bitdefender

INTERNET SECURITY 2009

Benutzerhandbuch

bitdefender

BitDefender Internet Security 2009

Benutzerhandbuch

Veröffentlicht 2009.01.30

Rechtlicher Hinweis

bitdefender

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.

PRODUKT REGISTRIERUNG: Mit der Zustimmung zu diesem Lizenzvertrag sind Sie einverstanden, sich im Internet über „Mein BitDefender“ zu registrieren. Damit stellen Sie den Gebrauch der Software und deren möglichen Updates sowie das Recht zur Wartung sicher. Durch diese Vorgehensweise stellen wir sicher, dass die Software nur auf Computern funktioniert, auf welchen die Software gültig lizensiert ist und dass Endkunden einen Wartungsservice erhalten, wenn eine gültige Lizenzierung vorliegt. Zur Registrierung benötigen Sie eine gültige Seriennummer des Produktes und eine gültige E-Mail Adresse, um Lizenzerneuerungen und weitere Informationen zu erhalten.

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 BITDEFENDER zur Benutzung des oben und folgend genannten BITDEFENDER 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 BITDEFENDER 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.

ABLAUF. Das Produkt stellt unverzüglich nach Ablauf des Lizenzzeitraums den Betrieb ein.

UPGRADES: Sollte das SOFTWAREPRODUKT BitDefender mit der Bezeichnung Upgrade gekennzeichnet sein, muss der Benutzer für eine berechtigte Nutzung eine gültige, von BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER. 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: BITDEFENDER 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 BITDEFENDER das Medium austauschen oder dem Benutzer den Betrag zurück erstatten, den der Benutzer für BitDefender bezahlt hat. BITDEFENDER gewährleistet weder die dauerhafte Verfügbarkeit, noch die Fehlerfreiheit von BitDefender, noch dass Unzulänglichkeiten und Fehler von BitDefender behoben werden. BITDEFENDER gewährleistet ebenso nicht, dass BitDefender den Anforderungen des Benutzers entspricht.

SOFERN IN DER VORLIEGENDEN VEREINBARUNG NICHT AUSDRÜCKLICH ANDERWEITIG FESTGELEGT, LEHNT BITDEFENDER ALLE ANDEREN AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN IM HINBLICK AUF DIE PRODUKTE, DAMIT ZUSAMMENHÄNGENDE VERBESSERUNGEN, WARTUNG ODER SUPPORT ODER ALLE ANDEREN VON BITDEFENDER GELIEFERTEN (MATERIELLEN ODER IMMATERIELLEN) MATERIALIEN ODER ERBRACHTEN DIENSTLEISTUNGEN AB. BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER über existierende und / oder mögliche Schäden informiert wurde.

IN EINIGEN EINZELSTAATEN IST DIE BESCHRÄNKUNG ODER DER AUSSCHLUSS DER HAFTUNG FÜR BEILÄUFIG ENTSTANDENE SCHÄDEN ODER FOLGESCHÄDEN NICHT ZULÄSSIG. DAHER GILT DIE VORSTEHENDE BESCHRÄNKUNG UNTER UMSTÄNDEN NICHT FÜR SIE.

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, usw.).

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.

Einverständnis zur elektronischen Kommunikation. BitDefender kann / wird Ihnen ggf. Informationen über Software und Wartungsdienstleistungen sowie die Bedienung und die Verwendung unserer Produkte zu kommen lassen. Desweiteren beinhalten diese Informationen auch rechtliche Notizen und andere Kommunikation über unsere Produkte. Diese Art der Kommunikation erfolgt über Informationen, die in das Produkt eingebunden sind, sowie an die hinterlegte E-Mail Adresse oder über das Internet auf

unseren Internetseiten, hauptsächlich an bei BitDefender registrierte Anwender. Mit der Zustimmung zu dieser Vereinbarung erklären Sie sich einverstanden, alle Informationen elektronisch zu empfangen. Dies heißt ausschließlich, dass Sie den Zugang zu diesen Informationsseiten bzw. zu diesem Informationsangebot haben und diesen einräumen bzw. nachweisen können.

Allgemein. Dieser Vertrag unterliegt dem Recht von Rumänien, internationalen Copyright 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 Vertrages wegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam oder wird sie für unwirksam erklärt, so wird hierdurch die Gültigkeit des übrigen, mit der unwirksamen Bestimmung nicht unmittelbar zusammenhängenden Vertragsteils, nicht berührt.

BitDefender und alle zugehörigen Logos sind eingetragene Titel und Marken von BITDEFENDER. Alle anderen Marken und Titel sind Eigentum der 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 BITDEFENDER oder einem Händler von BitDefender. Die Bestimmungen im Hinblick auf Geheimhaltung und Beschränkungen gelten über die Laufzeit der Lizenz hinaus.

BITDEFENDER 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 BITDEFENDER ausgegebene englische Fassung.

BitDefender Kontakt: West Gate Park, Building H2, 24 Preciziei Street, Sector 6, Bukarest, Rumänien, oder unter Tel.: +40-21-3001255 oder +40-21-3001254, E-Mail: office@bitdefender.com.

Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer vorgesehen, die sich für **BitDefender Internet Security 2009** 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.

In diesem Buch werden die Firma und das Team beschrieben die **BitDefender Internet Security 2009** entwickelt haben, Sie werden durch den Installationsprozess geführt und erfahren wie das Produkt optimal konfiguriert werden kann. So lernen Sie mit **BitDefender Internet Security 2009** umzugehen und es effektiv einzusetzen sowie Updates durchzuführen, es zu testen und Ihren Bedürfnissen anzupassen.

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. Web-Seiten oder FTP-Server.
support@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. xv)	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.

Erscheinungsbild	Beschreibung
`sample code listing`	Beispielquelltexte werden in einer Schriftart mit `fester Laufweite` angegeben.

1.2. Symbole

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

Das Buch besteht aus mehreren Teilen unterteilt in Hauptthemen. Ausserdem ist ein Glossar enthalten welcher einige technische Begriffe erklärt.

Installation. Schritt-für-Schritt Anleitung zur Installation von BitDefender auf Ihrem Computer. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender Internet Security 2009** und werden durch jeden Schritt begleitet. Zusätzlich wird beschreiben wie eine Deinstallation von BitDefender durchzuführen ist.

Grundkonfiguration. Beschreibung der Grundkonfiguration und Wartung von BitDefender.

Erweiterte Administration. Eine detaillierte Beschreibung der Sicherheitsfähigkeiten von BitDefender. Ihnen wird beigebracht wie Sie BitDefender konfigurieren und

Handhaben können um den bestmöglich Schutz vor allen Arten von Gefahren (Schädlingen, Spam, Hackern, unpassendem Inhalt und so weiter) zu erhalten.

