INTERNET SECURITY 2012

Benutzerhandbuch

Bitdefender Internet Security 2012
Benutzerhandbuch

Veröffentlicht 2011.07.27

Rechtlicher Hinweis


Bitdefender

Inhaltsverzeichnis

1. Installation

1.1. Vor der Installation

Bevor Sie Bitdefender Internet Security 2012 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. 1).
- Melden Sie sich mit einem Administrator-Konto am Computer an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Computer.Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen.Windows Defender wird während der Installation deaktiviert.
- 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 während der Installation deaktiviert.
- Ihr Computer sollte während der Installation mit dem Internet verbunden sein, selbst wenn Sie von CD oder DVD installieren.Falls neuere Versionen der Anwendungsdateien verfügbar sind, als die, die im Installationspaket enthalten sind, wird Bitdefender diese herunterladen und installieren.

1.2. Systemanforderungen

Sie können Bitdefender Internet Security 2012 nur auf Computern mit den folgenden Betriebssystemen installieren.

- Windows XP mit Service Pack 3 (32-Bit)
- Windows Vista mit Service Pack 2
- Windows 7 mit Service Pack 1

Stellen Sie vor der Installation sicher, dass Ihr Computer die Mindestsystemanforderungen 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.

1.2.1. Mindestsystemanforderungen

- 1,8 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- 800 MHz Prozessor
- 1 GB Arbeitsspeicher (RAM)

1.2.2. Empfohlene Systemanforderungen

- 2,8 GB freier Speicherplatz (davon mindestens 800 MB auf dem Systemlaufwerk)
- Intel CORE 2 Duo (1.66 GHz) oder gleichwertiger Prozessor
- Speicher (RAM):
  - 1 GB MB für Windows XP
  - 1.5 GB für Windows Vista und Windows 7

1.2.3. Software-Anforderungen

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

- Internet Explorer 7 oder höher
- Mozilla Firefox 3.6 (oder höher)
- Yahoo! Messenger 8.1 oder höher
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express und Windows Mail (auf 32-Bit-Systemen)
- Mozilla Thunderbird 3.0.4
- .NET Framework 3

1.3. Installieren Ihres Bitdefender-Produkts

Sie können Bitdefender von der Bitdefender-Installations-CD oder über ein Installationspaket installieren, das Sie von der Bitdefender- Website oder einer anderen autorisierten Website heruntergeladen haben (so z.B. von einer Bitdefender-Partner-Website oder einem Online-Shop).Sie können das Installationspaket von der Bitdefender Webseite unter folgender Adresse herunterladen: http://www.bitdefender.com/site/Downloads/.

- Um Bitdefender von der Installations-CD aus zu installieren, legen Sie die CD in das optische Laufwerk ein.Warten Sie einen Moment, bis der Willkommensbildschirm angezeigt wird. Folgen Sie den Anweisungen, um die Installation zu starten.

Beachten Sie

Im Willkommensbildschirm haben Sie die Möglichkeit, das Installationspaket von der Installations-CD auf einen USB-Speicherstick zu kopieren.Dies kann sich als

nützlich erweisen, wenn Sie Bitdefender auf einem Computer installieren wollen, der über kein Laufwerk verfügt (wie z.B. ein Netbook).Verbinden Sie das Speichermedium mit einem USB Port und klicken Sie auf **Kopiere auf USB**.Stecken Sie den Speicherstick anschließend in den USB-Port des Computers ohne Laufwerk und doppelklicken Sie in dem Ordner, in dem Sie das Installationspaket gespeichert haben, auf `runsetup.exe`.

Wenn der Willkommensbildschirm nicht angezeigt wird, gehen Sie in das Root-Verzeichnis Ihrer CD und doppelklicken Sie auf `autorun.exe`.

- Um Bitdefender über das von Ihnen heruntergeladene Installationspaket zu installieren, navigieren Sie zu der Datei und doppelklicken Sie darauf.Hierdurch wird der Download der Installationsdateien gestartet. Abhängig von Ihrer Internet-Verbindung kann dies einige Zeit in Anspruch nehmen.

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

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

Wenn ein inkompatibles Virenschutzprogramm oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen.Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden.

Beachten Sie
Unter Umständen müssen Sie Ihren Computer neu starten, um die Entfernung der erkannten Virenschutzprogramme abzuschließen.

Folgen Sie den Anweisungen des Installationsassistenten, um Bitdefender Internet Security 2012 zu installieren.

Schritt 1 - Willkommen

Bitte lesen Sie die Lizenzvereinbarung und wählen Sie **Zustimmen & fortfahren**.Die Lizenzvereinbarung enthält die Nutzungsbedingungen für Bitdefender Internet Security 2012.

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

Schritt 2 - Registrieren Sie Ihr Produkt

Um die Registrierung Ihres Produkts abzuschließen, müssen Sie einen Lizenzschlüssel eingeben und ein MyBitdefender-Benutzerkonto anlegen.Zudem wird eine aktive Internet-Verbindung benötigt.

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

- **Ich habe das Produkt erworben**

  In diesem Fall registrieren Sie das Produkt, indem Sie die folgenden Schritte ausführen:

  1. Wählen Sie den Punkt **Ich habe das Produkt erworben und möchte es jetzt registrieren**.
  2. Geben Sie den Lizenzschlüssel in das entsprechende Feld ein.

     Beachten Sie

     Sie finden den Lizenzschlüssel:
     - auf dem Label der CD/DVD.
     - Auf der Registrierungskarte des Produktes.
     - In der E-Mail-Bestätigung des Online-Kaufs.

  3. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein.

     Wichtig

     Eine gültige E-Mail-Adresse ist erforderlich.Eine Bestätigungsnachricht wird an die von Ihnen angegebene Adresse gesendet.

  4. Klicken Sie auf **Jetzt registrieren**.

- **Ich möchte Bitdefender testen**

  In diesem Fall können Sie das Produkt für 30 Tage nutzen.Um die Testphase zu starten, wählen Sie die Option **Ich möchte das Produkt testen**.

  Um die Online-Funktionen des Produkts nutzen zu können, müssen Sie ein MyBitdefender-Benutzerkonto anlegen.Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein, um ein Benutzerkonto anzulegen.Eine Bestätigungsnachricht wird an die von Ihnen angegebene Adresse gesendet.Falls Sie bereits über ein Benutzerkonto verfügen, geben Sie die damit verbundene E-Mail-Adresse ein, um das Produkt auf dieses Konto zu registrieren.

Benutzerdefinierte Einstellungen

Optional können Sie die Installationseinstellungen an Ihre individuellen Anforderungen anpassen, indem Sie auf **Benutzerdefinierte Einstellungen** klicken.

Installationspfad

Bitdefender Internet Security 2012 wird standardmäßig im Ordner `C:\Programme\Bitdefender\Bitdefender 2012`.Falls Sie ein anderes Installationsverzeichnis wählen möchten, klicken Sie auf **Ändern** und wählen Sie das Verzeichnis, in dem Sie Bitdefender installieren möchten.

Proxy-Einstellungen konfigurieren

Bitdefender Internet Security 2012 benötigt Zugriff auf das Internet, um die Produktregistrierung abzuschließen, Sicherheits- und Produkt-Updates herunterzuladen, In-the-Cloud-Komponenten zu nutzen usw.Wenn Sie eine Proxy-Verbindung anstelle einer direkten Internet-Verbindung nutzen, müssen Sie diese Option auswählen und die Proxy-Einstellungen konfigurieren.

Die Einstellungen können aus dem Standard-Browser importiert oder manuell eingegeben werden.

P2P-Update aktivieren

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.

Um während eines Updates die Auswirkungen des Netzwerkverkehrs auf die Systemleistung zu minimieren, nutzen Sie die Update-Sharing-Option.Bitdefender nutzt die Ports 8880 - 8889 für Peer-to-Peer-Updates.

Anonyme Nutzungsberichte senden

Standardmässig sind anonyme Benutzer Berichte aktiviert.Durch Aktivierung dieser Option, werden Berichte, die Informationen zu Ihrer Nutzung des Produktes an Bitdefender Server gesendet.Diese Information ist wichtig für die Verbesserung des Produktes.Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Klicken Sie auf **OK**, um Ihre Einstellungen zu bestätigen.

Klicken Sie auf **Installieren**, um die Installation zu starten.

Schritt 3 - Installationsfortschritt

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

Kritische Bereiche Ihres Systems werden nach Viren durchsucht, die neuesten Versionen der Anwendungsdateien heruntergeladen und installiert und die Bitdefender-Dienste gestartet.Dieser Schritt kann einige Minuten in Anspruch nehmen.

Schritt 4 - Fertigstellen

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

Klicken Sie auf **Fertigstellen**.

Wenn Sie auf Ihrem Computer Windows XP nutzen, wird der Installationsassistent alle Netzwerke erkennen, mit denen Sie verbunden sind, und Sie dazu auffordern, diese als Heim/Büro oder öffentlich zu definieren.

1.3.1. Upgrade für eine ältere Version installieren

Wenn Sie bereits eine ältere Version von Bitdefender nutzen, gibt es zwei Möglichkeiten ein Upgrade auf Bitdefender Internet Security 2012 zu vollziehen:

- Installieren Sie Bitdefender Internet Security 2012 direkt über die alte Version.Bitdefender wird die ältere Version erkennen und Sie bei der Entfernung unterstützen, bevor die neue Version installiert wird.Sie müssen den Computer während des Upgrades neu starten.
- Entfernen Sie die ältere Version, starten Sie Ihren Computer neu und installieren Sie die neue Version wie auf den vorangehenden Seiten beschrieben.Nutzen Sie diese Update-Methode falls, die andere fehlschlägt.

Beachten Sie
Produkteinstellungen und der Inhalt der Quarantäne werden nicht aus der älteren Version importiert.

2. Inbetriebnahme

Sobald Sie Bitdefender Internet Security 2012 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.

Der Auto-Pilot ist standardmäßig aktiviert und Sie müssen keinerlei Einstellungen vornehmen.Sie können jedoch auch die Bitdefender-Einstellungen für die Feineinstellung nutzen und Ihren Schutz verbessern.

Bitdefender trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen.Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster.Für weitere Informationen lesen Sie bitte *„Ereignisse“ (S. 14)*.

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 das Produkt bisher noch nicht registriert haben (einschließlich der Erstellung eines MyBitdefender-Kontos), holen Sie dies bitte noch vor Ablauf der Testphase nach. Sie müssen ein Benutzerkonto anlegen, um die Online-Funktionen des Produkts nutzen zu können.Weitere Informationen zum Registrierungsvorgang finden Sie im Kapitel *„Produktregistrierung“ (S. 8)*.

2.1. Öffnen Sie Bitdefender

Sie können die Benutzeroberfläche von Bitdefender Internet Security 2012 aus dem Windows-Startmenü heraus über den folgenden Pfad aufrufen: **Start → Alle Programme → Bitdefender 2012 → Bitdefender Internet Security 2012**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol  in der Task-Leiste.

Weitere Informationen zum Bitdefender-Fenster und das Symbol in der Task-Leiste finden Sie im Kapitel *„Bitdefender-Benutzeroberfläche“ (S. 20)*.

2.2. Was nach der Installation zu beachten ist

Wenn Sie wollen, dass Bitdefender alle sicherheitsrelevanten Entscheidungen für Sie trifft, lassen Sie den Auto-Pilot aktiviert.Für weitere Informationen lesen Sie bitte *„Auto-Pilot“ (S. 15)*.

Im Folgenden finden Sie eine Liste von Schritten, die Sie nach Abschluss der Installation unter Umständen ausführen sollten:

- Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 38) beschrieben konfigurieren.
- Wenn Sie Bitdefender auf mehr als einem Computer in Ihrem Heimnetzwerk installiert haben, können Sie alle Bitdefender-Produkte von einem einzigen Computer aus fernverwalten.Für weitere Informationen lesen Sie bitte *„Netzwerkplan“* (S. 111).
- Falls Sie Kinder haben, können Sie die Kindersicherung nutzen, um ihre Aktivitäten am Computer und im Internet zu überwachen und zu kontrollieren.Die Kindersicherung ist standardmäßig für alle eingeschränkten Windows-Benutzerkonten aktiviert. Zudem werden für Teenager geeignete Internet-Filterregeln angewandt.Für weitere Informationen lesen Sie bitte *„Jugendschutz“* (S. 84).
- Erstellen Sie Datenschutzregeln, um zu verhindern, dass wichtige persönliche Daten ohne Ihre Zustimmung preisgegeben werden.Für weitere Informationen lesen Sie bitte *„Datenschutz“* (S. 80).

2.3. Produktregistrierung

Um durch Bitdefender geschützt zu sein, müssen Sie Ihr Produkt durch die Eingabe eines Lizenzschlüssels und das Anlegen eines MyBitdefender-Benutzerkontos registrieren.

Die Lizenzschlüssel legt fest, für wie lange Sie das Produkt einsetzen können.Sobald der Lizenzschlüssel abgelaufen ist, wird Bitdefender alle Funktionen und somit den Schutz Ihres Computers einstellen.

Sie sollten einige Tage bevor die momentan genutzte Lizenz abläuft diese verlängern oder eine neue erwerben.Für weitere Informationen lesen Sie bitte *„Kaufen oder Erneuern von Lizenzschlüsseln“* (S. 11).Falls Sie eine Testversion von Bitdefender nutzen, müssen Sie diese mit einem Lizenzschlüssel registrieren, wenn Sie die Software auch nach Ablauf der Testphase weiterhin nutzen wollen.

Mit einem MyBitdefender-Konto haben Sie Zugriff auf Produkt-Upgrades und die von Bitdefender Internet Security 2012 angebotenen Online-Dienste.Wenn Sie bereits ein Benutzerkonto eingerichtet haben, registrieren Sie Ihr Bitdefender-Produkt unter diesem Konto.

Mit einem MyBitdefender-Konto können Sie:

- Ihr Produkt immer auf dem neuesten Stand halten.
- Ihren Lizenzschlüssel abrufen, sollten Sie ihn verloren haben.
- den Bitdefender-Kundendienst kontaktieren.
- die Aktivitäten Ihrer Kinder überwachen und die Kindersicherung konfigurieren, unabhängig davon, wo Sie sich gerade befinden.

- Ihr Facebook-Konto mit Safego schützen.

2.3.1. Eingeben des Lizenzschlüssels

Wenn Sie sich während der Installation entschieden haben, das Produkt zu testen, steht es Ihnen für eine 30-tägige Testphase zu Verfügung.Um Bitdefender auch nach Ablauf der Testphase weiterhin nutzen zu können, müssen Sie das Produkt mit einem Lizenzschlüssel registrieren.

Klicken Sie im unteren Bereich des Bitdefender-Fensters auf **Lizenzinfo**, um das Produkt mit einem Lizenzschlüssel zu registrieren oder den aktuellen Lizenzschlüssel zu ändern.Das Registrierungsfenster wird eingeblendet.

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

Um Bitdefender Internet Security 2012 zu registrieren:

1. Geben Sie den Lizenzschlüssel in das Editierfeld ein.

   Beachten Sie
   Sie finden den Lizenzschlüssel:
   - Auf dem CD-Aufdruck.
   - Auf der Registrierungskarte des Produktes.
   - In der E-Mail-Bestätigung des Online-Kaufs.

   Falls Sie über keinen Bitdefender-Lizenzschlüssel verfügen, klicken Sie auf den Link, der Ihnen in dem Fenster angezeigt wird. Dieser ruft eine Website auf, über die Sie einen Schlüssel erwerben können.

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

2.3.2. Anmelden bei MyBitdefender

Wenn Sie während der Installation eine E-Mail-Adresse angegeben haben, wurde an diese Adresse eine Bestätigungsnachricht geschickt.Klicken Sie auf den Link in der E-Mail, um die Registrierung abzuschließen.

Falls Sie die Registrierung noch nicht abgeschlossen haben, wird Bitdefender Sie daran erinnern.

Wichtig
Sie müssen sich innerhalb von 30 Tagen nach der Installation von Bitdefender bei einem Benutzerkonto angemeldet haben.Ansonsten erhält Bitdefender keine automatischen Updates.

Um ein MyBitdefender-Konto anzulegen oder sich bei einem Konto anzumelden, klicken Sie im unteren Bereich des Bitdefender-Fensters auf **Registrierung fertigstellen** bzw. **MyBitdefender**.

Das MyBitdefender-Fenster wird angezeigt.Fahren Sie entsprechend Ihrer Situation fort.

Ich möchte ein MyBitdefender-Konto anlegen

Um ein MyBitdefender-Konto erfolgreich anzulegen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Neues Konto erstellen**.

   Ein neues Fenster wird sich öffnen.

2. Geben Sie die Daten in die entsprechenden Felder ein.Die hier eingetragenen Daten bleiben vertraulich.

   - **Name** - Geben Sie einen Benutzernamen für Ihr Konto an. Dieses Feld ist optional.
   - **E-mail** - Geben Sie Ihre E-Mail-Adresse an.
   - **Passwort** - Geben Sie ein Passwort für Ihr Benutzerkonto ein.Das Passwort muss mindestens 6 Zeichen lang sein.
   - **Passwort bestätigen** - Geben Sie das Passwort erneut ein.
   - Auf Wunsch wird Bitdefender Sie über die E-Mail-Adresse in Ihrem Benutzerkonto über Sonderangebote und Werbeaktionen informieren.Um diese Option zu aktivieren, wählen Sie den Punkt **Ich gestatte Bitdefender, mir E-Mails zuzusenden**.

   Beachten Sie

   Sobald das Benutzerkonto angelegt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter http://my.bitdefender.com bei Ihrem Konto anmelden.

3. Klicken Sie auf **Übermitteln**.
4. Bevor Sie Ihr Konto nutzen können, müssen Sie zunächst die Registrierung abschließen.Rufen Sie Ihre E-Mails ab und folgen Sie den Anweisungen in der Bestätigungsnachricht, die Sie von Bitdefender erhalten haben.

Beachten Sie

Sie können sich auch über Ihr Facebook- oder Google-Konto anmelden.Weitere Informationen finden Sie unter „Ich möchte mich über mein Facebook- oder Google-Konto anmelden“ (S. 10)

Ich möchte mich über mein Facebook- oder Google-Konto anmelden

Um sich über Ihr Facebook- oder Google-Konto anzumelden, gehen Sie folgendermaßen vor:

1. Klicken Sie auf das Symbol für den Dienst, über den Sie sich anmelden wollen.Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.

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

Ich habe bereits ein MyBitdefender-Konto

Wenn Sie sich von Ihrem Produkt aus bereits zuvor bei einem Benutzerkonto angemeldet haben, wird Bitdefender dies erkennen und Sie bei diesem Benutzerkonto anmelden. Klicken Sie auf **Zu MyBitdefender**, um Ihr Benutzerkonto unter http://my.bitdefender.com aufzurufen.

Wenn Sie sich bei einem anderen Konto anmelden wollen, klicken Sie auf den entsprechenden Link und befolgen Sie die in den vorausgegangenen Abschnitten beschriebenen Anweisungen.

Wenn Sie bereits über ein aktives Benutzerkonto verfügen, Bitdefender dieses aber nicht findet, folgen Sie diesen Schritten, um sich bei diesem Konto anzumelden:

1. Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein.

Beachten Sie
Falls Sie Ihr Passwort vergessen haben, klicken Sie auf **Passwort vergessen** und folgen Sie den Anweisungen, um ein neues Passwort anzufordern.

2. Klicken Sie auf **Anmelden**.

2.3.3. Kaufen oder Erneuern von Lizenzschlüsseln

Wenn sich die Testperiode dem Ende zuneigt, sollten Sie einen Lizenzschlüssel erwerben und Ihr Produkt registrieren.Falls Ihr aktueller Lizenzschlüssel in Kürze abläuft, müssen Sie Ihre Lizenz verlängern.

Bitdefender wird Sie benachrichtigen, wenn das Ablaufdatum Ihrer aktuellen Lizenz näher rückt. Befolgen Sie die Anweisungen in der Benachrichtigung, um eine neue Lizenz zu erwerben.

Sie können zudem jederzeit eine Website aufrufen, über die Sie einen Lizenzschlüssel erwerben können. Gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie im unteren Bereich des Bitdefender-Fensters auf **Lizenzinfo**, um das Fenster für die Produktregistrierung zu öffnen.
3. Klicken Sie auf den Link am unteren Fensterrand.

2.4. 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.

Zu den erkannten Problemen gehören auch wichtige Schutzeinstellungen, die deaktiviert sind, und andere Umstände, die ein Sicherheitsrisiko darstellen. Dabei werden zwei Kategorien unterschieden:

- **Kritische Probleme** - Verhindern, dass Bitdefender Sie vor Malware schützt oder stellen ein erhebliches Sicherheitsrisiko dar.
- **Kleinere (nicht-kritische) Probleme** - Können Ihren Schutz in naher Zukunft beeinträchtigen.

Das Bitdefender-Symbol in der Task-Leiste weist Sie durch die folgenden Farbwechsel auf ausstehende Probleme hin:

Rot markiert: Kritische Probleme betreffen die Sicherheit Ihres Systems. Sie benötigen Ihre sofortige Aufmerksamkeit und müssen umgehend behoben werden.

Gelb markiert: Nicht-kritische Probleme beeinträchtigen die Sicherheit Ihres Systems. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

Wenn Sie den Mauszeiger über das Symbol bewegen, wird Ihnen angezeigt, dass ein Porblem existiert.

Wenn Sie das Bitdefender-Fenster öffnen, zeigt der Sicherheitsstatusbereich in der oberen Symbolleiste die Anzahl und Art der Probleme an, die Ihr System beeinträchtigen.

2.4.1. "Alle Probleme beheben"-Assistent

Um erkannte Probleme zu beheben, folgen Sie den Anweisungen des **Alle Probleme beheben**-Assistenten.

1. Befolgen Sie eine der folgenden Möglichkeiten, den Assistenten zu öffnen:
   - Rechtsklicken Sie auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie dann **Alle Probleme beheben**.Abhängig von dem erkannten Problem ist das Symbol entweder rot (und weist auf ein kritisches Problem hin) oder gelb (und weist somit auf ein nicht-kritisches Problem hin).

- Öffnen Sie das Bitdefender-Fenster und klicken Sie auf eine beliebige Stelle innerhalb des Sicherheitsstatusbereichs in der oberen Symbolleiste (Sie können zum Beispiel auf die Schaltfläche **Alle Probleme beheben** klicken).

2. Sie erhalten eine Übersicht aller Probleme, die die Sicherheit Ihres Computers und Ihrer Daten beeinträchtigen.Alle aktuellen Probleme sind markiert und werden behoben.

   Wenn Sie ein bestimmtes Problem nicht sofort beheben möchten, deaktivieren Sie das entsprechende Kästchen.Sie werden aufgefordert anzugeben, für wie lange die Behebung des Problems verschoben werden soll.Wählen Sie die gewünschte Option aus dem Menü und klicken Sie auf **OK**. Um die Überwachung der jeweiligen Problemkategorie zu beenden, wählen Sie den Punkt **Dauerhaft**.

   Der Status des Problems erscheint als **Aufschieben** und es wird keine Aktion zur Behebung des Problems durchgeführt.

3. Um die ausgewählten Risiken zu beheben, klicken Sie auf **Beheben**. Einige Risiken werden sofort behoben.Für die anderen, hilft Ihnen ein Assistent diese zu beheben.

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

- **Deaktivierte Sicherheitseinstellungen.** Solche Probleme werden sofort beseitigt, durch die entsprechenden Sicherheitseinstellungen.
- **Vorbeugende Sicherheitsaufgaben die Sie durchführen sollten.** Bei der beseitigung solcher Probleme, hilft Ihnen ein Assistent.

2.4.2. Konfigurieren von Statusbenachrichtigungen

Das Statuswarnsystem ist so vorkonfiguriert, dass die wichtigsten Sicherheitsrisiken für Ihr Systems und Ihre Daten überwacht und Sie darüber informiert werden.Neben den überwachten standard Problemen, 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.Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Erweitert**.
4. Suchen Sie den Link **Statusbenachrichtigungen konfigurieren** und klicken Sie darauf.
5. Klicken Sie auf die Schalter, um die Statusbenachrichtigungen entsprechend Ihrer Anforderungen zu aktivieren oder deaktivieren.

2.5. Ereignisse

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich aller Computer-Aktivitäten, die von der Kindersicherung überwacht werden).Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes.So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.Zudem können Sie bei Bedarf weitere Aktionen durchführen oder die von Bitdefender durchgeführten Aktionen anpassen.

Um das Ereignisfenster aufzurufen, öffnen Sie das Bitdefender-Fenster und klicken Sie in der oberen Symbolleiste auf **Ereignisse**.

Um Ihnen beim Filtern der Bitdefender-Ereignisse zu helfen, stehen Ihnen im Menü links die folgenden Kategorien zur Verfügung:

- **Virenschutz**
- **Spam-Schutz**
- **Jugendschutz**
- **Privatsphärenschutz**
- **Firewall**
- **Netzwerkplan**
- **Update**
- **SafeGo**
- **Registrierung**

Eine Liste von Ereignissen ist für jede Kategorie verfügbar.Um weitere Informationen über ein bestimmtes Ereignis in der Liste zu erhalten, müssen Sie nur darauf klicken. Details zu dem Ereignis werden in der unteren Hälfte des Fensters angezeigt.Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender für beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses.Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Sie können Ereignisse nach Ihrer Dringlichkeit ordnen.Es gibt drei Arten von Ereignissen. Diese werden durch verschiedene Symbole unterschieden:

Information Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.
Warnung Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
Kritisch Diese Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.

Um Ihnen die Verwaltung von protokollierten Ereignissen zu erleichtern, enthält jeder Abschnitt des Ereignisfensters Optionen, mit denen Sie alle Ereignisse in diesem Abschnitt löschen oder als gelesen markieren können.

2.6. Auto-Pilot

Für alle Benutzer, die nichts weiter von Ihrer Sicherheitslösung verlangen, als zuverlässigen Schutz ohne dabei ständig gestört zu werden, bietet Bitdefender Internet Security 2012 einen integrierten Auto-Pilot-Modus.

