bitdefender

INTERNET SECURITY v10

10th anniversary

Benutzerhandbuch

Antivirus

Firewall

AntiSpam

Antispyware

Kindersicherung

bitdefender
secure your every bit

BitDefender Internet Security v10

Benutzerhandbuch

BitDefender

Veröffentlicht 2007.01.16
Version 10.2

Rechtlicher Hinweis


bitdefender
secure your every bit

Inhaltsverzeichnis

Endbenutzer Software-Lizenzvertrag

Installieren Sie die Software nicht, wenn Sie diesen Lizenzbedingungen nicht zustimmen. Wenn Sie "Akzeptieren", "OK", "Weiter", "Einverstanden" auswählen, oder wenn Sie sie Software in irgendeiner Form installieren oder nutzen, erklären Sie, dass Sie die Bedingungen des Lizenzvertrages vollständig verstanden und akzeptiert haben.

Diese Bedingungen decken BitDefender Lösungen und Services ab, die wir Ihnen als Anwender lizenziert haben, einschließlich der entsprechenden Dokumentation und aller Updates und Upgrades der Anwendung, die Ihnen unter der gekauften Lizenz oder angeschlossener Service Vereinbarungen geliefert wurden, so wie in der Dokumentation und allen Kopien dieser Vertragsgegenstände festgelegt.

Der Lizenzvertrag und die Gewährleistungsbestimmungen sind ein rechtsgültiger Vertrag zwischen Ihnen (einer natürlichen oder juristischen Person, im Folgenden Benutzer genannt) und der SOFTWIN zur Benutzung des oben und folgend genannten SOFTWIN SOFTWAREPRODUKTES, welches außer dem eigentlichen SOFTWAREPRODUKT auch dazugehörige Medien, gedruckte Materialien und die Nutzung von Online- und anderen Medien oder elektronische Dokumentation (im weiteren bezeichnet BitDefender)beinhaltet. Das SOFTWAREPRODUKT und die zugehörigen Materialien sind durch US-amerikanische Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt. Indem Sie das SOFTWAREPRODUKT installieren, kopieren, downloaden, darauf zugreifen oder es anderweitig verwenden, erklären Sie sich damit einverstanden, durch die Bestimmungen des Lizenzvertrages und der Gewährleistungsbestimmungen gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrages und der Gewährleistungsbestimmungen nicht zustimmen, ist der Hersteller SOFTWIN nicht bereit, das SOFTWAREPRODUKT an Sie zu lizenzieren. In diesem Falle sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu verwenden oder zu kopieren.

Installieren oder nutzen Sie BitDefender nicht, wenn Sie dem Lizenzvertrag und den Gewährleistungsbestimmungen nicht zustimmen.

BitDefender Lizenz. Das SOFTWAREPRODUKT ist durch Urheberrechtsgesetze und internationale Urheberrechtsverträge genauso geschützt, wie durch andere Gesetze und Verträge zum Schutz des geistigen Eigentums. Das SOFTWAREPRODUKT wird an Sie lizenziert, nicht verkauft.

LIZENZEINRÄUMUNG: Dieser Vertrag gewährt Ihnen und nur Ihnen eine nicht ausschließliche, eingeschränkte, nicht übertragbare und kostenpflichtige Lizenz BitDefender zu nutzen.

Anwendung der Software. Sie können BitDefender installieren und nutzen, auf so vielen Computern wie nötig, mit der Einschränkung, dass diese Anzahl nicht die Anzahl der lizenzierten Anwender überschreitet. Es kann eine zusätzliche Kopie für ein Back-Up erstellt werden.

Desktop Anwender Lizenz. Diese Lizenz bezieht sich auf BitDefender Software, die auf einzelnen Computern installiert werden kann und keine Netzwerk Eigenschaften hat. Jeder direkte Anwender kann diese Software auf einem einzelnen Computer installieren und zu Back-up Zwecken eine zusätzliche Kopie auf einem anderen Computer erstellen. Die Anzahl der direkten Anwender entspricht der Anzahl der Lizenz Inhaber.

LIZENZBESTIMMUNGEN. Die hiermit gewährte Lizenz ist ab dem Kaufdatum von BitDefender bis zum Ende des Zeitraums, für den die Lizenz erworben wird, gültig.

UPGRADES: Sollte das SOFTWAREPRODUKT BitDefender mit der Bezeichnung Upgrade gekennzeichnet sein, muss der Benutzer für eine berechtigte Nutzung eine gültige, von SOFTWIN als berechtigte für BitDefender anerkannte, Softwarelizenz haben. Das als Upgrade gekennzeichnete SOFTWAREPRODUKT BitDefender ersetzt und / oder ergänzt das zum Upgrade berechtigende BitDefender. Der Benutzer darf das aus dem Upgrade resultierende SOFTWAREPRODUKT nur nach dem hier vorliegenden Lizenzvertrag nutzen. Sollte das als Upgrade gekennzeichnete BitDefender ein Upgrade für eine einzelne Komponente eines kompletten Softwarepaketes sein, darf das SOFTWAREPRODUKT BitDefender auch nur als einzelner Bestandteil dieses Softwarepaketes genutzt und transferiert werden und darf nicht als separates Produkt auf mehr als einem Einzelplatzrechner genutzt werden. Die Geschäftsbedingungen dieser Lizenz ersetzen und lösen alle vorangehenden Vereinbarungen ab, die zwischen Ihnen und Softwin bestanden haben in Bezug auf das Original Produkt und das daraus resultierende Upgrade Produkt.

URHEBERRECHT: Alle Rechte und geistigen Eigentumsrechte an BitDefender(einschließlich, aber nicht beschränkt auf Logos, Bilder, Fotografien, Animationen, Video, Audio, Musik, Text und "Applets", die in BitDefender enthalten sind), den gedruckten Begleitmaterialien und jeder Kopie von BitDefender liegen bei SOFTWIN. Das BitDefender ist durch anwendbare Urheberrechtsgesetze und andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Darum muss der Benutzer BitDefender wie jedes andere urheberrechtliche Produkt behandeln, mit der Ausnahme, dass er BitDefender auf einem Einzelplatzrechner installieren und das Original zu Sicherungszwecken speichern darf. Der Benutzer darf die zugehörigen, gedruckten Materialien nicht vervielfältigen. Der Benutzer muss BitDefender als Ganzes, wie erhalten, inklusiver aller Urheberrechtsvermerke und aller zugehörigen Materialien und Medien in der ihm vorliegenden Form bewahren. Der Benutzer ist nicht berechtigt, BitDefender weiter zu lizenzieren, zu vermieten, zu verleihen und / oder zu verkaufen. Der Benutzer darf BitDefender nicht zurückentwickeln (Reverse

Engineering), dekompilieren, disassemblieren, daraus Derivate erzeugen, modifizieren, übersetzen oder irgendeinen anderen Versuch starten, den Quellcode von BitDefender freizulegen.

EINGESCHRÄNKTE GEWÄHRLEISTUNG: SOFTWIN gewährleistet für einen Zeitraum von 30 Tagen, dass das Medium auf dem BitDefender geliefert wird, frei von allen Defekten ist. Sollte dies nicht der Fall sein, wird SOFTWIN das Medium austauschen oder dem Benutzer den Betrag zurück erstatten, den der Benutzer für BitDefender bezahlt hat. SOFTWIN gewährleistet weder die dauerhafte Verfügbarkeit, noch die Fehlerfreiheit von BitDefender, noch dass Unzulänglichkeiten und Fehler von BitDefender behoben werden. SOFTWIN gewährleistet ebenso nicht, dass BitDefender den Anforderungen des Benutzers entspricht.

SOFERN IN DER VORLIEGENDEN VEREINBARUNG NICHT AUSDRÜCKLICH ANDERWEITIG FESTGELEGT, LEHNT SOFTWIN ALLE ANDEREN AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN IM HINBLICK AUF DIE PRODUKTE, DAMIT ZUSAMMENHÄNGENDE VERBESSERUNGEN, WARTUNG ODER SUPPORT ODER ALLE ANDEREN VON SOFTWIN GELIEFERTEN (MATERIELLEN ODER IMMATERIELLEN) MATERIALIEN ODER ERBRACHTEN DIENSTLEISTUNGEN AB. SOFTWIN LEHNT HIERMIT AUSDRÜCKLICH ALLE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN UND ZUSICHERUNGEN AB, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE GEWÄHRLEISTUNG WEGEN RECHTSMÄNGEL, DIE GEWÄHRLEISTUNG DER NICHT-KOLLISION, DER GENAUIGKEIT VON DATEN UND INFORMATIONEN, DER SYSTEMINTEGRATION UND DER NICHTVERLETZUNG VON RECHTEN DRITTER DURCH DAS FILTERN, DEAKTIVIEREN ODER ENTFERNEN VON FREMDANBIETERSOFTWARE, SPYWARE, ADWARE, COOKIES, E-MAILS, DOKUMENTEN, ANZEIGEN ODER ÄHNLICHEM, UNABHÄNGIG DAVON, OB DIES AUFGRUND GESETZLICHER ANFORDERUNGEN, DER GESCHÄFTSTÄTIGKEIT, DES GEWOHNHEITSRECHTS UND DER PRAXIS ODER DES HANDELSGEBRAUCHS ERFOLGT.

BESCHRÄNKUNG DER HAFTUNG: Jeder Benutzer von BitDefender, der dieses benutzt, testet oder auch nur ausprobiert trägt alleinig das Risiko, das aus der Qualität und Performance von BitDefender entsteht. In keinem Fall können SOFTWIN oder ihre Lieferanten auf irgendeine Weise für, durch Verwendung von BitDefender, entstandene Schäden jeder Art haftbar gemacht werden, einschließlich und ohne Beschränkung, direkter und indirekter, zufälliger und spezieller Schäden die aus der Verwendung, Performance oder der Verfügbarmachung von BitDefender entstanden sind. Dies gilt auch dann, wenn SOFTWIN über existierende und / oder mögliche Schäden informiert wurde. IN KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN,

DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test, etc.).

Wichtige Informationen für die Anwender. WICHTIGE INFORMATION FÜR DEN BENUTZER: DIESES SOFTWAREPRODUKT IST NICHT FEHLERTOLERANT UND IST AUCH NICHT FÜR EINE NUTZUNG IN KRITISCHEN UMGEBUNGEN, IN DENEN ES AUF EINE AUSFALLSICHERE PERFORMANCE UND BEDIENUNG ANKOMMT, KONZIPIERT UND ERSTELLT. DIESES SOFTWAREPRODUKT IST NICHT GEEIGNET ZUR NUTZUNG IM LUFTVERKEHR, IN NUKLEARKRAFTWERKEN, IN KOMMUNIKATIONSSYSTEMEN, IN WAFFENSYSTEMEN, IN DIREKTEN ODER INDIREKTEN LEBENSERHALTUNGSSYSTEMEN ODER IRGENDEINEM ANDEREN SYSTEM, DESSEN AUSFALL ZU TODESFÄLLEN, KÖRPERLICHEN SCHÄDEN ODER VERMÖGENSSCHÄDEN FÜHREN KÖNNTE.

Allgemein. Dieser Vertrag unterliegt dem Recht von Rumänien, internationalen Copy Right Bestimmungen und Abkommen.

Preise, Kosten und Gebühren für die Nutzung von BitDefender gelten vorbehaltlich von Änderungen auch ohne vorherige Information.

Ist oder wird eine Bestimmung dieses Vertrageswegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam oderwird sie für unwirksam erklärt, so wird hierdurch die Gültigkeit des übrigen, mitder unwirksamen Bestimmung nicht unmittelbar zusammenhängenden Vertragsteils,nicht berührt.

BitDefender und alle zugehörigen Logos sind eingetrageneTitel und Marken von SOFTWIN. Alle anderen Marken und Titel sind Eigentumder jeweiligen Rechteinhaber.

Wenn Sie gegen eine Lizenzbestimmung verstoßen, wird die Lizenz unverzüglich fristlos beendet. Sie haben aufgrund der Beendigung keinen Anspruch auf eine Erstattung von SOFTWIN oder einem Händler von BitDefender. Die Bestimmungen im Hinblick auf Geheimhaltung und Beschränkungen gelten über die Laufzeit der Lizenz hinaus.

SOFTWIN ist berechtigt, die vorliegenden Bestimmungen jederzeit zu überarbeiten. Die überarbeiteten Bestimmungen gelten automatisch für die entsprechenden Software-Versionen, die mit den geänderten Bestimmungen geliefert werden. Sollte eine der vorliegenden Bestimmungen ungültig und nicht durchführbar sein, bleibt die Gültigkeit der übrigen Bestimmungen davon unberührt.

Im Fall von Widersprüchen oder Unstimmigkeiten zwischen übersetzten Fassungen der vorliegenden Bestimmungen gilt die von SOFTWIN ausgegebene englische Fassung.

Kontakt SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: <office@bitdefender.com>.

Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer vorgesehen, die sich für **BitDefender Internet Security 10** als Sicherheitslösung entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

Es wird beschrieben wie **BitDefender Internet Security 10** zu handhaben ist, wie das Produkt optimal konfiguriert werden kann und wie Sie die Einstellungen Ihren Bedürfnissen anpassen können. So lernen Sie optimal mit diesem Produkt umzugehen und es effektiv einzusetzen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

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

Erscheinungsbild	Beschreibung
`sample syntax`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Webseiten oder FTP-Server.
`<support@bitdefender.com>`	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. xvii)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`filename`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
option	Optionen wie z.B. Schaltflächen oder Checkbox-Elemente werden in **fett gedruckt** angegeben.
`sample code listing`	Beispielquelltexte werden in einer Schriftart mit `fester Laufweite` angegeben.

1.2. Warnungen

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

Anmerkung

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Struktur

Dieses Handbuch ist in sieben Abschnitte unterteilt, welche die folgenden Hauptthemen beinhalten: Über BitDefender, Installation von BitDefender, Beschreibung und Bestandteile, Die Management Konsole, Tipps und Tricks, BitDefender Notfall CD und Hilfe erhalten. Des Weiteren beinhaltet dieses Dokument ein Glossar und Anhänge um den ein oder anderen Aspekt zu klären, der sonst ggf. zu technischen Problemen führen könnte.

Über BitDefender. Eine kurze Einführung zu BitDefender und SOFTWIN, der Firma hinter diesem Produkt.

Produktinstallation. Schritt-für-Schritt Anleitung zur Installation von BitDefender auf Ihrem Computer. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender Internet Security 10** zu registrieren ist, wie ein Prüfvorgang durchgeführt werden kann, wie die Personal-Firewall konfiguriert wird, wie der AntiSpam-Filter eingerichtet wird und wie ein Update von BitDefender durchgeführt werden kann.

Beschreibung und Funktionen. Eine kurze Einführung in BitDefender welche erklärt, was BitDefender genau ist und welches Unternehmen dahinter steht. Sie erhalten eine Einführung in **BitDefender Internet Security 10**, die Funktionen dieses Produkts und Details zu den einzelnen Modulen.

Konfiguration. Beschreibt die einfache Verwaltung und Konfiguration von BitDefender. Dieser Abschnitt erklärt wie das **BitDefender Internet Security 10**zu registrieren ist, wie ein Prüfvorgang durchgeführt werden kann und wie ein Update von BitDefender durchgeführt werden kann.

Empfohlene Vorgehensweisen. Folgen Sie den angegebenen Schritten und Anweisungen um BitDefender bestmöglich zu nutzen.

BitDefender Notfall CD. Beschreibung der BitDefender Notfall CD. Erläutert die Funktionen und den Einsatz der startfähigen CD.

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

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen erklärt, die in diesem Dokument zu finden sind.

3. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

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

Wichtig

Bitte verfassen Sie alle auf die Dokumentation bezogenen E-Mails auf Englisch.

Über BitDefender

1. Was ist BitDefender?

BitDefender ist einer der weltweit führenden Hersteller von Sicherheitslösungen und bietet eine der schnellsten und höchst effizienten Sicherheitslösungen in diesem Industriesegment an. Produkte und Dienstleistungen von BitDefender kommen in über 41 Millionen Haushalten und Firmen in mehr als 180 Ländern weltweit zum Einsatz. BitDefender unterhält Büros in den **Vereinigten Staaten**, in **Großbritannien**, **Deutschland**, **Spanien** und **Rumänien**.

- Features: Antivirus, Firewall, Antispyware, Antispam, und Kindersicherung.
- Die BitDefender Produktreihe ist daraufhin ausgelegt in komplexen IT Strukturen (Work Stations, File Servers, Mail Servers und Gateways)implementiert zu werden und zwar für Windows, Linux und FreeBSD.
- Weltweite Distribution, Produkte in 18 Sprachen verfügbar;
- Einfache Bedienbarkeit kombiniert mit einem Installationsassistent welcher den lediglich Benutzer vereinzelte Fragen stellt;
- Internation zertifizierte Produkte: Virus Bulletin, ICSA Labs, Checkmar, IST Prize, usw;
- Rund um die Uhr Kundenbetreuung - 24 Stunden am Tag, 7 Tage die Woche;
- Blitzschnelle Reaktionszeiten beim Bereitstellen von Virensignaturen zur Bekämpfung von Schädlingen;
- Beste Erkennungsraten;
- Stündliche Updates für Virensignaturen - automatisch oder geplante Aktionen schützen vor neuen Viren und anderen Schädlingen.

1.1. Warum BitDefender?

Bewährt: Der reaktionsfähigste Hersteller von AntiViren-Produkten. Die Reaktionsfähigkeit von BitDefender wurde bereits bei den Ausbrüchen von CodeRed, Nimda, Sircam, Badtrans.B und weiteren Schädlingen auf die Probe gestellt. BitDefender war das erste AntiViren-Produkt welches effektive Gegenmittel, sog. „Removal Tools“, für die genannten Schädlinge bereitstellte und dies vollkommen kostenlos für Benutzer auf der ganzen Welt. Mit der kontinuierlichen Verbreitung immer neuer Schädlinge und Varianten gehört der effiziente Schutz vor solchen Bedrohungen mittlerweile zu einem „Must have“ für diejenigen, die tagtäglich mit Computersystemen arbeiten.

Innovation: Ausgezeichnet von der Europäischen Kommission und EuroCase. BitDefender wurde zum Gewinner des europäischen IST-Prize gekürt, welcher von der Europäischen Kommission und Vertreten von 18 Akademien in ganz Europa vergeben wird. Seit acht Jahren vergeben zählt der IST-Prize mittlerweile als Auszeichnung für wegweisende Innovationen und repräsentiert somit die beste Innovation der europäischen Informationstechnologie.

Umfassend: Sichert Einstiegspunkte im Netzwerk und bietet effektiven Schutz. Sicherheitslösungen mit BitDefender werden den Anforderungen in Unternehmensnetzwerken mehr als gerecht. Sie sind nicht nur geeignet für den Einsatz in kleinen und mittelständischen Unternehmen sondern auch in Multi-Plattform Netzwerken weltweit agierender Konzerne bietet BitDefender effektiven Schutz. Somit wird sichergestellt, dass Viren und andere Schädlinge erst gar keine Möglichkeit erhalten sich in Unternehmensnetzwerken zu verbreiten.

Optimaler Schutz: Sicherheit vor Bedrohungen auf Ihrem Computer. Da Virenerkennung basierend auf Quellcode-Analyse lange nicht mehr ausreicht um Schädlinge ausreichend früh zu erkennen, arbeitet das Team von BitDefender stets an neuen Technologien zur frühzeitigen Erkennung von Schädlingen und pro-aktivem Schutz vor diesen.

Sicherheitsprodukte wurden geschaffen um in Firmen, Einrichtungen und bei Privatpersonen die folgenden **möglichen Schäden** zu verhindern:

- Wurm-Angriffe
- Störung der Kommunikation durch infizierte E-Mails
- Zusammenbrechen von Servern
- Desinfizierung und Wiederherstellung von Computersystemen
- Produktivitätsverlust durch nicht verfügbare Systeme
- Cracking und unautorisierte Zugriffe auf sensible Daten

Durch die stetige Weiterentwicklung und den pro-aktiven Schutz von BitDefender können die folgenden **Vorteile** gesichert werden:

- Verbesserte Netzwerkverfügbarkeit durch rechtzeitige Unterbindung von Wurm-Angriffen.
- Schutz der Remote-Benutzer und Clients vor Viren-Angriffen.
- Minimierung des administrativen Aufwands und der Kosten durch Remote-Management Funktionalität der BitDefender-Produkte.
- Unterbindung der Verbreitung von Viren und anderen Schädlingen durch den Schutz der zentralen Kommunikationswege wie Fileserver, E-Mail-Server und Gateways mittels BitDefender.

Weitere Informationen über BitDefender erhalten Sie unter:www.bitdefender.de

1.2. Über SOFTWIN

Im Jahre 1990 gegründet und Gewinner des Europäischen IST-Prize in 2002, wird Softwin mittlerweile als führend in der Osteuropäischen Softwareindustrie angesehen, mit einer Zuwachsrate von 50% in den letzten 5 Jahren und 70 % Exportanteil am Jahreumsatz.

Mit einem Team von mehr als über 800 qualifizierten Mitarbeitern und mehr als 1000 Projekten bislang hat SOFTWIN es sich zur Aufgabe gemacht, Sicherheitslösungen und -dienste bereitzustellen, die den heutigen Anforderungen von schnell expandieren Firmen im Bereich IT-Sicherheit entsprechen und diesen Vorsprung auszubauen. Der Entwicklungsprozess bei Softwin ist ISO 9001 zertifiziert.

Da Softwin in den weit entwickelten IT Märkten in den USA und Europa aktiv ist gibt es 4 verbundene **Geschäftsbereiche** :

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management

Produktinstallation

2. Installation von BitDefender Internet Security v10

Der Abschnitt **Installation von BitDefender Internet Security 10** beschreibt die folgenden Themen:

- Systemanforderungen
- Installationsschritte
- Der Regelassistent
- Upgrade von einer vorherigen Version
- Ändern, Reparieren, Deinstallieren

2.1. Systemanforderungen

Für den sachgemäßen und fehlerfreien Betrieb sollten Sie vor der Installation sicherstellen, dass die folgenden Systemanforderungen erfüllt sind:

Windows 2000, Windows XP (32 Bit)

- Pentium II 350 MHZ oder höher
- 128 MB Arbeitsspeicher (256 MB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte
- Internet Explorer 5.5 (oder höher)

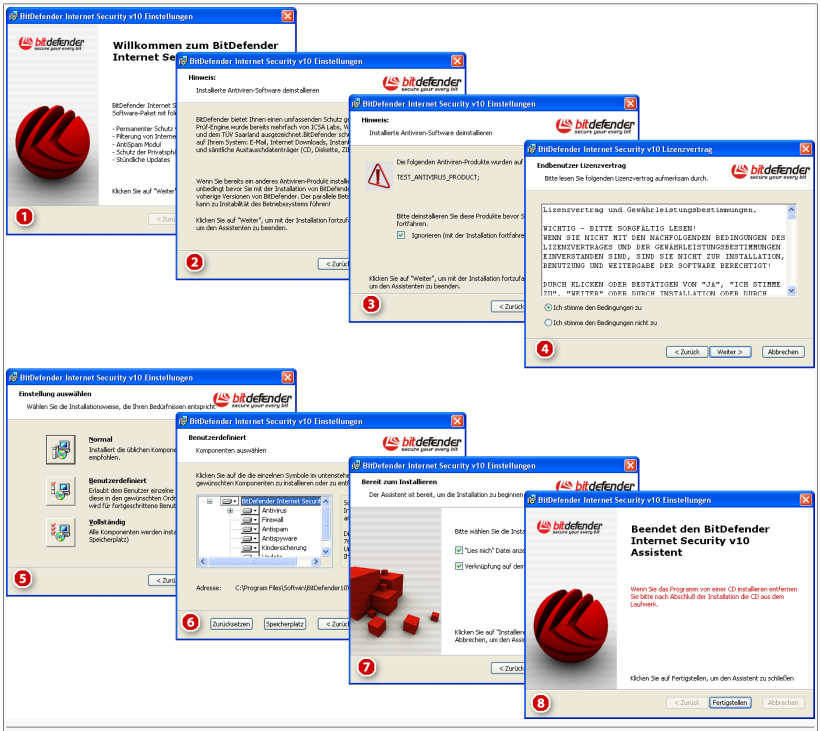
Microsoft Windows Vista (32-Bit)

- 800 MHz oder schneller
- 512 MB Arbeitsspeicher (1 GB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte

BitDefender Internet Security 10 kann als Testversion von der Webseite http://www.bitdefender.com heruntergeladen werden.

2.2. Installationsschritte

Lokalisieren Sie die Setup-Datei und führen Sie einen Doppelklick aus. Sie starten damit einen Assistenten, der Sie durch den Installationsprozess leitet.



Installationsschritte

1. Klicken Sie auf **Weiter**, um fortzufahren, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen.
2. Klicken Sie auf **Weiter** um fortzufahren, oder auf **Zurück** um wieder zum ersten Schritt zu gelangen.
3. BitDefender weist Sie daraufhin, falls Sie weitere Antiviren-Programme auf Ihrem Computer installiert sind.

Warnung

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

Klicken Sie auf **Zurück**, um zum letzten Schritt zurückzukehren, oder klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.

Anmerkung

Falls BitDefender keine weiteren Antiviren-Produkte auf diesem Computer erkennt wird dieser Schritt übersprungen.

4. Lesen Sie die Lizenzbedingungen, wählen Sie die Option **Ich stimme den Lizenzbedingungen zu**, und klicken Sie auf **Weiter**. Wenn Sie den Lizenzbestimmungen nicht zustimmen, klicken Sie auf **Abbrechen**. Der Installationsprozess wird abgebrochen und das Setup-Programm beendet.
5. Sie können bei der Installation zwischen verschieden Arten wählen: Normal, Benutzerdefiniert oder Vollständig.

   Typisch
   Das Programm wird mit den gebräuchlichen Einstellungen installiert. Dies ist die für die meisten Nutzer empfohlene Einstellung.

   Benutzerdefiniert
   Sie können die Einstellungen wählen, wenn Sie benutzerdefiniert installieren möchten. Diese Option wird nur erfahrenen Benutzern empfohlen.

   Vollständig
   Vollständige Installation. Alle Komponenten des Programms werden installiert.

   Wenn Sie **Typisch** oder **Vollständig** gewählt haben, überspringen Sie Schritt 6.
6. Wenn Sie **Benutzerdefiniert**, gewählt haben, öffnet sich ein Fenster mit allen BitDefender Komponenten, so dass Sie aus einer Liste wählen können, was Sie installieren möchten.

   Wenn Sie auf einen Komponentennamen klicken, wird auf der rechten Seite eine kurze Beschreibung angezeigt (in der auch der minimal erforderliche Festplattenplatz für die gewählte Option angegeben wird). Wenn Sie auf das Symbol einer Komponente klicken, wird ein Fenster angezeigt, in dem Sie die Auswahl bestätigen oder verwerfen können.

   Sie können den Ordner wählen, in dem das Produkt installiert werden soll. Standardmäßig wird BitDefender im Ordner `C:\Programme\Softwin\BitDefender 10` installiert.

   Falls Sie einen anderen Ordner wählen wollen, klicken Sie auf **Durchsuchen** und ein neues Fenster wird geöffnet, wo Sie einen neuen Ordner wählen können. Klicken Sie auf **Weiter**.
7. Sie haben zwei Möglichkeiten:

- **Öffnen der Readme Datei** - öffnen der Readme Datei am Ende der Installation.
- **Verknüpfung auf dem Desktop erstellen** - um ein Symbol am Ende der Installation auf Ihrem Desktop zu erstellen.

Klicken Sie auf **Installieren**, um mit der Installation des Produkts zu beginnen.

Wichtig

Während des Installationsprozesses wird ein Assistent erscheinen. Der Assistent hilft Ihnen dabei **BitDefender Internet Security v10** zu registrieren, ein Benutzerkonto einzurichten, und wichtige Sicherheitseinstellungen vorzunehmen. Vervollständigen Sie den Assistenten um zum nächsten Schritt zu gelangen.

8. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Wenn Sie die standardmäßigen Einstellungen für die Installation akzeptiert haben, wurde ein neuer Ordner mit dem Namen `Softwin` in `Programme Dateien` angelegt, der den Unterordner `BitDefender 10` beinhaltet.

Anmerkung

Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setup-Assistent das Setup beenden kann.

2.3. Einrichtungs-Assistent

Während des Installationsprozesses steht Ihnen der Assistent zur Verfügung. Der Assistent hilft Ihnen dabei **BitDefender Internet Security v10** zu registrieren, ein BitDefender Benutzerkonto einzurichten und BitDefender für wichtige Sicherheitseinstellungen einzurichten.

Den Assistenten zu beenden ist nicht verpflichtend. Wie auch immer, wir empfehlen dies um Ihnen Zeit zu sparen und Ihr System zu sichern selbst bevor Sie BitDefender installiert haben.

2.3.1. Schritt 1/8 - Willkommen zum BitDefender Einrichtungs-Assistent

Begrüßungsfenster

Klicken Sie auf **Weiter**.

2.3.2. Schritt 2/8 - BitDefender Internet Security v10 registrieren

Registrierung

Bitte verwenden Sie den Befehl **Aktualisieren** im Abschnitt **Aktivität** (um die letzten Aktivitäten der **Firewall** einsehen zu können).

Um das Produkt weiter zu testen, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**.

Klicken Sie auf **Weiter**.

2.3.3. Schritt 3/8 - BitDefender Benutzerkonto erstellen

Ich habe noch kein BitDefender Benutzerkonto

Um vom technischen Support von BitDefender zu profitieren und weitere zur Verfügung stehende Services zu erhalten müssen Sie ein Nutzerkonto einrichten.

Tragen Sie eine gültige E-Mail Adresse **E-mail** in das Feld ein. Legen Sie ein Passwort fest und geben es in das Feld **Password** ein. Bestätigen Sie das Passwort **durch Wiederholen** . Zum Einloggen in Ihr Nutzerkonto benutzen Sie Ihre E-Mail und das Passwort http://myaccount.bitdefender.com.

Anmerkung

Das Passwort sollte mindestens 4 Zeichen haben.

Um erfolgreich ein Nutzerkonto einzurichten müsssen Sie zunächste Ihre E-Mail Adresse aktivieren. Überprüfen Sie Ihre E-Mail Adresse und folgen Sie den Instruktionen, die Ihnen per E-Mail vom BitDefender Registrierungsservice zugeschickt wurden.

Wichtig

Bitte aktivieren Sie Ihr Nutzerkonto bevor Sie zum nächsten Schritt weitergehen.

Wenn Sie kein BitDefender Nutzerkonto einrichten wollen, klicken Sie auf **Diesen Schritt überspringen**. Überspringen Sie ebenfalls den nächsten Schritt des Assistenten.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

Ich habe bereits ein BitDefender Nutzerkonto.

Wenn Sie bereits ein aktives Nutzerkonto haben, geben Sie Ihre E-Mail und das Passwort ein. Wenn Sie ein falsches Passwort eingeben, werden Sie zur Wiederholung aufgefordert, wenn Sie auf **Weiter** klicken. Klicken Sie **Ok** um das Passwort nochmal einzugeben oder **abbrechen** um den Assistenten zu beenden.

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

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.4. Schritt 4/8 – Daten Nutzerkonto eingeben

Daten Nutzerkonto

Anmerkung

Sie können den Schritt auslassen, wenn Sie **Diesen Schritt auslassen anklicken** in dem Feld Schritt Drei.

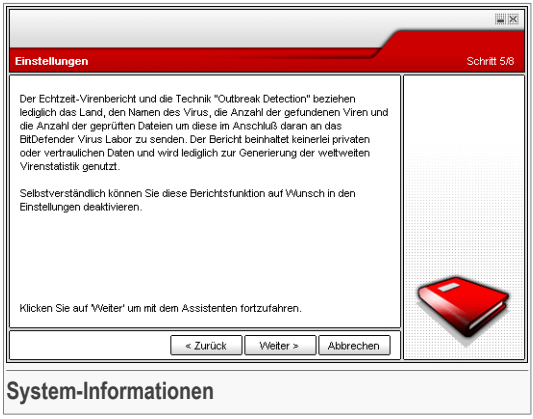
Tragen Sie bitte Ihren Vor- und Nachnahmen ein und wählen Sie ein Land aus.

Wenn Sie bereits ein Benutzerkonto haben wird der Assistent Ihnen die bereits eingetragenen Informationen anzeigen, falls Sie Daten hinterlegt haben. Sie können hier Änderungen vornehmen.

Wichtig
Die hier eingetragenen Daten bleiben vertraulich.

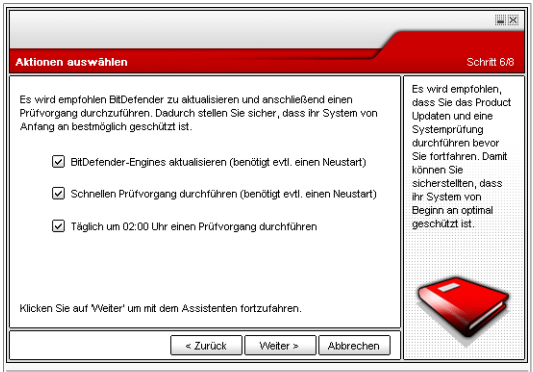
Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.5. Schritt 5/8 - Informationen über RTVR



Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.6. Schritt 6/8 – Aufgabentyp



Auswahl für Aktionen

Nehmen Sie hier die BitDefender Sicherheitseinstellungen für Ihr System vor.

Folgende Optionen stehen zur Verfügung:

- **Update von BitDefender (möglicherweise mit Neustart)** - beim nächsten Schritt wird ein Update der BitDefender Engine durchgeführt, um Ihren Computer gegen aktuelle Gefahren zu schützen.
- **Schnelle Systemprüfung (erfordert möglicherweise Neustart)** - Während des nächsten Schrittes wird eine Schnellprüfung durchgeführt, damit BitDefender sicherstellen kann, dass Ihre Dateien aus dem Verzeichnis `Windows` and `Program Files` nicht infiziert werden.
- **Jeden Tag um 02:00 Uhr einen Prüfvorgang ausführen** - führt jeden Freitag zur angegebenen Uhrzeit einen Prüfvorgang aus.

Wichtig

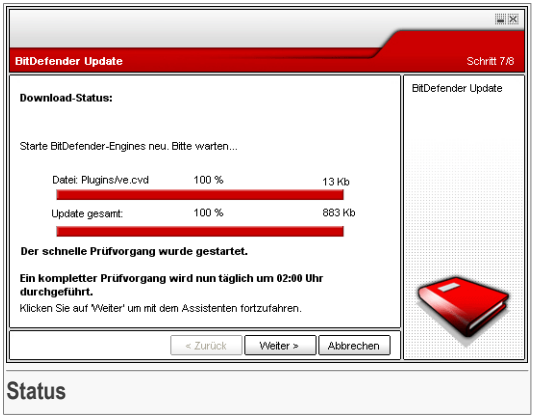
Wir empfehlen die Aktivierung dieser Optionen um die optimale Sicherheit Ihres Systems zu gewährleisten.

Wenn sie keine der Optionen oder nur die letzte auswählen wird der nächste Schritt übersprungen.

Sie können jedoch jegliche Veränderungen vornehmen, in dem Sie zu den vorherigen Schritten zurückkehren (Klicken Sie auf **Zurück**). Weiterhin, ist dieses Verfahren nicht umkehrbar: falls Sie fortsetzen auswählen, wird es nicht möglich sein zu den vorherigen Schritten zurückzukehren.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

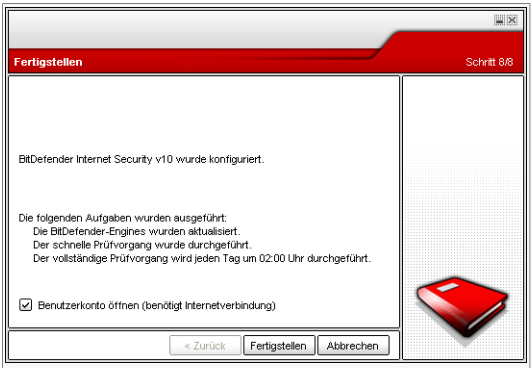
2.3.7. Schritt 7/8 - Warten bis Aufgaben vervollständigt wurden



Warten bis die Aufgaben vervollständigt wurden. Sie können den Status der Aufgaben nun sehen.

Klicken Sie auf **Weiter**. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

2.3.8. Schritt 8/8 – Aufgabenübersicht



Fertigstellen

Dies ist der letzte Schritt der Konfigurationsassistenten.

Klicken Sie in der BitDefender Management-Konsole auf die Option **Berichte**

Klicken Sie auf **Fertigstellen**, um den Installations-Assistent abzuschliessen und mit der Installation fortzusetzen.