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

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

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 bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

Installation

1. Systemanforderungen

Sie können BitDefender Internet Security 2009 nur auf Computern mit den folgenden Betreibssystemen installieren:

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

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

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

1.1. Hardware-Anforderungen

Für Windows XP

- 800 MHz Prozessor oder höher
- 256 MB Arbeitsspeicher (512 MB empfohlen)
- 170 MB freier Speicherplatz auf der Festplatte (200 MB empfohlen)

Für Windows Vista

- 800 MHz Prozessor oder höher
- Mindestens 512 MB Arbeitsspeicher (1 GB empfohlen)
- 170 MB freier Speicherplatz auf der Festplatte (200 MB empfohlen)

Für Windows Home Server

- 800 MHz Prozessor oder höher
- Mindestens 512 MB Arbeitsspeicher (1 GB empfohlen)
- 170 MB freier Speicherplatz auf der Festplatte (200 MB empfohlen)

1.2. Software-Anforderungen

- Internet Explorer 6.0 (oder höher)
- .NET Framework 1.1 (befindet sich ebenfalls im Installationspaket)

Der Antiphishingschutz arbeitet nur für:

- Internet Explorer 6.0 (oder höher)
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

Instant Messaging (IM) Verschlüsselung arbeitet nur für:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

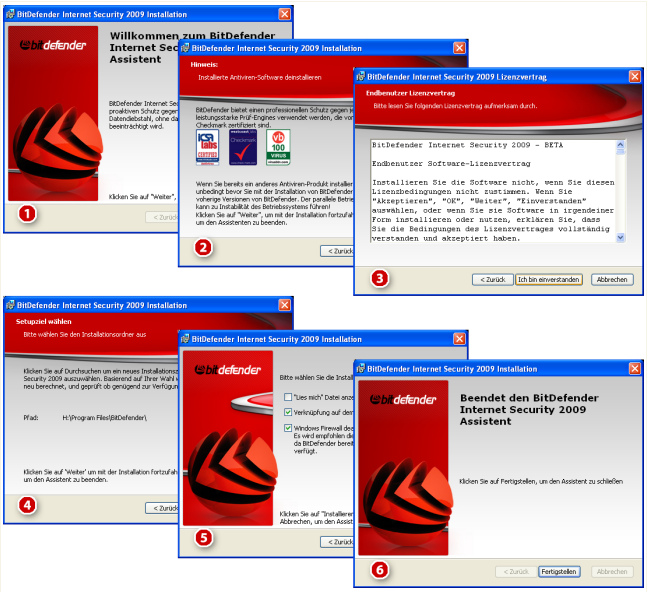
Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung. Die BitDefender Antispam Toolbar ist integriert in:

- Microsoft Outlook 2000 / 2002 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 1.5 und 2.0

2. BitDefender installieren

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

Bevor die Installation beginnt, prüft BitDefender, ob eine neuere Version des Installationspaketes verfügbar ist. Sollte dies der Fall sein, so werden Sie gefragt, ob Sie dieses herunterladen möchten. Klicken Sie **Ja** um die neue Version herunterzuladen oder **Nein** um die Installation mit der bereits vorhandenen Datei fortzuführen.



Installationsschritte

Befolgen Sie die folgenden Schritte um BitDefender Internet Security 2009 zu installieren:

1. Klicken Sie auf **Weiter**, um fortzufahren, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen.
2. Klicken Sie auf **Weiter**.

   BitDefender Internet Security 2009 weist Sie daraufhin, ob weitere Antiviren-Programme auf Ihrem Computer installiert sind. Klicken Sie auf **Entfernen**, um das betreffende Produkt zu deinstallieren. Sollten Sie fortfahren wollen ohne das entsprechende Produkt zu entfernen, dann klicken Sie auf **Weiter**.

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

3. Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Ich stimme zu**.

   Wichtig
   Wenn Sie diesen Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie werden das Setup verlassen.

4. Standardmäßig wird BitDefender Internet Security 2009 unter `C:\Programme\BitDefender\BitDefender 2009` installiert. Falls Sie einen anderen Ordner wählen möchten, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner in dem Sie BitDefender installieren möchten.

   Klicken Sie auf **Weiter**.

5. Optionen bezüglich der Installation auswählen. Manche werden standardmäßig gewählt:
   - **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 erstllen.
   - **CD nach Installation auswerfen** - um die CD nach Beendigen der Installation auszuwerfen. Diese Option erscheint nur, wenn Sie von CD installieren.
   - **Windows-Firewall ausschalten** -um die Windows eigene Firewall zu deaktivieren.

Wichtig

Wir empfehlen die windows-basierte Firewall zu deaktivieren. BitDefender Internet Security 2009 beinhaltet eine erweiterte Firewall. Der Gebrauch von zwei Firewalls auf ein und demselben Computer kann zu Problemen führen.

- **Ausschalten von Windows-Defender** - um den Windows-Defender zu deaktivieren; diese Option erscheint nur bei Windows Vista.

Klicken Sie auf **Installieren**, um mit der Installation des Produkts zu beginnen. BitDefender wird zuerst .NET Framework 1.1. installieren, falls dies noch nicht installiert ist.

Bitte warten Sie bis der Installationsvorgang beendet wurde.

6. Klicken Sie auf **Fertigstellen**. Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setup-Assistent den Installationsprozess fertigstellen kann. Wir raten dazu, das so bald wie möglich zu tun.

Wichtig

Nach dem Installationsprozesses und dem Neustart des Computers erscheinen ein Registrierungsassistent und ein Konfigurationsassistent. Führen Sie diese Assistenten durch, um BitDefender Internet Security 2009 zu registrieren und zu konfigurieren und um ein BitDefender Benutzerkonto zu erstellen.

Wenn Sie die Standardeinstellungen für den Installationspfad übernommen haben, so finden Sie unter `Programme/Dateien` einen neuen Ordner mit dem Namen `BitDefender` der den Unterordner `BitDefender 2009` beinhaltet.

2.1. Registrierungsassistent

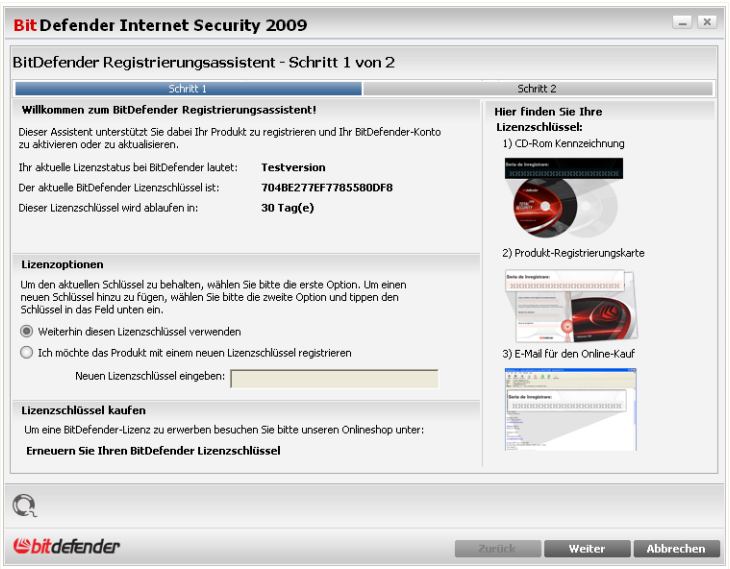
Nach der Installation und dem Neustart Ihres Computers erscheint ein Registrierungssassistent. Dieser Assistent hilft Ihnen dabei, BitDefender zu registrieren und ein BitDefender Benutzerkonto zu konfigurieren.