Solange der Auto-Pilot aktiviert ist, wird Bitdefender die optimale Sicherheitskonfiguration anwenden und alle sicherheitsrelevanten Entscheidungen für Sie treffen.Das bedeutet, dass keine Pop-ups oder Benachrichtigungen eingeblendet werden und Sie keinerlei Einstellungen vornehmen müssen.

Wenn der Auto-Pilot aktiviert ist, werden kritische Probleme von Bitdefender automatisch behoben. Zudem werden die folgenden Funktionen unauffällig im Hintergrund verwaltet:

- Virenschutz, gewährleistet durch Zugriff-Scans und ununterbrochenes Scanning.
- Firewall-Schutz.
- Privatsphärenschutz, gewährleistet durch die Phishing- und Malware-Filter für das Surfen im Internet.
- Automatische Updates.

Der Auto-Pilot wird standardmäßig aktiviert, sobald die Bitdefender-Installation abgeschlossen wurde.Wenn der Auto-Pilot aktiviert ist, erscheint folgendes Bitdefender-Symbol in der Task-Leiste:  .

Um den Auto-Pilot zu aktivieren oder deaktivieren, öffnen Sie das Bitdefender-Fenster und klicken Sie auf den **Auto Pilot**-Schalter in der oberen Symbolleiste.

Wichtig
Wenn der Auto-Pilot aktiviert ist und Sie eine der von ihm verwalteten Einstellungen verändern, wird er automatisch deaktiviert.

Um eine Übersicht der Aktionen anzuzeigen, die von Bitdefender durchgeführt wurden, während der Auto-Pilot aktiviert war, öffnen Sie das Fenster Ereignisse.

2.7. Spiele-Modus und Laptop-Modus

Einige Computeraktivitäten, wie Spiele oder Presentationen, benötigen erhöhte Ansprechbarkeit und Leistung ohne Unterbrechungen.Wenn Ihr Laptop auf Batteriebetrieb läuft ist es ratsamer unnötige Vorgänge, welche zusätzlich Strom verbrauchen, zu verschieben bis der Laptop extern mit Strom versorgt wird.

Um sich diesen besonderen Situationen anzupassen, hat Bitdefender Internet Security 2012 zwei spezielle Betriebsmodi:

- Spiele-Modus
- Laptop-Modus

2.7.1. Spiele-Modus

Der Spiele-Modus ändert die Schutzeinstellungen zeitweise, 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.
- Auto-Scan ist deaktiviert.Auto-Scan findet und nutzt Zeitabschnitte, während derer die Auslastung der Systemressourcen unter einen bestimmten Grenzwert fällt, um regelmäßige Scans des gesamten Systems durchzuführen.
- Die Bitdefender-Firewall befindet sich im Normalmodus (der **Paranoidmodus** ist deaktiviert).Das bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Auto-Update ist deaktiviert.
- Die Bitdefender-Symbolleiste in Ihrem Browser ist deaktiviert, wenn Sie Browser-basierte Online-Spiele spielen.

Wenn der Spiele-Modus aktiviert ist, sehen Sie den Buchstaben G über dem Bitdefender Symbol.

Spiele-Modus benutzen

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.Bitdefender wird selbstständig zum Normalbetriebsmodus zurückkehren wenn Sie das Spiel verlassen oder die erkannte Anwendung den Vollbildmodus verlässt.

Falls Sie den Spiele-Modus manuell aktivieren möchten, verwenden Sie eine der folgenden Methoden:

- Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol im System-Tray und wählen Sie **Spiele-Modus einschalten**.
- Drücken Sie `Strg+Shift+Alt+G` (Standard-Tastenkombination)

> **Wichtig**
> Vergessen Sie nicht den Spiele-Modus später wieder auszuschalten. Befolgen Sie dazu die selben Schritte wie zum Einschalten des Spiele-Modus.

Anpassen der Tastaturbefehle für den Spiele-Modus

Sie können den Spiele-Modus manuell über das Tastaturkürzel `Strg+Alt+Shift+G` aktivieren.Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Einstellungen**.
4. Wählen Sie unter der Option **Tastaturbefehle für Spiele-Modus aktivieren** den gewünschten Tastaturbefehl aus:

   a. Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).

   b. 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
Um den Tastaturbefehl zu deaktivieren, deaktivieren Sie die Option **Tastaturbefehle für Spiele-Modus aktivieren**.

Aktivieren / Deaktivieren des automatischen Spiele-Modus

Um den automatischen Spiele-Modus zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Einstellungen**.
4. Aktivieren oder deaktivieren Sie den automatischen Spiele-Modus, indem Sie auf den entsprechenden Schalter klicken.

2.7.2. 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.Wenn sich Bitdefender im Laptop-Modus befindet, sind die Auto-Scan- und Auto-Update-Funktionen deaktiviert, da diese mehr Systemressourcen in Anspruch nehmen und den Energieverbrauch unbemerkt steigern.

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.

Um den automatischen Laptop-Modus zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Einstellungen**.
4. Aktivieren oder deaktivieren Sie den automatischen Laptop-Modus, indem Sie auf den entsprechenden Schalter klicken.

Wenn Bitdefender nicht auf einem Laptop installiert ist, deaktivieren Sie den Laptop-Modus.

2.8. Passwortschutz für Bitdefender-Einstellungen

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

Um den Passwortschutz für die Bitdefender-Einstellungen zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Einstellungen**.
4. Aktivieren Sie im Bereich **Passwortschutzeinstellungen** den Passwortschutz, indem Sie auf den Schalter klicken.
5. Klicken Sie auf den Link **Passwort ändern**.
6. Geben Sie das Passwort in die beiden Felder ein und klicken Sie dann auf **OK**.Das Passwort muss mindestens 8 Zeichen lang sein.

Sobald Sie ein Passwort festgelegt haben, muss jeder, der die Bitdefender-Einstellungen verändern will, zunächst das Passwort eingeben.

Wichtig

Merken Sie sich Ihr Passwort gut oder schreiben Sie es auf und verwahren es an einem sicheren Platz.Wenn Sie Ihr Passwort vergessen haben, müssen Sie das Programm neu installieren oder den Kundendienst von Bitdefender kontaktieren.

Um den Passwortschutz zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.

3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Einstellungen**.
4. Deaktivieren Sie im Bereich **Passwortschutzeinstellungen** den Passwortschutz, indem Sie auf den Schalter klicken.
5. Geben Sie das Passwort ein und klicken Sie auf **OK**.

2.9. Anonyme Nutzungsberichte

Bitdefender verschickt standardmäßig Berichte mit Nutzungsinformationen an die Bitdefender-Server.Diese Information ist wichtig für die Verbesserung des Produktes.Bitte beachten Sie, dass diese Berichte weder vertrauliche Daten, wie Ihren Namen und Ihre IP Adresse, enthalten, noch werden diese Daten für kommerzielle Zwecke verwendet.

Wenn Sie das Versenden von anonymen Nutzungsberichten beenden wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Erweitert**.
4. Deaktivieren Sie die anonymen Nutzungsberichte, indem Sie auf den entsprechenden Schalter klicken.

2.10. Bitdefender reparieren oder entfernen

Wenn Sie Bitdefender Internet Security 2012 reparieren oder entfernen möchten, folgen Sie diesem Pfad vom Windows-Startmenü aus: **Start → Alle Programme → Bitdefender 2012 → 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.

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

Sie müssen den Computern neu starten, um den Vorgang abzuschließen.

3. Bitdefender-Benutzeroberfläche

Bitdefender Internet Security 2012 ist sowohl für Profis als auch für Computer-Neulinge geeignet. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

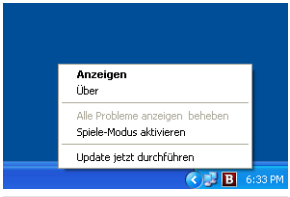
Um den Produktstatus abzurufen und grundlegende Aufgaben auszuführen, steht Ihnen das Bitdefender-Symbol in der Task-Leiste jederzeit zur Verfügung.

Über das Hauptfenster erhalten Sie schnellen Zugriff auf die Produktmodule und wichtige Produktinformationen. Zudem können Sie von hier aus die gebräuchlichsten Aufgaben ausführen.

Sie finden im Einstellungsfenster alle notwendigen Tools, um Ihr Bitdefender-Produkt im Detail zu konfigurieren und fortgeschrittene administrative Aufgaben durchzuführen.

3.1. Task-Leisten-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 das Bitdefender-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Bitdefender erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.
- **Alle Risiken beheben** - hilft bestehende Sicherheitsschwachstellen zu entfernen.Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme.Für weitere Informationen lesen Sie bitte *„Probleme beheben“ (S. 12)*.
- **Spiele-Modus An / Aus** - aktiviert / deaktiviert den Spiele-Modus.
- **Jetzt Aktualisieren** - startet ein sofortiges Update.Sie können den Update-Status im Update-Bereich des Bitdefender-Hauptfensters verfolgen.

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

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

Nicht-kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.

Das Produkt arbeitet im Spiele-Modus.

Bitdefender Auto Pilot is engaged.

Wenn Bitdefender nicht aktiv ist, ist das Symbol in der Task-Leiste 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.

3.2. Hauptfenster

Im Bitdefender-Hauptfenster können Sie häufige Aufgaben durchführen, Sicherheitsprobleme schnell und einfach beheben, Informationen über Ereignisse in der Programmausführung anzeigen und die Produkteinstellungen personalisieren.Und das alles mit nur wenigen Klicks.

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Obere Symbolleiste
: Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen und auf wichtige Aufgaben zugreifen.

Tafelbereich
: Hier können Sie die Hauptmodule von Bitdefender verwalten.

Zusätzlich finden Sie eine Reihe nützlicher Links im unteren Bereich des Fensters:

Link	Beschreibung
Ihre Meinung	Öffnet eine Webseite in Ihrem Browser, auf der Sie gebeten werden, an einer kurzen Umfrage zu Ihren Erfahrungen bei der Nutzung des Produkts teilzunehmen.Wir sind auf Ihre Meinung angewiesen, um die Bitdefender-Produkte immer weiter verbessern zu können.
Registrierung fertigstellen / MyBitdefender	Öffnet das Fenster für das MyBitdefender-Konto, von dem aus Sie ein Konto anlegen bzw. sich bei Ihrem Konto anmelden können.Sie benötigen ein MyBitdefender-Konto, um Updates zu erhalten und die Online-Funktionen Ihres Produkts nutzen zu können.Weitere Informationen zum Erstellen eines Benutzerkontos und zu den Vorteilen eines solchen Kontos finden Sie im Kapitel *„Anmelden bei MyBitdefender“* (S. 9).
Lizenzinfo	Öffnet ein Fenster, in dem die aktuellen Lizenzschlüsselinformationen angezeigt werden und in dem aus Sie einen neuen Lizenzschlüssel registrieren können.
Hilfe und Support	Klicken Sie auf diesen Link, wenn Sie Hilfe zu Bitdefender benötigen.

Link	Beschreibung
	Hiermit werden Fragezeichen in verschiedenen Bereichen des Bitdefender-Fenster eingeblendet, mit denen Sie schnellen Zugriff auf Informationen zu den verschiedenen Elementen der Bedienoberfläche erhalten. Bewegen Sie den Mauszeiger über ein Fragezeichen, um eine Kurzinformation über das Element daneben zu erhalten.

3.2.1. Obere Symbolleiste

Die obere Symbolleiste enthält die folgenden Elemente:

- **Sicherheitsstatusbereich** Dieser befindet sich auf der linken Seite der Symbolleiste und enthält Informationen darüber, ob Probleme die Sicherheit Ihres Computers beeinträchtigen und hilft Ihnen, diese zu beheben.

  Die Farbe des Sicherheitsstatusbereichs verändert sich abhängig von den erkannten Problemen. Zudem werden unterschiedliche Meldungen angezeigt:

  - **Der Bereich ist grün markiert.** Es müssen keine Probleme behoben werden.Ihr Rechner und Ihre Daten sind geschützt.
  - **Der Bereich ist gelb markiert.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt.Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
  - **Der Bereich ist rot markiert.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.Sie sollten sich umgehend um diese Probleme kümmern.

  Klicken Sie auf die Schaltfläche **Probleme anzeigen** in der Mitte der Symbolleiste oder auf eine beliebige Stelle im Sicherheitsstatusbereich links daneben, um einen Assistenten aufzurufen, mit dem Sie alle Bedrohungen leicht und schnell von Ihrem Computer entfernen können.Für weitere Informationen lesen Sie bitte *„Probleme beheben“* (S. 12).

- **Ereignisse** Hier können Sie eine detaillierte Übersicht aller relevanten Ereignisse abrufen, die aufgetreten sind, während das Produkt aktiv war.Für weitere Informationen lesen Sie bitte *„Ereignisse“* (S. 14).
- **Einstellungen** Öffnet das Einstellungsfenster, über das Sie die Produkteinstellungen konfigurieren können.Für weitere Informationen lesen Sie bitte *„Einstellungsfenster“* (S. 26).
- **Auto-Pilot** Hier können Sie den Auto-Pilot aktivieren und den unauffälligen Hintergrundschutz für sich arbeiten lassen.Für weitere Informationen lesen Sie bitte *„Auto-Pilot“* (S. 15).

3.2.2. Tafelbereich

Im Tafelbereich können Sie die Bitdefender-Module direkt verwalten.

Sie können die Tafeln nach Ihren Wünschen frei anordnen.Um diesen Bereich nach Ihren Anforderungen neu zu organisieren, können Sie die einzelnen Tafeln per Drag & Drop verschieben.

Benutzen Sie die Schieber unterhalb des Tafelbereichs oder die Pfeile auf der rechten und linken Seite, um durch die einzelnen Bereiche zu navigieren.

Jede Modultafel enthält die folgenden Elemente, von oben nach unten:

- Der Name des Moduls.
- Eine Statusmeldung.
- Das Modul-Symbol.Klicken Sie auf ein Modul-Symbol, um die entsprechenden Einstellungen im Einstellungsfenster vorzunehmen.
- Eine Schaltfläche, mit der Sie wichtige Aufgaben im Zusammenhang mit dem Modul ausführen können.
- Auf vielen Tafeln gibt es einen Schalter, mit dem Sie eine wichtige Funktion des Moduls aktivieren oder deaktivieren können.

In diesem Bereich stehen Ihnen die folgenden Tafeln zur Verfügung:

Virenschutz

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

Im Bereich Virenschutz können Sie schnell und einfach auf wichtige Scan-Aufgaben zugreifen.Klicken Sie auf **Jetzt scannen** und wählen Sie dann eine Aufgabe aus dem Dropdown-Menü:

- Quick Scan
- Vollständiger System-Scan
- Benutzerdefinierter Scan
- Schwachstellen Scan
- Rettungsmodus

Mit dem **Auto-Scan**-Schalter können Sie den Auto-Scan aktivieren oder deaktivieren.

Weitere Informationen zu den Scan-Aufgaben und eine Anleitung, wie Sie den Virenschutz konfigurieren können, finden Sie im Kapitel „*Virenschutz*“ (S. 40).

Firewall

Die Firewall schützt Sie, während Sie mit Netzwerken und dem Internet verbunden sind, indem alle Verbindungsversuche gefiltert werden.

Klicken Sie im Bereich Firewall auf **Netzwerkdetails**, um die Einstellungen für die Netzwerkverbindung zu konfigurieren.

Mit dem Schalter für die Firewall können Sie den Firewall-Schutz aktivieren oder deaktivieren.

Warnung

Die Deaktivierung der Firewall sollte immer nur von kurzer Dauer sein, da Ihr Computer so der Gefahr durch nicht autorisierte Verbindungen ausgesetzt wird.Aktivieren Sie die Firewall so schnell wie möglich wieder.

Weitere Informationen zur Firewall-Konfiguration finden Sie im Kapitel *„Firewall“* (S. 100).

Spam-Schutz

Das Spam-Schutz-Modul von Bitdefender stellt sicher, dass Ihr Posteingang von unerwünschten E-Mails frei bleibt, indem es den POP3-Nachrichtenverkehr filtert.

Klicken Sie im Bereich Spam-Schutz auf **Verwalten** und wählen Sie aus dem Dropdown-Menü den Punkt Freunde oder Spammer, um die entsprechende Adressenliste zu bearbeiten.

Mit dem Schalter für den Spam-Schutz können Sie den Spam-Schutz aktivieren oder deaktivieren.

Weitere Informationen zur Konfiguration des Spam-Schutzes finden Sie im Kapitel *„Spam-Schutz“* (S. 66).

Update

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

Standardmäßig sucht Bitdefender stündlich nach neuen Updates. Sie können die automatischen Updates mithilfe des **Auto-Update**-Schalters im Update-Bereich deaktivieren.

Warnung

Hierbei handelt es sich um ein großes Sicherheitsrisiko. Wir empfehlen, die Deaktivierung des automatischen Updates so kurz wie möglich zu halten, da Bitdefender Sie nur gegen die neuesten Bedrohungen schützen kann, wenn die Software immer auf dem neuesten Stand ist.

Klicken Sie in diesem Bereich auf **Update jetzt durchführen**, um ein sofortiges Update zu veranlassen.

Weitere Informationen über die Konfiguration von Updates finden Sie im Kapitel *„Update“* (S. 115).

Jugendschutz

Mit Bitdefender Internet Security 2012 erhalten Sie umfangreiche Funktionen für die Kindersicherung, mit denen Sie die Computer-Aktivitäten Ihrer Kinder sicherer machen und überwachen können.

Klicken Sie auf **Konten verwalten** im Bereich der Kindersicherung, um die Einstellungen für die Windows-Benutzerkonten auf Ihrem Computer zu konfigurieren.

Weitere Informationen zur Konfiguration der Kindersicherung finden Sie in Kapitel *„Jugendschutz“ (S. 84)*.

Privatsphärenschutz

Das Modul für den Privatsphärenschutz hilft Ihnen dabei, das wichtige persönliche Daten nicht in fremde Hände gelangen.Während Sie im Internet sind, schützt es Sie vor Phishing-Attacken, Betrugsversuchen, Missbrauch Ihrer privaten Daten und vielem mehr.

Klicken Sie im Bereich Privatsphärenschutz auf **Regeln verwalten**, um in den Bereich des Datenschutzes zu gelangen, in dem Sie die Privatsphärenregeln konfigurieren können.

Mit dem Schalter für den Phishing-Schutz, können Sie den Phishing-Schutz aktivieren oder deaktivieren.

Weitere Informationen, wie man Bitdefender zum Schutz Ihrer Privatsphäre konfigurieren kann, finden Sie im Kapitel *„Privatsphärenschutz“ (S. 77)*.

Netzwerkplan

Der Netzwerkplan macht es Ihnen einfach, die Sicherheit aller Computer bei Ihnen Zuhause von nur einem Computer aus zu verwalten.

Um zu beginnen, klicken Sie auf **Verwalten** im Bereich Netzwerkplan und wählen Sie dann **Netzwerk aktivieren**.

Sobald das Netzwerk aktiviert ist, erhalten Sie durch einen Klick auf die **Verwalten**-Schaltfläche im Bereich Netzwerkplan Zugriff auf die folgenden Optionen:

- **Verbindung deaktivieren** - Deaktiviert das Netzwerk.
- **Alle scannen** - Startet einen Schnell-Scan des gesamten Systems für alle verwalteten Computer.
- **Alle Computer aktualisieren** - Aktualisiert die Bitdefender-Produkte auf den verwalteten Computern.

Für weitere Informationen lesen Sie bitte *„Netzwerkplan“ (S. 111)*.

Safego

Um Sie bei der Nutzung von Facebook zu schützen, können Sie Safego, eine Bitdefender-Sicherheitslösung für soziale Netzwerke, direkt aus Ihrem Produkt heraus aufrufen.

Klicken Sie auf **Aktivieren**, um Safego von Ihrem Facebook-Konto aus zu aktivieren und zu verwalten.

Wenn Sie Safego bereits aktiviert haben, können Sie Zugriffsstatistiken hinsichtlich der Aktivität der Anwendung mit einem Klick auf die Schaltfläche **Berichte anzeigen** aufrufen.

Für weitere Informationen lesen Sie bitte *„Safego-Schutz für soziale Netzwerke“ (S. 119)*.

3.3. Einstellungsfenster

Über das Einstellungsfenster erhalten Sie Zugriff auf alle Produktkomponenten und persönlichen Benutzereinstellungen.Hier können Sie Bitdefender im Detail konfigurieren.

Auf der linken Seite des Fensters sehen Sie ein Menu, das alle Sicherheitsmodule beinhaltet:Jedes Modul verfügt über ein oder mehrere Tabs in welchem Sie die dazugehörigen Sicherheitseinstellungen konfigurieren oder Sicherheits- und administrative Aufgaben durchführen können. Die folgende Auflistung beschreibt in Kürze jedes Modul.

Allgemein

Hier können Sie allgemeine Produkteinstellungen vornehmen, so zum Beispiel für das Einstellungspasswort, den Spiele-Modus, die Proxy-Einstellungen und die Statusbenachrichtigungen.

Virenschutz

Hier können Sie Ihren Malware-Schutz konfigurieren, Systemschwachstellen identifizieren und beheben, Scan-Ausschlüsse festlegen und Dateien in Quarantäne verwalten.

Spam-Schutz

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

Jugendschutz

Hier können Sie Ihre Kinder gegen jugendgefährdende Inhalte schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

Privatsphärenschutz

Hier können Sie Datendiebstahl von Ihrem Computer verhindern und Ihre Privatsphäre bei Surfen im Internet schützen.Konfigurieren Sie den Schutz für Ihren Browser und Ihre Sofortnachrichten-Software, verwalten Sie den Datenschutz und vieles mehr.

Firewall
: Hier können Sie allgemeine Firewall-Einstellungen vornehmen, Firewall-Regeln festlegen, die Angriffserkennung konfigurieren und die Netzwerkaktivität überwachen.

Netzwerkplan
: Hier können Sie alle Bitdefender-Produkte, die auf Ihren Heimrechnern installiert sind, von nur einem Computer aus konfigurieren und verwalten.

Update
: Hier können Sie Informationen zu den neusten Updates abrufen, das Produkt aktualisieren und den Update-Vorgang im Detail konfigurieren.

Zusätzlich finden Sie eine Reihe nützlicher Links im unteren Bereich des Fensters:

Link	Beschreibung
Ihre Meinung	Öffnet eine Webseite in Ihrem Browser, auf der Sie gebeten werden, an einer kurzen Umfrage zu Ihren Erfahrungen bei der Nutzung des Produkts teilzunehmen.Wir sind auf Ihre Meinung angewiesen, um die Bitdefender-Produkte immer weiter verbessern zu können.
Registrierung fertigstellen / MyBitdefender	Öffnet das Fenster für das MyBitdefender-Konto, von dem aus Sie ein Konto anlegen bzw. sich bei Ihrem Konto anmelden können.Sie benötigen ein MyBitdefender-Konto, um Updates zu erhalten und die Online-Funktionen Ihres Produkts nutzen zu können.Weitere Informationen zum Erstellen eines Benutzerkontos und zu den Vorteilen eines solchen Kontos finden Sie im Kapitel *„Anmelden bei MyBitdefender“* (S. 9).
Lizenzinfo	Öffnet ein Fenster, in dem die aktuellen Lizenzschlüsselinformationen angezeigt werden und in dem aus Sie einen neuen Lizenzschlüssel registrieren können.
Hilfe und Support	Klicken Sie auf diesen Link, wenn Sie Hilfe zu Bitdefender benötigen.
	Hiermit werden Fragezeichen in verschiedenen Bereichen des Bitdefender-Fenster eingeblendet, mit denen Sie schnellen Zugriff auf Informationen zu den verschiedenen Elementen der Bedienoberfläche erhalten. Bewegen Sie den Mauszeiger über ein Fragezeichen, um eine Kurzinformation über das Element daneben zu erhalten.

Um in das Hauptfenster zurückzukehren, klicken Sie der oberen rechten Ecke des Fensters auf **Heim**.

4. Gewusst wie

Dieses Kapitel führt Sie Schritt für Schritt durch die Konfiguration der am häufigsten verwendeten Einstellungen und die Durchführung der gebräuchlichsten Aufgaben mit Bitdefender.Einige der Themen enthalten Verweise auf andere Themen, die Ihnen weiterführende Informationen liefern.

4.1. Wie kann ich eine Testversion registrieren?

Wenn Sie eine Testversion installiert haben, können Sie diese nur für einen begrenzten Zeitraum benutzen.Um Bitdefender auch nach Ablauf der Testphase nutzen zu können, müssen Sie Ihr Produkt mit einem Lizenzschlüssel registrieren und ein MyBitdefender-Benutzerkonto anlegen.

- Um Bitdefender zu registrieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie im unteren Bereich des Fensters auf **Lizenzinfo**.Das Registrierungsfenster wird eingeblendet.
3. Geben Sie den Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.

   Wenn Sie keinen Lizenzschlüssel haben, klicken Sie in dem Fenster auf den entsprechenden Link. Dieser führt Sie auf eine Website, auf der Sie einen Lizenzschlüssel erwerben können.
4. Warten Sie bis der Registrierungsvorgang abgeschlossen ist und schließen Sie dann das Fenster.

- Um ein MyBitdefender-Konto anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie am unteren Fensterrand auf **Registrierung fertigstellen**.Das Kontofenster wird angezeigt.
3. Wählen Sie den entsprechenden Link, um ein neues Konto anzulegen.
4. Geben Sie die Daten in die entsprechenden Felder ein.Die hier eingetragenen Daten bleiben vertraulich.

   Klicken Sie auf **Übermitteln**.
5. Rufen Sie Ihre E-Mails ab und befolgen Sie die erhaltenen Anweisungen, um die Registrierung abzuschließen.

Beachten Sie

Sie können die angegebene E-Mail-Adresse und das Passwort benutzen, um sich an Ihrem Konto unter http://my.bitdefender.com anzumelden.

4.2. Wie registriere ich Bitdefender ohne eine Internet-Verbindung?

Wenn Sie Bitdefender gerade erworben haben und über keine Internet-Verbindung verfügen, können Sie Bitdefender auch offline registrieren.