2.4. Upgrade

Die Prozedur für das Upgrade kann über zwei Schritte erfolgen:

- **Deinstallieren Sie bitte die Vorgängerversion und installieren Sie die neue Version. Dies gilt für alle BitDefender Versionen.**

  Deinstallieren Sie zunächst die Vorgängerversion. Starten Sie dann den Computer neu und installieren Sie die neue Version wie im Abschnitt „*Installationsschritte*“ (S. 9) beschrieben.

Wichtig

Falls Sie von einer vorherigen Version von BitDefender auf eine neuere aktualisieren, empfehlen wir Ihnen die persönlichen Einstellungen und ggf. die Liste der Spammer und Freunde zunächst zu exportieren. Nach der Aktualisierung können diese Daten anschließend wieder importiert werden.

2.5. Entfernen, reparieren oder ändern einzelner BitDefender Funktionen

Wenn Sie das Programm **BitDefender Internet Security 10** ändern, reparieren oder entfernen möchten, gehen Sie über das Windows-Startmenü wie folgt vor: **Start** → **Programme** → **BitDefender 10** → **Ändern, Reparieren, Deinstallation**

Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Weiter**. Ein neues Fenster mit folgenden Auswahloptionen wird angezeigt:

- **Ändern** - dient zum Hinzufügen bzw. Entfernen von Programmkomponenten;
- **Reparieren** - dient zur Neuinstallation sämtlicher Programmkomponenten, die beim vorhergegangenen Setup installiert wurden;

Wichtig

Wir empfehlen Ihnen, vor der Reparatur des Produktes die Liste der Freunde und die Liste der Spammer zu sichern. Außerdem sollten Sie die Einstellungen und die Definitionen für den Bayesian–Filter sichern. Nach dem Reparaturvorgang können alle Einstellungen wieder geladen werden.

- **Entfernen** - dient zum Entfernen aller installierten Komponenten.

Um mit dem Setup fortzufahren, wählen Sie bitte eine dieser aufgeführten Optionen. Wir empfehlen **Deinstallation** für eine saubere Installation. Nach dem Deinstallieren löschen Sie am besten den Ordner `Softwin` aus dem Ordner `Programme`.

Beschreibung und Funktionen

3. BitDefender Internet Security v10

Umfassender Schutz vor Gefahren aus dem Internet.

BitDefender Internet Security v10 schützt Sie und Ihre Familie zuverlässig vor Computerviren, Spam und E-Mails mit betrügerischen Absichten. Das Programm verhindert das Ausspionieren vertraulicher Inhalte und unterbindet unberechtigten Zugriff auf Ihren Rechner. Zudem sorgt es dafür, dass Ihre Kinder keine anstößigen Webinhalte zu sehen bekommen oder nächtelang am PC spielen oder surfen.

BitDefender v10 wurde so konzipiert, dass die Systemressourcen minimal belastet werden und es gleichzeitig ein Maximum an Schutz gegen Internet Gefahren bietet.

3.1. Antivirus

Die Aufgabe des Antivirus-Moduls ist sicherzustellen, dass alle Viren entdeckt und beseitigt werden. BitDefender nutzt robuste Scan-Maschinen, die von ICSA Labs, Virus Bulletin, Checkmark, Checkvir und TÜV zertifiziert worden sind.

Pro-aktiver Virenschutz. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments)ist eine verhaltensbasierte Heuristik-Analyse in virtueller Umgebung und simuliert einen Computer im Computer, in dem Teile der Software auf gefährliches Verhalten überprüft werden. Diese proaktive Technologie stellt eine weitere Sicherheitsebene dar, die das Betriebssystem vor unbekannten Viren schützt, indem gefährliche Kodierungen erkannt werden, für die noch keine Signaturen veröffentlicht wurden.

Permanenter Virenschutz. Die neuen und verbesserten BitDefender-Engines prüfen und desinfizieren infizierte Dateien auf Befehl und minimieren den Datenverlust. Infizierte Dokumente können nun wiederhergestellt werden, anstatt wie früher gelöscht werden zu müssen.

Erkennung und Entfernung von Rootkits. Ein neues BitDefender-Modul überprüft Ihren Computer auf Rootkits (bösartige Softare welche darauf ausgelegt ist verborgen zu bleiben und den Computer fernsteuern kann) und entfernt diese bei Erkennung.

Prüfvorgänge durchführen. Internet Datenverkehr wird in Echtzeit geprüft und bietet ein sicheres und unbeschwertes Surfvergnügen.

Peer-2-Peer Applikationsschutz: Scannt nach Viren, die durch Instant Messaging und Filesharing-Software verteilt werden.

Kompletter E-Mail Schutz: Diese Anwendung funktioniert unter POP3/SMTP Protokollebene und blockiert alle infizierten E-Mail Inhalte, ohne Rücksicht zu nehmen auf den genutzten E-Mail Client (MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.). Dies geschieht ohne zusätzlichen Konfigurationsaufwand.

3.2. Firewall

Die Firewall filtert den Netzwerk-Datenverkehr und überwacht, welche Nutzer und Programme wann auf das Internet zugreifen und ob sie dazu berechtigt sind. Im Tarnkappenmodus (Stealth Mode) „versteckt“ sie Ihren Computer vor bösartiger Software und Hackern. Bei optimaler Konfiguration wird der externe Dateizugriff komplett gesperrt. Die Firewall entdeckt ebenso automatisch sogenannte Port Scans mit denen Angreifer mögliche Zugangspunkte ausfindig machen.

Überwachung des Internetverkehrs: Legen Sie selbst genau fest, welchen Programmen es erlaubt ist, über das Internet Daten zu verschicken. Definieren Sie eigene Regeln für den Datenverkehr mit dem Internet (Protokolle, Ports, Programme oder Adressen auf fremden Rechnern), oder nutzen Sie den Wizzard um alle nötigen Regeln automatisch zu erstellen.

Bessere Programmkontrolle bei Internetzugriffen: BitDefender stellt eine Datenbank mit vertrauenswürdigen Anwendungen zur Verfügung und informiert den Nutzer darüber, ob eine Anwendung, die versucht auf das Netzwerk zuzugreifen vertrauenswürdig ist, damit Sie richtig entscheiden können. BitDefender kann auch automatisch für vertrauenswürdige Anwendungen Zugang gewähren.

Echtzeit-Verbindungsüberwachung: Mit BitDefender haben Sie jederzeit Kontrolle darüber, welche Programme gerade eine Verbindung zum Netzwerk geöffnet haben. Mit einem einzigen Mausklick können Sie bestimmen, ob Sie diese Verbindungen dauerhaft oder nur für die momentane Sitzung erlauben oder sperren möchten.

Stealth-Modus ("Tarnkappen-Modus"). Spione, die Böses im Schilde führen, geht es nichts an, dass es Ihren Computer überhaupt gibt – geschweige denn, ob er im Netz aktiv ist. Unberechtigte sollten nicht herausfinden können, über welche Ports Ihr Computer zum Internet hin geöffnet ist oder wo er sich befindet. Im Tarnkappenmodus ist Ihr Computer im Internet unsichtbar.

Portscan-Erkennung. Das Bitdefender Firewall Modul kann nun automatisch sogenannte Port Scans entdecken und blockieren. Mit Hilfe des Port Scans können Angreifer mögliche "Schwachpunkte" entdecken. Ähnlich wie z.B. Einbrecher, die ausprobieren, ob eine Tür abgeschlossen ist oder nicht.

Der Regelassistent. Der Firewall Assistent hilft Ihnen Ihr eigenes Sicherheitsprofil einzurichten, genau darauf abgestimmt, wo Sie sich gerade befinden - zu Hause, im Büro oder unterwegs.

3.3. AntiSpam

Die neue und verbesserte BitDefender Antispam Technologie enthält innovative Funktionalitäten, die es erlauben Spamming Angriffe abzuwehren während sie sich ausbreiten. E-Mails werden gemäß den Vorgaben des Anwenders gefiltert, damit möglichst wenig erlaubte Mails als Spam gekennzeichnet werden.

Lernfähige Filterung. BitDefender nutzt moderne Clustering Methoden und Techniken der Neuronalen Netzwerk Analyse um E-Mails basierend auf den Präferenzen des Nutzers zu filtern. Der Bayesianische Filter kann trainiert werden (einfach indem einige Mails als Spam oder erlaubt gekennzeichnet werden)und er trainiert sich selbts indem imer weitere Filter Regeln erstellt werden, aufgrund zuvor gemachter Entscheidungen.

Anti-Phishing: Dank des neuen BitDefender Phishing-Detektors bleiben Sie von betrügerischen E-Mails verschont, mit denen Sie überlistet werden sollen, Ihre Kontodaten preiszugeben. Insbesondere beim Online Banking und Broking erhöht dieser Detektor die Sicherheit.

Heuristik, White List/Black List, Zeichenfilter und Grafik-Filter: Der heuristische Filter prüft, ob eine E-Mail typische Spam-Kennzeichen aufweist. Der Whitelist/Blacklist-Filter weist alle E-Mails von Absendern zurück, die als Spamversender bekannt sind. E-Mails von Ihren Freunden werden durchgelassen. Der URL-Filter schützt Sie vor E-Mails, die bösartige Links enthalten. Der Zeichensatzfilter hält E-Mails zurück, die mit „fremden“ Zeichen geschrieben sind (zum Beispiel mit arabischen oder kyrillischen Buchstaben). Der Grafik-Filter kann feststellen, ob in E-Mails enthaltene Bilder typisch für Spam sind.

Kompatibel mit allen E-Mail Clients: BitDefender AntiSpam ist mit allen gängigen E-Mail-Programmen kompatibel und kann von der BitDefender Management Konsole aus konfiguriert werden. Darüber hinaus lässt es sich problemlos in Outlook und Outlook Express einbinden. Mit dem BitDefender Antispam-Symbolleiste in Microsoft Outlook™ und Outlook Express™ kann der Anwender den Bayesian-Filter trainieren.

3.4. Antispyware

Verhindern Sie, dass Ihr Computer durch Software bedroht ist, die Ihre Daten ausspioniert. Wehren Sie diese Spyware ab, bevor sie Schaden auf Ihrem System anrichtet. Unsere umfangreiche Datenbank hilft Ihnen dabei, Ihren Computer frei von Spyware zu halten. Die BitDefender Spyware Heuristik untersucht eingehende E-Mails nach typischen Spyware-Merkmalen und markiert diese automatisch als Spyware.

Echtzeit-Spywareschutz: BitDefender überwacht Duzende von möglichen Angriffspunkten („HotSpots“) in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft ebenfalls jede Veränderung innerhalb des Systems und der

vorhandenen Software. Bekannte Spyware-Programme werden sogar in Echtzeit blockiert.

Überprüfung des Systems: BitDefender kann Ihr System komplett oder teilweise nach Spyware absuchen. Dabei vergleicht das Programm die Merkmale von bekannter Spyware, die in der laufend aktualisierten Softwin Datenbank erfasst sind.

Schutz der Privatsphäre. Der private "Türsteher" überprüft kontinuierlich Internet (http) und Mail (SMTP) Verkehr der Ihren Computer verlässt, ob darin persönliche Daten wir Kreditkartennummer, Kontodaten oder andere Informationen wie z.B. Passwörter enthalten sind sind.

Dialer Schutz. Ein frei konfigurierbarer Dialer-Schutz verhindert, dass Programme ohne Ihr Wissen eine kostenpflichtige Verbindung zum Internet aufbauen können. So sind Sie vor bösen Überraschungen auf Ihrer nächsten Telefonrechnung sicher.

3.5. Kindersicherung

Mit dem BitDefender-Kindersicherungsmodul können Sie den Zugriff auf jugendgefährdende Internetseiten sperren oder die Nutzung des Internets zu bestimmten Uhrzeiten unterbinden. Spiel-, Chat-, Filesharing- und andere Programme können ebenfalls nach Ihren Vorgaben blockiert werden.

Web-Kontrolle: Über einen Filter können Sie den Zugriff auf Webinhalte verhindern, die Sie für nicht altersgerecht halten. Eine Liste geblockter Webseiten und Teilbereichen ist Ihnen bereits zur Verfügung gestellt und im Verlauf des normalen Update-Prozesses konstant erneuert.

Heuristischer Filter. Der heuristische Filter klassifiziert Internetseiten nach Inhalt oder anderen Anhaltspunkten. Anstatt nur Schlüsselwörter zu nutzen werden die gesamten Antispam Prinzipien angewandt. Es stehen auch vordefinierte Profile zur Verfügung abhängig vom Alter der Anwender.

Schlüsselwörter für den Web Filter: BitDefender Anwender können jetzt direkt alle Internetseiten sperren, die bestimmte Wörter oder Formulierungen enthalten.

Schlüsselwort Filter für Mail. Eingehenden E-Mail, die unangemessene Wörter oder Sätze enthalten können ausgefiltert werden, bevor Sie die Inbox erreichen.

Onlinezeitbegrenzung: Sie können den Zugriff auf das Internet für bestimmte Computernutzer oder Programme, z.B. Spiele auf festgelegte Uhrzeiten begrenzen (damit auch die Hausaufgaben und andere Aktivitäten nicht zu kurz kommen).

Programmkontrolle: Sie können jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software. Die gesperrten

Programme sind gleichzeitig gegen Veränderungen geschützt und lassen sich weder kopieren noch verschieben.

3.6. Weitere Eigenschaften

Einsatz und Anwendung. Ein Assistent startet automatisch nach der Installation und hilft den Anwendern die richtigen Einstellungen vorzunehmen, einen Zeitplan festzulegen und stellt einen schnellen Weg zur Registrierung und Aktivierung des Produktes zur Verfügung.

Für den Anwender. BitDefender hat mit Blick auf die Anwenderfreundlichkeit weiter an der Bedieneroberfläche gearbeitet um die einfache Bedienung und die Nutzung zu erleichtern. Als Ergebnis benötigen viele der BitDefender v10 Module deutlich weniger Anwender Interaktion mit Hilfe von bequemer Automatisierung und Lernfähigkeit der Programme.

Stündliche Aktualisierung: Bitdefender aktualisiert sich stündlich über das Internet. Dies geschieht über eine direkte Verbindung oder über einen Proxy-Server. Das Produkt ist darüber hinaus in der Lage sich selbst zu reparieren, indem es defekte oder fehlende Dateien aus dem Internet nachlädt. Besitzer einer BitDefender-Lizenz profitieren auch von kostenlosen Updates und Upgrades auf neuere Versionen.

Kostenloser Support. Werktags steht Ihnen unser deutschsprachiger Support von 8.00 Uhr bis 17.00 Uhr gerne für Fragen zur Verfügung. Unter www.bitdefender.de steht Ihnen unsere Datenbank mit Antworten auf mögliche Fragen rund um die Uhr zur Verfügung. Alle Updates und Produktverbesserungen (Upgrades) sind ab Installationsdatum für einen Zeitraum von 12 Monaten kostenlos. Weitere Informationen finden Sie unter www.bitdefender.de.

Notfall CD. Die **BitDefender Notfall CD** startet Ihren Computer vom CD ROM Laufwerk, falls Windows nicht mehr funktioniert. Danach repariert es mögliche Fehlerquellen und bereinigt Ihren Computer von Viren.

4. BitDefender Module

BitDefender Internet Security 10 beinhaltet die folgenden Module: **Allgemein**, **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Kindersicherung** und **Update**.

4.1. Das Modul Allgemein

BitDefender verfügt über eine vollständige Konfiguration für maximale Sicherheit.

Wesentliche Status-Informationen über alle BitDefender-Module werden im Allgemein-Modul angezeigt. Hier können Sie das Produkt registrieren und Grundeinstellungen von BitDefender anpassen.

4.2. Das Modul Antivirus

BitDefender schützt alle gängigen Angriffspunkte auf Ihrem System: E-Mail, Internet-Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP, USB-Speicher). Vom AntiVirus-Modul aus haben Sie Zugriff auf alle BitDefender-Einstellungen und BitDefender-Eigenschaften.

Der Virenschutz ist in zwei Kategorien aufgeteilt:

- Echtzeit-Virenschutz - verhindert, dass neue Viren Ihr System befallen. Dateien werden gescannt, sobald der Nutzer darauf zugreift. BitDefender zum Beispiel scannt ein Worddokument auf Viren, sobald Sie es öffnen, und E-Mails, sobald Sie sie erhalten. BitDefender prüft Ihre Dateien, sobald Sie sie nutzen.
- Prüfvorgang durchführen - entdeckt residente Viren auf Ihrem System. Das ist der klassische Virenscan, ausgelöst durch den Nutzer – Sie wählen ein Laufwerk einen Ordner oder eine Datei aus und BitDefender scannt sie – nach Aufforderung.

4.3. Das Modul Firewall

Das Personal-Firewall schützt Ihren Computer vor unberechtigten Zugriffen aus dem Internet. Sie überwacht Ihre Internetverbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.

Im Stealth-Modus wird ihr Computer im Netzwerk so gut wie unsichtbar vor Angriffen jeglicher Art. Das Firewall-Modul ist in der Lage Portscans zu erkennen und diese gezielt ins Leere laufen zu lassen - so als ob der Computer gar nicht existierte.

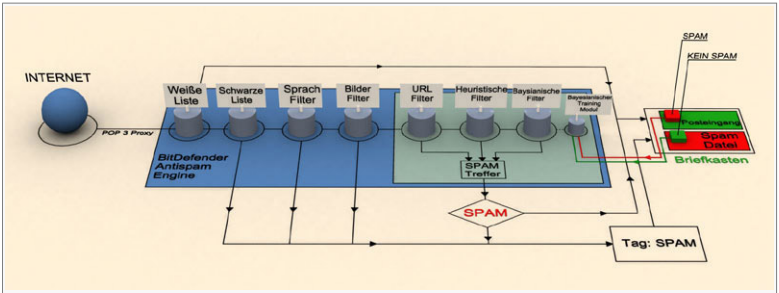
Die Firewall ist ein unersetzliches Instrument bei einer DSL- oder Breitbandverbindung.

4.4. Das Modul Antispam

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.

4.4.1. Arbeitsschemata

Das unten abgebildete Schema zeigt, wie BitDefender arbeitet.



AntiSpam Filter

Diese vorher genannten Filter (Liste der Freunde, Liste der Spammer, Zeichensatz-Filter, Grafik-Filter, URL-Filter, Heuristische Filter und Bayesian-Filter) werden in Verbindung mit dem BitDefender Antispam Modul verwendet, um herauszufiltern, ob eine E-Mail in Ihren **Posteingang** gelangt, oder nicht.

Jede E-Mail, die aus dem Internet kommt, wird zuerst mit den Filtern Weiße Liste/Schwarze Liste überprüft. Falls der Sender in der Weiße Liste gefunden wird, wird diese Mail direkt in Ihren **Posteingang** gesendet.

Der Filter Liste der Spammer überprüft, ob der Absender der E-Mail auf der gleichnamigen Liste eingetragen ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben (zu finden bei Microsoft Outlook).

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.

Falls die E-Mail diese Merkmale nicht aufweist, wird sie mit dem Grafik-Filter überprüft. Die **Grafik-Filter** erkennt E-Mail-Nachrichten, die Bilder bzw. Grafiken und Spam-Inhalte beinhalten.

Der URL-Filter überprüft die E-Mail nach Links und vergleicht diese mit jenen, die in der BitDefender-Datenbank stehen. Im Falle eines Treffers wird diese E-Mail als Spam verschoben.

Der Heuristische Filter testet die E-Mail auf den Inhalt, sucht nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam. Im Falle eines Treffers wird auch hier die E-Mail zum Spam hinzugefügt.

Anmerkung

Falls in der Betreffzeile Wörter mit sexuellem Inhalt gefunden werden, markiert BitDefender die E-Mail als Spam.

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

Falls die Summe aller Treffer (URL-Treffer + Heuristischer Treffer + Bayesian Treffer) die Spam-Treffer übersteigt (die durch den Benutzer in der AntiSpam-Sektion als Toleranzniveau festgelegt wird), wird die E-Mail als Spam deklariert.

Wichtig

Falls Sie einen anderen E-Mail Client außer Microsoft Outlook oder Microsoft Outlook Express verwenden, sollten Sie eine eigene Regel erstellen um E-Mails, die mit "[SPAM]" in der Betreffzeile als Spam markiert sind, in einen separaten Ordner zu verschieben. BitDefender wird jeder E-Mail den Text `[SPAM]` in der Betreffzeile hinzufügen.

4.4.2. AntiSpam Filter

BitDefender AntiSpam Maschinen arbeitet mit sieben verschiedenen Filtern, die sicherstellen, dass Ihr Posteingang spamfrei bleibt: Weiße Liste, Schwarze Liste, Zeichensatz-Filter, Grafik-Filter, URL-Filter, Heuristischer Filter und Bayesian-Filter.

Anmerkung

Sie können jeden dieser Filter im **AntiSpam**-Modul Einstellungen aktivieren/deaktivieren.

Weiße Liste / Schwarze 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).

Anmerkung

Die **Weiße Liste / Schwarze Liste** wird auch als **Freundes Liste / Spammer Liste** bezeichnet.

Sie können die **Freundes / Spammer Liste** in der BitDefender Management Konsole bearbeiten oder aber auch in der AntiSpam Sysmbolleiste (zu finden bei Outlook oder Outlook Express).

Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

Zeichensatz-Filter

Die meisten der Spam-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Konfigurieren Sie den Filter so, dass alle E-Mails ausgesondert werden, die diesen Kriterien entsprechen.

Grafik-Filter

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

URL-Filter

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

Jeder URL-Link innerhalb einer E-Mail wird mit der Datenbank verglichen und bei einem Treffer wird die Mail der Spamliste hinzugefügt. Im Falle einer Übereinstimmung wird die E-Mail als Spam gekennzeichnet.

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.

Entdeckt E-Mails mit dem Text "SEXUALLY EXPLICIT" in der Betreffzeile und markiert diese unverzüglich als Spam.

Anmerkung

Seit dem 19. Mai 2004 müssen E-Mails mit sexuellem Inhalt entsprechend markiert werden. D. h. in der Betreffzeile muss explizit auf den Inhalt hingewiesen werden.

Bayesian-Filter

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

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

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

Wichtig

Sie korrigieren das Modul, indem Sie die **Ist Spam** und **Kein Spam**-Buttons in „*AntiSpam Symbolleiste*“ (S. 119) anklicken (zu finden in Outlook und Outlook Express).

Anmerkung

Jedes mal wenn ein Update durchgeführt wird:

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

Somit wird die Effektivität des Antispam-Moduls laufend verbessert.

Wichtig

BitDefender kann automatische Updates durchführen. Lassen Sie daher das **Automatische Update** aktiviert.

4.5. Das Modul Antispyware

BitDefender überwacht dutzende von möglichen Angriffspunkten (sog. "HotSpots") in Ihrem System, die durch Spyware befallen werden könnten. Es überprüft ebenfalls jede Veränderung innerhalb des Systems und der vorhandenen Software. Bekannte Spyware-Programme werden in Echtzeit blockiert. Die BitDefender AntiSpyware ist höchst effizient in der Bekämpfung von Trojanischen Pferden oder auch anderen bösartigen Instrumenten von Crackern (oftmals als Hacker bezeichnet). Sie bietet einen zuverlässigen Schutz vor Angriffen auf Ihre Privatsphäre und dem unbefugten Versenden persönlicher Daten wie z.B. Kreditkartennummern, PINs oder TANs, usw. von Ihrem Computer zum Angreifer.

4.6. Das Modul Kindersicherung

Mit der Kindersicherung können Sie den Zugriff auf jugendgefährdende Internetseiten sperren oder die Nutzung des Internets zu bestimmten Uhrzeiten unterbinden. Spiel-, Chat-, Filesharing- und andere Programme können ebenfalls nach Ihren Vorgaben blockiert werden.

4.7. Das Modul Update

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm BitDefender stets mit den neuesten Virensignaturen betreiben. Standardmäßig prüft BitDefender automatisch im Abstand von drei Stunden, ob neue Updates zur Verfügung stehen.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die Antivirus-Module** - wenn neue Bedrohungen auftreten, müssen die Dateien, in den die Virensignaturen enthalten sind, aktualisiert werden, damit ein kontinuierlicher und aktueller Schutz auch vor den neuen Gefahren gewährleistet ist. Diese Update-Art wird auch als **Virendefinitions-Update** bezeichnet.
- **Updates für die AntiSpam Prüfung** - Um den Spamschutz zu verbessern, werden neue Regeln zur Heuristik und zum URL-Filter hinzugefügt. Diesen Vorgang nennt man **AntiSpam-Update**.
- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur BitDefender Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.

- **Produkt-Update** - Wenn eine neue Version von BitDefender erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Produkt-Update**.

Darüber hinaus müssen auch die Update-Arten aufgelistet werden, die einen Benutzereingriff erfordern.

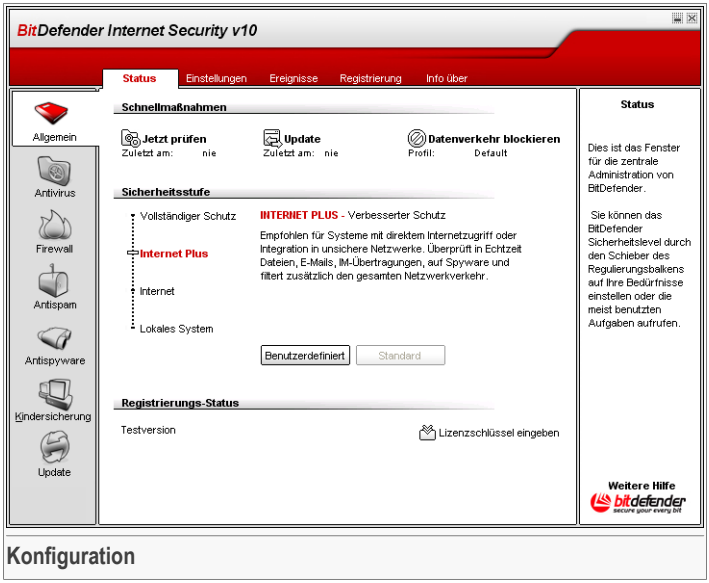
- Automatisches Update - BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind. Falls entsprechend eingestellt, aktualisiert BitDefender sich automatisch. Das automatische Update kann auch jederzeit über den Klick **Prüfen** gestartet werden.
- Manuelles Update - Download und Installation der neuesten Virendefinitionen erfolgen manuell.

Konfiguration

5. Überblick

BitDefender Internet Security v10 enthält eine zentrale Management-Konsole, die es erlaubt, die Schutzfunktionen für alle BitDefender-Module zu konfigurieren. Mit anderen Worten: Es reicht aus, die Management-Konsole zu öffnen, um Zugriff auf alle Module zu haben: **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Kindersicherung** und **Update**.

Sie erreichen die BitDefender Management-Konsole über das Windows-Startmenü: **Start → Programme → BitDefender v10 → BitDefender Internet Security v10**. Schneller geht es jedoch mittels Doppelklick auf das **BitDefender Symbol** in der Systemleiste.



Konfiguration

Auf der linken Seite der Management-Konsole sehen Sie die Modulauswahl:

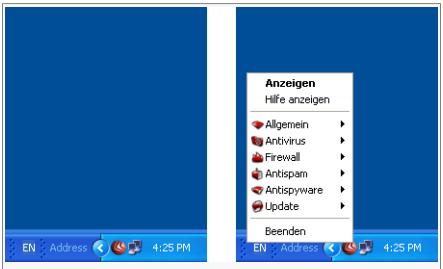
- Allgemein - Sie sehen eine Zusammenfassung aller BitDefender-Einstellungen, überdies Produktdetails und Kontaktinformationen. Hier können Sie auch das Produkt registrieren.
- Antivirus - In diesem Bereich können Sie das **AntiVirus**-Modul konfigurieren.

- Firewall - In diesem Bereich können Sie das **Firewall**-Modul konfigurieren.
- AntiSpam - In diesem Bereich können Sie das **AntiSpam**-Modul konfigurieren.
- AntiSpyware - In diesem Bereich können Sie das **AntiSpyware**-Modul konfigurieren.
- Kindersicherung - In diesem Bereich können Sie das Modul **Kindersicherung** konfigurieren.
- Update - In diesem Bereich können Sie **Updates** konfigurieren.

Im rechten Bereich der Management Konsole sehen Sie Informationen zum jeweiligen Abschnitt, in dem Sie sich befinden. Die Option **Weitere Hilfe**, platziert unten rechts, öffnet die **Online-Hilfe**.

5.1. Systemleiste

Wenn die Konsole minimiert ist, erscheint ein Symbol in der Symbolleiste:



BitDefender-Symbol im System-Tray

Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü mit folgenden Optionen für die schnelle Verwaltung von BitDefender:

- **Schließen** - minimiert das Programm.
- **Hilfe anzeigen** - öffnet die Hilfe-Datei.
- **Allgemein** - Klicken Sie auf den Button im Modul Allgemein .
  - **Geben Sie den neuen Lizenzschlüssel ein** - Startet den Assistenten, der Sie durch die Registrierung führt.
  - **Erstellen eines Nutzerkontos** - startet den Assistenten, der Ihnen beim Erstellen eines BitDefender Nutzerkontos hilft.
- **BitDefender AntiVirus** - klicken Sie auf diesen Button, um das AntiVirus Modul zu öffnen.
  - **Echtzeitschutz aktiviert/deaktiviert** - Zeigt den Status des Echtzeitschutzes an(aktiviert/deaktiviert). Klicken Sie diesen Button um den Echtzeitschutz zu aktivieren/deaktivieren.

- **Durchsuchen** - öffnet ein Fenster, in welchem Sie die Berichtsdateien, die Sie sich ansehen wollen, auswählen können.

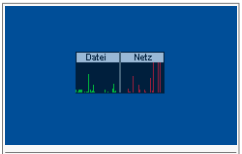
- **Firewall** - klicken Sie auf diesen Button, um das Modul Firewall zu öffnen.
  - **Firewall ist aktiviert/deaktiviert** - Status anzeigen firewall Schutz (aktiviert/deaktiviert). Klicken Sie hier um den Firewall Schutz zu deaktivieren/aktivieren.
  - Wählen Sie **Sämtlichen Datenverkehr sperren**, um alle Verbindungen zu stoppen.
- **BitDefender AntiSpam** - klicken Sie auf diesen Button, um die Management-Konsole zu öffnen.
  - **Antispam ist aktiviert/deaktiviert** - Zeigt den Status des Antispam Schutzes an (aktiviert/ deaktiviert). Klicken Sie hier um den Antispam Schutz zu aktivieren/deaktivieren.
  - **Freundes/Spammer listen** - aktiviert/deaktiviert den Freundes/Spammerliste;
  - **Spammerliste** - öffnet Spammerliste;
- **BitDefender AntiSpyware** - klicken Sie auf diesen Button, um das AntiSpyware Modul zu öffnen.
  - **Verhaltensbasierte Antispyware ist aktiviert/deaktiviert** - Zeigt den Status des Echtzeit AntiSpyware Schutzes an (aktiviert/ deaktiviert). Klicken Sie hier um den Echtzeit AntiSpyware Schutz zu aktivieren/deaktivieren.
  - **Erweiterte Einstellungen** - Möglichkeit die AntiSpyware Kontrolle zu konfigurieren.
- **Update** - klicken Sie auf diesen Button, um die Option Update zu öffnen.
  - **Update jetzt durchführen** - führt unverzüglich ein verfügbares Update von BitDefender durch.
  - **Automatisches Update ist aktiviert/ deaktiviert** - zeigt den Status des Automatischen update (aktiviert/deaktiviert). Klicken Sie hier um das Automatische Update zu aktivieren/deaktivieren.
- **Beenden** - beendet die Anwendung. Bei der Auswahl dieser Option verschwindet das Symbol von der Symbolleiste. Für einen erneuten Zugriff starten Sie aus dem Start-Menü.

Anmerkung

Wenn Sie ein oder mehrere Module von BitDefender deaktivieren verändert sich das Symbol von BitDefender in der System-Tray. So werden Sie auch bei geschlossener Konsole über den Status von BitDefender informiert.
Das BitDefender-Symbol blinkt wenn ein Update zur Verfügung steht.

5.2. Aktivitsänzeige

Die **Aktivitätsanzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.



Aktivitäsanzeige

Die grünen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50.

Die roten Balken in der **Netz-Zone** zeigen die Anzahl der transferierten KBytes (gesendet und empfangen aus dem Internet) pro Sekunde auf einer Skala von 0 bis 100.

Anmerkung

Die **Scan Aktions-Anzeige** informiert Sie mit einem roten „X“, wenn das Virus Schild oder die Firewall deaktiviert ist (**Datei** oder **Netz**). Somit sind Sie über diesen Zustand auch informiert, wenn die Management Konsole nicht geöffnet ist.

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**.

Anmerkung

Um das Fenster komplett zu verbergen, entfernen Sie das Häkchen bei **Aktivitätsanzeige einblenden** (im Abschnitt Einstellungen im Menüpunkt **Allgemein**).

6. Das Modul Allgemein

Der Abschnitt **Allgemein** behandelt und erklärt folgende Themen:

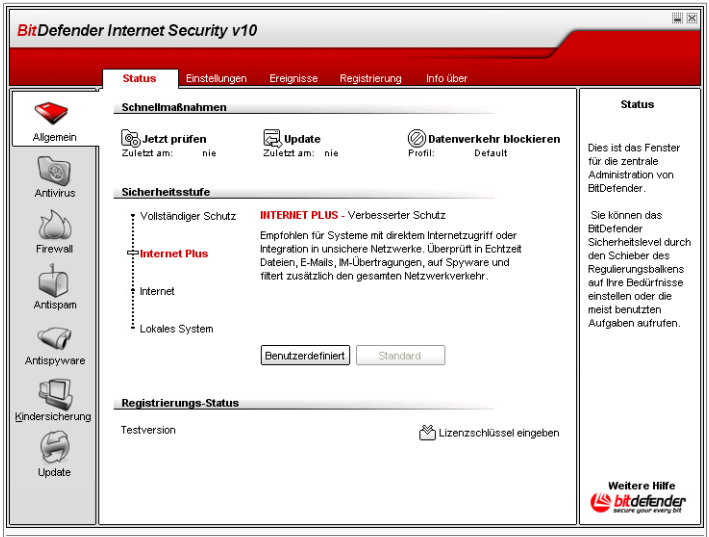
- Status aller BitDefender Module
- Allgemeine Einstellungen
- Ereignisanzeige
- Registrierung des Produkts
- Info über

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Allgemein** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Allgemein*“ (S. 29).

6.1. Status aller BitDefender Module

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Allgemein**.



Status aller BitDefender Module

In diesem Abschnitt können Sie alle wichtigen Sicherheitseinstellungen von BitDefender vornehmen. Hier können Sie das Produkt registrieren und das Ablaufdatum ablesen.

6.1.1. Schnell Einstellungen

BitDefender erlaubt schnellen Zugang zu allen Sicherheitseinstellungen. Mit Hilfe dieser Einstellungen bleibt BitDefender aktuell, Sie können das System prüfen oder Datenverkehr blockieren.

Um das gesamte System zu prüfen klicken Sie einfach **Jetzt scannen** - Das Prüffenster erscheint Prüffenster und die Systemprüfung wird gestartet.

Wichtig

Wir empfehlen dringend, einen kompletten Virenscan mindestens einmal in der Woche durchzuführen. Um einen kompletten Systemscan durchzuführen, aktivieren Sie das **AntiVirus**-Modul, Sektion Prüfen, wählen Sie die zu prüfenden **Lokalen Laufwerke** aus und klicken Sie dann auf **Prüfen**.

Bevor Sie die Systemprüfung starten, empfehlen wir Ihnen BitDefender zu aktualisieren. So können auch die neuesten Schädlinge entdeckt werden. Um BitDefener zu aktualisieren klicken Sie **Update**. Warten Sie bis der Update Prozess abgeschlossen ist. Sie könne auch unter Update den Update Status verfolgen.

Anmerkung

Weitere Informationen über den Update Prozess finden Sie im Kapitel Update in diesem Handbuch.

Um den Netzwerk/Internet Verkehr zu blockieren klicken Sie **Datenverkehr blockieren**. Ihr Computer ist dann von allen anderen Computern im Netzwerk isoliert.

Anmerkung

Für Informationen, wie Sie Ihren Computer effektiv innerhalb des Netzwerkes, in dem Sie eingebunden sind, schützen können klicken Sie auf das Firewall Module.

6.1.2. Sicherheitseinstellungen

Sie könnnen die Einstellungen so vornehmen, wie Sie Ihren Sicherheitsanforderungen am besten entsprechen. Ziehen Sie den Zeiger auf der Scala entlang, um Ihr Sicherheitslevel einzustellen.