Sie sollen ein BitDefender Benutzerkonto registrieren, um BitDefender Updates zu erhalten. Mit dem BitDefender Benutzerkonto haben Sie Zugang zu dem kostenfreien technischen Support und Sonderangeboten und -Aktionen. Wenn Sie Ihren BitDefender Lizenzschlüssel verlieren, können Sie sich unter http://myaccount.bitdefender.com in Ihr Konto einloggen, um ihn wieder zu erhalten.

Anmerkung

Wenn Sie diesen Assistenten schließen möchten, klicken Sie einfach auf **Abbrechen**. Sie können den Registrierungsassistent jederzeit erneut öffnen indem Sie auf den Link **Registrieren** klicken, der sich im unteren Bereich der Benutzeroberfläche befindet.

2.1.1. Schritt 1/2 - BitDefender Internet Security 2009 registrieren



Registrierung

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

Um BitDefender Internet Security 2009 zu registrieren:

1. Klicken Sie auf die Schaltfläche **Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren**.
2. Geben Sie den Lizenzschlüssel in das Editierfeld ein.

Anmerkung

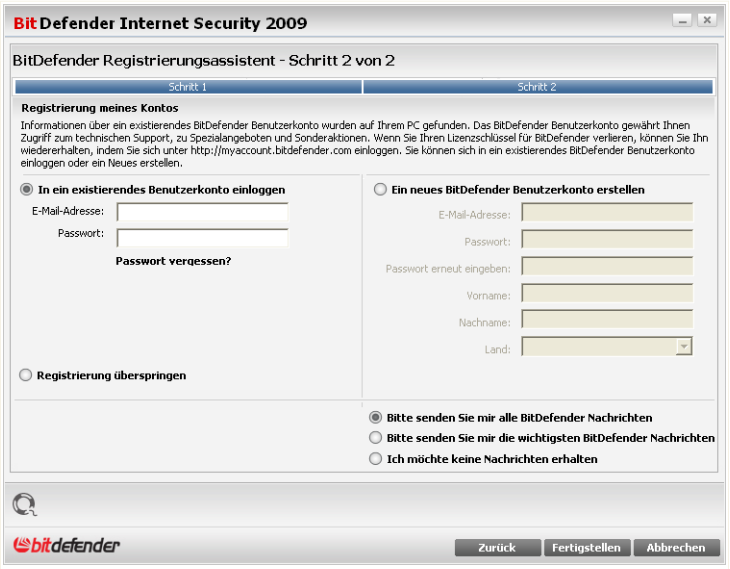
Sie finden den Lizenzschlüssel:

- Auf dem CD-Aufdruck.
- Auf der Registrierungskarte des Produktes.
- In der E-Mail-Bestätigung des Online-Kaufs.

Wenn Sie keinen Bitdefender-Lizenzschlüssel besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Klicken Sie auf **Weiter**.

2.1.2. Schritt 2/2 - BitDefender-Benutzerkonto erstellen



Kontoerstellung

Wenn Sie zur Zeit kein BitDefender Benutzerkonto einrichten wollen, klicken Sie auf **Registrierung überspringen** und dann auf **Beenden**. Andererseits gehen Sie je nach Ihren Wünschen wie folgt vor:

- „Ich habe noch kein BitDefender-Benutzerkonto“ (S. 9)
- „Ich habe bereits ein BitDefender Nutzerkonto.“ (S. 10)

Wichtig

Sie müssen innerhalb von 15 Tagen (Test-Version) bzw. 30 Tagen (lizensierte Version) nach Installation des BitDefender ein Benutzerkonto erstellen. Ansonsten, BitDefender wird keine automatische Updates erhalten.

Ich habe noch kein BitDefender-Benutzerkonto

Um ein BitDefender-Benutzerkonto zu erstellen, wählen Sie **Ein neues BitDefender Benutzerkonto erstellen** und geben Sie die benötigten Informationen ein. Die hier eingetragenen Daten bleiben vertraulich.

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.
- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort sollte mindestens 6 Zeichen haben.
- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.
- **Land** - wählen Sie das Land Ihres Wohnsitzes aus.

Benutzen Sie die angegebene E-Mail Adresse und das Passwort um sich in Ihr Benutzerkonto unter folgendem Link einzuloggen: http://myaccount.bitdefender.com.

Um erfolgreich ein Benutzerkonto einzurichten müssen Sie zunächst Ihre E-Mail Adresse aktivieren. Überprüfen Sie hierzu Ihre E-Mails der angegebenen Adresse und folgen Sie den Instruktionen, die Sie vom BitDefender Registrierungsservice zugesandt bekommen haben.

Auf Wunsch wird BitDefender Sie über die E-Mail-Adresse Ihres Benutzerkontos über Sonderangebote informieren. Wählen Sie eine der zur Verfügung stehenden Optionen:

- **Senden Sie mir alle BitDefender-Nachrichten**
- **Senden Sie mir nur die wichtigsten Nachrichten**
- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.

Ich habe bereits ein BitDefender Nutzerkonto.

BitDefender weist Sie daraufhin, falls bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert wurde. Geben Sie in diesem Fall das Passwort Ihres Benutzerkontos an.

Wenn Sie bereits ein aktives Benutzerkonto besitzen, BitDefender es jedoch nicht entdeckt, wählen Sie **In ein bestehendes BitDefender-Benutzerkonto einloggen** und geben Sie die E-Mail Adresse und das Passwort Ihres Benutzerkontos ein.

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

Auf Wunsch wird BitDefender Sie über die E-Mail-Adresse Ihres Benutzerkontos über Sonderangebote informieren. Wählen Sie eine der zur Verfügung stehenden Optionen:

- **Senden Sie mir alle BitDefender-Nachrichten**
- **Senden Sie mir nur die wichtigsten Nachrichten**
- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.

2.2. Konfigurationsassistent

Wenn Sie den Registrierungsassistenten beendet haben, erscheint ein Konfigurationsassistent. Der Assistent hilft Ihnen spezielle Produktmodule zu konfigurieren und BitDefender so einzustellen, dass er wichtige Sicherheitsaufgaben durchführt.

Es ist nicht notwendig den Assistenten erfolgreich zu beenden, dennoch empfehlen wir dies um Ihnen Zeit zu sparen und Ihr System zu sichern - noch bevor Sie BitDefender Internet Security 2009 vollständig installiert haben.

