus Scan-Assistent wird eingeblendet werdenund Sie durch den Scan-Vorgang führen.

Um festzulegen, dass eine Scan-Aufgabe automatisch ausgeführt wird, klicken Sie auf den Button **Planer** und konfigurieren Sie die Aufgabe wie gewünscht.

Wenn sie eine definierte Scan Aufgabe nicht mehr benötigen, können Sie diese löschen, indem Sie den **Löschen**-Button, rechts neben der Aufgabe klicken.Systemaufgaben und Verschiedene Aufgaben können nicht gelöscht werden.

Jede Scan-Aufgabe verfügt über ein Eigenschaftenfenster, in dem Sie die Einstellungen konfigurieren und sich die Scan-Protokolle ansehen können.Um dieses Fenster zu öffnen, klicken Sie auf den Button **Eigenschaften**, links neben der Aufgabe (oder rechtsklicken Sie auf die Aufgabe und wählen Sie **Eigenschaften**).

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Konfiguration der Scan-Einstellungen“* (S. 76)
- *„Festlegen der Scan-Ziele“* (S. 79)
- *„Planung/Terminierung von Scan-Aufgaben“* (S. 80)

Verwendung des Verknüpfungsmenüs

Für jede Aufgabe steht ein Verknüpfungsmenü zur Verfügung. Mit einem rechten Mausklick können Sie die ausgewählte Aufgabe öffnen.

Für System- und Benutzerdefinierte Aufgaben, stehen im Verknüpfungsmenü folgenden zur Verfügung:

- **Jetzt scannen** - führt die ausgewählte Aufgabe aus und startet einen sofortigen Scan.
- **Pfade** - Öffnet das **Eigenschaften**-Fenster, Reiter Pfade. Hier können Sie das Scan-Ziel für die ausgewählte Aufgabe ändern.Im Falle von Systemaufgaben wird diese Option durch **Scan-Pfade anzeigen** ersetzt.
- **Terminplan** - Öffnet das Fenster **Eigenschaften**, Reiter Terminplan, von wo Sie aus eine ausgewählte Aufgabe terminieren können.
- **Protokolle anzeigen** - Öffnet das Fenster **Eigenschafte**, Reiter Protokolle, in dem Sie die Protokolle sehen können, die nach dem Scan erstellt wurden.
- **Aufgabe klonen** - dupliziert die gewählte Aufgabe.Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.
- **Löschen** - löscht die ausgewählte Aufgabe.

Beachten Sie
Nur für benutzerdefinierte Aufgaben verfügbar. Voreingestellte Aufgaben können nicht gelöscht werden.

- **Eigenschaften** - Öffnet das Fenster **Eigenschaften**, Reiter Übersicht, wo Sie die Einstellungen für die ausgewählte Aufgabe ändern können.

Aufgrund der besonderen Beschaffenheit der Aufgabenkategorie **Verschiedene Aufgaben** können nur die Optionen **Eigenschaften** und **Protokolle ansehen** ausgewählt werden.

Konfiguration der Scan-Einstellungen

Um die Scan-Eigenschaften einer Scan-Aufgabe zu konfigurieren, klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Eigenschaften**.

Sie können die Konfiguration einfach durch das Wählen der Scan-Tiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie den gewünschten Level erreicht haben.Nutzen Sie die Beschreibung auf der rechten Seite, um die Schutzstufe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

Sie können auch folgende allgemeine Optionen konfigurieren:

- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Scans. Andere Programme werden somit schneller ausgeführt, der gesamte Scan dauert damit aber entsprechend länger.
- **Scan-Assistent in Systemleiste minimieren.** Das Scan-Fenster wird in die Symbolleiste minimiert. Wenn Sie auf das BitDefender-Symbol doppelklicken, wird es geöffnet.
- Wählen Sie die Aktion, die durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:

Erfahrene Anwender möchten sich eventuell näher mit den Scan-Einstellungen von BitDefender beschäftigen. Der Scanner kann so eingestellt werden, dass nur spezielle Dateiendungen oder spezielle Malware-Bedrohungen gescannt oder Archive übersprungen werden. So werden die Scan-Zeit verringert und die Antwortzeiten Ihres Rechners während eines Scans verbessert.

Konfiguration der Scan-Einstellungen im Detail:

1. Klicken Sie auf **Benutzerdefiniert**.
2. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.Um herauszufinden, was eine Option bewirkt, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Auch im Internet können Sie hilfreiche Informationen finden.
- **Scan-Einstufung.** Definieren Sie die Art von Malware, die BitDefender scannen soll, indem Sie die passenden Optionen wählen.
- **Dateien scannen.** Sie können BitDefender so programmieren, dass alle Dateien und Anwendungen (Programmdateien) oder nur bestimmte Dateitypen, die Sie als gefährlich einstufen, gescannt werden sollen.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 gegen Malware-Angriffe als andere Typen oder Dateien.Diese Kategorie beinhaltet die folgenden Dateierweiterungen:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Falls Sie sich für die Option **Anwenderdefinierte Erweiterungen scannen** entscheiden, empfehlen wir, dass Sie neben allen anderen Dateierweiterungen,

die Sie als potentiell gefährlich einstufen, auch alle Anwendungserweiterungen mit einschließen.

- **Nur neue und geänderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Archive scannen.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, 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.

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

- **Aktionsoptionen.** Legen Sie die durchzuführende Aktion für jede Kategorie von entdeckten Dateien fest, indem Sie die Optionen in dieser Kategorie verwenden.Es gibt drei Kategorien von gefundenen Dateien:

  - **Infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der BitDefender Malware-Signaturen-Datenbank überein.BitDefender kann im Normalfall Malware-Codes aus einer infizierten Datei entfernen und die Originaldatei wiederherstellen. Diese Aktion wird Desinfektion genannt.

    Beachten Sie
    Malware-Signaturen sind Code-Bruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet.
    Die BitDefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch BitDefender-Mitarbeiter upgedateten Malware-Signaturen.

  - **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.
  - **Verborgene Dateien (Rootkits).** Bitte beachten Sie, dass es sich bei den verborgenen Dateien nicht um absichtlich von Windows verborgenen Dateien handelt. In diesem Fall handelt es um versteckte Dateien, die von speziellen Programmen versteckten werden und als sog Rootkits bekannt sind.Rootkits sind nicht grundsätzlich schädlich. JSie werden jedochhäufig verwendet, um Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

Sie sollten die voreingestellten Aktionen für verdächtige Dateien nicht ändern, es sei denn, Sie haben einen guten Grund dafür.

Um eine neue Aktion festzulegen, klicken Sie auf **Erste Aktion** und wählen die gewünschte Option aus dem Menü.Legen Sie eine **Zweite Aktion** fest, die durchgeführt wird, falls die Erste fehlschlägt.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Scannen** klicken, wird der Scan ausgeführt.

Festlegen der Scan-Ziele

Scan-Ziele der Kategorie **Systemaufgaben** können nicht geändert werden.Das Scan-Ziel wird lediglich angezeigt.Um sich das Scan-Ziel einer bestimmten System-Scan-Aufgabe anzusehen, klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Aufgabenpfade anzeigen**.

Um das Scan-Ziel einer bestimmten Scan-Aufgabe festzulegen, rechtsklicken Sie die auf Aufgabe und wählen **Pfade**. Alternativ, können Sie auch auf den Reiter **Pfade** klicken, wenn Sie sich bereits im Eigenschaften-Fenster befinden.

Sie sehen die Liste mit lokalen Laufwerken, dem Netzwerk und Wechseldatenträgern sowie die kürzlich hinzugefügten Dateien und Verzeichnissen. Alle markierten Einträge werden beim Scan durchsucht.

Folgende Buttons stehen zur Verfügung:

- **Einträge hinzufügen** - öffnet ein Fenster in dem Sie die Dateien/Verzeichnisse auswählen können, die gescannt werden sollen.

Beachten Sie
Sie können die entsprechenden Dateien/Verzeichnisse auch per Drag&Drop in die Liste ziehen.

- **Einträge entfernen** - löscht die vorher für einen Scan ausgewählten Datei(en)/Verzeichnis(se).

Neben diesen Buttons gibt es weitere Optionen für ein schnelles Auswählen der Scan-Ziele.

- **Lokale Laufwerke** - scannt die lokalen Laufwerke.
- **Netzwerklaufwerke** - scannt die verfügbaren Netzwerklaufwerke.
- **Wechseldatenträger** - scannt alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke, USB-Sticks).
- **Alle Einträge** - scannt alle Laufwerke (egal ob sie lokal, im Netzwerk oder wechselbar sind).

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Scannen** klicken, wird der Scan ausgeführt.

Planung/Terminierung von Scan-Aufgaben

Umfassende Scans nehmen einige Zeit in Anspruch und laufen am besten, wenn Sie alle anderen Programme schließen. Aus diesem Grunde ist es ratsam, Scan so zu planen, dass Sie Ihren Computer in dieser Zeit nicht nutzen und er in den Standby-Modus gegangen ist.

Um die Planung einer bestimmten Aufgabe einzusehen oder zu modifizieren, rechtsklicken Sie auf die Aufgabe und wählen **Terminplan**. Falls Sie sich bereits im den Eigenschaften-Fenster der Aufgabe befinden, klicken Sie auf den Reiter **Terminplan** Tab.

Hier können Sie die Einstellungen zum geplanten Scan einsehen.

Wenn Sie Scans planen, müssen Sie eine der folgenden Optionen auswählen:

- **Nein** - führt den Scan nur auf Anfrage des Nutzers hin durch.
- **Einmalig** - führt den Scan einmalig zu einem bestimmten Zeitpunkt aus. Definieren Sie den Startzeitpunkt in den Feldern **Start Datum/Zeit**.
- **Regelmäßig** - führt den Scan regelmäßig in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) durch, beginnend mit dem festgelegten Datum und Uhrzeit.
- **Beim Systemstart** - führt den Scan nach einer festgelegten Anzahl von Minuten durch, nachdem der Benutzer sich bei Windows eingeloggt hat.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Scannen** klicken, wird der Scan ausgeführt.

15.3. Konfiguration der Scan-Ausschlüsse

In manchen Fällen kann es nötig sein, bestimmte Dateien vom Scan auszuschließen. So möchten Sie beispielsweise EICAR Testdateien vom Echtzeit-Scan oder `.avi`-Dateien vom "On-Demand-Scan" ausschließen.

BitDefender bietet die Möglichkeit, Objekte vom On-Access oder On-Deman-Scan oder von beidem auszuschließen. Dies soll der Erhöhung der Scan-Geschwindigkeit dienen und Wechselwirkungen mit Ihrer Arbeit vermeiden.

Zwei Arten von Objekten können vom Scan ausgenommen werden:

- **Pfade** - die Datei oder das Verzeichnis (inklusive der enthaltenen Objekte) dieses speziellen Pfads werden nicht gescannt.
- **Erweiterungen** - alle Dateien mit einer bestimmten Erweiterung werden vom Scan ausgeschlossen, unabhängig von deren Speicherort auf der Festplatte.

Die ausgenommenen Objekte werden nicht gescannt, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

Beachten Sie

Ausschlüsse 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**.

15.3.1. Dateien oder Verzeichnisse vom Scan ausschließen

Um Pfade vom Scan auszuschließen:

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

   Standard-Ansicht

   Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

   Klicken Sie auf den Reiter **Ausschlüsse**.

   Experten-Ansicht

   Gehen Sie zu **Antivirus > Ausschlüsse**.

   Beachten Sie

   In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

3. Markieren Sie das entsprechende Kästchen, um den Scan-Ausschluss zu ativieren.
4. So Starten Sie den Konfigurationsassistenten:
   - Rechtsklicken Sie auf die Tabelle mit den Dateien und Verzeichnissen und wählen Sie **Neuen Pfad hinzufügen**.
   - Klicken Sie auf den **Hinzufügen**-Button, dieser befindet sich am oberen Ende der Ausschluss Tabelle.
5. Folgen Sie dem Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.
   a. Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.Dieser Schritt wird nur eingeblendet, wenn Sie zum Starten des Assistenten auf den Button **Hinzufügen** geklickt haben.
   b. Um einen Pfad vom Scan auszuschließen, verwenden Sie eine der folgenden Methoden:
      - Klicken Sie auf **Durchsuchen** und wählen Sie das gewünschten Verzeichnis bzw. Datei, klicken Sie dann auf **Hinzufügen**.
      - Geben Sie den Pfad, der nicht gescannt werden soll, direkt in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

Der Pfad wird in dem Moment in der Tabelle angezeigt in dem Sie ihn hinzufügen.

c. Voreingestellt sind die Pfade von beiden Scan-Arten, dem On-Access und On-Demand-Scan ausgeschlossen. Um zu ändern, wann eine Ausnahme angewandt werden soll, klicken Sie auf die rechte Spalte und wählen Sie die gewünschte Option aus der Liste aus.

d. Wir empfehlen dringend, die Dateien der festgelegten Pfaden zuscannen, um sicherzustellen, dass diese nicht infiziert sind.Bitte markieren Sie das Kontrollkästchen, um diese Dateien zu scannen, bevor Sie von zukünftigen Scans ausgeschlossen werden.

Klicken Sie auf **Beenden**, um die Ausnahme hinzuzufügen.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

15.3.2. Dateierweiterungen vom Scan ausschließen

Dateierweiterungen vom Scan ausschließen:

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

Standard-Ansicht

Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

Klicken Sie auf den Reiter **Ausschlüsse**.

Experten-Ansicht

Gehen Sie zu **Antivirus > Ausschlüsse**.

Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

3. Markieren Sie das entsprechende Kästchen, um den Scan-Ausschluss zu ativieren.
4. So Starten Sie den Konfigurationsassistenten:
   - Rechtsklicken Sie auf die Erweiterungen Tabelle und wählen Sie **Neue Erweiterungen hinzufügen**.
   - Klicken Sie auf den **Hinzufügen**-Button, dieser befindet sich am oberen Ende der Ausschluss Tabelle.
5. Folgen Sie dem Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

a. Wählen Sie die Option, um eine Dateierweiterung vom Scan auszuschließen.Dieser Schritt wird nur eingeblendet, wenn Sie zum Starten des Assistenten auf den Button **Hinzufügen** geklickt haben.

b. Um die Erweiterungen festzulegen, die vom Scan ausgeschlossen werden sollen, verwenden Sie eine der folgenden Methoden:

- Wählen Sie die Erweiterung, die vom Scannen ausgeschlossen werden soll, aus dem Menü aus und klicken Sie auf **Hinzufügen**.

  Beachten Sie
  Das Menü enthält eine Liste der auf Ihrem System vorhandenen Erweiterungen. Wenn Sie eine Erweiterung auswählen erhalten Sie, falls vorhanden, eine Beschreibung zu dieser.

- Geben Sie die Erweiterung, die vom Scannen ausgeschlossen werden soll, in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

  Die hinzugefügten Erweiterungen sofort in der Tabelle angezeigt wenn Sie sie hinzufügen. Sie können beliebig viele Erweiterungen hinzufügen.

c. Voreingestellt werden die gewählten Erweiterungen von beiden Scan-Typen ausgeschlossen (On-Access und On-Demand-Scan). Um dies zu ändern, klicken Sie auf die rechte Spalte und wählen Sie die gewünschte Option.

d. Wir empfehlen dringend, die Dateien mit den festgelegten Erweiterungen zu scannen, um so sicherzustellen, dass sie nicht infiziert sind.

Klicken Sie auf **Beenden**, um die Ausnahme hinzuzufügen.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

15.3.3. Verwaltung von Scan-Ausschlüssen

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

Verwaltung von Scan-Ausschlüssen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Ausschlüsse**.

Um einen Eintrag aus der Liste zu entfernen, markieren Sie diesen und klicken Sie dann auf den **Entfernen**-Button.

Um einen Eintrag der Liste zu bearbeiten, klicken Sie auf den **Bearbeiten**-Button.Ein neues Fenster öffnet sich. In diesem können Sie wenn nötig die Erweiterungen oder den Pfad, der ausgeschlossen werden soll, (oder den Scan-Typ von dem sie ausgeschlossen werden sollen) ändern. Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf **OK**.

Beachten Sie
Sie können das Objekt auch mit der rechten Maustaste anklicken und die Optionen des Menüs nutzen, um es zu bearbeiten oder zu löschen.

Um die Scan-Ausschlüsse zu deaktivieren, löschen Sie die entsprechende Check-Box.

15.4. Quarantäne

BitDefender ermöglicht die Isolation von infizierten Dateien in einem sicheren Bereich, der so genannten Quarantäne. Durch die Isolation der infizierten Dateien in der Quarantäne reduziert sich das Risiko einer weiteren Infektion. Die infizierten Dateien können zur genaueren Analyse automatisch oder manuell an das BitDefender-Labor gesendet werden.

Beachten Sie
Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Zudem scannt BitDefender nach jedem Update der Malware-Signaturen die Dateien der Quarantäne.Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gespeichert.

Anzeige und Verwaltung der Quarantänedateien und Konfiguration derQuarantäneeinstellungen.

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

   Standard-Ansicht
   Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

   Gehen Sie auf den Reiter **Quarantäne**.

   Experten-Ansicht
   Gehen Sie zu **Antivirus > Quarantäne**.

Beachten Sie
In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

Verwaltung von Quarantäne-Dateien

Sie können jede ausgewählte Datei aus der Quarantäne an das BitDefender-Labor weiterleiten indem Sie auf **Senden** klicken.Voreingestellt überträgt BitDefender die Dateien in Quarantäne alle 60 Minuten.

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**.

Konfiguration der Quarantäne-Einstellungen

Wenn Sie die Quarantäne-Einstellungen konfigurieren möchten klicken Sie auf **Einstellungen**.Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:

Alte Dateien löschen. Um alte Quarantäne-Dateien automatisch zu löschen, aktivieren Sie die entsprechende Option.Sie können festlegen, nach wie vielen Tagen alte Dateien gelöscht werden sollen und wie oft BitDefender diese überprüfen soll.

Dateien automatisch senden. Um Dateien automatisch an das Labor weiterzuleiten, aktivieren Sie diese Option.Geben Sie an, wie oft die Dateien senden soll.

Dateien in der Quarantäne nach einem Update nochmals prüfen. Um Dateien in der Quarantäne nach jedem durchgeführten Update automatisch zu scannen, aktivieren Sie die entsprechende Option.Sie können festlegen, dass gereinigte Dateien automatisch an ihremursprünglichen Speicherort zurückgeschoben werden, indem Sie **Saubere Dateien wiederherstellen** wählen.

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

16. Antiphishing-Schutz

Die BitDefender Antiphishing-Funktion schützt Sie davor, dass persönliche Daten während des Surfens ins Internet gelangen können. Der Benutzer wird über potentielle Phishing-Webseiten alarmiert.

BitDefender bietet den Antiphishing-Schutz in Echtzeit für:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Konfiguration der Antiphishing White List

Sie können eine White List von Webseiten konfigurieren und verwalten. Die in dieser White Liste gelisteten Webseiten werden dann von der Antiphishing-Engine von BitDefender nicht gescannt.Die White List sollte nur Webseiten enthalten, denen Sie vollständig vertrauen.Fügen Sie beispielsweise Webseiten hinzu, auf denen Sie häufig einkaufen.

Beachten Sie

Mit Hilfe der BitDefender Antiphishing-Toolbar in Ihrem Webbrowser können Sie ganz einfach Webseiten zur White List hinzufügen.Weitere Informationen finden Sie unter *„Handhabung des BitDefender Antiphishing-Schutzes in Internet Explorer und Firefox“* (S. 87).

Konfigurierung und Verwaltung der Antiphishing White List:

- Wenn Sie einen unterstützten Web Browser verwenden, klicken Sie auf die BitDefender-Symbolleiste und wählen Sie im Menü **White List**.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
  2. Gehen Sie zu **Antivirus > Schild**.
  3. Klicken Sie auf **White List**.

Um eine Seite zur White List hinzuzufügen geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

Um eine Webseite aus der White List zu entfernen klicken Sie auf den Button **Entfernen**.

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

16.2. Handhabung des BitDefender Antiphishing-Schutzes in Internet Explorer und Firefox

BitDefender integriert sich über eine intuitive und einfach anzuwendende Toolbar in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox

Sie können die Antiphishing-Einstellungen und die White List leicht und effizient über die BitDefender Antiphishing-Leiste in den oben genannten Browsern verwalten.

Die Antiphishing-Leiste, dargestellt durch das BitDefender-Symbol, befindet sich im oberen Bereich des Browsers.Klicken Sie dieses an um die Leiste anzuzeigen.

Beachten Sie
Sollten Sie die Leiste nicht sehen, klicken Sie auf im Menü **Ansicht**, auf **Symbolleisten** und aktivieren Sie **BitDefender Symbolleiste**.

Folgende Aktionen stehen in der Leiste zur Verfügung:

- **Aktivieren/Deaktivieren** - aktiviert/deaktiviert die BitDefender Antiphishing-Leiste im aktuellen Browser.
- **Einstellungen** - öffnet ein Fenster, in dem Sie Einstellungen zur Antiphishing-Leiste vornehmen können.Die folgenden Optionen sind verfügbar:
  - **Echtzeit Antiphishing-Webschutz** - entdeckt und warnt Sie in Echtzeit, wenn eine Webseite "fischt" (also persönliche Informationen stiehlt).Diese Optionen steuert den BitDefender Antiphishing-Schutz ausschließlich im aktuellen Browser.
  - **Vor dem Hinzufügen zur White List fragen** - fragt Sie bevor eine Webseite zur White List hinzugefügt wird.
- **Zur White List hinzufügen** - fügt die momentane Webseite der White List hinzu.

Wichtig
Durch das Hinzufügen zur White List wird die Seite nicht mehr von BitDefender auf Phishing gescannt. Wir empfehlen Ihnen nur Seiten hinzuzufügen, denen Sie vollständig vertrauen.

- **White List zeigen** - Öffnet die White List.Weitere Informationen finden Sie unter *„Konfiguration der Antiphishing White List“* (S. 86).
- **Als Phishing protokollieren** - informiert das BitDefender-Labor dass Sie die fragliche Webseite im Verdacht haben, Datendiebstahl zu begehen.Durch das Melden von Phishing-Webseiten helfen Sie, dass Andere gegen Datendiebstahl geschützt sind.
- **Hilfe** - öffnet die Hilfedatei.

- **Über** - öffnet ein Fenster, in dem Sie Informationen über BitDefender erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.

17. Search Advisor

Der Search Advisor erhöht Ihren Online-Schutz gegen Bedrohungen, indem Sie über Phishing-Versuche und nicht vertrauenswürdige Webseiten direkt auf der Ergebnisseite von Suchmaschinen informiert werden.

Der Suchberater funktioniert mit jedem Web Browser und scannt die angezeigten Suchergebnisse der gängigsten Suchmaschinen:

- Google
- Yahoo!
- Bing

Der Search Advisor zeigt an, ob ein Suchabfrageergebnis sicher ist oder nicht, indem vor dem Link ein kleines Statussymbol eingeblendet ist.

Grüner Kreis mit einem Häkchen: Sie können den Link sicher öffnen.

Roter Kreis mit einem Ausrufezeichen: Dies ist eine Phishing- oder nicht vertrauenswürdige Webseite.Sie sollten diesen Link nicht öffnen.Wenn Sie den Internet Explorer oder Firefox verwenden und versuchen, diesen Link zu öffnen, wird BitDefender diese Webseite automatisch blockieren und eine Warnseite anzeigen.Wenn Sie die Warnungen ignorieren und auf die Webseite zugreifen wollen, folgen Sie den Anweisungen der Warnseite.

17.1. Deaktivierung des Search Advisors

Deaktivierung des Search Advisors:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Präferenzen**.
2. Gehen Sie zu **Sicherheitseinstellungen**.
3. Nutzen Sie den Schalter, um den Search Advisor zu deaktivieren.

18. Antispam

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet.Spams sind ein wachsendes Problem sowohl für Privatpersonen als auch für Unternehmen. Es ist nicht schön, Sie werden nicht wollen dass Ihre Kinder es sehen, Sie können gekündigt werden (weil Sie zu viel Zeit verschwenden oder weil Sie pornografische Nachrichten in Ihren geschäftlichen Mails erhalten) und Sie können Leute nicht davon abhalten, es zu senden. Das Nächstbeste ist es, diese Mailsgar nicht erst zu erhalten. Leider gibt es Spam in einer großen Anzahl von unterschiedlichen Arten und Größen.

BitDefender Antispam greift auf außergewöhnliche technologische Innovationen und Standard-Antispam-Filter zurück, um Spams auszusortieren, bevor dieser im Posteingang landen.Weitere Informationen finden Sie unter *„Antispam-Hintergründe“ (S. 91)*.

Der BitDefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen.POP3 ist eines der am meisten benutzten Protokolle für das Downloaden von Email-Nachrichten vom Mail-Server.

Beachten Sie

BitDefender bietet keinen Antispam-Schutz für Email-Konten, auf die Sie über einen web-basierten Email-Service zugreifen.

Von BitDefender aufgespürte Spams werden in der Betreffzeile mit dem `[spam]`-Marker gekennzeichnet.BitDefender legt Spam-Nachrichten automatisch in einem festgelegten Verzeichnis ab, wie folgt:

- In Microsoft Outlook, werden Spams verschoben in das **Spam**-Verzeichnis, zu finden unter im Verzeichnis **Gelöschte Objekte**.Das **Spam**-Verzeichnis wurde während der Installation von BitDefender erstellt.
- In Outlook Express und Windows Mail werden Spams direkt in **Gelöschte Objekte** verschoben.
- Im Mozilla Thunderbird, werden Spams in das **Spam**-Verzeichnis verschoben, das im Verzeichnis **Trash** zu finden ist.Das **Spam**-Verzeichnis wurde während der Installation von BitDefender erstellt.

Wenn Sie andere Mail Clients verwenden, müssen Sie eine Regel erstellen, damit Email-Nachrichten, die als [spam] markiert sind:`[spam]`von BitDefender in ein benutzerdefiniertes Quarantäne-Verzeichnis verschoben werden.

18.1. Antispam-Hintergründe

18.1.1. Antispam-Filter

Die BitDefender Antispam Engine arbeitet mit verschiedenen Filtern, die sicherstellen, dass Ihr Posteingang spamfrei bleibt: Freundeliste, Spammerliste, Charsetfilter, Bildfilter, URL-Filter, NeuNet (Heuristischer) Filter and Bayesianischer Filter.

Freundeliste/ Spammerliste

Viele Menschen kommunizieren regelmäßig mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Freunde-/Spammerliste** geführt, so können Sie festlegen, welche Emails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

Beachten Sie

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren Email-Adressen der **Freundeliste** hinzufügen, damit sichergestellt ist, dass nur solche Emails an Sie weitergeleitet werden. BitDefender blockt keine Nachrichten von solchen Absendern.

Charset-Filter (Zeichensatzfilter)

Viele der Spam-Mails sind in kyrillisch und/oder asiatisch Zeichensätzen verfasst. Der Schriftsatz-Filter erkennt diese Art von Nachrichten und stuft sie als SPAM ein.

Grafik-Filter

Um die Erkennung von Spam E-Mails durch heuristische Filtermethoden zu erschweren gehen immer mehr Versender von Spam dazu, über nur noch Grafiken zu versenden. Um auch solche E-Mails zu erkennen nutzt der neue **Grafik-Filter** eine Liste mit bereits bekannten Grafiken aus Spam E-Mails und vergleicht diese mit Grafiken aus eingehenden E-Mails. Kommt eine Übereinstimmung zustande so wird die Nachricht als Spam markiert.

URL-Filter

Viele Spam-Mails enthalten Links zu verschiedenen Webseiten (der Inhalt ist meist kommerziell). In der BitDefender-Datenbank sind diese Links aufgeführt.

Diese Datenbank wird von BitDefender ständig aktualisiert.Der URL-Filter scannt jede URL in einer Nachricht und vergleicht Sie mit der Datenbank. Sollten die URLs übereinstimmen wird die Nachricht als SPAM markiert.

NeuNet-Filter (Heuristischer Filter)

Der **Heuristischer Filter** führt eine Reihe von Tests mit allen Nachrichtinhalten durch (z. B. wird nicht nur die Betreffzeile, sondern auch der Nachrichtentext auf

HTML-Text überscannt), hält Ausschau nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spams.Basierend auf dem Resultat der Analyse wird ein SPAM Wert hinzugefügt.

Der Filter erkennt auch Nachrichten, die im Betreff als AUSDRÜCKLICH SEXUELLmarkiert wurden und klassifiziert diese als SPAM.

Beachten Sie

Seit dem 19. Mai 2004 müssen Emails mit sexuellem Inhalt entsprechend markiert werden (mit der `Warnung Ausdrücklich sexuell` in der Betreffzeile muss explizit auf den Inhalt hingewiesen werden.)

Bayesianischer Filter

Der **Bayesianische-Filter** klassifiziert Nachrichten anhand von statistischen Informationen bezüglich spezieller Wörter, die in den Nachrichten auftauchen, als Spam oder Nicht-Spam (nach Ihren Vorgaben oder dem heuristischen Filter).

Dies bedeutet beispielsweise, dass es sich, wenn ein bestimmtes Wort mehrfach erscheint, sich mit hoher Wahrscheinlichkeit um einen Spam handelt. Alle relevanten Wörter innerhalb einer Nachricht werden einbezogen.

Dieser Filter bietet eine weitere interessante Charakteristik: er ist lernfähig. Er speichert Informationen einer empfangenen Nachricht eines bestimmten Nutzers. Um korrekt zu funktionieren, muss der Filter trainiert werden, was bedeutet, dass er mit Mustern von legitimen Nachrichten gefüllt werden sollte. Ab und zu muss der Filter aktualisiert werden, besonders dann, wenn er eine falsche Entscheidung getroffen hat.

Wichtig

Sie korrigieren den bayesianischen Filter, indem Sie die **Ist Spam** und **Kein Spam** -Buttons in der Antispam-Symbolleiste benutzen.

18.1.2. Antispam-Vorgang

Die BitDefender Antispam Engine kombiniert alle Antispam-Filter um festzustellen, ob eine bestimmte Email in den **Posteingang** gelangen sollte, oder nicht.

Jede Email, die aus dem Internet kommt, wird zuerst mit den Filtern der Freundeliste/Spammerliste geüberscannt. Falls der Sender in der Freundeliste gefunden wird, wird diese Mail direkt in Ihren **Posteingang** gesendet.

Der Filter Spammerliste scannt, ob der Absender der Email auf der gleichnamigen Liste eingetragen ist. Falls dem so ist, wird die Email als Spam markiert und in den **Spam**-Verzeichnis verschoben.