Es gibt 4 mögliche Einstellungen:

Sicherheitseinstellungen	Beschreibung
Lokaler Rechner	Standard Einstellung, empfohlen für Computer ohne Netzwerk oder Internet Zugang. Sehr niedrige Belastung der Ressourcen. Prüft alle vorhanden Dateien.
Internet	Standardeinstellung für Computer, die direkt mit dem Internet oder unsicheren Netzwerken verbunden sind. Mittlere Belastung der Ressourcen. Dateien auf die Zugriffe erfolgten, E-Mails, Instant Messaging und der gesamte Netzwerk Datenverkehr werden überprüft um sicher vor Viren, Spyware und Hackern zu schützen.
Internet Plus	Bietet erweiterten Schutz für Computer, die direkt mit dem Internet oder unsicheren Netzwerken verbunden sind. Mittlere Belastung der Ressourcen. Dateien auf die Zugriffe erfolgten, E-Mails, Instant Messaging und der gesamte Netzwerk Datenverkehr werden überprüft um sicher vor Viren, Spyware, Hackern und Spam zu schützen.
Umfassender Schutz	Bietet umfassenden Schutz für Ihr System. Hohe Belastung der Ressourcen. Prüft Dateien auf die Zugriffe erfolgten, E-Mails, Instant Messaging und den gesamten Netzwerk Datenverkehr werden überprüft um sicher vor Viren, Spyware, Hackern, Spam (inkl. Phishing) und unerwünschten Inhalten zu schützen.

Sie können das Sicherheitslevel ändern, indem Sie auf **Benutzerdefiniert** klicken. Im neuen Fenster das nun erscheint können Sie die gewünschten Schutzmaßnahmen auswählen. Klicken Sie zum Bestätigen auf **OK**.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

6.1.3. Status der Registrierung

Dieser Abschnitt enthält Informationen zum Status Ihrer BitDefender Lizenz. Hier können Sie das Produkt registrieren und das Ablaufdatum ablesen.

Um einen neuen Lizenzschlüssel einzugeben klicken Sie **Neuen Lizenzschlüssel eingeben**. Beenden Registrierungs Assistent um BitDefender erfolgreich zu registrieren.

Anmerkung

Weitere Informationen über die Registrierung finden Sie im Kapitel Produkt Registrierungin diesem Handbuch.

6.2. Einstellungen der Management Konsole

Um diese Sektion zu öffnen klicken Sie bitte auf **Einstellungen** im Modul **Allgemein**.

Einstellungen der Management Konsole

Hier können Sie die umfassenden Einstellungen von BitDefender einsehen. Standardmäßig wird BitDefender beim Windowsstart geladen und läuft dann im Hintergrund.

Sie können zwischen 4 Kategorien auswählen: **Allgemeine Einstellungen**, **Einstellung Viren Report** , **Einfache Einstellung** und **Einstellungen verwalten**.

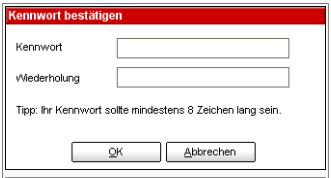
6.2.1. Allgemeine Einstellungen

- **Konsole per Kennwort schützen** - die Passwort-Einstellung aktivieren, um Ihre BitDefender-Einstellungen zu schützen.

Anmerkung

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

Wenn Sie diese Option wählen erscheint das folgende Fenster:



Kennwort bestätigen

Schreiben Sie ein Passwort in das **Kennwort**-Feld und wiederholen Sie es in dem Feld **Wiederholung**. Danach klicken Sie auf **OK**.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen von BitDefender ändern wollen.

Wichtig

Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie unter Reparieren Ihre BitDefender-Konfiguration modifizieren.

- **Sicherheits-Mitteilungen anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren.
- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart.

Anmerkung

Dies wird dringend empfohlen.

- **Prüfanzeige aktivieren (Grafische Anzeige Produkt Aktivität)** - (de)aktiviert auf Wunsch den Prüfanzeige von BitDefender.
- **Minimiert starten** - minimiert die BitDefender-Management-Konsole, nachdem das System gestartet worden ist. Nur das BitDefender Symbol erscheint in der Systemablage.

6.2.2. Einstellung Virenbericht

- **Viren-Meldung an das BitDefender Virus Labor** - sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Der Report enthält keinerlei vertrauliche Daten, wie z. B. Ihren Namen oder Ihre IP-Adresse, und wird nicht für kommerzielle Zwecke verwendet. Die gelieferten Informationen enthalten den Virennamen und werden lediglich für statistische Zwecke benötigt.

- **Viren-Meldung an das BitDefender Virus Labor** - sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Der Report enthält keinerlei vertrauliche Daten, wie z. B. Ihren Namen oder Ihre IP-Adresse, und wird nicht für kommerzielle Zwecke verwendet. Die gelieferten Informationen enthalten den Virennamen und werden lediglich für statistische Zwecke benötigt.

6.2.3. Auswahlfenster Einstellungen

Oberflächen - Datei erlaubt Ihnen, die Farbe der Management-Konsole zu wählen. Der Skin repräsentiert die Hintergrundgrafiken und Symbolfarben in der Benutzeroberfläche. Klicken Sie auf die jeweilige Bezeichnung, um die Benutzeroberfläche gemäß Ihren Wünschen anzupassen.

6.2.4. Update-Einstellungen

Verwenden Sie die Option **Alle Einstellungen speichern** / **Alle Einstellungen laden** um eine Sicherungskopie sämtlicher in BitDefender vorgenommenen Einstellungen zu exportieren und nach einer Reparatur wieder zu importieren.

Wichtig

Nur Anwender mit Administratoren Rechten können die Einstellungen ändern.

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

6.3. Ereignis

Um diese Sektion zu öffnen klicken Sie bitte auf **Ereignisse** im Modul **Allgemein**.

Ereignis

In dieser Sektion sind sämtliche von BitDefender erstellten Ereignisse angezeigt.

Es gibt drei Arten von Ereignissen: **Information**, **Warnung** und **Kritisch**.

Beispiel für solche Ereignisse:

- **Information** - Wenn eine E-Mail überprüft wurde;
- **Warnung** - Wenn eine verdächtige Datei gefunden wurde;
- **Kritisch** - Wenn eine infizierte Datei gefunden wurde.

Für jedes Ereignis werden die folgenden Informationen bereitgestellt: Datum und Uhrzeit, zu der das jeweilige Ereignis stattgefunden hat, eine kurze Beschreibung und seine Quelle (**AntiVirus**, **AntiSpyware** oder **Update**). Klicken Sie doppelt auf ein bestimmtes Ereignis und Sie erhalten weitere Informationen zu diesem.

Es ist möglich, die angezeigten Ereignisse auf zwei Arten zu filtern – nach Quelle oder nach Art:

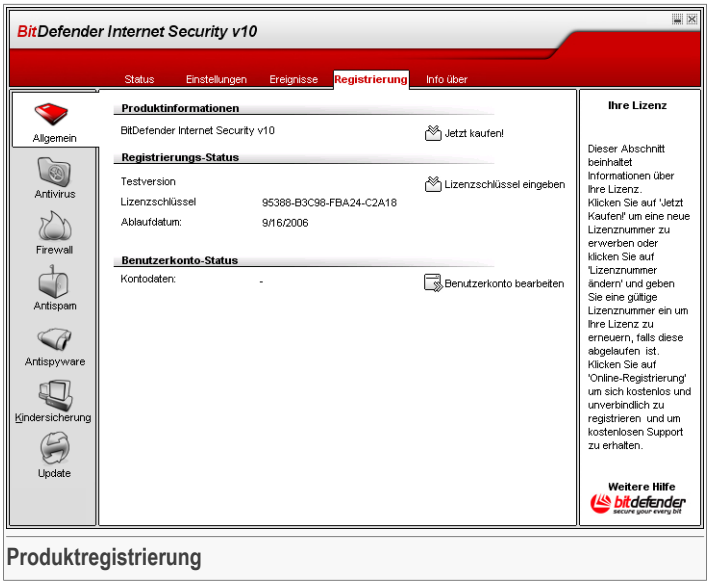
- Klicken Sie auf **Filter** und wählen Sie die gewünschte Ereignisart aus;
- Wählen Sie die Ereignisquelle, aus der gleichnamigen Dropdownliste.

Ist die Sektion **Ereignisse** bereits geöffnet, so müssen Sie auf die Schaltfläche **Aktualisieren**klicken, um neu hinzu gekommene Ereignisse anzeigen zu lassen.

Um alle Ereignisse zu löschen, klicken Sie bitte auf die Schaltfläche **Liste löschen**.

6.4. Produktregistrierung

Um diese Sektion zu öffnen klicken Sie bitte auf **Registrieren** im Modul **Allgemein**.



Produktregistrierung

Dieser Abschnitt enthält Informationen zum Produkt BitDefender (Status der Registrierung, Produkt ID, Ablaufdatum der Lizenz). Hier können Sie das Produkt registrieren und Ihr BitDefender Nutzerkonto konfigurieren.

Klicken Sie **Jetzt kaufen** um eine neue BitDefender Lizenz online zu kaufen.

Klicken Sie **Neuen Lizenzschlüsssel eingeben** Sie können das Produkt registrieren, die Registrierung oder Ihre Nutzerdaten ändern. Um Ihr Nutzerkonto zu konfigurieren klicken Sie **Nutzerkonto konfigurieren**. In beiden Fällen erscheint der Registrierungsassistent.

6.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus 5 einzelnen Schritten.

Schritt 1/5 - Willkommen beim BitDefender Konfigurations-Assistent.

Begrüßungsfenster

Klicken Sie auf **Weiter**.

Schritt 2/5 Wie kann ich BitDefender registrieren?

Registrierung

Bitte verwenden Sie den Befehl **Aktualisieren** im Abschnitt **Aktivität** (um die letzten Aktivitäten der **Firewall** einsehen zu können).

Um das Produkt weiter zu testen, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**.

Klicken Sie auf **Weiter**.

Schritt 3/5 – Einrichten eines BitDefender Nutzerkontos.

Kontoerstellung

Ich habe noch kein BitDefender Benutzerkonto

Um vom technischen Support von BitDefender zu profitieren und weitere zur Verfügung stehende Services zu erhalten müssen Sie ein Nutzerkonto einrichten.

Tragen Sie eine gültige E-Mail Adresse **E-mail** in das Feld ein. Legen Sie ein Passwort fest und geben es in das Feld **Password** ein. Bestätigen Sie das Passwort **durch Wiederholen** . Zum Einloggen in Ihr Nutzerkonto benutzen Sie Ihre E-Mail und das Passwort http://myaccount.bitdefender.com.

Anmerkung

Das Passwort sollte mindestens 4 Zeichen haben.

Um erfolgreich ein Nutzerkonto einzurichten müsssen Sie zunächste Ihre E-Mail Adresse aktivieren. Überprüfen Sie Ihre E-Mail Adresse und folgen Sie den Instruktionen, die Ihnen per E-Mail vom BitDefender Registrierungsservice zugeschickt wurden.

Wichtig

Bitte aktivieren Sie Ihr Nutzerkonto bevor Sie zum nächsten Schritt weitergehen.

Wenn Sie kein BitDefender Nutzerkonto einrichten wollen, klicken Sie auf **Diesen Schritt überspringen**. Überspringen Sie ebenfalls den nächsten Schritt des Assistenten.

Klicken Sie auf **Weiter**.

Ich habe bereits ein BitDefender Nutzerkonto.

Wenn Sie bereits ein aktives Nutzerkonto haben, geben Sie Ihre E-Mail und das Passwort ein. Wenn Sie ein falsches Passwort eingeben, werden Sie zur Wiederholung aufgefordert, wenn Sie auf **Weiter** klicken. Klicken Sie **Ok** um das Passwort nochmal einzugeben oder **abbrechen** um den Assistenten zu beenden.

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

Klicken Sie auf **Weiter**.

Schritt 4/5 - Auswählen der Prüfoptionen

Daten Nutzerkonto

Anmerkung

Dieser Schritt wird ausgelassen, wenn Sie auf **Schritt auslassen** klicken im Schritt 3.

Tragen Sie Ihren Vor- und Nachnahmen ein und wählen Sie ein Land aus.

Wenn Sie bereits ein BitDefender Nutzerkonto eingerichtet haben, wird der Assistent Ihnen die vorhandenen Informationen anzeigen. Sie können diese Informationen ändern.

Wichtig
Die hier eingetragenen Daten bleiben vertraulich.

Klicken Sie auf **Weiter**.

Schritt 5/5 – Übersicht

Fertigstellen

Dies ist der letzte Schritt der Konfigurationsassistenten. Sie können jedoch jegliche Veränderungen vornehmen, in dem Sie zu den vorherigen Schritten zurückkehren (Klicken Sie auf **Zurück**).

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

Klicken Sie in der BitDefender Management-Konsole auf die Option **Berichte**

6.5. Info

Um diese Sektion zu öffnen klicken Sie bitte auf **Info über** im Modul **Allgemein**.

Status aller BitDefender Module

Hier finden Sie eine Übersicht über den Produkt-Status und Kontakt Informationen.

BitDefender stellt Sicherheitslösungen bereit, die den heutigen Anforderungen an sichere Computersysteme gerecht werden. Mit über 41 Millionen Privat- und Unternehmenskunden in mehr als 100 verschiedenen Ländern ist BitDefender eine der meist genutzten Sicherheitslösungen weltweit.

Die Scan-Engine von BitDefender™ist von unabhängigen Instituten wie z.B. - **ICSA Labs**, **CheckMark** und **Virus Bulletin** zertifiziert. BitDefender ist überdies das einzige Sicherheitsprodukt, das eine Auszeichnung (**IST-Prize**) von der Europäischen Kommission erhalten hat.

Weitere Informationen über BitDefender erhalten Sie unter:www.bitdefender.de

7. Das Modul Antivirus

Der Abschnitt **AntiVirus** behandelt und erklärt folgende Themen:

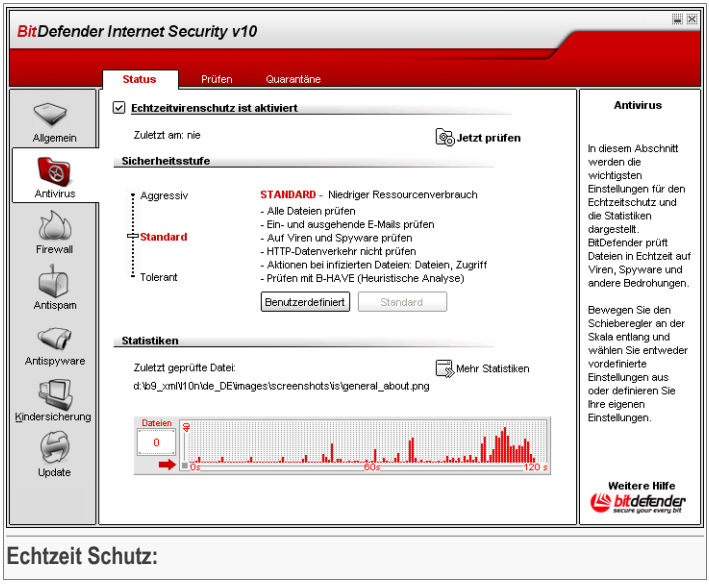
- Bei Zugriff scannen
- Nach Aufforderung prüfen
- Quarantäne

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **AntiVirus** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Antivirus*“ (S. 29).

7.1. On-Access-Scannen

Um diese Sektion zu öffnen klicken Sie bitte auf **Schild** im Modul **Antivirus**.



Echtzeit Schutz:

In diesem Abschnitt können Sie das **Virus Schild** konfigurieren und Informationen über dessen Aktivität einsehen. Das **Virus Schild** schützt alle gängigen Einstiegspunkte auf Ihrem System: E-Mail, Internet- Downloads, Instant Messaging,

Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP-Laufwerke, USB-Speicher).

Wichtig

Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie das **Virus Schild** immer aktiviert.

Am unteren Ende dieser Registerkarte sehen Sie die **Virus Schild**-Statistik über Dateien und E-Mail-Nachrichten. Klicken Sie auf **Mehr Statistiken**, wenn Sie mehr Informationen erhalten wollen.

7.1.1. Sicherheitseinstellung

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

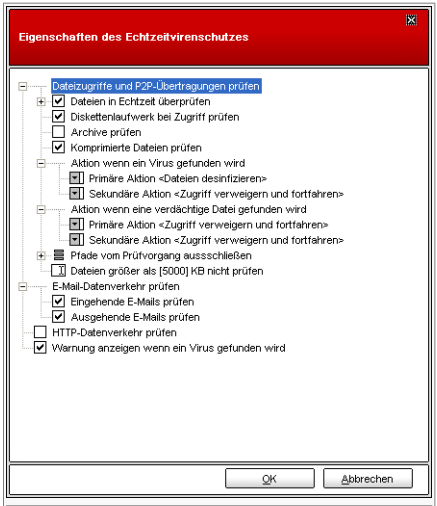
Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Zulassen	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. Programme und eingehende Nachrichten werden nur auf Viren hin geprüft. Neben den klassischen Signatur basierten Scans werden außerdem Heuristische Scans eingesetzt. Bei infizierten Dateien können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.
Standardeinstellung	Gewährleistet Standard Sicherheit. Belsatung der Ressourcen ist gering. Alle eingehenden und ausgehenden Nachrichten werden auf Viren und Spyware geprüft. Sowohl mit Hilfe des klassischen Scans als auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.
Aggressiv	Gewährleistet hohe Sicherheit. Mittlere Belastung der Ressourcen. Alle eingehenden und ausgehenden Nachrichten werden auf Viren und Spyware geprüft. Sowohl mit Hilfe des klassischen Scans als auch der Heuristik. Bie infizierten Dateinen können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von BitDefender genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden.

So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Sie können das Level für den gewünschten Schutz einstellen. Klicken Sie **Level anpassen**. Das folgende Fenster öffnet sich:



Einstellungen des Virus Schild

Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Sie können sehen, dass sich einige Prüfoptionen nicht öffnen lassen, obwohl das "+"- Zeichen sichtbar ist. Der Grund dafür ist, dass diese Optionen bisher nicht gewählt worden sind. Wenn Sie diese Optionen auswählen, können sie geöffnet werden.

- **Dateizugriffe und P2P-Übertragungen prüfen** - um alle Dateien und die Kommunikation mit Instant Messengers (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) zu überprüfen. Des Weiteren wählen Sie eine Datei aus, die Sie prüfen möchten.

Option		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm;

Option		Beschreibung
		.pdf; .msi; .ini; .csc; .cmd; .bas; .eml und .nws.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Auf Spyware prüfen	Sucht nach möglichen Spyware-Anwendungen. Entsprechende Riskware-Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist. Wählen Sie **Dialer und Anwendungen vom Scan ausschließen**, wenn Sie diese Dateien vom Scan ausschließen wollen.
Arbeitsspeicher prüfen		Scanned das CD Laufwerk auf Zugriff.
Archive prüfen		Auch der Inhalt von Archiven wird geprüft. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Komprimierte Dateien prüfen		Alle komprimierten Dateien werden überprüft.
Direktverbindung		Nun können Sie eine der folgenden Möglichkeiten auswählen:
	Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei säubern	Um die infizierte Datei zu desinfizieren.
	Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.
Aktionsoptionen		**Zweite Aktion, falls die erste fehlschlägt** - Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.

Option		Beschreibung
	Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.
Dateien größer als (x) nicht prüfen		**Dateien größer als [x] nicht prüfen** - geben Sie die maximale Größe der zu prüfenden Datei ein. Falls die Größe 0 Kb ist, werden alle Dateien geprüft.
Erweiterungen ausschließen		**Pfade nicht prüfen** - Klicken Sie auf "+" um einen Ordner auszuwählen, der nicht geprüft werden soll. Die Konsequenz ist, dass die Option ausgeweitet wird und `Neues Objekt` erscheint. Klicken Sie auf die dazu gehörende Box und wählen Sie aus dem Fenster die Datei aus, die nicht geprüft werden soll. Die hier ausgewählten Objekte werden vom Scan ausgeschlossen, unabhängig vom festgelegten Schutz Level. (nur für **Anpassen Level**).

- **E-Mails prüfen** - prüft alle E-Mail-Nachrichten.

  Folgende Optionen stehen zur Verfügung:

Option	Beschreibung
Eingehende E-Mails prüfen	Prüft alle eingehenden E-Mails und deren Attachments.
Ausgehende E-Mails prüfen	Prüft alle ausgehenden E-Mails.

- **HTTP Datenverkehr prüfen** - prüft HTTP Datenverkehr.
- **Warnen wenn ein Virus entdeckt wurde** - zeigt eine Warnmeldung an, wenn ein Virus in einer Datei oder E-Mail gefunden wurde.

  Ist eine Datei infiziert wird eine Warnmeldung ausgegeben, die Hinweise über die Art des Schädlings beinhaltet. Bei infizierten E-Mails erhält der Empfänger eine

Nachricht mit Hinweisen über die Art des Schädlings und Informationen über den Absender der Nachricht.

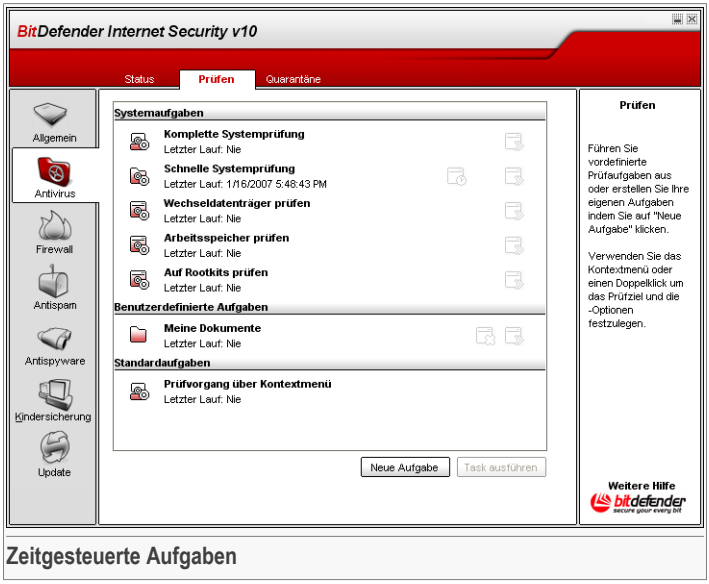
Im Falle eines Verdachts kann ein Assistent aufgerufen werden der Ihnen dabei hilft, verdächtige Dateien zur weiteren Analyse an das BitDefender Virus Labor zu senden. Optional können Sie Ihre E-Mail-Adresse angeben, um weitere Informationen zur Analyse zu erhalten.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn Sie zu den Standardeinstellungen zurückkehren wollen, klicken Sie auf **Standardeinstellung**.

7.2. On-Demand-Scannen

Um diese Sektion zu öffnen klicken Sie bitte auf **Prüfen** im Modul **Antivirus**.



Zeitgesteuerte Aufgaben

In diesem Fenster können Sie die BitDefender Einstellungen zur Prüfung Ihres Computers vornehmen.

Die Aufgabe der BitDefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird in erster Linie erreicht, indem Ihre E-Mail-Anhänge und

Downloads überprüft und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie BitDefender installieren. Deshalb sollten Sie Ihren Computer nach der Installation von BitDefender auf residente Viren prüfen. Übrigens sollten Sie Ihren Computer auch in Zukunft häufig auf Viren prüfen.

7.2.1. Zeitgesteuerte Aufgaben

Der On-Demand Scan richtet sich nach den Prüfoptionen. Der Anwender kann mit Hilfe der Standardeinstellungen oder eigenen Prüfoptionen den Scan durchführen.

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

- **System Einstellungen** - Enthält eine Liste von standard Systemeinstellungen. Die folgenen Einstellungen sind möglich:

Standard Einstellungen	Beschreibung
Tiefgehende Systemprüfung	Prüft alle vorhandenen Dateien auf Viren und Spyware.
Prüfen des gesamten Systems	Prüft alle vorhandenen Dateien mit Ausnahme von Archiven auf Viren und Spyware.
Schnelle Systemprüfung	Prüft alle Programmdateien auf Viren und Spyware.
Prüfen von Wechsellaufwerken	Prüft Wechsellaufwerke auf Viren und Spyware.
Arbeitsspeicher überprüfen	Überprüft den Arbeitsspeicher auf bekannte Malware.
Auf Rootkits prüfen	Prüft Speicher auf getarnte Malware.

- **Anwender Tasks** - enthält die Anwender definierten Tasks.

  Prüfoption `Meine Dokumente`. Nutzen Sie diese Prüfoption, um Ihre Dokumente im Verzeichnis `Meine Dokumente` zu prüfen.

- **Verschiedene Prüfoptionen** - enthält eine Liste verschiedener Prüfoptionen. Diese Optionen weisen auf andere Prüfoptionen hin, die in diesem Fenster nicht ausgeführt werden können. Sie können nur die Einstellungen ändern oder die Prüfberichte ansehen.

Drei Schaltflächen sind verfügbar:

- **Tasks planen** - zeigt an, dass die ausgewählte Aufgabe für später geplant ist. Klicken Sie **Geplante Tasks** - zeigt an, dass die ausgewählte Task zu einem späteren Zeitpunkt geplant ist. Klicken Sie auf Planer im Abschnitt **Eigenschaften** In diesem Fenster können Sie die Einstellungen ändern.
- **Löschen** - löscht die ausgewählte Aufgabe.

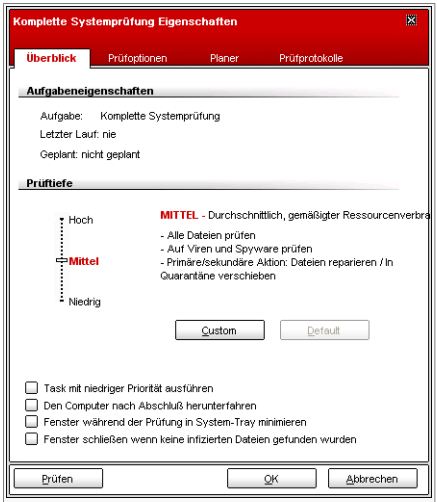
Anmerkung
Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus, indem ein immediate scan durchgeführt wird.

7.2.2. Eigenschaften der Prüfoptionen.

Jede Prüfung hat ihre eigenen **Eigenschaften** ein Fenster indem Sie die prüfoptionen konfigurieren können, das Ziel der Prüfung festlegen,die Tasks planen oder die Berichte ansehen. Öffnen Sie das Fenster mit einem Doppelklick. Das folgende Fenster erscheint:

Auswahlfenster Einstellungen



Auswahlfenster Einstellungen

Hier finden Sie Informationen über Aufgaben (Name, letzte Prüfung und geplante Tasks) und können die Prüfeinstellungen setzen.

Prüflevel

Sie müssen zunächst das Level der Prüfung einstellen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie das gewünschte Level erreicht haben.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Niedrig	Bietet ausreichende Entdeckung. Belastung der Ressourcen ist niedrig. Die Programme werden nur auf Viren hin geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel.

Sicherheitseinstellung	Beschreibung
	Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.
Hoch	Bietet eine hohe Entdeckung. Belastung der Ressourcen ist hoch. Alle Dateien und Archive werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt. Sie können im Falle von infizierten Dateien wählen: Datei reparieren/in Quarantäne verschieben.

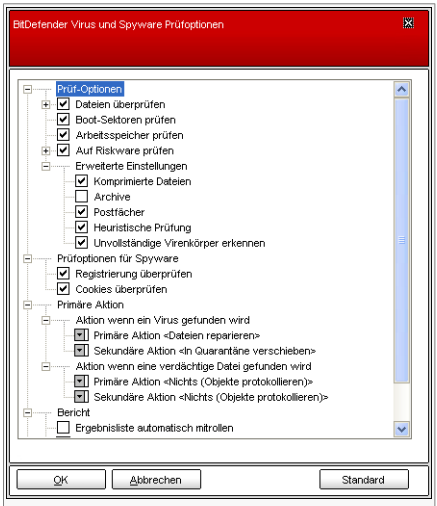
Wichtig

Auf Rootkits prüfen beinhaltet dieselbe Prüftiefe, jedoch gibt es unterschiedliche Optionen:

- **Niedrig** - Es werden nur Prozesse überprüft und bei Erkennung wird keine Aktion durchgeführt.
- **Mittel** - Dateien und Prozesse werden überprüft, es wird nach versteckten Objekten gesucht und bei Erkennung wird keine Aktion durchgeführt.
- **Hoch** - Dateien und Prozesse werden überprüft, es wird nach versteckten Objekten gesucht und bei Erkennung werden diese umbenannt.

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von BitDefender genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Anpassen - um Ihre eigenen Prüfoptionen zu setzen. Das folgende Fenster öffnet sich:



Auswahlfenster Einstellungen

Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Die Prüfoptionen sind in fünf Kategorien unterteilt:

- **Virus Prüfoptionen**
- **Spyware Prüfoptionen**
- **Aktionsoptionen**
- **Berichtoptionen**
- **Weitere Optionen**

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Wichtig

Für den **Auf Rootkits prüfen** Task sind drei Kategorien verfügbar: **Rootkit Prüfoptionen**, **Berichtsoptionen** und **Weitere Optionen**. In der ersten Kategorie können Sie wählen was geprüft werden soll (Dateien, Arbeitsspeicher, oder beides) und welche Aktion bei Erkennung durchgeführt werden soll (Keine (nur protokollieren) oder Umbenennen). Die letzten beiden Kategroien sind identisch mit den unten beschriebenen.

- Geben Sie an, welche Arten von Objekte geprüft werden sollen (Archiv, Postfächer, etc.). Weitere Optionen können über die Kategorie **Virus Prüfoptionen** angegeben werden.

Option		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` und `nws`.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
	Folgende Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Boot-Sektoren prüfen		Prüft die Bootsektoren des Systems.
Speicher prüfen		Prüft den Speicher auf Viren und andere Malware.
Auf Riskware prüfen		Sucht neben Viren ebenfalls nach anderen Bedrohungen wie Dialern und Adware. Entsprechende Riskware-Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist. Wählen Sie **Anwendungen und Dialer ausschließen**, wenn Sie diese Dateien von der Prüfung ausschließen wollen.
Erweiterte Prüfoptionen	**Komprimierte Dateien**	Alle komprimierten Dateien werden überprüft.
	Archive	Prüft den Inhalt von eingepackten Archiven.
	Postfächer	Prüft den Inhalt von E-Mails und deren Attachments.
	Heuristische Prüfung	Aktiviert den heuristischen Suchmodus. Mittels Heuristik können bisher unbekannte Viren auf

Option	Beschreibung
	Grundlage bestimmter Aktionsmuster und Verhaltensweisen, entdeckt werden. Dabei kann es auch zu Fehlalarmen kommen. Sollte eine verdächtige Datei auf Ihrem System gefunden werden, empfehlen wir, die Datei zur Überprüfung an das BitDefender-Virus-Labor zu schicken.
Unvollständige Virenkörper	Spürt unvollständige Virenkörper auf.

- Legt das Ziel für einen Spyware-Prüfvorgang fest (laufende Prozesse, Cookies und/oder Arbeitsspeicher). Weitere Optionen können über die Kategorie **Spyware Prüfoptionen** angegeben werden.

Option	Beschreibung
Systemregistrierung prüfen	Prüft Einträge in der Systemregistrierung.
Cookies prüfen	Prüft gespeicherte Cookies von Webseiten.

- Wählen Sie die Aktionen für infizierte und verdächtige Dateien aus. Öffnen Sie die **Aktionsoptionen**, um alle möglichen Aktionen für diese Dateien anzeigen zu lassen.

  Wählen Sie die Aktion, die durchzuführen ist, wenn eine infizierte oder verdächtige Datei gefunden wird. Sie können unterschiedliche Vorgehensweisen für infizierte und verdächtige Dateien festlegen. Sie können außerdem eine sekundäre Aktion festlegen, wenn die Primäre fehlschlägt.

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne Isolieren oder Löschen.
Dateien reparieren	Um die infizierte Datei zu desinfizieren.
Dateien löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.

Aktion	Beschreibung
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.
Dateien umbenennen	Die infizierte Datei wird umbenannt. Die neue Erweiterung der infizierten Dateien wird `.vir` sein. Durch die Umbenennung von infizierten Dateien ist es nicht länger möglich, diese Dateien auszuführen, um somit eine weitere Verbreitung zu verhindern. Außerdem kann die Datei für weitere Analysezwecke gespeichert werden.

Wichtig

Umbenennen hat denselben Effekt auf versteckte Objekte (Rootkits). Die neue Erweiterung der Datei lautetnach diesem Vorgang `.bd.ren`. Durch die Umbenennung erkannter Dateien wird die Möglichkeit einer Ausführung reduziert und die Verbreitung im Betriebssystem reduziert. Des weiteren kann die Datei für weitere Analysen abgespeichert werden.

- Optionen für Berichtsdateien angeben. Öffnen Sie die **Berichtsoptionen** um alle möglichen Optionen anzeigen zu lassen.

Option	Beschreibung
Alle geprüften Objekte anzeigen	Zeigt in einer Berichtdatei den Status und mögliche Infektionen aller geprüften Dateien an. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Berichte älter als (x) Tage löschen	In diesem Feld können Sie festlegen (wo möglich) wie lange ein Bericht gespeichert (erinnert, abgelegt, hinterlegt) werden soll Scan Logs section. Wählen Sie diese Option und geben Sie ein neues Zeitintervall ein. Die Standardeinstellung ist 180 Tage.

Anmerkung

Die Berichtsdatei kann im Abschnitt Berichte im Menüpunkt **Eigenschaften** eingesehen werden.

- Festlegen weiterer Optionen. Öffnen Sie den Abschnitt **Erweitert**, um folgende Optionen auszuwählen:

Option	Beschreibung
Versenden verdächtiger Dateien an das BitDefender Labor	Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

Andere Optionen

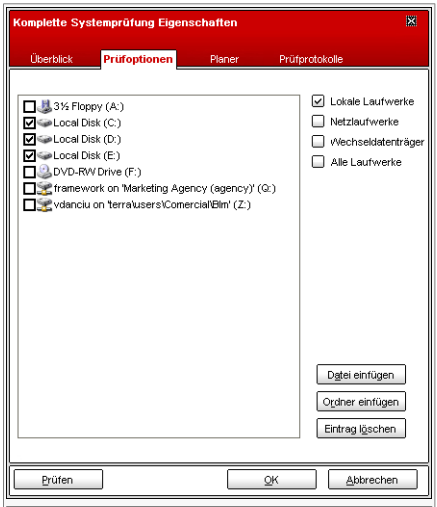
Eine Reihe von allgemeinen Optionen für den Prüfvorgang stehen ebenfalls zur Verfügung:

Option	Beschreibung
Aufgaben mit niedriger Priorität ausführen	Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
Herunterfahren des Computers nach erfolgtem Prüfvorgang	Der Rechner wird nach erfolgtem Prüfvorgang ausgeschaltet.
Versenden verdächtiger Dateien an das BitDefender Labor	Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.
Minimieren des Prüffensters beim Scan-Start	Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das BitDefender – Logo in der Symbolleiste wieder geöffnet werden.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüfen der Zielobjekte

Klicken Sie auf die ausgewählte Aufgabe und dann auf den Reiter **Prüfpfad** um in diesen Abschnitt zu kommen.



Prüfen der Zielobjekte

Hier können Sie den Prüfpfad festlegen.

Dieser Bereich enthält folgende Schaltflächen:

- **Datei hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen bestimmter, zu prüfender Dateien. Wenn Sie hierauf klicken, können Sie die Dateien im nächsten sich öffnenden Fenster auswählen.
- **Ordner hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen eines neuen, zu prüfenden Ordners. Wenn Sie hierauf klicken, können Sie den Ordner im nächsten, sich öffnenden Fenster auswählen.

Anmerkung

Ziehen Sie per Drag & Drop Dateien und Ordner auf die Prüfen-Sektion, um diese der Liste der zu prüfenden Objekte zuzufügen.

- **Eintrag löschen** - löscht die Datei/denOrdner, die/der vorher ausgewählt wurde.

Anmerkung

Nur die Dateien/Ordner, die nachträglich hinzugefügt wurden, können gelöscht werden. Dateien/Ordner, die von BitDefender vorgegeben wurden, können nicht gelöscht werden.

Optionen, die das schnelle Auswählen der Scan-Ziele erlauben.

- **Lokale Laufwerke** - prüft die lokalen Laufwerke.
- **Netzlaufwerke** - prüft die verfügbaren Netzwerklaufwerke.
- **Wechseldatenträger** - prüft alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke, USB-Sticks).
- **Alle Laufwerke** - prüft alle Laufwerke: lokale, entfernbare oder verfügbare Netzwerklaufwerke.