Anmerkung

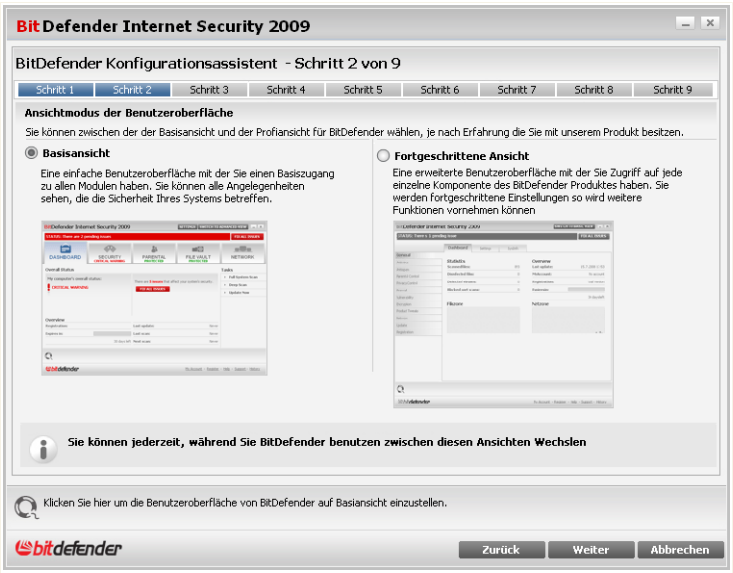
Wenn Sie diesen Assistenten schließen möchten, klicken Sie einfach auf **Abbrechen**. BitDefender wird Sie über die Komponenten informieren, die Sie konfigurieren müssen, wenn Sie die Benutzeroberfläche öffnen.

2.2.1. Schritt 1/9 - Willkommensfenster

Begrüßungsfenster

Klicken Sie auf **Weiter**.

2.2.2. Schritt 2/9 - Auswahl der Ansichtmodi



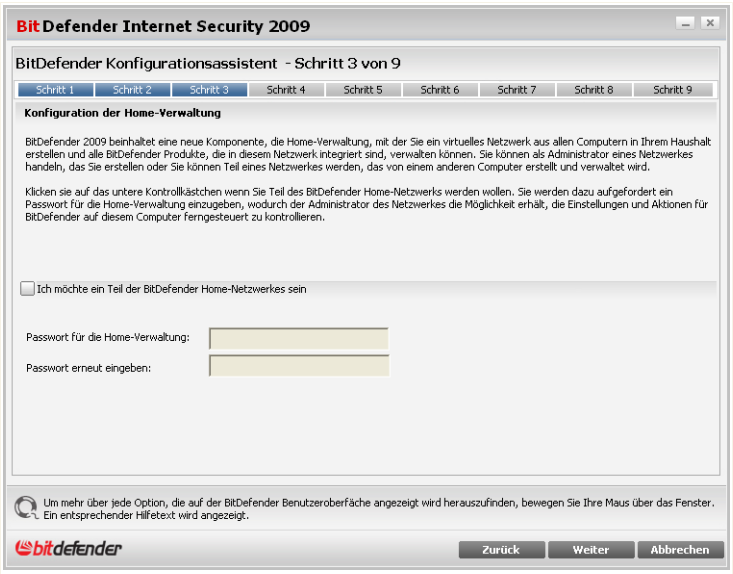
Ansichtmodi

Wählen sie zwischen zwei Benutzeroberflächen, entsprechend Ihrer Erfahrung mit BitDefender:

- **Basisansicht.** Eine einfache Benutzeroberfläche für Anfänger und Benutzer die Basisaufgaben durchführen und einfache Probleme lösen möchten. Sie müssen nur die Warnungen von BitDefender beachten und die auftauchenden Probleme lösen.
- **Fortgeschrittene Ansicht.** Die erweiterte Benutzeroberfläche richtet sich an erfahrenere Benutzer die das Produkt vollständig konfigurieren möchten. Sie können jede Produktkomponente konfigurieren und erweiterte Aufgaben durchführen.

Klicken Sie auf **Weiter**.

2.2.3. Schritt 3/9 - Konfigurieren Sie das BitDefender Netzwerk



BitDefender Netzwerkkonfiguration

BitDefender gibt Ihnen die Möglichkeit ein virtuelles Netzwerk mit den Computern in Ihrem Haushalt zu erstellen und alle BitDefender Produkte in diesem Netzwerk zu verwalten.

Wenn Sie möchten, dass dieser Computer Teil des BitDefender Home-Netzwerkes sein soll, befolgen Sie folgende Schritte:

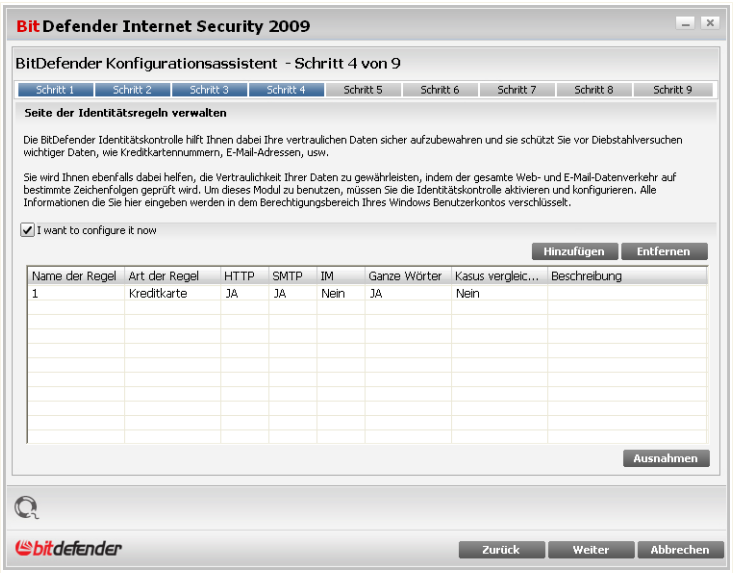
1. Wählen Sie **Ich möchte Teil des BitDefender Home-Netzwerkes sein** .
2. Geben Sie das selbe administrative Passwort in alle Editierfelder ein.

Wichtig

Das Passwort gibt dem Administrator die Möglichkeit das BitDefender Produkt, das auf diesem Computer installiert ist von einem anderen Computer aus zu verwalten.

Klicken Sie auf **Weiter**.

2.2.4. Schritt 4/9 - Identitätskontrolle konfigurieren



Identitätskontolle Konfiguration

Die Identitätskontrolle schützt Sie gegen den Diebstahl wichtiger Daten, wenn Sie online sind. Basierend auf Regeln, die von Ihnen erstellt wurden, prüft die Identitätskontrolle den Web-, Mail und IM-Datenverkehr auf spezielle Zeichenfolgen (zum Beispiel Ihre Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, E-Mail Adresse oder IM-Nachricht gefunden wird, werden diese sofort geblockt.

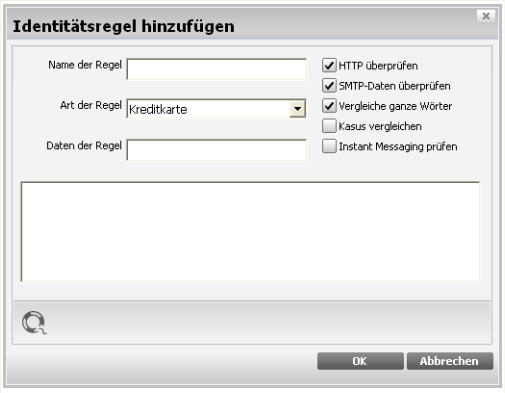
Wenn Sie die Identitätskontrolle verwenden möchten, befolgen Sie folgende Schritte:

1. Wählen Sie **Ich möchte die Identitätskontrolle konfigurieren**.
2. Erstellen Sie Regeln um wichtige Daten zu schützen. Für weitere Informationen lesen Sie bitte „Erstellen von Regeln für die Identitätskontrolle“ (S. 15).
3. Erstellen Sie, wenn nötig, spezielle Ausnahmen zu den Regeln, die Sie erstellt haben. Für weitere Informationen lesen Sie bitte „Erstellen von Ausnahmen der Identitätskontrolle“ (S. 16).