Der Zeichensatz-Filter scannt, ob die Email in kyrillisch oder mit asiatischen Schriftzeichen geschrieben worden ist. Wenn dem so ist, wird die Mail markiert und in den **Spam**-Verzeichnis verschoben.

Falls die Email diese Merkmale nicht aufweist, wird sie mit dem Grafik-Filter gescannt. Der **Grafik-Filter** erkennt Email-Nachrichten, die Bilder bzw. Grafiken und Spam-Inhalte beinhalten.

DerURL-Filter vergleicht die in Emails gefundenen Links mit den Links der BitDefender-Datenbank bekannter Spam-Links. Findet BitDefender eine Übereinstimmung, wird die Email als SPAM eingestuft.

Der NeuNet/Heuristische Filter testet die Emails auf den Inhalt und sucht nach Wörtern, Phrasen, Links oder anderen Charakteristiken von SPAMs.Basierend auf den Analyseergebnissen erhält die Email eine Spam-Marke.

Beachten Sie
Wenn die email in der Betreffzeile als „ausdrücklich sexuell“ gekennzeichnet wurde, stuft BitDefender die Email als Spam ein.

Der Bayesianische-Filter analysiert die Nachricht aufgrund statistischer Informationen in Bezug auf spezielle Wörter und vergleicht diese mit denen, die nicht als Spam klassifiziert sind. Das Ergebnis ist das Hinzufügen eines Spam-Score an die Email.

Wenn das Gesamt-Spam-Ergebnis (heuristische Einstufung + Bayesianische Einstufung) den Schwellenwert übersteigt, wird die Email als SPAM eingestuft.Die Schwelleneinstellung hängt ab von der Antispam Schutzeinstellung.Weitere Informationen finden Sie unter *„Anpassen der Sicherheitsstufe“ (S. 99)*.

18.1.3. Antispam-Updates

Bei jedem durchgeführten Update werden:

- werden neue Bildsignaturen dem **Grafik-Filter** hinzugefügt.
- werden neue Links dem **URL-Filter** hinzugefügt.
- werden dem **Heuristik-Filter** neue Regeln hinzugefügt.

Somit wird die Effektivität des AntiSpam-Moduls laufend verbessert.

Für einen fortlaufenden Schutz führt BitDefender automatische Updates durchführen. Lassen Sie daher die Funktion **Automatische Update** aktiviert.

18.2. Antispam Optimierungs-Assistent

Beim ersten Start Ihres Mail-Clients nach der Installation von BitDefender öffnet sich ein Assistent, der Sie dabei unterstützt, den Bayesianischen-Filter zu trainieren, sowie die Freundeliste und die Spammerliste zu konfigurieren, um die Effektivität der Antispamfilter zu erhöhen.

Beachten Sie
Der Assistent kann jederzeit über den Button **Assistent** in der Antispam-Symbolleisteaufgerufen werden.

Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Wenn Sie einen Konfigurationsschritt überspringen möchten, wählen Sie **Überspringen**.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Begrüßungsfenster**
2. **Kontakte zur Freundeliste hinzufügen**

   Hier sehen Sie alle Ihre Adressen aus Ihrem **Adressbuch**. Bitte wählen Sie all die Adressen aus, die Sie Ihrer **Freundeliste** hinzufügen möchten (wir empfehlen Ihnen, alle zu markieren). Sie werden dann alle Emails von diesen Adressen erhalten, egal welchen Inhalts.

   Um einen Kontakt zur Freundeliste hinzuzufügen, klicken Sie auf **Alle auswählen**.
3. **Bayesianische Datenbank löschen**

   Beachten Sie
   Wenn Sie den Assistenten das erste Mal ausführen, gehen Sie einfach zum nächsten Schritt.

   Sie haben eventuell bemerkt, dass Ihr Antispam-Filter an Effektivität verloren hat. Dies kann daher kommen, dass das Training nicht genau durchgeführt worden ist (z. B. haben Sie versehentlich eine Anzahl legitimer Mails als Spam markiert oder umgekehrt). Falls Ihr Filter sehr ungenau arbeitet, müssen Sie die Filterkriterien in Ihrer Datenbank löschen und neu definieren. Dabei hilft Ihnen der Assistent.

   Wählen Sie **Antispam Datenbank leeren**, wenn Sie die bayesianische Datenbank zurücksetzen möchten.

   Sie können die Bayes Datenbank in eine Datei speichern um Sie für andere BitDefender-Produkte oder nach einer BitDefender Neuinstallation verwenden zu können.Um die Datenbank des Bayes Filters zu speichern, klicken Sie auf den Button **Bayes speichern** und speichern Sie sie am gewünschten Speicherort.Die Datei wird `mit der Erweiterung.dat` gepeichert.

   Um eine gespeicherte Bayes Datenbank zu laden, wählen Sie **Bayes laden** und öffnen die entsprechende Datei.
4. **Trainieren des Bayesianischen Filters mit legitimen (Nicht-Spam) Emails**

   Bitte wählen Sie einen Verzeichnis, der legitime Emails enthält. Diese Nachrichten werden genutzt, um den Antispam-Filter zu trainieren.

   In der Verzeichnisliste finden Sie zwei weitere erweiterte Optionen:
   - **UnterVerzeichnis mit einbeziehen** - um UnterVerzeichnis in Ihre Auswahl mit einzubeziehen.
   - **Automatisch der Freundeliste hinzufügen** - um den Sender zu der Liste der Freunde hinzuzufügen.
5. **Trainieren des Bayesianischen Filter mit existierenden Spam-Emails**

Bitte wählen Sie einen Verzeichnis, der Spam-E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam-Filter zu trainieren.

Wichtig

Bitte vergewissern Sie sich, dass das von Ihnen gewählte Verzeichnis keine legitimen Emails enthält, ansonsten wird die Antispam-Leistung beträchtlich reduziert.

In der Verzeichnisliste finden Sie zwei weitere erweiterte Optionen:

- **UnterVerzeichnis mit einbeziehen** - um UnterVerzeichnis in Ihre Auswahl mit einzubeziehen.
- **Automatisch der Spamerliste hinzufügen** - um den Sender zu der Liste der Spammer hinzuzufügen.Email Nachrichten von diesem Sender werden immer als SPAM markiert und dementsprechend verarbeitet.

6. **Übersicht**

   In diesem Fenster können Sie alle Einstellungen einsehen, die mit dem Konfigurationsassistenten durchgeführt worden sind. Sie können noch Änderungen vornehmen, indem Sie zum vorherigen Fenster zurückkehren (**Zurück**).

   Wenn Sie keine Änderungen vornehmen wollen, klicken Sie auf **Fertigstellen**.

18.3. Verwendung der Antispam-Symbolleiste im Fenster "Ihr Mail Client"

Im oberen Teil Ihres Mail Client-Fensters sehen Sie die Antispam-Leiste.Die Antispam-Leiste hilft Ihnen beim Verwalten des Antispam-Schutzes direkt aus dem Email Client heraus.Sie können BitDefender ganz einfach korrigieren, falls eine reguläre Mail als Spam markiert wurde.

Wichtig

BitDefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Eine Komplettliste der unterstützten Email Clients finden Sie unter: *„Software-Anforderungen“* (S. 2).

Unten stehend finden Sie eine Beschreibung aller Buttons der BitDefender-Symbolleiste:

- **Ist Spam** - klicken Sie auf diesen Button und der Bayes-Filter erkennt die ausgewählten Mails als Spam. Sie werden als Spam markiert und in das **Spam**-Verzeichnis verschoben.

  Zukünftige Mails mit diesem Muster werden alle als Spam markiert.

- **Kein Spam** - teilt dem Bayes-Filter mit, dass die ausgewählte Email kein Spam ist und BitDefender sie nicht hätte markieren sollen.Die Email wird aus dem **Spam** -Verzeichnis in den **Posteingang** verschoben.

Zukünftige Emails mit diesem Muster werden nicht mehr als Spam markiert.

Wichtig

Der Button **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben von BitDefender (normalerweise werden diese Nachrichten in den **Spam**-Verzeichnis verschoben).

- **Spammer hinzufügen** - fügt den Absender der ausgewählten Email der Liste der Spammer hinzu.Klicken Sie zur Bestätigung **OK**.Die Email-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch als `[spam]` markiert.
- **Freund hinzufügen** - fügt den Sender der ausgewählten Email der Freundes-Liste hinzu.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt alle Emails dieses Absenders unabhängig von deren Inhalten empfangen.
- **Spammer** - öffnet die **Spammerliste**. Sie enthält alle Email-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts.Weitere Informationen finden Sie unter *„Konfiguration der Spammerliste“ (S. 100)*.
- **Freunde** - öffnet die **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts.Weitere Informationen finden Sie unter *„Konfiguration der Freundeliste“ (S. 99)*.
- **Einstellungen** - öffnet das Fenster **Einstellungen**, indem Sie weitere Optionen für das **Antispam**-Modul angeben können.
- **Assistent** - öffnet den Antispam Optimierungs-Assistenten.Mithilfe dieses Assistenten können Sie den Bayes-Filter füttern, um die Effizienz Ihres Antispam-Schutzes zu erhöhen.Sie können auch Adressen aus Ihrem Adressbuch der Freunde-/Spammer Liste hinzufügen.
- **BitDefender Antispam** - öffnet ein Fenster, in dem Sie die Antispam-Schutzeinstufung und die Antispam-Filter konfigurieren können.

18.3.1. Anzeige von Feststellungsfehler

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach den Antispam-Filter einfach korrigieren (indem Sie angeben, welche Emails nicht als `[spam]` markiert werden sollen). Dadurch wird die Effektivität des Antispam-Filters erheblich verbessert.Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie in das Junk Mail-Verzeichnis, in das die Spam-Nachrichten verschoben werden.
3. Wählen Sie die Nachricht, die von BitDefender fälschlicherweise als `[spam]` markiert wurde, aus.

4. Klicken Sie auf **Freund hinzufügen** in der BitDefender Antispam Toolbar.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt alle Emails dieses Absenders unabhängig von deren Inhalten empfangen.
5. Klicken Sie in der BitDefender Antispam-Symbolleiste (normalerweiseim oberen Teil des Mail Client-Fensters) auf **Kein Spam**. Dies teilt dem Bayes-Filter, dass die ausgewählte Nachricht kein Spam ist. Die Nachricht wird dann in den Posteingang verschoben.Die nächsten Emails, die dem gleichen Muster entsprechen, werden nicht als `[spam]` markiert.

18.3.2. Anzeige unentdeckter Spam-Nachrichten

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach angeben, welche Email-Nachrichten als Spam hätten markiert werden sollen. Dadurch erhöht sich die Effizienz des Antispam-Filters.Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie in den Posteingang.
3. Markieren Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der BitDefender Antispam-Symbolleiste (normalerweise im oberen Teil des Mail Client-Fensters) auf **Ist Spam**. Dies sagt dem Bayes-Filter dass es sich bei den ausgewählten Nachrichten um eine Spam-Nachricht handelt. Sie wird dann sofort als `[spam]` markiert und in den Junk Mail-Verzeichnis verschoben.Die nächsten Email-Nachrichten, mit demselben Muster werden automatisch als `[spam]` markiert.

18.3.3. Erneutes Trainieren des Bayes Filters

Arbeitet Ihr Antispam-Filter sehr ungenau arbeiten, sollten Sie eventuell die Bayes Datenbank aufräumen und den Bayes Filter neu definieren.

Bevor Sie den Bayes Filter trainieren, legen Sie ein Verzeichnis an, in dem ausschließlich Nachrichten enthalten sind sowie ein zweites Verzeichnis, das nur SPAM enthält.Der Bayes Filter wird trainiert, indem er die Verzeichnisse analysiert und lernt die Charakteristiken von Spams und legitimierten Nachrichten zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen mindestens 50 Nachrichten in jedem Verzeichnis vorhanden sein.

Um die Bayes Datenbank zurückzusetzen und sie neu zu trainieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der BitDefender Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.

4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispam-Filterdatenbank leeren** und klicken Sie auf **Weiter**.
6. Wählen Sie das Verzeichnis mit legitimierten Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie das Verzeichnis mit den SPAM-Nachrichten und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertigstellen** um den Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie auf **Schließen**.

18.3.4. Speichern und Laden der Bayes Datenbank

Sie können die Bayes Datenbank in eine Datei speichern um Sie für andere BitDefender-Produkte oder nach einer BitDefender Neuinstallation verwenden zu können.

Klicken Sie in der BitDefender Antispam-Symbolleiste auf den Button **Einstellungen**.

Um die Datenbank des Bayes Filters zu speichern, klicken Sie auf den Button **Bayes speichern** und speichern Sie sie am gewünschten Speicherort.Die Datei wird `mit der Erweiterung.dat` gepeichert.

Um eine gespeicherte Bayes Datenbank zu laden, wählen Sie **Bayes laden** und öffnen die entsprechende Datei.

18.3.5. Konfiguration der allgemeinen Einstellungen

Um die allgemeinen Antispam-Einstellungen für Ihren Mail Client zu konfigurieren, klicken Sie auf den Button **Einstellungen** in der BitDefender Antispam-Symbolleiste.

Die folgenden Optionen sind verfügbar:

- **Nachrichten in "Gelöschte Objekte" verschieben** verschiebt als Spam erkannte E-Mails in ein Unterverzeichnis des **Papierkorbs** (gilt nur für Outlook Express bzw. Windows Mail).
- **Nachricht als gelesen markieren** - markiert alle Spam Nachrichten als gelesen und stört somit den Arbeitsablauf nicht, wenn neue Nachrichten eintreffen.

Klicken Sie auf den Reiter **Alarme**, um Zugriff auf den Bereich zu erhalten, in dem Sie die Einblendung des Bestätigungsfensters für **Spammer hinzufügen** und **Freunde hinzufügen** deaktivieren können.

Im **Alarme** - Fenster können Sie die Anzeige des Alarms **Bitte wählen Sie eine Email-Nachricht** aktivieren/deaktivieren. Dieser Alarm wird eingeblendet wenn Sie eine Gruppe anstatt einer Email-Nachricht auswählen.

18.4. Anpassen der Sicherheitsstufe

Einige der Antispam-Filter können Spam-Emails direkt erkennen, andere fügen der Email eine Spam-Markierung hinzu, die auf den festgestellten Spam-Eigenschaften basiert.

Die Antispam-TresorSicherheitsstufe dient der Einschätzung einer Email als Spam, basierend auf deren Gesamt-Spam-Einstufung (die Sie erhalten, nachdem die Mail durch alle Antispam-Filter gelaufen ist).

Sie sollten die Antispam-TresorSicherheitsstufe nicht verändern, es sei denn, der Antispam-Tresor funktioniert nicht wie erwartet.Bevor Sie aber unabhängig die Tresoreinstellung ändern, empfehlen wir Ihnen, dass Sie sich zuerst den Punkt *„Antispam-Filter funktioniert nicht richtig“ (S. 188)* durchlesen, um das Problem zu beheben.

Um die Antispam-Sicherheitsstufe anzupassen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antispam > Status**.
3. Schieben Sie den Regler in die gewünschte TresorSicherheitsstufen-Position.Um den gewünschten Tresor-Level einzustellen. (**Moderat bis Aggressiv**), klicken Sie auf Sie **Standardeinstufung**.

Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.Die Beschreibung informiert Sie auch über zusätzlichen Aktionen, die Sie durchführen sollten, um mögliche Probleme zu vermeiden oder um die Effizienz des Antispams zu erhöhen.

18.5. Konfiguration der Freundeliste

Die **Freundeliste** ist eine Liste aller Email-Adressen, von denen Sie immer Mails erhalten wollen, egal welchen Inhalts diese sind. Nachrichten Ihrer Freunde werden nicht als Spam deklariert, auch wenn der Inhalt dem von Spams ähnlich sein sollte.

Beachten Sie
Jede Mail von einer Adresse Ihrer **Freundeliste** wird automatisch in Ihren Posteingang verschoben.

Konfigurierung und Verwaltung der Freundeliste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie auf den Button **Freunde** in der BitDefender Antispam-Symbolleiste, die in Ihren Mail Client integriert ist.
- Alternativ folgen Sie diesen drei Schritten:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antispam > Status**.
3. Klicken Sie auf **Freunde verwalten**.

Um eine Email-Adresse hinzuzufügen, wählen Sie die Option **Email-Adresse**, geben Sie die Adresse ein und klicken Sie auf den Button neben dem Bearbeiten-Feld.Syntax: name@domain.de.

Um alle Email-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie weiter zum Bearbeiten-Feld.Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *domain* - alle eingehenden Mails von domain werden ohne Überprüfung Ihres Inhaltes in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- *de - alle Mails mit der Domain-Endung de werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.Sie können beispielsweise die Email-Domain der Firma, für die Sie arbeiten, oder die von vertrauenswürdigen Partnern hinzufügen.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach zur Bestätigung auf **Ja**.

Sie können die Freundeliste speichern, so dass diese auf einem anderen Rechner oder nach einer Neuinstallation genutzt werden kann.Um die Freundeliste zu speichern klicken Sie auf **Speichern** und speichern Sie diese am den gewünschten Speicherort.Die Datei wird über die Erweiterung `.bwl` verfügen.

Um eine zuvor gespeicherte Freundeliste zu laden, klicken Sie auf **Laden** und öffnen die entsprechende `.bwl` Datei.Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Aktuelle Liste überschreiben**.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Freundeliste** zu schließen.

18.6. Konfiguration der Spammerliste

Spammerliste - Liste mit allen Email-Adressen, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts.Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.

Konfigurierung und Verwaltung der Spammer-Liste:

- Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, klicken Sie auf den Reiter **Spammer** in der BitDefender Antispam-Symbolleiste, die in Ihren Mail Client integriert ist.
- Alternativ folgen Sie diesen drei Schritten:
  1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
  2. Gehen Sie zu **Antispam > Status**.
  3. Klicken Sie auf **Spammer verwalten**.

Um eine Email-Adresse hinzuzufügen, wählen Sie die Option **Email-Adresse**, geben Sie die Adresse ein und klicken Sie auf den Button neben dem Bearbeiten-Feld.Syntax: name@domain.de.

Um alle Email-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie weiter zum Bearbeiten-Feld.Syntax:

- @domain.de, *domain.de und domain.de - alle eingehenden Mails von domain.de werden als Spam markiert;
- *domain* - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- *com - alle Mails mit dieser Endung com werden als Spam markiert.

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.

Warnung

Fügen Sie keine legitimen web-basierten Email-Anbieter (wie: Yahoo, Gmail, Hotmail oder andere) zu der Spammerliste hinzu. Andernfalls werden die E-Mail-Nachrichten, die von jedem möglichen Benutzer solch eines Anbieters gesendet werden, als Spam eingestufft.z.B: Wenn Sie beispielsweise `yahoo.com` der Spammerliste hinzufügen, werden alle Emails die von `yahoo.com` Adressen kommen, als `[spam]` markiert.

Um einen Eintrag aus der Liste zu entfernen markieren Sie diesen und klicken Sie dann auf **Entfernen**.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach zur Bestätigung auf **Ja**.

Sie können die Spammerliste in eine Datei sichern, damit Sie sie nach einer Neuinstallation oder auf einem anderen Computer nutzen können.Um die Spammerliste zu speichern klicken Sie auf **Speichern** und speichern sie diese am gewünschten Speicherort.Die Datei wird über die Erweiterung `.bwl` verfügen.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **Laden** und öffnen die entsprechende `.bwl`-Datei.Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Aktuelle Liste überschreiben**.

Klicken Sie auf **Übernehmen** und **OK**, um zu speichern und um die **Spammerliste** zu schließen.

18.7. Konfiguration der Antispam-Filter und -Einstellungen.

Wie in *„Antispam-Hintergründe“* (S. 91) beschrieben, nutzt BitDefender eine Kombination aus unterschiedlichen Antispam-Filtern, um Spams zu identifizieren.Die Antispam-Filter sind für einen effizienten Tresor vorkonfiguriert.

Sie können jeden dieser Filter deaktivieren oder dessen Einstellungen verändern, dies wird jedoch nicht empfohlen.Dies sind einige Änderungen, die Sie eventuell vornehmen möchten:

- Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt.

  Beachten Sie

  Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendetn(wie z. B. in der russischen oder chinesischen Programmversion).

- Wenn Sie nicht möchten, dass der Empfänger Ihrer gesendeten Email automatisch der Freundeliste hinzugefügt wird, können Sie die entsprechende Einstellung deaktivieren.In diesem Fall fügen Sie Ihre Kontakte der Freundeliste wie in *„Konfiguration der Freundeliste“* (S. 99) beschrieben hinzu.
- Fortgeschrittene Anwender können versuchen, die Größe des Bayes-Wörterbuches anzupassen, um so bessere Antispam-Ergebnisse zu erzielen.Eine geringere Anzahl an Worten resultiert in einer schnelleren, aber weniger präzisen Antispam-Verarbeitung.Eine höhere Anzahl an Wörtern erhöht die Genauigkeit des Antispams, dadurch wird aber auch die Zugriffszeit auf Ihre Emails länger.

  Beachten Sie

  Es können mehrere Anpassungen des Bayes-Wörterbuches notwendig sein, um das gewünschte Ergebnis zu erzielen.Wenn das Ergebnis nicht wie erwartet ist, setzten Sie die Voreinstellung auf die empfohlene Größe von 200.000 Wörtern zurück.

Um die Antispam-Einstellungen und Filter zu konfigurieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antispam > Einstellungen**.

3. Konfigurieren Sie die Einstellungen nach Ihren Wünschen. Um herauszufinden, was eine Option bewirkt, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Wenn Sie die Standardeinstellungen anwenden möchten, klicken Sie auf **Voreingestellt**.

19. Kindersicherung

Die BitDefender Kindersicherung ermöglicht es Ihnen den Zugriff auf dasInternet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkontoauf dem System zu kontrollieren.

Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Der Internetzugang zu bestimmten Zeiten (beispielsweise während der Schule).
- Webseiten, Mails und Instant Messaging-Nachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat oder Filesharing-Programme.
- Instant Messages, die nicht von erlaubten IM-Kontakten gesendet werden.

Wichtig

Nur Benutzer mit administrativen Rechten (Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.Um sicherzustellen, dass nur Sie die Einstellungen der Kindersicherung für alle Benutzer ändern können, sichern Sie sie mit einem Passwort.Sie werden dazu aufgefordert, das Passwort zu konfigurieren, wenn Sie die Kindersicherung für einen bestimmten Benutzer aktivieren.

Sobald Sie die Kindersicherung konfiguriert haben, können Sie einfach herausfinden, was Ihre Kinder auf dem Computer machen.

Auch wenn Sie nicht zu Hause sind, können Sie dennoch die Aktivitäten Ihrer Kinder überprüfen und die Einstellungen über die Remote Kindersicherung ändern.

19.1. Konfiguration der Kindersicherung

Bevor Sie mit der Konfiguration der Kindersicherung beginnen, erstellen Sie bitte für jedes Kind ein separates Benutzerkonto. Dadurch wissen Sie genau, was jedes Ihrer Kinder auf dem Computer macht. Sie sollten beschränkte (Standard) Benutzerkonten erstellen, so dass Ihre Kinder die Einstellungen der Kindersicherung nicht ändern können.Weitere Informationen finden Sie unter *„Wie erstelle ich ein Windows Benutzerkonto?“* (S. 172).

Haben Ihre Kinder Zugriff auf ein Administrator-Benutzerkonto auf ihrem Computer, müssen Sie ein Passwort festlegen, um die Einstellungen der Kindersicherung zu schützen.Weitere Informationen finden Sie unter *„Tresor der Kindersicherungs-Einstellungen“* (S. 106).

Konfiguration der Kindersicherung:

1. Stellen Sie sicher, dass Sie auf dem Computer eingeloggt sind, auf dem sich das Administrator-Benutzerkonto befindet.Nur Benutzer mit administrativen Rechten

(Systemadministratoren) können auf die Kindersicherung zugreifen und sie konfigurieren.

2. Öffnen Sie BitDefender.
3. Abhängig von der gewählten Ansicht greifen Sie auf die Kindersicherung wie folgt zu:

   Standard-Ansicht
   Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Kindersicherung**.

   Experten-Ansicht
   Klicken Sie im linken Menü auf **Kindersicherung**.

Beachten Sie

In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

Sie können Informationen bezüglich des Status der Kindersicherung für jedes WindowsBenutzerkonto einsehen.Die Alterskategorie erscheint unterhalb jedes Benutzernamens, wenn die Kindersicherung aktiviert ist.Wenn die Kindersicherung deaktiviert, ist der Status **nicht konfiguriert**.

Konfiguration der Kindersicherung für ein bestimmtes Benutzerkonto:

1. Verwenden Sie den Regler, um die Kindersicherung für dieses Benutzerkontozu aktivieren.
2. Sie werden aufgefordert, das Passwort für die Kindersicherung festzulegen.Stellen Sie ein Passwort ein, um Ihre Einstellungen für die Kindersicherung zu schützen.Weitere Informationen finden Sie unter *„Tresor der Kindersicherungs-Einstellungen“* (S. 106).
3. Legen Sie die Alterskategorie fest, so dass Ihrem Kind nur Zugriff auf altersgemäße Webseiten gestattet wird.Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.
4. Wenn Sie die Einstellungen für die Kindersicherungen im Detail konfigurieren möchten, klicken Sie auf **Einstellungen**.Klicken Sie auf einen Reiter, um die entsprechenden Kindersicherungs-Funktionen zu konfigurieren.

   - **Internet** - um die Web-Navigation gemäß der von Ihnen festgelegtenRegeln im Bereich Internet zu filtern.
   - **Anwendungen** - blockiert den Zugang auf die Programme, die Sie im Abschnitt Anwendungen festgelegt haben.

- **Schlüsselwörter** - filtert den Web-, Mail- und Instant Messaging-Zugriff nachden Regeln, die Sie im Abschnitt Schlüsselwörter festgelegt haben.
- **Messaging** - um den Chat mit IM-Kontakten, entsprechend der von Ihnen im Abschnitt Messaging festgelegten Regeln zu erlauben oder zu sperren.

Konfigurieren Sie die Überwachungsoptionen nach Ihren Bedürfnissen:

- **Aktivitätsbericht per Email an mich senden.** Eine Email-Benachrichtigung wird versendet, sobald die BitDefender-Kindersicherung eine Aktivität dieses Nutzers blockiert hat.Sie müssen zuerst die Benachrichtigungseinstellungen konfigurieren.
- **Internet-Datenverkehr-Protokoll speichern.** Protokolliert die besuchten Webseiten für Benutzer, für die die Kindersicherung aktiviert ist.

Weitere Informationen finden Sie unter *„Überwachung der Kinderaktivitäten“* (S. 113).

Wenn Sie die Computer-Aktivitäten Ihrer Kinder per Fernsteuerung überwachen und steuern möchten, aktivieren Sie mit diesem Schalter die Remote Kindersicherung.Weitere Informationen finden Sie unter *„Remote Kindersicherung“* (S. 116).

19.1.1. Tresor der Kindersicherungs-Einstellungen

Wenn Sie nicht der einzige Benutzer des Computers mit administrativen Rechten sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen der Kindersicherung mit einem Passwort zu schützen.Wenn Sie ein Passwort festlegen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.

BitDefender wird Sie nach der Festlegung eines Passwortes fragen, sobald Sie dieKindersicherung aktivieren.Um den PasswortTresor zu definieren, gehen Sie wie folgt vor:

1. Geben Sie das Passwort in das Feld **Passwort** ein.
2. Geben Sie das Passwort erneut in das Feld **Passwort wiederholen** ein, um es zu bestätigen.
3. Klicken Sie auf **OK**, um das Passwort zu speichern und das Fenster zu schließen.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen der Kindersicherung ändern wollen.Andere Systemadministratoren (falls vorhanden) müssen dieses Passwort ebenfalls angeben um Einstellungen der Kindersicherung zu ändern.

Beachten Sie

Dieses Passwort schützt nicht die anderen Einstellungen von BitDefender.

Wenn Sie kein Passwort definieren wollen und nicht möchten, dass dieses Fenster erneut eingeblendet wird, aktivieren Sie die Option **Nicht nach Passwort fragen,wenn die Kindersicherung aktiviert wird**.

Wichtig

Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von BitDefender kontaktieren.

Entfernen des PasswortTresores:

1. Öffnen Sie BitDefender und klicken Sie in der rechten oberen Bildschirmecke auf **Optionen**.
2. Gehen Sie zu **Allgemeine Einstellungen**.
3. Über den Schalter können Sie die Option **Passworteinstellungen** deaktivieren.
4. Geben Sie das Passwort ein.
5. Klicken Sie auf **OK**.

19.1.2. Internetkontrolle

Die **Web-Seiten-Kontrolle** ermöglicht Ihnen, Web-Seiten mit fragwürdigem Inhalt zu sperren. Eine Liste geblockter Webseiten und Teilbereichen ist Ihnen bereits zur Verfügung gestellt und im Verlauf des normalen Update-Prozesses konstant erneuert.

Beachten Sie

Wenn Sie die Kindersicherung aktivieren und das Alter Ihres Kindes festlegen, wird die Internetkontrolle automatisch aktiviert und konfiguriert, um den Zugriff auf für das Alter Ihres Kindes unangemessene Webseiten zu blockieren.

Konfiguration der Internetkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der BitDefender-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Internet** .
3. Nutzen Sie den Schalter um die Internetkontrolle zu aktivieren.
4. Sie können nun überprüfen, welche Web-Kategorien für die aktuell ausgewählteAltersgruppe automatisch gesperrt/beschränkt werden.Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie diese nach Ihren Wünschen konfigurieren.

   Um die Aktion, die für bestimmte Kategorien von Webinhalten definiert wurde, zu ändern, klicken Sie auf den aktuellen Status und wählen Sie im Menü die gewünschte Aktion.
5. Wenn Sie eigene Regeln erstellen möchten, um bestimmte Webseiten zu blockieren oder zuzulassen.Wenn die Kindersicherung automatisch den Zugriff

auf eine Webseite blockiert, können Sie eine Regel definieren, die den Zugriff auf diese Webseite explizit erlaubt.

6. Sie können Limits definieren, wie lange Ihr Kind im Internet surfen darf.Weitere Informationen finden Sie unter „Zeitliche Beschränkung des Internetzugangs“ (S. 108).

Erstellung von Internetkontrollregeln

Um den Zugriff auf eine Webseite zu blockieren oder zu erlauben, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Webseite zulassen** oder **Webseite blockieren**.
2. Geben Sie die Adresszeile der Internetseite in das Feld **Webseite** ein.
3. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Sperren**.
4. Klicken Sie auf **Beenden**, um die Regel hinzuzufügen.