Um Bitdefender mit Ihrem Lizenzschlüssel zu registrieren, gehen Sie folgendermaßen vor:

1. Finden Sie einen PC, der über eine Internet-Verbindung verfügt.Sie können zum Beispiel den Computer eines Freundes verwenden oder den PC in einer öffentlichen Einrichtung.
2. Rufen Sie die Seite https://my.bitdefender.com auf, um ein MyBitdefender-Konto anzulegen.

3. Melden Sie sich bei Ihrem Benutzerkonto an und wählen Sie den Punkt **Offline-Registrierung anfordern**.
4. Geben Sie den von Ihnen erworbenen Lizenzschlüssel ein.
5. Klicken Sie auf **Senden**, um einen Bestätigungscode zu erhalten.

   Wichtig
   Notieren Sie sich den Bestätigungscode.

6. Kehren Sie mit dem Bestätigungscode an Ihren PC zurück.
7. Öffnen Sie das Bitdefender-Fenster.
8. Klicken Sie im unteren Bereich des Fensters auf **Lizenzinfo**.Das Registrierungsfenster wird eingeblendet.
9. Wählen Sie die Option zur Registrierung des Produkts mit einem Bestätigungscode.
10. Geben Sie den Bestätigungscode in das entsprechende Feld ein und klicken Sie auf **Senden**.
11. Warten Sie bis der Registrierungsvorgang abgeschlossen ist und klicken Sie auf **Fertigstellen**.

4.3. Wie führe ich ein Upgrade auf ein anderes Bitdefender-2012-Produkt durch?

Das Upgrade von einem Bitdefender-2012-Produkt auf ein anderes ist Kinderleicht.

Gehen wir von folgendem Szenario aus: Sie nutzen Bitdefender Internet Security 2012 bereits seit einer Weile und haben sich nun entschieden, auf Bitdefender Total Security 2012 und die zusätzlichen Funktionen des Produkts umzusteigen.

Sie müssen lediglich einen Lizenzschlüssel für das Bitdefender-2012-Produkt erwerben, für das Sie ein Upgrade durchführen wollen und diesen in das Registrierungsfenster des Bitdefender-2012-Produkts eingeben, das Sie derzeit benutzen.

Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie im unteren Bereich des Fensters auf **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 den Anweisungen, um das Upgrade durchzuführen.

4.4. Wann sollte ich Bitdefender neu installieren?

Es gibt Situationen, die es erforderlich machen könnten, dass Sie Ihr Bitdefender-Produkt erneut installieren.

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

- Sie haben das Betriebssystem neu installiert.
- Sie haben einen neuen Computer erworben.
- Sie wollen die Anzeigesprache der Bitdefender-Benutzeroberfläche ändern.

Um Bitdefender neu zu installieren, können Sie die von Ihnen erworbene Installations-CD verwenden oder eine neue Version von der Bitdefender-Website herunterladen.

Während der Installation werden Sie aufgefordert, das Produkt mit Ihrem Lizenzschlüssel zu registrieren.

Falls Sie Ihren Lizenzschlüssel verloren haben, können Sie sich unter https://my.bitdefender.com bei Ihrem Benutzerkonto anmelden, um ihn abzurufen.Geben Sie die E-Mail-Adresse und das Kennwort Ihres Kontos in die entsprechenden Felder ein.

4.5. Wann läuft der Bitdefender-Schutz aus?

Um herauszufinden, wie viele Tage Ihr Lizenzschlüssel noch gültig ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie im unteren Bereich des Fensters auf **Lizenzinfo**.
3. In dem Fenster **Registrieren Sie Ihr Produkt** wird Ihnen angezeigt, wie viele Tage die Lizenz noch gültig ist.

4.6. Wie verlängere ich meinen Bitdefender-Schutz?

Wenn Ihr Bitdefender-Schutz auszulaufen droht, müssen Sie Ihren Lizenzschlüssel erneuern.

- Um eine Website aufzurufen, auf der Sie Ihren Bitdefender-Lizenzschlüssel erneuern können, gehen Sie folgendermaßen vor:

  1. Öffnen Sie das Bitdefender-Fenster.
  2. Klicken Sie im unteren Bereich des Fensters auf **Lizenzinfo**.

3. Klicken Sie auf **Sie haben keinen Lizenzschlüssel? Kaufen Sie jetzt einen!**
4. In Ihrem Browser öffnet sich eine Webseite, auf der Sie einen Bitdefender-Lizenzschlüssel erwerben können.

Beachten Sie
Alternativ können Sie auch den Einzelhändler kontaktieren, von dem Sie Ihr Bitdefender-Produkt erworben haben.

- Um Ihr Bitdefender-Produkt mit dem neuen Lizenzschlüssel zu registrieren, gehen Sie folgendermaßen vor:
  1. Öffnen Sie das Bitdefender-Fenster.
  2. Klicken Sie im unteren Bereich des Fensters auf **Lizenzinfo**.Das Registrierungsfenster wird eingeblendet.
  3. Geben Sie den Lizenzschlüssel ein und klicken Sie auf **Jetzt registrieren**.
  4. Warten Sie bis der Registrierungsvorgang abgeschlossen ist und schließen Sie dann das Fenster.

Wenn Sie weitere Informationen benötigen, kontaktieren Sie den Bitdefender-Support wie in Abschnitt *„Support“ (S. 145)* beschrieben.

4.7. Welches Bitdefender-Produkt nutze ich?

Um zu erfahren, welche Bitdefender-Anwendung bei Ihnen installiert ist, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Am oberen Rand des Fensters sollten Sie einen der folgenden Schriftzüge sehen:
   - Bitdefender Antivirus Plus 2012
   - Bitdefender Internet Security 2012
   - Bitdefender Total Security 2012

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

Um eine Datei oder einen Ordner zu scannen, rechtsklicken Sie auf das Objekt, das Sie scannen möchten und wählen Sie dann **Mit Bitdefender scannen** aus dem Menü. Dies ist der einfachste und empfohlene Weg.Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten.

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

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.

- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihren Rechner kopieren.

4.9. Wie scanne ich mein System?

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Vollständigen System-Scan** aus dem Dropdown-Menü.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen.

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

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

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Benutzerdefinierter Scan** aus dem Dropdown-Menü.
4. Klicken Sie auf **Ziel hinzufügen**, um die zu scannenden Dateien oder Verzeichnisse auszuwählen.
5. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Scan-Optionen**.

   Sie können auch die Option **Computer herunterfahren** auswählen.

   Falls während des Scans keine Bedrohungen gefunden werden, wird Ihr Computer nach Beendigung des Scans heruntergefahren.Bitte beachten Sie, dass dies das Standardverhalten beim Ausführen dieser Aufgabe ist.
6. Klicken Sie auf **Scan starten**, um die Ausgabe auszuführen.

4.11. Wie kann ich einen Ordner vom Scan ausnehmen?

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

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

- Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.
- Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren.Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

Um den Ordner des Ausschlussliste hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**.
5. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
6. Klicken Sie auf **Durchsuchen**, wählen Sie den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**.
7. Klicken Sie auf **Hinzufügen** und danach auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

4.12. Was ist zu tun, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

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

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
   c. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um den **Zugriff-Scan** zu deaktivieren.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 154).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.

c. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Quarantäne**.

d. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.

4. Fügen Sie die Datei zur Ausschlussliste hinzu.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich einen Ordner vom Scan ausnehmen?“ (S. 33)*.
5. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.
6. Setzten Sie sich mit unseren Support-Mitarbeitern in Verbindung, damit wir die Erkennungssignatur entfernen können.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“ (S. 146)*.

4.13. Wie lege ich Windows-Benutzerkonten an?

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. Melden Sie sich an Ihrem 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 "Eingeschränkt" und dann "Benutzerkonto anlegen". Eingeschränkte 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. Melden Sie sich an Ihrem 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". Eingeschränkte 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.

4.14. Wie kann ich meine Kinder vor Bedrohungen aus dem Internet schützen?

Die Kindersicherung von Bitdefender ermöglicht es, den Zugriff auf das Internet und bestimmte Applikationen zu beschränken, um so zu verhindern, dass sich Ihre Kinder unangemessene Inhalte ansehen, wenn Sie nicht anwesend sind.

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

- Unangemessene Webseiten.
- Den Internet-Zugang zu bestimmten Zeiten (beispielsweise während Unterrichtszeiten).
- Webseiten, E-Mail-Nachrichten und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Sofortnachrichtenprogramme, Filesharing-Software usw.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

Um die Kindersicherung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Erstellen Sie eingeschränkte (Standard-) Windows-Benutzerkonten für Ihre Kinder.Für weitere Informationen lesen Sie bitte *„Wie lege ich Windows-Benutzerkonten an?“* (S. 35).
2. 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.

3. Konfigurieren Sie die Kindersicherung für die Windows-Benutzerkonten Ihrer Kinder.
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Gehen Sie in den Bereich **Kindersicherung**.
   c. Klicken Sie auf **Konten verwalten** und stellen Sie sicher, dass die Kindersicherung für das Benutzerkonto Ihres Kindes aktiviert ist.
   d. Geben Sie das Alter Ihres Kindes an, indem Sie auf das dem **Alter** entsprechende Kästchen klicken.Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.
   e. Wenn Sie die Einstellungen für die Kindersicherungen im Detail konfigurieren möchten, klicken Sie auf **Einstellungen**.

Detaillierte Informationen zur Verwendung der Kindersicherung finden Sie im Kapitel „*Jugendschutz*“ (S. 84).

4.15. Wie kann ich die Blockierung einer Website durch die Kindersicherung wieder aufheben?

Mit der Bitdefender-Kindersicherung können Sie steuern, auf welche Inhalte Ihre Kinder zugreifen können, wenn Sie den Computer nutzen.

Wenn Sie in der Kindersicherung eine Alterskategorie für Ihr Kind festgelegt haben und nur ein Windows-Benutzerkonto nutzen, können Sie keine Webseiten aufrufen, die als ungeeignet für die gewählte Alterskategorie eingestuft wurden.

Wenn der Zugriff auf eine Website von der Kindersicherung blockiert wird, können Sie eine Regel erstellen, die den Zugriff auf diese Website ausdrücklich erlaubt.

Um den Zugriff auf eine bestimmte Website zu erlauben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den Bereich **Kindersicherung**.
3. Klicken Sie auf **Konten verwalten**.
4. Klicken Sie auf **Einstellungen**, um die Benutzereinstellungen zu konfigurieren.
5. Klicken Sie auf **Website erlauben**.
6. Geben Sie die Webseiten Adresse in das **Webseite** Feld ein.
7. Wählen Sie die gewünschte Aktion für diese Regel aus - **Zulassen** und danach auf **Fertigstellen** klicken, um die Regel hinzuzufügen.
8. Öffnen Sie Ihren Browser und rufen Sie die Website auf.

4.16. Wie schütze ich meine persönlichen Daten?

Der Privatsphärenschutz überwacht die Daten, die von Ihrem Computer aus per Internet-Formular, E-Mail oder Sofortnachricht übertragen werden.

Um sicherzustellen, dass persönliche Daten Ihren Computer nicht ohne Ihre Zustimmung verlassen, müssen Sie geeignete Datenschutzregeln und Ausnahmen von diesen Regeln festlegen.

Die Datenschutzregeln legen die Informationen fest, die blockiert werden sollen.

Um eine Datenschutzregel anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Privatsphärenschutz** und danach auf den Reiter **Datenschutz**.
4. Wenn der **Datenschutz** deaktiviert ist, aktivieren Sie ihn mithilfe des entsprechenden Schalters.
5. Wählen Sie die Option **Regel hinzufügen**, um den Assistenten für den Datenschutz zu starten.
6. Befolgen Sie die Anweisungen des Assistenten.

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

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

Wichtig

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

Um die Proxy-Einstellungen zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Allgemein** und danach auf den Reiter **Erweitert**.
4. Klicken Sie im Bereich **Proxy-Einstellungen** auf den Schalter, um die Proxy-Nutzung zu aktivieren.

5. Klicken Sie auf den Link **Proxyverwaltung**
6. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollten der Proxy-Server einen Benutzernamen und ein Passwort erfordern, müssen Sie diese in den entsprechenden Feldern angeben.

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

   - **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können.Die folgenden Einstellungen müssen angegeben werden:
     - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
     - **Port** - Geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
     - **Benutzername** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
     - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

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

Wichtig
Denken Sie daran, die Proxy-Nutzung zu deaktivieren, wenn Sie zu einer direkten Internet-Verbindung wechseln.

5. Virenschutz

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

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

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

  Wichtig
  Um zu verhindern, dass Viren Ihren Computer infizieren, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- On-demand Prüfung - 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.

  Wenn Auto-Scan aktiviert ist, besteht kaum noch ein Bedarf, Malware-Scans manuell auszuführen.Auto-Scan wird Ihren Computer immer wieder scannen und die notwendigen Maßnahmen einleiten, wenn Malware erkannt wird.Der Auto-Scan wird nur ausgeführt, wenn ausreichend Systemressourcen zur Verfügung stehen, damit die Geschwindigkeit Ihres Computers nicht beeinträchtigt wird.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Computer verbunden sind, um einen sicheren Zugriff zu garantieren.Für weitere Informationen lesen Sie bitte *„Automatischer Scan von Wechselmedien“ (S. 54)*.

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht wollen, dass bestimmte Dateien oder Dateitypen gescannt werden.Für weitere Informationen lesen Sie bitte *„Konfiguration der Scan-Ausschlüsse“ (S. 56)*.

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.Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“ (S. 58)*.

Wenn Ihr Computer mit Malware infiziert ist, siehe *„Malware von Ihrem System entfernen“ (S. 136)*.Um Ihnen bei der Entfernung von Malware zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden kann, stellt Bitdefender Ihnen einen Rettungsmodus zur Verfügung.Dabei handelt es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Malware dient und

es Ihnen ermöglicht, Ihren Computer unabhängig von Windows zu starten.Wenn der Computer im Rettungsmodus läuft, ist Windows-Malware inaktiv, wodurch sie sich leicht entfernen lässt.

Um Sie vor unbekannten schädlichen Anwendung zu schützen, nutzt Bitdefender mit Active Virus Control eine fortschrittliche heuristische Technologie, die alle Anwendungen auf Ihrem System ununterbrochen überwacht.Active Virus Control blockiert automatisch Anwendungen, die sich wie Malware verhalten, um zu verhindern, dass Sie Ihren Computer beschädigen.Mitunter werden auch legitime Anwendungen blockiert. In diesen Fällen können Sie Active Virus Control durch die Festlegung von Ausschlussregeln so konfigurieren, dass diese Anwendungen nicht noch einmal blockiert werden.Für weitere Informationen lesen Sie bitte das Kapitel *„Active Virus Control“* (S. 59).

Viele Malware-Typen sind darauf ausgelegt, Schwachstellen wie fehlende Updates des Betriebssystems oder veraltete Anwendungen auszunutzen, um Ihr System zu infizieren.Bitdefender hilft Ihnen dabei, Systemschwachstellen schnell und einfach zu identifizieren und zu beheben, um Ihren Computer besser vor Malware und Hacker-Angriffen zu schützen.Für weitere Informationen lesen Sie bitte *„Beheben von Systemschwachstellen“* (S. 62).

5.1. Zugriff-Scans (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 Sicherheitsstufe wählen.Wenn Sie ein fortgeschrittener Benutzer sind, können Sie die Scan-Einstellungen auch selbst im Detail konfigurieren, indem Sie eine benutzerdefinierte Schutzstufe definieren.

5.1.1. Überprüfen von Malware, die vom Zugriff-Scan erkannt wurde

Um Malware zu überprüfen, die vom Zugriff-Scan erkannt wurde, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Viren-Scan**.Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.

4. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.

5.1.2. Anpassen der Echtzeitsicherheitsstufe

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

Um die Echtzeitsicherheitsstufe anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Schieben Sie den Regler in die gewünschte Sicherheitsstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite, um die Sicherheitsstufe zu wählen, die am besten für Ihre Bedürfnisse geeignet ist.

5.1.3. Festlegen einer benutzerdefinierten Sicherheitsstufe

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen.Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Sicherheitsstufe festlegen.

Um eine benutzerdefinierte Sicherheitsstufe anzulegen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Klicken Sie auf **Benutzerdefiniert**.
5. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.
6. 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.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scan-Optionen für aufgerufene Dateien.** Sie können Bitdefender so einstellen, dass Dateien oder Anwendungen (Programmdateien) nur bei Zugriff gescannt werden.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:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Inhalt von Archiven 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.

  Wenn Sie sich entscheiden, diese Option zu nutzen, können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen.Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

- **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 und ausgehende E-Mails
  - ▶ 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).

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Nur neue und veränderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.

5.1.4. Wiederherstellen der Standardeinstellungen

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

Um die Standardeinstellungen für den Echtzeitschutz wiederherzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Klicken Sie auf **Standard**.

5.1.5. Aktivieren / Deaktivieren des Echtzeitschutzes

Um den Echtzeitschutz vor Malware zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Klicken Sie auf den Schalter, um den Zugriff-Scan zu aktivieren oder deaktivieren.
5. Wenn Sie den Echtzeitschutz deaktivieren möchten erscheint ein Warnfenster.Sie müssen die Deaktivierung bestätigen indem Sie wählen wie lange der Schutz deaktiviert werden soll. Zur Auswahl stehen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.

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

5.1.6. Verfügbare Aktionen für gefundene Malware

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.Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Bitdefender nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist.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 einzudämmen.

  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.

- Wenn eine verdächtige Datei gefunden wird, wird sie in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

5.2. On-Demand Prüfung

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.

Der Prüfvorgang basiert auf Prüfaufgaben welche die Einstellungen zum Vorgang sowie die zu prüfenden Objekte beinhalten.Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen.Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

5.2.1. Auto-Scan

Auto-Scan ist ein Bedarf-Scan, der Ihre Daten im Hintergrund nach Malware scannt und die notwendigen Maßnahmen ergreift, um gefundene Infektionen zu entfernen.Auto-Scan findet und nutzt Zeitabschnitte, während derer die Auslastung der Systemressourcen unter einen bestimmten Grenzwert fällt, um regelmäßige Scans des gesamten Systems durchzuführen.

Die Vorteile von Auto-Scan:

- Der Auswirkungen auf das System sind minimal.
- Wenn Sie einen Voraus-Scan der gesamten Festplatte durchführen, werden nachfolgenden Bedarf-Scans wesentlich schneller abgeschlossen.
- Zudem wird der Zugriff-Scan wesentlich weniger Zeit in Anspruch nehmen.

Um den Auto-Scan zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf den Schalter, um den Auto-Scan zu aktivieren oder deaktivieren.

5.2.2. Eine Datei oder einen Ordner nach Malware 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 Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

5.2.3. Ausführen eines Quick Scans

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

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Quick Scan** aus dem Dropdown-Menü.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen.

5.2.4. Ausführen eines vollständigen System-Scans

Der vollständige System-Scan scannt den gesamten Computer nach allen Malware-Typen, die ein Sicherheitsrisiko darstellen, so zum Beispiel Viren, Spyware, Adware, Rootkits usw.Wenn Sie Auto-Scan deaktiviert haben, empfiehlt es sich, mindestens einmal pro Woche einen vollständigen System-Scan durchzuführen.

Beachten Sie
Da ein **Vollständiger System-Scan** einen gründlichen Scan des gesamten Systems durchführt, kann dieser einige Zeit in Anspruch nehmen. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

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

- Stellen Sie sicher, dass die Malware-Signaturen von Bitdefender immer auf dem neuesten Stand sind. Wenn Sie Ihren Computer auf Grundlage einer veralteten Signaturdatenbank scannen, könnte dies verhindern, dass Bitdefender neue Malware erkennt, die seit dem letzten Update entdeckt wurde.Für weitere Informationen lesen Sie bitte *„Update“ (S. 115)*.
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.Für weitere Informationen lesen Sie bitte *„Konfigurieren und Ausführen eines benutzerdefinierten Scans“ (S. 48)*.

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Vollständigen System-Scan** aus dem Dropdown-Menü.
4. Folgen Sie den Anweisungen des Viren-Scan-Assistenten, um den Scan abzuschließen.

5.2.5. Konfigurieren und Ausführen eines benutzerdefinierten Scans

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

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Benutzerdefinierter Scan** aus dem Dropdown-Menü.
4. Klicken Sie auf **Ziel hinzufügen**, markieren Sie die Kästchen für die Bereiche, die Sie nach Malware durchsuchen wollen, und klicken Sie auf **OK**.
5. Klicken Sie auf **Scan-Optionen**, wenn Sie die Scan-Optionen konfigurieren wollen.Ein neues Fenster wird sich öffnen.Folgen Sie diesen Schritten:
   a. 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 der Skala, um die Schutzstufe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

      Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen.Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Benutzerdefiniert**. Weitere Informationen zu den Optionen finden Sie am Ende dieses Kapitels.

   b. Bitdefender versucht standardmäßig, Malware-Code aus infizierten Dateien zu entfernen, oder, sollte die Desinfektion fehlschlagen, die Dateien in die Quarantäne zu verschieben.Sollten beide Aktionen fehlschlagen, werden Sie aufgefordert eine Aktion für die ungelösten Bedrohungen auszuwählen.

      Wenn Sie wollen, dass Malware lediglich erkannt wird, ohne dass irgendwelche Aktionen durchgeführt werden, markieren Sie das entsprechende Kästchen im Bereich **Aktionen**.

   c. Sie können auch folgende allgemeine Optionen konfigurieren:

      - **Aufgabe mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.

- **Scan-Assistent in die Task-Leiste 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:

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

6. Klicken Sie auf **Scan starten** und folgen Sie den Anweisungen des Assistenten für den Viren-Scan, um den Scan abzuschließen.Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateien prüfen.** Sie können Bitdefender so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger gegen Malware-Angriffe als andere Typen oder Dateien.Diese Kategorie beinhaltet die folgenden Dateierweiterungen: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System

nur beeinflussen, wenn die 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.

- **Boot-Sektoren scannen.** Sie können Bitdefender einstellen, damit die Boot-Sektoren gescannt werden.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen.Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies prüfen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und veränderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen.Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.

5.2.6. Antivirus Prüfassistent

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.Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

Beachten Sie

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen.Sehen Sie nach dem  Prüffortschritticon im

Systemtray.Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

Schritt 1 - Scan-Bereiche auswählen

Dieser Schritt erscheint nur, wenn Sie den benutzerdefinierten Scan nutzen.Für weitere Informationen lesen Sie bitte *„Konfigurieren und Ausführen eines benutzerdefinierten Scans“* (S. 48).

Schritt 2 - Führen Sie den Scan durch

Bitdefender startet den Scan der aus gewählten Dateien und Verzeichnisse.

Sie können den Vorgangsstatus und die Statistiken hierzu sehen (Prüfgeschwindigkeit, vergangene Zeit, Anzahl der geprüften / infizierten / verdächtigen / versteckten Objekte).

Bitte warten Sie, bis Bitdefender den Scan beendet hat.

Beachten Sie
Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, 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 geprüft werden, außer wenn Sie das Passwort angeben.Die folgenden Optionen sind verfügbar:

- **Passwort eingeben.** Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an.Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach einem Passwort fragen und dieses Objekt bei der Prüfung überspringen.** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Alle Passwortgeschützte Datein überspringen ohne diese zu Prüfen.** 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 pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Schritt 3 - Wählen Sie entsprechende Aktionen aus

Wenn der Prüfvorgang beendet wurde wird Ihnen ein Fenster angezeigt in welchem Sie eine Zusammenfassung angezeigt bekommen.

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, je nach Malware, mit der sie infiziert sind.Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

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

Keine Aktion durchführen
Es wird keine Aktion für die infizierte Dateien ausgeführt.Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.

Desinfizieren
Den Malware-Code aus den entdeckten infizierten Dateien entfernen.

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 kein Infektionsrisiko?Für weitere Informationen lesen Sie bitte *„Verwalten von Dateien in Quarantäne“ (S. 58)*.

Dateien umbenennen
Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein.Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa.

Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits.Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

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

Schritt 4 - 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. 136).

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.

5.2.7. Überprüfen von Scan-Protokollen

Für jeden Scan wird ein Protokoll erstellt.Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten 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 zu einem späteren Zeitpunkt zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Viren-Scan**.Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.

4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden.Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

5.3. Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Computer verbinden und scannt diese im Hintergrund.Dies ist empfohlen um die Infizierung Ihres Systems durch Viren und andere Malware zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- verbundene (entfernte) Netzlaufwerke

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

5.3.1. Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen im Hintergrund nach Malware zu scannen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist).Ein Bitdefender-Scan-Symbol () erscheint in der Task-Leiste.Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

Wenn der Auto-Pilot aktiviert ist, läuft der Scan ohne Ihr Zutun.Der Scan wird lediglich protokolliert und Sie können die dazugehörigen Informationen im Ereignis-Fenster abrufen.

Wenn der Autopilot deaktiviert ist:

1. Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.
2. Wird ein passwortgeschütztes Archiv während des Scans gefunden, werden Sie unter Umständen um die Eingabe des Passwortes gebeten.Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben.Sie können das Passwort entweder eingeben, den Scan der Datei überspringen oder die Erkennung von passwortgeschützten Archiven deaktivieren.
3. In den meisten Fällen entfernt Bitdefender erkannte Malware automatisch oder isoliert infizierte Dateien in der Quarantäne.Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Beachten Sie

Bitte beachten Sie, dass für infizierte oder verdächtige Dateien auf CDs oder DVDs keine Aktionen durchgeführt werden können. Ebenso können für infizierte oder verdächtige Dateien auf abgebildeten Netzlaufwerken keine Aktionen durchgeführt werden, wenn Sie nicht die über die entsprechenden Rechte verfügen.

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

Diese Informationen könnten sich als hilfreich erweisen:

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

  Um zu erfahren, wie Sie mit Malware umgehen sollen, lesen Sie bitte das Kapitel *„Malware von Ihrem System entfernen“ (S. 136).