Klicken Sie auf **Weiter**.

Erstellen von Regeln für die Identitätskontrolle

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf **Hinzufügen** Das Konfigurationsfenster wird erscheinen.



Identitätskontrolle Regel

Hier können Sie die Parameter auswählen:

- **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Editierfeld ein.
- **Art der Regel** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- Geben Sie in das Feld **Daten der Regel** die Daten ein, die geschützt werden sollen. Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.

> ***Anmerkung***
> Wenn Sie weniger als drei Zeichen angeben werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern.

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

Um die Informationen die die Regel blockiert leicht identifizieren zu können, geben Sie eine detaillierte Regelbeschreibung in das Editierfeld ein.

Um die Art des zu prüfenden Datenverkehrs zu bestimmen, konfigurieren Sie diese Optionen:

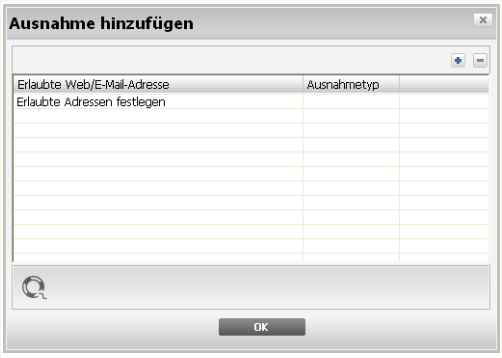
- **HTTP-Daten überprüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **SMTP-Daten überprüfen** - prüft alle ausgehenden E-Mail-Nachrichten.
- **Instant Messaging überprüfen** - prüft den Instant Messaging Datenverkehr und blockiert ausgehende Nachrichten, die die Regeldaten enthalten.

Klicken Sie auf **OK** um die Regel hinzuzufügen.

Erstellen von Ausnahmen der Identitätskontrolle

In manchen Fällen wird es nötig sein Ausnahmen für bestimmte Identitätsregeln zu erstellen. In manchen Fällen ist es nötig Ausnahmen für bestimmte Regeln zu erstellen. Zum Beispiel haben Sie eine Regeln angelegt welche verhindert das Ihre Kreditkartennummer per HTTP übertragen wird. Nun möchten Sie sich aber z.B. Schuhe auf einer bestimmten Webseite per Kreditkarte kaufen. In diesem Fall müssten Sie eine Ausnahme definieren um dies möglich zu machen.

Um eine solche Ausnahme zu erstellen klicken Sie auf die **Ausnahmen**-Schaltfläche.



Ausnahmen der Identitätskontrolle

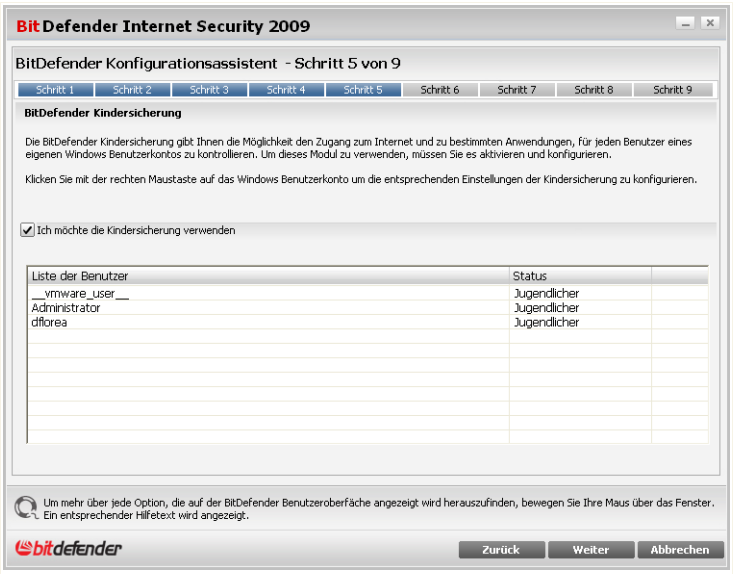
Um eine Ausnahme zu erstellen befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um einen neuen Eintrag in die Tabelle hinzuzufügen.
2. Doppelklicken Sie auf **Entsprechende Ausnahme eingeben** und geben Sie die gewünschte Adresse zum Ausnehmen ein.
3. Doppelklicken Sie dann auf **Typ wählen** und wählen Sie den gewünschten Eintrag aus dem Menü aus.
   - Wenn Sie eine Webseite eingegeben haben dann wählen Sie **HTTP**.
   - Wenn Sie eine E-Mail Adresse eingegeben haben dann wählen Sie **SMTP**.

Um eine Ausnahme zu entfernen, wählen Sie diese aus und klicken Sie die **Enternen** Schaltfläche.

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

2.2.5. Schritt 5/9 –Kindersicherung konfigurieren



Kindersicherung Konfiguration

Die BitDefender Kindersicherung gibt Ihnen die Möglichkeit den Zugriff auf das Internet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkonto auf dem System zu kontrollieren.

Um die Kindersicherung zu verwenden, befolgen Sie die folgenden Schritte:

1. Wählen Sie **Ich möchte die Kindersicherung verwenden**.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Windows Benutzerkontos und wählen Sie das Profil der Kindersicherung, das angewendet werden soll.

Profile	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.

Profile	Beschreibung
Jugendlicher	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.

Anmerkung

Um die Kindersicherung vollständig zu konfigurieren oder für bestimmte Windows-Benutzerkonten zu deaktivieren, starten Sie BitDefender, wechseln Sie zu der erweiterten Ansicht und klicken Sie auf Kindersicherung. Sie können die Kindersicherung so konfigurieren, dass Folgendes blockiert wird:

- Unangemessene Webseiten.
- Den Internetzugang zu bestimmten Zeiten (beispielsweise während dem Unterricht).
- Web-Seiten, Mails und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

Klicken Sie auf **Weiter**.

2.2.6. Schritt 6/9 - Virenberichte konfigurieren

Virenbericht-Optionen

BitDefender kann anonyme Berichte bezüglich der Virenfunde auf Ihrem Computer an das BitDefender Labor senden, um die Virenverbreitung nachzuverfolgen.