Verwaltung von Internetkontrollregeln

Die bereits konfigurierten Webseiten-Kontrollregeln sind in der Tabelle am unterenRand des Fensters aufgelistet. Die Adresse und der aktuelle Status jederWebkontroll-Regel werden aufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

Zeitliche Beschränkung des Internetzugangs

Im Bereich "Internetzugriff festlegen" können Sie definieren, wie viel Zeit Ihr Kind im Internet surft.

Um den Zugriff auf das Internet komplett zu sperren, wählen Sie **Internetzugriff sperren**.

Um Beschränkung des Internetzugangs auf bestimmte Tageszeiten festzulegen:

1. Wählen Sie **Zeitlimit Internetzugang**.
2. Klicken Sie auf **Terminplan ändern**.
3. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll.Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren.
4. Klicken Sie auf **Speichern**.

Beachten Sie

BitDefender führt unabhängig davon, ob der Internetzugriff gesperrt ist, stündliche Updates durch.

19.1.3. Programmkontrolle (Anwendungskontrolle)

Über die **Programmkontrolle** können Sie die Ausführung beliebiger Anwendungen sperren. Spiele, Medien- und Messaging Software als auch andere Programmkategorien oder Malware können so blockiert werden. Programme, die über diesen Weg gesperrt sind, können weder verändert, kopiert noch verschoben werden.Sie können Anwendungen permanent oder nur für bestimmte Zeitintervalle sperren (beispielsweise für den Zeitraum, in dem Ihre Kinder die Hausaufgaben erledigen).

Konfiguration der Programmkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der BitDefender-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Anwendungen**.
3. Aktivieren Sie die Programmkontrolle.
4. Erstellen Sie für die Anwendungen, die Sie sperren oder beschränken möchten, Regeln.

Erstellung von Anwendungskontrollregeln

Um den Zugriff auf eine Anwendung zu beschränken oder zu blockieren, gehen Siefolgendermaßen vor:

1. Klicken Sie auf **Anwendung blockieren** oder **Anwendung beschränken**.
2. Klicken Sie auf **Durchsuchen**, um die Anwendung, für die Sie den Zugriff blockieren/einschränken wollen, herauszusuchen.Installierte Anwendungen befinden sich in Normalfall im Verzeichnis `C:\Programmdateien`.
3. Wählen Sie die gewünschte Aktion:
   - **Dauerhaft sperren**, um den Zugriff auf die Anwendung vollständig zusperren.
   - **Sperren basierend auf dieser Planung**, um den Zugriff für bestimmteZeitintervalle einzuschränken.

   Wenn Sie sich für eine zeitliche Beschränkung anstatt einer Komplettsperrung einzuschränken entschieden haben, müssen Sie im Planungsraster die Tage und Zeitintervalle auswählen, währenddessen der Zugriff gesperrt ist.
4. Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

Verwaltung von Anwendung skontrollregeln

Die bereits erstellten Anwendungskontrollregeln werden in der Tabelle am unterenEnde des Fensters aufgelistet. Für jede Regel wird der Name der Anwendung, der Pfad und der aktuelle Status aufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

19.1.4. Schlüsselwortfilterung

Mit der Schlüsselwortfilterung können Sie den Zugriff auf Email-Nachrichten,Webseiten und InstantMessaging-Nachrichten, die bestimmte Wörter enthalten, blockieren.Mit der Schlüsselwortfilterung können Sie verhindern, dass Ihre Kinder unangemessene Wörter oder Sätze sehen, wenn sie online sind.

Beachten Sie
Die Schlüsselwortfilterung für Instant Messaging ist nur für Yahoo Messenger undWindows Live (MSN) Messenger verfügbar.

Konfiguration der Schlüsselwortkontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der BitDefender-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Schlüsselwörter**.
3. Aktivieren Sie die Schlüsselwortfilterung.
4. Erstellen Sie eine Schlüsselwortkontrollregel, um unangemessene Schlüsselwörterzu blockieren.
5. Um zu vermeiden, dass Ihre Kinder persönliche Daten (wie beispielsweise Ihre Adresse oder Telefonnummer) an Personen, die sie über das Internet kennen lernen, weitergeben, müssen Sie Identitätskontrollregeln definieren.Weitere Informationen finden Sie unter „Erstellung von Regeln für die Identitätskontrolle“ (S. 111).

Erstellen von Regeln für die Schlüsselwortfilterung

Um ein Wort oder einen Satz zu blockieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf **Schlüsselwort blockieren**.
2. Geben Sie das Wort oder den Satz in das Eingabefeld ein. Wenn nur ganze Wörter erkannt werden sollen, aktivieren Sie die Option **Nur ganze Wörter suchen**.
3. Wählen Sie den Datenverkehrstyp, den BitDefender nach den definierten Wortenscannen soll.

Optionen	Beschreibung
HTTP	Internet Seiten, die Schlüsselwörter enthalten, werden blockiert.
POP3	Email-Nachrichten, die das Schlüsselwort enthalten, werden blockiert.
Instant Messaging	Sofortnachrichten, die das Schlüsselwort enthalten, werden blockiert.

4. Klicken Sie auf **Beenden**, um die Regel hinzuzufügen.

Verwaltung der Regeln für die Schlüsselwortfilterung

Die konfigurierten Schlüsselwortfilterregeln werden in der Tabelle aufgelistet. Dort finden Sie detaillierte Informationen zu jeder Regel.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

Erstellung von Regeln für die Identitätskontrolle

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf den Button **Schlüsselwort blockieren** und folgen Sie den Schritten des Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Begrüßungsfenster**
2. **Regeltyp und Daten festlegen**

   Hier können Sie die Parameter definieren:

   - **Regelname** - legen Sie einen Namen für die Regel fest.
   - **Regeltyp** - wählen Sie den Regeltyp aus (Adresse, Name, Kreditkartennummer, PIN, usw).
   - **Regeldaten** - geben Sie die Daten, die geschützt werden sollen, in dieses Feld ein.Wenn Sie beispielsweise Ihre Kreditkartennummer schützen wollen, geben Sie sie diese in Teilbereichen oder ganz ein.

Wichtig

Wenn Sie weniger als drei Zeichen angeben, werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen, um ein versehentliches Blockieren von Nachrichten oder Webseiten zu verhindern.

Alle eingegebenen Daten werden verschlüsselt. Um wirklich sicherzugehen, geben Sie nicht die kompletten Daten ein, die Sie schützen möchten.

3. **Scan-Optionen wählen**

   Bitte wählen Sie den Datenverkehrstyp, den BitDefender scannen soll.

   - **Das Internet scannen (HTTP-Datenverkehr)** - scannt den HTTP-Datenverkehr und blockiert die ausgehende Daten, die den Regeln entsprechen.
   - **Emails scannen (SMTP-Datenverkehr)** - scannt alle ausgehenden Emails undblockiert die ausgehenden Daten, die den Regeln entsprechen.
   - **Instant Messaging Datenverkehr scannen** - scannt den Instant Messaging-Datenverkehr und blockiert ausgehende Nachrichten, die den Regeln entsprechen.

   Sie können wählen, ob die Regeln nur angewandt werden sollen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmenmuss.

4. **Beschreibung der Regel**

   Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.Da die blockierten Daten (Zeichenfolgen) nicht als vollständiger Text angezeigt werden, wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen, sie einfach zu identifizieren.

   Klicken Sie auf **Fertigstellen**.Die Regel wird in der Tabelle eingeblendet.

Ab jetzt wird jeder Versuch, spezifizierte Daten (über Email, Instant Messaging odereine Webseite) zu senden, fehlschlagen. Es wird ein Warnhinweis eingeblendet, dass BitDefender nicht zugelassen hat, dass identitätsspezifische Inhalte versendet wurden.

19.1.5. Instant Messaging-Kontrolle (IM-Kontrolle)

Die Instant Messaging-Kontrolle bietet Ihnen die Möglichkeit, die IM-Kontaktefestzulegen, mit denen Ihre Kinder kommunizieren darf.

Beachten Sie

Die IM-Kontrolle ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Konfiguration der IM-Kontrolle für ein bestimmtes Benutzerkonto:

1. Öffnen Sie das Einstellungen-Fenster der BitDefender-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Messaging**.
3. Aktivieren Sie die Option Instant Messaging-Kontrolle.

4. Wählen Sie die bevorzugte Filtermethode und erstellen Sie die entsprechenden Regeln nach Ihren Wünschen.

   - **IM mit allen Kontakten zulassen, außer denen, die sich auf der Liste befinden.**

     In diesem Fall müssen Sie die IM-IDs angeben, die blockiert werden sollen (Menschen, mit denen Ihr Kind nicht kommunizieren sollte).

   - **IM mit alle Kontakten blockieren, außer denen, die sich auf der Liste befinden**

     In diesem Fall müssen Sie die IM-IDs, mit denen Ihr Kind über Instant Messagingkommunizieren darf, ausdrücklich festlegen.Sie können beispielsweise Instant Messaging mit Familienmitgliedern, Schulfreunden oder Nachbarn erlauben.

     Diese zweite Option wird empfohlen, wenn Ihr Kind unter 14 Jahren alt ist.

Erstellen von Instant Messaging-Kontrollregeln

Um IM-Konversationen mit einem Kontakt zu erlauben oder zu blockieren, folgen Sie diesen Schritten:

1. Klicken Sie auf **IM-ID blockieren** oder **IM-ID zulassen**.
2. Geben Sie die Email-Adresse oder den Benutzernamen, der von dem IM-Kontaktgenutzt wird, in das Feld **Email oder IM-ID** ein.
3. Wählen Sie das Chatprogramm, das der Kontakt verwendet.
4. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Sperren**.
5. Klicken Sie auf **Beenden**, um die Regel hinzuzufügen.

Verwaltung von Instant Messaging-Kontrollregeln

Die konfigurierten IM-Kontrollregeln werden in der Tabelle unten im Bildschirmfensteraufgelistet.

Um eine Regel zu löschen, markieren Sie diese und klicken auf **Entfernen**.

Um eine Regel zu bearbeiten, markieren Sie diese und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel.Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

19.2. Überwachung der Kinderaktivitäten

BitDefender hilft Ihnen dabei festzustellen, was Ihre Kinder am Computer tun, auch wenn Sie nicht zu Hause sind.

Als Voreinstellung werden bei aktivierter Kindersicherung die Aktivitäten Ihrer Kinder aufgezeichnet. So wissen Sie jederzeit, welche Webseiten Ihre Kinder besucht,

welche Anwendungen sie verwendet haben und welche Aktivitäten von der Kindersicherung blockiert wurden etc.

Sie können BitDefender auch so konfigurieren, dass Sie eine Email-Benachrichtigungerhalten, wenn die Kindersicherung eine Aktivität blockiert.

19.2.1. Überprüfen der Kindersicherungsprotokolle

Eine Aufzeichnung darüber, was Ihre Kinder kürzlich auf dem Computer gemacht haben, finden Sie im Kindersicherungsprotokoll.Gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender.
2. Klicken Sie unten rechts im Fenster auf den Link **Protokolle ansehen**.
3. Klicken Sie im linken Menü auf **Kindersicherung**.

Beachten Sie

Diese Protokolle können Sie auch aus dem Fenster der Kindersicherung heraus öffnen, indem Sie auf **Protokolle ansehen** klicken.

Wenn Ihre Kinder und Sie nicht denselben Computer benutzen, können Sie das BitDefender-Heimnetzwerk so konfigurieren, dass Sie per Fernabfrage auf die Kindersicherungsprotokolle zugreifen können (von Ihrem Computer aus).Weitere Informationen finden Sie unter *„Heimnetzwerk“* (S. 156).

Das Kindersicherungsprotokoll bietet detaillierte Informationen über die Aktivitäten Ihrer Kinder auf dem Computer und im Internet.Die Information befinden sich in mehreren Reitern:

Allgemein

Bietet allgemeine Informationen über die kürzlichen Aktivitäten Ihrer Kinder, wie beispielsweise die am häufigsten aufgerufenen Webseiten und die am häufigsten verwendeten Anwendungen.

Sie können Informationen nach Benutzer und Zeitspanne filtern.

Anwendungsprotokoll

Hilft Ihnen herauszufinden, welche Anwendungen Ihre Kinder kürzlich aufgerufenhaben.

Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

Internet-Protokoll

Hilft Ihnen herauszufinden, welche Webseiten Ihre Kinder kürzlich aufgerufen haben.

Sie können Informationen nach Benutzer und Zeitspanne filtern.

Andere Ereignisse

Hier erhalten Sie detaillierte Informationen über die Kindersicherungsaktivitäten (wie beispielsweise die Kindersicherung aktiviert/deaktiviert wird, welche Ereignisse gesperrt wurden).

Doppelklicken Sie auf die Ereignisse in der Liste, um weitere Details zu erhalten.Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf ihn und wählen **Löschen**.

19.2.2. Konfiguration der Email-Benachrichtigungen

Um Email-Benachrichtigungen zu erhalten, wenn die Kindersicherung eine Aktivitätsperrt:

1. Öffnen Sie BitDefender.
2. Abhängig von der gewählten Ansicht greifen Sie auf die Kindersicherung wie folgt zu:

   Standard-Ansicht
   Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Kindersicherung**.

   Experten-Ansicht
   Klicken Sie im linken Menü auf **Kindersicherung**.

   Beachten Sie

   In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

3. Wählen Sie in den Einstellungen die Option **Aktivitätsbericht per Email senden**.
4. Sie werden aufgefordert, die Email-Kontoeinstellungen zu konfigurieren. Klicken Sie **Ja**, um das Konfigurationsfenster zu öffnen.

   Beachten Sie

   Sie können das Konfigurationsfenster auch zu einem späteren Zeitpunkt öffnen, indem Sie auf **Benachrichtigungseinstellungen** klicken.

5. Geben Sie die Email-Adresse, an die Benachrichtigungen gesendet werden sollen, ein.
6. Konfigurieren Sie die Email-Einstellungen des Servers, der für die Email-Benachrichtigungen genutzt wird.

Für die Konfiguration der Email-Einstellungen stehen drei Optionen zur Verfügung:

Aktuelle Client-Einstellungen verwenden

Diese Option ist voreingestellt, wenn BitDefender die Mail Server-Einstellungen von Ihrem Mail Client importieren kann.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

Aus einem der bekannten Server auswählen

Wählen Sie diese Option, wenn Sie einen Email-Account bei einem der in der Liste genannten web-basierten Dienste haben.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

Ich möchte die Server-Einstellungen selbst konfigurieren.

Wenn Sie die Mail Server-Einstellungen kennen, wählen Sie diese Option und konfigurieren Sie die Einstellungen wie folgt:

- **Ausgehender SMTP-Server** - geben Sie die Adresse des Mail Servers, derfür das Verschicken der Emails zuständig ist, ein.
- Falls der Server einen anderen als den Standardport 25 nutzt, geben Sie diesen bitte im entsprechenden Feld an.
- Falls der Server eine Authentifizierung verlangt, wählen Sie **Mein SMTP Serverbenötigt Authentifizierung** und geben den Benutzernamen und das Passwort in die dazugehörigen Felder ein.

Klicken Sie zur Bestätigung der Eingaben auf **Einstellungen testen**. Tretenwährend der Bestätigung Probleme auf, werden Sie darüber informiert, was Sietun müssen, um diese zu beheben.

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

19.3. Remote Kindersicherung

Über die Remote Kindersicherung können Sie die Aktivitäten Ihrer Kinder überwachen und die Einstellungen der Kindersicherung ändern, auch wenn Sie nicht zu Hause sind.Sie benötigen nur einen Computer mit Internetzugang und einen Webbrowser.

Die Remote Kindersicherung bietet eine diskrete Möglichkeit zu überprüfen, was Ihre Kinder online machen, ohne dabei aufdringlich zu sein.

19.3.1. Voraussetzungen für die Nutzung der Remote Kindersicherung

Um die Remote Kindersicherung nutzen zu können, müssen Sie folgende Vorbedingungen erfüllen:

1. Installieren Sie entweder BitDefender Internet Security 2011 oder BitDefender Total Security 2011 auf dem Computer Ihrer Kinder.
2. Aktivieren Sie das Produkt mithilfe eines BitDefender-Benutzerkontos.
3. Aktivieren Sie die Remote Kindersicherung.
4. Der Computer, von dem aus Sie auf die Fernsteuerung der Kindersicherung zugreifen möchten, muss mit dem Internet verbunden sein.

19.3.2. Aktivierung der Remote Kindersicherung

Aktivierung der Remote Kindersicherung:

1. Loggen Sie sich in ein Administrator-Benutzerkonto auf dem Computer ein, auf dem BitDefender installiert ist.Sie können dasselbe Benutzerkonto verwenden, das auch für die Installation benutzt wurde.
2. Öffnen Sie BitDefender.
3. Abhängig von der gewählten Ansicht greifen Sie auf die Kindersicherung wie folgt zu:

   Standard-Ansicht
   Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Kindersicherung**.

   Experten-Ansicht
   Klicken Sie im linken Menü auf **Kindersicherung**.

   Beachten Sie

   In der Basis- und Standard-Ansicht können Sie Verknüpfungen konfigurieren, so dass Sie auf diese Einstellungen vom Dashboard aus zugreifen können.Weitere Informationen finden Sie unter *„Meine Werkzeuge“* (S. 33).

4. Über diesen Regler können Sie die Remote Kindersicherung aktivieren.Die Remote Kindersicherung wird für alle Benutzerkonten auf diesem System aktiviert.

19.3.3. Zugriff auf die Remote Kindersicherung

Sie können von Ihrem BitDefender-Benutzerkonto aus auf die Remote Kindersicherung zugreifen.

1. Öffnen Sie auf einem Computer mit Internetzugang einen Webbrowser und gehenSie auf:

   http://myaccount.bitdefender.com

2. Loggen Sie sich mit Ihrem Benutzernamen und Passwort in Ihr BitDefender-Benutzerkonto ein.

3. Klicken Sie auf den Reiter **Kindersicherung**, um auf das Dashboard der Remote Kindersicherung zuzugreifen.
4. Sie können alle Benutzerkonten sehen, für die die Remote Kindersicherung aktiviert ist.

   Um zu überprüfen, welche Aktivitäten seit dem letzten Login für ein bestimmtes Benutzerkonto blockiert wurden, klicken Sie auf den Link, der die existierenden Warnungen anzeigt.

   Um die letzten Aktivitäten Ihrer Kinder zu überprüfen, klicken Sie im entsprechenden Benutzerkonto auf den Link **Kürzliche Aktivität**.

   Um die Einstellungen der Kindersicherung für ein bestimmtes Benutzerkonto zu ändern, klicken Sie auf den entsprechenden **Einstellungen**-Link.

19.3.4. Überwachung der Aktivitäten Ihrer Kinder (Remote)

Bevor Sie die Computer-Aktivitäten Ihrer Kinder per Fernabfrage überwachen können, müssen Sie auf deren Computern die Remote Kindersicherung aktivieren.Weitere Informationen finden Sie unter *„Aktivierung der Remote Kindersicherung“* (S. 117).

Um per Fernsteuerung zu überwachen, was Ihre Kinder auf deren Computern machen:

1. Öffnen Sie auf einem Computer mit Internetzugang einen Webbrowser und gehenSie auf:

   http://myaccount.bitdefender.com
2. Loggen Sie sich mit Ihrem Benutzernamen und Passwort in Ihr BitDefender-Benutzerkonto ein.
3. Klicken Sie auf den Reiter **Kindersicherung**, um auf das Dashboard der Remote Kindersicherung zuzugreifen.
4. Um zu überprüfen, welche Aktivitäten seit dem letzten Login für ein bestimmtes Benutzerkonto blockiert wurden, klicken Sie auf den Link, der die existierenden Warnungen anzeigt. Um die letzten Aktivitäten Ihrer Kinder zu überprüfen, klicken Sie im entsprechenden Benutzerkonto auf den Link **Kürzliche Aktivität**.

Auf der Warnseite sehen Sie, welche Webseiten, Anwendungen oder Instant Messaging-Kontakte seit dem letzten Einloggen blockiert wurden.

Auf der Seite "Kürzliche Aktivitäten" finden Sie nützliche Informationen über die letzten Aktivitäten Ihrer Kinder auf dem Computer:

- welches die am häufigsten besuchten und blockierten Webseiten sind.
- welches die am häufigsten besuchten und blockierten Anwendungen sind.
- welches die am häufigsten aufgerufenen und am häufigsten blockierten Instant Messaging IDs sind.

Sie können eine Webseite, Anwendung oder Instant Messaging ID direkt blockieren, indem Sie auf den entsprechenden Link **Blockieren** klicken.

Um eine Beschränkung zu löschen, klicken Sie auf den entsprechenden **Zulassen**-Link.

19.3.5. Remote-Änderung der Remote Kindersicherungseinstellungen

Bevor Sie per Fernsteuerung die Einstellungen der Kindersicherung ändern können, müssen Sie erst die Option "Remote Kindersicherung" auf den Computern Ihrer Kinder aktivieren.Weitere Informationen finden Sie unter *„Aktivierung der Remote Kindersicherung“ (S. 117)*.

Änderung der Kindersicherungseinstellung per Fernsteuerung (Remote):

1. Öffnen Sie auf einem Computer mit Internetzugang einen Webbrowser und gehenSie auf:

   http://myaccount.bitdefender.com

2. Loggen Sie sich mit Ihrem Benutzernamen und Passwort in Ihr BitDefender-Benutzerkonto ein.
3. Klicken Sie auf den Reiter **Kindersicherung**, um auf das Dashboard der Remote Kindersicherung zuzugreifen.
4. Sie können alle Benutzerkonten sehen, für die die Remote Kindersicherung aktiviert ist.Um die Einstellungen der Kindersicherung für ein bestimmtes Benutzerkonto zu ändern, klicken Sie auf den entsprechenden **Einstellungen**-Link.

Auf der Einstellungenseite werden die Webseiten, Anwendungen und Instant Messaging IDs angezeigt, die durch die Kindersicherung explizit gesperrt sind.Um eine Beschränkung zu löschen, klicken Sie auf den entsprechenden **Zulassen**-Link.

Informationen, wie Sie Beschränkungen festlegen, finden Sie unter:

„Zeitliche Beschränkung des Internetzugangs“ (S. 119)
„Webseiten blockieren“ (S. 120)
„Anwendungen blockieren“ (S. 120)
„IM-Kontakte blockieren“ (S. 120)

Zeitliche Beschränkung des Internetzugangs

Wählen Sie aus dem Menü eine Option, um festzulegen, wann Ihr Kind im Internet surfen darf.Um Beschränkung des Internetzugangs auf bestimmte Tageszeiten festzulegen:

1. Wählen Sie **Internetzugang terminieren**.
2. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll.Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und

mit der Maus einen längeren Zeitraum definieren.Um eine neue Auswahl zu starten, klicken Sie auf **Alle blockieren** oder **Alle zulassen**.

3. Klicken Sie auf **Änderungen übermitteln**.Nach der nächsten Synchronisation mit der Webseite für die Remote Kindersicherung (innerhalb von max. 10 Minuten) werden die Änderungen konfiguriert und auf dem Computer Ihres Kindes angewandt.

Webseiten blockieren

Blockierung einer Webseite:

1. Klicken Sie auf **Eine weitere Webseite blockieren**.
2. Geben Sie im entsprechenden Feld die Webseite ein. Alternativ können Sie die am häufigsten besuchten Webseiten, die Sie blockieren möchten, aus im Menü auswählen.
3. Klicken Sie auf **Blockieren**.Die Webseite wird der Liste der gesperrten Webseiten hinzugefügt.Nach der nächsten Synchronisation mit der Webseite für die Remote Kindersicherung (innerhalb von max. 10 Minuten) werden die Änderungen konfiguriert und auf dem Computer Ihres Kindes angewandt.

Wenn Sie Ihre Meinung ändern, klicken Sie auf den entsprechenden **Zulassen**-Link.

Anwendungen blockieren

Um eine Anwendung zu blockieren:

1. Klicken Sie auf **Eine weitere Anwendung blockieren**.
2. Wählen Sie die Anwendung, die blockiert werden soll, aus der Liste der am häufigsten genutzten Anwendungen aus.
3. Klicken Sie auf **Blockieren**.Die Anwendung wird der Liste der gesperrten Anwendungen hinzugefügt.Nach der nächsten Synchronisation mit der Webseite für die Remote Kindersicherung (innerhalb von max. 10 Minuten) werden die Änderungen konfiguriert und auf dem Computer Ihres Kindes angewandt.

Wenn Sie Ihre Meinung ändern, klicken Sie auf den entsprechenden **Zulassen**-Link.

IM-Kontakte blockieren

Instant Messaging mit einem bestimmten Kontakt blockieren:

1. Klicken Sie auf **Einen weiteren Kontakt blockieren**.
2. Geben Sie im entsprechenden Feld die Instant Messaging ID ein. Wenn Sie alternativ eine der am häufigsten kontaktierten Instant Messaging IDs sperren möchten, wählen Sie diese aus dem Menü.
3. Klicken Sie auf **Blockieren**.Die Instant Messaging ID wird der Liste der blockierten Instant Messaging IDs hinzugefügt.Nach der nächsten Synchronisation mit der

Webseite für die Remote Kindersicherung (innerhalb von max. 10 Minuten) werden die Änderungen konfiguriert und auf dem Computer Ihres Kindes angewandt.

Wenn Sie Ihre Meinung ändern, klicken Sie auf den entsprechenden **Zulassen**-Link.

20. Einstellungen zur Privatsphäre

BitDefender überwacht dutzende von möglichen Angriffspunkten (sog. "HotSpots") in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft zudem jede Veränderung des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden in Echtzeit blockiert. Die AntiSpyware ist effektiv in der Bekämpfung von Trojanischen Pferden anderen von Hackern installierten Tools, die versuchen Ihre Privatshpäre kompromittieren und Ihr persönlichen Daten wie z.B. Kreditkarennummern, von Ihrem Computer zum Hacker zu senden.

Die Privatsphäre-Funktion beinhaltet folgende Komponenten.

- Identitätskontrolle - stellt sicher, dass persönliche Informationen nicht ohne Ihre Zustimmung von Ihrem PC aus gesendet werden. Die Emails und Instant Messages Ihres PCs werden ebenso gescannt wie Daten, die über Internetseiten gesendet werden. Zudem werden alle Informationen geblockt, die über die von Ihnen definierten Regeln der Identitätskontrolle geschützt sind.
- Registry-Kontrolle - fragt immer um Erlaubnis, wenn ein Programm versucht die Registry zu ändern, um beim Windows Neustart ausgeführt zu werden.
- Cookie-Kontrolle - fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle - fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu aktivieren.

In der Voreinstellung ist nur die Funktion "Identitätskontrolle" aktiviert.Sie müssen passende Identitätskontrollregeln konfigurieren, um das nicht autorisierte Senden von der vertraulichen Information zu verhindern.Weitere Informationen finden Sie unter *„Konfiguration der Identitätskontrolle“* (S. 125).

Die weiteren Komponenten der Privatsphärekontrolle sind nicht aktiv. Falls Siediese aktivieren, werden Sie im Warnhinweisfenster gefragt, ob bestimmte Aktionenzugelassen oder geblockt werden sollen, wenn Sie auf neuen Internetseiten surfenoder eine neue Software installieren. Dies ist der Grund, wieso diese Einstellung im Normalfall von fortgeschrittenen Anwendern verwendet wird.

20.1. Konfiguration der TresorSicherheitsstufe

Die TresorSicherheitsstufe hilft Ihnen, die Komponenten der Privatsphäre-Funktion einfach zu aktivieren/deaktivieren.

Um die TresorSicherheitsstufe zu konfigurieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Status**.

3. Stellen Sie sicher, dass die Privatsphärefunktion aktiviert ist.
4. Es stehen zwei Optionen zur Verfügung:
   - Schieben Sie den Regler in die gewünschte TresorSicherheitsstufen-Position.Klicken Sie auf **Voreingestellt** um den Regler auf den voreingestellten Level zu positionieren.

     Nutzen Sie die Beschreibung auf der rechten Seite, um die TresorSicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.
   - Sie können die Sicherheitsstufe Tresorindividuell einstellen, indem Sie auf **Stufe anpassen** klicken.Wählen Sie im erscheinenden Fenster die Sicherheitseinstellungen die Sie aktivieren möchten und klicken Sie auf **OK**.

20.2. Identitätskontrolle

Die Identitätskontrolle schützt Sie gegen den Diebstahl sensibler Daten wenn Sie online sind.

Betrachten wir ein einfaches Beispiel: Sie haben eine Identitätskontrollregel zum Tresor Ihrer Kreditkartennummer definiert.Wenn es eine Spyware-Software auf irgendeine Weise geschafft hat, sich auf Ihrem Computer zu installieren, können dennoch keine Daten wie Ihre Kreditkartennummer via Email, Instant Messaging oder Webseiten gesendet werden. Zudem können auch Ihre Kinder die Kreditkartendaten nicht für Online-Käufe verwenden oder sie über das Internet preisgeben.

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Über die Identitätskontrolle“* (S. 123).
- *„Konfiguration der Identitätskontrolle“* (S. 125).
- *„Regeln verwalten“* (S. 127).

20.2.1. Über die Identitätskontrolle

Vertrauliche Daten zu sichern ist ein Thema, welches uns alle beunruhigt. Datendiebstahl hat mit der Entwicklung der Internetkommunikation standgehalten und wendet immerwieder neue Methoden an, um Anwender zu täuschen und private Informationen zuerhalten.

Ob es sich um Ihre Email-Adresse handelt oder um Ihre Kreditkartennummer, wennsie in die falschen Hände geraten, können diese Informationen großen Schadenanrichten: Sie ersticken möglicherweise in Spam-Mails oder wundern sich über eingeleertes Konto.

Die Identitätskontrolle schützt Sie gegen den Diebstahl sensibler Daten wenn Sie online sind.Basierend auf Regeln, die von Ihnen erstellt wurden, scannt die

Identitätskontrolle den Web-, Mail und IM-Datenverkehr auf spezielle Zeichenfolgen (zum Beispiel Ihre Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, Email-Adresse oder IM-Nachricht gefunden wird, wird diese sofort geblockt.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie alspersönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder Email-Adressebis hin zu Ihren Bankdaten.Es wird eine Multiuser-Unterstützung zur Verfügung gestellt, wodurch Benutzer die sich in verschiedene Windows-Benutzerkonten einloggen, Ihre eigenen Regeln zur Identitätskontrolle konfigurieren können.Falls Ihr Windows-Benutzerkonto ein Administratorkonto ist, können die von Ihnen definierten Regeln auch angewandt werden, wenn andere Benutzer mit deren Konten in Windows eingeloggt sind.

Warum sollten Sie die Identitätskontrolle verwenden?