5.3.2. Verwalten des Scans für Wechselmedien

Um die automatischen Scans für Wechselmedien zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Wählen Sie im Bereich **Erkannte Geräte scannen** die Arten von Speichermedien aus, die automatisch gescannt werden sollen.Klicken Sie auf die Schalter, um den automatischen Scan zu aktivieren oder deaktivieren.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, den automatischen Scan für alle Arten von Wechselmedien zu aktivieren.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert.Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese zu desinfizieren (d.h. den Malware zu entfernen) oder in die Quarantäne zu verschieben. Sollten

beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen.Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

5.4. Konfiguration der Scan-Ausschlüsse

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

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

Beachten Sie

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**.

5.4.1. Dateien oder Ordner vom Scan ausschließen

Um bestimmte Dateien oder Ordner vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.
5. Klicken Sie auf den Link **Ausgeschlossene Dateien und Ordner**.Es erscheint ein Fenster. Hier können Sie die Dateien und Ordner verwalten, die vom Scan ausgeschlossen sind.
6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Datei oder den Ordner, der vom Scan ausgeschlossen werden soll, und klicken Sie auf **OK**.Alternativ können Sie den Datei- oder Ordnerpfad auch manuell (oder per Kopieren und Einfügen) in das Bearbeitungsfeld eingeben.

c. Standardmäßig werden die ausgewählten Dateien oder Ordner sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.

d. Klicken Sie auf **Hinzufügen**.

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

5.4.2. Dateiendungen vom Scan ausschließen

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

Wichtig
Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausschließen, da solche Ausschlüsse Ihren Computer anfällig für Malware-Bedrohungen machen können.

Um Dateiendungen vom Scan auszuschließen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Aktivieren Sie Scan-Ausschlüsse für Dateien durch Anklicken des entsprechenden Schalters.
5. Klicken Sie auf den Link **Ausgeschlossene Dateiendungen**.In dem Fenster, das jetzt angezeigt wird, können Sie die Dateiendungen verwalten, die vom Scan ausgenommen sind.
6. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Geben Sie die Dateiendungen ein, die vom Scan ausgeschlossen werden sollen. Trennen Sie einzelne Endungen mit einem Semikolon (;).Hier ein Beispiel:

      ```
      txt;avi;jpg
      ```

   c. Standardmäßig werden alle Dateien mit den festgelegten Dateiendungen sowohl vom Zugriff-Scan als auch vom Bedarf-Scan ausgeschlossen. Wählen Sie eine der anderen Optionen, um die Anwendung der Ausschlussregel anzupassen.
   d. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

5.4.3. Verwalten von Scan-Ausschlüssen

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

Um die Scan-Ausschlüsse zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.Nutzen Sie die Optionen im Bereich **Dateien und Ordner**, um Scan-Ausschlüsse zu verwalten.
4. Um Scan-Ausschlüsse zu entfernen oder zu bearbeiten, klicken Sie auf einen der verfügbaren Links.Gehen Sie wie folgt vor:
   - Um einen Eintrag aus der Tabelle zu entfernen, markieren Sie diesen und klicken dann auf **Entfernen**.
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten(oder markieren Sie den Eintrag und klicken Sie dann auf **Bearbeiten**.)Ein neues Fenster wird eingeblendet, in dem Sie sowohl die Dateiendungen oder die Pfade ändern können, die vom Scan ausgeschlossen werden sollen, als auch die Art von Scan, für den der Ausschluss gelten soll. Nehmen Sie die notwendigen Änderungen vor und klicken Sie dann auf **Ändern**.
5. Nutzen Sie den entsprechenden Schalter, um die Scan-Ausschlüsse zu deaktivieren.

5.5. Verwalten von Dateien in Quarantäne

Bitdefender isoliert mit Malware infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien in einem sicheren Bereich, der sogenannten Quarantäne.Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

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

Um Dateien in Quarantäne zu überprüfen und zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.

2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Quarantäne**.
4. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet.Sie können die Quarantäneeinstellungen an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.

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

   Quarantäne-Dateien zur Analyse an Bitdefender senden
   Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch an das Bitdefender-Labor zu schicken.Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

   Inhalte löschen, die älter als {30} Tage sind
   Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht.Wenn Sie diesen Zeitraum verändern möchten, geben Sie einen neuen Wert in das entsprechende Feld ein.Um das automatische Löschen von alten Dateien in Quarantäne zu deaktivieren, geben Sie eine 0 ein.
5. Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**.Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

5.6. Active Virus Control

Active Virus Control von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

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 Gesamteinstufung erstellt.Wenn diese Gesamteinstufung für einen Prozess einen bestimmten Grenzwert überschreitet, wird der entsprechende Prozess als schädlich eingestuft und automatisch blockiert.

Wenn der Auto-Pilot deaktiviert ist, wird Sie ein Pop-up-Fenster über die blockierte Anwendung informieren.Andernfalls wird die Anwendung ohne Benachrichtigung

blockiert.Im Ereignis-Fenster können Sie überprüfen, welche Anwendungen von Active Virus Control erkannt wurden.

5.6.1. Überprüfen erkannter Anwendungen

Um die Anwendungen zu überprüfen, die von Active Virus Control erkannt wurden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Active Virus Control**.
4. Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Wenn Sie der Anwendung vertrauen, klicken Sie auf **Zulassen und überwachen**, um Active Virus Control so zu konfigurieren, dass sie nicht mehr blockiert wird.Active Virus Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

5.6.2. Aktivieren / Deaktivieren von Active Virus Control

Um Active Virus Control zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Klicken Sie auf den Schalter, um Active Virus Control zu aktivieren oder deaktivieren.

5.6.3. Anpassen des Active-Virus-Control-Schutzes

Sollte Ihnen auffallen, das Active Virus Control häufig ungefährliche Anwendung erkennt, sollten Sie eine tolerantere Sicherheitsstufe auswählen.

Um den Schutz durch Active Virus Control anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
4. Stellen Sie sicher, dass Active Virus Control aktiviert ist.

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

Beachten Sie
Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Active Virus Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen und zudem die Wahrscheinlichkeit von Fehlalarmen (ungefährliche Anwendungen, die als schädlich eingestuft wurden).

5.6.4. Verwalten von ausgeschlossenen Prozessen

Sie können Ausschlussregeln für vertrauenswürdige Anwendungen festlegen, damit Active Virus Control diese nicht blockiert, wenn sie sich wie Malware verhalten.Active Virus Control wird ausgeschlossene Anwendungen auch weiterhin überwachen. Wird bei einer ausgeschlossenen Anwendung verdächtiges Verhalten erkannt, wird das Ereignis lediglich protokolliert und als Erkennungsfehler in die Bitdefender-Cloud gemeldet.

Um die Prozesse zu verwalten, die von Active Virus Control ausgeschlossen sind, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Klicken Sie auf den Link **Ausgeschlossene Prozesse**.Ein Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Virus Control ausgeschlossen sind.

Beachten Sie
Prozessauschlüsse gelten auch für das Angriffserkennungssystem, das in die Bitdefender-Firewall integriert ist.

5. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.
   c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Virus Control die Anwendung blockiert.
   d. Klicken Sie auf **Hinzufügen**.

6. Um Ausschlüsse zu entfernen oder zu bearbeiten, gehen Sie folgendermaßen vor:
   - Um einen Eintrag aus der Tabelle zu entfernen, markieren Sie diesen und klicken dann auf **Entfernen**.
   - Doppelklicken Sie auf einen Tabelleneintrag, um diesen zu bearbeiten(oder markieren Sie den Eintrag und klicken Sie dann auf **Bearbeiten**.)Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

5.7. Beheben von Systemschwachstellen

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand eu halten.Sie sollten zudem in Betracht ziehen, die Windows-Einstellungen zu deaktivieren, die das System anfälliger für Malware machen.Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

Bitdefender bietet Ihnen zwei einfache Möglichkeiten, die Schwachstellen Ihres Systems zu beheben:

- Sie können Ihr System nach Schwachstellen durchsuchen und diese Schritt für Schritt beheben, indem Sie den Assistenten für den **Schwachstellen-Scan** ausführen.
- Mithilfe der automatischen Schwachstellenüberwachung können Sie im Ereignis-Fenster erkannte Schwachstellen überprüfen und beheben.

Sie sollten Ihr System alle ein bis zwei Wochen nach Schwachstellen durchsuchen und diese beheben.

5.7.1. Scannen des Computers nach Schwachstellen

Um Systemschwachstellen mithilfe des Assistenten für den Schwachstellen-Scan zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Virenschutz**-Bereich.
3. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Schwachstellen-Scan**.
4. Folgen Sie der sechsstufigen Anleitung, um die Schwachstellen Ihres Systems zu entfernen.Innerhalb des Assistenten können Sie über die Schaltfläche **Weiter** navigieren. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

   a. **Schützen Sie Ihren PC**

Wählen Sie die zu scannenden Schwachstellen.

b. **Nach Problemen suchen**

Bitte warten Sie, bis Bitdefender den Scan auf Schwachstellen beendet hat.

c. **Windows-Updates**

Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zur Zeit nicht auf Ihrem Computer installiert sind.Wählen Sie die Updates, die Sie installieren möchten.

Um die Installation der gewählten Updates zu starten, klicken Sie auf **Weiter**.Bitte beachten Sie, dass die Installation der Updates einige Zeit in Anspruch nehmen kann und dass manche Updates einen Neustart erfordern, um die Installation abzuschließen.Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

d. **Anwendungs-Updates**

Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

e. **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.Sie können den jeweiligen Benutzer auffordern, das Passwort bei der nächsten Anmeldung zu ändern oder das Passwort an Ort und Stelle selbst ändern.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

f. **Übersicht**

Hier können Sie das Ergebnis der Operation sehen.

5.7.2. Automatische Schwachstellenüberwachung

Bitdefender scannt Ihr System im Hintergrund regelmäßig nach Schwachstellen und erfasst alle erkannten Probleme im Ereignis-Fenster.

Um die erkannten Probleme zu untersuchen und zu beheben, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schwachstelle**.

4. Sie erhalten detaillierte Informationen zu den erkannten Systemschwachstellen.Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:

   - Wenn Windows-Updates zur Verfügung stehen, klicken Sie auf **Update jetzt durchführen**, um den Assistenten für den Schwachstellen-Scan aufzurufen und diese zu installieren.
   - Falls eine Anwendung nicht mehr auf dem neuesten Stand ist, klicken Sie auf **Update jetzt durchführen**, um einen Link zur Website des Anbieters zu finden, von der aus Sie die neueste Version der Anwendung installieren können.
   - Wenn ein Windows-Benutzerkonto mit einem schwachen Passwort gesichert ist, klicken Sie auf **Passwort reparieren**, um den Benutzer dazu zu zwingen, das Passwort bei der nächsten Anmeldung zu ändern oder es selbst zu ändern.Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).
   - Sollte die Autorun-Funktion in Windows aktiviert sein, klicken Sie auf **Deaktivieren**, um es zu deaktivieren.

Um die Einstellungen für die Schwachstellenüberwachung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schwachstelle**.
4. Klicken Sie auf den Schalter, um den automatischen Schwachstellen-Scan zu aktivieren oder deaktivieren.

   Wichtig
   Um automatisch über Schwachstellen im System oder in Anwendungen benachrichtigt zu werden, lassen Sie die Option **Automatischer Schwachstellen-Scan** aktiviert.

5. Nutzen Sie die entsprechenden Schalter, um die Systemschwachstellen auszuwählen, die Sie regelmäßig überprüfen möchten.

   Kritische Windows-Updates
   Überprüfen Sie, ob die neuesten kritischen Microsoft-Sicherheits-Updates auf Ihrem Windows-Betriebssystem installiert sind.

   Normale Windows-Updates
   Überprüfen Sie, ob auf Ihrem Windows-Betriebssystem die neuesten Microsoft-Sicherheits-Updates installiert sind.

Anwendungs-Updates

Überprüfen Sie ob wichtige auf Ihrem System installierte Anwendungen, die Verbindungen zum Internet aufbauen können, auch aktuell sind.Veraltete Anwendungen können von schädlicher Software ausgenutzt werden und Ihren PC so anfällig für Angriffe von außen machen.

Unsichere Passwörter

Überprüfen Sie, ob die Passwörter der Windows-Benutzerkonten, leicht zu erraten sind oder nicht.Passwörter, die schwer zu erraten sind (starke Passwörter), mache es sehr schwierig für Hacker, in Ihr System einzudringen.Ein starkes Passwort sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z.B. #, $ oder @) bestehen.

Autostart externer Medien

Überprüfen Sie den Status der Windows-Autorun-Funktion.Mit dieser Funktion lassen sich Anwendungen automatisch direkt von CD, DVD, USB-Stick oder anderen externen Speichermedien starten.

Manche Malware-Typen nutzen Autorun, um automatisch von Wechselmedien auf den PC zu gelangen. Aus diesem Grund sollten Sie diese Windows-Funktion deaktivieren.

Beachten Sie

Wenn Sie die Überwachung einer bestimmten Schwachstelle deaktivieren, werden damit zusammenhängende Ereignisse nicht mehr im Ereignisfenster erfasst.

6. Spam-Schutz

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet.Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

Bitdefender Antispam greift auf außergewöhnliche technologische Innovationen und Standard-Antispam-Filter zurück, um Spams auszusortieren, bevor dieser im Posteingang landen.Für weitere Informationen lesen Sie bitte *„Wie funktioniert der Spam-Schutz?“* (S. 66).

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 der E-Mail-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, Spams werden verschoben in den **Spam** Ordner, zu finden unter **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 den **Spam** Ordner verschoben, der unter **Trash** Ordner zu finden ist.Das **Spam**-Verzeichnis wurde während der Installation von Bitdefender erstellt.

Wenn Sie andere Mail Clients verwenden, müssen Sie eine Regel erstellen, um Email-Nachrichten zu verschieben, die folgendermaßen markiert sind: `[spam]` von Bitdefender in ein benutzerdefiniertes Quarantäne-Verzeichnis verschoben werden.

6.1. Wie funktioniert der Spam-Schutz?

6.1.1. AntiSpam Filter

Der Spam-Schutz-Engine von Bitdefender kombiniert verschiedene Filter, um sicherzustellen, dass Ihr Posteingang von SPAM verschont bleibt: Freundesliste, Spammer-Liste, Zeichensatzfilter, Link-Filter, Signaturenfilter, NeuNet- (heuristischer) Filter and In-the-Cloud-Erkennung.

Freundesliste/ Spammer-Liste

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Liste der Freunde bzw. Spammer** geführt, so können Sie festlegen, welche E-Mails 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.

Zeichensatz-Filter

Viele der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Schriftsatz-Filter erkannt diese Art von Nachrichten und behandelt diese als SPAM.

Link-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 Link-Filter überprüft jeden in einer Nachricht enthaltenen URL-Link auf Grundlage seiner Datenbank. Wird eine Übereinstimmung gefunden, wird die Nachricht als SPAM markiert.

Signaturenfilter

Die Bitdefender-Spam-Forscher analysieren unentwegt die Spam-Nachrichten, die sich im Umlauf befinden, und veröffentlichen Spam-Signaturen, um deren Erkennung zu ermöglichen.

Der Signaturenfilter vergleicht E-Mails mit den Spam-Signaturen in der lokalen Datenbank.Wird eine Übereinstimmung gefunden, wird die Nachricht als SPAM markiert.

Beachten Sie
Anders als die anderen Filter, kann der Signaturenfilter nicht unabhängig vom Spam-Schutz deaktiviert werden.

NeuNet-Filter (Heuristik)

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 überprüft), hält Ausschau nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam.Basierend auf den Analyseergebnissen wird für die E-Mail eine Spam-Marke vergeben.

Wenn die Spam-Marke den Grenzwert überschreitet, wird die E-Mail als SPAM eingestuft.Der Grenzwert hängt von der Empfindlichkeitsstufe des Spam-Schutzes ab.Für weitere Informationen lesen Sie bitte *„Anpassen der Empfindlichkeitsstufe“ (S. 74)*.

Der Filter erkennt auch Nachrichten welche im Betreff als `Ausdrücklich Sexuel` markiert wurden und markiert diese als SPAM.

Beachten Sie

Seit dem 19. Mai 2004 müssen E-Mails mit sexuellem Inhalt entsprechend markiert werden `Sexual ausdrücklich:` und in der Betreffzeile muss explizit auf den Inhalt hingewiesen werden.

In-the-Cloud-Erkennung

Die In-the-Cloud-Erkennung nutzt die Bitdefender-Cloud-Dienste, um Ihnen effizienten und stets aktuellen Spam-Schutz bieten zu können.

E-Mails werden nur dann in der Cloud überprüft, wenn die lokalen Spam-Schutz-Filter kein eindeutiges Ergebnis liefern.

6.1.2. Spam-Schutz

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

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Freundesliste/Spammerliste überprüft. Falls der Sender in der Freundesliste 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 überprüft, ob die E-Mail in Kyrillisch oder mit asiatischen Buchstaben geschrieben worden ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben.

Der Link-Filter vergleicht die Links in der E-Mail mit den Links in der Bitdefender-Datenbank, die als Spam-Links bekannt sind. Falls eine Übereinstimmung gefunden wird, wird die E-Mail als SPAM eingestuft.

Im nächsten Schritt vergleicht der Signaturenfilter die E-Mail mit den Spam-Signaturen in der lokalen Datenbank.Wird eine Übereinstimmung gefunden, wird die Nachricht als SPAM markiert.

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 wird für die E-Mail eine Spam-Marke vergeben.

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

Wenn die Spam-Marke den Grenzwert überschreitet, wird die E-Mail als SPAM eingestuft.Die Schwelleneinstellung hängt ab von der Antispam Schutzeinstellung.Für weitere Informationen lesen Sie bitte *„Anpassen der Empfindlichkeitsstufe“ (S. 74)*.

Wenn die lokalen Spam-Schutz-Filter zu keinem eindeutigen Ergebnis kommen, wird die E-Mail mithilfe der In-the-Cloud-Erkennung überprüft. Diese entscheidet dann auch letztlich, ob es sich bei der E-Mail um Spam handelt oder nicht.

6.1.3. Spam-Schutz-Updates

Immer wenn ein Update durchgeführt wird, werden neue Signaturen für bekannte Spam-Nachrichten und Links zur Datenbank 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.

6.1.4. Unterstützte E-Mail-Clients und Protokolle

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

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express und Windows Mail (auf 32-Bit-Systemen)
- Mozilla Thunderbird 3.0.4

6.2. Aktivieren / Deaktivieren des Spam-Schutzes

Um den Spam-Schutz zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Spam-Schutz**-Bereich.
3. Klicken Sie auf den Schalter, um den Spam-Schutz zu aktivieren oder deaktivieren.

6.3. Verwenden der Spam-Schutz-Symbolleiste in Ihrem Mail-Client-Fenster

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen.Die Antispamleiste hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus.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.Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“ (S. 69)*.

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

Ist Spam - Gibt an, dass es sich bei der ausgewählten E-Mail um Spam handelt.Die E-Mail wird sofort in den **Spam**-Ordner verschoben.Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.

Kein Spam - Zeigt an, dass es sich bei der angezeigten E-Mail nicht um Spam handelt und dass Bitdefender sie nicht als solche hätte kennzeichnen sollen.Die E-Mail wird aus dem **Spam** Ordner ins **Inbox** Ordner verschoben.Wenn die Cloud-Dienste für den Spam-Schutz aktiviert sind, wird die Nachricht zur weiteren Analyse in die Bitdefender-Cloud geschickt.

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 E-Mail zur Liste der Spammer hinzu.Klicken Sie zur Bestätigung **OK**.Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als `[spam]`.

Freund hinzufügen - fügt den Sender der ausgewählten E-Mail der Liste der Freunde hinzu.Klicken Sie zur Bestätigung **OK**.Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Spammer - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen Inhalts.Für weitere Informationen lesen Sie bitte *„Konfigurieren der Spammerliste“ (S. 73)*.

Freunde - Öffnen Sie **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen Inhalts.Für weitere Informationen lesen Sie bitte *„Freundesliste konfigurieren“ (S. 72)*.

Einstellungen - Öffnet eine Fenster, in dem Sie die Spam-Filter und die Einstellungen für die Symbolleiste konfigurieren können.

6.3.1. Anzeigen von Erkennungsfehlern

Wenn Sie einen unterstützten Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie anzeigen, welche E-Mail-Nachrichten nicht als `[spam]` hätten gekennzeichnet werden sollen). Dies wird die Effizienz des Spam-Filters verbessern.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin 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 immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Kein Spam**.Die E-Mail wird in den Posteingangsordner verschoben.

6.3.2. Hinweisen auf unerkannte Spam-Nachrichten

Wenn Sie einen unterstützten Mail-Client verwenden, können Sie einfach darauf hinweisen, welche E-Mail-Nachrichten als Spam hätten erkannt werden sollen. Dies wird die Effizienz des Spam-Filters verbessern.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden sofort als [spam] markiert und in den Junk-Mail-Ordner verschoben.

6.3.3. Konfigurieren der Symbolleisteneinstellungen

Um die Einstellungen für die Spam-Schutz-Symbolleiste zu konfigurieren, klicken Sie in der Symbolleiste auf die Schaltfläche **Einstellungen** und danach auf den Reiter **Symbolleisteneinstellungen**.

Die Einstellungen sind in zwei Kategorien unterteilt:

- Unter **E-Mail-Regeln** können Sie die Verarbeitungsregeln für die von Bitdefender erkannten Spam-Nachrichten konfigurieren.
  - **Nachricht verschieben nach Gelöschte Objekte** (nur für Microsoft Outlook Express / Windows Mail)

> **Beachten Sie**
> In Microsoft Outlook / Mozilla Thunderbird werden erkannte Spam-Nachrichten automatisch in einen Spam-Ordner verschoben, der sich wiederum im Ordner für gelöschte Elemente / Papierkorb befindet.

- **Markieren Sie Spam-E-Mail Nachrichten als 'gelesen'** - Markiert die Spam-Nachrichten automatisch als gelesen, so dass sie nicht stören wenn Sie ankommen.

- Unter **Mitteilungen** können Sie festlegen, ob Bestätigungsfenster angezeigt werden sollen, wenn Sie in der Spam-Schutz-Symbolleiste die Schaltflächen **Spammer hinzufügen** und **Freund hinzufügen** anklicken.Bestätigungsfenster verhindern, dass Sie die Absender von E-Mail-Nachrichten versehentlich zu Ihrer Freundes- bzw. Spam-Liste hinzufügen.

6.4. Freundesliste konfigurieren

Liste der Freunde – die Liste aller E-Mail-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 Spam ähnlich sein sollte.

Beachten Sie

Jede Mail von einer Adresse Ihrer **Freundesliste** 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 das Bitdefender-Fenster.
  2. Gehen Sie in den **Spam-Schutz**-Bereich.
  3. Klicken Sie auf **Verwalten** und wählen Sie dann **Freunde** aus dem Menü.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**.Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**.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;
- *com - alle Mails mit der Endung com 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 ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Liste der Freunde speichern, so das diese auf einen anderen Rechner oder nach einer neuinstallation benutzt werden kann.Um die Freundesliste zu speichern klicken Sie auf **Speichern** und speichern sie diese an den gewünschten Ort.Die Datei wird `.bwl` als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste 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 **Liste beim Laden leeren**.

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

6.5. Konfigurieren der Spammerliste

Liste der Spammer - Liste die alle E-Mail-Adressen enthält, 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 das Bitdefender-Fenster.
  2. Gehen Sie in den **Spam-Schutz**-Bereich.
  3. Klicken Sie auf **Verwalten** und wählen Sie dann **Spammer** aus dem Menü.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse** und klicken Sie dann auf **Hinzufügen**.Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Domain-Namen ein und klicken Sie auf **Hinzufügen**.Syntax:

- @domain.com, *domain.com und domain.com - alle eingehenden Mails von domain.com 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 legitime Webbasierte E-Mail Anbieter (wie: Yahoo, Gmail, Hotmail oder andere) zu der Spammerliste hinzu. Andernfalls werden die E-Mail-Nachrichten, die von jedem möglichem Benutzer solch eines Anbieters gesendet werden, als Spam eingestufft.z.B: wenn Sie `yahoo.com` zu Spammerliste hinzufügen, werden alle E-Mails die von `yahoo.com` Adressen kommen, als `[spam]` markiert.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den entsprechenden **Entfernen**-Link.Um alle Einträge zu löschen, klicken Sie auf **Liste löschen** und danach auf **Ja** um dies zu bestätigen.

Sie können die Spammer Liste 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 an den gewünschten Ort.Die Datei wird `.bwl` als Erweiterung haben.

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 **Liste beim Laden leeren**.

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

6.6. Anpassen der Empfindlichkeitsstufe

Falls Sie bemerken, dass legitime E-Mails zum Teil als Spam markiert werden oder viele Spam-Nachrichten nicht erkannt werden, können Sie versuchen, das Problem zu lösen, indem Sie die Spam-Empfindlichkeitsstufe anpassen.Bevor Sie die Empfindlichkeitsstufe selbst ändern, sollten Sie zunächst *„Der Spam-Schutz-Filter funktioniert nicht richtig“ (S. 128)* lesen und den Anweisungen folgen, um das Problem zu beheben.

Um die Empfindlichkeitsstufe des Spam-Schutzes anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie Bitdefender.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie auf **Update** im Baummenu und dann auf den Tab **Einstellungen** um diesen Bereich zu öffnen.
4. Die Beschreibung auf der rechten Seite der Skala hilft Ihnen dabei, die Empfindlichkeitsstufe einzustellen, die zu Ihren Sicherheitsanforderungen passt.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.

6.7. Konfigurieren der lokalen Spam-Schutz-Filter

Wie in *„Wie funktioniert der Spam-Schutz?“* (S. 66) beschrieben, nutzt Bitdefender eine Kombination aus unterschiedlichen Spam-Filtern, um Spam zu identifizieren.Die Spam-Filter sind für effizienten Schutz vorkonfiguriert.

Wichtig

Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt.Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendetn(wie z. B. in der russischen oder chinesischen Programmversion).

Um die lokalen Spam-Schutz-Filter zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie auf **Update** im Baummenu und dann auf den Tab **Einstellungen** um diesen Bereich zu öffnen.
4. Klicken Sie auf die Schalter, um die lokalen Spam-Filter zu aktivieren oder deaktivieren.

Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, können Sie die lokalen Spam-Filter direkt aus Ihrem Mail-Client heraus konfigurieren.Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Einstellungen** und wählen Sie dann den Reiter **Spam-Filter** aus.