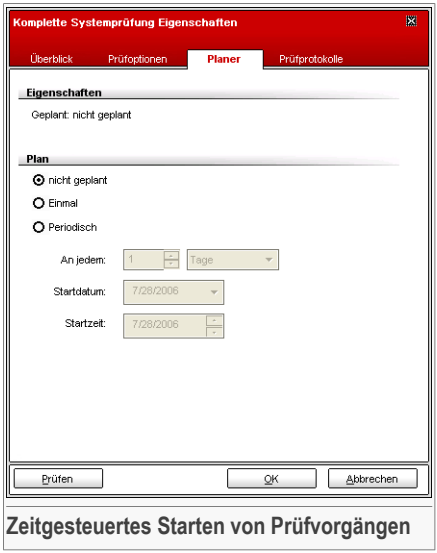
Anmerkung

Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Zeitgesteuertes Starten von Prüfvorgängen

Über den Abschnitt **Zeitgesteuerte Aufgaben** können Sie beliebige Zeiten für den Scanvorgang festlegen.



Zeitgesteuertes Starten von Prüfvorgängen

Hier können Sie nachsehen, ob eine Aufgabe geplant ist oder nicht und Sie können die Eigenschaften ändern.

Wichtig

Während umfassender Prüfungen kann der Prüfprozess eingige Zeit in Anspruch nehmen und läuft reibungslos, wenn Sei währenddessen alle anderen Programme schließen. Aus diesem Grunde ist es ratsam die Prüfvorgänge zu planen, wenn Sie Ihren Computer nicht nutzen oder er im Standby Modus ist.

Wenn Sie Prüfvorgänge planen müssen Sie eine der folgenden Optionen auswählen:

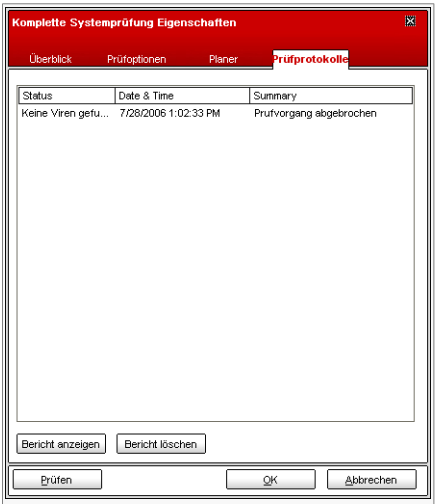
- **nicht geplant** - führt den Scan nur auf Anfrage des Nutzers hin durch.
- **Einmal** - führt den Scan nur einmal, zu einem bestimmten Zeitpunkt aus. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.
- **Periodisch** - startet den Prüfvorgang in festgelegten Zeitabständen (Stunden, Tage, Wochen, Monate, Jahre) beginnend mit einem fest definierten Zeitpunkt (Datum und Uhrzeit).

  Wenn der Scanvorgang nach einem bestimmten Zeitraum wiederholt werden soll, aktivieren Sie das Kontrollkästchen **Regelmäßig**, und geben Sie in das Textfeld **Alle** die entsprechende Anzahl von Minuten/Stunden/Tage/Wochen/Monate/Jahre ein, nach der die Wiederholung erfolgen soll. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

Prüfberichte

Klicken Sie auf due ausgewählte Aufgabe und wählen Sie **Berichtsdateien** um in diesen Abschnitt zu gelangen.



Prüfberichte

Hier können Sie nach jeder durchgeführten Prüfung die Berichtsdateien einsehen. Jede Datei beinhaltet Informationen über den Status (sauber/infiziert), das Datum und die Zeit wann die Prüfung durchgeführt wurde und eine Zusammenfassung (Prüfung beendet).

Zwei Schaltflächen sind verfügbar:

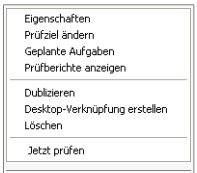
- **Anzeigen** - öffnet die ausgewählte Berichtsdatei;
- **Löschen** - löscht die ausgewählte Berichtsdatei;

Sie könne auch um eine Datei anzusehen oder zu löschen einfach mit einem rechten Mausklick die entsprechende Option aus dem Shortcut Menu auswählen.

Klicken Sie auf **OK** um die Änderungen zu speichern und das Fenster zu schließen. Wenn Sie auf **Prüfen** klicken wird die Prüfung ausgeführt.

7.2.3. Shortcut Menü

Für jede Aufgabe steht ein Shortcut Menü zur Verfügung. Mit einem rechten MAusklick könne Sie die ausgewählte Aufgabe öffnen:



Shortcut Menü

Folgende Aktionen stehen zur Verfügung:

- **Eigenschaften** - öffnet das Fenster **Eigenschaften**, **Übersicht** tab, wo Sie die Einstellungen für die ausgewählte Aufgabe ändern können;
- **Zielprüfung ändern** - öffnet **Eigenschaften** Fenster, **Prüfpfad** tab, wo Sie das Prüfziel für die ausgewählte Aufgabe ändern können.
- **Planen** - öffnet das Fenster **Eigenschaften** , **Planer**, wo Sie die ausgewählten Aufgaben planen können;
- **Prüfberichte anzeigen** - öffnet das Fenster **Eigenschaften** , **Prüfberichte**, wo Sie die Berichte sehen, die nach der Prüfung erstellt wurden.
- **Wiederholen** - wiederholt die ausgewählte Aufgabe.

Anmerkung

Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.

- **Shortcut auf den Desktop** - Erstellt einen Shortcut zum Desktop über die ausgewählte Aufgabe.
- **Löschen** - löscht die ausgewählte Aufgabe.

Anmerkung

Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **jetzt prüfen** - führt die ausgewählte Aufgabe aus und startet eine sofortige Prüfung.

Wichtig

Aufgrund ihrer speziellen Beschaffenheit können nur die Optionen **Eigenschaften** und **Berichtsdateien ansehen** unter dem Punkt **Verschiedene Aufgaben** ausgewählt werden.

7.2.4. On-Demand-Scanner.

BitDefender bietet drei verschiedene On-Demand-Scan-Typen:

- Sofortiges prüfen - folgen Sie den unten angegebenen Schritten, um Ihren Computer auf Viren zu prüfen;
- Kontextbezogenes Prüfen - Rechtsklick auf eine Datei oder einen Ordner und wählen Sie im Kontextmenü BitDefender AntiVirus v10 aus;
- Prüfen per Drag& Drop - verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitäts-Anzeige;

Sofortiges Scannen

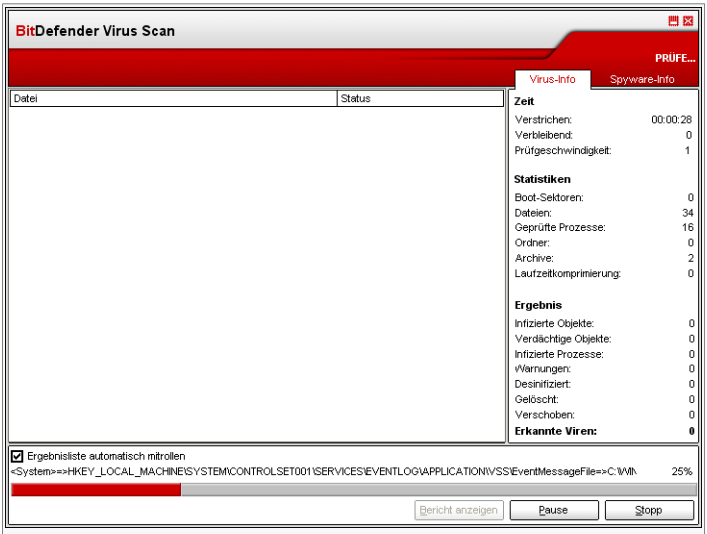
Um Ihren Computer oder Teile Ihres Computers zu prüfen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben einrichten. Es gibt zwei Möglichkeiten Aufgaben einzurichten:

- Wiederholen einer existierenden Regel, neu benennen und machen Sie die nötigen Änderungen im Fenster Eigenschaften;
- Klicken Sie unter **Neue Aufgaben** auf Konfigurieren,.

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

Da es täglich neue Bedrohungen durch Viren und Würmer gibt, sollten Sie, bevor Sie den Suchlauf starten, BitDefender mit Hilfe des Update Moduls aktualisieren.

Um die Prüfung zu starten wählen Sie die gewünschten Prüfaufgaben aus der Liste aus und klicken Sie **Jetzt prüfen** auf dem rechten Button. Sie könne auch auf den Button **Aufgabe ausführen** klicken. Das Prüffenster wird dann geöffnet:



Prüffenster

Es wird ein Symbol in der Symbolleiste angezeigt, wenn ein Prüfvorgang aktiv ist.

Während des Prüfvorgangs wird BitDefender den Fortschritt anzeigen und Sie benachrichtigen, wenn Bedrohungen gefunden wurden. Auf der rechten Seite können Sie die Statistiken des Prüfvorgangs sehen. Abhängig von der ausgewählten Prüf-Option (Spyware oder Viren) sind Informationen verfügbar. Wenn beide Optionen verfügbar sind wählen Sie die dementsprechenden Informationen aus um mehr über den Prüfvorgang nach Spyware oder Viren zu erfahren.

Wählen Sie die Checkbox **Zuletzt geprüfte Dateien anzeigen** und Sie sehen nur Informationen über die zuletzt geprüften Dateien.

Anmerkung

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Drei Schaltflächen sind verfügbar:

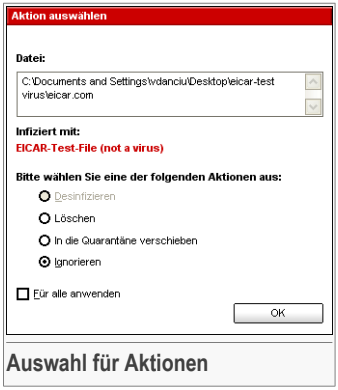
- **Stopp** - Ein neues Fenster öffnet sich und Sie werden gefragt, ob Sie die Systemprüfung stoppen möchten. Klicken Sie auf **Ja**&**Schließen**, um das Fenster und den Prüfvorgang zu schließen.

- **Pause** - Hält den Prüfvorgang für eine bestimmte Zeit an; klicken Sie auf **Fortsetzen**, um ihn wieder zu starten.
- **Bericht anzeigen** - Der Prüfbericht wird geöffnet und die zurzeit überprüften Dateien werden laufend angezeigt.

Anmerkung

Mit einem rechten Mausklick auf eine laufende Aufgabe, einen Shortcut (kontext) Menü erscheint das Prüffenster. Die Optionen (**Pause / Fortsetzen**, **Stop** und **Stoppen und schließen**)sind den Buttons des Prüffensters ähnlich.

Wenn die Einstellung **Eingabeaufforderung** eingestellt ist im Fenster Properties , wird ein Fenster geöffnet, in dem Sie aufgefordert werden die Aktion auszuwählen, die im Falle einer infizierten Datei ausgeführt werden soll.



Auswahl für Aktionen

Sie sehen den Namen der Datei und den Namen des Virus.

Nun können Sie eine der folgenden Möglichkeiten auswählen:

- **Desinfizieren** - reinigt die infizierten Dateien;
- **Löschen** - löscht automatisch alle infizierten Dateien, ohne eine Warnmeldung auszugeben;
- **In Quarantäne verschieben** - verschiebt die infizierten Dateien in die Quarantäne;
- **Ignorieren** - In diesem Fall wird die Infizierung ignoriert und keine Aktion ausgeführt.

Wenn Sie einen gesamten Ordner überprüfen und die ausgewählte Aktion auf alle gefundenen Schädlinge übertragen möchten, so wählen Sie bitte die Option **Für alle anwenden**.

Anmerkung

Ist die Option **Desinfizieren** nicht verfügbar, so bedeutet dies, das die Datei nicht desinfiziert werden kann. Die beste Alternative ist, die Datei in der Quarantäne zu isolieren und diese später zwecks Analyse an das Virenlabor zu senden.

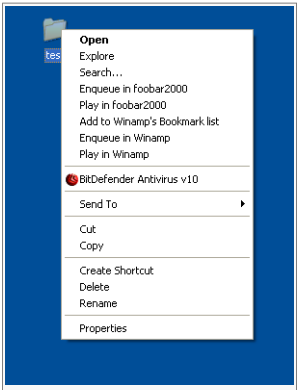
Klicken Sie auf **OK**.

Anmerkung

Die Berichtsdatei wird automatisch im Abschnitt Berichte im Menüpunkt **AntiVirus** gesichert.

Scannen mit dem Kontextmenü

Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei. Wählen Sie **BitDefender Antivirus v10** aus.

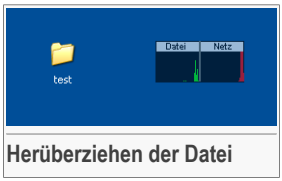


Kontextmenü

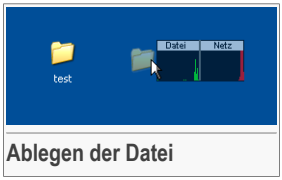
Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster Eigenschaften auf **Prüfen Kontext Menü** klicken.

Prüfen per Drag & Drop

Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.



Herüberziehen der Datei



Ablegen der Datei

Wenn eine infizierte Datei entdeckkt wurde erscheint ein Alarm Fenster und fragt welche Aktion durchgeführt werden soll.

In beiden möglichen Prüfalternativen (Kontext Menü und drag&drop) erscheint Prüffenster .

7.2.5. Prüfen auf Rootkits

Mit der neu eingeführten Antirootkit-Technologie wird die Effizienz von BitDefender noch einmal gesteigert. Dadurch ist BitDefender nun in der Lage Rootkits aufzuspüren und unschädlich zu machen.

Um Ihren Computer auf Rootkits zu prüfen starten Sie bitte den Task **Auf Rootkits prüfen**. Anschließend erscheint das Prüffenster.

Wichtig

Es wird empfohlen keine Aktion auf versteckte Objekte anzuwenden wenn BitDefender den Computer auf Rootkits überprüft.

Am Ende eines jeden Prüfvorgangs bekommen Sie den Prüfbericht angezeigt. Überprüfen Sie gefundene, versteckte Objekte sorgfältig: Das Vorhandensein von solchen ist eventuell ein Indikator für ein kompromitiertes System.

Wenn Sie sicher sind das es sich bei einer erkannten Datei um Malware handelt, empfehlen wir Ihnen die Aktion auf **Umbenennen** zu stellen und erneut die Aufgabe **Auf Rootkits prüfen** durchzuführen. So stellen Sie sicher, dass die versteckten Dateien unbrauchbar gemacht werden.

Warnung

WARNUNG: NICHT ALLE VERSTECKTEN OBJEKTE SIND MALWARE! Stellen Sie vor dem Umbenennen-Vorgang sicher, dass die jeweiligen Objekte nicht zu einer auf dem Computer installierten, legitimen Anwendung gehören. Ein Umbenennen solch einer Datei kann Ihr System unbrauchbar machen.

Wichtig

Ist ein Computer erst einmal durch ein Rootkit kompromitiert worden, gibt es lediglich eine Lösung um diesen vollständig zu säubern: Eine Neuinstallation des Betriebssystems.

7.3. Quarantäne

Um diese Sektion zu öffnen klicken Sie bitte auf **Quarantäne** im Modul **Antivirus**.

Quarantäne

Mit BitDefender können Sie infizierte oder "verdächtige" Dateien in einem sicheren Bereich, der als Quarantäne bezeichnet wird, isolieren. Durch das Isolieren dieser Dateien in einem Quarantänebereich wird das Infektionsrisiko eliminiert und gleichzeitig können diese Dateien zu weiteren Analysezwecken an das BitDefender Lab gesendet werden.

Der Bestandteil, der die Verwaltung der isolierten Dateien sicherstellt, ist die **Quarantäne**. Dieses Modul enthält eine Funktion, die die infizierten Dateien auf Wunsch automatisch zum BitDefender-Labor sendet.

Wie Sie sicherlich bereits festgestellt haben, enthält der Abschnitt **Quarantäne** eine Liste aller Dateien, die isoliert wurden. Zu jeder Datei sind die folgenden Informationen verfügbar: Name, Dateigröße, Isolationsdatum und Übertragungsdatum. Um weitere Informationen anzuzeigen, klicken Sie bitte auf **Mehr Infos**.

Anmerkung

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

Klicken Sie **Hinzufügen** um eine verdächtige Datei zur Quarantäne hinzuzufügen. Es öffnet sich dann ein Fenster und Sie können die Datei auf dem Laufwerk auswählen. Dann wird die Datei in Quarantäne kopiert. Wenn die Datei in Quarantäne geschoben werden soll wählen Sie **löschen in ursprünglicher Speicherstelle** . Ein schnellerer Weg eine verdächtige Datei zur Quarantäne hinzuzufügen ist drag&drop sie in die Quarantäne.

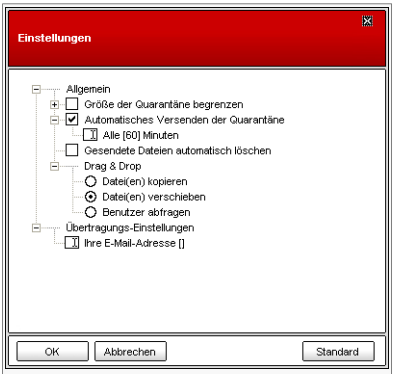
Um eine ausgewählte Datei aus der Quarantäne zu löschen klicken Sie the **entfernen**. Wenn Sie eine infizierte Datei wiederherstellen wollen in ihrem original Speicherort klicken Sie **Wiederherstellen**.

Sie können jede ausgewählte Datei aus der Quarantäne in das BitDefender labor senden in dem Sie **Senden** klicken.

Wichtig

Sie müssen zunächst weitere Informationen angeben, bevor Sie Dateien übertragen. Klicken Sie zunächst auf **Einstellungen** und füllen Sie dort das Feld **E-Mail-Adresse** aus.

Click **Einstellungen** um die erweiterten Optionen für die Quarantäne zu öffnen. Das folgender Fenster erscheint:



Quarantäne-Einstellungen

Die Quarantäne-Einstellungen sind in zwei Kategorien unterteilt:

- **Allgemein**
- **Übertragungs-Einstellungen**

Anmerkung

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Allgemein

- **Größe der Quarantäne begrenzen** - Hält die Größe der Quarantäne unter Kontrolle. Diese Option ist in der Voreinstellung aktiviert und liegt bei 12.000 KB. Wenn Sie diesen Wert ändern möchten, klicken Sie bitte in das Eingabefeld und tragen Sie einen neuen Wert ein. Wenn Sie das Ankreuzfeld **Alte Dateien automatisch löschen** auswählen und das Quarantäne-Verzeichnis die maximale Größe erreicht hat, werden automatisch die ältesten Dateien gelöscht, um den verwendeten Speicherplatz für neuere Dateien freizugeben.
- **Automatisches Versenden der Quarantäne** - sendet automatisch alle Dateien aus dem Quarantäne-Ordner zur Überprüfung an das BitDefender-Virenlabor. Sie können das Intervall bestimmen, in dem der **Inhalt der Quarantäne automatisch versendet wird**.
- **Gesendete Dateien automatisch löschen** - löscht automatisch die aus der Quarantäne gesendeten Dateien.

- **Drag & Drop settings** - für die Drag & Drop-Funktion des Quarantäne-Ordners können Sie hier die Art des Drag & Drop einstellen: Kopieren der Dateien, Verschieben der Dateien, Benutzer abfragen.

Übertragungs-Einstellungen

- **Ihre E-Mail-Adresse** - geben Sie hier Ihre E-Mail-Adresse an, wenn Sie eine Antwort bezüglich der eingesendeten Dateien aus dem Virenlabor haben möchten.

Klicken Sie auf **OK** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

8. Das Modul Firewall

Der Abschnitt **Firewall** behandelt und erklärt folgende Themen:

- Der Regelassistent
- Status der Personal-Firewall
- Firewallregeln
- Erweiterte Einstellungen
- Aktivitätsanzeige

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Personal-Firewall** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Firewall*“ (S. 29).

8.1. Der Regelassistent

Nutzen Sie BitDefender zum ersten Mal, wird Ihnen ein Assistent helfen, die Firewall zu konfigurieren und wichtige Einstellungen bzw. Regeln festzulegen. Diese Regeln sind absolut notwendig für die gängigsten Anwendungen. Das Ergebnis der vorgenommenen Einstellungen ist ein zuverlässig geschützter Computer, ein sicheres E-Mail-Programm und ein geschützter Zugang über Ihren Internet Browser.

Anmerkung

Der Assistent kann jederzeit mit einem Klick auf **Profil Rekonfigurieren** erreicht werden über den Bereich Verkehr .

Wichtig

Wird der Assistenz nicht ordnungsgemäß beendet, wird die Firewall deaktiviert. Der Assistent erscheint dann automatisch, sobald Sie die Firewall aktivieren möchten.

8.1.1. Schritt 1/7 - Willkommensfenster

Begrüßungsfenster

Geben Sie den Namen für das neue Netzwerk Profil ein im Feld **Profil Name**.

Wählen Sie **neues Profil erstellen** um dem Assistenten zu folgen und erstellen Sie eine Reihe von Regeln für die Firewall.

Wenn Sie **Regeln von vorhandenen Profil importieren** wählen, wählen Sie ein Netzwerk Profil von der Liste. Die neue Regel importiert alle Regeln der des ausgwählten Profils. Sie kommen direkt zum letzten Schritt des Assistenten ohne zusätzliche Konfiguration.

Wählen Sie **Allgemeines Profil erstellen und es allen neuen Netzwerkverbindungen zuweisen** um ein allgemeines Profil zu erstellen oder um das bestehende zu überschreiben. Dieses Profil wird jedes mal angewendet sobald BitDefender ein noch unbekanntes Netzwerk erkennt.

Anmerkung

Öffnen Sie bitte den Abschnitt Erweitert im Bereich Firewall und deaktivieren Sie dort den Eintrag **Neu erkannten Netzwerken das allgemeine Profil zuweisen** um dieses Feature zu deaktivieren.

Klicken Sie auf **Weiter**.

8.1.2. Schritt 2/7 – Erweiterte Firewall Einstellungen

Erweiterte Einstellungen

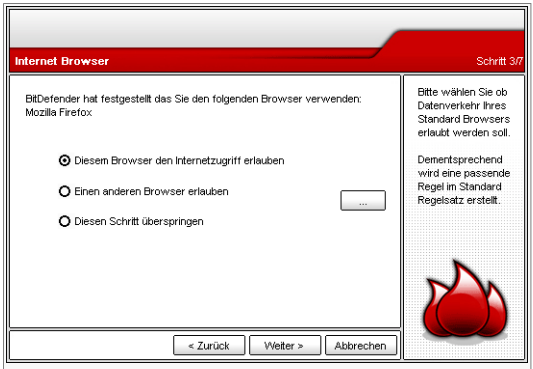
Konfigurieren der erweiterten Firewall Einstellungen des derzeitigen Netzwerk Profiles.

Folgende Optionen stehen zur Verfügung:

Option	Beschreibung
Erlauben	Erlaubt automatisch ausgehende Verbindungsversuche von Programmen, die bei BitDefender als erlaubt bekannt sind. Basierend auf dieser Option werden Regeln, die diese Verbindungen erlauben erstellt in Datenverkehr ohne Ihren Eingriff. Ein Pop-Up Fenster wird Sie informieren, wenn eine solche Regel erstellt wird. Programme mit Freundleslisten sind die am weitesten verbreiteten Programme weltweit. Sie beinhalten die bekanntesten Web Browsers, audio&video Players, Chat und Filesharing Programme, ebenso wie Server Clients und Betriebssystem Anwendungen.
Internet Connection Sharing (ICS)erlauben auf diesem Computer	Erlaubt Ihrem Computer Internet Connection Sharing(ICS)zu unterstützen. Diese Option erlaubt Ihrem Computer nicht automatisch ICS, sondern erlaubt diese Art Verbindung nur, wenn sie dies in Ihrem Betriebssystem eingestellt haben.

Option	Beschreibung
	Internet Connection Sharing (ICS) erlaubt Mitgliedern von lokalen Netzwerken von ihrem Computer aus eine Internetverbindung aufzubauen. Das ist sinnvoll wenn Sie eine spezielle/besondere Internet Verbindung haben (z.B. drahtlose Anbindung) und Sie möchten diese mit anderen Mitgliedern im Netzwerk teilen.

8.1.3. Schritt 3/7 – Internet Browser



Die Browser Optionen

BitDefender erkennt den von Ihren ausgewählten Internet–Browser vollautomatisch. Wählen Sie bitte, ob der Netzwerk- bzw. Internetdatenaustausch über den von Ihnen gewählten Browser erfolgen soll, oder ob Sie einen anderen Browser verwenden möchten.

Wichtig

Falls Sie sich entscheiden, diesen Schritt zu überspringen, werden die Einstellungen in diesem Fenster nicht vorgenommen. Sie müssen diese Regeln dann eigenständig erstellen. Bitte überspringen Sie diesen Schritt nicht, wenn Sie sich nicht sicher sind, ob Sie die notwendigen Regeln selber erstellen können.

Klicken Sie auf **Weiter**.

8.1.4. Schritt 4/7 – E-Mail-Programm

E-Mail-Programm Optionen

BitDefender erkennt Ihr ausgewähltes E-Mail-Programm. Wählen Sie bitte, ob der Netzwerk- bzw. Internetdatenaustausch über das von Ihnen gewählte E-Mail-Programm erfolgen soll, oder ob Sie einen anderen Client verwenden möchten.

Wichtig

Falls Sie sich entscheiden, diesen Schritt zu überspringen, werden die Einstellungen in diesem Fenster nicht vorgenommen. Sie müssen diese Regeln dann eigenständig erstellen. Bitte überspringen Sie diesen Schritt nicht, wenn Sie sich nicht sicher sind, ob Sie die notwendigen Regeln selber erstellen können.

Klicken Sie auf **Weiter**.

8.1.5. Schritt 5/7 – Proxy-Server

Proxy Server Optionen

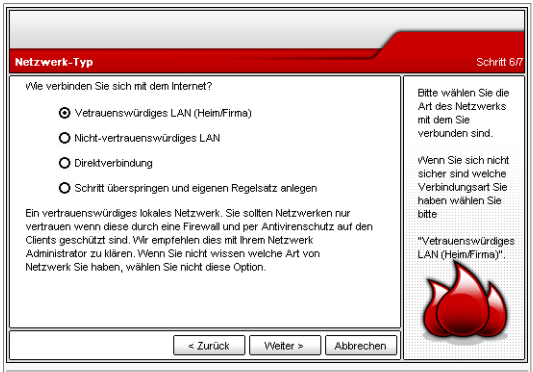
Falls Sie einen Proxy-Server zum Verbindungsaufbau zum Internet verwenden, wird BitDefender dies automatisch erkennen. Bitte wählen Sie, ob der Datentransfer über das Internet/Netzwerk über den Proxy-Server generell erlaubt werden soll oder klicken Sie . . . analog zu **Ich nutze einen anderen Proxy Server** und geben Sie die Proxy Server IP Adresse und den Port ein.

Wichtig

Falls Sie sich entscheiden, diesen Schritt zu überspringen, werden die Einstellungen in diesem Fenster nicht vorgenommen. Sie müssen diese Regeln dann eigenständig erstellen. Bitte überspringen Sie diesen Schritt nicht, wenn Sie sich nicht sicher sind, ob Sie die notwendigen Regeln selber erstellen können.

Klicken Sie auf **Weiter**.

8.1.6. Schritt 6/7 - Netzwerk-Typ



Netzwerkauswahl

Bitte wählen Sie den verwendeten Netzwerktypen bzw. die Internetverbindung. Die folgenden Optionen stehen Ihnen zur Verfügung:

Option	Beschreibung
Vertrauenswürdiges LAN (Heim/Firma)	Sie sollten nur einer Netzwerkverbindung trauen, die durch eine Firewall und ein Antivirusprogramm geschützt ist. Bitte vergewissern Sie sich bei dem Netzwerkadministrator. Falls Sie nicht wissen, welche Verbindung vorhanden ist, wählen Sie diese Option nicht.
Nicht-vertrauenswürdiges LAN	Wählen Sie diese Verbindung, falls Sie sich als Gast in einem anderen Netzwerk angemeldet haben. Genau dieses Netzwerk darf nicht bei Ihnen zu Hause oder im Büro existieren. Falls Sie nicht wissen, welche Verbindung vorhanden ist, wählen Sie diese Option nicht.
Direktverbindung	Wählen Sie diese Verbindung, falls Sie direkt mit dem Internet verbunden sind, oder wenn Sie nicht genau wissen, welche Verbindung vorhanden ist. Alle eingehenden Verbindungsversuche werden automatisch abgelehnt. Obwohl es dazu führen kann, dass einige Anwendungen ihre Verbindung verlieren, besteht jedoch

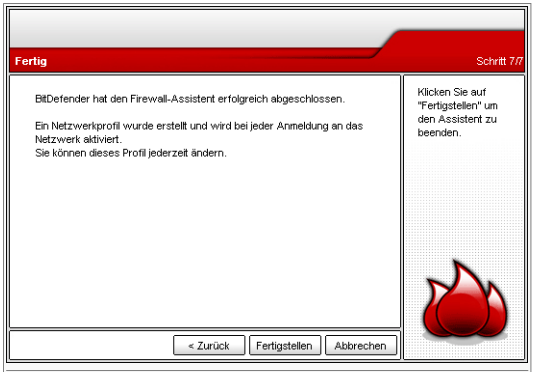
Option	Beschreibung
	der höchst mögliche Grad an Sicherheit. Sie können jedoch einige Regeln so verändern, dass die von Ihnen ausgeführten Anwendungen stabil laufen.

Wichtig

Falls Sie sich entscheiden, diesen Schritt zu überspringen, werden die Einstellungen in diesem Fenster nicht vorgenommen. Sie müssen diese Regeln dann eigenständig erstellen. Bitte überspringen Sie diesen Schritt nicht, wenn Sie sich nicht sicher sind, ob Sie die notwendigen Regeln selber erstellen können.

Klicken Sie auf **Weiter**.

8.1.7. Schritt 7/7 – Übersicht



Übersicht

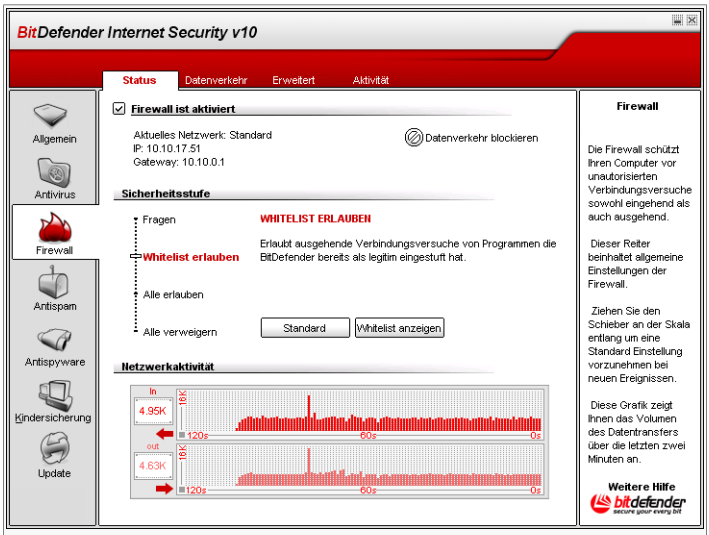
Dies ist der letzte Schritt der Konfigurationsassistenten. Sie können jedoch jegliche Veränderungen vornehmen, in dem Sie zu den vorherigen Schritten zurückkehren (Klicken Sie auf **Zurück**).

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

Sie können den Firewall Assistenten jederzeit erneut aufrufen indem Sie **Profil Rekonfigurieren** klicken im Abschnitt Datenverkehr.

8.2. Status der Firewall

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Firewall**.



Status der Firewall

In diesem Menü können Sie die **Firewall** aktivieren bzw. deaktivieren, den gesamten Netzwerk- und Internetverkehr blockieren und Regeln für neue Ereignisse erstellen.

Wichtig

Um den Schutz vor Angriffen aus dem Internet zu gewährleisten, halten Sie Ihre **Firewall** Funktion jederzeit aktiviert.

Um den Netzwerk/Internet Datenverkehr zu blockieren klicken Sie den Button **Datenverkehr blockieren**.

Im unteren Bereich der Maske können Sie eine Statistik bezüglich des eingehenden und ausgehenden Datentransfers beobachten. Diese Grafik zeigt Ihnen das Volumen des Datentransfers über die letzten zwei Minuten an.

Anmerkung

Diese Grafik erscheint auch bei deaktivierter **Firewall**.

8.2.1. Sicherheitseinstellung

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 4 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Verweigern	**Verweigern** - Verweigert sämtliche Verbindungsversuche für die keine Regel existiert ohne weitere Nachfrage. Verwenden Sie diese Richtlinie nur wenn Sie bereits für alle Programme eine Regel erstellt haben.
Erlauben	**Erlauben** - Erlaubt sämtliche Verbindungsversuche, für die keine Regel existiert ohne weitere Nachfrage. Es wird nicht empfohlen diese Richtlinie zu verwenden.
Erlauben	Erlaubt alle ausgehenden Verbindungsversuche von Programmen, die von BitDefender als erlaubt eingestuft werden. Sie können die Regeln sehen wie Sie in dem Abschnitt Datenverkehr stehen. Programme mit Freundleslisten sind die am weitesten verbreiteten Programme weltweit. Sie beinhalten die bekanntesten Web Browsers, audio&video Players, Chat und Filesharing Programme, ebenso wie Server Clients und Betriebssystem Anwendungen.
Fragen	**Fragen** - Existiert keine Regel für einen Verbindungsversuch, so erhalten Sie eine Abfrage, um eine neue Regel zu erstellen. Dies ist die Standard-Richtlinie.

Wichtig

Falls das Menü für die Management Konsole bereits geschlossen ist, und keine Regeln für neue Ereignisse definiert wurden, wird jede Aktion grundsätzlich **Verweigern**.

Klicken Sie **Standardeinstellung** um die Standard Regel (**Alle Einträge der Freundesliste erlauben**).

Sollen keine Änderungen durchgeführt werden, klicken Sie auf **Fertigstellen**.

8.3. Firewall Regeln

Um diese Sektion zu Öffnen klicken Sie bitte auf **Regeln** im Modul **Firewall**.

Firewall Regeln

Legen Sie selbst genau fest, welchen Programmen es erlaubt ist, über das Internet Daten zu verschicken. Definieren Sie eigene Regeln für den Datenverkehr mit dem Internet (Protokolle, Ports, Programme oder Adressen auf fremden Rechnern), oder nutzen Sie den Wizzard um alle nötigen Regeln automatisch zu erstellen.

Verwenden Sie die Checkbox **System-Prozesse verbergen** um Anwendungen des Betriebssystems und von BitDefender nicht anzeigen zu lassen.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

8.3.1. Regeln automatisch hinzufügen

Falls ein neues Programm eine Verbindung zum Internet aufbauen will, müssen Sie zunächst die BitDefender Fragen zu diesem Programm beantworten. Danach werden die Regeln zum Regelwerk hinzugefügt.

Bei aktivierter **Firewall** fragt BitDefender bei jedem Verbindungsaufbau zum Internet ab, ob diese zugelassen werden soll:

Firewall Alarm

Hier wird folgendes dargestellt: die Anwendung versucht eine Verbindung zum Internet aufzubauen. Es wird dokumentiert, um welchen Port, Protokoll und IP Adresse es sich handelt.

Bitte verwenden Sie die Funktion **Zugriff** und wählen Sie die gewünschte **Aktion** aus dem Aufklappmenü und klicken Sie **OK**. Nun wird die selektierte Einstellung wirksam und entsprechend im Regelwerk dokumentiert. Danach werden Sie bei Wiederholung dieses Vorganges nicht mehr benachrichtigt.

Folgende Optionen sind wählbar:

Aktion	Beschreibung
Erlauben	Zulassen des Datenverkehrs mit dieser Anwendung und dem entsprechenden Protokoll.
Verweigern	Blockieren des Datenverkehrs mit dieser Anwendung und dem entsprechenden Protokoll.
Erlauben des Datenverkehrs mit dieser Anwendung	Zulassen des Datenverkehrs mit dieser Anwendung über alle IP Protokolle.
Verweigern des Datenverkehrs mit dieser Anwendung	Blockieren des Datenverkehrs mit dieser Anwendung über alle IP Adressen.
Nur diesen Anbieter erlauben	Zulassen des Datenverkehrs über diesen spezifischen Datenbankanbieter und einem speziellen Protokoll.
Nur diesen Port erlauben	Zulassen des Datenverkehrs über ein spezifisches Protokoll und einem speziellen Port für jede Zieladresse.
Entfernten Host verweigern	Verweigern des Datenbankverkehrs über ein spezifisches Protokoll und dem entfernten Host.

Aktion	Beschreibung
Diesen Port verweigern	Verweigern des Datenbankverkehrs über ein spezifisches Protokoll und einem definierten Port für alle Zieladressen.