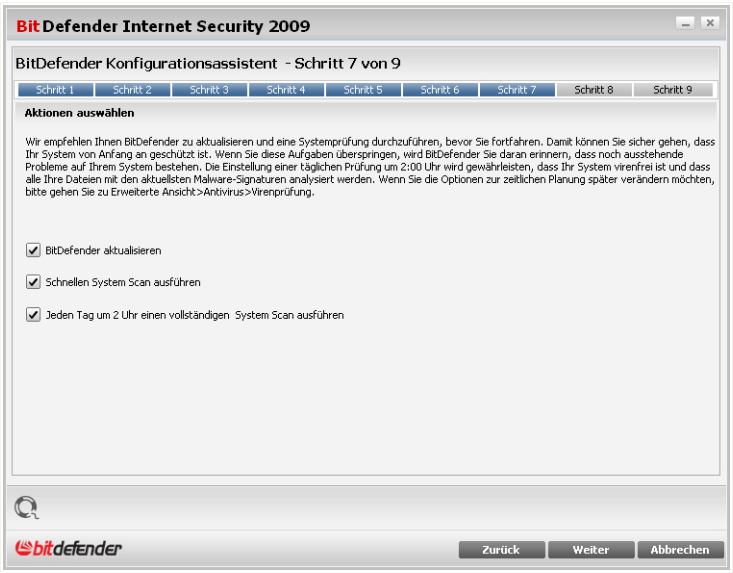
Folgende Optionen können konfiguriert werden:

- **Virenbericht senden** - sendet Berichte an das Bitdefender Labor über die auf Ihrem Computer entdeckten Viren.
- **BitDefender Outbreak Erkennung aktivieren** - sendet Berichte über potentiele Virenausbrüche an das BitDefender Labor.

Anmerkung
Diese Berichte beinhalten keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse und werden nicht für kommerzielle Zwecke verwendet.

Klicken Sie auf **Weiter**.

2.2.7. Schritt 7/9 – Auszuführende Aufgaben auswählen



Auswahl für Aktionen

Nehmen Sie hier die BitDefender Sicherheitseinstellungen für Ihr System vor. Die folgenden Optionen sind verfügbar:

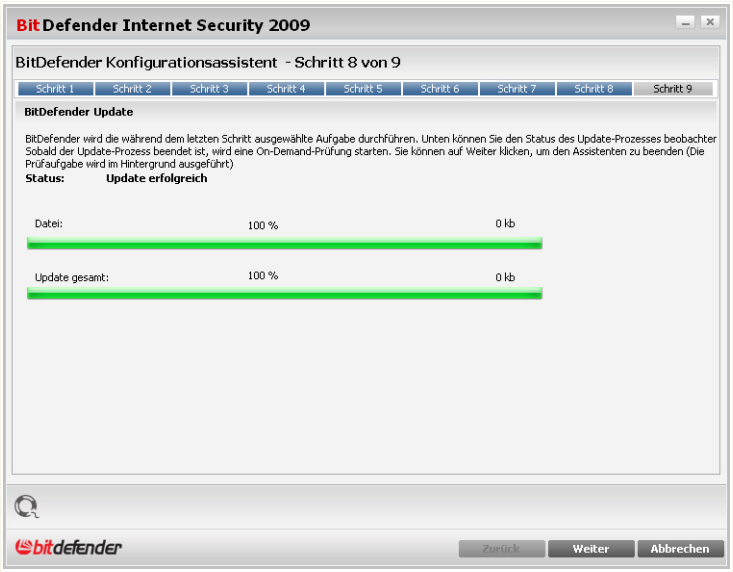
- **Update der BitDefender-Engine (möglicherweise mit Neustart)** - Beim nächsten Schritt wird ein Update der BitDefender-Engine durchgeführt, um Ihren Computer gegen aktuelle Gefahren zu schützen.
- **Schnelle Systemprüfung (erfordert möglicherweise einen Neustart)** - Während des nächsten Schrittes wird eine Schnellprüfung durchgeführt, damit BitDefender sicherstellen kann, dass Ihre Dateien in den Verzeichnissen `Windows` und `Programme` nicht infiziert sind.
- **Jeden Tag um 02:00 Uhr einen Prüfvorgang ausführen** - führt jeden Tag 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.

Klicken Sie auf **Weiter**.

2.2.8. Schritt 8/9 - Warten bis Aufgaben vervollständigt wurden

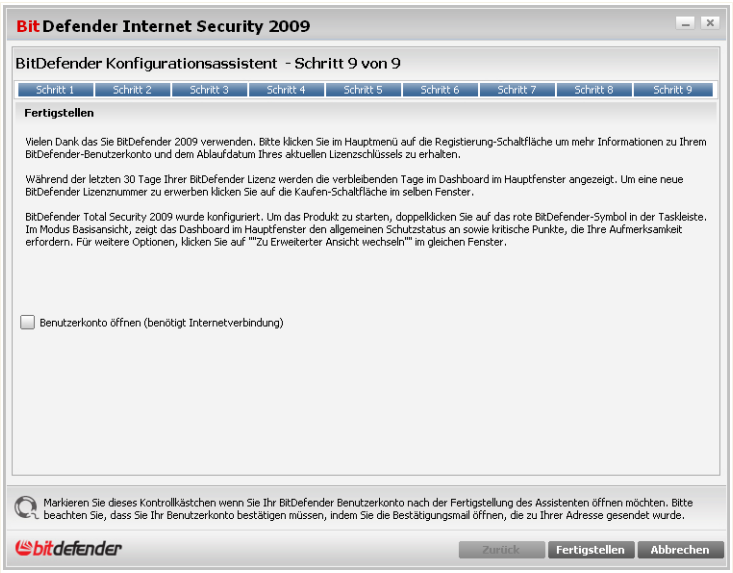


Status

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

Klicken Sie auf **Weiter**.

2.2.9. Schritt 9/9 - Fertigstellen



Fertigstellen

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

Klicken Sie auf **Fertigstellen**.

3. Upgrade

Um den Upgrade von einer älteren BitDefender Version auf den BitDefender Internet Security 2009 durchzuführen, befolgen Sie die folgenden Schritte:

1. **Optional!** Falls diese Version Antispam enthält, können Sie vor dem Upgrade des Produktes die Freunde und Spammer Liste speichern. Nach dem Upgrade können diese wieder geladen werden. Für weitere Informationen benutzen Sie die Hilfedatei oder das Handbuch des Produktes.
2. Wir empfehlen eine ältere Version von BitDefender zu entfernen. Für weitere Informationen benutzen Sie die Hilfedatei oder das Handbuch des Produktes.
3. Bitte starten Sie Ihren Computer neu.
4. Installieren Sie den BitDefender Internet Security 2009 wie es hier beschrieben ist: „*BitDefender installieren*“ (S. 4).

4. BitDefender reparieren oder entfernen

Wenn Sie das Programm **BitDefender Internet Security 2009**reparieren oder entfernen möchten, gehen Sie über das Windows-Startmenü wie folgt vor: **Start** → **Programme** → **BitDefender 2009** → **Reparieren oder Deinstallieren**.

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

- **Reparieren** - dient zur Neuinstallation sämtlicher Programmkomponenten, die beim vorhergegangenen Setup installiert wurden.

  Wenn Sie Reparieren von BitDefender wählen erscheint ein neues Fenster. Klicken Sie auf **Reparieren** um die Reparatur zu starten.

  Starten Sie den Computer neu wenn Sie dazu aufgefordert werden, anschliessend klicken Sie bitte auf **Installieren** um BitDefender Internet Security 2009 neu zu installieren.

  Wenn der Installationsprozess abgeschlossen wurde erscheint ein neues Fenster. Klicken Sie auf **Fertigstellen**.