6.8. Konfigurieren der In-the-Cloud-Erkennung

Die In-the-Cloud-Erkennung nutzt die Bitdefender-Cloud-Dienste, um Ihnen effizienten und stets aktuellen Spam-Schutz bieten zu können.

Um die In-the-Cloud-Erkennung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Spam-Schutz** und danach auf den Reiter **Cloud**.
4. Klicken Sie auf den Schalter, um die In-the-Cloud-Erkennung zu aktivieren oder deaktivieren.
5. Beispiele von legitimen E-Mails und Spam-Nachrichten können in die Bitdefender-Cloud geschickt werden, wenn Sie auf Erkennungsfehler oder unerkannte Spam-Nachrichten hinweisen. Dies trägt dazu bei, die Bitdefender-Spam-Erkennung zu verbessern.Konfigurieren Sie die Übermittlung

der E-Mail-Beispiele an die Bitdefender-Cloud, indem Sie die gewünschten Optionen auswählen.

Wenn Sie Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird nutzen, können Sie die In-the-Cloud-Erkennung direkt aus Ihrem Mail-Client heraus konfigurieren.Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Einstellungen** und wählen Sie dann den Reiter **Cloud-Einstellungen** aus.

7. Privatsphärenschutz

Ihre persönlichen Daten sind immer ein beliebtes Ziel für Internet-Kriminelle.Die Bedrohung erstreckt sich mittlerweile auf nahezu alle Bereiche Ihrer Internet-Aktivitäten und so können Sie durch nur unzureichend geschützte E-Mails, Sofortnachrichten und Besuche von Webseiten schnell unfreiwillig Informationen preisgeben und Ihre Privatsphäre aufs Spiel setzten.

Der Bitdefender-Privatsphärenschutz bietet eine Vielzahl von Komponenten, um diese Bedrohungen abzuwehren.

- Phishing-Schutz - Bietet Ihnen umfangreiche Funktionen, die das Surfen im Internet rundum absichern. Es wird zudem verhindert, dass Sie persönliche Daten auf betrügerischen Webseiten preisgeben, die sich als harmlose Website getarnt haben.
- Datenschutz - Hilft Ihnen sicherzustellen, dass Ihre persönlichen Daten Ihren Computer nicht ohne Ihre Zustimmung verlassen.Ausgehende E-Mails und Sofortnachrichten sowie über Webseiten versandte Daten werden gescannt. Alle Informationen, die über die von Ihnen festgelegten Datenschutzregeln geschützt sind, werden blockiert.
- Chat-Verschlüsselung - Verschlüsselt Ihre Sofortnachrichten, um sicherzustellen, dass die Inhalte Ihrer Unterhaltungen nicht von Dritten eingesehen werden können.

7.1. Phishing-Schutz

Der Bitdefender-Phishing-Schutz schützt Sie davor, dass persönliche Daten während des Surfens ins Internet gelangen können. Der Benutzer wird vor potenziellen Phishing-Webseiten gewarnt.

Bitdefender bietet Echtzeit-Phishing-Schutz für:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Um die Phishing-Schutz-Einstellungen vorzunehmen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Privatsphärenschutz** und danach auf den Reiter **Phishing-Schutz**.

Die Einstellungen sind in zwei Kategorien unterteilt:

Funktionen der Symbolleiste

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

- Anzeige der Bitdefender-Symbolleiste im Web-Browser.
- Suchberater: Diese Komponente bewertet neben den Suchergebnissen von Google, Bing und Yahoo! auch Links auf Facebook und Twitter und platziert ein entsprechendes Symbol vor jedem Ergebnis:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen wollen.

  Diese Seite ist sicher.
- SSL-Datenverkehr-Scans.

  Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen.Darum empfiehlt es sich, den SSL-Scan zu aktivieren.

Web-Browser-Schutz

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

- Schutz vor Betrug.
- Schutz vor Phishing-Attacken.
- Schutz für Sofortnachrichten.

Sie können eine Liste mit Websites anlegen, die nicht von den Bitdefender-Phishing-Schutz-Engines gescannt werden sollen.Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.Fügen Sie beispielsweise Websites hinzu, auf denen Sie häufig einkaufen.

Um die Phishing-Schutz-Whitelist zu konfigurieren und zu verwalten, klicken Sie auf den **Whitelist**-Link.Ein neues Fenster wird sich öffnen.

Um eine Website zur Whitelist hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

Um eine Website aus der Liste zu entfernen, wählen Sie sie aus der Liste aus und klicken Sie auf den entsprechenden **Entfernen**-Link.

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

7.1.1. Bitdefender-Schutz in Ihrem Browser

Bitdefender integriert sich über eine intuitive und einfach zu bedienende Symbolleiste in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten.Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird.Klicken Sie darauf, um die Symbolleiste anzuzeigen.

Die Bitdefender-Symbolleiste enthält die folgenden Elemente:

Seitenbewertung

Abhängig davon, wie Bitdefender die Webseite, die sie gerade besuchen, einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste eingeblendet:

- Die Nachricht "Diese Website ist nicht sicher" erscheint auf rotem Hintergrund - Sie sollten diese Website umgehend verlassen.
- Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund erscheint - diese Webseite könnte gefährliche Inhalte enthalten.Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen wollen.
- Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund - Sie können diese ohne Risiko aufrufen.

Sandbox

Klicken Sie auf , um den Browser in einer von Bitdefender gestellten Umgebung zu starten und ihn so vom Betriebssystem zu isolieren.Dadurch wird verhindert, dass Browser-basierte Bedrohungen Schwachstellen in Ihrem Browser ausnutzen, um die Kontrolle über Ihr System zu erlangen.Nutzen Sie die Sandbox, wenn Sie Webseiten aufrufen, auf denen Sie Malware vermuten.

Beachten Sie
Die Sandbox ist nicht auf Computern mit Windows XP verfügbar.

Einstellungen

Klicken Sie auf , um einzelne Funktionen auszuwählen, die Sie aktivieren oder deaktivieren wollen:

- Phishing-Filter
- Malware-Filter
- Suchberater

Hauptschalter

Um die Funktionen der Symbolleiste vollständig zu aktivieren oder deaktivieren, klicken Sie auf auf der rechten Seite der Symbolleiste.

7.1.2. Bitdefender-Benachrichtigungen im Browser

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

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

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

- Rufen Sie eine andere Website auf.
- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.
- Fügen Sie die Seite der Phishing-Schutz-Whitelist hinzu, indem Sie auf **Zur Whitelist hinzufügen** klicken.Diese Seite wird nicht mehr von den Phishing-Schutz-Engines von Bitdefender gescannt.

7.2. Datenschutz

Der Datenschutz verhindert, dass sensible Daten in fremde Hände gelangen, wenn Sie online sind.

Gehen wir von einem einfachen Beispiel aus: Sie haben eine Datenschutzregel definiert, die Ihre Kreditkartennummer schützt.Falls es eine Spyware-Software irgendwie schafft, sich auf Ihrem Computer zu installieren, kann sie Ihre Kreditkartennummer nicht per E-Mail, Sofortnachricht oder über eine Website versenden.Zudem können Ihre Kinder sie nicht benutzen, um online einzukaufen oder Sie an Personen weiterzugeben, mit denen sie im Internet Kontakt haben.

Weitere Informationen zu folgenden Themen sind verfügbar:

- *„Informationen zum Datenschutz“* (S. 80).
- *„Konfigurieren des Datenschutzes“* (S. 81).
- *„Regeln bearbeiten“* (S. 82).

7.2.1. Informationen zum Datenschutz

Ob es sich um Ihre E-Mail-Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten, können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam-Nachrichten ertrinken oder sich über ein geleertes Konto wundern.

Der Datenschutz durchsucht den ausgehenden Web-, E-Mail- und Sofortnachrichtenverkehr anhand der von Ihnen festgelegten Regeln nach bestimmten Zeichenfolgen (z.B. nach Ihrer Kreditkartennummer). Wird eine

Übereinstimmung gefunden, wird die entsprechende Website, E-Mail oder Sofortnachricht blockiert.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie als persönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder E-Mail-Adresse bis hin zu Ihren Bankkontoangaben.Es besteht die Möglichkeit der Mehrbenutzerunterstützung, wodurch die Benutzer, die sich an den verschiedenen Windows-Benutzerkonten anmelden, Ihre eigenen Regeln konfigurieren und anwenden können.Falls Ihr Windows-Benutzerkonto ein Administratorkonto ist, können Sie festlegen, dass erstellte Regeln auch für andere Benutzer gelten, wenn diese sich unter ihrem Benutzernamen bei Windows anmelden.

7.2.2. Konfigurieren des Datenschutzes

Wenn Sie den Datenschutz nutzen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Privatsphärenschutz** und danach auf den Reiter **Datenschutz**.
4. Stellen Sie sicher, dass der Datenschutz aktiviert ist.
5. Erstellen Sie Regeln, um wichtige Daten zu schützen.Für weitere Informationen lesen Sie bitte *„Erstellen von Datenschutzregeln “* (S. 81).

Erstellen von Datenschutzregeln

Um eine Regel anzulegen, klicken Sie auf **Regel hinzufügen** und folgen Sie den Anweisungen des Konfigurationsassistenten.Über die Schaltflächen **Weiter** und **Zurück** können Sie im Assistenten blättern.Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.

1. **Typ und Richtung auswählen**

   Hier können Sie die Parameter auswählen:

   - **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Bearbeitungsfeld ein.
   - **Regeltyp** - Wählen Sie den Regeltyp aus (Adresse, Name, Kreditkartennummer, PIN, TAN usw.).
   - **Regeldaten** - Geben Sie hier die Daten ein, die geschützt werden sollen.Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.

Wichtig

Wenn Sie weniger als drei Zeichen eingeben, werden Sie aufgefordert, die Daten zu bestätigen. Wir empfehlen die Eingabe von mindestens drei Zeichen, um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern.

Alle Daten, die Sie eingeben, sind verschlüsselt. Um zusätzliche Sicherheit zu schaffen, geben Sie nicht die vollständigen Daten ein, die Sie schützen möchten.

2. **Art des Datenverkehrs und Benutzer auswählen**

   a. Bitte wählen Sie die Datenverkehrsart, die Bitdefender scannen soll.

   - **HTTP-Datenverkehr scannen** - Scannt den HTTP- (Web-) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
   - **E-Mails scannen (SMTP-Datenverkehr)** - Scannt den SMTP- (E-Mail-) Datenverkehr und blockiert alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.
   - **Sofortnachrichten scannen** - scannt den Instant-Messaging-Datenverkehr und blockiert ausgehende Nachrichten, die den Regeln entsprechen.

   Sie können wählen, ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

   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.
   - **Eingeschränkte Benutzerkonten** - Die Regel wird für Ihr Benutzerkonto und alle anderen eingeschränkten Windows-Benutzerkonten angewandt.
   - **Alle Benutzer** - Die Regel wird für alle Windows-Benutzerkonten angewandt.

3. **Beschreibung der Regel**

   Geben Sie eine kurze Beschreibung der Regel im Bearbeitungsfeld ein.Da die blockierten Daten (Zeichenfolgen) nicht als ein 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 erscheinen.

Von jetzt an wird jeder Versuch, die festgelegten Daten zu versenden (als E-Mail, Sofortnachricht oder über eine Website), fehlschlagen. Im Ereignis-Fenster wird ein Eintrag angezeigt, der darauf hinweist, dass Bitdefender das Versenden von identitätsspezifischen Inhalten blockiert hat.

7.2.3. Regeln bearbeiten

Verwalten Sie die Datenschutzregeln wie folgt:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Privatsphärenschutz** und danach auf den Reiter **Datenschutz**.

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, markieren Sie diese und klicken dann auf die Schaltfläche **Regel löschen**.

Um eine Regel zu bearbeiten und klicken Sie auf die Schaltfläche **Regel bearbeiten**. Ein neues Fenster wird geöffnet.Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK**, um die Änderungen zu speichern.

7.3. Chat-Verschlüsselung

Die Inhalte Ihrer Sofortnachrichten sollten zwischen Ihnen und Ihrem Gesprächspartner 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 Sofortnachrichtensitzungen, vorausgesetzt dass:

- Ihr Gesprächspartner hat ein Bitdefender-Produkt installiert, das die Chat-Verschlüsselung unterstützt, und die Chat-Verschlüsselung wurde für die genutzte Sofortnachrichtenanwendung aktiviert.
- Sie und Ihr Gesprächspartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.

Wichtig

Bitdefender wird die Konversationen nicht verschlüsseln, wenn ein Gesprächspartner eine web-basierte Sofortnachrichtenanwendung (wie Meebo) verwendet oder wenn ein Gesprächspartner Yahoo! und der andere Windows Live (MSN) verwendet.

Um die Sofortnachrichtenverschlüsselung zu konfigurieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Privatsphärenschutz** und danach auf den Reiter **Verschlüsselung**.

Standardmäßig ist die Chat-Verschlüsselung sowohl für den Yahoo Messenger als auch für den Windows Live (MSN) Messenger aktiviert.Sie können die Chat-Verschlüsselung für eine oder beide Anwendungen deaktivieren, indem Sie auf den entsprechenden Schalter klicken.

8. Jugendschutz

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.
- Den Internet-Zugang zu bestimmten Zeiten (beispielsweise während Unterrichtszeiten).
- Webseiten, E-Mail-Nachrichten und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht 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.

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.

8.1. Kindersicherung konfigurieren

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.Für weitere Informationen lesen Sie bitte *„Wie lege ich Windows-Benutzerkonten an?“* (S. 35).

Haben Ihre Kinder Zugriff auf ein Administrator-Benutzerkonto auf ihrem Computer, müssen Sie ein Passwort festlegen, um die Einstellungen der Kindersicherung zu schützen.Für weitere Informationen lesen Sie bitte *„Passwortschutz für Bitdefender-Einstellungen“* (S. 18).

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 das Bitdefender-Fenster.
3. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
4. Klicken Sie im Menü links auf **Kindersicherung** und danach auf den Reiter **Konten**.Hier können Sie die Einstellungen der Kindersicherung für jedes Windows-Benutzerkonto überprüfen und konfigurieren.Wenn die Kindersicherung aktiviert ist, können Sie sich die ausgewählte Alterskategorie und den Status der Kindersicherung anzeigen lassen (wie im Folgenden beschrieben).

Konfiguration der Kindersicherung für ein bestimmtes Benutzerkonto:

1. Verwenden Sie den Regler, um die Kindersicherung für dieses Benutzerkontozu aktivieren.
2. Geben Sie das Alter Ihres Kindes an, indem Sie auf das dem **Alter** entsprechende Kästchen klicken.Durch die Angabe des Kindesalters werden automatisch für diese Altersstufe als geeignet eingeschätzte Einstellungen geladen. Diese Einstellungen basieren auf der Standard-Entwicklung von Kindern.
3. 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.

   - **Web** - Filtern Sie die Web-Navigation und definieren Sie zeitliche Beschränkungen für den Internet-Zugang mithilfe der Website-Steuerung.
   - **Anwendungen** - Konfigurieren Sie die Anwendungssteuerung, um den Zugang zu bestimmten Anwendungen zu blockieren oder einzuschränken.
   - **Schlüsselwörter** - Filtern Sie den Zugang zum Internet, E-Mails und Sofortnachrichten anhand von Schlüsselwörtern mithilfe der Schlüsselwortsteuerung.
   - **Instant Messaging** - Erlaubt Ihnen, die Chat-Steuerung so zu konfigurieren, dass Unterhaltungen mit bestimmten Sofortnachrichtenkontakten bei Yahoo! Messenger und Windows Live (MSN) Messenger zugelassen oder blockiert werden.
   - **Kategorien** - Blockieren Sie bestimmte Kategorien von Web-Inhalten mithilfe des Kategoriefilters.

   Um das Einstellungsfenster für die Kindersicherung zu schließen, klicken Sie auf das X in der oberen rechten Ecke.Die Einstellungen, die Sie konfiguriert haben, werden automatisch gespeichert.

Um die Optionen für die Aktivitätsüberwachung und die Fern-Kindersicherung zu konfigurieren, klicken Sie auf den Reiter **Einstellungen**.Konfigurieren Sie die Überwachungsoptionen nach Ihren Bedürfnissen:

Versenden von Aktivitätsberichten per E-Mail
Eine Email-Benachrichtigung wird versendet, sobald die Bitdefender-Kindersicherung eine Aktivität dieses Nutzers blockiert hat.Sie müssen zuerst die Benachrichtigungseinstellungen konfigurieren.

Protokoll für den Internet-Datenverkehr speichern
Protokolliert die besuchten Webseiten für Benutzer, für die die Kindersicherung aktiviert ist.

Für weitere Informationen lesen Sie bitte *„Überwachen der Aktivitäten Ihrer Kinder“ (S. 92)*.

Wenn Sie die Computer-Aktivitäten Ihrer Kinder per Fernsteuerung überwachen und steuern möchten, aktivieren Sie mit diesem Schalter die Remote Kindersicherung.Für weitere Informationen lesen Sie bitte *„Fern-Kindersicherung“ (S. 94)*.

8.1.1. Web Kontrolle

Die Website-Steuerung hilft Ihnen dabei, Websites mit unangemessenen Inhalten zu blockieren und den Internet-Zugang zeitlich zu beschränken.

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. 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.
5. Sie können Limits definieren, wie lange Ihr Kind im Internet surfen darf.Für weitere Informationen lesen Sie bitte „Zeitliche Beschränkung des Internet-Zugangs“ (S. 87).

Web-Kontroll Regel erstellen

Um den Zugriff auf eine Webseite zu blockieren oder zu erlauben, folgen Sie diesen Schritten:

1. Klicken Sie auf **Webseite zulassen** oder **Webseite blockieren**.
2. Geben Sie die Webseiten Adresse in das **Webseite** Feld ein.
3. Wählen Sie die gewünschte Aktion für diese Regel aus - **Erlauben** oder **Blocken**.
4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

Web-Kontroll Regeln verwalten

Die bereits konfigurierten Webseitenkontrollregeln sind in der Tabelle am unteren Rand des Fensters aufgelistet. Die Adresse und der aktulle Status jeder Webkontroll-Regel sind aufgelistet.

Um eine Regel zu entfernen, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Rechtsklicken Sie auf eine Regel, um sie zu bearbeiten (oder wählen Sie sie aus und klicken Sie dann auf **Bearbeiten**).Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

Zeitliche Beschränkung des Internet-Zugangs

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 **Zeitbegrenzung für den Internet-Zugang**.
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.Um eine neue Auswahl zu starten, klicken Sie auf **Alle blockieren** oder **Alle zulassen**.
4. Klicken Sie auf **Speichern**.

Beachten Sie

Bitdefender führt unabhängig davon, ob der Internetzugriff gesperrt ist, stündliche Updates durch.

8.1.2. Anwendungssteuerung

Die **Programm-Kontrolle** unterstützt Sie bei der Sperrung jeglicher Programmanwendungen. Spiele, Medien- und Messaging Software als auch andere Kategorien von Programmen oder gefährlicher Software können auf diesem Wege blockiert werden. Programme, die über diesen Weg gesperrt sind, können weder verändert, kopiert noch verschoben werden.Sie können Anwendungen permanent blocken oder nur für bestimmte Zeitintervalle, wie solche in denen Ihre Kinder Hausaufgaben zu erledigen haben.

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.

Anwendungskontrollregeln erstellen

Um den Zugriff auf eine Anwendung zu beschränken oder zu blockieren, befolgen Sie diese Schritte:

1. Klicken Sie auf **Blockieren** oder **Beschränken**.
2. Klicken Sie **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 Aktion der Regel:
   - **Dauerhaft blockieren** um den Zugriff auf die Anwendung vollständig zu blockieren.
   - **Blockieren basierend auf dieser Planung** um den Zugriff für bestimmte Zeitintervalle einzuschränken.

   Wenn Sie sich entscheiden den Zugriff einzuschränken statt die Anwendung komplett zu blockieren, so müssen Sie im Planungsgitter die Tage und das Zeitintervall auswählen währenddessen der Zugriff blockiert ist.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**.
4. Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

Anwendungs-Kontrolle Regeln verwalten.

Die bereits erstellten Anwenungskontrollregeln werden in der Tabelle am unteren Ende des Fensters aufgelistet. Es wird für jede Regel der Name der Anwendung, der Pfad und der aktuelle Status aufgelistet.

Um eine Regel zu entfernen, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Rechtsklicken Sie auf eine Regel, um sie zu bearbeiten (oder wählen Sie sie aus und klicken Sie dann auf **Bearbeiten**).Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

8.1.3. Schlüsselwortsteuerung

Mit der Schlüsselwortfilterung können Sie den Zugang zu E-Mail Nachrichten, Webseiten und Sofortnachrichten, die bestimmte Wörter enthalten, blockieren.Mit der Schlüsselwortfilterung können Sie verhindern, dass Ihre Kinder unangemessene

Wörter oder Sätze sehen, wenn sie online sind.Zusätzlich können Sie sicher stellen dass sie keine persönlichen Daten (z.B. Adresse oder Telefonnummer) an Leute geben, die sie im Internet getroffen haben.

Beachten Sie

Die Schlüsselwortfilterung für Instant Messaging ist nur für Yahoo Messenger und Windows 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. Definiere Schlüsselwörter-Kontroll Regeln, um die Anzeige von unangebrachten Wörtern oder das Senden von wichtigen Informationen zu verhindern.

Erstellen von Regeln für die Schlüsselwortfilterung

Um ein Wort oder eine Phrase zu blockieren folgen Sie diesen Schritten:

1. Klicken Sie auf **Schlüsselwort blockieren**.
2. Schlüsselwort Informationen eingeben.
   - **Schlüsselwort Kategorie** - tippen Sie den Namen der Regel in dieses Feld.
   - **Schlüsselwort** - geben Sie das Wort oder den Satzteil, den Sie blockieren möchten, in das Feld ein.Wenn Sie möchten dass nur ganze Wörter erkannt werden, wählen Sie **ganze Wörter** Kontrollkästchen.
3. Wählen Sie den Filtertyp.
   - **Anzeigen blockieren** - Wählen Sie diese Option für Regeln, die verhindern sollen, dass unangemessene Wörter angezeigt werden.
   - **Senden blockieren** - wählen Sie diese Option für Regeln, die geschaffen wurden um zu verhindern, dass wichtigen Informationen versendet werden.
4. Wählen Sie den Datenverkehrstyp, den Bitdefender nach den definierten Wortenscannen soll.

Optionen	Beschreibung
Web	Internet Seiten, die Schlüsselwörter enthalten, werden geblockt.
E-Mail	E-Mail Nachrichten, die das Schlüsselwort enthalten werden blockiert.

Optionen	Beschreibung
Instant Messaging	Sofortnachrichten, die das Schlüsselwort enthalten werden blockiert.

5. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

Ab jetzt wird jeder Versuch, die festgelegten Daten (über E-Mail, Sofortnachricht oder eine Webseite) zu senden, fehlschlagen. Es wird eine Benachrichtigung eingeblendet, dass Bitdefender nicht zugelassen hat, dass identitätsspezifische Inhalte versendet wurden.

Regeln für die Schlüsselwortfilterung verwalten

Die konfigurierten Schlüsselwortfilterregeln werden in der Tabelle aufgelistet. Dort finden Sie detaillierte Informationen zu jeder Regel.

Um eine Regel zu entfernen, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Rechtsklicken Sie auf eine Regel, um sie zu bearbeiten (oder wählen Sie sie aus und klicken Sie dann auf **Bearbeiten**).Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

8.1.4. Instant Messenger Kontrollassistent

Die Instant Messaging (IM) Kontrolle gibt Ihnen die Möglichkeit IM-Kontakte festzulegen, mit denen Ihre Kinder chatten dürfen.

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 **Instant 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 Sofortnachrichtenregeln

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 E-Mail Adresse oder den Nutzernamen, der von dem IM Kontakt genutzt wird, in das Feld **E-Mail 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 **Blocken**.
5. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

Verwalten der Sofortnachrichtenregeln

Die konfigurierten IM-Kontrollregeln werden in der Tabelle unten im Bildschirmfensteraufgelistet.

Um eine Regel zu entfernen, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Rechtsklicken Sie auf eine Regel, um sie zu bearbeiten (oder wählen Sie sie aus und klicken Sie dann auf **Bearbeiten**).Nehmen Sie die notwendigen Änderungen im Konfigurationsfenster vor.

8.1.5. Kategoriefilter

Der Kategoriefilter filtert den Zugriff auf Webseiten dynamisch anhand derer Inhalte.Wenn Sie die Kindersicherung aktivieren und das Alter Ihres Kindes angeben, wird der Kategoriefilter automatisch alle Website-Kategorien blockieren, die als unangemessen für diese Altersklasse angesehen werden.Diese Konfiguration ist in den meisten Fällen ausreichend.

Wenn Sie die Inhalte, denen Ihr Kind im Internet ausgesetzt ist, besser kontrollieren möchten, können Sie bestimmte Website-Kategorien auswählen, die vom Kategoriefilter blockiert werden sollen.

Um die Einstellungen des Kategoriefilters im Detail zu überprüfen und zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Einstellungen-Fenster der Bitdefender-Kindersicherung für das entsprechende Benutzerkonto.
2. Klicken Sie auf den Reiter **Kategorien**.
3. Die Kategoriesteuerung ist standardmäßig aktiviert.Sie können die Kategoriesteuerung auch deaktivieren und mithilfe der Website-Steuerung selbst eine Liste mit bestimmten Websites anlegen, die blockiert werden sollen. Dies wird aber nicht empfohlen.
4. Sie können nun überprüfen, welche Web-Kategorien für die aktuell ausgewählteAltersgruppe automatisch gesperrt/beschränkt werden.Wenn beispielsweise der Status der Kategorie Suchmaschine auf **Blockiert** gesetzt ist, darf Ihr Kind keine Suchmaschinen benutzen.Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie diese nach Ihren Wünschen konfigurieren.

   Um die Aktion zu verändern, die für eine bestimmte Web-Inhaltskategorie konfiguriert wurde, klicken Sie auf den aktuellen Status und wählen Sie die gewünschte Aktion aus dem Menü.