Wichtig

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

Jede Regel, die einmal definiert wurde, kann über das Menü **Regeln** aufgerufen und entsprechenden modifiziert werden.

Wichtig

Die Regeln sind gemäß ihrer Priorität von oben beginnend gelistet. Dies bedeutet, die erste Regel hat auch die höchste Priorität. Bitte klicken Sie auf **Detailansicht**, um die Reihenfolge der festgelegten Regeln zu ändern.

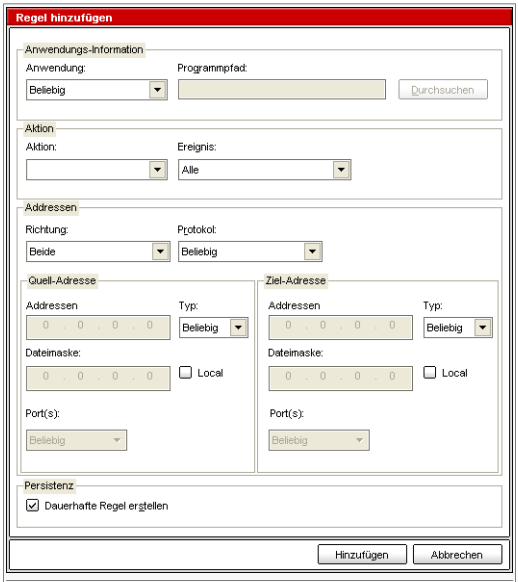
Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

Anmerkung

Ein Kontextmenü ist ebenfalls verfügbar und es enthält die folgenden Optionen: **Regel erstellen**, **Regel löschen** und **Regel editieren**.

8.3.2. Regeln manuell hinzufügen

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.



Wählen der Parameter

Hier können Sie die Parameter auswählen:

- **Anwendung** - Wählen Sie die Regel für die entsprechende Anwendung aus. Sie können auch nur eine spezielle Anwendung auswählen. Dazu wählen Sie **Auswahl der gewünschten Anwendung** im Aufklappmenü aus und definieren Sie dann den **Pfad\Dateiname**. Klicken Sie nun auf **Durchsuchen** und wählen Sie die entsprechende Anwendung aus. Um alle Anwendungen auszuwählen, markieren Sie **Beliebig** in dem Aufklappmenü.
- **Aktion** - wählen Sie die entsprechende Aktion zu dem dazugehörigen Ereignis. Selbstverständlich können auch mehrere Ereignisse ausgewählt werden.

Aktion	Beschreibung
Erlauben	Die Aktion wird erlaubt.
Verweigern	Die Aktion wird verweigert.

- **Adressen** - wählen Sie die Richtung des Datentransfers und das Protokoll für diese Regel.

Richtung - Wählen Sie die Richtung des Datenverkehrs aus.

Typ	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.

Protokoll - Bitte wählen Sie den gewünschten Protokolltyp aus: ICMP, TCP, UDP, IGMP, oder Beliebig.

Eine Liste mit den geläufigsten Protokollen steht Ihnen ebenfalls zur Verfügung, um Ihnen die Auswahl eines speziellen Protokolls zu erleichtern. Wählen Sie das gewünschte Protokoll aus dem Aufklappmenü aus (auf die die festegelegten Regeln dann zutreffen sollen), oder wählen Sie **Beliebig** um jedes Protokoll zuzulassen.

Protokoll	Beschreibung
ICMP	Internet Control Message Protocol (ICMP) benutzt wie TCP und UDP das Internet Protocol IP, ist also ein Teil der Internet-Protokoll-Familie. Es dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen. Obwohl ICMP eine Ebene über IP angeordnet ist, ist es in IP integriert. Es wird von jedem Router und PC erwartet, ICM-Protokoll zu sprechen. Die meisten ICMP-Pakete enthalten Diagnose-Informationen, sie werden vom Router zur Quelle (engl. source) zurückgeschickt, wenn der Router Pakete verwirft, z.B. weil das Ziel (engl. destination) nicht erreichbar ist, die TTL abgelaufen ist, usw. Es gilt der Grundsatz, dass ein ICMP-Paket niemals ein anderes ICMP-Paket auslöst, d.h. die Tatsache, dass ein ICMP Paket nicht zugestellt werden konnte wird nicht durch ein Weiteres signalisiert. Eine Ausnahme zu diesem Grundsatz bildet die Echo-Funktion. Echo-ICMP-Pakete werden z.B. durch das Programm Ping verschickt. ICMP-Nachrichten werden beim Versand im Datenteil von IP-Datagrammen eingekapselt. Dabei sind im IP-Header der Servicetyp immer 0 und die Protokollnummer immer 1.
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

Protokoll	Beschreibung
	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 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.

- **Quell-Adresse** - Bitte definieren Sie Ihre IP Adresse, die Maske oder prüfen Sie im Menü **Lokal**, ob die Regeln für den Computer anwendbar sind. Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Ziel-Adresse** - Bitte definieren Sie Ihre IP Adresse, die Maske oder prüfen Sie im Menü **Lokal**, ob die Regeln für den Computer anwendbar sind. Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Persistenz** - Bitte setzen Sie in die Checkbox **Dauerhafte Regel erstellen** ein Häkchen um diese Regel für zukünftige Sitzungen zu speichern. Falls Sie diese Option nicht gewählt haben, wird sie am Ende der Sitzung gelöscht.

Klicken Sie auf **Hinzufügen**.

Wichtig

Die Regeln sind gemäß ihrer Priorität von oben beginnend gelistet. Dies bedeutet, die erste Regel hat auch die höchste Priorität. Bitte klicken Sie auf **Detailansicht**, um die Reihenfolge der festgelegten Regeln zu ändern.

Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

Anmerkung

Ein Kontextmenü ist ebenfalls verfügbar und es enthält die folgenden Optionen: **Regel erstellen**, **Regel löschen** und **Regel editieren**.

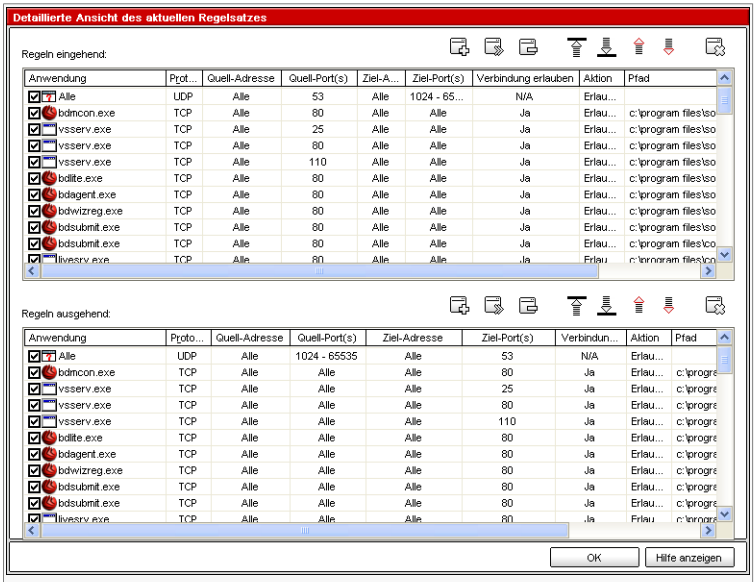
8.3.3. Profile ändern

Bevor das Firewall Modul aktiviert wird, werden Sie aufgefordert den Assistenten zu beenden um ein neues Netzwerkprofil zu erstellen. Der Assistent hilft Ihnen dabei eine Reihe von wichtigen Regeln für die firewall zu erstellen, für die Anwendungen, die Sie gewöhnlich nutzen. Klicken Sie **Profil rekonfigurieren** um den Assitenten zu aktivieren und die Profile zu rekonfigurieren.

Wichtig

Alle Regeln, die in diesem Abschnitt hinzugefügt werden, gehen verloren, wenn Sie das Netzwerk Profil rekonfigurieren.

Sie können das Profil ändern wenn Sie auf **Profil bearbeiten** klicken. Das folgende Fenster öffnet sich:



Detaillierte Ansicht

Die Regeln sind in 2 Bereiche eingeteilt: Regeln Dateneingang und Regeln Datenausgang. Sie können die Anwendungen und Parameter für jede Regel sehen (Absender, Adressat, Absende Ports, Adressierte Ports, Aktion, etc.).

Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

Sie können die Priorität einer Regel erhöhen oder heruntersetzen. Klicken Sie **In der Liste hochsetzen** um die ausgewählte Regel um ein Level nach oben zu setzen. Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herunterzusetzen.

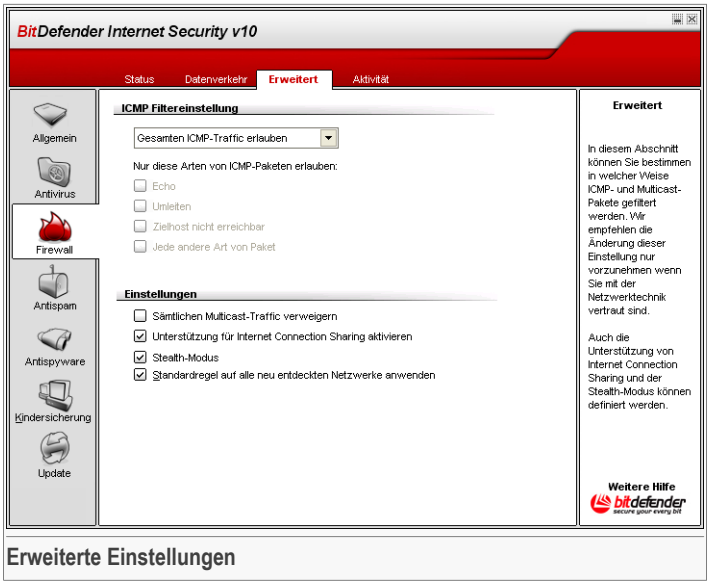
Anmerkung

Ein Kontextmenü ist ebenfalls verfügbar und es enthält die folgenden Optionen: **Regel hinzufügen**, **Regel editieren**, **Regel löschen**, **Hochsetzen**, **Heruntersetzen** und **Liste bereinigen**.

OK - zurück zur Management-Konsole.

8.4. Erweiterte Einstellungen

Um diese Sektion zu öffnen klicken Sie bitte auf **Erweitert** im Modul **Firewall**.



Erweiterte Einstellungen

In diesem Abschnitt können Sie die erweiterten Einstellungen der BitDefender Firewall konfigurieren. Die erweiterte Einstellung erlaubt es, spezielle Filterregeln für den ICMP Verkehr (ICMP Filter Einstellungen) festzulegen und den multicast Verkehr zu blockieren, Ihre Internet Verbindung zu teilen oder Ihren Computer unsichtbar für schädliche Software und Hacker zu machen. (Settings).

8.4.1. ICMP Filter Einstellungen

Sie können aus dem Menü eine der folgenden Regeln auswählen, um den ICMP Verkehr zu filtern:

- Klicken Sie auf **Gesamten ICMP Verkehr erlauben** wenn Sie sämtlichen ICMP Datenverkehr erlauben möchten.

- Klicken Sie auf **Gesamten ICMP Verkehr blockieren** wenn Sie sämtlichen ICMP Datenverkehr unterbinden möchten.
- Wählen Sie **Eigene ICMP Filtereinstellungen** und Sie können den Filter mit folgenden Optionen konfigurieren:

Option	Beschreibung
Echo	Der Echo-Netzwerkdienst ist ein einfacher Dienst auf Basis des Internet Protokolls. Aufgabe des Dienstes ist es, alle empfangenen Daten unverändert zum Client zurückzusenden. Er eignet sich somit zum Test und zur Fehlersuche während der Entwicklung von Clientprogrammen. Ping (in Anlehnung an das Geräusch eines Sonars) sendet ein ICMP-Echo-Request-Paket an die Zieladresse des zu überprüfenden Hosts. Der Empfänger muss, insofern er das Protokoll unterstützt, laut Protokollspezifikation eine Antwort zurücksenden: ICMP Echo-Reply. Ist der Zielrechner nicht erreichbar, antwortet der Router: Network unreachable (Zielhost nicht erreichbar) oder Host unreachable (Gegenstelle nicht erreichbar). Aus einer fehlenden Antwort kann man allerdings nicht eindeutig darauf schließen, dass die Gegenstelle nicht erreichbar ist. Manche Hosts sind nämlich so konfiguriert, dass sie ICMP-Pakete ignorieren und verwerfen.
Umleiten	Dies ist eine ICMP Nachricht, die den Host informiert, dass die Informationen umgeleitet wurden (sendet die Datenpakete über einen alternativen Weg). Wenn der Host versucht, Daten über einen Router (R1) zu übermitteln, jedoch ein zweiter angesprochener Router (R2) den Host erreicht, wird die Umleitungsfunktion den Host über diesen zweiten Weg infomieren. Der Router wird aber weiterhin den Datensatz zu der ursprünglichen Adresse schicken. Falls der Datensatz Routing Informationen besitzt, wird die Nachricht nicht gesendet, obwohl eine bessere Verbindung besteht.
Zielhost nicht erreichbar	Dies ist eine Nachricht des ICMP Protokolls, die durch den Router generiert wird und mitteilt, dass das E-Mail Programm den Empfänger nicht erreichen kann, es

Option	Beschreibung
	sein denn, der Datensatz hat eine Mulitcast Adresse. Gründe dafür sind, dass die physikalische Adresse zum Host nicht existiert (die Distanz ist unerheblich), das angesprochene Protokoll oder der Port nicht aktiv sind oder die Daten fragmentiertwerden müssen und der Befehl „nicht fragmentieren“ist aktiviert.
Jede andere Art von Paket	Wenn Sie diese Option frei geschaltet ist, werden alle anderen Pakete außer **Echo**, **Zielhost nicht erreichbar** oder **Umleiten** durchgelassen.

- **Bestehendes Regelwerk auf ICMP anwenden** - wendet die bestehenden Einstellungen auf den ICMP Datenverkehr an, die im Status section of the **Firewall** Modul angelegt sind.

8.4.2. Einstellungen

Folgende Aktionen stehen zur Verfügung:

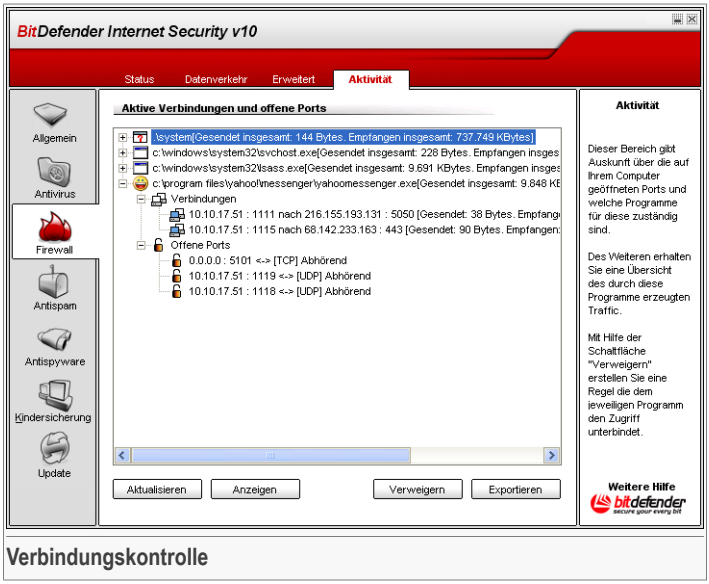
Option	Beschreibung
Sämtlichen Multicast-Traffic verweigern	Mit dieser frei geschalteten Option werden alle erhaltenene Multicast Pakete fallengelassen. Multicast Datenverkehr ist auf eine spezielle Gruppe innerhalb eines Netzwerkes ausgerichtet. Pakete werden an eine spezielle Adresse gesendet von der aus der Multicast Clients sie empfangen kann, wenn er es erlaubt. Wenn zum Beispiel ein Mitglied im Netzwerk, der einen TV-Tuner zur Verfügung hat, an alle Mitglieder im Netzwerk oder per Multicast an spezielle Adressen einen Video Stream aussendet, können die Computer mit der Multicast Adresse dieses Paket akzeptieren oder ablehnen. Wenn das Paket akzeptiert wird, kann der Stream mit den Multicast Clients angesehen werden. Große Mengen an Multicast Datenverkehr benötigen sehr viel Bandbreite und Ressourcen. Wenn Sie diese Option auswählen wird jedes empfangene Multicast

Option	Beschreibung
	Paket abgelehnt. Wie auch immer, es wird nicht empfohlen diese Option auszuwählen.
Internetverbindung	Erlaubt die Unterstützung von Internet Connection Sharing (ICS). Diese Option erlaubt nicht automatisch ICS auf Ihrem System sondern erlaubt diese Art von Verbindung nur, wenn Sie es von Ihrem Betriebssystem aus freigeben. Internet Connection Sharing (ICS) erlaubt Mitgliedern von lokalen Netzwerken von ihrem Computer aus eine Internetverbindung aufzubauen. Das ist sinnvoll wenn Sie eine spezielle/besondere Internet Verbindung haben (z.B. drahtlose Anbindung) und Sie möchten diese mit anderen Mitgliedern im Netzwerk teilen. Das Teilen von Internet Verbindungen mit anderen Mitgliedern im lokalen Netzwerk für zu einem höheren Ressourcen Verbrauch und birgt gewisse Risiken. Es belegt zudem einige Ihrer Ports (solche die von den Mitgliedern geöffnet werden, die die Internet Verbindung nutzen).
Stealth-Modus	Macht Ihren Computer unsichtbar für schädliche Software und Hacker. Personen oder Software mit betrügerischer Absicht sollten keinesfalls erfahren, dass Ihr Computer überhaupt existiert, geschweige denn mit dem Netzwerk Daten austauscht. Der **Stealth-Modus** verhindert, dass Ihr Computer auf Zugriffsversuche reagiert, die versuchen, an Informationen über offene Ports und deren Herkunft zu gelangen. Ein einfacher Weg um herauszufinden, ob Ihr Computer angreifbar ist, ist es die Ports zu verbinden und zu sehen, ob eine Antwort erfolgt. Das ist ein sogenannter Port Scan. BitDefender entdeckt und blockiert automatisch solche Port Scans.
Dieses Profil allen neuen Netzwerken zuordnen	Wendet ein allgemeines Profil an wenn neue Netzwerke erkannt werden. Dies hat keinen Effekt auf bereits erkannte Netzwerke oder solche die bereits ein zugewiesenes Profil aufweisen. Deaktivieren Sie diese

Option	Beschreibung
	Option, wenn Sie den Firewall-Assistent angezeigt bekommen möchten sobald ein neues Netzwerk erkannt wird. Das allgemeine Profil wird erstellt sobald Sie den Firewall-Assistent abgeschlossen und die Option **Dieses Profil zu einem allgemeinen Profil machen** aktiviert haben.

8.5. Verbindungskontrolle

Um diese Sektion zu öffnen klicken Sie bitte auf **Aktivität** im Modul **Firewall**.



Verbindungskontrolle

In diesem Abschnitt können Sie erkennen welches aktuelle Netzwerk- und Internetaktivität(über TCP und UDP) vorhanden ist. Diese Aktivität ist nach den einzelnen Anwendungen unterteilt. Sie haben auch die Möglichkeit die Berichtsdatei der BitDefender-Firewall hier einzusehen.

Klicken Sie auf **Verweigern**, um eine Regeln zu erstellen, die den Datenverkehr für ausgewählte Anwendungen, Ports oder Verbindungen einschränken. Sie werden

aufgefordert Ihre Auswahl zu bestätigen. Die Regeln können unter dem Link Datenverkehr für weitere Feineinstellungen eingesehen werden.

Bitte verwenden Sie den Befehl **Aktualisieren** im Abschnitt **Aktivität** (um die letzten Aktivitäten der **Firewall** einsehen zu können).

Klicken Sie auf **Exportieren**, um die Liste zu Diagnosezwecken als `.txt` auf Ihrer Festplatte zu speichern.

Außerdem kann eine Liste generiert werden, die Aufschluss über Aktivitäten gibt (geprüfte Ports, Verweigern von Zugriffsversuchen, Tarnkappenmodus oder Datenverkehr gemäß den Einstellungen). Für diese detaillierte Liste klicken Sie bitte auf **Anzeigen**. Diese Datei finden Sie alternativ auch im Verzeichnis: `...\Aplication Data\ Bitdefender\Firewall\ log` auf Ihrer lokalen Festplatte.

9. Das Modul Antispam

Der Abschnitt **AntiSpam** behandelt und erklärt folgende Themen:

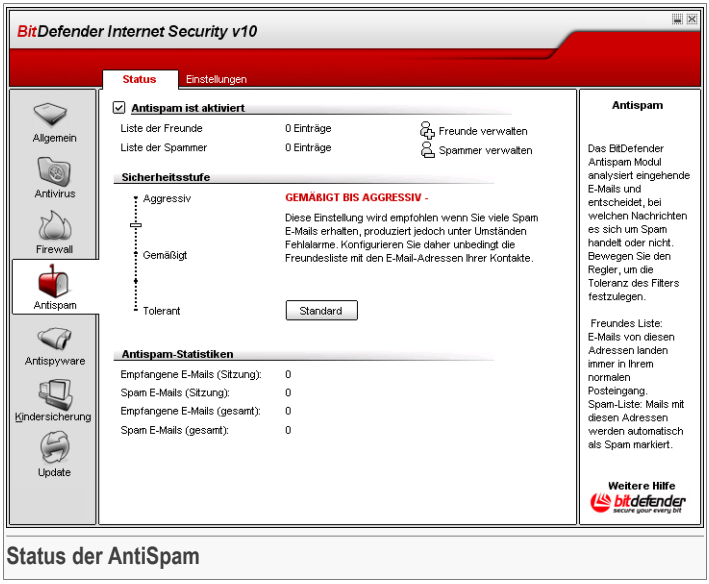
- Status der AntiSpam
- AntiSpam-Einstellungen
- Konfigurieren von BitDefender AntiSpam für Microsoft Outlook / Outlook Express

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **AntiSpam** finden Sie in der Produktbeschreibung auf Seite *„Das Modul Antispam“* (S. 30).

9.1. Status der AntiSpam

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Antispam**.



Status der AntiSpam

In dieser Sektion können Sie das **AntiSpam**-Modul konfigurieren und Informationen über seine Einstellungen erhalten.

Wichtig

Um zu verhindern, dass Spam in Ihren **Posteingang** gelangt, aktivieren Sie die **AntiSpam Filter**.

In der **Statistiken**-Sektion erhalten Sie einen Einblick in die Statistiken des AntiSpam-Moduls. Die Ergebnisse werden pro Sitzung (seitdem Sie Ihren Computer gestartet haben) angezeigt. Sie können aber auch einen Überblick seit der Installation der AntiSpam-Filter bekommen.

Um das **AntiSpam** Modul zu konfigurieren, folgen Sie diesen Schritten:

9.1.1. Ausfüllen der Adressliste

Die Adressliste enthält E-Mail-Adressen, unter denen Ihnen reguläre Mails und auch Spam gesendet wurde.

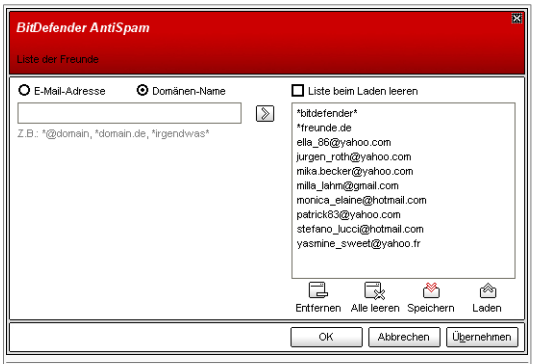
Liste der Freunde

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.

Anmerkung

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Um die **Freundesliste** zu handhaben, klicken Sie auf >>> (übereinstimmend mit Ihrer **Freundesliste**) oder klicken Sie auf den **Freunde**-Button vom *„AntiSpam Symbolleiste“* (S. 119).



Liste der Freunde

Hier können Sie die Einträge Ihrer **Freundesliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den -Button. Die Adresse wird Ihrer **Freundesliste** hinzugefügt.

Wichtig

Syntax: `<name@domain.com>`.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den -Button. Die Domain wird Ihrer **Freundesliste** hinzugefügt.

Wichtig

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;

Um ein Objekt von der Liste zu löschen, wählen Sie es aus und klicken **Entfernen**. Wenn Sie auf **Liste löschen** klicken, werden alle Einträge von der Liste gelöscht, bitte beachten Sie: Die Einträge können nicht wieder hergestellt werden.

Benutzen Sie die **Speichern**/ **Laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung `.bwl` haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Während des Ladens, aktuelle Liste leeren**.

Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

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

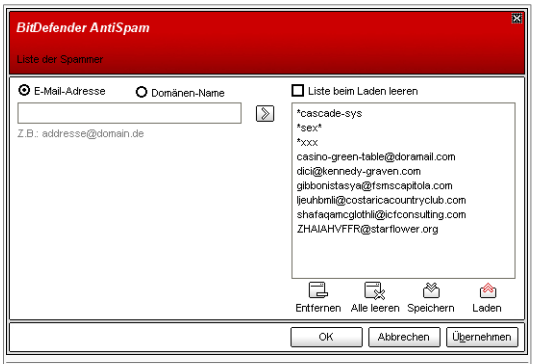
Liste der Spammer

Liste der Spammer - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts.

Anmerkung

Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.

Um die **Spammer-Liste** zu bearbeiten, klicken Sie auf (übereinstimmend mit Ihrer **Spammer-Liste**) oder klicken Sie auf den **Spammer**-Button vom *„AntiSpam Symbolleiste“* (S. 119).



Liste der Spammer

Hier können Sie die Einträge Ihrer **Spammerliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den -Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.

Wichtig

Syntax: `<name@domain.com>`.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den -Button. Die Domain wird Ihrer **Spammerliste** hinzugefügt.

Wichtig

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.

Um ein Objekt von der Liste zu löschen, wählen Sie es aus und klicken **Entfernen**. Wenn Sie auf **Liste löschen** klicken, werden alle Einträge von der Liste gelöscht, bitte beachten Sie: Die Einträge können nicht wieder hergestellt werden.

Benutzen Sie die **Speichern**/ **Laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung `.bwl` haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Während des Ladens, aktuelle Liste leeren**.

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

Wichtig

Wenn Sie BitDefender erneut installieren möchten, sollten sie Ihre **Freundes -** / **Spammerliste** speichern und nach der Neuinstallation wieder laden.

9.1.2. Einstellen des Toleranz Levels

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

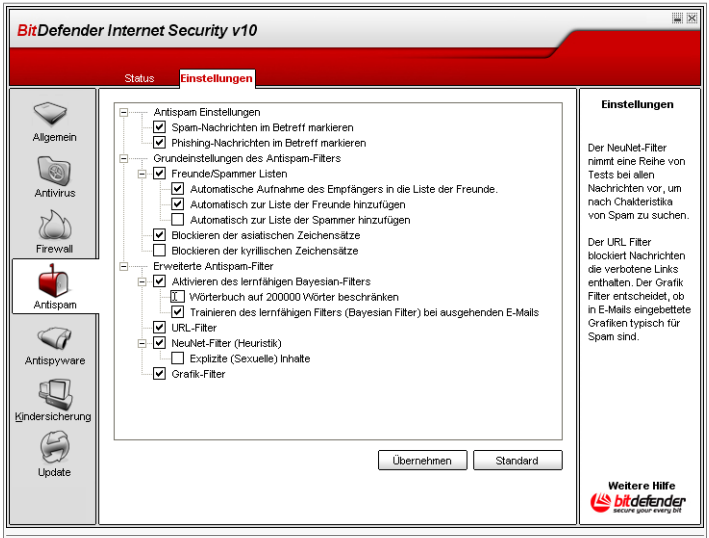
Es stehen 5 Toleranz Level zur Verfügung:

Toleranz Level	Beschreibung
Tolerant	Bietet Schutz für E-Mail Accounts, die eine Menge von erlaubter kommerzieller E-Mail erhalten. Der Filter wird den meisten E-Mail Verkehr zulassen, aber möglicherweise falsche E-Mails durchlassen (Spam eingeordnet als erlaubte Mail)
Mittlere Toleranz	Bietet Schutz für E-Mail Accounts, die ein paar erlaubte kommerzielle E-Mails erhalten. Der Filter wird den meisten E-Mail Verkehr zulassen, aber möglicherweise falsche E-Mails durchlassen (Spam eingeordnet als erlaubte Mail)
Mittel	Bietet Schutz für reguläre Accounts. Der Filter blockiert die meisten Spam Mails und vermeidet Fehlalarme.
Mittel bis aggressiv	Bietet Schutz für E-Mail Accounts, die regelmäßig ein hohes Volumen an Spam erhalten. Der Filter läßt extrem wenig Spam durch, aber es kann zu Fehlalarmen kommen indem erlaubte Mails als Spam gekennzeichnet werden.

Toleranz Level	Beschreibung
	Konfigurieren der **Freunde/Spammer Liste** und Training des **Bayesian Filter** um die Anzahl an Fehlalarmen zu reduzieren.
Aggressiv	Bietet Schutz für E-Mails Accounts, die regelmäßig eine hohe Zahl an Spam Mails erhalten. Der Filter läßt extrem wenig Spam durch, aber es kann zu Fehlalarmen kommen indem erlaubte Mails als Spam gekennzeichnet werden. Fügen Sie Ihre Kontakte zur **Freundesliste** hinzu, um die Anzahl an Fehlalarmen zu reduzieren.

9.2. AntiSpam-Einstellungen

Um diese Sektion zu öffnen klicken Sie bitte auf **Einstellungen** im Modul **Antispam**.



AntiSpam-Einstellungen

Hier können Sie die einzelnen AntiSpam-Filter (de)aktivieren und weitere Einstellungen am AntiSpam-Modul vornehmen.

Drei Kategorien von Einstellungen sind möglich (**Allgemein**, **Erweitert** und **AntiSpam Filter**). Sie sind erweiterbar wie ein Menü, vergleichbar mit denen von Windows.

Anmerkung

Klicken Sie auf eine Box mit einem "+", um ein Menü auszuklappen, und auf ein "-", um es zu schließen.

9.2.1. AntiSpam-Einstellungen

- **Spam-Nachrichten im Betreff markieren** - alle E-Mails, die als SPAM Mails eingestuft werden, erhalten eine SPAM-Markierung in der Betreffzeile.
- **Phishing (Schutz vor Diebstahl von Zugangsdaten) Nachrichten im Betreff kennzeichnen** - alle E-Mails, die als Phishing Mails eingestuft werden, erhalten eine SPAM-Markierung in der Betreffzeile.

9.2.2. AntiSpam Filter

- **Freundes/Spammer listen** - aktiviert/deaktiviert den Freundes/Spammerliste;
  - **Zur Liste der Freunde hinzufügen** - um die Sender in Ihre **Freundesliste** übernehmen.
  - **Automatisch zur Liste der Freunde hinzufügen** - wird beim nächsten Klick auf den **Kein Spam**-Button in der *„AntiSpam Symbolleiste“* (S. 119) den Sender automatisch zu **Liste der Freunde** hinzugefügt.
  - **Automatisch zur Liste der Spammer hinzufügen** - wird beim nächsten Klick auf den **Ist Spam**-Button in der *„AntiSpam Symbolleiste“* (S. 119) den Sender automatisch zu **Liste der Spammer** hinzugefügt.

Anmerkung

Die **Kein Spam** und **Ist Spam**-Buttons werden durch den Bayesian Filter trainiert.

- **Asiatische Zeichen blockieren** - blockiert Nachrichten mit Asiatische Zeichen.
- **Kyrillische Zeichen blockieren** - blockiert Nachrichten mit Kyrillische Zeichen.

9.2.3. AntiSpam Filter

- **Bayesian-Filter** - aktiviert/deaktiviert den Bayesian-Filter;
  - **Wörterbuch auf 200.000 Wörter beschränken** - mit dieser Option können Sie die Größe des bayesianischen Verzeichnisses begrenzen – kleiner ist schneller, größer ist akkurater.

Anmerkung

Die empfohlene Größe sind 200.000 Wörter.

- **Trainieren des Bayesian Filter für ausgehende E-Mails** - trainieren des Bayesian Filter für ausgehende E-Mails.

- **URL Filter** - aktiviert/deaktiviert den URL Filter;
- **Heuristischer Filter** - aktiviert/deaktiviert den Heuristischer Filter;
  - **Explizite (Sexuelle) Inhalte** - aktiviert/deaktiviert den Filter für eindeutige Inhalte;
- **Grafik-Filter** - aktiviert/deaktiviert den Filter für Bilder bzw. Grafiken.

Anmerkung

Um einen Filter zu (de)aktivieren setzen bzw. entfernen Sie das jeweilige Häkchen in der Checkbox.

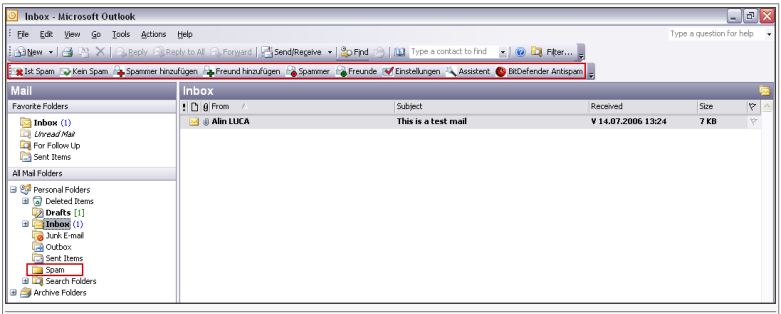
Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

9.3. Konfigurieren von BitDefender AntiSpam für Microsoft Outlook / Outlook Express

BitDefender integriert sich über eine intuitive Symbolleiste nahtlos in Microsoft Office Outlook bzw. Outlook Express.

9.3.1. AntiSpam Symbolleiste

Im oberen Bereich von Microsoft Outlook / Outlook Express sehen Sie die BitDefender-Symbolleiste.



AntiSpam Symbolleiste

Wichtig

Der Hauptunterschied bei BitDefender AntiSpam für Microsoft Outlook und Outlook Express ist, dass Spam-Nachrichten bei Microsoft Outlook in den **Spam**-Ordner und bei Outlook Express in einen Unterordner des **Papierkorbs** verschoben werden. In beiden Fällen werden die Mails in der Betreffzeile als Spam markiert.

Der **Spam**-Ordner der von BitDefender AntiSpam für Microsoft Outlook entwickelt wurde, liegt auf derselben Ebene wie die **Ordnerliste**(Kalender, Kontakte usw.).

Jede Schaltfläche wird unten beschrieben:

- **Ist Spam** - Klicken Sie auf diesen Button und das bayesianische Modul erkennt die ausgewählten Mails als Spam. Sie werden als Spam markiert und in den **Spam**-Ordner verschoben.

  Zukünftige Mails mit diesem Muster werden alle als Spam markiert.

  Anmerkung

  Sie können eine oder mehrere E-Mails markieren.

- **Kein Spam** - Klicken Sie auf diesen Button und das bayesianische Modul erkennt die ausgewählten Mails nicht als Spam. Sie werden nicht als **Spam** markiert und in den **Posteingang** verschoben.

  Zukünftige E-Mails mit diesem Muster werden nicht mehr als Spam markiert.

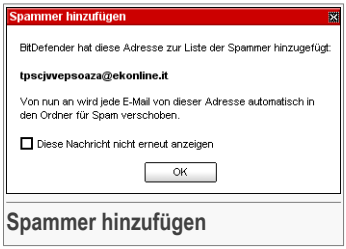
  Anmerkung

  Sie können eine oder mehrere E-Mails markieren.

Wichtig

Die Schaltfläche **Kein Spam** wird aktiv, wenn Sie eine Nachricht als Spam markiert haben (normalerweise werden diese Nachrichten in den **Spam**-Ordner verschoben).

- **Spammer hinzufügen** - Klicken Sie diesen Button, um die ausgewählte Nachricht Ihrer **Spammerliste** hinzuzufügen.



Spammer hinzufügen

Wählen Sie **Diese Nachricht nicht erneut anzeigen**, um dieses Fenster nicht mehr zu sehen, wenn Sie eine neue Spam-Mail in die Liste aufnehmen.

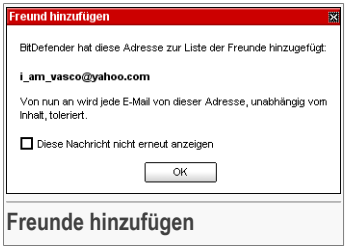
Klicken Sie auf **OK**, um dieses Fenster zu schließen.

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

Anmerkung

Sie können einen oder mehrere Absender auswählen.

- **Freunde hinzufügen** - Klicken Sie auf diesen Button, um den Absender dieser Mail Ihrer **Freundesliste** hinzuzufügen.