- Die Identitätskontrolle kann Keylogger-Spyware sehr effektiv blockieren.Diese schädlichen Anwendungen speichern Ihre eingegebenen Tastenfolgen und senden sie über das Internet an Hacker.Der Hacker kann so gestohlenen Daten und sensible Informationen wie Kontonummern und Passwörter erfahren und Sie zu seinem eigenen Vorteil verwenden.

  Auch wenn es eine solche Anwendung schaffen sollte, der Antivirus-Entdeckung zu umgehen, kann es die gestohlenen Daten nicht über Email, das Internet oderChatprogramme senden, wenn Sie entsprechende Regeln für die Identitätskontrolleeingestellt haben.

- Die Identitätskontrolle kann Sie vor Phishing schützen (Versuche, persönliche Daten zu stehlen).Die meisten Phishing-Versuche verwenden eine betrügerische Email, um Sie dazu zu bringen persönliche Daten an eine gefälschte Webseite zu senden.

  So können Sie beispielsweise eine Email erhalten, die behauptet von Ihrer Bank zu kommen und Sie dazu auffordert, Ihre Bankangaben dringend zu aktualisieren.In der Email befindet sich ein Link zu einer Webseite, auf der Sie Ihre persönlichen Daten angeben sollen.Auch wenn dies alles echt erscheint, sind sowohl die Email als auch die genannte Webseite Fälschungen.Wenn Sie auf den Link in der Mail klicken und Ihre persönlichen Daten an die Webseite senden, werden Sie diese Informationen an die Hacker weiterleiten, die diesen Phishing-Versuch erstellt haben.

  Wenn entsprechende Regeln für die Identitätskontrolle eingestellt sind, können Sie die persönlichen Daten (so wie Ihre Kreditkartennummer) nicht an eine Webseite senden, außer wenn Sie die entsprechende Seite explizit als Ausnahme festgelegt haben.

- Durch die Verwendung von Identitätskontrollregeln können Sie verhindern, dass Ihre Kinder persönliche Daten (wie z. B. Ihre Adresse oder Telefonnummer) über das Internet weitergeben. Zudem können Sie auch eine Regel zum Tresor Ihrer

Kreditkartendaten definieren, so dass Ihre Kinder mit dieser Karte ohne Ihre Zustimmung nichts kaufen können.

20.2.2. Konfiguration der Identitätskontrolle

Wenn Sie die Identitätskontrolle nutzen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Identität**.
3. Stellen Sie sicher, dass die Identitätskontrolle aktiviert ist.

   Beachten Sie
   Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Erstellen Sie Regeln um wichtige Daten zu schützen.Weitere Informationen finden Sie unter *„Erstellung von Regeln für die Identitätskontrolle“ (S. 125)*.
5. Definieren Sie, wenn nötig, spezielle Ausnahmen für die erstellten Regeln.Wenn Sie beispielsweise eine Regel zum Tresor Ihrer Kreditkarte definiert haben, dann setzen Sie die Webseiten, auf denen Sie normalerweise Ihre Kreditkarte einsetzen, auf die Ausschlussliste.Weitere Informationen finden Sie unter *„Definition von Ausnahmen“ (S. 127)*.

Erstellung von Regeln für die Identitätskontrolle

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf den Button **Hinzufügen** und befolgen Sie die Schritte des Konfigurationsassistenten.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Begrüßungsfenster**
2. **Regeltyp und Daten festlegen**

   Hier können Sie die Parameter definieren:

   - **Regelname** - legen Sie einen Namen für die Regel fest.
   - **Regeltyp** - wählen Sie den Regeltyp aus (Adresse, Name, Kreditkartennummer, PIN, usw).
   - **Regeldaten** - geben Sie die Daten, die geschützt werden sollen, in dieses Feld ein.Wenn Sie beispielsweise Ihre Kreditkartennummer schützen wollen, geben Sie sie diese in Teilbereichen oder ganz ein.

Wichtig

Wenn Sie weniger als drei Zeichen angeben, werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen, um ein versehentliches Blockieren von Nachrichten oder Webseiten zu verhindern.

Alle eingegebenen Daten werden verschlüsselt. Um wirklich sicherzugehen, geben Sie nicht die kompletten Daten ein, die Sie schützen möchten.

3. **Datenverkehrstyp und Benutzer auswählen**

   a. Bitte wählen Sie den Datenverkehrstyp, den BitDefender scannen soll.

   - **Das Internet scannen (HTTP-Datenverkehr)** - scannt den HTTP-Datenverkehr und blockiert die ausgehende Daten, die den Regeln entsprechen.
   - **Emails scannen (SMTP-Datenverkehr)** - scannt alle ausgehenden Emails undblockiert die ausgehenden Daten, die den Regeln entsprechen.
   - **Instant Messaging Datenverkehr scannen** - scannt den Instant Messaging-Datenverkehr und blockiert ausgehende Nachrichten, die den Regeln entsprechen.

   Sie können wählen, ob die Regeln nur angewandt werden sollen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmenmuss.

   b. Geben Sie den Benutzer an, für den die Regel angewendet werden soll.

   - **Nur für mich (Aktueller Benutzer)** - die Regel wird nur für Ihr Benutzerkonto angewandt.
   - **Beschränkte Benutzerkonten** - die Regel wird auf Ihr und alle anderen beschränkten Windows-Benutzerkonten angewandt.
   - **Alle Benutzer** - die Regel wird für alle Windows-Benutzerkonten angewandt.

4. **Beschreibung der Regel**

   Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.Da die blockierten Daten (Zeichenfolgen) nicht als vollständiger Text angezeigt werden, wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen, sie einfach zu identifizieren.

   Klicken Sie auf **Fertigstellen**.Die Regel wird in der Tabelle eingeblendet.

Ab jetzt wird jeder Versuch, spezifizierte Daten (über Email, Instant Messaging odereine Webseite) zu senden, fehlschlagen. Es wird ein Warnhinweis eingeblendet, dass BitDefender nicht zugelassen hat, dass identitätsspezifische Inhalte versendet wurden.

Definition von Ausnahmen

In manchen Fällen wird es nötig sein, Ausnahmen für bestimmte Identitätsregeln zu erstellen.Zum Beispiel haben Sie eine Regeln angelegt, welche verhindert das Ihre Kreditkartennummer per HTTP übertragen wird. Nun möchten Sie sich aber z.B. Schuhe auf einer bestimmten Webseite per Kreditkarte kaufen. In diesem Fall müssten Sie eine Ausnahme definieren, um dies möglich zu machen.

Um eine solche Ausnahme zu erstellen, klicken Sie auf die **Ausnahmen**-Schaltfläche.

Um eine Ausnahme zu erstellen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Button **Hinzufügen**, um der Tabelle einen neuen Eintrag hinzuzufügen.
2. Doppelklicken Sie auf **Ausgeschlossenen Eintrag definieren** und geben Sie die gewünschte URL, Email-Adresse oder IM-Kontakt ein, um diese auszuschließen.
3. Doppelklicken Sie dann auf **Datenverkehrstyp** und wählen Sie den gewünschten Eintrag aus dem Menü aus.
   - Wenn Sie eine Webseite eingegeben haben, wählen Sie **HTTP**.
   - Wenn Sie eine Email-Adresse eingegeben haben dann wählen Sie **Email (SMTP)**.
   - Wenn Sie einen IM-Kontakt eingegeben haben, wählen Sie **IM**.

Um eine Ausnahme aus der Liste zu entfernen, wählen Sie diese aus und klicken auf den **Entfernen**-Button.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

20.2.3. Regeln verwalten

Verwaltung der Identitätskontrollregeln:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Identität**.

Die bisher erstellten Regeln werden in einer Tabelle aufgelistet.

Um eine Regel zu löschen, wählen Sie diese aus und klicken auf den **Löschen**-Button.

Um eine Regel zu bearbeiten, wählen Sie die Regel aus und klicken auf den Button **Bearbeiten** oder doppelklicken auf die Regel. Ein neues Fenster wird eingeblendet.Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern (Typ, Daten und Datenverkehr). Klicken Sie **OK**, um die Änderungen zu speichern.

20.3. Registry Control

Ein sehr wichtiger Teil von Windows ist die **Registry**. Dort werden von Windows alle Einstellungen, installierten Programme, Nutzerinformationen und so weiter verwaltet.

Die **Registry** bestimmt u. a., welche Programme automatisch beim Start von Windows geladen werden. Viren versuchen häufig hier anzusetzen, damit auch sie automatisch mit geladen werden, wenn der Nutzer seinen Computer startet.

Registry Control überwacht die Windows-Registry – dies ist auch sehr hilfreich beim Aufspüren von Trojanern. Sie werden alarmiert, wann immer ein Programm versucht, einen Eintrag in die Registry zu unternehmen, um beim nächsten Windows-Start geladen zu werden.Weitere Informationen finden Sie unter *„Registry-Alarme.“* (S. 40).

Für die Konfigurierung der Registry Control:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Registry**.
3. Klicken Sie das entsprechende Kästchen an, um die Registry Control zu aktivieren.

Beachten Sie
Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

Regeln verwalten

Um eine Regel zu löschen, wählen Sie diese aus und klicken auf den **Löschen**-Button.

20.4. Cookie-Kontrolle

Cookies werden von den meisten Webseiten im Internet verwendet. Es sind kleine Dateien, die auf Ihrem Computer gespeichert werden. Webseiten verschicken diese Cookies, um das Surfen zu beschleunigen, aber auch um Informationen über Sie zu erhalten.

Generell erleichtern Cookies das tägliche Internetleben. Zum Beispiel ermöglichen sie einer Webseite, Ihren Namen und sonstige Angaben zu speichern, so dass Sie diese nicht bei jedem Besuch erneut eingeben müssen.

Cookies können jedoch auch missbräuchlich verwendet werden und Ihre Privatsphäre gefährden, indem Ihre Surfdaten an Dritte weitergegeben werden.

Hier hilft die Cookie-Kontrolle.Wenn Sie aktiviert ist, wird die Cookie-Kontrolle bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches

Einverständnis erfragen.Weitere Informationen finden Sie unter *„Cookie-Alarme“ (S. 41)*.

Um die Cookie-Steuerung zu konfigurieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Cookie**.
3. Markieren Sie das entsprechende Kästchen, um die Cookie Control zu aktivieren.

   Beachten Sie
   Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Sie können für die Webseiten, die Sie regelmäßig besuchen, Regeln konfigurieren, dies ist aber nicht unbedingt notwendig.Basierend auf Ihrer Antwort werden durch das Warnhinweisfenster automatisch Regeln erstellt.

Beachten Sie
Aufgrund der großen Anzahl von Cookies, die heute im Internet verwendet werden, kann die **Cookie-Kontrolle** zu Beginn sehr viele Fragen über Webseiten stellen, die versuchen Cookies auf Ihrem Rechner zu installieren. Sobald Sie die von Ihnen regelmäßig besuchten Seiten in die Regelliste aufgenommen haben, wird Ihr Surfen im Internet aber wieder wie zuvor sein.

Regeln manuell erstellen

Um eine Regel manuell zu erstellen, klicken Sie auf den Button **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.Hier können Sie die Parameter definieren:

- **Domain-Adresse** - tippen Sie die Domain, auf die Regel angewandt werden soll, ein.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Der Cookie dieser Domain wird ausgeführt.
Blockieren	Der Cookie dieser Domain wird nicht ausgeführt.

- **Richtung** - Wählen Sie die Richtung des Datenverkehrs aus.

Typ	Beschreibung
Ausgang	Die Regel bezieht sich nur auf Cookies, die zurück zur verbundenen Seite versendet werden.

Typ	Beschreibung
Eingang	Die Regel bezieht sich nur auf Cookies, die von der verbundene Seite empfangen werden.
Beide	Die Regeln findet in beide Richtungen Anwendung.

Beachten Sie

Sie können Cookies akzeptieren, diese aber niemals zurückschicken, indem Sie die Aktion **Verweigern** und die Richtung **Ausgehend** angeben.

Klicken Sie auf **Fertigstellen**.

Regeln verwalten

Um eine Regel zu löschen, wählen Sie diese aus und klicken auf den **Löschen**-Button.Zum Bearbeiten von Regelparametern wählen Sie die Regel aus und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel. Ein neues Fenster eingeblendet, in dem Sie die gewünschte Konfiguration durchführen können.

20.5. Skript-Kontrolle

Skripte und andere Codes wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

Wenn Sie die Funktion "Skript-Kontrolle" aktivieren, wird immer eine Anfrage an Sie gerichtet, wenn eine neue Webseite versucht, ein Skript oder einen anderen aktiven Inhalte zu verankern.Weitere Informationen finden Sie unter *„Skript-Alarme“* (S. 41).

Um die Skript-Kontrolle zu konfigurieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Privatsphäre > Skript**.
3. Klicken Sie das entsprechende Kästchen an, um die Skript-Kontrolle zu aktivieren.

Beachten Sie

Wenn die Option nicht konfiguriert werden kann, gehen Sie in den Reiter **Status** und aktivieren Sie die Funktion "Privatsphäre".

4. Sie können für die Webseiten, die Sie regelmäßig besuchen, Regeln konfigurieren, dies ist aber nicht unbedingt notwendig.Basierend auf Ihrer Antwort werden durch das Warnhinweisfenster automatisch Regeln erstellt.

Regeln manuell erstellen

Um eine Regel manuell zu erstellen, klicken Sie auf den Button **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.Hier können Sie die Parameter definieren:

- **Domain-Adresse** - tippen Sie die Domain, auf die Regel angewandt werden soll, ein.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Die Skripts dieser Domain werden ausgeführt.
Blockieren	Die Skipts dieser Domain werden nicht ausgeführt.

Klicken Sie auf **Fertigstellen**.

Regeln verwalten

Um eine Regel zu löschen, wählen Sie diese aus und klicken auf den **Löschen**-Button.Zum Bearbeiten von Regelparametern wählen Sie die Regel aus und klicken auf **Bearbeiten** oder doppelklicken Sie auf die entsprechende Regel. Ein neues Fenster eingeblendet, in dem Sie die gewünschte Konfiguration durchführen können.

21. Firewall

Die Firewall schützt Ihren Computer vor unberechtigten eigehenden und ausgehenden Verbindungsversuchen. Sie überwacht Ihre Verbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.

Beachten Sie

Die Firewall ist ein unersetzliches Instrument bei einer DSL- oder Breitbandverbindungen.

Im Stealth-Modus wird ihr Computer im Netzwerk so gut wie unsichtbar vor Angriffen jeglicher Art „versteckt“. Das Firewall-Modul ist in der Lage Portscans zu erkennen und diese gezielt ins Leere laufen zu lassen - so als ob der Computer gar nicht existierte.

21.1. Tresoreinstellungen

Um den Firewall-Tresor zu aktivieren/deaktivieren und zu konfigurieren, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Einstellungen**.

Experten-Ansicht

Gehen Sie zu **Firewall > Einstellungen**.

Wichtig

Um den Tresor vor Angriffen aus dem Internet zu gewährleisten, lassen Sie Ihre **Firewall** Funktion jederzeit aktiviert.

Zu Beginn des Bereichs sehen Sie verschiedene Statistiken zu den festgestellten Aktivitäten.

Im unteren Bereich finden Sie eine BitDefender-Statistik bezüglich des ein- und ausgehenden Datenverkehrs. Diese Grafik zeigt Ihnen das Volumen des Internet-Datentransfers der letzten zwei Minuten an.

Beachten Sie

Diese Graphik wird nur in der Experten-Ansicht dargestellt.

21.1.1. Einstellen der Standardaktionen

Standardmäßig erlaubt BitDefender automatisch allen Programmen der White List eine Verbindung zum Netzwerk und dem Internet herzustellen.Für alle anderen

Programme fordert BitDefender Sie über ein Benachrichtigungsfenster dazu auf, die durchzuführende Aktion festzulegen.Die von Ihnen festgelegte Aktion wird immer dann durchgeführt, wenn das entsprechende Programm versucht auf das Netzwerk/Internet zuzugreifen.

Ziehen Sie den Zeiger an der Skala entlang, um die Standardaktion festzulegen, die durchgeführt werden soll, wenn das Programm versucht auf das Netzwerk/Internet zuzugreifen.

- Alle zulassen
- Bekannte Programme zulassen
- Protokoll
- Alle verweigern

Wenn Sie eine Aktion auswählen, wird ein kurzer Erklärungstext eingeblendet.

21.1.2. Konfiguration der erweiterten Einstellungen der Firewall

In der Experten-Ansicht können Sie die erweiterten Firewall-Einstellungen durch Klicken auf **Erweiterte Einstellungen** konfigurieren.

Die folgenden Optionen sind verfügbar:

- **Unterstützung für Internet Connection Sharing aktivieren** - erlaubt die Unterstützung von Internet Connection Sharing (ICS).

  Beachten Sie

  Diese Option erlaubt nicht automatisch ICS auf Ihrem System sondern erlaubt diese Art von Verbindung nur, wenn Sie sie es von Ihrem Betriebssystem aus freigeben.

- **Findet Anwendungen die sich seit dem Erstellen der Firewall-Regel verändert haben** - scannt jede Anwendung die versucht eine Verbindung zum Internet herzustellen, um zu erkennen ob sich bei dieser seit dem Hinzufügen der Regel, die den Zugriff überwacht, etwas verändert hat. Falls sich etwas verändert hat, wird eine Warnung Sie auffordern den Zugriff zu erlauben oder zu blockieren.

  Beachten Sie

  Anwendungen können durch Malware verändert werden.Wir empfehlen Ihnen die Option aktiviert zu lassen und den Zugriff nur für die Anwendungen zuzulassen, von denen Sie denken, dass Sie geändert wurden, nachdem die Regel erstellt wurde.

  Signierte Anwendungen sind im Normalfall vertrauenswürdig und sind im Regelfall sicherer.Signierte Anwendungen haben einen höheren Sicherheitsfaktor. Sie können diesen Anwendungen den Zugriff erlauben, auch wenn diese verändert

wurden, indem Sie die Option **Änderungen von signiertenAnwendungen ignorieren** aktivieren.

- **WLAN-Benachrichtigungen anzeigen** - wenn Sie mit einem drahtlosen Netzwerk verbunden sind, werden Informationsfenster bezüglich bestimmter Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer dem Netzwerk beitritt).
- **Port-Scans blockieren** - entdeckt und blockiert Versuche offene Ports zu finden.

  Port-Scans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind.Wenn sie einen unsicheren Port finden, könnten sie in Ihren Computer eindringen.
- **Genaue automatische Regeln aktivieren** -erstellt genaue Regeln bezüglich der Verwendung des Benachrichtigungsfensters der Firewall.Wenn diese Option aktiviert ist, wird BitDefender Sie dazu auffordern für jede Anwendung, die versucht auf das Netzwerk oder das Internet zuzugreifen, eine Aktion durchzuführen und Regeln zu erstellen.

21.2. Zugriffsregel für Anwendungen

Um die Firewall-Regeln zu verwalten, die den Zugriff von Anwendungen auf Netzwerkressourcen und das Internet kontrollieren, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Programme**.

Experten-Ansicht
: Gehen Sie zu **Firewall > Programme**.

In der Standard-Ansicht haben Sie Zugriff auf die Basis-Konfigurationseinstellungen. Für zusätzliche benutzerdefinierte Optionen wechseln Sie in die Experten-Ansicht.

21.2.1. Aktuelle Regeln ansehen

Sie können die Programme (Prozesse), für die Firewall-Regel erstellt wurde, in der Tabelle sehen.

In der Experten-Ansicht erhalten Sie detaillierte Informationen zu jeder Regel, so wie in den Spalten der Tabelle dargestellt.Um die Regeln zu sehen, die für eine bestimmte Anwendung erstellt wurden, klicken Sie auf das Kästchen neben der entsprechenden Anwendung.Deaktivieren Sie das Kontrollkästchen **Systemregeln verbergen** frei, wenn Sie auch die Regeln bezüglich des Systems oder der BitDefender-Prozessen sehen möchten.

- **Prozess/Netzwerkarten** - der Prozess und die Netzwerkadapter-Typen für die die Regel angewendet wird.Regeln werden automatisch erstellt, um den Netzwerk-oder Internetzugriff über jeden Adapters zu filtern.Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten, um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).
- **Befehlszeile** - der Befehl in der Windows Befehlszeile der verwendet wird um den Prozess zu starten (**cmd**).
- **Protokoll** - die für das IP-Protokoll angewandte Regel. Folgende Varianten sind verfügbar:Sie werden eines der Folgenden sehen:

Protokoll	Beschreibung
Alle	Beinhaltet alle IP-Protokolle.
TCP	Transmission Control Protocol - TCP Ermöglicht es zwei Hosts, eine Verbindung zu etablieren und Datenströme auszutauschen. TCP garantiert die Lieferung der Daten und stellt sicher, dass Pakete inderselben Reihenfolge, in der sie gesendet wurden, geliefert werden.
UDP	User Datagram Protocol - UDP ist ein IP-basierter Transport, programmiert für Hochleistung. Spiele und andere Video-basierte Anwendungen nutzen oftmals die UDP-Technologie.
Eine Nummer	Steht für ein besonderes IP-Protokoll (neben TCP und UDP).Steht für ein besonderes IP-Protokoll (anders als TCP und UDP). Eine komplette Liste von aller zugewiesenen IP-Protokollnummern finden Sie unter www.iana.org/assignments/protocol-numbers.

- **Netzwerkereignisse** - die Netzwerkereignisse für die die Regel angewendet wird.Folgende Ereignisse können auftreten:

Ereignisse	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen.Mit verbindungsorientierten Protokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Abhören	Status in dem eine Anwendung das Netzwerk überwacht und darauf wartet ein Verbindung herzustellen, oder Informationen von einer gleichgestellten Anwendung zu erhalten.

- **Lokale Ports** - die Ports auf Ihrem Computer, für die die Regel angewendet wird.
- **Remote-Ports** - die Ports auf den Remote-Computern, für die die Regel angewendet wird.
- **Lokal** - ob die Regel nur für Computer im lokalen Netzwerk angewendet wird.
- **Aktion** - ob der Anwendung unter den festgelegten Umständen der Zugriff auf das Netzwerk/Internet erlaubt oder verweigert wird.

21.2.2. Regeln automatisch hinzufügen

Bei aktivierter **Firewall** überwacht BitDefender alle Anwendungen und erstellt automatisch eine Regel, wenn eine Anwendung versucht, eine Internetverbindung herzustellen.Abhängig von der Anwendung und den BitDefender Firewall-Einstellungen geschieht dies mit oder ohne Ihren Eingriff.

Wenn Sie die Basis- oder Standard-Ansicht verwenden, wird der Verbindungsaufbau von einer unbekannten Anwendung aus automatisch blockiert.

Wenn Sie die Experten-Ansicht verwenden, werden Sie über Warnhinweisfenster zu Aktionen aufgefordert, wenn eine unbekannte Anwendung versucht, sich mit dem Internet zu verbinden.

Sie können folgendes sehen: die Anwendung, die versucht, auf das Internet zuzugreifen, den Anwendung spfad, den Zielort, das verwendete Protokoll und der Port, über den die Applikation versucht die Verbindung herzustellen.

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellte Protokoll zu erlauben (eingehend und ausgehend). Wenn Sie **Blockieren**wählen, wird der Zugriff entsprechend blockiert.

Wichtig
Erlauben Sie eingehende Verbindungen nur von IP-Adressen oder Internet-Domänen, denen Sie wirklich vertrauen.

Basierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen, wird die Regeln automatisch angewendet.

21.2.3. Regeln manuell hinzufügen

Das manuelle Erstellen von Regeln unterscheidet sich in den verschiedenen Ansichtsmodi.

Standard-Ansicht

1. Klicken Sie in **Neues Programm hinzufügen** auf **Blättern**.
2. Finden Sie das Programm, für das die Regel erstellt werden soll und klicken Sie auf **Öffnen**.

3. Klicken Sie auf **Regel hinzufügen**.

   Beachten Sie, dass die Regel nun in der Tabelle angezeigt wird.

4. Wählen Sie in der Spalte **Aktion**: Zugriff erlauben oder verweigern.

   Die Aktion wird auf alle Regelparameter angewendet.

Experten-Ansicht

1. Klicken Sie auf den Button **Regel hinzufügen**.Das Konfigurationsfenster wird eingeblendet.
2. Konfigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK** um die neue Regel hinzuzufügen.

Regeln können nur modifiziert werden, wenn die Firewall in der Experten-Ansicht konfiguriert wird.Um eine bestehende Regel zu bearbeiten, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Button **Regel bearbeiten** oder doppelklicken Sie auf die Regel.Das Konfigurationsfenster wird eingeblendet.
2. Konfigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Allgemeine Parameter konfigurieren

Der Reiter **Allgemein** des Konfigurationsfensters bietet Ihnen die Möglichkeit die allgemeinen Regelparameter zu konfigurieren.

Folgende Parameter können konfiguriert werden:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm, auf das die Regel angewendet wird.Wenn Sie möchten, dass die Regel für alle Programme angewendet wird, wählen Sie **Alle**.
- **Befehlszeile.** Wenn Sie möchten, dass die Regel nur angewendet wird, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Befehlszeile von Windows geöffnet wird, deaktivieren Sie das Kontrollkästchen **Alle** und geben Sie den entsprechenden Befehl in das Bearbeitenfeld ein.
- **Protokoll.** Wählen Sie aus dem Menü das IP-Protokoll für das die Regel angewendet wird.
  - Wenn die Regel für alle Protokolle angewandt werden soll, wählen Sie **Alle**.
  - Wenn die Regel für TCP-Protokolle angewandt werden soll, wählen Sie **TCP**.
  - Wenn die Regel für UDP-Protokolle angewandt werden soll, wählen Sie **UDP**.
  - Wenn die Regel für ein bestimmtes Protokoll angewandt werden soll, wählen Sie **Andere**.Ein Editierfeld wird erscheinen.Geben Sie im eingeblendeten Fenster

die dem entsprechenden Protokoll zugewiesene Nummer, die im Bearbeitenfeld gefiltertwerden soll, ein.

Beachten Sie

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen.Steht für ein besonderes IP-Protokoll (anders als TCP und UDP). Eine komplette Liste von aller zugewiesenen IP-Protokollnummern finden Sie unter www.iana.org/assignments/protocol-numbers.

- **Ereignisanzeige.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, für die die Regel angewendet werden soll.Folgende Ereignisse können auftreten:

Ereignisse	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen.Mit verbindungsorientierten Protokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Abhören	Status in dem eine Anwendung das Netzwerk überwacht und darauf wartet ein Verbindung herzustellen, oder Informationen von einer gleichgestellten Anwendung zu erhalten.

- **Adapter-Typen:** Wählen Sie den Adaptertyp, auf den diese Regel angewendet werden soll:
- **Aktion.** Folgende Aktionen sind wählbar:

Aktion	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Blockieren	Die entsprechende Anwendung kann unter den festgelegten Bedingungen nicht auf das Internet zugreifen.

Erweiterte Parameter konfigurieren

Der Reiter **Erweitert** des Konfigurationsfensters gibt Ihnen die Möglichkeit erweiterte Regelparameter zu konfigurieren.

Folgende erweiterte Parameter können konfiguriert werden:

- **Richtung.** Wählen Sie aus dem Menü die Richtung des Datenverkehrs, für den die Regel angewendet werden soll.

Richtung	Beschreibung
Ausgehend	Die Regeln beziehen sich nur auf ausgehenden Datenverkehr.
Eingehend	Die Regeln beziehen sich nur auch eingehenden Datenverkehr.
Beide	Die Regeln findet in beide Richtungen Anwendung.

- **IP-Version.** Wählen Sie aus dem Menü die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Lokale Adresse.** Bestimmen Sie die lokale IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - Wenn Sie mehr als einen Netzwerkadapter haben, deaktivieren Sie das Kontrollkästchen **Alle** und geben Sie eine bestimmte IP-Addresse eingeben.
  - Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Remote-Adresse.** Legen Sie wie folgt die Remote-IP-Adresse und den Port fest, für die die Regel angewendet werden soll, wie folgt:
  - Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, deaktivieren Sie das Kontrollkästchen **Alle** und geben Sie dessen IP-Adresse ein.
  - Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Diese Regel nur für direkt verbundene Computer anwenden.** Wählen Sie diese Option, wenn Sie möchten dass diese Regel nur für den lokalen Datenverkehr angewendet werden soll.
- **Den Originalablauf für das ursprüngliche Ereignis überprüfen.** Sie können diesen Parameter nur verändern, wenn Sie die Option **Genaue automatische Regeln** aktiviert haben (öffnen Sie den Reiter Einstellungen und klicken Sie auf **Erweiterte Einstellungen**).Genaue Regeln bedeuten, dass BitDefender Sie jedes Mal auffordert eine Aktion durchzuführen, wenn eine Anwendung versucht, eine Verbindung mit dem Netzwerk/Internet herzustellen, wenn der vorangegangene Prozess ein anderer war.

21.2.4. Erweiterte Regelverwaltung

Wenn Sie die Regeln, die die Anwendungen regeln, einsehen oder bearbeiten möchten, klicken Sie auf den Button **Erweitert**, der verfügbar wird, wenn Sie in der Experten-Ansicht die Firewall konfigurieren.

Eine Liste der Firewall-Regeln, geordnet nach dem Datum der Erstellung wird eingeblendet.In den Spalten finden Sie umfassende Informationen zu jeder Regel.

Beachten Sie

Wenn ein Verbindungsversuch ausgeführt wurde (sowohl eingehend als auch ausgehend), wendet BitDefender die Aktion der ersten Regel an, die auf die entsprechende Verbindung zutrifft.Deshalb ist die Reihenfolge der Regeln sehr wichtig.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf den Button **Regel löschen**.

Um eine bereits existierende Regel zu bearbeiten, klicken Sie auf diese und danach auf **Regel bearbeiten** oder doppelklicken Sie darauf.

Sie können die Priorität einer Regel erhöhen oder herabsetzen. Klicken Sie **In der Liste hochsetzen**, um die ausgewählte Regel um einen Level nach oben zu setzen. Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herabzusetzen.Um einer Regel die höchste Priorität zu geben, klicken Sie auf die **Als erste**-Schaltfläche. Um einer Regel die niedrigste Priorität zu zuweisen, klicken Sie auf die **Als letzte**-Schaltfläche.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

21.2.5. Löschen und Zurücksetzen von Regeln

Nur bei einer Konfiguration in der Experten-Ansicht können die Firewall-Einstellungen gelöscht oder zurückgesetzt werden.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf den Button **Regel löschen**.Sie können eine oder auch mehrere Regeln auswählen und löschen.

Möchten Sie alle für eine bestimmte Anwendung erstellen Regeln löschen, wählen Sie die Anwendung aus der Liste und klicken auf den Button **Regel löschen**.

Falls Sie für die gewählte Sicherheitsstufe den Standardregelsatz laden wollen, klicken Sie **Regeln zurücksetzen**.