8.2. Überwachen der Aktivitäten Ihrer Kinder

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.

8.2.1. Überprüfen der Kindersicherungsprotokolle

Eine Aufzeichnung darüber, was Ihre Kinder kürzlich auf dem Computer gemacht haben, finden Sie im Kindersicherungsprotokoll.Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Ereignisse**.
3. Klicken Sie im Menü links auf **Kindersicherung**.

Beachten Sie

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).Für weitere Informationen lesen Sie bitte *„Netzwerkplan“* (S. 111).

Das Kindersicherungsprotokoll bietet detaillierte Informationen über die Aktivitäten Ihrer Kinder auf dem Computer und im Internet.Die Information befinden sich in mehreren Reitern:

Ereignisse

Hier erhalten Sie detaillierte Informationen über die Kindersicherungsaktivitäten (wie beispielsweise die Kindersicherung aktiviert/deaktiviert wird, welche Ereignisse gesperrt wurden).

Klicken Sie auf eine Ereignis, um mehr darüber zu erfahren.

Anwendungsnutzung

Hilft Ihnen herauszufinden, welche Anwendungen Ihre Kinder kürzlich aufgerufenhaben.

Sie können Informationen nach Benutzer und Zeitspanne filtern.Klicken Sie auf eine Ereignis, um mehr darüber zu erfahren.

Internet-Protokoll

Hilft Ihnen herauszufinden, welche Webseiten Ihre Kinder kürzlich aufgerufen haben.

Sie können Informationen nach Benutzer und Zeitspanne filtern.Klicken Sie auf eine Ereignis, um mehr darüber zu erfahren.

8.2.2. E-Mail-Benachrichtigung konfigurieren

Um Email-Benachrichtigungen zu erhalten, wenn die Kindersicherung eine Aktivitätsperrt:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Kindersicherung** und danach auf den Reiter **Einstellungen**.
4. Aktivieren Sie die Option **Aktivitätsberichte per E-Mail senden**, indem Sie auf den entsprechenden Schalter klicken.
5. Sie werden aufgefordert die E-Mail-Kontoeinstellungen zu konfigurieren. Klicken Sie **Ja** um das Konfigurationsfenster zu öffnen.

   Beachten Sie
   Sie können das Konfigurationsfenster später öffnen indem Sie **Benachrichtigungseinstellungen** klicken.

6. Geben Sie die Email-Adresse, an die Benachrichtigungen gesendet werden sollen, ein.

7. 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 E-Mail-Client-Einstellungen verwenden
   Diese Option ist voreingestellt, wenn Bitdefender die Mail Server-Einstellungen von Ihrem Mail Client importieren kann.

   Die eines bekannten Servers wählen
   Wählen Sie diese Option, wenn Sie einen Email-Account bei einem der in der Liste genannten web-basierten Dienste haben.

   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:

   - **Ausgehnder SMTP Server** - geben Sie die Adresse des Mail Servers, der für das Verschicken der E-Mails zuständig ist, ein.
   - Falls der Server einen anderen als den Standardport 25 nutzt, geben Sie diesen bitte im entsprechenden Feld an.
   - Falls der Server Authentifikation verlangt, wählen Sie **Mein SMTP Server erfordert Authentifikation** aus und geben den Benutzernamen und das Passwort in die dazugehörigen Felder ein.
   - Wenn der Server eine sichere SSL-Verbindung benötigt, markieren Sie das Kästchen **SSL verwenden**.

8. 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.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

8.3. Fern-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.

8.3.1. Voraussetzungen für die Nutzung der Fern-Kindersicherung

Um die Remote Kindersicherung nutzen zu können, müssen Sie folgende Vorbedingungen erfüllen:

1. Installieren Sie entweder Bitdefender Internet Security 2012 oder Bitdefender Total Security 2012 auf dem Computer Ihrer Kinder.

2. Achten Sie darauf, dass Sie die Produktregistrieren abschließen, indem Sie Ihr Produkt mit einem MyBitdefender-Konto verknüpfen.Für weitere Informationen lesen Sie bitte „*Produktregistrierung*“ (S. 8).
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.

8.3.2. 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 das Bitdefender-Fenster.
3. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
4. Klicken Sie im Menü links auf **Kindersicherung** und danach auf den Reiter **Einstellungen**.
5. Aktivieren Sie die Fern-Kindersicherung mithilfe des entsprechenden Schalters.Die Remote Kindersicherung wird für alle Benutzerkonten auf diesem System aktiviert.

8.3.3. Zugriff auf die Remote Kindersicherung

Melden Sie sich bei MyBitdefender an, um auf die Fern-Kindersicherung zuzugreifen.

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   https://my.bitdefender.com
2. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
3. Klicken Sie unter Dienste auf **Hilfe für Eltern**, um das Dashboard für die Fern-Kindersicherung aufzurufen.
4. Ihnen werden alle Computer und die dazugehörigen Benutzerkonten angezeigt, für die die Fern-Kindersicherung aktiviert ist.Für jedes Benutzerkonto stehen drei Schaltflächen zur Verfügung:
   - **Benachrichtigungen** - Hier können Sie überprüfen, welche Aktivitäten für das jeweilige Benutzerkonto seit Ihrer letzten Anmeldung blockiert wurden.
   - **Aktivität** - Hier können Sie die kürzlichen Aktivitäten Ihrer Kinder überprüfen.
   - **Einstellungen** - Hier können Sie die Einstellungen der Kindersicherung für das jeweilige Benutzerkonto anpassen.

Wenn Sie auf eine dieser Schaltflächen klicken, gelangen Sie in den Bereich der Fern-Kindersicherung für das entsprechende Benutzerkonto.

8.3.4. Überwachen der Aktivitäten Ihrer Kinder per Fernzugriff

Bevor Sie die Computer-Aktivitäten Ihrer Kinder per Fernabfrage überwachen können, müssen Sie auf deren Computern die Remote Kindersicherung aktivieren.Für weitere Informationen lesen Sie bitte *„Aktivierung der Remote Kindersicherung“* (S. 95).

Um per Fernsteuerung zu überwachen, was Ihre Kinder auf deren Computern machen:

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   https://my.bitdefender.com

2. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei Ihrem Konto an.
3. Klicken Sie unter Dienste auf **Hilfe für Eltern**, um das Dashboard für die Fern-Kindersicherung aufzurufen.
4. Finden Sie das Benutzerkonto, das Ihr Kind nutzt, und klicken Sie auf eine der folgenden Schaltflächen:

   - **Benachrichtigungen** - Hier können Sie überprüfen, welche Aktivitäten für das jeweilige Benutzerkonto seit Ihrer letzten Anmeldung blockiert wurden.
   - **Aktivität** - Hier können Sie die kürzlichen Aktivitäten Ihrer Kinder überprüfen.

Auf der Benachrichtigungsseite sehen Sie, welche Webseiten, Anwendungen oder Sofortnachrichtenkontakte seit der letzten Anmeldung blockiert wurden.Um eine Einschränkung zu entfernen, klicken Sie auf die entsprechende **Zulassen**-Schaltfläche.

Auf der Aktivitätsseite finden Sie nützliche Informationen über die kürzlichen Aktivitäten Ihrer Kinder:

- 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 Website, eine Anwendung oder einen Sofortnachrichtenkontakt sofort blockieren, indem Sie auf die entsprechende **Blockieren**-Schaltfläche klicken.

Um die angezeigten Daten zu filtern, klicken Sie auf **Anzeigen** und wählen Sie gewünschte Option aus.

8.3.5. Verändern der Kindersicherungseinstellungen per Fernzugriff

Bevor Sie per Fernsteuerung die Einstellungen der Kindersicherung ändern können, müssen Sie erst die Option "Remote Kindersicherung" auf den Computern Ihrer Kinder aktivieren.Für weitere Informationen lesen Sie bitte *„Aktivierung der Remote Kindersicherung“* (S. 95).

Änderung der Kindersicherungseinstellung per Fernsteuerung (Remote):

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   https://my.bitdefender.com

2. Loggen Sie sich mit Ihrem Benutzernamen und Passwort in Ihr Bitdefender-Benutzerkonto ein.
3. Klicken Sie unter Dienste auf **Hilfe für Eltern**, um das Dashboard für die Fern-Kindersicherung aufzurufen.Sie können alle Benutzerkonten sehen, für die die Remote Kindersicherung aktiviert ist.
4. Finden Sie das Benutzerkonto, das Ihr Kind nutzt, und klicken Sie auf eine der folgenden Schaltflächen:
   - **Benachrichtigungen** - Hier können Sie eine Liste der Aktivitäten abrufen, die kürzlich blockiert wurden, sowie Einschränkungen entfernen.
   - **Aktivität** - Hier können Sie die kürzlichen Aktivitäten Ihrer Kinder überprüfen und nicht erwünschte Aktivitäten blockieren.
   - **Einstellungen** - Hier können Sie die Einstellungen der Kindersicherung für das jeweilige Benutzerkonto anpassen.
5. Definieren und entfernen Sie Beschränkungen nach Ihren Wünschen.

Zeitliche Beschränkung des Internet-Zugangs

Unter **Einstellungen** finden Sie den **Zeitplan für den Internet-Zugang**, mit dessen Optionen Sie festlegen können, wann Ihr Kind Zugriff auf das Internet hat.

Um Beschränkung des Internetzugangs auf bestimmte Tageszeiten festzulegen:

1. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert sein soll.Um eine neue Auswahl zu starten, klicken Sie auf **Alle blockieren** oder **Alle zulassen**.
2. Klicken Sie auf **Speichern**.

Um den Internet-Zugang vollständig zu sperren, klicken Sie unterhalb des Zeitrasters auf **Alle blockieren** und danach auf **Speichern**.

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.

Blockieren von Websites

Blockierung einer Webseite:

1. Rufen Sie die Seite **Einstellungen** auf.
2. Geben Sie die Website in das entsprechende Feld ein.
3. Klicken Sie auf **Übermitteln**.Die Website wird der Liste der ausstehenden Aktionen hinzugefügt.Falls Sie es sich anders überlegen, klicken Sie auf die entsprechende **Aktion abbrechen**-Schaltfläche.

Beachten Sie

Alternativ können Sie die Seite **Aktivität** aufrufen, die Liste der besuchten Websites anzeigen und auf die entsprechende **Blockieren**-Schaltfläche klicken, wenn Sie eine Website blockieren wollen.

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.

Blockieren von Sofortnachrichtenkontakten

Instant Messaging mit einem bestimmten Kontakt blockieren:

1. Rufen Sie die Seite **Einstellungen** auf.
2. Geben Sie im entsprechenden Feld die Kontaktinformationen ein.
3. Klicken Sie auf **Blockieren**.Der Sofortnachrichtenkontakt wird der Liste der ausstehenden Aktionen hinzugefügt.Falls Sie es sich anders überlegen, klicken Sie auf die entsprechende **Aktion abbrechen**-Schaltfläche.

Beachten Sie

Alternativ können Sie die Seite **Aktivität** aufrufen, die Liste der Kontakte anzeigen, mit denen Ihr Kind Sofortnachrichten ausgetauscht hat, und auf die entsprechende **Blockieren**-Schaltfläche klicken, wenn Sie einen unerwünschten Kontakt finden.

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.

Blockieren von Anwendungen

Um eine Anwendung zu blockieren:

1. Rufen Sie die **Aktivitäts**seite auf.
2. Überprüfen Sie die Liste der aufgerufenen Anwendungen und klicken Sie auf die entsprechende **Blockieren**-Schaltfläche, wenn Sie eine unerwünschte Anwendung entdecken.

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.

Blockierungen von Webseiten, Anwendungen oder Sofortnachrichtenkontakten aufheben

Auf der Benachrichtigungsseite werden die Websites, Anwendungen und Sofortnachrichtenkontakte angezeigt, die von der Kindersicherung blockiert wurden.Um eine Einschränkung zu entfernen, klicken Sie auf die entsprechende **Zulassen**-Schaltfläche.Die Einschränkung wird nach der nächsten Synchronisation mit der Website für die Fern-Kindersicherung vom Computer Ihres Kindes entfernt (innerhalb von maximal 10 Minuten).

9. Firewall

Schützt Ihren Computer vor unerwünschten Verbindungen.Sie funktioniert im Prinzip wie ein Wächter an Ihrem Tor - sie überwacht alle Verbindungsversuche und entscheidet, welche Verbindungen zugelassen und welche blockiert werden.

Beachten Sie
Die Firewall ist ein unersetzliches Instrument bei einer DSL- oder Breitbandverbindung.

Wenn Sie auf Ihrem Computer Windows Vista oder Windows 7 nutzen, wird Bitdefender automatisch jeder erkannten Netzwerkverbindung den entsprechenden Netzwerktyp zuordnen.Auf Computern mit Windows XP werden Sie aufgefordert, den Netzwerktyp auszuwählen.Um mehr über die Firewall-Einstellungen für jeden Netzwerktyp und die Bearbeitung der Netzwerkeinstellungen zu erfahren, lesen Sie bitte das Kapitel *„Konfigurieren der Einstellungen für die Netzwerkverbindung“ (S. 101)*.

Die Bitdefender-Firewall nutzt eine Regelwerk, um den eingehenden und ausgehenden Datenverkehr auf Ihrem System zu filtern.Die Regeln sind in drei Kategorien unterteilt:

Allgemeine Regeln
: Regeln, mit denen die Protokolle festgelegt werden, über die die Kommunikation stattfinden darf.

  Dabei kommt ein Standardregelwerk zum Einsatz, das optimalen Schutz gewährleistet.Sie können die Regeln bearbeiten, indem Sie Verbindungen über bestimmte Protokolle zulassen oder verweigern.

Anwendungsregeln
: Regeln, die festlegen, wie jede einzelne Anwendung auf Netzwerkressourcen und das Internet zugreifen kann.

  Unter normalen Umständen legt Bitdefender automatisch eine Regel an, sobald eine Anwendung versucht, auf das Internet zuzugreifen.Sie können Anwendungsregeln zudem manuell hinzufügen oder bearbeiten.

Adapterregeln
: Regeln, die festlegen, ob Ihr Computer mit bestimmten anderen Computern kommunizieren darf.

  Sie müssen Regeln anlegen, um Datenverkehr ausdrücklich zuzulassen oder zu verweigern.

Das Angriffserkennungssystem bietet zusätzlichen Schutz.Das Angriffserkennungssystem überwacht das Netzwerk und Systemaktivitäten, um Malware-Aktivitäten und Richtlinienverstöße zu erkennen.Es erkennt und blockiert Versuche, kritische Systemdateien, Bitdefender-Dateien und Registry-Einträge zu

verändern. Darüber hinaus erkennt es die Installation von Malware-Treibern und Angriffe durch Code-Injektionen (DLL-Injektionen).

9.1. Aktivieren / Deaktivieren des Firewall-Schutzes

Um den Firewall-Schutz zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den Bereich **Firewall**.
3. Klicken Sie auf den Firewall-Schalter.

Warnung

Die Deaktivierung der Firewall sollte immer nur von kurzer Dauer sein, da Ihr Computer so der Gefahr durch nicht autorisierte Verbindungen ausgesetzt wird.Aktivieren Sie die Firewall so schnell wie möglich wieder.

9.2. Konfigurieren der Einstellungen für die Netzwerkverbindung

Um die Einstellungen für die Netzwerkverbindung anzuzeigen und zu bearbeiten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den Bereich **Firewall**.
3. Klicken Sie auf **Netzwerkdetails**.

Ein neues Fenster wird sich öffnen.Das Diagramm im oberen Teil des Fensters zeigt Ihnen Informationen zum eingehenden und ausgehenden Datenverkehr in Echtzeit.

Unter dem Diagramm werden die folgenden Informationen zu jeder Netzwerkverbindung angezeigt:

- **Netzwerktyp** - Der Netzwerktyp, mit dem Ihr Computer verbunden ist.Bitdefender verwendet grundlegende Firewall-Einstellung in Abhängigkeit von dem Netzwerktyp, mit dem Sie verbunden sind.

  Sie können den Netzwerktyp ändern, indem Sie das Dropdown-Menü unter **Netzwerktyp** öffnen und einen der verfügbaren Netzwerktypen aus der Liste auswählen.

Netzwerktyp	Beschreibung
Vertrauenswürdig	Deaktiviert die Firewall für den entsprechenden Adapter.
Heim/Büro	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.

Netzwerktyp	Beschreibung
Öffentlich	Sämtlicher Datenverkehr wird gefiltert.
Unsicher	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

- **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
An	Stealth-Modus ist aktiviert.Ihr Computer ist sowohl im lokalen Netzwerk als auch im Internet unsichtbar.
Aus	Stealth-Modus ist deaktiviert.Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken.
Remote	Ihr Computer kann nicht im Internet entdeckt werden.Benutzer im lokalen Netzwerk können Ihren Computer entdecken

- **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**.

9.3. Einbruchserkennung

Um das Angriffserkennungssystem zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Einstellungen**.
4. Um das Angriffserkennungssystem zu aktivieren, klicken Sie auf den entsprechenden Schalter.
5. Schieben Sie den Regler in die gewünschte Schutzstufenposition.Nutzen Sie die Beschreibung auf der rechten Seite der Skala, um die Stufe zu wählen, die für Ihre Sicherheitsbedürfnisse am besten geeignet ist.

Im Ereignis-Fenster können Sie überprüfen, welche Anwendungen vom Angriffserkennungssystem erkannt wurden.

Sie können für Anwendungen, denen Sie vertrauen und die daher nicht vom Angriffserkennungssystem gescannt werden sollen, Ausschlussregeln festlegen.Um eine Anwendung vom Scan auszuschließen, befolgen Sie die Anweisungen im Kapitel *„Verwalten von ausgeschlossenen Prozessen“* (S. 61).

Beachten Sie

Die Ausführung des Angriffserkennungssystems steht im Zusammenhang mit der Ausführung von Active Virus Control.Ausschlussregeln für Prozesse gelten für beide Systeme.

9.4. Konfigurieren der Datenverkehrseinstellungen

Um die Datenverkehrseinstellung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Einstellungen**.

Die folgenden Funktionen könne im Bereich **Datenverkehr** aktiviert oder deaktiviert werden.

- **Unterstützung für die Gemeinsame Nutzung der Internetverbindung aktivieren** - Aktiviert die Unterstützung für die Gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing).

  Beachten Sie

  Diese Option erlaubt nicht automatisch ICS auf Ihrem System sondern erlaubt diese Art von Verbindung nur, wenn Sie es von Ihrem Betriebssystem aus freigeben.

- **Portscans blockieren** - entdeckt und blockiert Versuche offene Ports zu finden.

  Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Computer geöffnet sind.Wenn Sie dann einen unsicheren Port finden, können Sie in Ihren Computer eindringen.

- **Ausführliche Protokolle** - Sie erhalten ein ausführlicheres Firewall-Protokoll.

  Bitdefender erstellt ein Protokoll der Ereignisse, die im Zusammenhang mit der Nutzung des Firewall-Moduls auftreten (Aktivieren/Deaktivieren der Firewall, Blockieren des Datenverkehrs, Einstellungsänderungen) und die durch Aktivitäten erzeugt wurden, die von diesem Modul erkannt wurden (Port-Scans, regelbasiertes Blockieren von Verbindungsversuchen und Datenverkehr).Das Protokoll kann über das Fenster **Firewall-Aktivität** aufgerufen werden, indem Sie auf **Protokoll anzeigen** klicken.Die Protokolldatei finden Sie unter `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

- **WLAN Benachrichtigungen aktivieren** - wenn Sie mit einem drahtlosen Netzwerk verbunden sind, werden Informationsfenster bezüglich bestimmter Netzwerkereignisse angezeigt (z.B. wenn ein neuer Computer dem Netzwerk beitritt).

9.5. Allgemeine Regeln

Wenn Daten über das Internet übertragen werden, werden bestimmte Protokolle genutzt.

Über die allgemeinen Regeln können Sie die Protokolle konfigurieren, über die Datenverkehr stattfinden darf.Um die Regeln zu bearbeiten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Unter Firewall-Regeln, klicken Sie auf **Allgemeine Regeln**.

Ein neues Fenster wird sich öffnen.Die aktuellen Regeln werden angezeigt.

Um eine Regel zu bearbeiten, klicken Sie in der Spalte **Aktion** auf den entsprechenden Pfeil und wählen Sie **Zulassen** oder **Verweigern**.

DNS über UDP / TCP
DNS über UDP und TCP zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Eingehende ICMP / ICMPv6
ICMP- / ICMPv6-Nachrichten zulassen oder verweigern.

ICMP-Nachrichten werden häufig von Hackern für Angriffe auf Computer-Netzwerke genutzt.Diese Verbindungsart wird standardmäßig verweigert.

Versenden von E-Mails
Versand von E-Mails über SMTP zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Web-Browsing HTTP
HTTP-Browsing zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Eingehende Remote-Desktop-Verbindungen
Den Zugriff anderer Computer über Remote-Desktop-Verbindungen zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig zugelassen.

Windows-Explorer-Datenverkehr auf HTTP / FTP

HTTP- und FTP-Datenverkehr aus Windows Explorer heraus zulassen oder verweigern.

Diese Verbindungsart wird standardmäßig verweigert.

9.6. Anwendungsregeln

Klicken Sie auf **Anwendungsregeln**, um die Firewall-Regeln anzuzeigen und zu verwalten, die den Zugang von Anwendungen zu Netzwerkressourcen und dem Internet steuern.

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Klicken Sie im Bereich Firewall-Regeln auf **Anwendungsregeln**.

Sie können die Programme (Prozesse), für die Firewall-Regel erstellt wurde, in der Tabelle sehen.Um die Regeln einzusehen, die für eine bestimmte Anwendung angelegt wurden, klicken Sie auf das +-Kästchen neben der entsprechenden Anwendung oder doppelklicken Sie einfach darauf.

Für jede Regel werden die folgenden Informationen angezeigt:

- **Prozess-/Netzwerktypen** - Die Prozess- und Netzwerkadaptertypen für die die Regel angewendet wird.Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes 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).
- **Protokoll** - das IP-Protokoll für das die Regel angewendet wird.Sie werden eines der Folgenden sehen:

Protokoll	Beschreibung
Alle	Beinhaltet alle IP-Protokolle.
TCP	Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle am Datenaustausch beteiligten Computer kennen diese Vereinbarungen und befolgen sie. Es ist damit ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Computernetzwerken. Es ist Teil der TCP/IP-Protokollfamilie. Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, dauerte mehrere Jahre. Die erste Standardisierung von

Protokoll	Beschreibung
	TCP erfolgte deshalb erst im Jahre 1981 als RFC 793. TCP stellt einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt.
UDP	User Datagram Protocol (UDP) ist ein minimales, verbindungsloses Netzprotokoll. Es gehört zur Transportschicht der TCP/IP-Protokollfamilie und ist im Gegensatz zu TCP nicht auf Zuverlässigkeit ausgelegt. UDP erfüllt im Wesentlichen den Zweck, die durch die IP-Schicht hergestellte Endsystemverbindung um eine Anwendungsschnittstelle (Ports) zu erweitern. Die Qualität der darunter liegenden Dienste, insbesondere die Zuverlässigkeit der Übertragung, erhöht UDP hingegen nicht.
Eine Nummer	Stellt ein besonderes IP-Protokoll dar (anders als TCP und UDP).Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Aktion** - Gibt an, ob der Zugriff der Anwendung auf das Netzwerk oder das Internet unter den festgelegten Umständen zugelassen oder verweigert wird.

Um die Regeln zu veralten, nutzen Sie die Schaltflächen im unteren Bereich des Fensters:

- **Regel hinzufügen** - Öffnet das Fenster Anwendungsregel hinzufügen. Hier können Sie eine neue Regel anlegen.
- **Regel bearbeiten** - Öffnet das Fenster Anwendungsregel bearbeiten, in dem Sie die Einstellungen für eine ausgewählte Regel bearbeiten können.
- **Regel entfernen** - Löscht die ausgewählte Regel.

Anwendungsregeln hinzufügen / bearbeiten

Um eine Anwendungsregel hinzuzufügen oder zu bearbeiten, klicken Sie auf die entsprechende Schaltfläche.Ein neues Fenster wird geöffnet. Gehen Sie wie folgt vor:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird.
- **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, können sie die Markierung im Kästchen **Alle** aufheben und eine bestimmte IP-Adresse eingeben.

- **Remote-Adresse.** Bestimmen Sie die Remote-IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie dessen IP-Adresse an.
- **Netzwerktyp.** Wählen Sie den Netzwerktyp aus, für den die Regel angewendet werden soll.
- **Ereignisse.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, für die die Regel angewendet werden soll.Folgende Ereignisse können auftreten:

Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen.Mit Verbindungsprotokollen 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, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Protokoll.** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - Wenn Sie möchten, dass die Regel für ein bestimmtes Protokoll angewendet wird, wählen Sie **Andere**.Ein Editierfeld wird erscheinen.Geben Sie die dem Protokoll, das gefiltert werden soll, zugewiesene Nummer in das Editierfeld ein.

    Beachten Sie

    Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen.Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

Richtung	Beschreibung
Ausgehend	Die Regeln beziehen sich nur auf ausgehenden Datenverkehr.
Eingehend	Die Regeln beziehen sich nur auch eingehenden Datenverkehr.
Beide	Die Regeln finden in beide Richtungen Anwendung.

- **IP-Version.** Wählen Sie aus dem Menu die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Erlaubnis.** Wählen Sie eine der zur Verfügung stehenden Erlaubnis-Optionen:

Erlaubnis	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

9.7. Adapterregeln

Für jede Netzwerkverbindung können Sie spezielle vertrauenswürdige oder nicht vertrauenswürdige Zonen konfigurieren.

Ein vertrauenswürdige Zone ist ein Gerät (zum Beispiel ein anderer Computer oder ein Drucker), dem Sie uneingeschränkt vertrauen.Jeglicher Datenverkehr zwischen Ihrem Computer und einem vertrauenswürdigen Gerät wird zugelassen.Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Eine nicht vertrauenswürdige Zone ist ein Gerät, das mit Ihrem Computer unter keinen Umständen kommunizieren soll.