Freunde hinzufügen

Wählen Sie **Diese Nachricht nicht erneut anzeigen**, um dieses Fenster nicht mehr zu sehen, wenn Sie eine neue Freundesmail in die Liste aufnehmen.

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

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

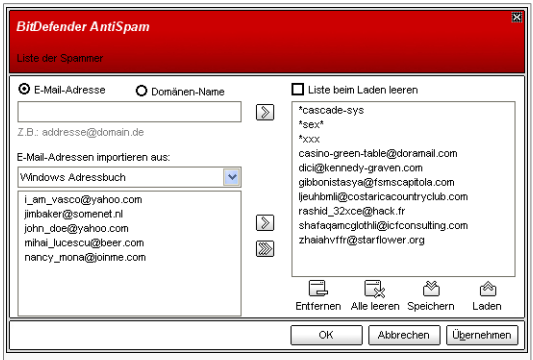
Anmerkung

Sie können einen oder mehrere Absender auswählen.

- **Spammer** - Klicken Sie auf diesen Button, um die **Spammerliste** zu öffnen. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleich welchen Inhalts.

Anmerkung

Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch in Ihren Papierkorb verschoben.



Liste der Spammer

Hier können Sie die Einträge Ihrer **Spammerliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den -Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.

Wichtig

Syntax: `<name@domain.com>`.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie sie und tragen Sie sie in das Feld **Domänen-Name** ein; klicken Sie auf den -Button. Die Domäne wird Ihrer **Spammerliste** hinzugefügt.

Wichtig

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.

Um E-Mail Adressen aus **Microsoft Outlook/Outlook Express** zu importieren, wählen Sie im Aufklapp–Menü unter **E-Mail Adresse importieren aus** die Option **Windows Adressbuch/Outlook Express Ordner**.

Für **Microsoft Outlook Express** öffnet sich ein neues Fenster. Sie können nun den Ordner mit E-Mail Adressen auswählen, den Sie zur **Liste der Spammer** hinzufügen möchten. Klicken Sie anschließend auf **Auswählen**.

In beiden Fällen werden die E-Mail-Adressen in der Importliste erscheinen. Wählen Sie die gewünschten E-Mail-Adressen aus und klicken Sie auf den -Button, um sie zur **Spammerliste** hinzuzufügen. Wenn Sie anklicken, werden alle E-Mail-Adressen zur Spammerliste hinzugefügt.

Um ein Objekt von der Liste zu löschen, wählen Sie es aus und klicken **Entfernen**. Wenn Sie auf **Liste löschen** klicken, werden alle Einträge von der Liste gelöscht, bitte beachten Sie: Die Einträge können nicht wieder hergestellt werden.

Benutzen Sie die **Speichern**/ **Laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung .bwl haben.

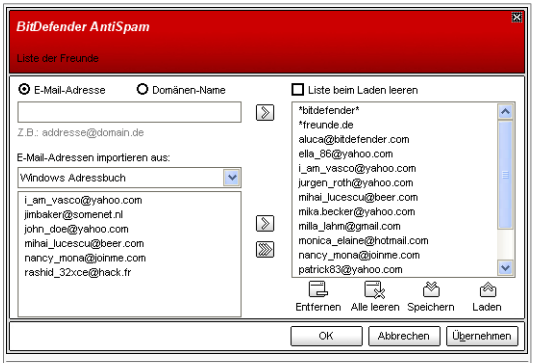
Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Während des Ladens, aktuelle Liste leeren**.

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

- **Freunde** - Klicken Sie auf diesen Button, um die **Freundesliste** zu öffnen Sie enthält alle E-Mail-Adressen, von denen Sie Nachrichten erhalten wollen, gleich welchen Inhalts.

Anmerkung

Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.



Liste der Freunde

Hier können Sie die Einträge Ihrer **Freundesliste** ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adresse**, tragen Sie sie ein und klicken Sie auf den -Button. Die Adresse wird Ihrer **Spammerliste** hinzugefügt.

Wichtig

Syntax: `<name@domain.com>`.

Falls Sie eine Domain hinzufügen möchten, kontrollieren Sie diese und schreiben Sie sie in das Feld **Domänen-Name**; klicken Sie auf den -Button. Die Domain wird Ihrer **Freundesliste** hinzugefügt.

Wichtig

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;

Um E-Mail Adressen aus **Microsoft Outlook/Outlook Express** zu importieren, wählen Sie im Aufklapp–Menü unter **E-Mail Adresse importieren aus** die Option **Windows Adressbuch/Outlook Express Ordner**.

Für **Microsoft Outlook Express** öffnet sich ein neues Fenster. Sie können nun den Ordner mit E-Mail Adressen auswählen, den Sie zur **Liste der Freunde** hinzufügen möchten. Klicken Sie anschließend auf **Auswählen**.

In beiden Fällen werden die E-Mail-Adressen in der Importliste erscheinen. Wählen Sie die gewünschten E-Mail-Adressen aus und klicken Sie auf den -Button, um sie zur **Freundesliste** hinzuzufügen. Wenn Sie anklicken, werden alle E-Mail-Adressen zur Freundesliste hinzugefügt.

Um ein Objekt von der Liste zu löschen, wählen Sie es aus und klicken **Entfernen**. Wenn Sie auf **Liste löschen** klicken, werden alle Einträge von der Liste gelöscht, bitte beachten Sie: Die Einträge können nicht wieder hergestellt werden.

Benutzen Sie die **Speichern**/ **Laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung `.bwl` haben.

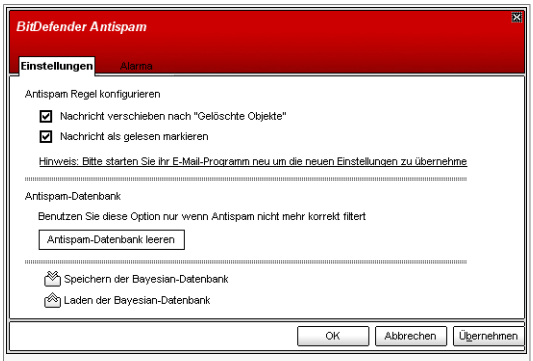
Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Während des Ladens, aktuelle Liste leeren**.

Anmerkung

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren E-Mail-Adressen der **Freundesliste** hinzufügen, damit sichergestellt ist, dass nur solche E-Mails an Sie weitergeleitet werden.

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

- **Einstellungen** - Öffnet das Fenster **Einstellungen**, indem Sie weitere Optionen für das **AntiSpam**-Modul angeben können.



Einstellungen

Folgende Optionen stehen zur Verfügung:

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

Wenn Ihr AntiSpam-Filter ungenau arbeitet, sollten Sie die Filter-Datenbank löschen und den Bayesian-Filter neu trainieren. Klicken Sie auf **AntiSpam Datenbank leeren**, um danach die Bayesian Datenbank neu aufzubauen.

Über die Funktion **Speichern der Bayesian Datenbank**/ **Laden der Bayesian Datenbank** können Sie die Datenbank des Bayesian-Filters aufrufen oder speichern und dies an einem von Ihnen festgelegten Speicherort. Diese Datei hat die Erweiterung `.dat`.

Klicken Sie auf **Alarma**, um Zugriff auf die Sektion haben, in der Sie die Erscheinung des Bestätigungsfensters für **Spammer hinzufügen** und **Freunde hinzufügen** deaktivieren können.

Anmerkung

In dem **Alarma** Fenster können Sie den Alarm **Bitte wählen Sie eine E-Mail-Nachricht** aktivieren/deaktivieren.Dieses Alarm erscheint wenn Sie eine Gruppe anstatt einer E-Mail-Nachricht auswählen.

- **Assistent** - klicken Sie auf diesen Button, um das Training für den Bayesian Filter zu starten, so dass die Effizienz von BitDefender-AntiSpam früh eintritt. Sie können auch Adressen aus Ihrem **Adressbuch** in Ihre **Freundes** / **Spammerliste** übernehmen.
- **BitDefender AntiSpam** - klicken Sie auf diesen Button, um die Management-Konsole zu öffnen.

9.3.2. Konfigurationsassistent

Beim ersten Start von Outlook bzw. Windows Mail nach der Installation von BitDefender bekommen Sie einen Assistenten angezeigt, der Sie dabei unterstützt, den Bayesian-Filter, die Liste der Freunde und die Liste der Spammer zu trainieren.

Anmerkung

Der Assistent kann jederzeit über die **Assistent** Schaltfläche in der *„AntiSpam Symbolleiste“* (S. 119) aufgerufen werden.

Schritt 1/6 - Einführung

Begrüßungsfenster

Klicken Sie auf **Weiter**.

Schritt 2/6 - Ausfüllen der Freundes-Liste

Ausfüllen der Freundesliste

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

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht ausführen wollen. Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren.

Schritt 3/6 - Bayesianische Daten löschen

Bayesianische Daten löschen

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

Wählen Sie **AntiSpam Datenbank leeren**, wenn Sie die bayesianische Datenbank neu starten wollen.

Über die Funktion **Speichern der Bayesian Datenbank**/ **Laden der Bayesian Datenbank** können Sie die Datenbank des Bayesian-Filters aufrufen oder speichern und dies an einem von Ihnen festgelegten Speicherort. Diese Datei hat die Erweiterung `.dat`.

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht ausführen wollen. Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren.

Schritt 4/6 -Trainieren des Bayesian-Filters mit legitimen E-Mails

Trainieren des Bayesian-Filters mit legitimen E-Mails

Bitte wählen Sie einen Ordner, der legitime E-Mails enthält. Diese Nachrichten werden genutzt, um den AntiSpam Filter zu trainieren.

Oben in diesem Fenster sind zwei Optionen wählbar:

- **Unterordner mit einbeziehen** - um Unterordner in Ihre Auswahl zu übernehmen;
- **Zur Liste der Freunde hinzufügen** - um die Sender in Ihre **Freundesliste** übernehmen.

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht ausführen wollen. Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren.

Schritt 5/6 - Trainieren des Bayesian-Filters mit Spam-Mails

Trainieren des Bayesian-Filters mit Spam-Mails

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

Wichtig

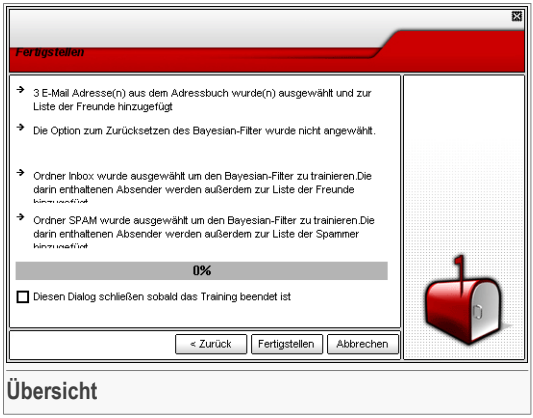
Bitte vergewissern Sie sich, dass der von Ihnen gewählte Ordner keine legitimen E-Mails enthält, ansonsten wird die AntiSpam-Leistung beträchtlich reduziert.

Oben in diesem Fenster sind zwei Optionen wählbar:

- **Unterordner mit einbeziehen** - um Unterordner in Ihre Auswahl zu übernehmen;
- **Zur Liste der Spammer hinzufügen** - um die Sender in Ihre **Spammerliste** zu übernehmen.

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht ausführen wollen. Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren.

Schritt 6/6 - Assistent abgeschlossen



Übersicht

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

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

10. Das Modul Antispyware

Der Abschnitt **AntiSpyware** behandelt und erklärt folgende Themen:

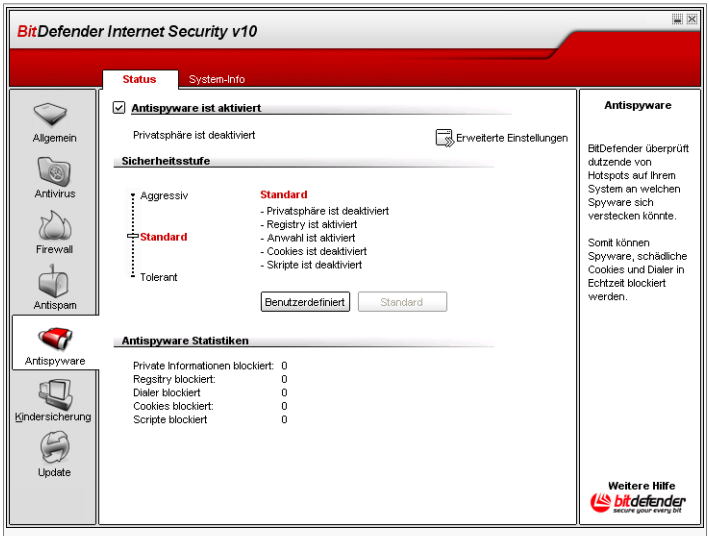
- Status der AntiSpyware
- Registrierung prüfen
- Registrierung prüfen
- Anwahl-Kontrolle
- Cookie-Kontrolle
- Skript-Kontrolle
- System-Informationen

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **AntiSpyware** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Antispyware*“ (S. 34).

10.1. Status der AntiSpyware

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Antispyware**.



Status der AntiSpyware

In dieser Sektion können Sie das **AntiSpyware**-Modul konfigurieren und Informationen über seine Einstellungen erhalten.

Wichtig

Um sicherzustellen, dass keine Spyware Ihren Computer infiziert, halten Sie das **Schutzschild** bitte immer aktiviert.

Am Schluss dieser Sektion können Sie die Statistiken einsehen.

Das **Spyware Schutzschild** schützt Ihren Computer vor Spyware durch 5 wichtige Kontrollmechanismen.

- Privacy Control - schützt Ihre vertraulichen Daten indem aller ausgehender HTTP und SMTP Datenverkehr aufgrund der erstellten Regeln Privacy geprüft wird.
- Registry Control - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.
- Dial Control - Fragt um Erlaubnis immer wenn ein Dialer versucht sich in den Computer einzuwählen.

- Hier hilft Ihnen die **Cookie-Kontrolle**. Wenn Sie aktiviert ist, wird die **Cookie-Kontrolle** bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis abfragen:
- Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. BitDefender wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:

Um diese Einstellungen zu konfigurieren klicken Sie Erweiterte Einstellungen.

10.1.1. Sicherheitseinstellung

Sie können die Sicherheitseinstellung an Ihre Anforderungen anpassen. Ziehen Sie die Anzeige auf der Scala auf die richtige Einstellung.

Es gibt 3 mögliche Einstellungen:

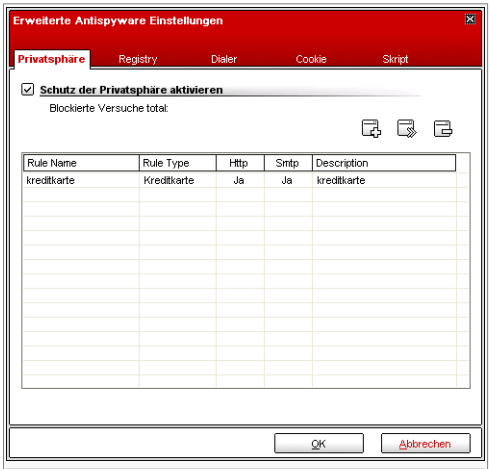
Sicherheitseinstellung	Beschreibung
Zulassen	**Registrierung** aktiviert.
Standardeinstellung	**Registry Kontrolle** und **Dialer Kontrolle** sind aktiviert.
Aggressiv	**Registry Kontrolle**, **Dialer Kontrolle** und **Privacy Control** sind aktiviert.

Das Sicherheitslevel kann mit einem Klick auf **Benutzerdefiniert** angepasst werden. In einem neuen Fenster können Sie nun die Einstellungen anpassen und anschließend mit **OK** bestätigen.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen.

10.2. Erweiterte Einstellungen - Privacy Kontrolle

Um auf diesen Bereich zuzugreifen klicken Sie **Erweiterte Einstellungen** im Feld **Antispyware** Modul, Status.



Privacy-Kontrolle

Vertrauliche Daten zu sichern ist für alle Anwender äußerst wichtig. Datenklau hat mit der Entwicklung der Internet Kommunikation standgehalten und wendet immer wieder neue Methoden an um Anwender zu täuschen und private Informationen zu erhalten.

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 Mails ertrinken oder sich über ein geleertes Konto wundern.

Privacy Kontrolle hilft Ihre privaten Daten zu sichern. Sie prüft den HTTP oder SMTP Datenverkehr, oder beides, für spezielle Strings, die Sie definieren. Wenn eine Übereinstimmung gefunden wird, mit einer Internet Seite oder einer E-Mail Adresse, werden diese sofort geblockt.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

10.2.1. Konfigurations-Assistent

Der Konfigurationsassistent wird in 3 Schritten eingestellt.

Schritt 1/3 - Typ und Richtung auswählen

Typ und Richtung auswählen

Geben Sie den Namen der Regel im Bearbeitungsfeld ein.

Hier können Sie die Parameter auswählen:

- **Regeltyp** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- **Regel für Daten** - Geben Sie die Regel für Daten ein.

Alle Daten, die Sie eingeben sind verschlüsselt. Um wirklich sicher zu gehen, geben Sie nicht alle Daten ein, die Sie schützen möchten.

Klicken Sie auf **Weiter**.

Schritt 2/3 - Datenverkehr auswählen

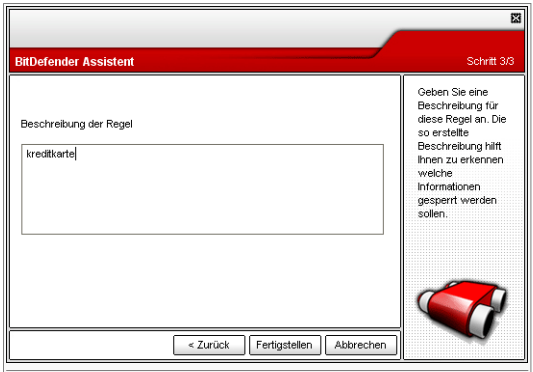
Datenverkehr auswählen

Bitte wählen Sie den verwendeten Netzwerktypen bzw. die Internetverbindung. Die folgenden Optionen stehen Ihnen zur Verfügung:

- **HTTP prüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **Ausgehende E-Mails prüfen** - prüft alle ausgehenden E-Mail-Nachrichten.

Klicken Sie auf **Weiter**.

Schritt 3/3 – Beschreibung der Regel



Beschreibung der Regel

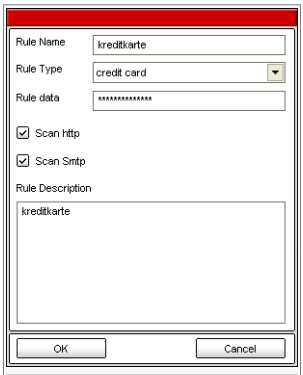
Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.

Klicken Sie auf **Fertigstellen**.

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, wählen Sie sie einfach aus und klicken **Löschen**. Um eine Regel zu deaktivieren ohen sie zu löschen, entfernen Sie den Haken in der entsprechenden Checkbox.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken **Bearbeiten** oder machen Sie einen Doppelklick. Das folgende Fenster erscheint:



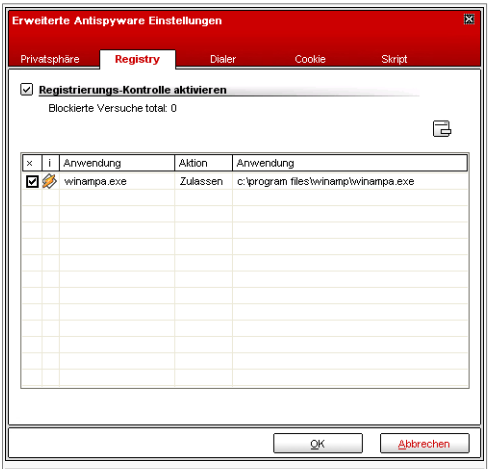
Regel bearbeiten

Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK**um die Änderungen zu speichern.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.3. Registry Kontrolle

Für diesen Bereich klicken Sie auf das Fenster **Advanced Antispyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Registry**.



Registry Kontrolle

Ein sehr wichtiger Teil von Windows ist die **Registry**. Dort werden von Windows alle Einstellungen, installierten Programme, Nutzerinformationen und so weiter verwaltet.

Die **Registry** bestimmt u. a., welche Programme automatisch beim Start von Windows geladen werden. Viren versuchen häufig hier anzusetzen, damit auch sie automatisch mit geladen werden, wenn der Nutzer seinen Computer startet.

Registry Kontrolle beobachtet die Windows-Registry – dies ist auch sehr hilfreich beim Aufspüren von Trojanern. Sie werden alarmiert, wann immer ein Programm versucht, einen Eintrag in die Registry zu unternehmen, um beim nächsten Windows-Start geladen zu werden.

Registry Alarm

Sie können die Änderung ablehnen, indem Sie auf **Nein** klicken, oder aber zulassen, indem Sie mit **Ja** bestätigen.

Wenn Sie möchten, dass BitDefender Ihre Antwort speichern soll, wählen Sie die Option: **Diese Antwort merken** aus.

Anmerkung

Wählen Sie Ja oder Nein auf der Grundlage Ihrer eigenen Sicherheitsrichtlinien.

Um einen Registry-Eintrag zu löschen, klicken Sie auf **Löschen**. Um zeitweise einen Registry Eintrag zu deaktivieren, ohne ihn zu löschen, entfernen Sie das Häkchen, indem Sie auf es klicken.

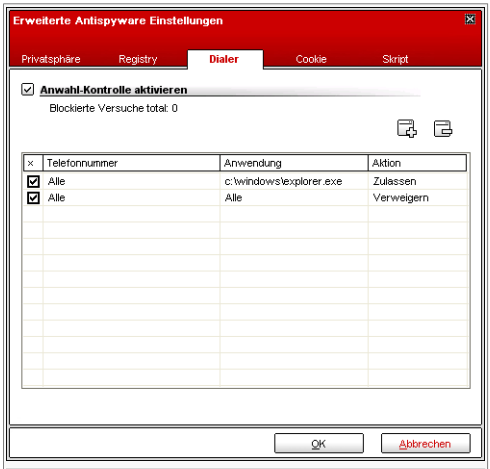
Anmerkung

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

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

10.4. Erweiterte Einstellungen - Dialer Kontrolle

Für diesen Bereich klicken Sie auf das Fenster **Erweiterte Antispyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Anwahl**.



Anwahl-Kontrolle

So genannte Dialer sind Anwendungen, die über Computer-Modems verschiedene Telefonnummern anwählen. Normalerweise werden Dialer genutzt, um unbemerkt kostenintensive Telefonnummern anzuwählen.

Mit der **Anwahl-Kontrolle** entscheiden Sie, welche Verbindung mit welcher Telefonnummer Sie zulassen oder unterbinden wollen. Die Anwahl-Kontrolle überwacht alle Dialer, die auf ein Computer-Modem zugreifen wollen, warnt den Benutzer unmittelbar und verlangt die Ablehnung oder Zustimmung zu solch einer Operation:

Anwahl-Alarme

Sie sehen den Namen der Anwendung und die vorgesehene Telefonnummer.

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Bei einer Wiederholung dieser Anwahl werden Sie nicht mehr informiert.

Jede erstellte Regel kann später über **Anwahl** aufgerufen und weiter bearbeitet werden.

Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

10.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus zwei Schritten.

Schritt 1/2 - Anwendung und Aktion auswählen

Anwendung und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Anwendung** - wählen Sie die Anwendung für die Regel. Sie können eine bestimmte Anwendung wählen (klicken Sie **Anwendung auswählen**, **Durchsuchen** und wählen Sie eine bestimmte Anwendung) oder alle Anwendungen (markieren Sie **Alle**).

- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Die Aktion wird erlaubt.
Verweigern	Die Aktion wird verweigert.

Klicken Sie auf **Weiter**.

Schritt 2/2 - Telefonnummer auswählen

Telefonnummer auswählen

Markieren Sie **Telefonnummer angeben**, geben Sie die Telefonnummer, für welche die Regel erstellt werden soll, in das darunter liegende Feld ein und klicken Sie auf **Hinzufügen**.

Anmerkung

Sie können Platzhalter in Ihrer Liste von nicht erlaubten Telefonnummern verwenden, z.B. : 1900* bedeutet, dass alle mit 1900 beginnenden Telefonnummern blockiert werden.

Markieren Sie **Alle**, falls diese Regel für alle Telefonnummern gelten soll. Falls Sie eine Nummer löschen möchten, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Anmerkung

Sie können ebenfalls eine Regel definieren, die einem bestimmten Programm nur erlaubt, bestimmte Telefonnummern zur Anwahl zu verwenden (zum Beispiel die Ihres Internet-Providers oder Ihres Fax- oder News-Services).

Klicken Sie auf **Fertigstellen**.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.5. Erweiterte Einstellungen

Um diesen Bereich zu bearbeiten klicken Sie **Erweiterte Antispyware Einstellungen**(gehen Sie auf **Antispyware** Modul, Status und klicken Sie **Erweiterte Einstellungen**) und klicken den Reiter **Cookie**.

Cookie-Kontrolle

Cookies werden von den meisten Webseiten im Internet verwendet. Es sind kleine Dateien, die auf Ihrem Computer gespeichert werden. Webseiten verschicken diese Cookies, um das Surfen zu beschleunigen, aber auch um Informationen über Sie zu erhalten.

Generell erleichtern Cookies das tägliche Internet-Leben. Zum Beispiel ermöglichen sie einer Webseite, Ihren Namen und sonstige Angaben zu speichern, so dass Sie diese nicht bei jedem Besuch eingeben müssen.

Cookies können jedoch auch missbräuchlich verwendet werden und Ihre Privatsphäre gefährden, indem Ihre Surfdaten an Dritte weitergegeben werden.

Hier hilft Ihnen die **Cookie-Kontrolle**. Wenn Sie aktiviert ist, wird die **Cookie-Kontrolle** bei jedem Versuch einer Webseite, einen Cookie anzubringen, Ihr diesbezügliches Einverständnis abfragen:

Cookie Alarm

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

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Sie werden dann nicht wieder informiert, wenn Sie das nächste Mal mit derselben Seite in Verbindung treten.

So werden Sie bei der Unterscheidung von zuverlässigen und unzuverlässigen Webseiten unterstützt.

Anmerkung

Aufgrund der großen Anzahl von Cookies, die heute im Internet verwendet werden, kann die **Cookie-Kontrolle** zu Beginn sehr oft nachfragen. Sobald Sie die von Ihnen regelmäßig besuchten Seiten in die Regelliste aufgenommen haben, wird Ihr Surfen im Internet aber wieder wie zuvor sein.

Jede erstellte Regel kann später über den Reiter **Cookies** aufgerufen und weiter bearbeitet werden.

Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

10.5.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 - Domäne(n) und Aktion auswählen

Domäne(n) und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

Aktion	Beschreibung
Zulassen	Das Cookie dieser Domäne wird ausgeführt.
Verweigern	Das Cookie dieser Domäne wird nicht ausgeführt.

- **Richtung** - Wählen Sie die Richtung des Datenverkehrs aus.

Typ	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf Cookies, welche von der verbundenen Seite versendet werden.
Eingehend	Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden.

Typ	Beschreibung
Beide	Die Regeln finden in beide Richtungen Anwendung.

Klicken Sie auf **Fertigstellen**.

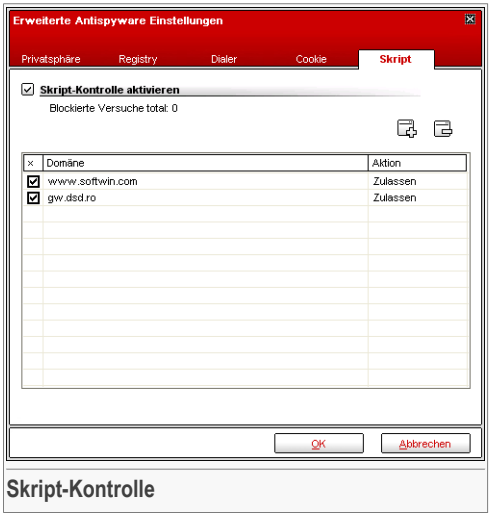
Anmerkung

Sie können Cookies akzeptieren, diese aber nicht zurücknehmen, indem Sie die Aktion **Verweigern** und die Richtung **Ausgehend** angeben.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.6. Erweiterte Einstellungen

Um diesen Bereich zu bearbeiten klicken Sie **Erweiterte AntiSpyware Einstellungen** (gehen Sie auf **Antispyware** module, Status und klicken **Erweiterte Einstellungen**) und klicken den Reiter **Script**.



Skript-Kontrolle

Skripte und andere Programmierungen, wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten

versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

BitDefender ermöglicht Ihnen die Auswahl solche Elemente zuzulassen oder deren Ausführung zu blockieren.

Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. BitDefender wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:

Skript Alarm

Der Namen der Quelle wird Ihnen angezeigt.

Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Falls die gleiche Seite erneut Ihren aktiven Inhalt versenden will, werden Sie nicht wieder informiert.

Jede erstellte Regel kann später über den Reiter **Skripte** aufgerufen und weiter bearbeitet werden.

Wichtig

Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Fenster „Alarm“) oder manuell (bitte klicken Sie dazu **Hinzufügen**) erstellt werden und wählen Sie dann die entsprechenden Parameter aus.

10.6.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 - Adresse und Aktion auswählen

Adresse und Aktion auswählen

Hier können Sie die Parameter auswählen:

- **Domäne angeben** - schreiben Sie die Domäne, auf welche die Regel angewendet werden soll, in das darunter stehende Feld.
- **Aktion** - wählen Sie die Aktion der Regel.

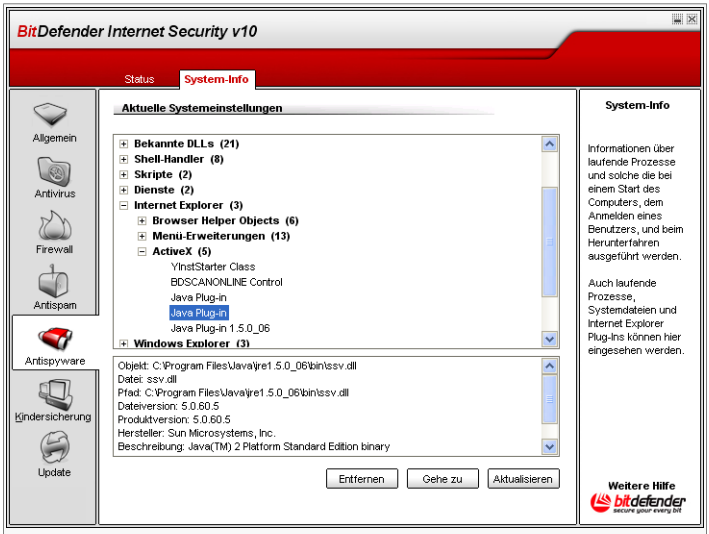
Aktion	Beschreibung
Zulassen	Die Scripts auf dieser Domäne werden ausgeführt.
Verweigern	Die Scripts auf dieser Domäne werden nicht ausgeführt.

Klicken Sie auf **Fertigstellen**.

Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.7. System-Informationen

Um diese Sektion zu öffnen klicken Sie bitte auf **System-Info** im Modul **Antispyware**.



System-Informationen

In diesem Bereich können Sie Ihre Basiseinstellungen einsehen und verändern.

Die Auflistung enthält alle Einstellungen die angewendet werden, sowohl wenn der Computer gestartet wird als auch wenn spezielle Anwendungen aufgerufen werden und gesonderte Regeln besitzen.

Drei Schaltflächen sind verfügbar:

- **Löschen** - löscht das ausgewählte Objekt.
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt.
- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.

11. Das Modul Kindersicherung

Der Abschnitt **Kindersicherung** behandelt und erklärt folgende Themen:

- Status der Kindersicherung
- Webseiten-Kontrolle
- Programm-Kontrolle
- Webseiten-Kontrolle
- Zeitplan

Anmerkung

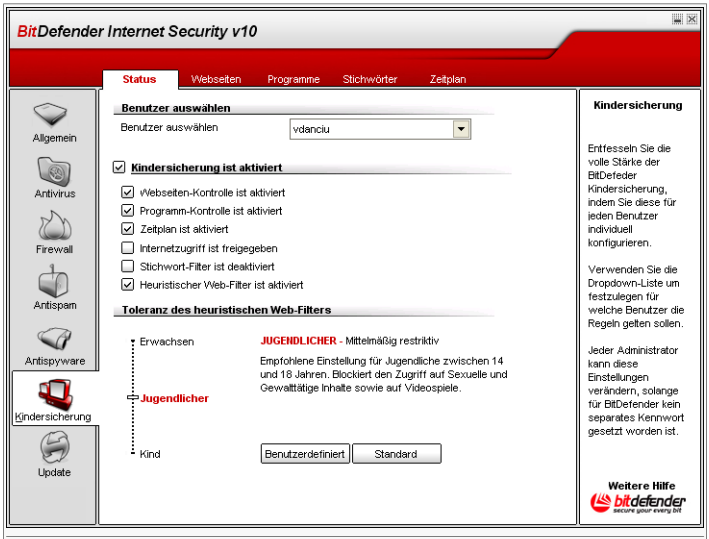
Weitere Inhalte und Einzelheiten zum Modul **Kindersicherung** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Kindersicherung*“ (S. 34).

Wichtig

Dieses Modul kann nur von Anwendern mit Administratoren Rechten bearbeitet und konfiguriert werden (System Administratoren). Wenn die Einstellungen Passwort geschütz sind, können Sie nur mit Passwort geändert werden. Ein Administrator kann keine Regeln für einen Anwender aufstellen, für den schon vorher von einem anderen Administrator Regeln aufgestellt worden sind.

11.1. Status der Kindersicherung

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Kindersicherung**.



Status der Kindersicherung

In dieser Sektion können Sie die **Kindersicherung** konfigurieren und Sie können für auswählte Nutzer das Level für den Schutz festlegen.

Wichtig

Lassen Sie die **Kindersicherung** aktiviert, um Ihre Kinder gegen Jugendgefährdende Internet Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.

Anmerkung

Falls Sie nicht die einzige Person sind, die diesen Computer verwendet, empfehlen wir, Ihre BitDefender–Einstellungen mit einem Kennwort zu schützen. Um ein Kennwort einzurichten, wechseln Sie bitte zum Modul **Allgemein**, starten Sie den Bereich Einstellungen und aktivieren Sie die Option **BitDefender per Kennwort schützen**.

Um die Regeln für den gewünschten Schutz zu konfigurieren müssen Sie zunächst den Anwender auswählen, für den diese Regeln gelten sollen. Anschließend können Sie folgende Level für den Schutz konfigurieren:

- Klicken Sie **Sperren**, um den Zugriff aller Webseiten zu sperren (damit sind nicht nur die Web-Seiten gemeint, die unter der Sektion Web-Seiten angegeben sind).

- **Anwendungen** - enable **Anwendungen** um Zugang zu Anwendungen auf Ihrem Computer zu blockieren, gemäß den Regeln, die Sie unter Applications angelegt haben.
- **Web Time Limiter** - aktivieren **Web Time Limiter** um den Zugang zum Internet zeitlich einzugrenzen klicken Sie Zeit begrenzen.
- Klicken Sie **Sperren**, um den Zugriff aller Webseiten zu sperren (damit sind nicht nur die Web-Seiten gemeint, die unter der Sektion Web-Seiten angegeben sind).
- **Keyword Filtering** - aktivieren **Keyword Filtering** um Internet Inhalte und Mails zu filtern gemäß Ihren Regeln klicken Sie Keywords.
- **Heuristic web filter** - aktivieren Sie diese Option um den Internet Zugang zu filtern gemäß den Regeln, die auf dem Alter der Anwender basieren.

11.1.1. Heuristischer Filter

Ziehen Sie den Zeiger an der Scala entlang um das Level für den gewünschten Schutz einzustellen, den Sie für den Anwender für angemessen halten.

Es gibt 3 mögliche Einstellungen:

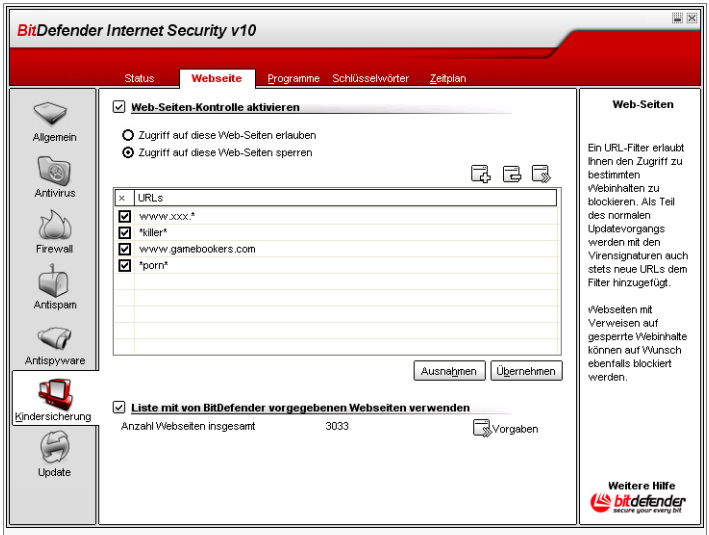
Sicherheitseinstellung	Beschreibung
Kind	Bietet eingeschränkten Zugriff auf das Internet, gemäß den Empfehlungen für Anwender unter 14 Jahren. Internet Seiten mit möglicherweise schädlichen Inhalten für Kinder (Porno Seiten, Sex Seiten etc.) werden blockiert.
Teenager	Bietet eingeschränkten Zugriff auf das Internet, gemäß den Empfehlungen für Anwender von 14 bis 18 Jahren. Internet Seiten mit sexuellen oder pornographischen Inhalten werden blockiert.
Erwachsen	Bietet uneingeschränkten Zugang zum Internet unabhängig von den Inhalten der Internetseiten.