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

  Anmerkung
  Wir empfehlen die Option **Entfernen** zu verwenden um eine saubere Neuinstallation durchzuführen.

  Wenn Sie BitDefender entfernen wählen erscheint ein neues Fenster.

  Wichtig
  Durch das Entfernen von BitDefender sind Sie nicht länger vor Viren, Spyware und Hackern geschützt. Wenn Sie möchten das die Windows Firewall und Windows Defender (Nur in Windows Vista) nach der Deinstallation wieder aktiviert werden, selektieren Sie die entsprechende Option.

  Klicken Sie auf **Entfernen** um mit der Deinstallation von BitDefender Internet Security 2009 zu beginnen.

  Während der Deinstallation werden Sie gefragt ob Sie uns ein Feedback senden möchten. Bitte klicken Sie auf **OK** um an einer Onlineumfrage mit höchstens fünf Fragen teilzunehmen. Wenn Sie nicht an der Umfrage teilnehmen möchten klicken Sie einfach auf **Abbrechen**.

Sobald der Entfernungsprozess abgeschlossen wurde erscheint ein neues Fenster. Klicken Sie auf **Fertigstellen**.

Während dem Entfernen ist ein Fehler aufgetreten

Wenn während der Deinstallation von BitDefender ein Fehler auftritt wird der Vorgang abgebrochen, ein neues Fenster öffnet sich. Klicken Sie auf **Uninstall Tool starten** um sicher zu stellen das BitDefender vollständig entfernt wurde. Das Uninstall Tool entfernt alle Dateien und Registryeinträge welche durch die automatische Deinstallation nicht entfernt wurden.

Grundkonfiguration

5. Erste Schritte

Sobald Sie BitDefender installiert haben ist Ihr Computer geschützt.

5.1. BitDefender Internet Security 2009 starten

Der erste Schritt besteht in dem Starten von BitDefender.

Sie erreichen die Benutzeroberfläche von BitDefender Internet Security 2009 über das Windows-Startmenü: **Start** → **Programme** → **BitDefender 2009** → **BitDefender Internet Security 2009**. Schneller geht es jedoch mittels Doppelklick auf das **BitDefender Symbol** in der Systemleiste.

5.2. Ansichtmodus der Benutzeroberfläche

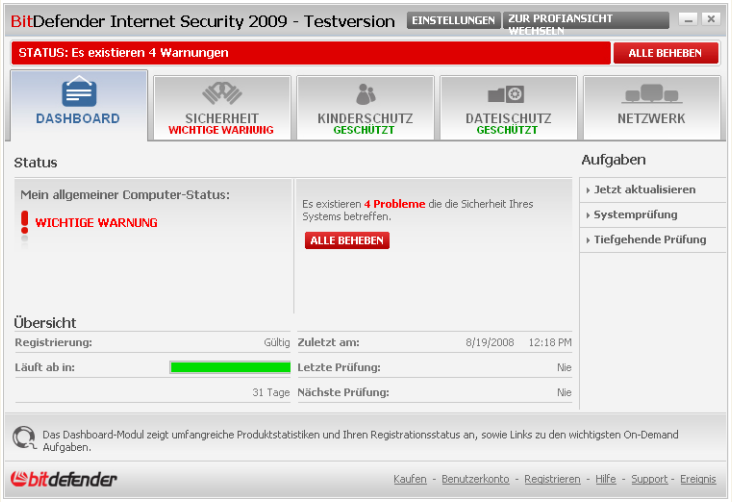
BitDefender Internet Security 2009 entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.

Sie können wählen ob Sie BitDefender im Basis- oder erweitertem Modus betrachten möchten, je nach Ihrer Erfahrung mit dem Produkt.

Anmerkung
Sie können ganz einfach eines dieser Fenster auswählen, indem Sie entweder auf die Schaltfläche **Zur Basisansicht wechseln** oder auf **Zur erweiterten Ansicht wechseln** klicken.

5.2.1. Basisansicht

Die Basisansicht ist eine einfache Benutzeroberfläche, mit der Sie Zugang zu den Basiseinstellungen aller Module haben. Sie müssen nur die Warnungen beachten und ungewünschte Probleme lösen.



Basisansicht

- Wie Sie leicht bemerken können befinden sich im oberen Bereich des Fensters zwei Schaltflächen und eine Statusleiste.

Objekt	Beschreibung
Einstellungen	Öffnet ein Fenster in dem Sie wichtige Sicherheitsmodule einfach aktivieren oder deaktivieren können (Firewall, Stealth-Modus, Automatisches Update, Spiele-Modus, usw).
Zur erweiterten Ansicht wechseln	Öffnet das Fenster der erweiterten Ansicht. Hier können Sie die vollständige Liste der Module sehen und jede Komponente bis ins Detail konfigurieren. BitDefender wird Sie an diese Option erinnern, wenn Sie das nächste Mal die Benutzeroberfläche öffnen.
Status	Beinhaltet Informationen und hilft Ihnen Anfälligkeiten der Sicherheit Ihres Computers zu beheben.

- In der Mitte des Fensters befinden sich fünf Tabs.

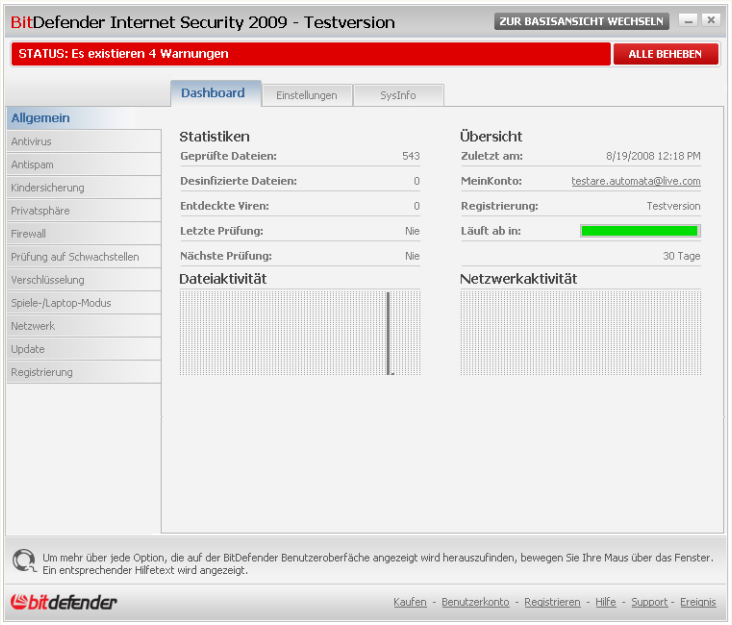
Tab	Beschreibung
Dashboard	Zeigt wichtige Produktstatistiken und Ihren Registrierungsstatus an sowie Links zu den wichtigsten On-Demand Aufgaben.
Sicherheit	Zeigt den Status der Sicherheitsmodule an (Antivirus, Antiphishing, Firewall, Antispam, IM-Verschlüsselung, Privatsphäre, Prüfung auf Anfälligkeit und Update-Module) sowie Links zu Antivirus-, Update- und Anfälligkeitsprüfungs-Aufgaben.
Kindersicherung	Zeigt den Status der Module an mit denen Sie den Zugriff Ihrer Kinder auf das Internet oder auf bestimmte Programme begrenzen können.
Datei-Manager	Zeigt den Status des Dateischutzes an sowie Links zum Dateischutz.
Netzwerk	Zeigt die Struktur des BitDefender Home-Netzwerkes an.