21.3. Netzwerk-Einstellungen

Um die Netzwerkverbindung-Einstellungen zu konfigurieren, öffnen Sie BitDefender und gehen Sie, abhängig von der Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie auf den Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**. Wählen Sie im neu eingeblendeten Fenster den Reiter **Netzwerk**.

Experten-Ansicht

Gehen Sie zu **Firewall > Netzwerk**.

Die Spalte **Netzwerkkonfiguration** bietet eine Reihe von Detailinformationen über das verbundene Netzwerk und ermöglicht eine Konfiguration folgender Einstellungen:

- **Adapter** - der Netzwerkadapter, den Ihr Computer verwendet, um eine Verbindung mit dem Netzwerk oder dem Internet herzustellen.
- **Netzwerktypen** - der Netzwerktyp, mit dem der Adapter verbunden ist.Abhängig von der Netzwerkadapter-Konfiguration wird BitDefender automatisch einen Netzwerktyp wählen oder Sie um weitere Angaben bitten.

  Durch Klicken auf den Pfeil ▾ in der Spalte **Netzwerktyp** können Sie den Typ ändern oder aus der Liste einen verfügbaren Typ wählen.

Netzwerktyp	Beschreibung
Vertrauenswürdig	Deaktiviert die Firewall für den entsprechenden Adapter.
Zuhause/Büro	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.
Öffentlichkeit	Sämtlicher Datenverkehr wird gefiltert.
Nicht vertrauenswürdig	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

- **VPN** - ob es sich bei der Verbindung um eine VPN handelt.

  Der durch die VPN-Verbindung gehende Datenverkehr wird anders gefiltert als der Datenverkehr über Netzwerkverbindungen.Handelt es sich bei der Verbindung um eine VPN, klicken Sie auf den Pfeil ▾ der Spalte **VPN** und wählen Sie **Ja**.

In der Experten-Ansicht werden zwei zusätzliche Spalten angezeigt:

- **Stealth Modus** - ob Sie von anderen Computern entdeckt werden können.

  Um den Stealth-Modus zu konfigurieren, klicken Sie auf den Pfeil ▾ in der Spalte **Stealth-Modus** und wählen Sie die gewünschte Option.

Stealth-Option	Beschreibung
Aktiviert	Stealth-Modus ist aktiviert.Ihr Computer ist weder im lokalen Netzwerk noch im Internet sichtbar.

Stealth-Option	Beschreibung
Deaktiviert	Stealth-Modus ist deaktiviert.Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer finden.
Entfernt	Ihr Computer kann nicht im Internet entdeckt werden.Benutzer im lokalen Netzwerk können Ihren Computer finden.

- **Allgemein** - ob die allgemeinen Regeln für diese Verbindung angewendet werden sollen.

  Wenn sich die IP-Adresse eines Netzwerkadapters geändert hat, verändert BitDefender die Vertrauensstufe entsprechend.Wenn Sie denselben Typ beibehalten möchten, klicken Sie auf den Pfeil in der Spalte **Generisch** und dann auf **Ja**.

21.3.1. Netzwerk-Zonen

Sie können einem bestimmten Adpater erlaubte oder blockierte Computer hinzufügen.

Ein vertrauenswürdiger Bereich ist ein Computer, dem Sie vollständig vertrauen.Zwischen Ihrem Computer und den Computern, denen Sie vertrauen, ist jeglicher Datenaustausch erlaubt.Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Ein blockierter Bereich ist ein Computer, mit dem Ihr Computer in keiner Weise kommunizieren soll.

In der Tabelle **Netzwerkzonen** werden die aktuellen Netzwerkzonen pro Adapter angezeigt.

Um eine Zone hinzufügen, wählen Sie den Adapter und klicken dann auf **Zone hinzufügen**. Ein neues Fenster wird geöffnet.

Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers der hinzugefügt werden soll.
2. Wählen Sie eine Aktion:
   - **Zulassen** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird erlaubt.
   - **Verweigern** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird blockiert.
3. Klicken Sie auf **OK**.

21.4. Geräte

Um die an das Netzwerk angeschlossenen Geräte zu verwalten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neu eingeblendeten Fenster den Reiter **Geräte**.

Experten-Ansicht
: Gehe zu **Firewall > Geräte**.

Die Drucker, Faxgeräte und Scanner Ihres Netzwerks und die für diese Geräte voreingestellten Aktionen werden in der Tabelle aufgelistet.Um den Status eines Gerätes zu ändern, doppelklicken Sie auf die Tabelle und wählen Sie eine der eingeblendeten Aktionen: Kommunikation mit dem Gerät zulassen oder blockieren.

Über die verfügbaren Buttons können Sie die Geräteliste verwalten:

- **Add** - ein Gerät hinzufügen, das nicht in der Liste aufgeführt ist.
- **Entfernen** - ein ausgewähltes Gerät aus der Liste entfernen.
- **Geräte aktualisieren** - Durchführen eines neuen Scans, um die Geräteliste des Netzwerks zu aktualisieren.

21.5. Verbindungskontrolle

Um die aktuellen Netzwerk-/Internetaktivitäten (über TCP und UDP), sortiert nach Anwendungen, zu überwachen und um das BitDefender Firewall-Protokoll zu öffnen, folgen Sie folgenden Schritten:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Firewall > Aktivität**.

Hier können Sie den gesamten Datenverkehr, sortiert nach Anwendungen, einsehen. Für jede Anwendung können Sie die Verbindungen und offenen Ports sehen, außerdem Statistiken zur Geschwindigkeit des ausgehenden und eingehenden Datenverkehrs und das gesamte Volumen der gesendeten/empfangenen Daten.

Wenn Sie auch die inaktiven Prozesse sehen möchten, deaktivieren Sie das Kontrollkästchen **Inaktive Prozesse verbergen**.

Die Bedeutung der Symbole ist wie folgt:

- Zeigt eine ausgehende Verbindung an.
- Zeigt eine eingehende Verbindung an.

- Zeigt einen offenen Port auf Ihrem Computer an.

Das Fenster zeigt die aktuellen Netzwerk/Internetaktivitäten in Echtzeit. Wenn einzelne Verbindungen oder Ports geschlossen werden, können Sie sehen, wie diese grau hinterlegt und evtl. ausgeblendet werden.Analog geschieht dies auch für alle Statistiken in Zusammenhang mit einer Anwendung, die einen Datenfluss erzeugt oder offene Ports hat und die Sie schließen.

Eine umfangreiche Ereignisliste zur Verwendung des Firewall-Moduls (Firewall aktivieren/deaktivieren, Datenverkehr blockieren, Einstellungen verändern) oder durch die von diesem Modul entdeckten Aktivitäten (Port-Scan, Verbindungsversuche oder Datenverkehr entsprechend den Regeln blockieren), finden Sie im BitDefender Firewall-Protokoll. Klicken Sie auf **Protokoll anzeigen**.Die Datei befindet sich im Verzeichnis Gemeinsame Dateien des aktuellen Windows-Benutzers unter dem folgenden Pfad: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Wenn Sie möchten, dass das Protokoll noch mehr Informationen enthält, wählen Sie **Protokollumfang erweitern**.

21.6. Fehlersuche Firewall

Falls Sie ein Problem feststellen, dass möglicherweise mit der BitDefender-Firewall zusammenhängt, steht ein Fehlersuche-Assistent zur Verfügung, der Ihnen bei der Lösung des Problems hilft.

Um den Assistenten zu starten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Der Assistent kann Ihnen dabei helfen, die folgenden, normalerweise mit der Firewall-Konfiguration zusammenhängenden, Verbindungsprobleme schnell zu lösen:

- Ich versuche etwas auszudrucken, dies ist aber nicht möglich.
- Ich versuche auf einen Computer meines Netzwerks zuzugreifen, dies funktioniert aber nicht.
- Ich versuche ins Internet zu gehen, dies funktioniert aber nicht.

Falls keine der Beschreibungen auf Ihr Problem zutrifft, wählen Sie **Andere Firewall-Probleme**, um das **Support-Tool** zu öffnen.

Weitere Informationen zu diesem Assistenten finden Sie im Kapitel Fehlersuche in dieser Anleitung.

22. Schwachstellen

Ein wichtiger Schritt für den Tresor Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand zu halten.Um einen ungewünschten Zugriff auf Ihren Computer zu verhindern, müssen sichere Passwörter (Passwörter die nicht einfach erraten werden können) für jedes Windows-Benutzerkonto konfiguriert werden.

BitDefender scannt Ihr System regelmäßig auf Schwachstellen und benachrichtigt Sie über die bestehenden Probleme.

22.1. Auf Schwachstellen scannen

Sie können Schwachstellen überprüfen und diese beseitigen, indem Sie den Assistenten für den **Schwachstellen-Scan** zu Hilfe ziehen.Um den Assistenten zu starten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Schwachstellen-Scan**.

Experten-Ansicht
: Gehen Sie zu **Schwachstellen> Status** und klicken Sie auf **Jetzt überprüfen**.

Folgen Sie der sechsstufigen Anleitung, um die Schwachstellen Ihres Systems zu entfernen.Innerhalb des Assistenten können Sie über den Button **Weiter** navigieren. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Schützen Sie Ihren Rechner**

   Wählen Sie die zu scannenden Schwachstellen.

2. **Ausgewählte Einträge scannen...**

   Bitte warten Sie, bis BitDefender den Scan auf Schwachstellen beendet hat.

3. **Windows Updates**

   Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zurzeit nicht auf Ihrem Computer installiert sind.Wählen Sie die Updates, die Sie installieren möchten.

4. **Anwendungs-Updates**

   Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

5. **Unsichere Passwörter**

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.Klicken Sie auf **Beheben**, um unsichere Passwörter zu ändern.

6. **Übersicht**

   Hier können Sie das Ergebnis der Operation sehen.

22.2. Status

Um den aktuellen Schwachstellenstatus zu sehen und den automatischen Schwachstellen-Scan zu aktivieren/deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Schwachstellen> Status**.

Jede Tabelle zeigt die gelösten Objekte aus der letzten Schwachstellenprüfung und deren aktuellen Status an.Hier können Sie sehen, welche Aktion Sie durchführen sollen, um jede Schwachstelle (falls vorhanden) zu beheben.Wenn die Aktion**Keine** ist, dann wird diese Angelegenheit keine Schwachstelle darstellen.

Wichtig
Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Automatischer-Scan** aktiviert.

Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:

- Wenn Windows Updates verfügbar sind, klicken Sie in der Spalte **Aktion** auf **Installieren**.
- Wenn eine Anwendung veraltet ist, klicken Sie auf **Mehr Infos**, um sich die Versionsinformationen anzusehen und um einen Link auf die Herstellerseite der jeweiligen Software zu finden, von der aus Sie die aktuellste Software-Version installieren können.
- Falls ein Windowskonto über ein schwaches Passwort verfügt, klicken Sie auf **Ansicht& Beheben** und fordern Sie den Benutzer beim nächsten Windows-Login auf, das Passwort zu ändern oder ändern Sie es selbst.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ oder @).
- Wenn in Windows die Media Autorun-Funktion aktiviert ist, klicken Sie auf **Fest**, um diese zu deaktivieren.

22.3. Einstellungen

Um die Einstellungen für die automatische Schwachstellenüberprüfung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Schwachstellen> Einstellungen**.
3. Markieren Sie die Kontrollkästchen der entsprechenden Systemschwachstellen die regelmäßig überscannt werden sollen.
   - **Wichtige Windows-Updates**
   - **Reguläre Windows Updates**
   - **Anwendungs-Updates**
   - **Unsichere Passwörter**
   - **Media Autorun**

Beachten Sie

Wenn Sie das Kontrollkästchen für eine bestimmte Schwachstelle freilassen, wird Bitdefender Sie nicht über die entsprechenden Probleme und Risiken informieren.

23. Instant-Messaging-Verschlüsselung

Die Inhalte Ihrer InstantMessaging-Konversationen sollten zwischen Ihnen und Ihrem Chat-Partner bleiben.Durch die Verschlüsselung Ihrer Konversationen können Sie sicherstellen, dass niemand die Inhalte dieser Konversationen auf dem Weg von und zu Ihnen lesen kann.

BitDefender verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

- Ihr Chatpartner eine BitDefender Version installiert hat, die die IM-Verschlüsselung unterstützt und die IM-Verschlüsselung für die Instant Messaging-Anwendung aktiviert ist.
- Sie und Ihr Chatpartner entweder Yahoo Messenger oder Windows Live (MSN) Messenger verwenden.

Wichtig
BitDefender wird die Konversationen nicht verschlüssel, wenn ein Chat-Partner eine webbasierte Chat-Anwendung (wie Meebo) oder eine andere Anwendung, die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt, verwendet.

Um die Instant Messaging-Verschlüsselung zu konfigurieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Verschlüsselung > IM-Verschlüsselung**.

Beachten Sie
Sie können die IM-Verschlüsselung für jeden Chat-Partner einfach über die BitDefender-Symbolleiste im Chat-Fenster konfigurieren.

Die IM-Verschlüsselung ist standardmäßig für Yahoo Messenger und Windows Live (MSN) Messenger aktiviert.Sie können die IM-Verschlüsselung für eine bestimmte Anwendung oder komplett deaktivieren.

Zwei Tabellen werden angezeigt:

- **Verschlüsselungsausnahmen** - listet die Benutzer-IDs und das entsprechende IM-Programm auf, für den die Verschlüsselung deaktiviert ist.Um einen Kontakt aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf den Button **Entfernen**.
- **Aktuelle Verbindungen** - listet die aktuellen Instant Messaging Verbindungen auf (Benutzer ID und entsprechendes IM-Programm) und zeigt an, ob diese verschlüsselt sind oder nicht.Eine Verbindung kann aus folgenden Gründen nicht verschlüsselt sein:

- Sie haben die Verschlüsselung für den entsprechenden Kontakt deaktiviert.
- Ihr Kontakt hat keine BitDefender-Version installiert, die eine IM-Verschlüsselung unterstützt.

23.1. Deaktivierung der Verschlüsselung für bestimmte Benutzer

Um die Verschlüsselung für einen bestimmten Benutzer zu deaktivieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Button **Hinzufügen**, um das Konfigurationsfenster zu öffnen.
2. Geben Sie die Benutzer-ID Ihres Kontaktes in das Editierfeld ein.
3. Wählen Sie die Chat-Anwendung des Kontaktes.
4. Klicken Sie auf **OK**.

23.2. BitDefender-Symbolleiste im Chat-Fenster

Sie können die IM-Verschlüsselung einfach über die BitDefender Symbolleiste aus dem Chat-Fenster heraus konfigurieren.

Die Symbolleiste sollte sich in der unteren rechten Ecke des Chat-Fensters befinden. Sehen Sie nach dem BitDefender Logo um sie zu finden.

Beachten Sie

Die Symbolleiste zeigt durch eine kleine Taste 🗝 direkt neben dem BitDefender-Logo an, dass eine Konversation verschlüsselt wurde.

Durch Klicken auf die BitDefender-Symbolleiste, erhalten Sie die folgenden Optionen:

- **Dauerhaft die Verschlüsselung für Kontakt deaktivieren.**
- **Kontakt einladen. Verschlüsselung zu verwenden.** Um Ihre Konversation zu verschlüsseln, muss auch das Gegenüber BitDefender installiert haben und ein kompatibles IM Programm verwenden.
- **Kontakt zur Blacklist der Kindersicherung hinzufügen.** Wenn Sie den Kontakt zur Blacklist der Kindersicherung hinzufügen und diese aktiviert ist, so werden Sie keine weitere Nachricht von diesem Kontakt sehen.Um Kontakte aus der Blacklist zu entfernen klicken Sie in der Toolbar auf **Kontakt aus der Blacklist der Kindersicherung entfernen**.

24. Spiele-/Laptop-Modus

Das Modul Spiele-/Laptop-Modus bietet ihnen die Möglichkeit spezielle Betriebsmodi von BitDefender zu konfigurieren.

- Der Spiele-Modus verändert vorübergehend die Produkteinstellungen, um die Systembelastung während des Spielens möglichst gering ist.
- Der Laptop-Modus stoppt voreingestellte Aufgaben, wenn der Laptop im Akkubetrieb läuft, um dessen Laufzeit zu verlängern.
- Stumm-Modus modifiziert vorübergehend die Produkteinstellungen, so dass das Ansehen eines Films oder das Halten einer Präsentation nicht unterbrochen wird.

24.1. Spiele-Modus

Der Spiele-Modus verändert vorübergehend die Schutzeinstellungen so, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.Wenn Sie den Spiele-Modus aktivieren, werden folgende Einstellungen angewendet:

- Alle BitDefender-Alarme und Pop-ups werden deaktiviert.
- Der BitDefender Echtzeitschutz wird auf **Tolerant** gestellt.
- Die BitDefender Firewall ist auf**Alle zulassen** eingestellt.Dies bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Updates werden nicht standardmäßig durchgeführt.

> **Beachten Sie**
> Um diese Einstellung zu ändern, gehen Sie zu Update > Einstellungen und deaktivieren Sie das Kontrollkästchen **Kein Update im Spiele-Modus**.

BitDefender wechselt standardmäßig in den Spiele-Modus, wenn Sie ein Spiel starten, das sich auf der Liste der bekannten Spiele von BitDefender befindet, oder wenn eine Anwendung im Vollbildmodus ausgeführt wird.Sie können den Spiele-Modus manuell über das Tastaturkürzel `Strg+Alt+Shift+G` aktivieren.Es wird dringend empfohlen dass Sie den Spiele-Modus verlassen, wenn Sie mit dem Spielen fertig sind (Sie können dafür das selbe Tastenkürzel verwenden `Ctrl+Alt+Shift+G`).

> **Beachten Sie**
> Wenn der Spiele-Modus aktiviert ist, sehen Sie den Buchstaben `G` über dem BitDefender Symbol.

Konfiguration des Spiele-Modus:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

2. Gehen Sie zu **Spiele-/Laptop-Modus> Spiele-Modus**.

Im oberen Bereich des Abschnitts können Sie den Status des Spiele-Modus sehen.Um den aktuellen Status zu ändern, können Sie auf **Spiele-Modus ist aktiviert** oder **Spiele-Modus ist deaktiviert** klicken.

24.1.1. Konfiguration des Automatischen Spiele-Modus

Im automatischen Spiele-Modus kann BitDefender selbständig den Spiele-Modus starten, wenn ein Spiel gefunden wird.Folgende Optionen können konfiguriert werden:

- **Die BitDefender-Standardspieleliste verwenden** - damit BitDefender automatisch in den Spiele-Modus wechselt, wenn Sie ein in der Liste aufgeführtes Spiel starten.Diese Liste finden Sie unter **Spiele verwalten**, **Spieleliste**.
- **Vollbildmodus** - Sie können wählen, ob BitDefender automatisch in den Spiele- oder Stumm-Modus wechseln soll, sobald eine Anwendung im Vollbildmodus angezeigt wird.
- **Vollbild-Anwendung der Spieleliste hinzufügen?** - um aufgefordert zu werden, ob eine neue Anwendung zur Spieleliste hinzugefügt werden soll, wenn Sie das Vollbild verlassen.Indem Sie eine neue Anwendung zur Spieleliste hinzufügen, wird BitDefender den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

Beachten Sie
Wenn Sie nicht möchten, dass BitDefender den Spiele-Modus automatisch startet, lassen Sie das Kontrollkästchen **Automatischer Spiele-Modus ist aktiviert** frei.

24.1.2. Verwaltung der Spieleliste

BitDefender startet den Spiele-Modus automatisch, wenn eine Anwendung gestartet wird, die sich auf der Spieleliste befindet.Um die Spieleliste zu sehen und zu verwalten, klicken Sie auf**Spiele verwalten**.Ein neues Fenster wird geöffnet.

Neue Anwendungen werden automatisch der Liste hinzugefügt, wenn:

- Sie ein Spiel starten, das BitDefender bekannt ist.Diese Liste finden Sie unter **Spieleliste**.
- Nachdem Sie den Vollbildmodus verlassen haben, können Sie das Spiel über das Aufforderungsfenster der Spieleliste hinzufügen.

Wenn Sie den automatischen Spiele-Modus für eine bestimmte Anwendung auf der Liste deaktivieren möchten, lassen Sie das entsprechende Kontrollkästchen frei.Sie sollten den automatischen Spiele-Modus für reguläre Anwendungen, die den gesamten Bildschirm verwenden, wie Web-Browser und Mediaplayer, deaktiviert lassen.

Um die Spieleliste zu verwalten, können Sie den Buttonn verwenden, die sich im oberen Bereich der Tabelle befineden:

- **Hinzufügen** - eine neue Anwendung wird der Spieleliste hinzugefügt.
- **Entfernen** - eine Anwendung wird aus der Spieleliste gelöscht.
- **Bearbeiten** - ein existierender Eintrag der Spieleliste kann hier bearbeitet werden.

24.1.3. Spiele hinzufügen oder bearbeiten

Wenn Sie der Spieleliste einen Eintrag hinzufügen oder bearbeiten möchten, wird folgendes Fenster eingeblendet:

Klicken Sie auf **Durchsuchen**, um die Anwendung auszuwählen oder geben Sie den vollständigen Pfad der Anwendung in das Editierfeld ein.

Wenn Sie nicht möchten, dass automatisch in den Spiele-Modus wechselt, wenn eine bestimmte Anwendung gestartet wird, wählen Sie **Deaktivieren**.

Klicken Sie auf **OK**, um den Eintrag der Spieleliste hinzuzufügen.

24.1.4. Konfiguration der Einstellungen des Spiele-Modus

Um das Verhalten geplanter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Scan-Aufgaben zubearbeiten** - um zu verhindern, dass geplante Scan-Aufgaben starten, während der Spiele-Modus aktiviert ist.Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die geplante Aufgabe sofort ausgeführen, wenn der Spiele-Modus beendet wird.

Um die BitDefender Firewall automatisch zu deaktivieren, wenn der Spiele-Modus ausgeführt wird, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Erweiterte Einstellungen**.Ein neues Fenster wird geöffnet.
2. Aktivieren Sie die Option **Firewall im Spiele-Modus auf Alle erlauben setzen**.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

24.1.5. Änderung der Tastenkombination des Spiele-Modus

Sie können den Spiele-Modus manuell aktivieren, indem Sie die VoreinstellungCtrl+Alt+Shift+GHotkey.Diese Tastenkombination können Sie bei Bedarf folgendermaßen ändern:

1. Klicken Sie auf **Erweiterte Einstellungen**.Ein neues Fenster wird geöffnet.
2. In der Option **Tastaturkürzel verwenden** können Sie die gewünschte Tastenkombination festlegen:
   - Wählen Sie die gewünschte Tastenkombination aus indem Sie eine der folgenden Varianten auswählen: Steuerung (Strg), Shift (Shift) oder Alt-Taste (Alt).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination Strg+Alt+D benutzen möchten, markieren Sie Strg und Alt und geben Sie D ein.

   Beachten Sie
   Wenn Sie die Markierung neben **Tastenkombination** entfernen, wird die Tastenkombination deaktiviert.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

24.2. Laptop-Modus

Der Laptop-Modus wurde für Nutzer von Laptops und Notebooks konzipiert. Er soll den Energieverbrauch von BitDefender so gering wie möglich halten um den Einfluss auf die Akkulaufzeit zu minimieren.

Während der Laptop-Modus ausgeführt wird, werden voreingestellte Aufgaben standardmäßig nicht durchgeführt.

BitDefender erkennt, wenn Ihr Laptop im Akkubetrieb läuft und startet den Laptop-Modus automatisch.Ebenso beendet BitDefender automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Konfiguration des Laptop-Modus:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Spiele-/Laptop-Modus> Laptop-Modus**.

Sie sehen, ob der Laptop-Modus aktiviert ist.Ist der Laptop-Modus aktiviert, wird BitDefender die konfigurierten Einstellungen anwenden, während der Laptop über einen Akku betrieben wird.

24.2.1. Konfiguration der Einstellungen des Laptop-Modus

Um das Verhalten geplanter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antivirus-Scan-Aufgaben zu bearbeiten** - um zu verhindern dass geplante Scan-Aufgaben starten, während der Laptopmodus aktiviert ist.Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die Aufgabe wird sofort durchgeführt, sobald der Laptop-Modus verlassen wird.

24.3. Stumm-Modus

Der Stumm-Modus ändert die Tresoreinstellungen vorübergehend, so dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist.Wenn der Stumm-Modus aktiviert ist, werden folgende Einstellungen angewendet:

- Alle BitDefender-Alarme und Pop-ups werden deaktiviert.
- Die BitDefender Firewall ist auf**Alle zulassen** eingestellt.Dies bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Voreingestellte Scan-Aufgaben sind standardmäßig deaktiviert.

Als Voreinstellung wechselt BitDefender automatisch in den Stumm-Modus, sobald Sie einen Film ansehen, eine Präsentation halten oder eine Anwendung im Vollbildmodus nutzen.Wir empfehlen dringend, den Stumm-Modus zu verlassen, wenn Sie den Film zu Ende gesehen oder die Präsentation beendet haben.

Beachten Sie

Wenn Sie sich im Stumm-Modus befinden, verändert sich das kleine BitDefender-Symbol neben der Computeruhr ein wenig.

Konfiguration des Stumm-Modus:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Spiele-/Laptop-Modus> Stumm-Modus**.

Im oberen Bereich des Abschnitts können Sie den Status des Stumm-Modus sehen.Um den aktuellen Status zu ändern, können Sie auf **Stumm-Modus ist aktiviert** oder **Stumm-Modus ist deaktiviert** klicken.

24.3.1. Konfiguration Vollbildschirmaktion

Folgende Optionen können konfiguriert werden:

- **Vollbildmodus** - Sie können wählen, ob BitDefender automatisch in den Spiele- oder Stumm-Modus wechseln soll, sobald eine Anwendung im Vollbildmodus angezeigt wird.

Beachten Sie

Wenn Sie nicht möchten, dass BitDefender automatisch in den Stumm-Modus wechselt, deaktivieren Sie die Option **Vollbildschirm-Aktion**.

24.3.2. Konfiguration der Einstellungen des Stumm-Modus

Um das Verhalten geplanter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Dieses Modul aktivieren, um geplante Antiviren-Scans zu bearbeiten** - um zu verhindern, dass geplante Scans starten, während der Stumm-Modus aktiviert ist.Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die Aufgabe wird sofort durchgeführt, sobald der Stumm-Modus verlassen wird.

25. Heimnetzwerk

Mit dem Netzwerk-Modul können Sie die auf den Computern Ihres Haushalts installierten BitDefender-Produkte von einem Computer aus verwalten.Um auf das Modul "Heimnetzwerk" zuzugreifen, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
Gehen Sie auf den Reiter **Netzwerk**.

Experten-Ansicht
Gehe zu **Heimnetzwerk**.

Beachten Sie
Im Bereich Meine Werkzeuge können Sie eine Verknüpfung hinzufügen.

Um die BitDefender Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

1. Aktivieren Sie das BitDefender-Heimnetzwerk auf Ihrem Computer.Legen Sie Ihren Computer als Server fest.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Heimnetzwerk hinzu (legen Sie das Passwort fest).Defenieren Sie jeden Computer als Normal.
3. Fügen Sie die Computer, die Sie verwalten möchten, auf Ihrem Computer hinzu.

25.1. Aktivierung des BitDefender-Netzwerks

Zur Aktivierung des BitDefender-Heimnetzwerks gehen Sie folgendermaßen vor:

1. Klicken Sie **Netzwerk aktivieren**.Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.
2. Geben Sie dasselbe Passwort in jedes der Editierfelder ein.
3. Legen Sie die Rolle des Computers im BitDefender-Heimnetzwerk fest:
   - **Server-Computer** - aktivieren Sie diese Option auf dem Computer, von dem aus alle anderen verwaltet werden sollen.
   - **Normaler Computer** - aktivieren Sie diese Option auf den Computern, die vom Server-Computer aus verwaltet werden.
4. Klicken Sie auf **OK**.

Sie sehen den Namen des Computers in der Netzwerkübersicht.

Der Button **Netzwerk deaktivieren** wird eingeblendet.

25.2. Computer dem BitDefender-Netzwerk hinzufügen

Jeder Computer, der die folgenden Kriterien erfüllt, wird automatisch dem Netzwerk hinzugefügt:

- das BitDefender-Heimnetzwerk ist auf diesem Computer aktiviert.
- der Computer wurde als normaler Computer definiert.
- das Passwort für die Aktivierung des Netzwerks ist dasselbe wie für den Server-Computer.

Beachten Sie
In der Experten-Ansicht können Sie jederzeit das Heimnetzwerk auf Computer scannen, die den Kriterien entsprechen, indem Sie auf den Button **Auto-Suche** klicken.

Um vom Master Computer aus einen Computer dem BitDefender-Heimnetzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **PC hinzufügen**.
2. Geben Sie das Passwort für die Heimnetzwerk-Verwaltung ein und klicken Sie auf **OK**.Ein neues Fenster wird geöffnet.

   Sie sehen eine Computerliste des Netzwerks.Die Bedeutung des Symbols ist wie folgt:

    Zeigt einen Online-Computer an, auf dem keine BitDefender-Produkte installiert sind.
    Zeigt einen Online-Computer an, auf dem BitDefender installiert ist.
    Zeigt einen Offline-Computer an, auf dem BitDefender installiert ist.
3. Sie können hierzu eine der folgenden Aktionen wählen:
   - Wählen Sie aus der Liste den Namen des Computers aus, der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll, in das dafür vorgesehene Feld ein.
4. Klicken Sie auf **Hinzufügen**.Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.
5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.
6. Klicken Sie auf **OK**.Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

25.3. Verwaltung des BitDefender-Netzwerks

Wenn Sie das BitDefender Heimnetzwerk erstellt haben, können Sie alle BitDefender Produkte von einem Computer aus verwalten.

Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Systemsicherheitsprobleme die, BitDefender-Registrierungsstatus).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **BitDefender auf diesem Computer registrieren**

  Erlaubt Ihnen BitDefender auf diesen Rechner, durch Eintragen eines Lizenzschlüssels, zu registrieren.

- **Einstellungenpasswort für Remote PC festlegen**

  Erlaubt Ihnen einen Passwort zu erstellen um den Zugang zu den BitDefender Einstellungen auf diesem PC einzuschränken.

- **On-Deman-Scan-Aufgabe ausführen**

  Lässt sie einen On-Demand-Scan auf dem Remote-PC durchführen. Sie können jede der folgenden Scans ausführen: Meine Dokumente, System-, oder Tiefensystem-Scan.

- **Alle Probleme auf diesem PC beheben**

  Lässt Sie alle Sicherheitsprobleme auf diesem PC beheben, indemSie den Anweisungen des Alle Probleme beheben-Assistenten folgen.