Falls Sie einen anderen Ordner wählen wollen, klicken Sie auf **Durchsuchen** und ein neues Fenster wird geöffnet, wo Sie einen neuen Ordner wählen können. Klicken Sie auf **Weiter**.

Klicken Sie auf **Standard Einstellung**, um den Zeiger auf die Standard Einstellung zu ziehen.

11.2. Webseiten-Kontrolle

Um diese Sektion zu öffnen klicken Sie bitte auf **Web** im Modul **Kindersicherung**.



Webseiten-Kontrolle

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

Um diese Funktion zu aktivieren, setzen Sie bitte das entsprechende Häkchen in der Checkbox analog zu **Webseiten-Kontrolle aktivieren**.

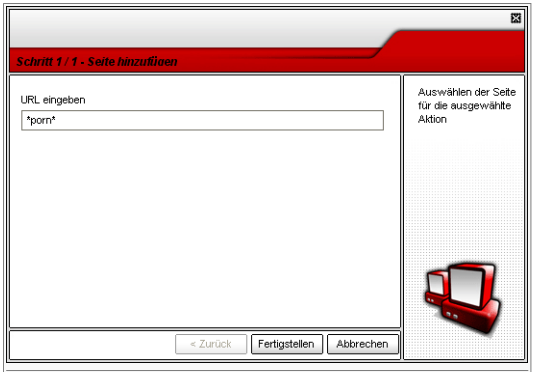
Wählen Sie die entsprechende Häkchenbox analog zu **Zugriff auf diese Webseiten erlauben/Zugriff auf diese Webseiten sperren** um Zugriffe zu erlauben oder zu verweigern. Die Web-Seiten werden wie folgt definiert.

Wählen Sie die entsprechende Häkchenbox analog zu **Zugriff auf diese Webseiten erlauben/Zugriff auf diese Webseiten sperren** um Zugriffe zu erlauben oder zu verweigern. Die Web-Seiten werden wie folgt definiert.

11.2.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 – Definieren der Webseiten



Definieren von Webseiten

Klicken Sie **Hinzufügen** und geben Sie den Namen der Webseite ein, auf die die oben genannten Regeln zutreffen sollen. Danach klicken Sie bitte **Übernehmen**.

Wichtig

Syntax:

- `<*.xxx.com>` - die definierte Regel trifft auf alle Webseiten mit dem Suffix `<.xxx.com>` zu;
- `<*porn*>` - die definierte Regel trifft auf alle Webseiten zu, die das Wort `<porn>` in der Webadresse verwenden;
- `<www.*.com>` - die definierte Regel trifft auf alle Webseiten mit dem Suffix `<com>` zu;
- `<www.xxx.*>` - die definierte Regel trifft auf alle Webseiten mit Namen `<www.xxx.>` zu, ohne Rücksicht auf den Suffix;

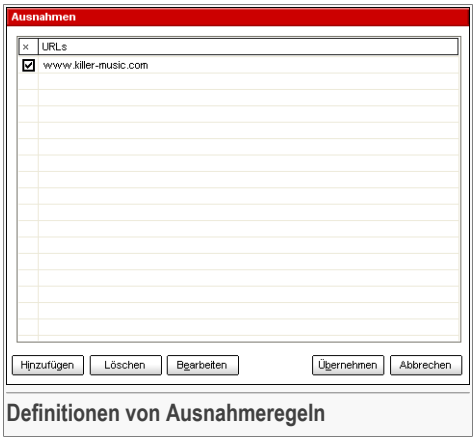
Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

11.2.2. Definitionen von Ausnahmeregeln

Manchmal müssen Sie für eine bestimmte Regel Ausnahmen definieren. Zum Beispiel, erstellen Sie eine Regel, die Seiten mit dem Begriff "killer" blockiert in der Adresse (syntax: `*killer*`). Sie kennen aber auch eine Seite die heißt `killer-music` wo Anwender online Musik hören können. Um eine Ausnahme zu der festgesetzten Regel zu machen , gehen Sie auf **Ausnahme** und definieren Sie die Ausnahme von der Regel.

Klicken Sie **Ausnahmen...**. Ein weiteres Fenster wird angezeigt:



Definitionen von Ausnahmeregeln

Klicken Sie **Hinzufügen...** um Ausnahmen festzulegen. Der configuration Assistent erscheint. Schließen Sie den Assistenten ab, um die Ausnahme festzulegen..

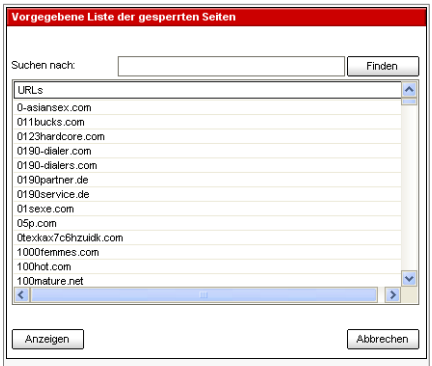
Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Um eine Regel zu löschen, klicken Sie bitte **Löschen**. Um eine Regel zu verändern, wählen Sie die entsprechende Web-Seiten und klicken Sie auf **Bearbeiten**, oder nutzen Sie den Doppelklick. Um eine Regel kurzzeitig zu deaktivieren, ohne sie zu löschen, markieren Sie die entsprechenden Funktion in der Checkbox.

11.2.3. BitDefender Schwarze Liste Internet

Um Ihnen zu helfen Ihre Kinder zu schützen stellt BitDefender Schwarze Listen von Internetseiten zur Verfügung, die unangemessene oder gefährliche Inhalte haben. Um die Seiten auf dieser Liste zu blockieren wählen Sie **Nutzen der von BitDefender bereitgestellten Liste**.

Sie können die Anzahl der blockierten Seiten sehen. Um die Seiten zu sehen klicken Sie **Liste Standardeinstellung**. Das folgende Fenster erscheint:



BitDefender Schwarze Liste Internet

Wählen Sie eine Seite aus und klicken Sie **Seite ansehen**um den Inhalt zu sehen.

Wenn Sie eine Seite blockieren wollen, schauen Sie erst auf der Schwarzen Liste nach. Geben Sie die Adresse oder die ersten Buchstaben in das Bearbeitungsfeld ein und klicken Sie **Finden**. Wenn der String einem Eintrag entspricht, wird der Eintrag angezeigt.

11.3. Programm-Kontrolle

Um diese Sektion zu öffnen klicken Sie bitte auf **Anwendungen** im Modul **Kindersicherung**.

Programm-Kontrolle

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.

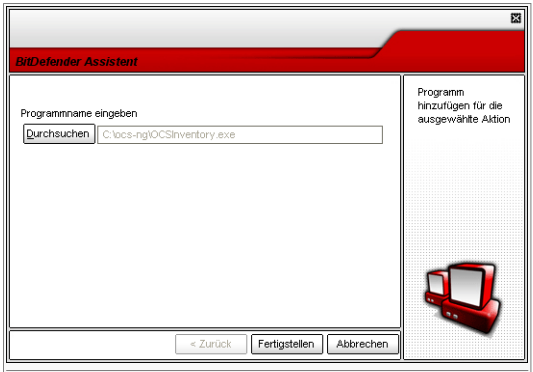
Um diese Funktion zu aktivieren, markieren Sie die entsprechende Funktion in der Häkchenbox analog zu **Programm-Kontrolle aktivieren**.

Die Regeln müssen von Hand eigegeben werden. Klicken Sie **Hinzufügen...** um den Assistenten zu starten.

11.3.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 – Auswahl der zu sperrenden Anwendung



Auswahl der zu sperrenden Anwendung

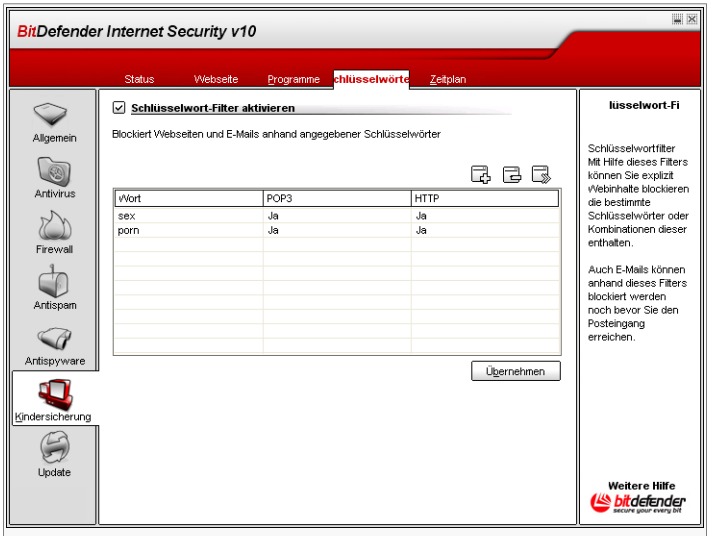
Klicken Sie bitte **Hinzufügen**, dann **Durchsuchen** und wählen Sie dann die zu sperrende Anwendung. Danach klicken Sie **Übernehmen**.

Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

11.4. Filtern nach Schlüsselwörtern

Um diese Sektion zu öffnen klicken Sie bitte auf **Schlüsselwörter** im Modul **Kindersicherung**.



Filtern nach Schlüsselwörtern

Der **Schlüsselwort Filter**hilft Ihnen Internet Seiten oder E-Mail zu blockieren, die bestimmte Wörter enthalten. Auf diesem Weg können Sie Anwender vor unangemessenen Wörtern und Sätzen schützen.

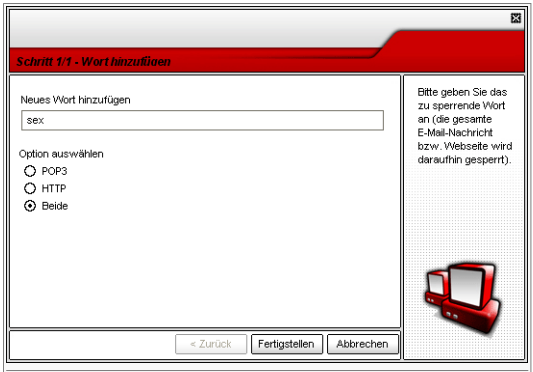
Um diese Funktion zu aktivieren, setzen Sie bitte das entsprechende Häkchen in der Checkbox analog zu **Web-Seiten-Kontrolle aktivieren**.

Die Regeln müssen von Hand eigegeben werden. Klicken Sie **Hinzufügen...** um den Assistenten zu starten.

11.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Kennwort eingeben



Kennwort bestätigen

Hier können Sie die Parameter auswählen:

- **Schlüsselwort** - Geben Sie im Bearbeitungsfeld das Wort oder den Satz ein, den Sie blockieren möchten.
- **Protokoll** - wählen Sie das Protokoll, dass BitDefender für spezielle Begriffe prüfen soll.

  Folgende Optionen stehen zur Verfügung:

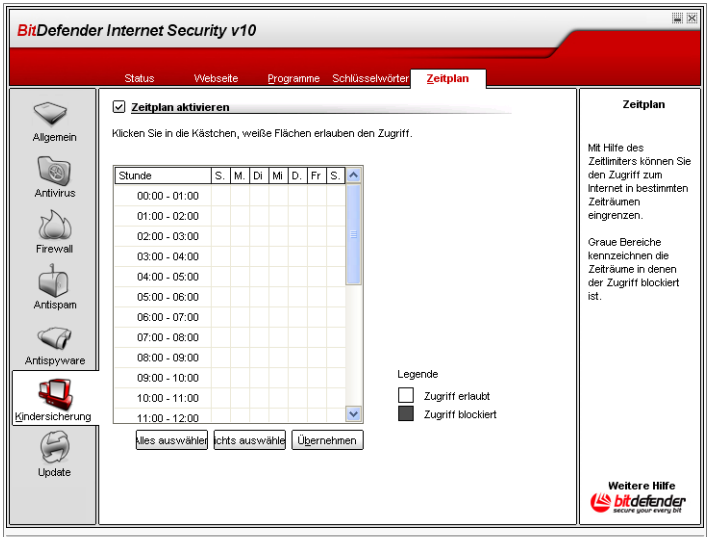
Option	Beschreibung
POP3	E-Mail Nachrichten, die das Schlüsselwort enthalten werden blockiert.
HTTP	Internet Seiten, die Schlüsselwörter enthalten, werden geblockt.
Beide	Sowohl E-Mail Nachrichten als auch Internet Seiten, die Schlüsselwörter enthalten werden geblockt.

Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Um eine Regel zu löschen, markieren Sie diese Regel und klicken Sie **Löschen**. Im der **Detailansicht** können Sie alle definierten Regeln löschen, in dem Sie **Alle löschen** klicken. Um Regeln zu modifizieren, wählen Sie die entsprechende Regel aus und klicken Sie **Regel editieren**. Um eine Regel zeitweise außer Kraft zu setzen ohne sie zu löschen, markieren Sie dies bitte über die entsprechende Checkbox.

11.5. Zeitplan

Um diese Sektion zu öffnen klicken Sie bitte auf **Zeitplan** im Modul **Kindersicherung**.



Zeitplan

Dieser **Zeitplan** erlaubt Ihnen, den Zugriff zum Internet über Personen oder Programme zeitlich zu bestimmten.

Anmerkung

BitDefender arbeitet unabhängig von dieser zeitlichen Begrenzung konstant im Hintergrund und lädt alle neu verfügbaren Updates.

Um diese Schutzfunktion zu aktivieren, setzen Sie bitte das entsprechende Häkchen in der Häkchenbox analog zu **Zeitplan aktivieren**.

Wählen Sie dann die entsprechenden Zeitintervalle, in denen das Internet gesperrt werden soll, aus. Sie können einzelne, kleine Intervalle wählen, oder über Klicken und Herüberziehen längere Zeitfenster definieren. Sie können ebenso **Alle auswählen** auswählen, um vorbehaltlos den Zugriff auf Webseiten zu sperren. Wenn Sie **Nichts auswählen** anklicken ist der Zugriff auf Webseiten jederzeit erlaubt.

Wichtig

Die grau markierten Fenster entsprechen den Zeitintervallen, in denen alle Internetaktivitäten gesperrt sind.

Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

12. Das Modul Update

Der Abschnitt **Update** behandelt und erklärt folgende Themen:

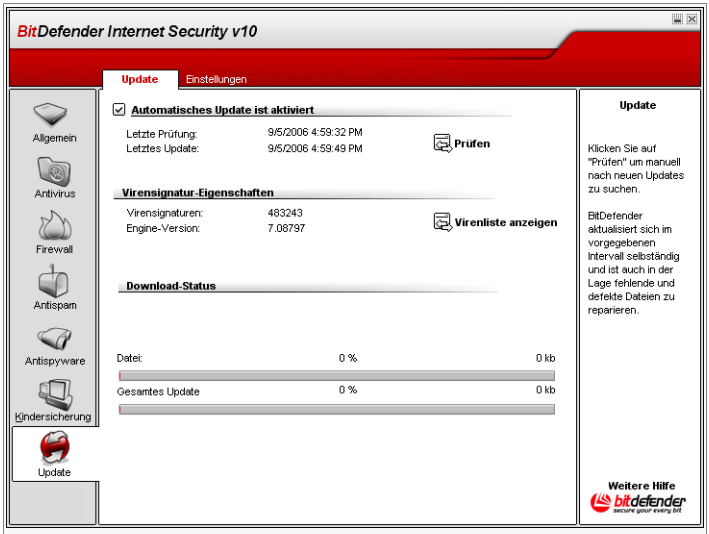
- Automatisches Update
- Manuelles Update
- Update-Einstellungen

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Update** finden Sie in der Produktbeschreibung auf Seite „*Das Modul Update*“ (S. 34).

12.1. Automatisches Update

Um diese Sektion zu öffnen klicken Sie bitte auf **Update** im Modul **Update**.



Automatisches Update

Hier finden Sie eine Übersicht über den Produkt-Status.

Wichtig

Um den Schutz vor Spyware aus dem Internet zu gewährleisten, halten Sie Ihre **Automatisches Update** Funktion jederzeit aktiviert.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet BitDefender eigenständig. Es prüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und fährt nach Bedarf sogar **stündliche** Updates.

Wenn ein neues Update verfügbar ist, handelt BitDefender je nach vorgenommener Einstellung im Menü Einstellungen. Entweder werden Sie darum gebeten, den neu verfügbaren Download jetzt herunter zu laden oder das Update erfolgt automatisch.

Das automatische Update kann auch jederzeit über den Klick **Prüfen** erfolgen. Diese Funktion wird auch als **benutzergesteuertes Update** bezeichnet.

Das **Update** module Modul verbindet Ihren Computer mit dem BitDefender Update Server und benachrichtigt Sie bei einem neu verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder darum gebeten, das Update Download jetzt herunter zu laden, oder das Update erfolgt automatisch.

Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.

Anmerkung

Falls Sie über eine Internet by Call Verbindung verfügen, ist es sinnvoll, regelmäßig ein manuelles Update durchzuführen. Diese Vorgehensweise sollten Sie sich dann zu Eigen machen.

Sie können ein BitDefender Signaturen Update durchführen indem Sie klicken auf **Viren Liste**. Eine HTML Datei zeigt alle erstellten Signaturen. Klicken Sie noch mal **Viren Liste** um die Liste einzusehen. Sie können die Datenbank auf spezifische Signatur hin durchsuchen oder klicken Sie **BitDefender Virus Liste** um auf die online BitDefender Signaturen Datenbank zu gehen.

12.2. Manuelles Update

Diese Methode erlaubt Ihnen, durch die Installation der neusten Virensignaturen den bestmöglichen Virenschutz zu erhalten. Für die Installation des neusten Produktupdates wählen Sie bitte das automatische Update.

Wichtig

Nutzen Sie das manuelle Update, wenn das automatische Update nicht durchgeführt werden kann oder wenn der Computer nicht mit dem Internet verbunden ist.

Es gibt zwei mögliche Varianten, ein manuelles Update durchzuführen:

- Mit einer `weekly.exe` Datei;
- Mit einem `zip Archiv`.

12.2.1. Das manuelle Update mit der `weekly.exe` Datei

Das Update Paket `weekly.exe` wird jeden Freitag frei geschaltet und enthält alle neuen Virusdefinitionen und Prüfmechanismen bis zum Freigabedatum.

Um das BitDefender Update über die Datei `weekly.exe`, durchzuführen, folgen Sie den nächsten Schritten:

1. Herunterladen der weekly.exe und speichern dieser Datei lokal auf Ihrer Festplatte.
2. Rufen Sie die herunter geladene Datei auf und mit einem Doppelklick rufen Sie den Update Assistenten auf.
3. Klicken Sie auf **Weiter**.
4. Überprüfen Sie **Ich akzeptiere die Lizenzvereinbarungen** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Installieren**.
6. Klicken Sie auf **Fertigstellen**.

12.2.2. Das manuelle Update per `ZIP Archiv`

Auf dem Update-Server sind zwei Zip-Archive abgelegt, die die Updates für die Scan-Module bzw. für die Virensignaturen enthalten: `cumulative.zip` und `daily.zip`.

- Der `cumulative.zip` wird jede Woche montags veröffentlicht und beinhaltet alle neuen Virus Definitionen und Prüfmechanismen bis zum Datum der Veröffentlichung.
- Der `daily.zip` wird jeden Tag veröffentlicht und enthält alle neuen Virus Definitionen und Prüfmechanismen ausgehend von der letzten, erfolgten Zusammenstellung bis zum aktuellen Tag.

BitDefender verwendet eine servicebasierte Architektur. Aufgrund dieser Vorgehensweise ist die Erneuerung der Viren-Definitionen abhängig vom Betriebssystem:

- Windows 2000, Windows XP.

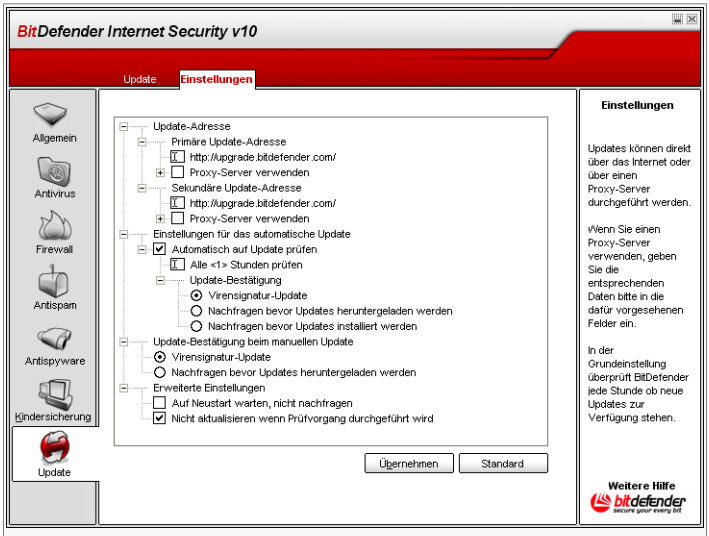
Windows 2000, Windows XP

Gehen Sie wie folgt vor:

1. **Herunterladen des richtigen Updates.** Laden Sie montags die Datei cumulative.zip herunter, und speichern Sie das Archiv auf der Festplatte. Laden Sie an anderen Tagen die Datei daily.zip herunter, und speichern Sie das Archiv auf der Festplatte. Wenn Sie zum ersten Mal ein manuelles Update durchführen, laden Sie beide Archive herunter.
2. **Beenden der BitDefender Virusschutzfunktion.**
   - **Verlassen Sie bitte die BitDefender Management Konsole.** Klicken Sie auf das BitDefender Symbol in der Systemleiste, und wählen Sie die Option **Beenden**.
   - **Öffnen der Dienste.** Klicken Sie auf **Starten**, dann auf **Systemsteuerung**, doppelklicken Sie auf **Verwaltung**, und klicken Sie auf **Dienste**.
   - **Stoppen des BitDefender Virus Schild.** Wählen Sie den Service **BitDefender Virus Schild** aus der angezeigten Liste und klicken sie auf **Stoppen**.
   - **Stoppen der BitDefender Scan Server.** Wählen Sie den Service **BitDefender Scan Server** aus der angezeigten Liste und klicken Sie auf **Stoppen**.
3. **Extrahieren der Archivinhalte.** Starten Sie bitte mit dem Archiv `cumulative.zip` sobald beide Archive verfügbar sind. Extrahieren Sie die Inhalte in das Verzeichnis `?:\Program Files\Common Files\Softwin\AV\Plugins` und bestätigen Sie das Überschreiben der bestehenden Dateien.
4. **Starten Sie den BitDefender Virenschutz wieder.**
   - **Starten des BitDefender Scan Server.** Wählen Sie **BitDefender Scan Server** in der angezeigten Liste und klicken Sie **Starten**.
   - **Starten des BitDefender Virus Schild.** Wählen Sie **BitDefender Virus Schild** von der angezeigten Liste und klicken Sie **Starten**.
   - **Öffnen Sie die BitDefender Management-Konsole.**

12.3. Update-Einstellungen

Um diese Sektion zu öffnen klicken Sie bitte auf **Update** im Modul **Einstellungen**.



Update-Einstellungen

Die Updates können im lokalen Netzwerk, über das Internet, direkt oder über einen Proxy-Server durchgeführt werden.

Das Fenster mit den Update-Einstellungen enthält 4 aufklappbare Optionskategorien (**Update-Adresse**, **Automatisches Update**, **Update-Bestätigung beim manuellen Update** und **Erweiterte Einstellungen**), ähnlich wie in den Windowsmenüs.

Anmerkung

Klicken Sie auf eine Box mit einem "+", um ein Menü auszuklappen, und auf ein "-", um es zu schließen.

12.3.1. Update-Adresse

Für ein zuverlässigeres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Die folgenden Optionen sind verfügbar:

- **Ablagebereich für Updates** - bei einer Verbindung mit einem lokalen Netzwerk, in dem BitDefender Virendefinitionen lokal abgelegt werden, können Sie mit dieser Option den Pfad zum Ablageordner ändern. Standardmäßig lautet der Pfad: http://upgrade.bitdefender.com.

- **Proxy-Server verwenden** - Falls Sie einen Proxy-Server einsetzen, muss die entsprechende Markierung gesetzt werden. Nehmen Sie dann folgende Einstellungen vor:
  - **Adresse** - Geben Sie hier die IP-Adresse oder den Hostnamen des Proxy-Servers ein, den BitDefender verwendet.

    Wichtig

    Syntax: `name:port` oder `ip:port`.

  - **Benutzername** - Geben Sie den Benutzernamen ein, wenn der Proxy-Server eine Anmeldung erfordert.

    Wichtig

    Syntax: `domain\user`.

  - **Kennwort** - Geben Sie das Kennwort ein, wenn der Proxy-Server eine Anmeldung mit Kennwort erfordert.

12.3.2. Automatisches Update

- **Automatisch auf Update prüfen** - BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind.
- **Alle (1) Stunden prüfen** - Definiert, wie oft auf verfügbare Updates geprüft werden soll. Standard ist 1 Stunde.
- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.
- **Vor der Installation fragen** - BitDefender informiert den Benutzer vor der Installation neuer Updates.

Wichtig

Wenn Sie die Optionen **Vor dem Herunterladen fragen** oder **Vor der Installation fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden automatische Updates nicht durchgeführt.

12.3.3. Update-Bestätigung beim manuellen Update

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.

Wichtig

Wenn Sie die Optionen **Vor dem Herunterladen fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden manuelle Updates nicht durchgeführt.

12.3.4. Erweiterte Einstellungen

- **Auf Neustart warten, nicht nachfragen** - Mit der Aktivierung dieser Einstellung wird der Benutzer nicht gefragt, ob ein Update durch Neustart durchgeführt werden soll. Somit wird der Benutzer während der Arbeit nicht durch BitDefender unterbrochen. Ohne Aktivierung teilt BitDefender mit, dass ein Update den Neustart des Computers benötigt und fragt den Benutzer ob der Neustart nun durchgeführt werden soll.
- **Nicht aktualisieren wenn Prüfvorgang durchgeführt wird** - BitDefender kann während des Prüfvorganges kein Update durchführen. Auf diese Weise kann der Update-Vorgang den Prüfvorgang nicht beeinflussen.

Anmerkung

Sollte BitDefender während eines Prüfvorganges aktualisiert werden, wird der Prüfvorgang abgebrochen.

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

Empfohlene Vorgehensweisen

13. Empfohlene Vorgehensweisen

Der Abschnitt **Tipps und Tricks** behandelt und erklärt folgende Themen:

- Wie Sie Ihren Computer im Internet schützen können
- AntiVirus
- Konfigurieren der Prüfung
- Konfigurieren der Firewall
- Wie Sie Ihren Computer von Spam freihalten
- Wie Sie Ihre Kinder vor unangemessenen Inhalten schützen

13.1. Wie Sie Ihren Computer im Internet schützen können

Folgen Sie diesen Schritten um Ihren Computer im Internet zu schützen:

1. **Beenden Sie den Installations-Assistenten.** Während der Installation erscheint der Installations-Assistent. Dieser wird Ihnenhelfen BitDefender zu registrieren und ein Benutzerkonto einzurichten, um vom Technischen Support zu profitieren. Er hilftaußerdem dabei zu prüfen, ob Ihr System sicher ist, indem ein Update und eine schnelle Systemprüfung gestartet wird. Es erlaubt ebenso eine tägliche komplette Systemprüfung.

   Wichtig

   Wenn Sie eine BitDefender Notfall CD haben, prüfen Sie Ihr System vor der Installation von BitDefender um sicher zu stellen, dass sich keine schädliche Software auf Ihrem Computer versteckt.

2. **Wie kann ich BitDefender aktualisieren?** Wenn Sie den Installations-Assistenten nicht beendet haben, starten Sie ein Update auf Anforderung (gehen Sie auf **Update** Modul, Update section, und klicken Sie **Jetzt Updaten**).

3. **Wie kann ich einen Prüfvorgang starten?** Gehen Sie in das Modul **Antivirus**, Shieldund klicken Sie **Jetzt prüfen**.

   Anmerkung

   Klicken Sie auf Prüfen um eine vollständige Systemprüfung zu starten und wählen Sie dort den Reiter **vollständige System Prüfung** und prüfen Sie **Aufgabe ausführen**.

4. **Infektion abwehren.** Halten Sie im Bereich **Virus Schild** die Option Echtzeit-Schutz aktiviert um in Echtzeit vor Schädlingen geschützt zu sein. Stellen Sie das Schutzlevel gemäß Ihren Bedürfnissen ein. Des weiteren können Sie auf Anpassen klicken um die Stufe selbst zu definieren.

   Wichtig

   Programmieren Sie den BitDefender Virenschutz so, dass Ihr System mindestens einmal pro Woche gescannt wird. Entsprechende Anleitungen finden Sie in diesem Handbuch unter „*Zeitgesteuertes Starten von Prüfvorgängen*“ (S. 73).

5. **Halten Sie Ihr BitDefender-Produkt auf dem neuesten Stand.** Im Modul **Update**, Update , aktiviern Sie bitte das **Automatische Update**ein, um optimal gegen die neuesten Bedrohungen geschützt zu sein.
6. **Internet Bedrohungen abwehren.** Konfigurieren der BitDefender Firewall um gegen Bedrohungen aus dem Internet geschützt zu sein.
7. **Spyware blockieren.** Im Modul **Antispyware**, Status aktivieren Sie diesen Schutz. Die empfohlene Sicherheitsstufe sollte eingestellt werden. So sind Sie gegen illegale Programme geschützt, die versuchen Registry-Einträge zu ändern und kostenpflichtige Einwahlprogramme (Dialer) installieren. Wenn Sie Ihre vertraulichen Daten sichern möchten aktivieren Sie Privacy Control und erstellen Sie entsprechende Regeln.
8. **Spam abwehren.** Wenn Sie Ihr E-Mail Account schützen möchten gehen Sie zu Konfigurieren Antispam.
9. **Zugang zu unangemessenen Inhalten blockieren.** Wenn Ihre Kunden den Computer nutzen, sollten Sie sie vor unangemessenen Inhalten schützen indem Sie auf Konfigurieren gehen und im Modul Kindersicherung.

13.2. Wie Sie Ihren Computer vor Malware Attacken schützen

Folgen Sie diesen Schritten, um Ihren Computer gegen Viren, Spyware und andere Malware zu schützen.

1. **Beenden Sie den Installations-Assistenten.** Während der Installation erscheint der Installations-Assistent. Dieser wird Ihnenhelfen BitDefender zu registrieren und ein Benutzerkonto einzurichten, um vom Technischen Support zu profitieren. Er hilftaußerdem dabei zu prüfen, ob Ihr System sicher ist, indem ein Update und eine schnelle Systemprüfung gestartet wird. Es erlaubt ebenso eine tägliche komplette Systemprüfung.

Wichtig

Wenn Sie eine BitDefender Notfall CD haben, prüfen Sie Ihr System vor der BitDefender-Installation um sicher zu stellen, dass sich keine schädliche Software auf Ihrem Computer versteckt.

2. **Wie kann ich BitDefender aktualisieren?** Wenn Sie den Installations-Assistenten nicht beendet haben, starten Sie ein Update auf Anforderung (gehen Sie auf **Update** Modul, Update section, und klicken Sie **Jetzt Updaten**).
3. **Wie kann ich einen Prüfvorgang starten?** Gehen Sie in das Modul **Antivirus**, Shieldund klicken Sie **Jetzt prüfen**.

Anmerkung

Klicken Sie auf Prüfen um eine vollständige Systemprüfung zu starten und wählen Sie dort den Reiter **vollständige System Prüfung** und prüfen Sie **Aufgabe ausführen**.

4. **Infektion abwehren.** Halten Sie im Bereich **Virus Schild** die Option Echtzeit-Schutz aktiviert um in Echtzeit vor Schädlingen geschützt zu sein. Stellen Sie das Schutzlevel gemäß Ihren Bedürfnissen ein. Des weiteren können Sie auf Anpassen klicken um die Stufe selbst zu definieren.

Wichtig

Programmieren Sie den BitDefender Virenschutz so, dass Ihr System mindestens einmal pro Woche geprüft wird. Entsprechende Anleitungen finden Sie in diesem Handbuch unter „*Zeitgesteuertes Starten von Prüfvorgängen*“ (S. 73).

5. **Halten Sie Ihr BitDefender-Produkt auf dem neuesten Stand.** Im Modul **Update**, Update , aktiviern Sie bitte das **Automatische Update**ein, um optimal gegen die neuesten Bedrohungen geschützt zu sein.
6. **Eine komplette Systemprüfung planen.** Gehen Sie auf **Prüfen** und starten Sie BitDefender System Prüfung wenigstens einmal die Woche Planen the **Systemprüfung**

13.3. Konfiguration einer Prüfung

So richten Sie einen zeitgesteuerten Scanvorgang ein:

1. **Neue Aufgabe erstellen.** Im Abschnitt Prüfen und klicken Sie auf **Neue Aufgaben**. Das Fenster Einstellungen erscheint.

Anmerkung

Sie können auch neue Aufgaben erstellen mit Kopieren mit Hilfe einer bereits vorhandenen. Um das zu tun, gehen Sie mit dem rechten Mausklick auf Aufgabe und wählen Sie **Kopieren**im Shortcut menu. Doppelklick auf öffnen im Fenster **Eigenschaften**.

2. **Einstellen des Levels.** Gehen Sie in den Abschnitt **Übersicht** um den Level einzustellen. Wenn Sie möchten können Sie das Level anpassen unter Anpassen **Anpassen**.
3. **Weiterhin müssen Sie die Prüfart auswählen:** Gehen Sie im Abschnitt**Prüfpfad** auf auf wählen Sie die Objekte, die Sie prüfen wollen.
4. **Zeitgesteuerte Aufgaben.** Wenn die Aufgabe umfassend ist, sollten Sie die Prüfung auf später verschieben, wenn Ihr Computer im Stand-By Modus ist. Das gewährt eine korrekte Prüfung Ihres Systems durch BitDefender. Gehen Sie auf **Planen** zu Prüfung planen.

13.4. Wie Sie das Firewall Modul konfigurieren

Um die **Firewall** zu konfigurieren, folgen Sie bitte den nächsten Schritten:

1. **Erstellen Sie ein Netzwerk Profil.** Jedesmal, wenn Sie sich ins Netzwerk einwählen erscheint Assistent. Beenden Sie den Firewall Assistenten um eine Reihe von Regeln für Ihr Netzwerk Profil einzurichten.

   Anmerkung

   Sie können den Assistenten jederzeit aufrufen unter **Profil rekonfigirieren** im Abschnitt Datenverkehr.

2. **Einstellen des aggressivsten Levels.** Im Abschnitt **Status** gehen Sie auf Erstellen der Regeln für die Firewall (**Alle ablehnen**, **Alle erlauben**, **Alle der Freundesliste erlauben** , **Fragen**).

   Wichtig

   Wir empfehlen die Einstellung **Alle auf der Whitelist erlauben**. Auf diesem Weg erstellt BitDefender Regeln für die gängigsten Anwendungen ohne Sie zu stören.

3. **Regeln erstellen.** Gehen Sie in den Abschnitt **Datenverkehr**, klicken Sie dort auf **Hinzufügen** um Regeln zu erstellen für die am häufigsten genutzten Anwendungen. Sie müssen die Parameter definieren.

4. **Erweiterte Firewall Einstellungen.** Gehen Sie auf **Erweitert** und definieren Sie im Abschnitt Filter Regeln für den ICMP Datenverkehr und oder Firewall Einstellungen.