Um die Zonen in Ihren Netzwerkadaptern anzuzeigen und zu verwalten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Klicken Sie im Bereich Firewall-Regeln auf **Adapterregeln**.

Ein neues Fenster wird sich öffnen.Die aktuellen Netzwerkzonen werden pro Adapter angezeigt.

Um die Zonen zu verwalten, nutzen Sie die Schaltflächen im oberen Bereich des Fensters:

- **Zone hinzufügen** - Öffnet das Fenster IP-Adresse hinzufügen, in dem Sie eine neue Zone für einen ausgewählten Adapter anlegen können.
- **Zone bearbeiten** - Öffnet das Fenster Regel bearbeiten. Hier können Sie die Einstellungen für die ausgewählte Zone bearbeiten.
- **Zone entfernen** - Löscht die ausgewählte Zone.

Hinzufügen / Bearbeiten von Zonen

Um eine Zone hinzuzufügen oder zu bearbeiten, klicken Sie auf die entsprechende Schaltfläche.Ein neues Fenster mit den IP-Adressen der mit dem Netzwerk verbundenen Geräte wird angezeigt.Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers, den Sie hinzufügen wollen, aus oder geben Sie eine Adresse oder einen Adressbereich in das entsprechende Textfeld ein.
2. Wählen Sie eine Aktion:
   - **Erlauben** - 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**, um die Änderungen zu speichern und das Fenster zu schließen.

9.8. Überwachen der Netzwerkaktivität

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 das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Unter Netzwerkaktivität, klicken Sie auf **Firewall-Aktivität**.

Ein neues Fenster wird sich öffnen.Hier können Sie den Datenvekehr sortiert nach Anwendung einsehen. Für jede Anwendung können Sie die Verbindungen und offenen Ports sehen. Ausserdem Statistiken zum ausgehenden &eingehenden Datenverkehr.

Neben jeder Verbindung wird ein Symbol angezeigt.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 ausgrauen, und evtl. verschwinden.Das selbe kann auch mit Anwendungen im Fenster geschehen welche geschlossen werden.

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**.

10. Netzwerkplan

Mit dem Netzwerk-Modul können Sie die auf den Computern Ihres Haushalts installierten Bitdefender-Produkte von einem Computer aus verwalten.

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-Netzwerk auf Ihrem Computer.Legen Sie Ihren Computer als **Server-Computer** fest.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).Definieren Sie jeden Computer als **normalen Computer**.
3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

10.1. Aktivieren des Bitdefender-Netzwerks

Um das Bitdefender-Netzwerk zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Netzwerkplan**.
4. Klicken Sie **Netzwerk aktivieren**.Sie werden aufgefordert, das Verwaltungspasswort für den Netzwerkplan festzulegen.
5. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
6. Legen Sie die Rolle des Computers im Bitdefender-Netzwerkplan fest:
   - **Server-Computer** - Aktivieren Sie diese Option auf dem Computer, der zur Verwaltung der anderen Computer eingesetzt wird.
   - **Normaler Computer** - Aktivieren Sie diese Option auf den Computern, die von dem Server-Computer verwaltet werden.
7. Klicken Sie auf **OK**.

   Sie sehen den Namen des Computers in der Netzwerkübersicht.

   Die Schaltfläche **Verbindung deaktivieren** wird eingeblendet.

Beachten Sie

Sie können den Netzwerkplan auch vom Bitdefender-Hauptfenster aus aktivieren:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den Bereich **Netzwerkplan**.

3. Klicken Sie auf **Verwalten** und wählen Sie dann **Netzwerk aktivieren** aus dem Dropdown-Menü.

10.2. Hinzufügen von Computern zum Bitdefender-Netzwerk

Jeder Computer, der die folgenden Kriterien erfüllt, wird automatisch dem Netzwerk hinzugefügt:

- der Bitdefender-Netzwerkplan wurde auf dem 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
Sie können den Netzwerkplan jederzeit nach Computern durchsuchen, die diese Kriterien erfüllen, indem Sie auf die Schaltfläche **Autom. Erkennung** klicken.

Um einen Computer manuell vom Server-Computer aus zum Bitdefender-Netzwerkplan hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Netzwerkplan**.
4. Klicken Sie auf **PC hinzufügen**.
5. Geben Sie das Passwort für die Verwaltung ein und klicken Sie auf **OK**.Ein neues Fenster wird sich öffnen.

   Sie können eine Liste der Computer im Netzwerk sehen.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.
6. Sie können hierzu eine der folgenden Methoden wählen:
   - Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.
7. Klicken Sie auf **Hinzufügen**.
8. Geben Sie das Verwaltungspasswort ein, dass auf dem jeweiligen Computer angelegt wurde.

9. Klicken Sie auf **OK**.Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

10.3. Verwalten des Bitdefender-Netzwerks

Nachdem Sie einen Bitdefender-Netzwerkplan erfolgreich angelegt haben, können Sie alle Bitdefender-Produkte vom Server-Computer aus verwalten.

Um mehrere Aufgaben auf allen verwalteten Computern auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den Bereich **Netzwerkplan**.
3. Klicken Sie auf **Verwalten** und wählen Sie die entsprechenden Schaltflächen aus dem Dropdown-Menü:
   - **Verbindung deaktivieren** - Hiermit können Sie das Netzwerk deaktivieren.
   - **Alle prüfen** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu prüfen.
   - **Alle aktualisieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu aktualisieren.

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen, werden Sie aufgefordert, das lokale Verwaltungspasswort anzugeben.Geben Sie das Passwort für die Verwaltung ein und klicken Sie auf **OK**.

Um den gesamten Netzwerkplan anzuzeigen und auf alle Verwaltungsaufgaben zuzugreifen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Netzwerkplan**.

Wenn Sie den Mauszeiger auf einen Computer im Netzwerkplan bewegen, erhalten Sie über diesen Computer Kurzinformationen (IP-Adresse, Anzahl der Probleme, die die Sicherheit des Systems beeinträchtigen, 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.

Produkt registrieren
Erlaubt Ihnen Bitdefender auf diesen Rechner, durch Eintragen eines Lizenzschlüssels, zu registrieren.

Passwort für Produkteinstellungen konfigurieren
Erlaubt Ihnen einen Passwort zu erstellen um den Zugang zu den Bitdefender Einstellungen auf diesem PC einzuschränken.

Bedarf-Scan-Aufgabe starten
Ermöglicht Ihnen das Ausführen von Bedarf-Scans auf einem Remote-Computer. Sie können die folgenden Scan-Aufgaben durchführen: Quick Scan oder vollständiger System-Scan.

Alle Probleme beheben
Lässt Sie alle Risiken die die Sicherheit Ihres Systems gefährden beheben, indem Sie dem Alle Risiken beheben Assistenten folgen.

Ereignisse anzeigen
Ermöglicht Ihnen den Zugriff auf das **Ereignis**-Modul des Bitdefender-Produkts, das auf diesem Computer installiert ist.

Update Now
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 festlegen
Erlaubt Ihnen, diesen Rechner als Update-Server, für alle Rechner des Netzwerks auf denen wo Bitdefender installiert ist, festzulegen.Unter Verwendung dieser Option, wird der Internetverkehr verringert, weil nur ein Rechner aus dem Netzwerk sich an das Internet anschließt um die Updates herunterzuladen.

Den PC aus dem Netzwerkplan entfernen
Erlaubt Ihnen einen Pc aus dem Netzwerk entfernen.

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.

11. Update

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie Bitdefender stets mit den neuesten Malware-Signaturen 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 neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Der Update-Vorgang wird "on-the-fly" durchgeführt. Das bedeutet, dass die Dateien, die aktualisiert werden sollen, nach und nach ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

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

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

- Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen wie unter *„Wie konfiguriere ich Bitdefender für die Nutzung einer Proxy-Verbindung?“* (S. 38) beschrieben konfigurieren.
- Wenn Sie über keine Internet-Verbindung verfügen, können Sie Bitdefender, wie im Kapitel *„Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren? “* (S. 127) beschrieben, auch manuell aktualisieren.Die Datei für das manuelle Update wird einmal pro Woche veröffentlicht.
- Bei einer langsamen Internetverbindung können Fehler beim Herunterladen von Updates auftreten.Um zu erfahren, wie Sie solche Fehlern vermeiden können, lesen Sie bitte das Kapitel *„Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann“* (S. 126).
- Falls Sie sich per Einwahl mit dem Internet verbinden, ist es sinnvoll, regelmäßig ein manuelles Bitdefender-Update durchzuführen.Für weitere Informationen lesen Sie bitte *„Durchführung eines Updates“* (S. 116).

11.1. Überprüfen, ob Bitdefender auf dem neuesten Stand ist

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

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Update**-Bereich.

3. Der Zeitpunkt des letzten Updates wird direkt unter dem Namen des Bereichs eingeblendet.

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

1. Klicken Sie im Hauptfenster in der oberen Symbolleiste auf **Ereignisse**.
2. Klicken Sie im Menü links auf **Update**.

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

11.2. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Sie haben folgende Möglichkeiten, ein Update zu starten:

- Öffnen Sie das Bitdefender-Fenster, gehen Sie in den **Update**-Bereich und klicken Sie auf **Update jetzt durchführen**.
- Rechtsklicken Sie  in der Task-Leiste auf das Bitdefender-Symbol und wählen Sie **Update jetzt durchführen**.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates.Wenn ein Update erkannt wird, werden Sie abhängig von den Update-Einstellungen entweder aufgefordert, dies zu bestätigen oder das Update wird automatisch durchgeführt.

Wichtig

Möglicherweise kann ein Neustart nach Abschluss des Updates notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst zeitnah durchzuführen.

11.3. Aktivieren / Deaktivieren der automatischen Updates

Um das automatische Update zu aktivieren oder deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Update**-Bereich.
3. Klicken Sie auf den Schalter, um automatische Updates zu aktivieren oder deaktivieren.
4. Wenn Sie versuchen, automatische Updates zu deaktivieren, wird ein Warnfenster angezeigt.Sie müssen Ihre Einstellung bestätigen, indem Sie definieren, wie lange das automatische Update deaktiviert bleiben soll. Zur Verfügung stehen die

Optionen 5, 15 oder 30 Minuten, eine Stunde, immer oder bis zum nächsten Systemstart.

Warnung
Hierbei handelt es sich um ein großes Sicherheitsrisiko. Wir empfehlen, die Deaktivierung des automatischen Updates so kurz wie möglich zu halten, da Bitdefender Sie nur gegen die neuesten Bedrohungen schützen kann, wenn die Software immer auf dem neuesten Stand ist.

11.4. Update-Einstellungen anpassen

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

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

Um die Update-Einstellungen anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Update**.
4. Passen Sie die Einstellungen Ihren Anforderungen entsprechend an.

Update-Adresse

Bitdefender ist so konfiguriert, dass Updates von den Bitdefender-Update-Servern aus dem Internet heruntergeladen werden.Die Update-Adresse lautet `http://upgrade.bitdefender.com`. Dabei handelt es sich um eine allgemeine Internet-Adresse. Sie werden automatisch an den Bitdefender-Update-Server weitergeleitet, der Ihrem Standort am nächsten ist.

Verändern Sie die Update-Adresse nicht, es sei denn, Sie werden von einem Bitdefender-Mitarbeiter oder Ihrem Netzwerkadministrator (falls Sie mit einem Unternehmensnetzwerk verbunden sind) ausdrücklich dazu aufgefordert.

Wenn Sie Bitdefender auf mehreren Computern in Ihrem Haushalt installiert haben, können Sie ein Bitdefender-Heimnetzwerk einrichten und einen Ihrer Computer als Update-Server festlegen.Ausführliche Informationen finden Sie unter *„Netzwerkplan“ (S. 111)*.Die Bitdefender-Anwendung, die auf dem als Update-Server festgelegten Computer installiert ist, wird sich über das Internet aktualisieren. Die Bitdefender-Anwendungen auf den anderen Computern erhalten Ihre Updates über den lokalen Update-Server (deren Update-Adresse wird dementsprechend automatisch angepasst).Diese Konfiguration soll den Internet-Datenverkehr minimieren und Upgrades optimieren.

Klicken Sie auf **Standard**, um die ursprüngliche Update-Adresse wiederherzustellen.

Update-Verarbeitungsregeln

Es gibt drei Möglichkeiten, Updates herunterzuladen und zu installieren:

- **Update im Hintergrund** - Bitdefender Updates werden automatisch heruntergeladen und installiert.
- **Vor dem Download nachfragen** - Sobald ein Update verfügbar ist, werden Sie gefragt, ob es heruntergeladen werden soll.
- **Vor der Installation nachfragen** - Sobald ein Update heruntergeladen wurde, werden Sie gefragt, ob die Installation durchgeführt werden soll.

Manche Updates erfordern einen Neustart, um die Installation abzuschließen.Sollte ein Update einen Neustart erforderlich machen, arbeitet Bitdefender standardmäßig mit den alten Dateien weiter, bis der Benutzer den Computer aus eigenen Stücken neu startet. Dadurch soll verhindert werden, dass der Update-Prozess von Bitdefender den Benutzer in seiner Arbeit behindert.

Wenn Sie eine Meldung erhalten möchten, sobald ein Update einen Neustart erfordert, deaktivieren Sie die Option **Neustart verschieben**, indem Sie auf den entsprechenden Schalter klicken.

P2P-Updates

Neben dem normalen Update-Mechanismus, nutzt Bitdefender zudem ein intelligentes Update-Sharing-System, das ein Peer-to-Peer-Protokoll (P2P) nutzt, um Updates von Malware-Signaturen zwischen Bitdefender-Benutzern auszutauschen.

Sie können die P2P-Update-Optionen aktivieren oder deaktivieren, indem Sie auf die entsprechenden Schalter klicken.

P2P-Update-System verwenden

Aktivieren Sie diese Option, um Updates der Malware-Signaturen von anderen Bitdefender-Anwendern mithilfe des P2P-Update-Systems herunterzuladen.Bitdefender nutzt die Ports 8880 - 8889 für Peer-to-Peer-Updates.

Bitdefender-Dateien verteilen

Aktivieren Sie diese Option, um die neuesten Malware-Signaturen auf Ihrem Computer mit anderen Bitdefender-Anwendern zu teilen.

12. Safego-Schutz für soziale Netzwerke

Sie vertrauen Ihren Online-Freunden.Aber vertrauen Sie auch Ihren Computern?Nutzen Sie den Safego-Schutz für soziale Netzwerke, um Ihr eigenes Benutzerkonto und das Ihrer Freunde vor Bedrohungen aus dem Internet zu schützen.

Safego ist eine Facebook-Anwendung, die von Bitdefender entwickelt wurde, um Ihr soziales Netzwerk zu schützen.Ihre Aufgabe besteht darin, die Links, die Sie von Ihren Facebook-Freunden erhalten, zu scannen und die Privatsphäreeinstellungen Ihres Benutzerkontos zu überwachen.

Beachten Sie
Sie benötigen ein MyBitdefender-Konto, um diese Funktion nutzen zu können. Für weitere Informationen lesen Sie bitte *„Produktregistrierung“* (S. 8).

Dies sind die Hauptfunktionen:

- Scannt die Einträge in Ihren Neuigkeiten automatisch nach schädlichen Links.
- Schützt Ihr Konto vor Bedrohungen aus dem Internet.

  Wenn ein Beitrag oder Kommentar entdeckt wird, bei dem es sich um Spam, einen Phishing-Versuch oder eine Malware-Bedrohung handelt, erhalten Sie eine Warnmeldung.
- Warnt Ihre Freunde vor verdächtigen Links, die unter ihren Neuigkeiten eingestellt wurden.
- Hilft Ihnen dabei, ein sicheres Freundesnetzwerk mithilfe der **Friend-O-Meter**-Funktion aufzubauen.
- Überprüft den Status Ihrer Systemsicherheit mithilfe des Bitdefender-Quick Scan.

Um auf Safego von Ihrem Bitdefender-Produkt aus zuzugreifen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Safego**-Bereich.
3. Klicken Sie auf **Aktivieren**.Sie werden zu Ihrem Konto weitergeleitet.

   Wenn Sie Safego bereits aktiviert haben, können Sie Zugriffsstatistiken hinsichtlich der Aktivität der Anwendung mit einem Klick auf die Schaltfläche **Berichte anzeigen** aufrufen.
4. Nutzen Sie Ihre Facebook-Anmeldeinformationen, um sich mit der Safego-Anwendung zu verbinden.
5. Erlauben Sie Safego, auf Ihr Facebook-Konto zuzugreifen.

13. 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. 145) beschrieben, kontaktieren.

13.1. Mein System scheint langsamer zu sein

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

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

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

  Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jedes andere Virenschutzprogramm von Ihrem Rechner zu entfernen, bevor Sie die Installation

von Bitdefender starten.Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“ (S. 151)*.

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

  Wenn Ihr PC die Mindestsystemanforderungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen.Für weitere Informationen lesen Sie bitte *„Mindestsystemanforderungen“ (S. 2)*.

- **Ihre Festplatte ist zu fragmentiert.**

  Dateifragmentierung verzögert den Zugriff auf Dateien und verschlechtert die Systemleistung.

  Um Ihre Festplatte mithilfe Ihres Windows-Betriebssystems zu defragmentieren, folgen Sie diesem Pfad vom Windows-Startmenü aus: **Start → Alle Programme → Zubehör → Systemprogramme → Defragmentierung**.

13.2. Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

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

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie Bitdefender vollständig von Ihrem System:
     a. Gehen Sie auf http://www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
     b. Starten Sie das Deinstallations-Tool unter Verwendung eines Kontos mit Administratorrechten.
     c. Starten Sie Ihren Computer neu.
  2. Installieren Sie Bitdefender neu.

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

  Befolgen Sie dafür die folgenden Schritte:

  1. Entfernen Sie die andere Sicherheitslösung.Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“ (S. 151)*.
  2. Entfernen Sie Bitdefender vollständig von Ihrem System:
     a. Gehen Sie auf http://www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
     b. Starten Sie das Deinstallations-Tool unter Verwendung eines Kontos mit Administratorrechten.

c. Starten Sie Ihren Computer neu.

3. Installieren Sie Bitdefender neu.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

13.3. Ich kann eine Anwendung nicht mehr ausführen

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 fälschlicherweise 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 potenziell 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 das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Ausschlüsse**.
4. Klicken Sie auf den Link **Ausgeschlossene Prozesse**.Ein Fenster wird angezeigt. Hier können Sie die Prozesse verwalten, die von Active Virus Control ausgeschlossen sind.
5. Fügen Sie Ausschlüsse hinzu, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie im oberen Teil der Ausschlusstabelle auf **Hinzufügen**.
   b. Klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung, die ausgeschlossen werden soll und klicken Sie dann auf **OK**.

c. Lassen Sie die **Zulassen**-Option aktiviert, um zu verhindern, dass Active Virus Control die Anwendung blockiert.

d. Klicken Sie auf **Hinzufügen**.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

13.4. Ich kann keine Verbindung zum Internet herstellen

Nach der Installation von Bitdefender werden Sie unter Umständen bemerken, dass ein Programm oder ein Browser keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu der jeweiligen Software-Anwendung automatisch zugelassen werden:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Klicken Sie im Bereich Firewall-Regeln auf **Anwendungsregeln**.
5. Um eine Anwendungsregel hinzuzufügen, klicken Sie auf die entsprechende Schaltfläche.
6. Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird.
7. Wählen Sie alle verfügbaren Netzwerktypen aus.
8. Wählen Sie unter **Erlaubnis** den Punkt **Zulassen**.

Schließen Sie Bitdefender, öffnen Sie die Software-Anwendung und versuchen Sie erneut, eine Verbindung mit dem Internet aufzubauen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

13.5. Ich kann auf ein Gerät in meinem Netzwerk nicht zugreifen

Abhängig von dem Netzwerk mit dem Sie verbunden sind, könnte die Bitdefender-Firewall die Verbindung zwischen Ihrem System und einem anderen Gerät (zum Beispiel einem anderen Computer oder Drucker) blockieren. Dadurch sind Sie vielleicht nicht mehr in der Lage, Dateien auszutauschen oder zu drucken.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu dem jeweiligen Gerät automatisch zugelassen werden.Sie

können für jede Netzwerkverbindung eine eigene vertrauenswürdige Zone konfigurieren.

Ein vertrauenswürdige Zone ist ein Gerät, dem Sie uneingeschränkt vertrauen.Jeglicher Datenverkehr zwischen Ihrem Computer und dem vertrauenswürdigen Gerät wird zugelassen.Um Ressourcen mit bestimmten Geräten wie anderen Computern oder Druckern zu teilen, fügen Sie diese als vertrauenswürdige Zonen hinzu.

Um Ihren Netzwerkadaptern eine vertrauenswürdige Zone hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Erweitert**.
4. Klicken Sie im Bereich Firewall-Regeln auf **Adapterregeln**.
5. Um eine Zone hinzuzufügen, klicken Sie auf die entsprechende Schaltfläche.Ein neues Fenster mit den IP-Adressen der mit dem Netzwerk verbundenen Geräte wird angezeigt.
6. Wählen Sie die IP-Adresse des Computers oder den Drucker, den Sie hinzufügen wollen, oder geben Sie eine Adresse oder einen Adressbereich in das entsprechende Textfeld ein.
7. Wählen Sie unter **Erlaubnis** den Punkt **Zulassen**.

Wenn eine Verbindung mit dem Gerät immer noch nicht möglich ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen.

Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Computer könnte die Nutzung des gemeinsamen Druckers oder der Datei blockieren.
  - Wenn die Windows-Firewall genutzt wird, kann diese folgendermaßen konfiguriert werden, um die Datei- und Druckerfreigabe zu erlauben: Öffnen Sie das Einstellungsfenster für die Windows-Firewall, unter **Ausnahmen**, wählen Sie die Option **Datei- und Druckerfreigabe**.
  - Wenn eine andere Firewall verwendet wird, greifen Sie bitte auf die entsprechende Dokumentation oder Hilfedatei zurück.
- Allgemeine Umstände, die eine Benutzung des oder Verbindung mit dem freigegebenen Drucker verhindern könnten:
  - Möglicherweise müssen Sie sich als Windows-Administrator anmelden, um auf den freigegebenen Drucker zugreifen zu können.
  - Für den gemeinsam genutzten Drucker werden Rechte vergeben, so dass dieser nur bestimmten Computern und Benutzern den Zugriff erlaubt.Falls Sie Ihren

Drucker zur gemeinsamen Nutzung freigegeben haben, überprüfen Sie die Rechte, die für den Drucker vergeben wurden, um festzustellen, ob der Nutzer des anderen Computers Zugriffsrechte erhalten hat.Wenn Sie versuchen, eine Verbindung zu einem freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer auf dem anderen Computer abklären, ob Sie die benötigten Rechte haben.

- Der Drucker, der mit Ihren Computer oder dem anderen Computer verbunden ist, ist nicht freigegeben.
- Der freigegebene Drucker wurde dem Computer nicht hinzugefügt.

Beachten Sie

Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können (Drucker freigeben, Rechte vergeben oder entziehen, Verbindungen mit einen freigegebenen Drucker herstellen), klicken sie im Windows-Startmenü auf **Hilfe und Support**).

- Der Zugriff auf einen Netzwerkdrucker könnte auf bestimmte Computer oder Benutzer beschränkt sein. Fragen Sie Ihren Netzwerkadministrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

13.6. 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 das Bitdefender-Fenster.
2. Gehen Sie in den **Firewall**-Bereich und klicken Sie auf den Schalter, um sie zu deaktivieren.
3. Überprüfen Sie, ob Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können.
   - Sollte Ihre Internet-Verbindung immer noch zu langsam sein, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen. Sie sollten sich an Ihren Internet-Anbieter wenden, um zu erfahren, ob es auf Anbieterseite Probleme gibt.

     Wenn Sie von Ihrem Internet-Anbieter die Bestätigung erhalten, dass es auf Anbieterseite keine Probleme gibt und das Problem besteht weiterhin, kontaktieren Sie Bitdefender wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

- Falls Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können, gehen Sie folgendermaßen vor:
  a. Öffnen Sie das Bitdefender-Fenster.
  b. Gehen Sie in den **Firewall**-Bereich und klicken Sie auf den Schalter, um sie zu aktivieren.
  c. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
  d. Klicken Sie im Menü links auf **Firewall** und danach auf den Reiter **Einstellungen**.
  e. Gehen Sie in den Bereich **Internet-Verbindung teilen** und klicken Sie auf den Schalter, um dies zu aktivieren.
  f. Klicken Sie unter **Port-Scans blockieren** auf den Schalter, um dies zu deaktivieren.
  g. Klicken Sie in der oberen Symbolleiste auf **Heim**.
  h. Gehen Sie in den **Firewall**-Bereich und klicken Sie auf **Netzwerkdetails**.
  i. Wählen Sie unter **Netzwerktyp** den Punkt **Heim/Büro**.
  j. Wählen Sie **Tarnkappe** und stellen Sie die Option **Remote** ein. Unter **Generisch** wählen Sie **Ja**.
  k. Schließen Sie Bitdefender, starten Sie das System neu und überprüfen Sie die Internet-Verbindungsgeschwindigkeit.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt „*Hilfe anfordern*“ (S. 146) beschrieben.

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

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

Um Ihr System hinsichtlich Bitdefender-Malware-Signaturen auf dem neuesten Stand zu halten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Update** und danach auf den Reiter **Update**.
4. Unter **Update-Verarbeitungsregeln** klicken Sie auf **Vor dem Download nachfragen**.
5. Klicken Sie in der oberen Symbolleiste auf **Heim**.
6. Gehen Sie in den **Update**-Bereich und klicken Sie auf **Update jetzt durchführen**.

7. Wählen Sie nur **Signatur-Updates** und klicken Sie dann auf **OK**.
8. Bitdefender wird nur die Malware-Signatur-Updates herunterladen und installieren.

13.8. Mein Computer ist nicht mit dem Internet verbunden. Wie kann ich Bitdefender aktualisieren?

Wenn Ihr Computer über keine Internet-Verbindung verfügt, müssen Sie die Updates manuell auf einen Computer mit Internet-Zugang herunterladen und dann über einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick auf Ihren Rechner transferieren.