- **Historie/Ereignisse anzeigen**

  Erlaubt den Zugriff auf das Modul **Verlauf & Ereignisse** des auf diesem PC installierten BitDefender-Produkts.

- **Jetzt aktualisieren**

  Startet das Update für das auf diesem Computer installierte BitDefender-Produkt.

- **Kindersicherungsprofil festlegen**

  Erlaubt die Festlegung des Alterskategoriefilters, der für diesen PC verwendet werden soll.

- **Als Update-Server für dieses Netzwerk festlegen**

  Erlaubt Ihnen, diesen Rechner als Update-Server, für alle Rechner des Netzwerks auf denen wo BitDefender installiert ist, festzulegen.Mithilfe dieser Option wird der Internetverkehr verringert, weil nur ein Rechner aus dem Netzwerk sich in das Internet einwählt, um die Updates herunterzuladen.

- **PC aus dem Heimnetzwerk entfernen**

  Erlaubt Ihnen, einen Pc aus dem Netzwerk zu entfernen.

Wenn BitDefender in der Standard-Ansicht läuft, können Sie mehrere Aufgaben auf allen Netzwerk-Computern gleichzeitig ausführen, indem Sie auf die entsprechenden Buttons klicken.

- **Alle scannen** - bietet Ihnen die Möglichkeit, alle verwalteten Computer gleichzeitig zu scannen.
- **Alle aktualisieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu aktualisieren.
- **Alle registrieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu registrieren.

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert, das Passwort für das Heimnetzwerk anzugeben.Geben Sie das Passwort für die Heimnetzwerk-Verwaltung ein und klicken Sie auf **OK**.

Beachten Sie

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**.Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

26. Update

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm BitDefender stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet die BitDefender-Software eigenständig. Sie überprüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und sucht nach Bedarf anschließend jede **Stunde** nach Updates.

Wenn ein Update gefunden wird, können Sie um eine Bestätigung für das Update gebeten werden oder das Update wird automatisch durchgeführt abhängig von Ihren Einstellungen für das automatische Update.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien werden stufenweise aktualisiert. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System nicht gefährdet.

Wichtig
Um den Schutz vor Spyware aus dem Internet zu gewährleisten, halten Sie Ihre **Automatische Update** Funktion jederzeit aktiviert.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Antivirus-Updates** - täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **Antispam-Updates** - um den Spamschutz zu verbessern, werden neue Regeln zur Heuristik und zum URL-Filter hinzugefügt. Diesen Vorgang nennt man **Antispam-Update**.
- **AntiSpyware-Updates** - neue Spyware-Signaturen werden kontinuierlich zur Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.
- **Produkt-Upgrades** - erscheint eine neue Version erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringen, erhalten Sie diese per Update. Diesen Vorgang nennt man **Produkt-Upgrade**.

26.1. Durchführung eines Updates

Das automatische Update kann auch jederzeit über den Klick **Jetzt aktualisieren** erfolgen. Diese Funktion wird auch als **Benutzergesteuertes Update** bezeichnet.

Für ein BitDefender-Update gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Basis-Ansicht
Klicken Sie im Bereich "Meinen PC schützen" auf das Symbol **Jetzt aktualisieren**.

Standard-Ansicht
Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Jetzt aktualisieren**.

Experten-Ansicht
Gehen Sie zu **Update > Update**.

Das **Update**-Modul verbindet Ihren Computer automatisch mit dem BitDefender Update Server und informiert Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt, ob das Update erfolgen soll oder das Update erfolgt automatisch.

Wichtig
Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.

Beachten Sie

Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen.Weitere Informationen finden Sie unter *„Wie Sie ein BitDefender-Update mit einer langsamen Internetverbindung durchführen.“* (S. 186).

26.2. Konfiguration der Update-Einstellungen

Updates können vom lokalen Netz, 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.

Konfiguration der Update-Einstellungen:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Update > Einstellungen**.
3. Konfigurieren Sie die Einstellungen nach Ihren Wünschen. Um herauszufinden, was eine Option bewirkt, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Wenn Sie die Standardeinstellungen anwenden möchten, klicken Sie auf **Voreingestellt**.

Die Update-Einstellung ist in vier Kategorien unterteilt: (**Update-Speicherorteinstellungen**, **Einstellungen für das Automatische**

Update, **Einstellungen für das manuelle Update** und **Erweiterte Einstellungen**). Jede Kategorie wird seperat erläutert.

26.2.1. Festlegen des Update-Speicherorts

Um eine Update-Adresse festzulegen, verwenden Sie die Optionen der Kategorie **Update-Speicherorteinstellungen**.

Beachten Sie

Ändern Sie diese Einstellungn nur wenn Sie mit einem BitDefender lokalen Update-Server verbunden sind oder wenn das Update über einen Proxy erfolgt.

Für ein zuverlässigeres und schnelleres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Standardmäßig stimmen diese beiden Adressen überein: `http://upgrade.bitdefender.com`.

Um die Update-Adresse zu ändern geben Sie die Adresse des lokalen Servers in das gewünschte **URL** Feld ein.

Beachten Sie

Wir empfehlen den Primären Updateserver auf den lokalen Server zu ändern und den sekundären Server unverändert zu belassen sodass im Falle eines lokalen Serverausfalls dennoch Updates durchgeführt werden können.

Wenn Sie für den Zugang zum Internet einen Proxy verwenden, wählen Sie die Option **Proxy verwenden**, und klicken dann auf **Proxy-Einstellungen** um diese zu konfigurieren.Weitere Informationen finden Sie unter „Verbindungseinstellungen“ (S. 58)

26.2.2. Konfiguration Automatisches Update

Um die Optionen des BitDefender Automatischen Updates zu konfigurieren verwenden Sie die Optionen der Kategorie **Einstellungen für das Automatische Update**.

Sie können die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen im Feld **Zeitinterval** festlegen. Standardmäßig ist dieses auf eine Stunde eingestellt.

Um festzulegen wie das automatische Update durchgeführt werden soll können Sie zwischen den folgenden Optionen wählen:

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Nachfragen, bevor Update heruntergeladen werden** - immer wenn ein Update verfügbar ist, werden Sie gefragt, ob dieses heruntergeladen werden soll.
- **Nachfragen bevor Updates installiert werden** - frägt Sie bevor ein Update installiert wird.

26.2.3. Konfiguration Manuelles Update

Um festzulegen wie ein manuelles Update durchgeführt wird wählen Sie ein der folgenden Optionen in der Kategorie **Einstellungen für das manuelle Update**:

- **Update im Hintergrund** - führt Updates komplett selbständig im Hintergrund durch.
- **Nachfragen, bevor Update heruntergeladen werden** - immer wenn ein Update verfügbar ist, werden Sie gefragt, ob dieses heruntergeladen werden soll.

26.2.4. Konfiguration der Erweiterten Einstellungen

Um sicherzustellen, dass Sie bei der Arbeit nicht vom BitDefender Update-Vorgang gestört werden, stehen in der Kategorie **Erweiterte Einstellungen** folgende Optionen zur Verfügung:

- **Auf Neustart warten, anstatt nachzufragen** - Ist für ein Update ein Neustart notwendig von BitDefender, arbeitet das System bis zum nächsten Neustart mit den alten Dateien weiter. Der Benutzer wird nicht um einen Neustart gebeten und somit nicht bei seiner Arbeit gestört.
- **Nicht aktualisieren, wenn ein Scan durchgeführt wird** - BitDefender wird kein Update durchführen, solange ein Scan läuft. Auf diese Weise beeinflusst der BitDefender Update-Vorgang nicht den Scan-Ablauf.

Beachten Sie

Sollte BitDefender während eines Scans aktualisiert werden, wird der Scan abgebrochen.

- **Nicht aktualisieren, wenn der Spiele-Modus aktiv ist** - wenn der Spiele-Modus aktiviert ist, wird BitDefender kein Update durchführen.Durch diese Option können Sie den Einfluss der Anwendung, auf die Geschwindigkeit während des Spielens minimieren.
- **Update-Sharing zulassen** - wenn Sie den Einfluss des Netzwerk-Datenverkehrs auf Ihre Systemleistung während der Durchführung von Updates minimieren möchten, aktivieren Sie die Option "Update-Sharing".
- **BitDefender-Dateien von diesem PC uploaden** - BitDefender ermöglicht das Teilen der neuesten Antiviren-Signaturen auf Ihrem PC mit anderen BitDefender-Benutzern.

Kurzanleitungen

27. Wie kann ich Dateien und Verzeichnisse scannen?

Scannen mit BitDefender ist einfach und flexibel.Es gibt mehrere Arten, wie das Scannen von Dateien und Verzeichnissen auf Viren und andere Malware durch BitDefender gehandhabt werden kann:

- Verwendung des Windows Kontextmenüs
- Verwendung von Scan-Aufgaben
- Nutzung der Scan-Aktivitätsleiste

Sobald Sie den Scan eingeleitet haben, wird der Antivirus Scan-Assistent eingeblendet und Sie durch den Prozess leiten.Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Scan Assistent“ (S. 70)*.

Beachten Sie

Um herauszufinden, wie Sie mit BitDefender im abgesicherten Modus von Windows scannen, siehe *„Wie scanne ich meinen Computer im abgesicherten Modus?“ (S. 200)*.

27.1. Verwendung des Windows Kontextmenüs

Dies ist der einfachste und empfohlene Weg, eine Datei oder Verzeichnis auf Ihrem Computer zu scannen.Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Mit BitDefender prüfen** aus dem Menü aus.Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.

Typische Situationen, in welchen Sie diese Scan-Methode verwenden sollten, sind:

- Sie verdächtigen eine bestimmte Datei oder Verzeichnis infiziert zu sein.
- Sie laden Internetdateien herunter und möchten überprüfen, ob diese einwandfrei sind.
- Sie möchten ein Verzeichnis scannen, bevor Sie Dateien dieses Verzeichnisses auf Ihren Rechner kopieren.

27.2. Verwendung von Scan-Aufgaben

Wenn Sie Ihren Computer oder bestimmte Verzeichnisse regelmässig scannen lassen möchten, sollten Sie in Betracht ziehen, hierfür eine Scan-Aufgabe zu definieren.Scan-Aufgaben weisen BitDefender an, wo zu scannen ist und welche Option und Aktionen zu tätigen sind. Außerdem können Sie diese Aufgaben planen und sie regelmäßig oder zu einer bestimmten Zeit laufen lassen.

Um Ihren Computer unter Verwendung von Scan-Aufgaben scannen zu lassen, öffnen Sie die BitDefender Benutzeroberfläche und starten dort die gewünschte Scan-Aufgabe.Abhängig von der Benutzeransicht sind verschiedene Schritte zurDurchführung einer Scan-Aufgabe nötig.

Starten von Scan-Aufgaben in der Basisansicht

In der Basis-Ansicht können Sie eine Reihe von vorkonfigurierten Scan-Aufgaben ausführen.Klicken Sie auf den Button **Sicherheit** und wählen Sie eine der verfügbaren Scan-Aufgaben.Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.

Ausführen einer Scan-Aufgabe in der Standard-Ansicht

In der Standard-Ansicht können Sie eine Reihe von vorkonfigurierten Scan-Aufgaben ausführen. Zudem können benutzerdefinierte Scan-Aufgaben konfiguriert und ausgeführt werden, um bestimmte Bereiche Ihres PCs zu scannen.Folgen Sie diesen Schritten, um in der Standard-Ansicht eine Scan-Aufgabe auszuführen:

1. Klicken Sie das Reiter **Sicherheit**.
2. Klicken Sie im Quick Task-Bereich links auf **Vollsystem-Scan** und wählen Sie die gewünschte Scan-Aufgabe.Um eine benutzerdefinierte Prüfung zu konfigurieren und zu starten, klicken Sie **Benutzerdefinierter Scan**.
3. Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.Falls Sie einen benutzerdefinierte Scan durchführen, muss zuvor der entsprechende Assistent abgeschlossen werden.

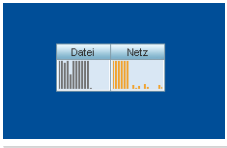
Ausführen der Scan-Aufgaben in der Experten-Ansicht

In der Experten-Ansicht können Sie alle vorkonfigurierten Scan-Aufgaben durchführen und deren Scan-Optionen ändern. Außerdem können Sie dort selbst Scan-Aufgaben erstellen, wenn Sie bestimmte Bereiche Ihres Computers scannen möchten.Folgen Sie diesen Schritten, um in der Experten-Ansicht eine Scan-Aufgabe auszuführen:

1. Klicken Sie imMenü auf der linken Seite auf **Antivirus**.
2. Klicken Sie auf den Reiter **Virenscan**.Hier finden Sie eine Reihe von vordefinierten Scan-Aufgaben und können hier Ihre eigenen Scan-Aufgaben erstellen.
3. Doppelklicken Sie auf die Scan-Aufgabe, die Sie ausführen möchten.
4. Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.

27.3. Nutzung der Scan-Aktivitätsleiste

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung des Scan-Vorgangs.Dieses kleine Fenster steht in der Voreinstellung nur in der Experten-Ansicht zur Verfügung.



Scan-Aktivitätsanzeige

Sie können die Aktivitätsanzeige verwenden, um schnell Dateien und Verzeichnisse zu scannen.Ziehen Sie (Drag & Drop) die gewünschte Datei oder Verzeichnis in die

Scan-Aktivitätsanzeige.Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.

Beachten Sie
Weitere Informationen finden Sie unter „*Scan-Aktivitätsanzeige*“ (S. 21).

28. Wie erstelle ich eine benutzerdefinierte Scan-Aufgabe?

Um eine neue Scan-Aufgabe zu definieren, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht

Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Benutzerdefinierter Scan**.

Ein Assistent wird eingeblendet, um Ihnen beim Erstellen der gewünschten Scan-Aufgabe zu helfen.Über die Buttons **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**
2. **Ziel wählen**

   Klicken Sie auf **Ziel hinzufügen**, um die zu scannenden Dateien oder Verzeichnisse auszuwählen.

   Klicken Sie auf **Erweiterte Einstellungen**.Im Reiter **Übersicht** können Sie die Scan-Optionen durch Verschieben des Reglers anpassen.Wenn Sie die Scan-Optionen konfigurieren möchten, klicken Sie auf **Benutzerdefiniert**.Gehen Sie auf den Reiter **Planer**, um zu wählen, wann die Aufgabe ausgeführt werden soll.
3. **Fertigstellen**

   Hier können Sie einen Aufgabennamen eingeben und optional den Scan dem Quick Task-Bereich hinzufügen.

   Klicken Sie auf **Scan starten**, um die Aufgabe zu erstellen und den Scan-Assistenten zu öffnen.

Experten-Ansicht

1. Gehen Sie zu **Antivirus > Virusen-Scan**.
2. Klicken Sie auf **Neue Aufgabe**, ein neues Fenster wird geöffnet.

Beachten Sie

Sie können auch per Mausdoppelklick auf eine vordefinierte Scan-Aufgabe wie **Vollsystem-Scan** klicken und dann **Aufgabe kopieren** wählen.Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die Aufgabe, die Sie dupliziert haben, geändert werden können.

3. Geben Sie im Reiter **Übersicht** den Aufgabennamen ein und passen Sie die Scan-Optionen an, indem Sie den Cursor des Schiebers entsprechend verschieben.

   Wenn Sie die Scan-Optionen konfigurieren möchten, klicken Sie auf **Benutzerdefiniert**.

4. Gehen Sie auf den Reiter **Pfade**, um das Scan-Ziel auszuwählen. Klicken Sie auf **Eintrag(e) hinzufügen**, um die zu scannenden Dateien oder Verzeichnisse auszuwählen.

5. Gehen Sie auf den Reiter **Planer**, um zu wählen, wann die Aufgabe ausgeführt werden soll.

6. Klicken Sie auf **OK**, um die Aufgabe zu speichern.Die neue Aufgabe erscheint unter den benutzerdefinierten Aufgaben und kann jederzeit aus diesem Fenster heraus bearbeitet, entfernt oder gestartet werden.

29. Wie plane ich einen Scan?

Ihren Computer regelmässig scannen zu lassen, ist die beste Art ihn frei von Maleware zu halten.BitDefender bietet Ihnen die Möglichkeit, Scan-Aufgaben einzuplanen, so dass Sie Ihren Computer automatisch scannen lassen können.

Um BitDefender eine geplante Scan-Aufgabe durchführen zu lassen folgen Sie den Schritten:

1. Öffnen Sie BitDefender.
2. Gehen Sie, abhängig von der gewählten Ansicht, wie folgt vor:

   Standard-Ansicht
   Klicken Sie auf den Reiter **Sicherheit** und dann im Quick Task-Bereich auf der linken Bildschirmseite auf **Antivirus konfigurieren**.

   Experten-Ansicht
   Klicken Sie imMenü auf der linken Seite auf **Antivirus**.
3. Klicken Sie auf den Reiter **Virenscan**.Hier finden Sie eine Reihe von vordefinierten Scan-Aufgaben und können hier Ihre eigenen Scan-Aufgaben erstellen.

   - Systemaufgaben sind verfügbar und können unter jedem Windows Benutzerkonto gestartet werden.
   - Benutzeraufgaben sind ausschliesslich für den Benutzer verfügbar der sie erstellt hat und können auch nur von diesem gestartet werden.

   Dies sind die vordefinierten Scan-Aufgaben, die Sie terminlich planen können:

   Vollsystem-Scan
   Scannt alle Dateien mit Ausnahme von Archiven.In der Standardkonfiguration, wird nach allen Arten von Malware mit Ausnahme von Rootkits gescannt.

   Quick Scan
   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 Virenscan in Anspruch nehmen würde.

   Auto-logon Scan
   Scannt die Einträge, die ausgeführt werden, wenn ein Benutzer sich in Windows anmeldet.Um diese Aufgabe zu nutzen, muss definiert werden, dass Sie beimSystemstart ausgeführt wird.In der Voreinstellung ist der Auto-logon Scan deaktiviert.

   Tiefensystem-Scan
   Scannt das komplette System.In der Voreinstellung wird auf alle Arten von Bedrohungen gescannt, wie z.B. Viren, Spyware, Adware, Rootkits etc.

Meine Dokumente

Verwenden Sie diese Aufgaben, um die folgenden für den jeweiligen Benutzer Verzeichnisse zu scannen: `Eigene Dateien`, `Desktop` und `Autostart`. Dadurch wird die sichergestellt, dass Ihre eigenen Daten, ein sicherer Arbeitsplatz sowie eine saubere Ausführung der Anwendungen beim Systemstart gewährleistet.

Falls keine der Scan-Aufgaben Ihren Bedürfnissen entspricht können Sie eine neue Scan-Aufgabe erstellen, die Sie dann nach Bedarf terminlich einplanen können.

4. Rechtsklicken Sie auf die gewünschte Scan-Aufgabe und wählen Sie **Planer**.Ein neues Fenster wird geöffnet.
5. Planen Sie die Aufgabe nach Bedarf:
   - Um die Aufgabe einmalig durchzuführen, wählen Sie **Einmalig** und bestimmen Sie das Startdatum und die Zeit.
   - Um die Scan-Aufgabe nach dem Systemstart durchzuführen, wählen Sie **Beim Systemstart**.Sie können festlegen, wie lange nach dem Systemstart die Aufgabe gestartet werden soll (in Minuten).
   - Um die Aufgabe regelmäßig durchzuführen wählen Sie **Periodisch** und bestimmen Sie die Häufigkeit, das Startdatum und die Zeit.

   Beachten Sie

   Um beispielsweise Ihren Computer jeden Samstag um 2:00Uhr scannen zu lassen, gehen Sie folgendermaßen vor:

   a. Wählen Sie **Periodisch**.

   b. Im **Täglich** Feld, geben Sie 1 ein und wählen dann**Wochen** im Menü.Auf diese Art wird die Aufgabe einmal wöchentlich durchgeführt.

   c. Legen Sie als Startdatum den kommenden Samstag fest.

   d. Legen Sie als Startzeit `2:00:00 Uhr`fest.

6. Klicken Sie **OK** um die Planung zu speichern.Die Scan-Aufgabe wird automatisch, gemäß der definierten Planung, durchgeführt.Falls der Computer im Moment der geplanten Aufgabe abgeschaltet ist, wird die Aufgabe beim nächsten Computerstart gestartet.

30. Wie erstelle ich ein Windows Benutzerkonto?

Ein Windows-Benutzerkonto ist ein eindeutiges Profil, zu dem alle Einstellungen, Zugriffsrechte und persönlichen Dateien des entsprechenden Benutzers gehören.

Windows-Benutzerkonten lassen den Heim PC-Administrator den Zugriff für jeden Benutzer kontrollieren.

Das Anlegen von Benutzerkonten ist dann sinnvoll, wenn sowohl Erwachsene als auch Kinder den PC benutzen - ein Elternteil kann für jedes Kind ein separates Benutzerkonto anlegen.

Wählen Sie Ihr Betriebssystem, um so herauszufinden, wie Sie Windows Benutzerkonten erstellen können.

- Windows XP:
  1. Loggen Sie sich in Ihren Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".
  3. Klicken Sie auf "Neues Benutzerkonto erstellen".
  4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
  5. Für diesen Benutzerkontentyp wählen Sie "Begrenzt" und dann "Benutzerkonto anlegen". Begrenzte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Anwendungen nicht installiert werden können.
  6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.
- Windows Vista oder Windows 7:
  1. Loggen Sie sich in Ihren Computer als Administrator ein.
  2. Klicken Sie auf "Start", klicken Sie auf "Systemsteuerung" und dann auf "Benutzerkonten".
  3. Klicken Sie auf "Neues Benutzerkonto erstellen".
  4. Geben Sie den Namen des Benutzers ein. Sie können den vollständigen Namen der Person, den Vornamen oder einen Spitznamen verwenden. Klicken Sie dann auf "Weiter".
  5. Für diesen Benutzerkontentyp klicken Sie auf "Standard" und dann auf "Benutzerkonto anlegen". Beschränkte Benutzerkonten sind vor allem für Kinder geeignet, da keine systemübergreifenden Änderungen vorgenommen oder bestimmte Anwendungen nicht installiert werden können.

6. Ihr neues Benutzerkonto wird erstellt und dieses wird im Bildschirm "Benutzerkonten verwalten" aufgelistet.

Beachten Sie

Nun, da Sie neue Benutzerkonten hinzugefügt haben, können Sie für diese Passwörter vergeben.

31. Wie kann ich BitDefender über einen Proxy-Server aktualisieren?

Normalerweise findet und importiert BitDefender automatisch die Proxy-Einstellungen Ihres Systems.Wenn Ihre Internetverbindung über einen Proxy Server hergestellt wird, müssen Sie eventuell die Proxy-Einstellungen finden und BitDefender dementsprechend konfigurieren.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wo finde ich "Meine Proxy-Einstellungen"?“* (S. 214).

Nachdem Sie die Proxy-Einstellungen gefunden haben, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Allgemein> Einstellungen**.
3. Klicken Sie in den **Verbindungseinstellungen** auf **Proxy-Einstellungen**.
4. Geben Sie im entsprechenden Feld die Proxy-Einstellungen ein.
5. Klicken Sie auf **OK**.

Beachten Sie

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

32. Wie führe ein Upgrade zu einem anderen BitDefender 2011 Produkt durch?

Mit BitDefender 2011 können Sie einfach von einem BitDefender 2011 zu einem anderen upgraden.

Stellen wir uns einmal folgendes Szenario vor: Sie nutzen BitDefender Internet Security 2011 2011 bereits seit einiger Zeit und haben sich kürzlich entschieden, BitDefender Total Security 2011 mit dessen Extrafunktionen zu kaufen.

Sie müssen nur einen Lizenzschlüssel für das BitDefender 2011-Produkt, das Sie upgraden möchten, kaufen und diesen im Registrierungsfenster des BitDefender 2011-Produkts, das Sie gerade verwenden, eingeben.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender.
2. Klicken Sie im unteren Bildschirmbereich auf den Link **Lizenzinfo**.Das Registrierungsfenster wird eingeblendet.
3. Geben Sie den Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.
4. BitDefender informiert Sie, dass der Lizenzschlüssel für eine anderes Produkt bestimmt ist und bietet Ihnen die Option, dieses zu installieren.Klicken Sie auf den entsprechenden Link und folgen Sie der dreistufigen Anleitung, um das Upgrade durchzuführen.

   a. **Aktion bestätigen**

   b. **Upgrade wird durchgeführt**

      Warten Sie, bis BitDefender den Upgrade-Vorgang abgeschlossen hat.Dies kann einige Minuten in Anspruch nehmen.

   c. **Upgrade abgeschlossen**

      Der Vorgang ist abgeschlossen. Es kann ein Neustart nötig sein.

Fehlersuche und Hilfe

33. Problemlösung

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 „*Support*“ (S. 205) beschrieben, kontaktieren.

33.1. Installationsprobleme

Dieses Kapitel hilft Ihnen, die häufigsten Installationsprobleme von BitDefender zu beheben.Diese Probleme können in die folgenden Kategorien gruppiert werden:

- Installationsgültigkeitsstörungen: der Setup-Assistent kann wegen bestimmter Bedingungen auf Ihrem System nicht ausgeführt werden.
- Installation fehlgeschlagen: Sie haben eine Installation über den Setup-Assistenten gestartet, diese wurde aber nicht erfolgreich abgeschlossen.

33.1.1. Installationsbestätigungs-Fehler

Beim Start des Setup-Assistenten werden eine Anzahl von Bedingungen überprüft um zu gewährleisten, dass die Installation starten kann.Die folgende Tabelle zeigt Ihnen die häufigsten Problemquellen während der Installation und mögliche Vorschläge um diese zu beheben.

Fehler	Beschreibung&Lösung
Sie haben nicht genügende Rechte um das Programm zu installieren.	Um den Setup-Assistenten zu starten und BitDefender zu installieren, benötigen Sie Administratorrechte.Wählen Sie eine der folgenden Methoden: ● Loggen Sie sich in ein Windows-Administratorkonto ein und starten Sie den Setup-Assistenten erneut. ● Klicken Sie mit der rechten Maustaste auf die Installationsdatei und wählen Sie **Ausführen als...**.Geben Sie den Benutzernamen und Passwort des Windows Administratorkontos ein.
Der Installer hat eine ältere BitDefender Version entdeckt, die nicht richtig deinstalliert wurde.	BitDefender war vorher auf Ihrem System installiert, aber die Installation wurde nicht vollständig entfernt. Diese blockiert eine neue Installation von BitDefender.

Fehler	Beschreibung&Lösung
	Um diese Problem zu beheben und BitDefender zu installieren, gehen Sie folgendermaßen vor: 1. Gehen Sie auf www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner. 2. Starten Sie das Uninstall Tool unter Verwendung eines Kontos mit Administratorrechten. 3. Starten Sie Ihren Computer neu. 4. Starten Sie den Setup-Assistenten enreut, um BitDefender nun zu installieren.
Bitdefender ist mit Ihren Betriebsystem nicht kompatibel.	Sie versuchen BitDefender auf einen nicht unterstützten Betriebssystem zu installieren.Überprüfen Sie bitte die *„Systemanforderungen“* (S. 2) um herauszufinden auf welchen Betriebssystemen Sie BitDefender installieren können. Sollte Ihr Betriebssystem Windows XP mit Service Pack 1 oder niedriger sein, können Sie das Service Pack 2 oder einen höheren installieren und den Setup-Assistenten erneut ausführen.
Die Installationsdatei wurde für eine andere Art von Prozessoren entwickelt.	Wenn Sie eine solche Fehlermeldung erhalten, bedeutet dies, dass Sie eine falsche Version der Installationsdatei ausführen.Es gibt zwei Versionen der BitDefender-Installationsdatei: eine für 32-bit-Prozessoren und eine andere für 64-bit-Prozessoren. Um sicherzugehen, dass Sie die richtige Version für Ihr System erhalten, downloaden Sie die Installationsdatei Bitte direkt unter:www.bitdefender.com.

33.1.2. Installation fehlgeschlagen

Es gibt mehrere Ursachen, wieso eine Installation fehlschlägt:

- Während der Installation wird ein Fehlerbildschirm eingeblendet.Sie werden möglicherweise gebeten, die Installation abzubrechen oder der Button "Deinstallation" wird eingeblendet. Durch eine Deinstallation werden mögliche Reste einer früheren Installation entfernt.

Beachten Sie

Sofort nach dem Start der Installation von BitDefender erhalten Sie möglicherweise eine Benachrichtigung, dass nicht genügend freier Speicherplatz auf Ihrer Festplatte zur Verfügung steht. In diesem Fall müssen Sie den benötigten Platz auf der Zielpartition frei machen und danach die Installation von BitDefender fortsetzen oder neu starten.

- Die Installation hängt und möglicherweise stürzt Ihr System ab.Nur ein Neustart stellt das Systemsreaktionsvermögen wieder her.
- Installation wurde abgeschlossen, aber Sie können einige oder alle BitDefender Funktionen nicht verwenden.

Um eine Fehlinstallation zu überprüfen und BitDefender zu installieren, folgen Sie diesen Schritten:

1. **Reinigen Sie das System nach der fehlerhaften Installation.** Falls die Installation fehlschlägt, bleiben einige BitDefender Registry-Schlüssel und Dateien in Ihrem System. Solche Rückstände können eine erneute Installation verhindern von BitDefender. Ebenso kann die Systemleistung und Stabilität darunter leiden. Aus diesem Grund müssen diese vor einer erneuten Produktinstallation entfernt werden.

   Sollte dies der Fall sein, ist die einfachste Lösung, BitDefender komplett vom System zu entfernen und wieder neu zu installieren.Weitere Informationen finden Sie unter *„Wie entferne ich BitDefender vollständig?“* (S. 214).

2. **Überprüfen Sie mögliche Ursachen, warum die Installation fehlschlug.** Bevor Sie mit der Neuinstallation fortfahren, überprüfen und beheben Sie mögliche Ursachen, die die fehlerhafte Installation verursacht haben könnte:

   a. Überprüfen Sie, ob Sie ein anderes Sicherheitsprogramm installiert haben, da diese den Normalbetrieb von BitDefender stören könnte. Sollte dies der Fall sein, empfehlen wir Ihnen alle anderen Sicherheitsprogramme zu entfernen und BitDefender wieder neu zu installieren.

   b. Überprüfen Sie auch ob Ihr System infiziert ist.Wählen Sie eine der folgenden Methoden:

      - Benutzen Sie die BitDefender Notfall CD, um Ihren Computer zu scannen und alle vorhandenen Bedrohungen zu entfernen.Weitere Informationen finden Sie unter *„BitDefender Rescue-CD“* (S. 196).
      - Öffnen Sie den Internet Explorer, gehen Sie auf www.bitdefender.com, und führen Sie einen Online-Scan durch (klicken Sie auf **Online scannen**).