13.5. Wie Sie Ihren Computer Spam frei halten

Um einen spamfreien Computer zu generieren, folgen Sie bitte den nächsten Schritten:

1. **Einstellen des aggressivsten Levels.** Im Abschnitt **Antispam**, Status können Sie die Toleranz einstellen. Wählen Sie die passende Stufe aus, das alle Ihre erlaubten E-Mails im Posteingang zuläßt, gleich ob Sie eine große Zahl an erlaubten, kommerziellen Mails erhalten oder ein hohes Volumen an Spam.
2. **Konfigurationsassistent.** Bei Verwendung von Microsoft Outlook oder Outlook Express bzw. Windows Mail folgen Sie bitte dem Konfigurationsassistenten, der sich beim erstmaligen Start des E-Mail-Programms öffnet. Sie können den Assistenten auch über das Menü *„AntiSpam Symbolleiste“* (S. 119) öffnen.
3. **Ausfüllen der Freundesliste.** Um die **Freundesliste** zu handhaben, klicken Sie auf (übereinstimmend mit Ihrer **Freundesliste**) oder klicken Sie auf den **Freunde**-Button vom *„AntiSpam Symbolleiste“* (S. 119). Fügen Sie die Adressen der Leute hinzu deren E-Mails Sie auf jeden Fall erreichen sollen. Friends list.

   Anmerkung

   BitDefender blockiert keine Nachrichten dieser Absender. Somit stellt die Liste der Freunde sicher, dass alle legitimen Nachrichten auch ankommen.

4. **Trainieren des Bayesianischen Filters.** Trainieren Sie die *„ Bayesian-Filter “* (S. 33). Sie sollten alle E-Mails, die Sie als Spam definieren und von BitDefender nicht als solches erkannt wurde, markieren. Dies erfolgt über die Funktion **Ist Spam** in der Funktionsleiste. Zukünftige Nachrichten dieser Art werden somit als Spam erkannt.

   Anmerkung

   Der **Bayesian-Filter** wird erst aktiv, sobald Sie den Filter mit mehr als 60 legitimen E-Mails trainiert haben. Dazu müssen Sie den Vorgaben des Konfigurationsassistenten folgen.

5. **Halten Sie Ihr BitDefender-Produkt auf dem neuesten Stand.** Im Modul **Update**, Update, aktivieren Sie bitte das **Automatische Update**, um optimal gegen die neuesten Bedrohungen geschützt zu sein.

Anmerkung

Jedes mal wenn ein Update durchgeführt wird:
- werden neue Bildsignaturen zum **Grafik-Filter** hinzugefügt;
- werden neue Links zum **URL-Filter** hinzugefügt;
- werden dem **Heuristik-Filter** neue Regeln hinzugefügt.

Somit wird die Effektivität des Antispam-Moduls laufend verbessert.

6. **Konfigurieren Sie den Charset Filter.** Viele Spam E-Mails sind in Kyrillischen und/oder Asiatischen Zeichen verfasst. Im Modul **Antispam**, Einstellungen können Sie über die Option **Zeichensatzfilter** wählen ob Sie solche E-Mails ablehnen möchten.

Anmerkung

Sie können jeden dieser Filter im **AntiSpam**-Modul Einstellungen aktivieren/deaktivieren.

13.6. Wie Sie Ihre Kinder gegen unangemessene Inhalte schützen können

Folgen Sie diesen Schritten, um Ihr Kind gegen unangemessene Inhalte zu schützen:

1. **Erstellen Sie ein eingeschränktes Windows User Account.** Damit Ihre Kinder nicht auf das Modul **Kindersicherung** zugreifen oder die Einstellungen dort verändern müssen sie eingeschränkte Rechte auf Ihrem Computer haben.
2. **Anwender auswählen.** Die Liste der Anwender, die den Computer nutzen finden Sie im Abschnitt Status.Wählen Sie die Anwender aus, die nicht auf die Kindersicherung zugreifen sollen **Kindersicherung**.
3. **Allgemeine Einstellungen.** Gehen Sie auf **Status** und aktivieren Sie protection controls für Ihr Kind. Wenn Sie die **heuristic web filter** aktivieren, gehen Sie in protection level.
4. **Internetseiten blockieren.** Gehen Sie auf im Abschnitt **Internet**auf erstellen Sie eine Liste von Internetseiten die für Ihr Kind erlaubt bzw. nicht erlaubt sind. Wenn nötig können Sie Ausnahmen definieren. Sie können auch den Zugriff blockieren unter mit einer Liste von Internetseiten die BitDefender zur Verfügung stellt. Diese Internetseiten haben unangemessene und möglicherweise schädliche Inhalte.
5. **Anwendungen blockieren.** Gehen Sie auf im Abschnitt auf **Anwendungen** und blockieren Sie die Anwendungen, , die Ihr Kind nicht nutzen soll.

Anmerkung

Wenn Sie das Gefühl haben, Ihr Kind verbringt zu viel Zeit am Computer können Sie den Zugriff blockieren.

6. **Bestimmte Wörter blockieren.** Um Ihr Kind von möglicherweise schädlichen Inhalten zu schützen sowohl im Internet als auch bei E-Mails verwenden Sie den **Schlüsselwort-Filter** um bestimmte Wörter oder Sätze zu finden, die diese beinhalten. Im Abschnitt **Schlüsselwörter** können Regeln definiert werden unter zum blockieren von Internetseiten oder E-Mail Nachrichten, oder beidem, wenn Sie gewisse Wörter enthalten.
7. **Internet Zugang kontrollieren.** Im Abschnitt **Zeit einschränken** unter definieren Sie den Zeitplan nach dem der Internetzugang erlaubt ist.
8. **Schützen Sie Ihre Einstellungen mit einem Passwort.** Im Modul **Allgemeine** module, Einstellungen gehen Sie auf **Passwort Schutz für Produkt Einstellungen aktivieren** . Nur Anwender, die das Passwort kennen sind dann berechtigt Einstellungen zu ändern, die für einen bestimmten Nutzer eingerichtet wurden.

BitDefender Notfall CD

BitDefender v10 Internet Security verfügt über eine bootfähige CD-ROM (BitDefender Notfall CD basierend auf LinuxDefender) die fähig ist, alle Festplatten zu prüfen und zu desinfizieren, bevor Ihr Betriebssystem startet.

Sie sollten die BitDefender Notfall CD immer dann verwenden, wenn Ihr System aufgrund von Virusinfektionen nicht mehr richtig funktioniert. Dies passiert für gewöhnlich, wenn Sie kein AntiVirus-Programm benutzen.

Das Update der Virensignaturen wird automatisch ohne Benutzereingriff jedes Mal vollzogen, wenn Sie die BitDefender Notfall CD starten.

LinuxDefender ist eine mit BitDefender erweiterte Knoppix-Distribution, welche die neueste Version von BitDefender für Linux in das GNU/Linux integriert. Es beinhaltet einen SMTP AntiVirus/AntiSpam-Schutz und einen On Demand Scanner, der in der Lage ist, Festplatten (inkl. Windows NTFS-Partition), Samba-Freigaben und NFS Mount Points zu überprüfen und zu desinfizieren. Eine web-basierte Konfigurationsschnittstelle zu den BitDefender-Lösungen ist ebenfalls enthalten.

14. Überblick

Aktuelle Bestandteile

- Direkte Überprüfung von E-Mails (AntiVirus & AntiSpam)
- AntiVirus-Lösungen für Ihre Festplatten
- NTFS Schreib-Unterstützung (über Captive-Projekt)
- Desinfektion infizierter Dateien von Partitionen unter Windows XP (NTFS)

14.1. Was ist Knoppix?

Auszug aus http://knopper.net/knoppix:

„ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. “

14.2. Systemanforderungen

Bevor Sie LinuxDefender booten stellen Sie bitte sicher, dass Ihr System die folgenden Vorraussetzungen erfüllt:

Prozessortyp
X86 kompatibel mit einem Minimum von 166 MHz, aber bitte erwarten Sie in diesem Falle keine zufrieden stellende Systemleistung. Eine i686 Prozessorgeneration mit 800 MHz wäre die bessere Wahl.

Speicher
Die mindestens benötigte Speichergröße liegt bei 64 MB, für eine bessere Systemleistung wird jedoch 128 MB empfohlen.

CD-ROM
CD-Rom-Laufwerk und die BIOS-Einstellungen, um von CD zu booten.

Internetverbindung
Obwohl LinuxDefender auch ohne Internetverbindung lauffähig ist, benötigen die Update-Vorgänge eine aktive HTTP-Verbindung oder durch einen Proxy Server. Daher ist für einen aktuellen Schutz eine Internetverbindung ein MUSS.

Grafische Auflösung
800x600 für die web-basierte Administration.

14.3. Integrierte Software

Die Bitdefender Notfall CD enthält die folgenden Software-Pakete.

- BitDefender SMTP Proxy (AntiSpam & AntiVirus)
- BitDefender Remote Admin
- BitDefender Linux Edition (AntiVirus) + GTK Interface
- BitDefender Documentation (PDF- & HTML-Format)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Werkzeuge zur Datenwiederherstellung
- Netzwerk- und Sicherheits-Analyse Werkzeuge für Administratoren
- Amanda Backup Lösung
- thttpd Tiny HTTP Daemon (Web-Server)
- Ethereal (Netzwerkdatenverkehrs-Analyse)
- Nessus (Netzwerkdatenverkehrs-Analyse)
- Parted, QTParted und Partimage (Partitionierungs-Werkzeuge)
- Adobe Reader (Zur Anzeige von PDF-Dokumenten)
- Mozilla Firefox Web Browser

14.4. BitDefender Lösungen für Linux

Die LinuxDefender Notfall CD beinhaltet die BitDefender SMTP Proxy Lösung für Linux mit integriertem AntiVirus/AntiSpam, BitDefender Remote Admin (einer web-basierten Verwaltungsoberfläche) und einer BitDefender Linux Edition (On-Demand Kommandozeilen-Scanner).

14.4.1. BitDefender SMTP Proxy

BitDefender für Linux Mail Server – SMTP Proxy ist eine Content-Inspection-Lösung, welche neben dem Schutz vor Viren zusätzlich AntiSpam-Funktionalitäten beinhaltet. Beide Schutzvarianten arbeiten direkt auf Gateway-Ebene, um somit den gesamten E-Mail-Datenverkehr zu überprüfen und effektiv sichern zu können. Durch die Verwendung fortschrittlichster Technologien ist BitDefender für Linux Mail Server mit allen gängigen E-Mail-Servern kompatibel und erhielt außerdem die Zertifizierung „Red Hat Ready“.

Die AntiVirus- und AntiSpam-Lösungen überprüfen, desinfizieren und filtern E-Mails auf allen gängigen E-Mail-Servern und auf nahezu jeder Betriebssystem-Plattform. BitDefender für Linux Mail Server – SMTP Proxy wird direkt beim Bootvorgang gestartet und überprüft alle eingehenden E-Mails. Um das Produkt zu konfigurieren, kann BitDefender Remote Admin eine web-basierte Konfigurationsschnittstelle verwenden.

14.4.2. BitDefender Remote Admin

Die BitDefender-Dienste können sowohl lokal als auch extern verwaltet werden. Gehen Sie hierzu bitte wie folgt vor:

1. Starten Sie den Firefox Web-Browser und öffnen Sie die Internetadresse: https://localhost:8139 (oder klicken Sie bitte doppelt auf das BitDefender Remote Admin Symbol auf Ihrem Desktop)
2. Melden Sie sich mit dem Benutzer „bd“ und dem Kennwort „bd“ am System an
3. Wählen Sie „SMTP Proxy“ aus dem linken Menü
4. Tragen Sie den „echten“ SMTP-Server und den Port ein
5. Fügen Sie E-Mail-Domains zum Relaying hinzu
6. Fügen Sie Netzwerk-Domains zum Relaying hinzu
7. Wählen Sie „AntiSpam“ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
8. Wählen Sie „AntiVirus“ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
9. Zusätzlich können Sie per „Mail Notifications“ die Benachrichtigungen konfigurieren

14.4.3. BitDefender Linux Edition

Der AntiViren-Scanner von BitDefender Linux Edition integriert sich direkt auf den Linux Desktop. Diese Version des Produkts beinhaltet eine auf GTK+ basierende grafische Benutzeroberfläche, über die der Prüfvorgang durchgeführt werden kann.

Wählen Sie in der Benutzeroberfläche einfach den zu überprüfenden Pfad bzw. das Laufwerk aus und klicken Sie mit der rechten Maustaste auf das jeweilige Objekt. Wählen Sie nun aus dem Kontextmenü den Eintrag „Scan with BitDefender“. Der Prüfvorgang wird nun gestartet und der Status des Prüfvorgangs inkl. eines abschließenden Berichts wird angezeigt. Für die Option Feineinstellungen lesen Sie bitte in der Linux Edition Dokumentation (in dem BitDefender Verzeichnis für Dokumentation oder entsprechenden Handbuchseite) und dem **/opt/BitDefender/lib/bdc** Programm nach.

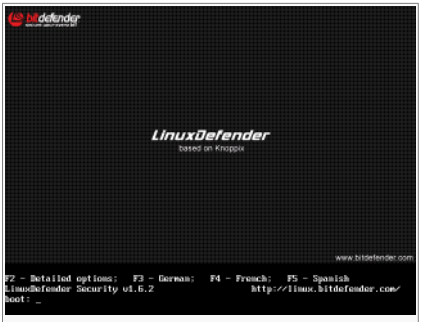
15. LinuxDefender Kurzanleitung

15.1. Starten und Beenden

15.1.1. LinuxDefender starten

Um von der CD-ROM starten zu können, müssen Sie zunächst das BIOS Ihres Computers so konfigurieren, dass die Bootreihenfolge folgendermaßen aussieht: CD-ROM Laufwerk, Floppy-Laufwerk, Festplatte.

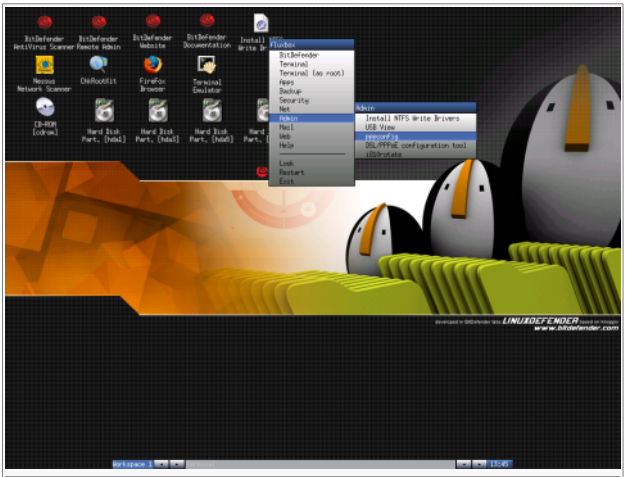
Starten Sie nun Ihren Computer neu und warten Sie, bis der initiale Bootvorgang abgeschlossen wurde. Sie bekommen nun den LinuxDefender Startbildschirm angezeigt. Folgen Sie nun bitte den angegebenen Schritten, um LinuxDefender zu starten.



LinuxDefender Startbildschirm

Drücken Sie `F2` um die erweiterten Einstellungen anzuzeigen. Drücken Sie bitte die Taste `F3` für die erweiterten Einstellungen in deutscher Sprache. Drücken Sie bitte die Taste `F4` für die erweiterten Einstellungen in französische Sprache. Drücken Sie bitte die Taste `F5` für die erweiterten Einstellungen in spanische Sprache. Um das System direkt zu starten, drücken Sie bitte die Taste `ENTER`.

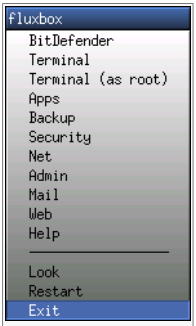
Sobald der Bootvorgang abgeschlossen wurde, wird der LinuxDefender Desktop angezeigt. Sie können nun damit beginnen, LinuxDefender zu verwenden.



Der LinuxDefender Desktop

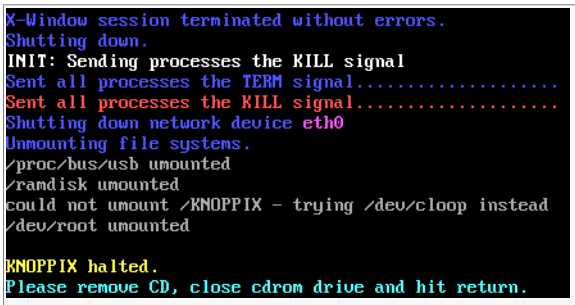
15.1.2. LinuxDefender beenden

Um LinuxDefender ornungsgemäß zu beenden wird empfohlen alle Partitionen mit dem Befehl zu schließen **umount** oder klicken Sie per Rechtsklick auf das jweilige Festplatten Symbol auf dem Desktopund wählen Sie **Unmount**. Danach können Sie den Computer sicher herunterfahren indem Sie im Linux Defender Menü auf **Exit** klicken. (öffnen mit rechter Maustaste) oder indem Sie den Befehl **halt** im Terminal eingeben.



Wählen Sie "EXIT"

Sobald LinuxDefender alle Programme beendet hat, bekommen Sie eine textbasierte Ausgabe angezeigt. Sobald der Satz **Please remove CD, close cd-rom drive and hit return** angezeigt wird, können Sie die CD aus dem Laufwerk entfernen, den Einschub schließen und die Taste ENTER betätigen. Der Computer führt nun einen Neustart mit Ihrem bevorzugten Betriebssystem durch.



Warten auf diese Nachricht, wenn der Rechner heruntergefahren wird

15.2. Internetverbindung konfigurieren

Falls Sie über ein Netzwerk mit DHCP-Funktionalität verfügen und eine Netzwerkkarte in Ihrem Computer installiert ist, sollte LinuxDefender die notwendigen Einstellungen automatisch erkennen. Für eine manuelle Konfiguration folgen Sie bitte den folgenden Schritten.

1. Öffnen Sie per Rechtsklick auf den Desktop das Kontextmenü und wählen Sie **Terminal**.
2. Geben Sie **netcardconfig** als Befehl ein und drücken Sie die Taste ENTER.
3. Falls Sie DHCP in Ihrem Netzwerk verwenden, wählen Sie bitte **yes**.
4. Die Netzwerkkonfiguration sollte nun automatisch erkannt werden. Mit dem **ifconfig** können Sie Ihre IP Adresse und Netzwerkkarteneinstellungen einsehen.
5. Falls Sie eine statische IP-Adresse verwenden (kein DHCP), wählen Sie stattdessen **No**.
6. Folgen Sie den Instruktionen auf dem Bildschirm und konsultieren Sie Ihren Administrator.

Sollten diese Schritte erfolgreich abgeschlossen haben, können Sie die Verbindung folgendermaßen überprüfen. Geben Sie dazu den folgenden Befehl in das Terminal ein und drücken Sie ENTER.

```
$ ping -c 3 bitdefender.com
```

Falls Sie eine Einwahlverbindung verwenden, wählen Sie bitte **pppconfig** vom LinuxDefender Administrationsmenü. Folgen Sie bitte dann den Bildschirminstruktionen, um die PPP Internet Verbindung einzustellen.

15.3. BitDefender per Update aktualisieren

Die BitDefender Pakete für die LinuxDefender verwenden den Festplattenspeicher des Systems für erneuerbare Dateien. Über diesen Weg können Sie die neuen Virensignaturen, Prüfmaschinen oder die AntiSpam Datenbank aktualisieren. Dies geschieht sogar, wenn das System über Read only Medien, wie z.B. LinuxDefender CD, arbeitet.

Stellen Sie bitte zunächst sicher, ob Ihre Internetverbindung funktioniert. Öffnen Sie nun BitDefender Remote Admin und wählen Sie im linken Menü **Live! Update**. Klicken Sie nun auf die Schaltfläche **Update Now**, um das Update durchzuführen.

Alternativ können Sie auch ein Update über das Terminal durchführen. Dazu verwenden Sie bitte den folgenden Befehl.

```
# /opt/BitDefender/bin/bd  update
```

Sämtliche Updatevorgänge werden in einer Berichtsdatei protokolliert. Diese können Sie mit dem folgenden Befehl im Terminal einsehen.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Falls Sie einen Proxy-Server zum Herstellen einer Internetverbindung verwenden, müssen Sie diesen Server zunächst im BitDefender Remote Admin, im Bereich **Live! Update** über die Schaltfläche **Configuration** angeben.

15.4. Prüfvorgänge durchführen

15.4.1. Wie erhalte ich Zugriff auf meine Daten unter Windows?

NTFS Schreibzugriff

Der NTFS Schreibzugriff wird über das Captive NTFS write project realisiert. Um diesen Zugriff zu verwenden, benötigen Sie die folgenden Dateien Ihrer Windows-Installation: `ntoskrnl.exe` und `ntfs.sys`. Derzeit werden nur Windows XP Treiber unterstützt. Sie können diese Treiber jedoch auch dazu verwenden, um auf Partitionen von Windows NT 4.0, 2000 und 2003 zu zugreifen. Für Windows 98 und ME werden keinerlei Treiber zum Schreibzugriff benötigt.

Installieren der NTFS Treiber

Um einen Zugriff zu Ihren Windows-Partitionen mit NTFS-Dateisystem zu erhalten und auf diesen schreiben zu können, müssen Sie zunächst die NTFS Treiber installieren. Wird dieser Schritt nicht durchgeführt, erhalten Sie nur schreibgeschützten Zugriff. Falls Sie FAT und nicht NTFS für Ihre Windows Partitionen verwenden oder lediglich einen Lesezugriff für Ihre Daten benötigen, können Sie die Laufwerke direkt einbinden und somit einen Zugriff auf Windows Laufwerke erhalten, als wären es Linux Laufwerke.

Um die Schreibunterstützung zu erhalten, speichern Sie die NTFS Treiber auf Ihrer lokalen Festplatte, entfernte Netzlaufwerke, einen USB Stick oder beziehen Sie diese Treiber direkt über das Windows Update. Es wird empfohlen, nicht die Treiber der verwendeten Windows-Installation einzusetzen, da diese im Falle einer Infizierung durch einen Virus ggf. ebenfalls beschädigt sind und nicht korrekt funktionieren.

Klicken Sie doppelt auf das Desktop-Symbol **Install NTFS Write Drivers**, um den Installationsvorgang zu starten. Wählen Sie die erste Option, wenn Sie die Treiber von der lokalen Festplatte installieren möchten.

Haben Sie die Treiber an einem anderen Ort gespeichert, wählen Sie bitte **Quick search** aus, um nach den Treiber suchen zu lassen.

Alternativ können Sie selbst einen Speicherort angeben oder die Treiber direkt über den Download des Service Pack 1 für Windows XP beziehen.

Die Treiber werden nicht auf Ihrer Festplatte installiert, sondern lediglich temporär von LinuxDefender verwendet, um auf die NTFS-Partitionen zu zugreifen. Sofern das Programm die Treiber installiert hat, können Sie die entsprechenden Partitionen per Doppelklick aufrufen und deren Inhalt einsehen. Für einen wirkungsvollen Datei Manager verwenden Sie bitte den Midnight Commander von dem LinuxDefender Menü (oder geben Sie **mc** in der Konsole ein).

15.4.2. Wie führe ich einen Prüfvorgang durch?

Wählen Sie die gewünschten Ordner aus und klicken Sie per Rechtsklick auf diese. Wählen Sie nun aus dem Kontextmenü den Eintrag **Send to** und klicken Sie nun auf **BitDefender Scanner**.

Alternativ kann der Prüfvorgang auch mit Rechten des Benutzers root über den Terminal durchgeführt werden. Geben Sie dazu den folgenden Befehl im Terminal ein und bestätigen Sie mit der Taste ENTER.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Klicken Sie nun in der Benutzeroberfläche auf **Start Scan**.

Falls Sie weitere Einstellungen vornehmen möchten, klicken Sie zuvor bitte auf **Configure Antivirus**.

15.5. Erstellen einer Ad-Hoc Mail-Filterungs-Lösung

Sie können LinuxDefender dazu benutzen eine Ad-Hoc Mail-Filter-Lösung zu erstellen, ohne dass Sie eine Software installieren oder den E-Mail-Server modifizieren müssen. Die Idee dahinter ist, dass Sie ein LinuxDefender System vor Ihrem Mail-Server benutzen und BitDefender erlauben, jeden SMTP-Verkehr nach Spam und Viren zu scannen und ihn anschließend gefiltert an den Mail-Server weiterzugeben.

15.5.1. Vorbereitende Maßnahmen

Sie benötigen mindestens einen Computer mit einer Pentium 3-kompatiblen CPU, 256 MB RAM und ein CD/DVD-Laufwerk, um davon zu starten. LinuxDefender muss den SMTP-Verkehr anstelle des eigentlichen E-Mail-Server bekommen. Es gibt verschiedene Wege um dies einzustellen.

1. Ändern Sie die IP des eigentlichen Mail-Servers und vergeben die alte IP an das LinuxDefender System
2. Ändern Sie Ihre DNS-Einträge, sodass der MX-Eintrag für Ihre Domains zu dem LinuxDefender System zeigt
3. Stellen Sie Ihre Mail-Clients auf das neue LinuxDefender System als SMTP-Server ein
4. Ändern Sie Ihre Firewall-Einstellungen so ab, dass alle SMTP-Serververbindungen an LinuxDefender weitergeleitet werden, anstatt an den eigentlichen Mail-Server

Das Linux How To wird die obigen Anweisungen nicht erklären. Für weitere Informationen konsultieren Sie bitte Linux Networking guides und Netfilter documentation.

15.5.2. Der Mail-Filter

Starten Sie Ihre LinuxDefender CD-ROM und warten Sie, bis das X Windows-System geladen ist.

Um den BitDefender SMTP-Proxy zu konfigurieren, doppelklicken Sie auf das **BitDefender Remote Admin** Symbol auf dem Desktop. Ein weiteres Fenster wird erscheinen. Benutzen Sie als Benutzernamen und als Kennwort `bd`, um sich anzumelden.

Nach dem erfolgreichen Login bekommen Sie die Möglichkeit, den BitDefender SMTP-Proxy zu konfigurieren.

Wählen Sie **SMTP Proxy** aus, um den eigentlichen Mail-Server einzutragen, den Sie vor Viren und Spam schützen möchten.

Klicken Sie auf die Kategorie **Email domains**, um alle Domains einzugeben, von denen Sie E-Mails akzeptieren möchten.

Wählen Sie **Add Email Domain** oder **Add Bulk Domains** und folgen den Anweisungen, um die Relays einzustellen.

Wählen Sie die Kategorie **Net domains**, um alle Netzwerke einzugeben, die Sie relayen möchten.

Wählen Sie **Add Net Domain** oder **Add Bulk Net Domains** und folgen den Anweisungen um die Relays einzustellen.

Wählen Sie **Antivirus** aus dem linken Menü, um auszuwählen was zu tun ist, wenn ein Virus gefunden wird, und um andere AntiVirus-Optionen zu konfigurieren.

Nun wird der gesamte SMTP-Verkehr von BitDefender gescannt und gefiltert. Standardmäßig werden alle virusinfizierte Mails gesäubert und alle Spam E-Mails von BitDefender werden im Betreff der Mail mit dem Wort `[SPAM]` gekennzeichnet. Ein E-Mail-Header (`X-BitDefender-Spam: Yes/No`) wird zu jeder Mail hinzugefügt, um die client-seitige Filterung zu erleichtern.

15.6. Eine Netzwerk-Sicherheitsprüfung durchführen

Neben den Möglichkeiten der Erkennung von Schädlingen und dem Filtern von Emails ist es mit LinuxDefender auch möglich, Ihr Netzwerk einer Sicherheitsprüfung zu unterziehen. Für diesen Fall sind Computer-forensische Werkzeuge auf dieser CD-ROM enthalten, mit denen es möglich ist, kompromittierte Systeme zu überprüfen und das Netzwerk auf Eindringlinge zu untersuchen. Bitte lesen Sie diese kurze Einführung, um mehr darüber zu erfahren, wie man eine kurze Prozessanalyse der Server und des Netzwerks vornimmt.

15.6.1. Auf Rootkits überprüfen

Bevor Sie Ihr Netzwerk einer solchen Prüfung unterziehen, sollten Sie zunächst sicherstellen, dass der Host, von dem Sie die Prüfung durchführen, nicht kompromittiert wurde. Starten Sie hierfür zunächst einen Prüfvorgang mit BitDefender. Sie können einen Prüfvorgang für die installierten Festplatten vornehmen, beschrieben in der Einführung für **Scan for viruses**, oder Sie können auf Unix rootkits (ähnlich zu trojanischen Pferden) prüfen.

Überprüfen Sie nun, ob eventuelle Eindringlinge einen Rootkit (eine Art Hintertür) auf dem System installiert haben. Zu diesem Zwecke wird das Programm **ChkRootKit** mitgeliefert. Um bestimmte Festplatten mittels diesem Programm zu überprüfen, verwenden Sie bitte den folgenden Befehl im Terminal und bestätigen Sie diesen anschließend mit der Taste ENTER. `-r NEWROOT` Parameter um das das neue (root) Verzeichnis auf dem Host zu definieren.

```
# chkrootkit  -r  /dev/hda3
```

Wird ein Rootkit gefunden, so zeigt das Programm diese Ausgabe in **fetter Schrift** im Terminal an.

15.6.2. Nessus – der Netzwerk Scanner

> Nessus ist die beliebteste Open-Source Software zum Entdecken von Sicherheitslücken in Netzwerken und wird von über 75.000 Unternehmen weltweit eingesetzt. Nessus kann dazu eingesetzt werden, remote das Netzwerk auf verschiedenste Sicherheitslücken zu überprüfen und schlägt diverse Verbesserungsvorschläge vor, um das Netzwerk zu sichern und das Risiko eines Einbruchs zu minimieren.
>
> *—www.nessus.org*

Nessus ist die beliebteste Open-Source Software zum Entdecken von Sicherheitslücken in Netzwerken und wird von über 75.000 Unternehmen weltweit eingesetzt. Nessus kann dazu eingesetzt werden, remote das Netzwerk auf verschiedenste Sicherheitslücken zu überprüfen und schlägt diverse Verbesserungsvorschläge vor, um das Netzwerk zu sichern und das Risiko eines Einbruchs zu minimieren.

Klicken Sie doppelt auf das Desktop-Symbol **Nessus Security Scanner** oder starten Sie das Programm über den Befehl **startnessus** im Terminal. Warten Sie nun bis das Fenster angezeigt wird. Dies kann je nach Hardware-Konfiguration 5 bis 10 Minuten andauern, da die Software über 5.000 Plug-Ins beinhaltet. Verwenden Sie den Benutzer `knoppix` und das Kennwort `knoppix` um sich anzumelden.

Klicken Sie auf den Abschnitt **Target selection** und geben Sie die IP-Adressen bzw. Hostnamen der Computer an, die Sie auf mögliche Sicherheitslücken überprüfen möchten. Stellen Sie danach sicher, dass die Prüfoptionen gemäß den Gegebenheiten in Ihrem Netzwerk angepasst sind. Somit können Sie Ressourcen und Bandbreite einsparen und erhalten ein akkurateres Prüfergebnis. Klicken Sie nun auf **Start the scan** um den Prüfvorgang zu starten.

Nach Abschluss des Prüfvorgangs erhalten Sie einen ausführlichen Bericht des Programms angezeigt, welcher Sie auf Schwachstellen hinweist und entsprechende Empfehlungen zu diesen bereitstellt. Der gespeicherte Bericht kann in dem von Ihnen bevorzugten Browser eingesehen werden.

15.7. Den Arbeitsspeicher (RAM) Ihres Computers überprüfen

Sollte Ihr Computer des Öfteren unerwartet abstürzen oder sog. „Blue Screens“ anzeigen, empfehlen wir Ihnen, den Arbeitsspeicher (RAM) Ihres Computers zu überprüfen. Dies können Sie ebenfalls mittels der LinuxDefender Notfall CD durchführen. Gehen Sie hierzu bitte wie folgt beschrieben vor.

Starten Sie Ihren Computer von der LinuxDefender CD und warten Sie, bis die den Startbildschirm mit erweiterten Einstellungsmöglichkeiten angezeigt bekommen. Tippen Sie nun den Befehl **memtest** ein und bestätigen Sie diesen mit drücken der Tast ENTER.

Das Programm zum Überprüfen des Arbeitsspeichers startet nun automatisch und überprüft diesen in mehreren Durchgängen. Sie können die Einstellungen des Speichertests jederzeit durch Drücken der Taste `c` auf Ihrer Tastatur beliebig anpassen.

Ein vollständiger Test des Arbeitsspeichers benötigt circa 8 Stunden, abhängig von der Kapazität und Geschwindigkeit des Speichers. Es wird empfohlen, diesen Test komplett durchlaufen zu lassen, er kann jedoch jederzeit durch drücken der Taste `ESC` auf Ihrer Tastatur abgebrochen werden.

Falls Sie vor kurzem neuen Arbeitsspeicher erworben haben, empfehlen wir Ihnen diesen einmal mittels dieser Methode zu überprüfen, um eventuelle Produktionsfehler noch vor Ablauf der Garantie zu erkennen und somit Systemabstürze und Datenverlust zu vermeiden.

Hilfe erhalten

16. Support

16.1. Technische Beratung

Als eines der führenden Dienstleistungsunternehmen für IT Sicherheitslösungen möchten wir Ihnen eine möglichst schnelle, kompetente und unkomplizierte technische Unterstützung bei auftretenden Fragen anbieten.Unser technischer Support ist zu diesem Zweck stets mit den aktuellsten Virensignaturen, neuesten Informationen und präzisen Antworten auf wiederkehrende Fragen ausgestattet.

Insbesondere zeichnet sich SOFTWIN durch ein hohes Maß an Innovation, ein hervorragendes Preis-Leistungsverhältnis und eine kurze Reaktionszeit in allen Belangen aus.Kundenzufriedenheit ist für uns nicht nur eine Floskel, sondern Firmenphilosophie.Es ist jedoch leider nicht vollkommen auszuschließen, dass es bei der Bearbeitung Ihrer Anfragen zu Engpässen kommen kann und bitten diesbezüglich um Nachsicht.

Wir freuen uns auf die Kontaktaufnahme zu unseren technischen Support und stehen Ihnen mit Rat und Tat zur Seite. Nutzen Sie hierfür einfach unseren E-Mail Kontakt <support@bitdefender.de> oder rufen Sie uns Werktags unter (075 42) 94 44-60 an.Falls Sie den Weg über E-Mail bevorzugen, teilen Sie uns bitte mit, welches Produkt und Betriebssystem Sie verwenden und beschreiben Sie das aufgetretene Problem so detailliert als möglich.

16.2. Online-Hilfe

16.2.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen und hilfreichen Tipps & Tricks rund um die Produkte.In leicht verständlicher Form bietet die Knowledge Base Informationen, Anleitungen und Berichte über neue Patches und behobene Probleme.Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar.Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Knowledge Base ist jederzeit unter der Internet-Adresse http://kb.bitdefender.de erreichbar.

16.3. Kontaktinformationen

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell.Seit mehr als 10 Jahren überbietet SOFTWIN konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen.

16.3.1. Kontaktadressen

Vertrieb: <vertrieb@bitdefender.de>
Technische Beratung: <support@bitdefender.de>
Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse <documentation@bitdefender.com> kontaktieren.
Vertrieb: <vertrieb@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
<presse@bitdefender.de>
Jobs: <jobs@bitdefender.com>
Virus-Einsendungen: <virus_submission@bitdefender.com>
Spam-Einsendungen: <spam_submission@bitdefender.com>
Viren melden: <abuse@bitdefender.com>
Webseite: http://www.bitdefender.de
Webseite: http://www.bitdefender.de
Lokale Anbieter: http://www.bitdefender.de
BitDefender Knowledge-Base: http://kb.bitdefender.de

16.3.2. Niederlassungen

Die BitDefender Niederlassungen stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

Deutschland

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Deutschland

Phone: +49 (0)75 42 -94 44 44
Fax: +49 (0)75 42 - 94 44 99
<support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Web: http://www.bitdefender.de
Technische Beratung: <support@bitdefender.de>

Großbritannien und Irland

One Victoria Square
Birmingham
B1 1BD
Phone: +44 207 153 9959
Fax: +40 21 - 233 07 63
<support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Web: http://www.bitdefender.de
Technische Beratung: <support@bitdefender.de>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A.

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support:
<support@bitdefender.com>
Customer Service: 954-776-6262
http://www.bitdefender.com

Romania

SOFTWIN

5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Glossar

ActiveX

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

Erwähnenswert ist, dass bei ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

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.

Archiv

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.

Backdoor (Hintertür)

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

Bootsektor

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

Bootvirus

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

Browser

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.

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.

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.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download (Herunterladen)

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

E-Mail

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

Ereignis

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.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese 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.

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.

E-Mail Client

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

Arbeitsspeicher

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

Nicht heuristisch

Diese 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.

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.

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.

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.

Logdatei (Berichtsdatei)

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

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, 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.

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 private und geheime Anwenderdaten überwacht und über seine Internetverbindung 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.

Startup Objekt (Autostart-Objekt)

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.

Systemleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Er 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 (Aktualisierung)

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 hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen 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.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

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