Folgen Sie diesen Schritten:

1. Öffnen Sie auf einem Computer mit Internet-Zugang einen Web-Browser und gehen Sie auf:

   http://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 auf Ihrem Computer eine 32-Bit- oder 64-Bit-Version von Windows ausgeführt wird, lesen Sie bitte *„Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?“* (S. 152).
3. Speichern Sie die Datei namens `weekly.exe` im System.
4. Übertragen Sie die heruntergeladene Datei zunächst auf einen Wechseldatenträger wie beispielsweise einen USB-Speicherstick und dann auf Ihren Computer.
5. Doppelklicken Sie auf die Datei und folgen Sie den Anweisungen des Assistenten.

13.9. Bitdefender-Dienste antworten nicht

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

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

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- 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.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert.Der Fehler könnte vorübergehend sein.
2. Starten Sie den Rechner neu und warten Sie einige Momente, bis Bitdefender geladen ist. Starten Sie Bitdefender und überprüfen Sie, ob das Problem weiterhin besteht.Durch einen Neustart des Computers wird das Problem normalerweise gelöst.
3. Überprüfen Sie, ob Sie ein anderes Sicherheitsprogramm installiert haben, da dieses 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.

   Für weitere Informationen lesen Sie bitte *„Wie entferne ich andere Sicherheitslösungen?“* (S. 151).

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 146) beschrieben.

13.10. Der Spam-Schutz-Filter funktioniert nicht richtig

Dieser Artikel hilft Ihnen, folgende Probleme mit dem Bitdefender Antispam-Filter lösen:

- Eine Anzahl von seriösen E-Mails werden markiert als `[spam]`.
- Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.
- Der Antispam-Filter entdeckt keine Spamnachrichten.

13.10.1. Legitime 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 angemessen konfigurieren.

Bitdefender fügt die Empfänger Ihrer Mails automatisch der Freundeliste hinzu.Die erhaltenen E-Mail der in der Freundesliste geführten Kontakte werden als seriös angesehen. Sie werden nicht vom Antispam Filter geprüft und deshalb auch nicht als `[spam]` markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten.In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere.Andere Lösungen sind in diesem Fall erforderlich.

1. Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf Erkennungsfehler hin.

   Beachten Sie

   Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“* (S. 69).

2. Antispam Sicherheitsstufe reduzieren. Indem die Sicherheitsstufe reduziert wird, benötigt der Antispam Filter mehr Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen.Probieren Sie diese Lösung nur, wenn legitime Nachrichten (inklusive kommerzielle Nachrichten) fälschlicherweise als Spam erkannt werden.

Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen.Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie in der Bitdefender Antispam-Systemleiste auf den Button **Freund hinzufügen**, um den Adressaten Ihrer Freundeliste hinzuzufügen.
3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der Bitdefender-Oberfläche aus Kontakte der Freundeliste hinzufügen.Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Spam-Schutz**-Bereich.
3. Klicken Sie auf **Verwalten** und wählen Sie dann **Freunde** aus dem Menü.Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adresse ein, von der Sie immer E-Mails empfangen wollen und klicken Sie auf **Hinzufügen**.Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Auf Erkennungsfehler hinweisen

Wenn Sie einen unterstützten Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie anzeigen, welche E-Mail-Nachrichten nicht als [spam] hätten gekennzeichnet werden sollen). Dies wird die Effizienz des Spam-Filters verbessern.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin 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 immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Kein Spam**.Die E-Mail wird in den Posteingangsordner verschoben.

Reduzieren der Spam-Sicherheitsstufe

Um die Antispam Sichereitsstufe herabzusetzen, folgen Sie diese Schritte:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie im Menü links auf **Spam-Schutz**.
4. Verschieben Sie den Schieber auf der Skala nach unten.

13.10.2. Eine Vielzahl von Spam-Nachrichten wird nicht erkannt

Wenn Sie viele Nachrichten erhalten, die nicht als [spam] markiert sind, konfigurieren Sie den Bitdefender Antispam-Filter, um seine Effektivität zu erhöhen.

Versuchen Sie die folgenden Lösungsansätze:

1. Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integriert, weisen Sie auf unerkannte Spam-Nachrichten hin.

Beachten Sie

Bitdefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam-Symbolleiste.Um die komplette Liste der unterstützen E-Mail Clients, lesen Sie bitte: *„Unterstützte E-Mail-Clients und Protokolle“ (S. 69)*.

2. Spammer zur Spammerliste hinzufügen. Die E-Mail-Nachrichten, die von den Adressen aus der Spammerliste empfangen werden, werden automatisch markiert als [spam].
3. Antispam Sicherheitsstufe erhöhen. Indem die Sicherheitsstufe erhöht wird, benötigt der Antispam Filter weniger Spamanzeigen, um eine E-Mail-Nachricht als Spam einzustufen.

Auf unerkannte Spam-Nachrichten hinweisen

Wenn Sie einen unterstützten Mail-Client verwenden, können Sie einfach darauf hinweisen, welche E-Mail-Nachrichten als Spam hätten erkannt werden sollen. Dies wird die Effizienz des Spam-Filters verbessern.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden sofort als [spam] markiert und in den Junk-Mail-Ordner verschoben.

Hinzufügen von Spammern zur Spammer-Liste

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen.Folgen Sie diesen Schritten:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin 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. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde.Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **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.Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Gehen Sie in den **Spam-Schutz**-Bereich.

3. Klicken Sie auf **Verwalten** und wählen Sie dann **Spammer** aus dem Menü.Ein Konfigurationsfenster wird sich öffnen.
4. Geben Sie die E-Mail-Adresse des Spammers ein und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Erhöhen Sie die Spam-Sicherheitsstufe

Um die Antispam Schutzstufe zu erhöhen, folgen Sie diese Schritte:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
3. Klicken Sie auf **Antispam** im Menü auf der linken Seite.
4. Verschieben Sie den Schieber höher auf der Skala.

13.10.3. Der Spam-Schutz-Filter erkennt keine Spam-Nachrichten

Wenn keine Nachrichten als [spam] markiert werden, könnte es möglicherweise am Bitdefender Antispam Fileter liegen.Vor der Fehlersuche dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Spam-Schutz ist unter Umständen deaktiviert.Um den Status des Spam-Schutzes zu überprüfen, öffnen Sie das Bitdefender-Fenster und kontrollieren Sie den Schalter im Bereich **Spam-Schutz**.

  Falls der Spam-Schutz deaktiviert ist, so liegt hier die Ursache Ihres Problems.Klicken Sie auf den Schalter, um Ihren Spam-Schutz zu aktivieren.

- Der Bitdefender Antispam-Schutz ist nur für Email Clients verfügbar, die Emails über das POP3-Protokoll zu empfangen.Das 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 der E-Mail-Nachrichten vom Mail-Server.Falls Sie das Protokoll nicht kennen, das von Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Bitdefender Internet Security 2012 scannt keine POP3-Übertragungen von Lotus Notes.

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. 145) beschrieben.

13.11. 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 eine Schaltfläche, über die Sie ein Deinstallations-Tool ausführen können, durch das Ihr System bereinigt wird.
- Die Deinstallation hängt und Ihr System ist möglicherweise abgestürzt.Klicken Sie auf **Abbrechen** um die Deinstallation abzubrechen. Sollte dies nicht funktionieren, starten Sie das System neu.

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

Um Bitdefender vollständig von Ihrem System zu entfernen, gehen Sie folgendermaßen vor:

1. Gehen Sie auf http://www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
2. Starten Sie das Deinstallations-Tool unter Verwendung eines Kontos mit Administratorrechten.
3. Starten Sie Ihren Computer neu.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“ (S. 146)* beschrieben.

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

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

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

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

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

  Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 152).
  2. Entfernen Sie Bitdefender von Ihrem System:
     a. Gehen Sie auf http://www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
     b. Starten Sie das Deinstallations-Tool unter Verwendung eines Kontos mit Administratorrechten.
     c. Starten Sie Ihren Computer neu.
  3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

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

  Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 152).
  2. Entfernen Sie Bitdefender von Ihrem System:
     a. Gehen Sie auf http://www.bitdefender.com/uninstall und speichern Sie das Deinstallations-Tool auf Ihren Rechner.
     b. Starten Sie das Deinstallations-Tool unter Verwendung eines Kontos mit Administratorrechten.
     c. Starten Sie Ihren Computer neu.
  3. Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.
  4. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

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

Um dieses Problem zu lösen, gehen Sie folgendermaßen vor:

1. Starten Sie Ihren Computer im abgesicherten Modus neu.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 152).
2. Nutzen Sie die Systemwiederherstellung von Windows, um den Computer zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie nutze ich die Systemwiederherstellung unter Windows?“* (S. 153).
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt *„Hilfe anfordern“* (S. 146) beschrieben.

14. 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 ihr 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.

- *„Bitdefender-Rettungsmodus“* (S. 136)
- *„Was ist zu tun, wenn Bitdefender einen Virus auf Ihrem Computer findet?“* (S. 138)
- *„Wie entferne ich einen Virus aus einem Archiv?“* (S. 139)
- *„Wie entferne ich einen Virus aus einem E-Mail-Archiv?“* (S. 141)
- *„Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?“* (S. 141)
- *„Wie Sie infizierte Dateien aus dem Ordner "System Volume Information" entfernen können“* (S. 142)
- *„Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?“* (S. 143)
- *„Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?“* (S. 144)
- *„Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?“* (S. 144)
- *„Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?“* (S. 144)

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. 145) beschrieben, kontaktieren.

14.1. Bitdefender-Rettungsmodus

Der **Rettungsmodus** ist eine Bitdefender-Funktion, mit der Sie alle bestehenden Festplattenpartitionen unabhängig von Ihrem Betriebssystem scannen und desinfizieren können.

Sobald Bitdefender Internet Security 2012 installiert wurde, kann der Rettungsmodus genutzt werden, selbst wenn Sie Ihr System unter Windows nicht mehr hochfahren können.

Starten Ihres Systems im Rettungsmodus

Es gibt zwei Möglichkeiten, den Rettungsmodus zu starten:

Aus dem Bitdefender-Fenster heraus

Um den Rettungsmodus direkt aus Bitdefender heraus zu starten, gehen Sie folgendermaßen vor:

1. Gehen Sie in den **Virenschutz**-Bereich.
2. Klicken Sie auf **Jetzt scannen** und wählen Sie dann **Rettungsmodus** aus dem Dropdown-Menü.

   Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um Ihren Computer neu zu starten.
3. Nach dem Neustart des Computers erscheint ein Menü, das Sie dazu auffordert, ein Betriebssystem auszuwählen.Wählen Sie **Bitdefender Rescue Image** und drücken Sie die **Eingabetaste**, um den Computer in einer Bitdefender-Umgebung zu starten, von der aus Sie Ihre Windows-Partition bereinigen können.
4. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht.Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Starten des Computers im Rettungsmodus

Wenn Windows nicht mehr startet, können Sie Ihren Computer direkt im Bitdefender-Rettungsmodus neu starten, indem die folgenden Anweisungen befolgen:

Beachten Sie

Diese Methode ist auf Computern mit Windows XP nicht verfügbar.

1. Starten Sie Ihren Computer bzw. führen Sie einen Neustart durch und fangen Sie an, die **Leertaste** zu drücken, bevor das Windows-Logo erscheint.
2. Ein Menü erscheint und fordert Sie auf, ein Betriebssystem für den Start auszuwählen.Drücken Sie auf die **Tabulatortaste**, um in den Tools-Bereich zu wechseln.Wählen Sie **Bitdefender Rescue Image** und drücken Sie die **Eingabetaste**, um den Computer in einer Bitdefender-Umgebung zu starten, von der aus Sie Ihre Windows-Partition bereinigen können.
3. Wenn Sie dazu aufgefordert werden, drücken Sie die **Enter**-Taste und wählen Sie die Bildschirmauflösung, die am ehesten der von Ihnen sonst verwendeten Auflösung entspricht.Drücken Sie die **Eingabetaste** erneut.

   Der Bitdefender-Rettungsmodus wird innerhalb weniger Momente geladen.

Scannen Ihres Systems im Rettungsmodus

Um Ihr System im Rettungsmodus zu scannen, gehen Sie folgendermaßen vor:

1. Starten Sie den Rettungsmodus, wie in Kapitel „Starten Ihres Systems im Rettungsmodus“ (S. 136) beschrieben.
2. Das Bitdefender-Logo wird angezeigt und der Kopiervorgang für die Virenschutz-Engines beginnt.
3. Ein Willkommensfenster wird angezeigt.Klicken Sie auf **Fortfahren**.
4. Ein Update der Virensignaturen wird gestartet.
5. Nachdem das Update abgeschlossen ist, erscheint das Fenster für den Bitdefender-Bedarf-Scan.
6. Klicken Sie auf **Jetzt scannen**, wählen Sie in dem jetzt erscheinenden Fenster das Scan-Ziel aus und klicken Sie auf **Öffnen**, um den Scan zu starten.

   Wir empfehlen Ihnen, Ihre gesamte Windows-Partition zu scannen.

   Beachten Sie

   Wenn Sie den Rettungsmodus nutzen, werden Ihnen die Namen der Partitionen im Linux-Format angezeigt.Die Festplattenpartitionen werden angezeigt als `sda1`, was wahrscheinlich der Windows-Partition `(C:)` entspricht, `sda2`, was `(D:)` entspricht usw.

7. Warten Sie bis der Scan abgeschlossen ist. Falls Malware gefunden wurde, folgen Sie den Anweisungen, um die Bedrohung zu entfernen.
8. Um den Rettungsmodus zu beenden, rechtsklicken Sie auf einen leeren Bereich auf dem Desktop, klicken Sie im Kontextmenü auf **Logout** und wählen Sie dann, ob Sie den Computer neu starten oder herunterfahren wollen.

14.2. Was ist zu tun, wenn Bitdefender einen Virus auf Ihrem Computer findet?

Es gibt verschiedene Möglichkeiten, Ihnen mitzuteilen, ob sich auf Ihrem Computer Viren befinden:

- Sie haben einen Scan durchgeführt und Bitdefender hat infizierte Einträge gefunden.
- Ein Virenwarnhinweis informiert Sie, dass Bitdefender einen oder mehrere Viren auf Ihrem Computer geblockt hat.

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

Sobald der vollständige Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte (desinfizieren, löschen, in die Quarantäne verschieben).

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

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

Die erste Methode kann im Normalmodus eingesetzt werden:

1. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
   c. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um den **Zugriff-Scan** zu deaktivieren.
2. Lassen Sie sich die verborgenen Objekte in Windows anzeigen.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 154).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

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 hier vorgehen sollen, lesen Sie bitte *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 152).
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 neu und starten Sie den Normalmodus.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt *„Hilfe anfordern“* (S. 146) beschrieben.

14.3. 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. Führen Sie einen vollständigen System-Scan durch, um das Archiv zu finden, in sich der Virus befindet.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
   c. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um den **Zugriff-Scan** zu deaktivieren.
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 „*Hilfe anfordern*“ (S. 146) beschrieben.

14.4. Wie entferne ich einen Virus aus einem E-Mail-Archiv?

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

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

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

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Bitdefender-Echtzeitvirenschutz:
   a. Öffnen Sie das Bitdefender-Fenster.
   b. Klicken Sie in der oberen Symbolleiste auf **Einstellungen**.
   c. Klicken Sie im Menü links auf **Virenschutz** und danach auf den Reiter **Schild**.
   d. Klicken Sie auf den Schalter, um den **Zugriff-Scan** zu deaktivieren.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht.Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie wiederhergestellt werden können.Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Outlook Express:Klicken Sie im Dateimenü auf "Verzeichnis", dann auf "Alle Verzeichnisse komprimieren".
   - In Microsoft Outlook:Klicken Sie im Dateimenü auf "Datendateiverwaltung".Wählen Sie das persönliche Verzeichnis (.pst), das Sie komprimieren möchten und klicken Sie auf "Einstellungen".Klicken Sie auf Kompakt.
6. Aktivieren Sie den Bitdefender-Echtzeitvirenschutz.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den Bitdefender-Support wie im Abschnitt „*Hilfe anfordern*“ (S. 146) beschrieben.

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

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

Um sicherzustellen, dass Ihr System geschützt ist, gehen Sie folgendermaßen vor:

1. Führen Sie einen **vollständigen System-Scan** mit Bitdefender durch.Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Wie scanne ich mein System?“ (S. 33)*.
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.

   Um herauszufinden, wie Sie hier vorgehen sollen, lesen Sie bitte *„Hilfe anfordern“ (S. 146)*.

14.6. Wie Sie infizierte Dateien aus dem Ordner "System Volume Information" entfernen können

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 Systemwiederherstellungsverzeichnissen 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 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 Administratorpassworts 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 *„Hilfe anfordern“ (S. 146)* beschrieben.

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

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

Am häufigsten sind passwortgeschützte Objekte:

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

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

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres 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.

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

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

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

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

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

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

14.10. Warum hat Bitdefender ein infizierte Datei automatisch gelöscht?

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

Bestimmte 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 Seiten heruntergeladen werden.Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

15. Hilfe erhalten

15.1. 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.

15.1.1. Online-Ressourcen

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

- Bitdefender-Support-Center:http://www.bitdefender.de/site/contact/1/
- Bitdefender Support-Forum:http://forum.bitdefender.com
- das Malware City Computer Sicherheitsportal:http://www.malwarecity.com

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

Bitdefender-Support-Center

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

Das Bitdefender-Support-Center ist öffentlich zugänglich und frei durchsuchbar.Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden.Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Support-Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender-Support-Center steht Ihnen jederzeit unter der folgenden Adresse zur Verfügung: http://www.bitdefender.de/site/contact/1/.

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**.

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.

15.1.2. Hilfe anfordern

Unter **Problemlösung** finden Sie alle notwendigen Informationen zu den häufigsten Problemen, die bei der Verwendung 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 heraus“ (S. 147)
- „Kontaktieren Sie uns über unser Online-Support-Center“ (S. 147)

Wichtig

Um den Bitdefender-Kundendienst kontaktieren zu können, müssen Sie Ihr Bitdefender-Produkt registrieren.Für weitere Informationen lesen Sie bitte *„Produktregistrierung“* (S. 8).

Kontaktieren Sie uns direkt aus Ihrem Bitdefender-Produkt heraus

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

Folgen Sie diesen Schritten:

1. Öffnen Sie das Bitdefender-Fenster.
2. Klicken Sie auf der unteren rechten Seite des Bildschirms auf **Hilfe und Support**.
3. Sie haben die folgenden Möglichkeiten:
   - Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.
   - Suchen Sie in unserer Datenbank nach der Information, die Sie brauchen.
   - Klicken Sie auf die Schaltfläche **Kundendienst kontaktieren**, um das Support-Tool aufzurufen und den Kundendienst zu kontaktieren.Innerhalb des Assistenten können Sie über die Schaltfläche **Weiter** navigieren. Um den Assistenten zu verlassen, klicken Sie auf **Abbrechen**.
     a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.
     b. Geben Sie in das Formular die nötigen Daten ein:
        i. Geben Sie Ihre E-Mail-Adresse ein.
        ii. Geben Sie Ihren vollen Namen ein.
        iii. Wählen Sie Ihr Land aus dem entsprechenden Menü.
        iv. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.
     c. Bitte warten Sie einige Minuten, während Bitdefender die produkt-relevanten Informationen einholt. Diese Informationen helfen unseren Mitarbeitern, eine Lösung für Ihr Problem zu finden.
     d. Klicken Sie auf **Beenden**, um die Information an den Bitdefender-Kundendienst zu senden. Sie werden schnellstmöglich kontaktiert.

Kontaktieren Sie uns über unser Online-Support-Center

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

1. Gehen Sie zu http://www.bitdefender.com/help.Im Bitdefender-Support-Center finden Sie eine Vielzahl von Beiträgen, die Lösungen zu Problemen im Zusammenhang mit Bitdefender bereithalten.
2. Wählen Sie Ihr Produkt aus der linken Spalte aus und suchen Sie im Bitdefender-Support-Center nach Artikeln, die Ihnen eine Lösung für Ihr Problem liefern können.

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.

15.2. 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.

15.2.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center:http://www.bitdefender.de/site/contact/1/
Dokumentation: documentation@bitdefender.com
Händler vor Ort:http://www.bitdefender.com/partners
Partnerprogramm: partners@bitdefender.com
Medienkontakt: pr@bitdefender.com
Karriere: jobs@bitdefender.com
Viruseinsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Missbrauch melden: abuse@bitdefender.com
Website:http://www.bitdefender.de/

15.2.2. Lokale Vertriebspartner

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

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.com/site/Partnership/list/.
2. Die Kontaktinformationen der lokalen Bitdefender-Vertriebspartner sollten automatisch angezeigt werden. Falls dies nicht der Fall ist, wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
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.

15.2.3. Bitdefender-Niederlassungen

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.

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (Geschäftsstelle& Vertrieb): 1-954-776-6262
Sales: sales@bitdefender.com
Technischer Support: http://www.bitdefender.de/site/contact/1/
Web: http://www.bitdefender.de/

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-Mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Sales: sales@bitdefender.co.uk
Technischer Support: http://www.bitdefender.de/site/contact/1/
Web: http://www.bitdefender.co.uk

Deutschland

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Geschäftsstelle: +49 2301 91 84 0
Sales: vertrieb@bitdefender.de
Technischer Support: http://kb.bitdefender.de
Web: http://www.bitdefender.de

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
Sales: comercial@bitdefender.es

Technischer Support: http://www.bitdefender.es/ayuda
Webseite: http://www.bitdefender.es

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

16. Nützliche Informationen

In diesem Kapitel finden Sie einige wichtige Vorgehensweisen, die Sie kennen sollten, bevor Sie wegen eines technischen Problems die Fehlersuche starten.

Für die Fehlersuche und -behebung eines technischen Problems in Bitdefender sind gewisse Kenntnisse von Windows erforderlich. Deshalb beziehen sich die nächsten Schritte vor allem auf das Windows-Betriebssystem.

- *„Wie entferne ich andere Sicherheitslösungen?“* (S. 151)
- *„Wie führe ich einen Neustart im abgesicherten Modus durch?“* (S. 152)
- *„Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?“* (S. 152)
- *„Wie nutze ich die Systemwiederherstellung unter Windows?“* (S. 153)
- *„Wie kann ich in Windows versteckte Objekte anzeigen?“* (S. 154)

16.1. Wie entferne ich andere Sicherheitslösungen?

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

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Computer verwenden, wird dadurch das System instabil.Der Bitdefender Internet Security 2012-Installer findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheits-Software 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 Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

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

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen.Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu 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 wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, falls Sie Zugang zum Internet haben möchten.
4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
5. Dieser Vorgang endet mit einer Bestätigungsbenachrichtigung.Klicken Sie zur Bestätigung auf **Ok**.
6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

16.3. 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 wie folgt vor:

- In **Windows XP**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Arbeitsplatz** im Menü **Start**.
  3. Rechtsklicken Sie auf **Arbeitsplatz** 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 Sie den Punkt **x64 Edition** nicht finden, wird auf Ihrem Computer eine 32-Bit-Version von Windows XP ausgeführt.
- In **Windows Vista** und **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Finden Sie **Computer** im **Start**-Menü.
  3. Rechtsklicken Sie auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.

16.4. Wie nutze ich die Systemwiederherstellung unter Windows?

Wenn Sie den Computer nicht im Normalmodus starten können, starten Sie ihn im abgesicherten Modus und nutzen Sie die Systemwiederherstellung, um das System zu einem Zeitpunkt wiederherzustellen, an dem es ordnungsgemäß ausgeführt wurde.

Um eine Systemwiederherstellung durchzuführen, müssen Sie als Administrator bei Windows angemeldet sein.

Um die System-Wiederherstellung zu nutzen, gehen Sie folgendermaßen vor:

- In Windows XP:
  1. Starten Sie Windows im abgesicherten Modus.
  2. Folgen Sie diesem Pfad aus dem Windows-Startmenü heraus: **Alle Programme → Zubehör → Systemprogramme → Systemwiederherstellung**.
  3. Klicken Sie in dem Bildschirm **Willkommen zur Systemwiederherstellung** auf die Option **Meinen Computer zu einem früheren Zeitpunkt wiederherstellen** und danach auf Weiter.
  4. Wenn Sie den Anweisungen des Assistenten folgen, sollten Sie in der Lage sein, das System im Normalmodus zu starten.
- Für Windows Vista und Windows 7:
  1. Starten Sie Windows im abgesicherten Modus.

2. Folgen Sie diesem Pfad aus dem Windows-Startmenü heraus: **Alle Programme → Zubehör → Systemprogramme → Systemwiederherstellung**.
3. Wenn Sie den Anweisungen des Assistenten folgen, sollten Sie in der Lage sein, das System im Normalmodus zu starten.

16.5. Wie kann ich in Windows versteckte Objekte anzeigen?

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 **Ordneroptionen**.
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

Adware

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

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

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.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

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

Autostart-Einträge

Jede Datei, die sich in diesem Ordner 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 Ordner gelegt.

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.

Befehlszeile

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

Bootsektor

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

Bootvirus

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

Cookie

In der 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 dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, 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.

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.

Download

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

Durchsuchen

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

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

E-Mail Client

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

Ereignisse

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

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Heuristik

Eine Methode, um neue Viren zu identifizieren.Diese Prüfmethode 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 Domäne lesen und beschreiben können, die sie unterstützen.

Keylogger

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

Keylogger sind nicht grundsätzlich als schädlich anzusehen. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen vorsätzlich als kriminelles Mittel eingesetzt (um beispielsweise private Daten wie Anmeldedaten oder Kreditkartendaten zu sammeln).

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 ein.

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.Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert Bitdefender eine Logdatei mit den gescannten Pfaden, Verzeichnissen und der Archivanzahl sowie den gescannten, infizierten oder verdächtigen Dateien.

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.

Nicht heuristisch

Diese Prüfmethode 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.

Pfad

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

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

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen.Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf 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.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Software-Tools 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, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

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.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann.Rechner haben verschiedenartige 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.

Skript

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

Spam

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

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 ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, 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, indem 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.

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 vernichtendes 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 welches 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.

Virussignatur

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.