3. Versuchen Sie erneut BitDefender zu installieren.Es wird empfohlen dass Sie die aktuellste Version der Installationsdatei von www.bitdefender.com herunterladen und ausführen.

4. Wenn die Installation wieder fehlschlägt, nehmen Sie bitte Kontakt zum BitDefender-Support auf, siehe in *„Support“ (S. 205)*.

33.2. Mein System scheint zu langsam 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 Sicherheitssoftware.**

  Obwohl BitDefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jedes andere Antivirenprogramm von Ihrem Rechner zu entfernen, bevor Sie die Installation von BitDefender starten.Weitere Informationen finden Sie unter *„Wie entferne ich andere Sicherheitsprogramme?“ (S. 212)*.

- **Die Mindestsystemanforderungen für das Ausführen von BitDefender sind nicht vorhanden.**

  Wenn Ihr PC nicht über die Mindestsystemanforderungen verfügt, verlangsamt dies Ihr System, besonders dann, wenn mehrere Anwendungen gleichzeitig laufen.Weitere Informationen finden Sie unter *„Mindestsystemanforderungen“ (S. 2)*.

- **Ihre Festplatte ist zu fragmentiert.**

  Eine Datei-Fragmentierung verzögert den Zugriff auf Dateien und verschlechtert die Systemleistung.

  Um Ihre Festplatte mithilfe Ihres Windows Betriebssystems zu defragmentieren, folgen Sie dem Pfad im Windows Startmenü:**Start → Alle Programme → Zubehör → Systemprogramme → Defragmentierung**.

33.3. 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**.

  Sollte dies der Fall sein, ist die einfachste Lösung, BitDefender komplett vom System zu entfernen und wieder neu zu installieren.Weitere Informationen finden Sie unter *„Wie entferne ich BitDefender vollständig?“ (S. 214)*.

- **BitDefender ist nicht die einzige auf Ihrem System installierte Sicherheitssoftware**.

Befolgen Sie dafür die folgenden Schritte:

1. Entfernen Sie die anderen Sicherheitslösungen entfernen.Weitere Informationen finden Sie unter *„Wie entferne ich andere Sicherheitsprogramme?“ (S. 212).
2. Löschen Sie BitDefender vollständig vom System.
3. Installieren Sie BitDefender neu.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

33.4. Ich kann eine Anwendung nicht länger benutzen

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

Es 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 das Active Virus Control-Modul versehentlich eine Anwendung als Malware einstuft.

Active Virus Control ist ein BitDefender-Modul, das ständig die laufenden Programme Ihres Systems überwacht und einen Bericht über jene sendet, die sich potentiell gefährlich verhalten.Da diese Funktion auf dem heuristischen System basiert, kann es Fälle geben, in denen einwandfreie Anwendungen im Bericht der Active Virus Control aufgelistet werden.

Wenn diese Situation eintritt, können Sie die entsprechende Anwendung von der Überwachung durch Active Virus Control ausschließen.

Wenn Sie das Programm der Ausschlussliste hinzufügen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus > Schild**.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Gehen Sie im neuen Fenster auf den Reiter **Ausschlüsse**, klicken Sie auf den Button **Hinzufügen** und suchen Sie die .exe-Datei des Programms (normalerweise unter `C:\Programmdateien`).
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

6. Schließen Sie das BitDefender-Fenster und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt „*Support*“ (S. 205) beschrieben.

33.5. Ich kann keine Verbindung zum Internet herstellen.

Nach einer Installation von BitDefender werden Sie unter Umständen bemerken, dass ein Programm keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche ins Internet zu gehen, dies funktioniert aber nicht**.

2. **Problem identifizieren**

   Klicken Sie auf **Anwendung wählen** und **Blättern**, um die .exe-Datei der Anwendung zu finden (normalerweise finden Sie diese unter `C:\Programmdateien`, z.B. Firefox.exe).Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt „*Support*“ (S. 205) beschrieben.

33.6. Ich kann den Drucker nicht benutzen

Abhängig vom angeschlossenen Netzwerk könnte die BitDefender-Firewall die Verbindung zwischen Ihrem Computer und einen Netzwerkdrucker blockieren.

In diesem Fall ist die beste Lösung, BitDefender so zu konfigurieren, dass eine Verbindung von und zum entsprechenden Drucker automatisch zugelassen wird.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche etwas auszudrucken, dies ist aber nicht möglich**.

2. **Problem identifizieren**

   Klicken Sie auf **Drucker wählen**.Wählen Sie den Drucker aus der Liste aus (entweder Druckername oder IP-Adresse).Wenn Sie das Gerät in der Liste nicht finden können, geben Sie die IP-Adresse manuell im Bearbeiten-Feld ein.Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Falls der Fehlersuche-Assistent anzeigt, dass das Problem nicht von der BitDefender-Firewall auf Ihrem Computer verursacht wird, überprüfen Sie andere potentielle Ursachen, wie beispielsweise:

- Die Firewall auf dem anderen Computer könnte die Nutzung des gemeinsamen Druckers oder der Datei blockieren.
  - Wenn die Windows Firewall benutzt wird, kann diese so konfiguriert werden dass der Zugriff auf Drucker oder Datenaustausch zugelassen wird: Öffnen Sie das Windows Firewall-Einstellungsfenster, wählen Sie unter **Ausnahmen** die Option **Datei- und Druckeraustausch**.
  - Wenn eine andere Firewall verwendet wird, schlagen Sie bitte in den entsprechenden Unterlagen oder Hilfsdateien nach.
- Allgemeine Bedingungen, die die Nutzung von oder Verbindung zu einemfreigegebenen Drucker verhindern können:

- Möglicherweise müssen Sie sich mit einem Windows-Adminstratorkonto anmelden, um auf die Druckerfreigabe zugreifen zu können.
- Rechte werden für gemeinsam genutzte Drucker festgelegt, so dass nur der Zugriff auf spezifische Computer und Benutzer erlaubt wird.Falls Sie Ihren Drucker freigegeben haben, überprüfen Sie die Rechte, die für den Drucker gesetzt sind, um zu sehen, ob der Benutzer auf dem anderen Computer, den Zugang zum Drucker erlaubt.Wenn Sie versuchen eine Verbindung zum freigegebenen Drucker aufzubauen, sollten Sie den Benutzer auf dem anderen Computer überprüfen, ob dieser über die nötigen Rechte verfügt.
- Der Drucker, der mit Ihrem oder einem anderen Computer verbunden ist, ist nicht freigegeben.
- Der freigegebene Drucker wurde dem Computer nicht hinzugefügt.

Beachten Sie
Um mehr darüber zu erfahren, wie Sie Druckerfreigaben (Druckertausch, Festlegen oder Entfernen von Druckerechten, Verbindung zu einem Netzwerkdrucker oder einen gemeinsam genutzten Drucker) verwalten können, öffnen Sie im Windows-Startmenü den Bereich **Hilfe und Support**).

- Der Zugriff auf einen Netzwerk-Drucker könnte auf bestimmte Computer oder Nutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

33.7. Ich kann keine Dateien mit anderen Computern teilen

Abhängig vom angeschlossenen Netzwerk könnte die BitDefender-Firewall die Verbindung zwischen Ihrem Computer und einem anderen Netzwerkcomputer blockieren.Als Ergebnis können Sie nicht mehr länger Dateien mit anderen Computern teilen.In diesem Fall ist die beste Lösung, BitDefender so zu konfigurieren, dass eine Verbindung von und zum entsprechenden System automatisch zugelassen wird.

Der Fehlersuche-Assistent hilft Ihnen, die Verbindungsprobleme zu identifizieren und zu lösen.Um den Assistenten zu starten, öffnen Sie BitDefender und gehen Sie, abhängig von der gewählten Ansicht, folgendermaßen vor:

Standard-Ansicht
: Gehen Sie zum Reiter **Sicherheit** und klicken Sie im Quick Task-Bereich auf der linken Bildschirmseite auf **Firewall konfigurieren**.Wählen Sie im neuen Fenster den Reiter **Einstellungen** und klicken Sie auf **Fehlersuche**.

Experten-Ansicht
: Gehen Sie auf **Firewall > Einstellungen** und klicken Sie auf **Fehlersuche**.

Folgen Sie der dreiteiligen Anleitung, um die Fehlersuche zu starten.Über den Button **Weiter** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Willkommen**

   Wählen Sie **Ich versuche auf einen Computer meines Netzwerks zuzugreifen, dies funktioniert aber nicht**.

2. **Problem identifizieren**

   Klicken Sie auf **Computer wählen**.Wählen Sie den Computer aus der Liste aus (entweder Computername oder IP-Adresse).Wenn Sie den Computer nicht in der Liste finden können, geben Sie die IP-Adresse manuell im Bearbeiten-Feld ein.Klicken Sie auf **Hinzufügen**.

3. **Empfohlene Problemlösung**

   Wählen Sie **Ja, Zugriff zulassen**.Klicken Sie auf **Beenden** und überprüfen Sie, ob das Problem weiterhin auftritt.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

33.8. Meine Internetverbindung ist langsam

Diese Situation könnte nach der Installation von BitDefender eintreten.Das Problem könnte aufgrund von Konfigurationsfehlern der BitDefender-Firewall auftreten.

Zur Behebung dieses Problems gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Firewall > Einstellungen**.
3. Deaktivieren Sie das Häkchen der Option **Firewall ist aktiviert**, um diese vorübergehend auszuschalten.
4. Überprüfen Sie, ob Sie nun eine Internetverbindung herstellen können, wenn die BitDefender-Firewall deaktiviert ist.
   - Wenn Sie weiterhin keine Internetverbindung herstellen können, wird das Problem wahrscheinlich nicht von BitDefender verursacht. Sie sollten Ihren Internet Service Provider kontaktieren, um abzuklären, dass es keine Verbindungsprobleme gibt.

     Wenn Sie von Ihrem Internet Service Provider die Bestätigung erhalten, dass es von Provider-Seite keine Probleme gibt und das Problem besteht weiterhin, kontaktieren Sie BitDefender wie im Abschnitt *„Support“ (S. 205)* beschrieben.
   - Falls Sie nach der Deaktivierung der BitDefender-Firewall eine Internetverbindung herstellen können, gehen Sie folgendermaßen vor:

a. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.

b. Gehen Sie zu **Firewall > Einstellungen** und setzen Sie ein Häkchen, um die Firewall zu aktivieren.

c. Klicken Sie auf **Erweiterte Einstellungen**, wählen Sie **Internetverbindungs-Sharing aktivieren** und deaktivieren Sie **Port Scans blockieren**.

d. Gehen Sie im Hauptfenster auf den Reiter **Netzwerk** .

e. Blättern Sie im Drop-Down-Menü der Spalte **Netzwerktyp** nach unten und wählen Sie **Zuhause/ Büro**.

f. Gehen Sie in die Spalte **Allgemein** und wählen Sie dort **Ja** vor. Setzen Sie den **Stealth-Modus** auf **Remote**.

g. Überprüfen Sie, ob Sie eine Verbindung zum Internet herstellen können.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

33.9. Wie Sie ein BitDefender-Update mit einer langsamen Internetverbindung durchführen.

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

Um Ihr System hinsichtlich BitDefender Malware-Signaturen auf dem neuesten Stand zu halten, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Update > Einstellungen**.
3. Unter **Manuelle Update-Einstellungen** wählen Sie **Vor dem Download von Updates nachfragen**.
4. Klicken Sie auf **Anwenden** und gehen Sie zum Reiter **Update**.
5. Klicken Sie auf **Jetzt updaten**, es wird ein neues Fenster eingeblendet.
6. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
7. BitDefender wird nur die Malware-Signatur-Updates downloaden und installieren.

33.10. Ich verfüge über keinen Internetzugang. Wie führe ich ein Update von BitDefender durch?

Wenn Ihr Computer über keine Internetverbindung verfügt, müssen Sie die Updates manuell auf einen Computer mit Internetzugang downloaden und dann über einen

Wechseldatenträger wie beispielsweise einen USB Speicherstick auf Ihren Rechner transferieren.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie auf einem Computer mit Internetzugang einen Webbrowser und gehenSie auf:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. Klicken Sie in der Spalte **Manuelles Update** auf den entsprechenden Link für Ihr Produkt und Ihre Systemarchitektur.Wenn Sie nicht wissen, ob Ihr Windows im 32- oder 64 bit-Betrieb läuft, lesen Sie bitte *„Ist auf meinem System die 32- oder 64-bit-Version von Windows installiert?“ (S. 213)*.

3. Speichern Sie die Datei namens `weekly.exe` im System.

4. Übertragen Sie die Download-Datei auf einen Wechseldatenträger wie beispielsweise einen USB Speicherstick und gehen Sie dann zu Ihrem Computer.

5. Doppelklicken Sie auf die Datei und folgen Sie der Anleitung des Assistenten.

33.11. BitDefender-Dienste antworten nicht.

Dieser Artikel hilft Ihnen bei der Lösung des Problems *BitDefender Dienste antworten nicht*.Diese Fehlermeldung kann folgendermaßen auftauchen:

- Das BitDefender-Symbol in System Tray ist ausgegraut und ein Pop-up informiert Sie, dass die BitDefender-Dienste nicht antworten.
- Das BitDefender-Fenster zeigt an, dass die BitDefender-Dienste nicht antworten.

Der Fehler kann durch einen der folgenden Bedingungen verursacht werden:

- Ein wichtiges Update wird installiert.
- Temporäre Kommunikationsstörungen zwischen den BitDefender-Diensten.
- Einige der BitDefender-Dienste wurden angehalten.
- Andere Sicherheitslösungen laufen gleichzeitig mit BitDefender auf Ihrem Rechner.
- Viren auf Ihrem System beeinflussen den Normalbetrieb von BitDefender.

Um diese Probleme zu beheben, versuchen Sie diese Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert.Die Störung könnte vorübergehend sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis BitDefender geladen ist. Öffnen Sie BitDefender und überprüffen Sie ob das Problem weiterhin besteht.Das Neustarten des Rechners behebt normalerweise das Problem.
3. Überprüfen Sie, ob Sie ein anderes Sicherheitsprogramm installiert haben, da diese den Normalbetrieb von BitDefender stören könnte. Sollte dies der Fall sein,

empfehlen wir Ihnen alle anderen Sicherheitsprogramme zu entfernen und BitDefender wieder neu zu installieren.

4. Besteht das Problem auch weiterhin, kann es sich um ein ernsteres Problem handeln (z.B. könnte der Rechner mit einem Virus infiziert sein, wodurch BitDefender behindert wird).Bitte kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

33.12. Antispam-Filter funktioniert nicht richtig

Dieser Artikel hilft Ihnen, folgende Probleme mit dem BitDefender Antispam-Filter lösen:

- Eine Anzahl von seriösen Emails werden als [spam] markiert.
- Viele Spam-Mails werden nicht als solche markiert.
- Der Antispam-Filter entdeckt keinerlei Spamnachrichten.

33.12.1. Legitimierte Nachrichten werden als [spam] markiert

Seriöse Nachrichten werden als [spam] markiert, einfach deshalb weil sie für den BitDefender Antispam-Filter wie solche aussehen.Im Normalfall können Sie dieses Problem lösen, indem Sie den Antispam-Filter entsprechend konfigurieren.

BitDefender fügt die Empfänger Ihrer Mails automatisch der Freundeliste hinzu.Die erhaltenen Emails von in der Freundeliste geführten Kontakten werden als seriös angesehen. Sie werden nicht vom Antispam-Filter gescannt und deshalb auch nicht als [spam] markiert.

Die automatische Konfiguration der Freundeliste verhindert nicht das Auftreten folgender Störungen:

- Sie empfangen viele angeforderte Werbe-Emails, weil Sie sich auf auf verschiedenen Webseiten angemeldet haben.In diesem Fall sollten Sie die Email-Adressen, von denen Sie solche Emails bekommen, auf die Freundeliste setzen.
- Ein erheblicher Teil Ihrer legitimierten Email stammt von Menschen, die bisher keine Emails von Ihnen erhalten haben, z. B. Kunden, potentielle Geschäftspartner und andere.Für diese Fälle sind andere Lösungen erforderlich.

Wenn Sie einen Email Client benutzen, in den sich BitDefender integriert, versuchen Sie folgendes:

1. Erkennungsfehler anzeigen. Dadurch wird der Bayesianische Filter trainiert, dies hilft zukünftig Erkennungsfehler zu vermeiden.Der Bayesianische Filter analysiert die Nachrichten und lernt deren Muster.Die nächsten Emails mit dem identischen Muster werden nicht als [spam] markiert.

2. Antispam-Sicherheitsstufe herabsetzen. Indem die Sicherheitsstufe herabgesetzt wird, benötigt der Antispam-Filter mehr Indikatoren, um eine Email als Spam einzustufen.Versuchen Sie diese Lösung nur, wenn legitimierte Nachrichten(inklusive kommerzielle Nachrichten) fälschlicherweise als Spam erkannt werden.
3. Trainieren Sie die lernfähige Engine (des Bayesianischen Filters) erneut. Versuchen Sie diese Lösung nur, wenn vorangegangene Lösungsansätze keinen Erfolg gebracht haben.

Beachten Sie

BitDefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Eine Komplettliste der unterstützten Email Clients finden Sie unter: *„Software-Anforderungen“* (S. 2).

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesianischen Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz herabzusetzen.

Kontakte zur Freundeliste hinzufügen

Wenn Sie einen unterstützten Email Client verwenden, können Sie den Absernder ganz leicht zu der Freundeliste hinzufügen.Gehen Sie folgendermaßen vor:

1. Wählen Sie in Ihrem Mail Client eine Mail des Absenders, den Sie der Freundeliste hinzufügen möchten.
2. Klicken Sie in der BitDefender Antispam-Systemleiste auf den Button **Freund hinzufügen**, um den Adressaten Ihrer Freundeliste hinzuzufügen.
3. Unter Umständen müssen Sie dies noch einmal bestätigen.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie auf **OK**.

Sie werden jetzt alle Emails dieses Absenders unabhängig von deren Inhalten empfangen.

Falls Sie einen anderen Mail Client verwenden, können Sie von der BitDefender-Oberfläche aus Kontakte der Freundeliste hinzufügen.Gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie im Menü auf der linken Seite auf **Antispam**.
3. Klicken Sie auf den Reiter **Status**.
4. Klicken Sie auf **Freunde verwalten**.Ein Konfigurationsfenster wird geöffnet.
5. Geben Sie die Email-Adresse ein, von der Sie Email-Nachrichten erhalten wollen und klicken Sie auf den Button , um die Adresse der Freundeliste hinzuzufügen.

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

Erfassungsfehler anzeigen

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach den Antispam-Filter einfach korrigieren (indem Sie angeben, welche Emails nicht als [spam] markiert werden sollen). Dadurch wird die Effektivität des Antispam-Filters erheblich verbessert.Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie in das Junk Mail-Verzeichnis, in das die Spam-Nachrichten verschoben werden.
3. Wählen Sie die Nachricht, die von BitDefender fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf **Freund hinzufügen** in der BitDefender Antispam Toolbar.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt alle Emails dieses Absenders unabhängig von deren Inhalten empfangen.
5. Klicken Sie in der BitDefender Antispam-Symbolleiste (normalerweiseim oberen Teil des Mail Client-Fensters) auf **Kein Spam**. Dies teilt dem Bayes-Filter, dass die ausgewählte Nachricht kein Spam ist. Die Nachricht wird dann in den Posteingang verschoben.Die nächsten Emails, die dem gleichen Muster entsprechen, werden nicht als [spam] markiert.

Antispam-Sicherheitsstufe herabsetzen

Um die Antispam-Sicherheitsstufe herabzusetzen, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie im Menü auf der linken Seite auf **Antispam**.
3. Klicken Sie auf den Reiter **Status**.
4. Verschieben Sie den Schieber auf der Skala nach unten.

Es wird empfohlen, den Schutz nur um eine Stufe herabzusetzen und nach einer ausreichenden Zeit die Resultate einzuschätzen.Wenn weiterhin legitime Email als [spam] markiert werden, können sie den Schutzgrad weiter herabstufen. Stellen Sie fest, dass viele Nachrichten nicht als Spam erkannt werden, sollten Sie den Schutzgrad nicht herabsetzen.

Erneutes Trainieren des Bayesianischen Filters

Bevor Sie den Bayes Filter trainieren, legen Sie ein Verzeichnis an, in dem ausschließlich Nachrichten enthalten sind sowie ein zweites Verzeichnis, das nur SPAM enthält.Der Bayes Filter wird trainiert, indem er die Verzeichnisse analysiert und lernt die Charakteristiken von Spams und legitimierten Nachrichten zu

unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen mindestens 50 Nachrichten in jedem Verzeichnis vorhanden sein.

Um die Bayes Datenbank zurückzusetzen und sie neu zu trainieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der BitDefender Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispam-Filterdatenbank leeren** und klicken Sie auf **Weiter**.
6. Wählen Sie das Verzeichnis mit legitimierten Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie das Verzeichnis mit den SPAM-Nachrichten und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertigstellen** um den Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie auf **Schließen**.

Hilfestellung

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

33.12.2. Viele Spam-Nachrichten werden nicht entdeckt.

Wenn Sie viele Nachrichten erhalten, die nicht als `[spam]` markiert sind, konfigurieren Sie den BitDefender Antispam-Filter, um seine Effektivität zu erhöhen.

Wenn Sie einen Email Client benutzen, in den sich BitDefender integriert, versuchen Sie folgende Schritte (einzeln):

1. Unentdeckte Spam-Nachrichten anzeigen. Dadurch wird der Bayesianische Filter trainiert (Teil des Antispam-Filters) trainiert und die Antispam-Erkennungsrate erhöht.Der Bayesianische Filter analysiert die Nachrichten und lernt deren Muster.Die nächsten Email-Nachrichten, mit demselben Muster werden automatisch als `[spam]` markiert.
2. Spammer der Spammerliste hinzufügen. Die Email-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch als `[spam]` markiert.
3. Erhöhung der Antispam-Schutzeinstufung. Indem die Sicherheitsstufe erhöht wird, benötigt der Antispam-Filter weniger Spamanzeichen, um eine Email-Nachricht als Spam einzustufen.

4. Trainieren Sie die lernfähige Engine (des Bayesianischen Filters) erneut. Nutzen Sie diese Lösung, wenn die Erkennungsrate des Antispam-Filters sehr schlecht ist und das Anzeigen nicht markierter Nachrichten nicht funktioniert.

Beachten Sie

BitDefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Eine Komplettliste der unterstützten Email Clients finden Sie unter: *„Software-Anforderungen“* (S. 2).

Wenn Sie einen anderen Mail Client benutzen, können Sie keine Erkennungsfehler angeben und den Bayesianischen Filter trainieren. Um das Problem zu lösen, versuchen Sie den Antispam Schutz heraufzusetzen und setzen Sie Spammer auf die Spammer Liste.

Unentdeckte Spam-Nachrichten anzeigen

Wenn Sie einen unterstützten Mail Client verwenden, können Sie einfach angeben, welche Email-Nachrichten als Spam hätten markiert werden sollen. Dadurch erhöht sich die Effizienz des Antispam-Filters.Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie in den Posteingang.
3. Markieren Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der BitDefender Antispam-Symbolleiste (normalerweise im oberen Teil des Mail Client-Fensters) auf **Ist Spam**. Dies sagt dem Bayes-Filter dass es sich bei den ausgewählten Nachrichten um eine Spam-Nachricht handelt. Sie wird dann sofort als `[spam]` markiert und in den Junk Mail-Verzeichnis verschoben.Die nächsten Email-Nachrichten, mit demselben Muster werden automatisch als `[spam]` markiert.

Spammer der Spammerliste hinzufügen

Wenn Sie einen unterstützten Email Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen.Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie in das Junk Mail-Verzeichnis, in das die Spam-Nachrichten verschoben werden.
3. Markieren Sie die Nachricht die von BitDefender als `[spam]` markiert wurde.
4. Klicken Sie in der BitDefender Antispam-Leiste auf **Spammer hinzufügen**.
5. Sie müssen diese Auswahl unter Umständen bestätigen.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie auf **OK**.

Benutzen Sie einen anderen Mail Client, können Sie manuell von der BitDefender Benutzeoberfläche aus Spammer der Spammer Liste hinzufügen. Dies macht nur Sinn, wenn Sie bereits mehrere Spam-Nachrichten vom gleichen Absender erhalten haben.Gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie im Menü auf der linken Seite auf **Antispam**.
3. Klicken Sie auf den Reiter **Status**.
4. Klicken Sie auf **Spammer verwalten**.Ein Konfigurationsfenster wird geöffnet.
5. Geben Sie die Email-Adresse des Spammer ein und klicken Sie auf den Button , um die Adresse der Spammerliste hinzuzufügen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Erhöhung der Antispam-Schutzeinstufung

Um die Antispam-Schutzeinstufung zu erhöhen, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Klicken Sie im Menü auf der linken Seite auf **Antispam**.
3. Klicken Sie auf den Reiter **Status**.
4. Verschieben Sie den Schieber entsprechend.

Erneutes Trainieren des Bayesianischen Filters

Bevor Sie den Bayes Filter trainieren, legen Sie ein Verzeichnis an, in dem ausschließlich Nachrichten enthalten sind sowie ein zweites Verzeichnis, das nur SPAM enthält.Der Bayes Filter wird trainiert, indem er die Verzeichnisse analysiert und lernt die Charakteristiken von Spams und legitimierten Nachrichten zu unterscheiden. Um die Effektivität des Trainings zu gewährleisten, müssen mindestens 50 Nachrichten in jedem Verzeichnis vorhanden sein.

Um die Bayes Datenbank zurückzusetzen und sie neu zu trainieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Mail Client.
2. Klicken Sie in der BitDefender Antispam-Leiste auf den Button **Assistent**, um den Antispam-Konfigurierungsassistent zu starten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Überspringen** und klicken Sie auf **Weiter**.
5. Wählen Sie **Antispam-Filterdatenbank leeren** und klicken Sie auf **Weiter**.

6. Wählen Sie das Verzeichnis mit legitimierten Nachrichten und klicken Sie auf **Weiter**.
7. Wählen Sie das Verzeichnis mit den SPAM-Nachrichten und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertigstellen** um den Trainingsprozess zu starten.
9. Nach Abschluss des Trainings, klicken Sie auf **Schließen**.

Hilfestellung

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

33.12.3. Antispam-Filter entdeckt keine Spam-Nachrichten.

Wenn keine Nachrichten als [spam] markiert werden, könnte es möglicherweise am BitDefender Antispam Fileter liegen.Bevor Sie die Ursache dieses Problems suchen, sollten Sie sicherstellen, dass sie nicht durch eine der folgenden Bedingungen verursacht werden:

- Der BitDefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen.Dies bedeutet folgendes:
  - Die Email-Nachrichten, die über web-basierte Email-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) gehen nichtdurch den BitDefender Spam-Filter.
  - Wenn Ihr Email Client konfiguriert ist, Emails unter Verwendung anderer Protokolle als POP3 zu empfangen (z.B., IMAP4), scannt der BitDefender Antispam-Filter diese Emails nicht auf Spam-Mails.

  Beachten Sie

  POP3 ist eines der am meisten benutzten Protokolle für das Downloaden von Email-Nachrichten vom Mail-Server.Falls Sie das Protokoll nicht kennen, das von Ihrem Email Client benutzt wird, um Emails herunterzuladen, fragen Sie die Person, die Ihren Email Client konfiguriert hat.

- BitDefender Internet Security 2011 scannt keine POP3-Übertragungen von Lotus Notes.

Sie sollten außerdem die folgenden möglichen Ursachen überprüfen:

1. Vergewissern Sie sich dass die Funktion Antispam aktiviert ist.
   a. Öffnen Sie BitDefender.
   b. Klicken Sie in der oberen rechten Bildschirmecke auf **Optionen** und wählen Sie **Einstellungen**.
   c. Überprüfen Sie in der Kategorie Sicherheitseinstellungen den Antispam-Status.

Falls Antispam deaktiviert ist, liegt darin der Grund ihres Problems.Aktivieren Sie Antispam und überwachen Sie den Antispam-Betrieb, um zu erkennen, ob das Problem behoben wurde.

2. Auch wenn es sehr unwahrscheinlich ist, sollten Sie überprüfen, ob BitDefender von Ihnen (oder einer anderen Person) so konfiguriert wurde, dass SPAM-Nachrichten nicht als [spam] markiert werden.
   a. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
   b. Klicken Sie im Menü auf der linken Seite auf **Antispam** und dann auf den Reiter **Einstellungen**.
   c. Stellen Sie sicher, dass die Option **Spam-Nachrichten im Betreff markieren** ausgewählt ist.

Eine mögliche Lösung wäre auch, das Produkt zu reparieren oder erneut zu installieren. Falls Sie lieber den BitDefender-Kundendienst kontaktieren möchten, folgen Sie der Beschreibung wie im Abschnitt „*Support*“ (S. 205) beschrieben.

33.13. Entfernen von BitDefender ist fehlgeschlagen

Dieser Artikel hilft Ihnen bei Fehlern, die bei der Deinstallation von BitDefender auftreten können.Es gibt zwei mögliche Situationen:

- Während der Deinstallation wird ein Fehlerbildschirm eingeblendet.In diesem Fenster finden Sie einen Button, über den Sie ein Deinstallations-Werkzeug ausführen können, durch das Ihr Sytem gereinigt wird.
- Die Deinstallation hängt und Ihr System ist möglicherweise abgestürzt.Klicken Sie auf **Abbrechen** um die Deinstallation abzubrechen. Sollt dies nicht funktionieren, neustarten Sie das System.

Falls die Deinstallation fehlschlägt, bleiben einige BitDefender Registry-Schlüssel und Dateien in Ihrem System. Solche Rückstände können eine erneute Installation verhindern von BitDefender. Ebenso kann die Systemleistung und Stabilität darunter leiden.Um den BitDefender vollständig von Ihrem System zu entfernen führen Sie das "Uninstall Tool" aus.

Weitere Informationen finden Sie unter „*Wie entferne ich BitDefender vollständig?*“ (S. 214).

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt „*Support*“ (S. 205) beschrieben.

34. Malware von Ihrem System entfernen

Malware kann Ihr System auf vielfältige Art und Weise beeinflussen. Wie BitDefender auf diese Malware reagiert, hängt von der Art des Malware-Angriffs ab.Da Viren Ihr Verhalten ständig ändern, ist es schwierig ein Muster für Verhalten und Aktionen festzulegen.

Es gibt Situationen, in denen BitDefender eine Malware-Infizierung Ihres Systems nicht automatisch entfernen kann.In solch einem Fall ist Ihre Intervention nötig.

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 *„Support“ (S. 205)* beschrieben, kontaktieren.

34.1. BitDefender Rescue-CD

Die **BitDefender Rescue CD** ist eine Funktion, die auf den meisten BitDefender Installations-CDs enthalten ist. Mithilfe dieser CD können Sie alle existierenden Festplatten scannen und desinfizieren, bevor Sie Ihr Betriebssystem starten.Diese Funktion kann Ihnen auch helfen, Daten von einem gefährdeten Windows PC auf einen Wechseldatenträger speichern.

Falls Sie keine Rescue CD für BitDefender haben, können Sie sich diese in Form eines ISO-Images von diesem Speicherort downloaden:

http://download.bitdefender.com/rescue_cd/

Downloaden Sie die .iso-Datei und brennen Sie sie auf CD oder DVD mit einem Programm Ihrer Wahl.

Scan des Systems mit der BitDefender Rescue CD

Um Ihr System mit der BitDefender Rescue CD zu scannen, gehen Sie folgendermaßen vor:

1. Konfigurieren Sie das BIOS Ihres Computers so, dass er von CD bootet.
2. Legen Sie die CD in das Laufwerk und booten Sie Ihren Computer neu.
3. Warten Sie, bis der BitDefender-Bildschirm eingeblendet wird und wählen Sie dann **BitDefender Rescue CD starten** in der gewünschten Sprache.
4. Warten Sie, bis der Neustart abgeschlossen ist. Dies kann eine Weile dauern.
5. Sobald der Neustartvorgang abgeschlossen ist, werden die BitDefender-Signaturen automatisch aktualisiert und ein Scan aller festgestellten Festplattenpartitionen wird gestartet.

Sichern von Daten mit der BitDefender Rescue CD

Angenommen, Sie können Ihr Betriebssystem aus unbekannten Gründen nicht mehr starten, benötigen aber dringend Dateien, die auf dem PC gespeichert sind. Hier kann Ihnen die BitDefender Notfall CD behilflich sein.

Um Ihre Daten von Ihrem Computer auf einen Wechseldatenträger, wie z.B. einen USB-Stick zu sichern, gehen Sie folgendermaßen vor:

1. Konfigurieren Sie das BIOS Ihres Computers so, dass er von CD bootet.
2. Legen Sie die CD in das Laufwerk und booten Sie Ihren Computer neu.
3. Warten Sie, bis der BitDefender-Bildschirm eingeblendet wird und wählen Sie dann **BitDefender Rescue CD starten** in der gewünschten Sprache.
4. Warten Sie, bis der Neustart abgeschlossen ist. Dies kann eine Weile dauern.
5. Sobald der Neustartvorgang abgeschlossen ist, werden die BitDefender-Signaturen automatisch aktualisiert und ein Scan aller festgestellten Festplattenpartitionen wird gestartet.

   Ihre Festplattenpartitionen werden auf dem Desktop angezeigt. Sollen die Inhalte einer Festplatte ähnlich wie in Windows Explorer dargestellt werden, doppelklicken Sie darauf.

   Beachten Sie
   Beim Arbeiten mit der BitDefender Rescue CD, haben Sie es mit Linux-Partitionsbezeichnungen zu tun. Laufwerke, die nicht unter Windows benannt wurden, werden als `[LocalDisk-0]` dargestellt und beziehen sich wahrscheinlich auf `(C:)` Windows-basierte Typenpartition, `[LocalDisk-1]` bezieht sich auf `(D:)` und so weiter.

6. Stecken Sie den Wechseldatenträger in einen USB-Anschluss Ihres Computers. In wenigen Augenblicken wird ein Fenster eingeblendet, in dem die Inhalte des Geräts angezeigt werden.
7. Das Kopieren von Dateien und Verzeichnissen erfolgt wie im normalen Windows-Umfeld.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205) beschrieben.

34.2. Was ist zu tun, wenn BitDefender auf Ihrem Computer einen Virus findet?

Sie erfahren wahrscheinlich auf folgende Weisen, ob sich auf Ihrem Computer Viren befinden:

- Sie haben einen Scan durchgeführt und BitDefender hat infizierte Einträge gefunden.
- Ein Virenwarnhinweis informiert Sie, dass BitDefender eine oder mehrere Viren auf Ihrem Computer geblockt hat.

In solchen Situationen führen Sie bitte ein BitDefender-Update durch, um sicherzustellen, dass Sie über die neuesten Malware-Signaturen verfügen und führen Sie einen Vollsystem-Scan durch, um Ihr System zu analysieren.

Sobald der Tiefen-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Einträge (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 durchgeführt werden:

1. Deaktivieren Sie denBitDefender Echtzeit-Antivirenschutz.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie aktiviere/deaktiviere ich den Echtzeitschutz?“* (S. 215).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie kann ich verborgene Objekte in Windows anzeigen lassen?“* (S. 215).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den BitDefender Echtzeit-Antivirenschutz wieder.

Sollte die erste Methode, die Infizierung zu entfernen, fehlgeschlagen sein, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 213).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer im Normalmodus neu.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

34.3. Wie entferne ich einen Virus 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 Viren innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

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

So können Sie einen in einem Archiv gespeicherten Virus entfernen.

1. Identifizieren Sie das Archiv, in dem der Virus verborgen ist, indem Sie einen Vollsystem-Scan durchführen.
2. Deaktivieren Sie denBitDefender Echtzeit-Antivirenschutz.
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 Vollsystem-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

Beachten Sie

Es ist wichtig zu beachten, dass ein in einem Archiv gespeicherter Virus für Ihr System keine unmittelbare Bedrohung darstellt, da der Virus dekomprimiert und ausgeführt werden muss, um Ihr System zu infizieren.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt „*Support*“ (S. 205) beschrieben.

34.4. Wie entferne ich einen Virus aus einem Email-Archiv?

BitDefender kann auch Viren von auf Festplatten gespeicherten Email-Datenbanken und Email-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 Email-Archiv gespeicherte Viren entfernen:

1. Scannen Sie die Email-Datenbank mit BitDefender.
2. Deaktivieren Sie denBitDefender Echtzeit-Antivirenschutz.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen Email-Client zu finden.
4. Löschen Sie die infizierte Nachricht.Die meisten Email-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungs-Verzeichnis, 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 Outlook Express:klicken Sie im Dateimenü auf "Verzeichnis", dann auf "Alle Verzeichnisse komprimieren".
   - In Microsoft Outlook:klicken Sie im Dateimenü auf "Dateidatenverwaltung".Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen".Klicken Sie auf Kompakt.
6. Aktivieren Sie den BitDefender Echtzeit-Antivirenschutz wieder.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

34.5. Wie scanne ich meinen Computer im abgesicherten Modus?

BitDefender manueller Scan lässt Sie eine Prüfung eines bestimmten Verzeichnisses oder einer Festplattenpartition durchführen, ohne dafür eine Scan-Aufgabe erstellen zu müssen.

Diese Funktion wurde zur Verwendung im abgesicherten Modus vonWindows programmiert.

Falls Ihr System mit einem Virus infiziert wurde, der im Normalmodus nicht entfernt werden kann, so können Sie versuchen, diesen zu entfernen, indem Sie Windows im abgesicherten Modus starten und mit dem manuellen Scan von BitDefender jede Festplattenpartition scannen.

Wie Sie Zugriff aus den abgesicherter Modus erhalten, finden Sie unter *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 213).

1. Um Ihr System mithilfe eines manuellen Scans durch BitDefender zu überprüfen, folgen Sie folgendem Pfad im Windows Startmenü: **Start → Alle Programme → BitDefender 2011 → BitDefender Manueller Scan**.
2. Klicken Sie auf **Verzeichnis hinzufügen**, um ein Scan-Ziel auszuwählen. Ein neues Fenster wird eingeblendet.
3. Wählen Sie das Scan-Ziel:
   - Um Ihren Desktop zu scannen, wählen Sie einfach **Desktop**.
   - Um eine komplette Festplatten-Partition zu scannen, wählen Sie diese in **Mein Computer** aus.
   - Um ein bestimmtes Verzeichnis zu scannen, suchen Sie dieses und markieren es.
4. Klicken Sie auf **OK** und **Weiter**, um den Scan zu starten.
5. Folgen Sie dem Antivirus Scan-Assistenten, um der Scan abzuschließen.

34.6. Was ist zu tun, wenn BitDefender eine saubere Datei als infiziert klassifiziert?

Es gibt Fälle, in denen BitDefender einwandfreie Dateien irrtümlicherweise als Bedrohung (ein falsches Positiv) einstuft.Um diesen Fehler zu korrigieren, fügen Sie die Datei der BitDefender Ausschlussliste hinzu:

1. Deaktivieren Sie denBitDefender Echtzeit-Antivirenschutz.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie aktiviere/deaktiviere ich den Echtzeitschutz?“* (S. 215).
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie dafür vorgehen sollen, lesen Sie bitte *„Wie kann ich verborgene Objekte in Windows anzeigen lassen?“* (S. 215).
3. Stellen Sie die Datei aus der Quarantäne wieder her.
4. Geben Sie im Ausschlussbereich die Datei ein.
5. Aktivieren Sie den BitDefender Echtzeit-Antivirenschutz wieder.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“* (S. 205) beschrieben.

34.7. Wie säubern Sie infizierte Dateien in den System Volume Information

Das Verzeichnis "System Volume Information" ist ein Bereich auf Ihrer Festplatte, der vom Betriebssystem erstellt und von Windows zum Speichern von kritischen Informationen genutzt wird, die in Zusammenhang mit der Systemkonfiguration stehen.

Die BitDefender-Engine kann infizierte Dateien, die im Verzeichnis "System Volume Information" gespeichert wurden, aufspüren. Da es sich hierbei aber um einen geschützten Bereich handelt, kann die infizierte Datei unter Umständen nicht entfernt werden.

Die in den Systemwiederherstellungs-Verzeichnissen gefundenen infizierten Dateien werden im Scan-Protokoll wie folgt angezeigt:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Um infizierte Datei(en) sofort und vollständig aus der Datenspeicherung zu entfernen, deaktivieren und reaktivieren Sie die Funktion "Systemwiederherstellung".

Wenn die Option "Systemwiederherstellung" deaktiviert ist, werden alle Wiederherstellungspunkte entfernt.

Wenn die Systemwiederherstellung erneut aktiviert wird, werden neue Wiederherstellungspunkte entsprechend dem Zeitplan und den Ereignissen erstellt.

Um die Systemwiederherstellung zu deaktivieren, gehen Sie folgendermaßen vor:

- **In Windows XP:**
  1. Folgen Sie diesem Pfad: **Start → Alle Programme → Zubehör → System Tool → Systemwiederherstellung**
  2. Klicken Sie in der linken Bildschirmseite auf **Einstellungen Systemwiederherstellung**.
  3. Wählen Sie **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
  4. Wenn Sie einen Warnhinweis erhalten, dass alle existierenden Wiederherstellungspunkte gelöscht werden, klicken Sie zum Fortfahren auf **Ja**.
  5. Um die Systemwiederherstellung einzuschalten, deaktivieren Sie das Kästchen der Option **Systemwiederherstellung ausschalten** für alle Laufwerke und klicken dann auf **Anwenden**.
- **In Windows Vista:**
  1. Folgen Sie diesem Pfad: **Start → Systemsteuerung → System und Wartung → System**
  2. Klicken Sie im linken Feld auf **Systemschutz**.

Wenn Sie zur Eingabe eines Administrator-Passwortes oder einer Bestätigung aufgefordert werden, geben Sie das Passwort oder die gewünschte Bestätigung ein.

3. Um die Funktion "Systemwiederherstellung" auszuschalten, deaktivieren Sie die entsprechenden Kästchen für jedes Laufwerk und klicken Sie auf **Ok**.
4. Um die Systemwiederherstellung zu aktivieren, klicken Sie für jedes Laufwerk die entsprechenden Kästchen an und klicken Sie auf **Ok**.

- **In Windows 7:**
  1. Klicken Sie auf **Start**, rechtsklicken Sie auf **Computer** und danach auf **Eigenschaften**.
  2. Klicken Sie im linken Feld auf den Link **Systemschutz**.
  3. Wählen Sie im Optionenfenster die Option **Systemschutz**, markieren Sie jeden Laufwerksbuchstaben und klicken dann auf **Konfigurieren**.
  4. Wählen Sie **Systemschutz ausschalten** und klicken Sie auf **Anwenden**.
  5. Klicken Sie auf **Löschen**, dann auf **Fortfahren**, wenn Sie dazu aufgefordert werden, und dann auf **Ok**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie im Abschnitt *„Support“ (S. 205)* beschrieben.

34.8. Welches sind die 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 Computers 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.

34.9. Was sind die übersprungenen Einträge 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.

34.10. Was sind die überkomprimierten Dateien im Scan-Protokoll?

Die überkomprimierten Einträge sind Elemente, die durch die Scanning-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.

34.11. Warum hat BitDefender automatisch eine infizierte Datei 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 in Schach zu halten.

Bestimmte Malware-Typen 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 Webseiten downgeloadet werden.Wenn Sie auf ein solches Problem stoßen, downloaden Sie die Installationsdatei von der Hersteller-Webseite oder einer anderen vertrauenswürdigen Webseite.

35. Support

BitDefender ist stets bemüht, seinen Kunden einen einmalig schnellen und sorgfältigen Support zu bieten.Sollten Sie mit Ihrem BitDefender-Produkt Probleme haben oder es hat sich eine Frage ergeben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie schnell eine Antwort oder Lösung finden können.Sie können auch das Kundenbetreuungs-Team von BitDefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

35.1. Online-Ressourcen

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

- BitDefender Wissensdatenbank:http://www.bitdefender.com/help
- BitDefender Support-Forum:http://forum.bitdefender.com
- das Malware City Computer Sicherheitsportal:http://www.malwarecity.com
- die Video Tutorials

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

35.1.1. BitDefender Wissensdatenbank

Bei der BitDefender Wissensdatenbank handelt es sich um eine Datenbank mit Informationen rund um die BitDefender Produkte. In leicht verständlicher Form bietet die Datenbank Informationen, Anleitungen und Berichte über neue BitDefender Patches und Problemlösungen. Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von BitDefender-Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Wissensdatenbank ist jederzeit unter der Internet Adresse http://kb.bitdefender.com erreichbar.

35.1.2. 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 Viren nicht von Ihrem Computer 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 das Forum auf neue Einträge, um Ihnen zu helfen. 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 bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das BitDefender Support-Forum finden Sie unter http://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**.

35.1.3. Malware City Portal

Das Malware City Portal ist eine umfangreiche Informationsquelle über Computersicherheit. Hier erfahren Sie mehr über die verschiedenen Bedrohungen, denen Ihr Computer während einer bestehenden Internetverbindung ausgesetzt ist (Malware, Phishing, Spams, Cyber-Kriminelle).Ein nützliches Wörterbuch hilft Ihnen, die unbekannten Computersicherheits-Fachausdrücke zu verstehen.

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

Die Webseite Malware City finden Sie unter http://www.malwarecity.com.

35.1.4. Video Tutorials

Die Video Tutorials leiten Sie Schritt für Schritt durch die Konfiguration des Produkts.Sie werden in offener, sachlicher und verständlicher Manier erstellt.

Das wichtigste Ziel ist es, eine angenehme Erfahrung sicherzustellen, indem allgemeine und weitergehende Informationen zu Sicherheitsgrundsätzen genannt werden sowie wie man BitDefender konfiguriert und nutzt.

Die wichtigste Zielsetzung ist es, die Notwendigkeit für spezialisierte Hilfe durch die Nutzung von solchen Video Tutorials zu ersetzen, die Informationen speziell zur Nutzung und Konfiguration von BitDefender anbieten.

Bevor Sie den BitDefender-Kundendienst kontaktieren oder versuchen, komplizierte Lösungen umzusetzen, können Sie beispielsweise auch eines der Video-Tutorials ansehen und den vorgeschlagenen Schritten folgen.

35.2. Hilfestellung

Der Bereich **Fehlersuche und Wie Sie Hilfe erhalten** bietet Ihnen die notwendigen Informationen für die häufigsten Problemstellungen, die bei der Nutzung dieses Produkts auftreten können.

Wenn Sie in den vorhandenen Quellen keine Lösung für Ihr Problem finden, können Sie uns direkt kontaktieren:

- „Kontaktieren Sie uns direkt aus Ihrem BitDefender-Produkt“ (S. 207)
- „Kontaktieren Sie uns über unsere Online-Wissensdatenbank“ (S. 208)

Wichtig

Um den Kundendienst von BitDefender kontaktieren zu können, muss Ihr BitDefender-Produkt aktiviert sein.Weitere Informationen finden Sie unter *„Registrierung und My-Account“* (S. 52).

Kontaktieren Sie uns direkt aus Ihrem BitDefender-Produkt

Falls Sie über eine Internetverbindung (Internetzugang) verfügen, können Sie BitDefender für Hilfestellung direkt aus dem Programm (Programmfenster) heraus kontaktieren.

Für Hilfestellung können Sie den in diesem Produkt integrierten Support nutzen.

Um den integrierten Support zu nutzen, gehen Sie folgendermaßen vor:

1. Öffnen Sie BitDefender.
2. Klicken Sie in der unteren rechten Bildschirmseite auf **Hilfe und Support**.
3. Sie haben nun zwei Möglichkeiten:
   - Suchen Sie in unserer Datenbank nach der Information, die Sie brauchen.
   - Wählen Sie die Fachabteilung, die für Ihr Problem zuständig ist.

     Kundendienst betreut Sie bei Fragen zum Kauf, Lizenzen, Erstattungen oder Verlängerungen.

     Technischer Kundendienst befasst sich mit Problemen zum Produkt selbst und seiner Funktionalität.

     Malwarebekämpfung kümmert sich um virenbezogene Probleme.
4. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
5. Falls der Lösungsvorschlag Ihr Problem nicht beheben kann, nutzen Sie den Link im Artikel, um den Kundendienst zu kontaktieren.
6. Geben Sie Ihre Email-Adresse ein, wählen Sie die Fachabteilung und beschreiben Sie kurz Ihr Problem.

Klicken Sie auf **Weiter**.

7. Bitte warten Sie einige Minuten, während BitDefender die produkt-relevanten Informationen einholt. Diese Informationen helfen unseren Mitarbeitern, eine Lösung für Ihr Problem zu finden.

   Klicken Sie auf **Weiter**.

8. Klicken Sie auf **Beenden**, um die Information an den BitDefender-Kundendienst zu senden. Sie werden schnellstmöglich kontaktiert.

Kontaktieren Sie uns über unsere Online-Wissensdatenbank

Wenn Sie auf die notwendigen Informationen nicht direkt aus BitDefender zugreifen können, gehen Sie auf unsere Online-Wissensdatenbank:

1. Gehen Sie zu http://www.bitdefender.com/help.Die BitDefender Wissensdatenbank bietet zahlreiche Artikel mit Lösungen zu BitDefender-bezogenen Problemen.
2. Suchen Sie in der BitDefender Wissensdatenbank nach Artikeln, die möglicherweise eine Lösung zu Ihrem Problem bieten.
3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
4. Falls der Lösungsvorschlag Ihr Problem nicht beheben kann, nutzen Sie den Link im Artikel, um den Kundendienst von BitDefender zu kontaktieren.
5. Kontaktieren Sie die BitDefender Support-Mitarbeiter per Email, Chat oder Telefon.

36. Kontaktinformationen

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Seit mehr als 10 Jahren übertrifft BITDEFENDER kontinuierlich die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

36.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Technischer Support:www.bitdefender.com/help
Dokumentation: documentation@bitdefender.com
Partnerprogramm: vertrieb@bitdefender.de
Marketing: marketing@bitdefender.de
Presse: presse@bitdefender.de
Jobs: jobs@bitdefender.de
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Produkt Webseite:http://www.bitdefender.com
Produkt-FTP-Archive:ftp://ftp.bitdefender.com/pub
Händler vor Ort:http://www.bitdefender.com/site/Partnership/list/
BitDefender Wissensdatenbank:http://kb.bitdefender.com

36.2. Händler vor Ort

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.com/site/Partnership/list/.
2. Die Kontaktinformationen zum örtlichen BitDefender-Händler sollten automatisch eingeblendet werden. Sollte dies nicht geschehen, nutzen Sie bitte das Tool "Partner finden" im linken Menü. Wählen Sie dort das Land aus, in dem Sie wohnen.
3. Falls Sie in Ihrem Land keinen BitDefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren.Bitte schreiben Sie uns Ihre Email in englischer Sprache, damit wir Ihnen umgehend helfen können.

36.3. BitDefender Geschäftsstellen

Die BitDefender-Niederlassungen stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der untenstehenden Auflistung.

Deutschland

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Geschäftsstelle: +49 2301 91 84 222
Vertrieb: vertrieb@bitdefender.de
Technischer Support: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Rumänien

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb E-Mail: sales@bitdefender.ro
Technischer Support: http://www.bitdefender.ro/suport
Webseite: http://www.bitdefender.ro

U.S.A

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (Geschäftsstelle&Vertrieb): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Technischer Support: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Großbritannien und Irland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Email: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096

Vertrieb: sales@bitdefender.co.uk
Technischer Support: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Spain

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vertrieb: comercial@bitdefender.es
Technischer Support: www.bitdefender.es/ayuda
Webseite: http://www.bitdefender.es

37. Nützliche Information

In diesem Kapitel finden Sie einige wichtige Vorgehensweisen, über die Sie Bescheid wissen sollten, bevor Sie wegen eines technischen Problems die Fehlersuche starten.

Für die Fehlersuche und -behebung eines technischen Problems in BitDefender sind etwas tiefergehende Kenntnisse von Windows erforderlich. Deshalb beziehen sich die nächsten Schritte vor allem auf das Windows Betriebssystem.

37.1. Wie entferne ich andere Sicherheitsprogramme?

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 nur eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.Der BitDefender Internet Security 2011-Installer findet automatisch andere auf dem System existierende Sicherheitssoftware und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC existierende Sicherheitssoftware nicht während der Installation entfernt haben, gehen Sie folgendermaßen vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**, klicken Sie auf **Systemsteuerung** und doppelklicken Sie auf **Programme hinzufügen/entfernen**.
  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 dann Ihr System neu.
- In **Windows Vista** und **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 dann Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheitssoftware zu entfernen, besorgen Sie sich das Deinstalllations-Werkzeug von der Webseite des entsprechenden Herstellers oder kontaktieren Sie ihn direkt für eine Anleitung zum sauberen Deinstallieren der Software.

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

Der abgesicherte Modus ist ein diagnostischer Operations-Modus, der hauptsächlich bei der Fehlersuche von normalen Windows-Operationen zum Einsatz kommt.Solche Probleme reichen von sich widersprechenden Treibern bis hin zu Viren, 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 Viren inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

1. Starten Sie Ihren Computer neu.
2. Drücken Sie die **F8**-Taste mehrere Male, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
3. Wählen Sie im Boot-Menü die Option **abgesicherter Modus** und drücken Sie auf **Enter**.
4. Warten Sie, während Windows im abgesicherter Modus geladen wird.
5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung.Klicken Sie zur Bestätigung auf **Ok**.
6. Um Windows normal zu starten, rebooten Sie einfach Ihr System.

37.3. Ist auf meinem System die 32- oder 64-bit-Version von Windows installiert?

Um herauszufinden, ob auf Ihrem Computer ein 32- oder 64-bit-Betriebssystem installiert ist, gehen Sie vor wie folgt:

- In **Windows XP**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Mein Computer** im Menü **Start**.
  3. Rechtsklicken Sie auf **Mein Computer** und wählen Sie **Eigenschaften**.
  4. Wenn unter **System x64 Edition** aufgelistet ist, ist auf Ihrem System die 64-Bit-Version von Windows XP installiert.

Wenn die Option **64 Edition** nicht aufgelistet ist, ist auf Ihrem System die 32-bit-Version von Windows XP installiert.

- In **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Mein Computer** im Menü **Start**.
  3. Rechtsklicken Sie auf **Mein Computer** und wählen Sie **Eigenschaften**.
  4. In **System** können Sie die Systeminformationen einsehen.

37.4. Wo finde ich "Meine Proxy-Einstellungen"?

Um diese Einstellungen zu finden, gehen Sie folgendermaßen vor:

- In Internet Explorer 8:
  1. Öffnen Sie den Internet Explorer.
  2. Wählen Sie **Werkzeuge** > **Internet-Optionen**.
  3. Klicken Sie im Reiter **Verbindungen** auf **LAN-Einstellungen**.
  4. Suchen Sie unter **Für Ihr LAN einen Proxy-Server verwenden**, dort sollten Sie die **Adresse** und den **Port** des Proxys finden.
- In Mozilla Firefox 3.6:
  1. Öffnen Sie den Firefox.
  2. Wählen Sie **Werkzeuge** > **Optionen**.
  3. Gehen Sie im Reiter **Erweitert** auf **Netzwerk**.
  4. Klicken Sie auf **Einstellungen**.
- In Opera 10.51:
  1. Öffnen Sie Opera.
  2. Wählen Sie **Werkzeuge** > **Präferenzen**.
  3. Gehen Sie im Reiter **Erweitert** auf **Netzwerk**.
  4. Klicken Sie auf den Button **Proxy Server**, um das Dialogfenster mit den Proxy-Einstellungen zu öffnen.

37.5. Wie entferne ich BitDefender vollständig?

Um BitDefender korrekt zu entfernen, gehen Sie folgendermaßen vor:

1. Gehen Sie auf www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
2. Starten Sie das Uninstall Tool unter Verwendung eines Kontos mit Administratorrechten.

3. Starten Sie Ihren Computer neu.

37.6. Wie aktiviere/deaktiviere ich den Echtzeitschutz?

BitDefender bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie Email-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) gescannt werden.

Normalerweise ist der Echtzeitschutz von BitDefender aktiviert, diesen sollten Sie auch nicht deaktivieren.

Wenn Sie ein Problem beheben oder einen Virus entfernen möchten, müssen Sie eventuell den Echtzeitschutz deaktivieren. Dies gilt für folgende Situationen:

- Ein Verlangsamungsproblem des Systems nach der Installation von BitDefender
- Ein Problem mit einem der Programme oder Anwendungen nach der Installation BitDefender
- Kurz nach der Installation von BitDefender könnten Fehlermeldungen eingeblendet werden.

Gehen Sie folgendermaßen vor, um den Echtzeitschutz vorübergehend zu aktivieren/deaktivieren:

1. Öffnen Sie BitDefender, klicken Sie in der rechten Bildschirmecke auf **Optionen** und wählen Sie **Experten-Ansicht**.
2. Gehen Sie zu **Antivirus** > **Schild**.
3. Deaktivieren Sie die Option **Echzeitschutz ist aktiviert**, um so den Antiviren-Schutz vorübergehend auszuschalten (oder platzieren Sie das Häkchen, falls Sie den Schutz einschalten möchten).
4. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll.

Beachten Sie

Die Schritte zur Deaktivierung des Echtzeitschutzes von BitDefender sollten nur als vorübergehende Lösung betrachtet und nur für einen kurzen Zeitraum angewendet werden.

37.7. Wie kann ich verborgene Objekte in Windows anzeigen lassen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Malware-Situation 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**, klicken Sie auf **Systemsteuerung** und wählen Sie **Verzeichnisoptionen**.
2. Gehen Sie auf den Reiter **Ansicht**.
3. Wählen Sie **Inhalte des Systemverzeichnisses anzeigen** (nur für Windows XP).
4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Deaktivieren Sie **Dateierweiterungen für bekannte Dateitypen verbergen**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und dann auf **Ok**.

Glossar

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 Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei ActiveX jegliche Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

Adware

Adware ist häufig mit einer Host-Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen müssen in der Regel installiert werden, 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 Pop-Up-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemleistung 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.

Archive

Ein Datenträger, ein Magnetband oder ein Verzeichnis mit Dateien, die von einer Datensicherung/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 Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

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

Bootvirus

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.

Durchsuchen

Kurzform für Web-Browser, eine Software-Anwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Mozilla Firefox und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen. Zudem können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

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 Buchstaben zusammensetzen. Als Eingabegerät wird die Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. In 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.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen entspricht.Für viele ist dies aber wie ein zweischneidiges Schwert.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, erhält, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download

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

Email

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

Ereignisanzeige

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

Fehlalarm

Dies geschieht, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

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 enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte.Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Heuristik

Eine Methode, um neue Viren zu identifizieren.Diese Scan-Methode beruht nicht auf spezifische Virussignaturen.Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann.Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

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) des Applets an.Wenn die Webseite abgerufen wird, lädt der Browser

das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

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

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige 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.

Email-Client

Ein Email Client ist eine Anwendung, die das Senden und Empfangen von Emails ermöglicht.

Arbeitsspeicher

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

Nicht heuristisch

Diese Scan-Methode beruht auf einer spezifischen Virussignatur.Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Komprimierte Programme

Eine Datei in einem komprimierten Format.Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt.Zum Beispiel: angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält.Normalerweise nehmen diese 10 Bytes Speicherplatz in Anspruch.

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

Pfad

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

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

Phishing

Dabei wird eine Email mit einer betrügerischen Absicht an einen Nutzer gesendet. Der Inhalt dieser Email gibt vor, von einem bekannten und seriösen Unternehmen zu stammen. Zweck dieser Email ist es dann, private und geheime Nutzerdaten zu erhalten, womit der Absender beabsichtigt, die Identität des Nutzers anzunehmen.Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben.Dies soll aus Gründen der Aktualisierung geschehen.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.

Schnittstelle

Schnittstelle im Rechner, an die ein Gerät angeschlossen werden kann.Rechner verfügen über verschiedene Schnittstellen.Intern 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.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit den gescannten Pfaden, Verzeichnissen und der Archivanzahl sowie den gescannten, infizierten oder verdächtigen Dateien.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen

oder Peripheriegeräten abfangen, falls Sie in eine entsprechende Software eingebettet sind.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

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 Email.

Spyware

Software, die unentdeckt vom Nutzer Anwenderdaten über seine Internetverbindung sammelt und abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware sind. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über Email-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware insofern, als dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren.Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, da über seine Internetverbindung 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 Eintrag (Autostart-Objekt)

Jede Datei, die sich in diesem Verzeichnis befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein.Gewöhnlich wird eine

Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Verzeichnis gelegt.

Symbolleiste

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

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden.TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein schädliches Programm, das sich als eine freundliche Anwendung tarnt und auftritt.Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein.Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.Viele Trojaner öffnen den Rechner für den Zugriff von außen.

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

Update

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

BitDefender verfügt über ein eigenes Update-Modul, das manuelle oderautomatische Scans nach Updates ermöglicht.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und das sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch

einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

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