- Außerdem enthält die BitDefender Basisansicht mehrere nützliche Verknüpfungen.

Link	Beschreibung
Mein Benutzerkonto	Bietet Ihnen die Möglichkeit, ein BitDefender Benutzerkonto zu erstellen oder sich in ein bestehendes einzuloggen.
Registrieren	Bietet Ihnen die Möglichkeit einen neuen Lizenzschlüssel einzugeben oder den aktuellen Lizenzschlüssel und den Registrierungsstatus zu betrachten.
Hilfe anzeigen	Gibt Ihnen Zugriff auf eine Hilfedatei die Sie bei der Verwendung von BitDefender unterstützt.
Support	Bietet Ihnen die Möglichkeit das BitDefender Support Team zu kontaktieren.
Historie	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.

5.2.2. Fortgeschrittene Ansicht

Die erweiterte Ansicht bietet Ihnen Zugriff zu jeder einzelnen Komponente des BitDefender Produktes. Sie werden die erweiterten Einstellungen konfigurieren sowie erweiterte Funktionen anwenden können.



Fortgeschrittene Ansicht

- Wie Sie bemerken werden befinden sich im oberen Teil des Fensters eine Schaltfläche und eine Statusleiste.

Objekt	Beschreibung
Zu Basisansicht wechseln	Öffnet das Fenster der Basisansicht. Hier können Sie die Basisbenutzeroberfläche von BitDefender sehen, einschließlich der wichtigsten Module (Sicherheit, Tuning, Datei-Manager, Netzwerk) sowie ein Dashboard. BitDefender

Objekt	Beschreibung
	wird Sie an diese Option erinnern wenn Sie die Benutzeroberfläche das nächste Mal öffnen.
Status	Beinhaltet Informationen und hilft Ihnen Anfälligkeiten der Sicherheit Ihres Computers zu beheben.

- Auf der linken Seite des Fensters sehen Sie ein Menu, das alle Sicherheitsmodule beinhaltet:

Modul	Beschreibung
Allgemein	Hier haben Sie Zugriff zu den allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen betrachten.
Antivirus	Bietet Ihnen die Möglichkeit Ihr Virus-Schild und Prüfprozesse zu konfigurieren, Ausnahmen festzulegen und das Quarantäne-Modul zu konfigurieren.
Antispam	Bietet Ihnen die Möglichkeit Ihr Postfach SPAM-frei zu halten und die Antispam-Einstellungen zu konfigurieren.
Firewall	Die Firewall schützt Ihren Computer vor unberechtigten eingehenden und ausgehenden Zugriffen. Sie überwacht Ihre Verbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.
Privatsphäre-Kontrolle	Bietet Ihnen die Möglichkeit Datendiebstahl von Ihrem Computer vorzubeugen und Ihre Privatsphäre zu schützen während Sie online sind.
Kindersicherung	Bietet Ihnen die Möglichkeit Ihre Kinder gegen jugendgefährdende Inhalte zu schützen. Nutzen Sie dabei Ihre selbst festgelegten Regeln.
Verschlüsselung	Bietet Ihnen die Möglichkeit Unterhaltungen über Yahoo und Windows Live (MSN) Messenger zu verschlüsseln und Ihre wichtigen Dateien, Ordner und Partitionen lokal zu verschlüsseln.
Schwachstellen	Bietet Ihnen die Möglichkeit wichtige Software auf Ihrem PC stets auf dem neusten Stand zu halten.

Modul	Beschreibung
Spiele-/Laptop-Modus	Bietet Ihnen die Möglichkeit voreingestellte Prüfaufgaben, während Ihr Laptop über einen Akku betrieben wird. Weiterhin können Pop-ups und Benachrichtigungen vermieden werden während Sie spielen.
Netzwerk	Bietet Ihnen die Möglichkeit mehrere Computer in Ihrem Haushalt zu verwalten und konfigurieren.
Update	Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.
Registrierung	Bietet Ihnen die Möglichkeit BitDefender Internet Security 2009 zu registrieren, einen Lizenzschlüssel zu wechseln oder ein BitDefender Benutzerkonto zu erstellen.

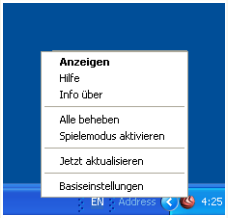
- Außerdem enthält die erweiterte Ansicht von BitDefender mehrere nutzliche Verknüpfungen.

Link	Beschreibung
Mein Benutzerkonto	Bietet Ihnen die Möglichkeit, ein BitDefender Benutzerkonto zu erstellen oder sich in ein bestehendes einzuloggen.
Registrieren	Bietet Ihnen die Möglichkeit einen neuen Lizenzschlüssel einzugeben oder den aktuellen Lizenzschlüssel und den Registrierungsstatus zu betrachten.
Hilfe anzeigen	Gibt Ihnen Zugriff auf eine Hilfedatei die Sie bei der Verwendung von BitDefender unterstützt.
Support	Bietet Ihnen die Möglichkeit das BitDefender Support Team zu kontaktieren.
Historie	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.

5.3. BitDefender Symbol im Infobereich der Taskleiste

Um das Produkt schneller zu verwalten können Sie auch das BitDefender Icon im Systemtray verwenden.

Wenn Sie dieses Icon doppelklicken öffnet sich BitDefender. Außerdem haben Sie die Möglichkeit das Produkt zu konfigurieren indem Sie das Icon mit der rechten Maustaste anklicken.



BitDefender Symbol

- **Anzeigen** - Öffnet BitDefender.
- **Hilfe** - Öffnet die Hilfedatei in der BitDefender Internet Security 2009 genau erklärt wird.
- **Über** - Öffnet die BitDefender Webseite.
- **Alle beheben** - Hilft Ihnen bei der Behebung von Sicherheitsrisiken.
- **Spielmodus ein-/ausschalten** - aktiviert/deaktiviert den Spielmodus.
- **Jetzt Aktualisieren** - ein Update wird unverzüglich durchgeführt. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.
- **Basiseinstellungen** - bietet Ihnen die Möglichkeit wichtige Sicherheitsmodule einfach zu aktivieren/deaktivieren. Ein neues Fenster wird erscheinen, in dem Sie sie mit einem einzigen Klick aktivieren/deaktivieren können.

Wenn der Spielmodus aktiviert ist, sehen Sie den Buchstaben G über dem BitDefender Symbol.

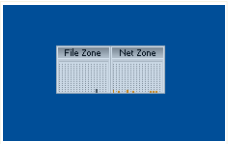
Wenn die Sicherheit Ihres Systems bedroht ist, sehen Sie ein Ausrufezeichen über dem BitDefender Symbol. Sie bekommen die Anzahl der Gefahren für Ihr System angezeigt, wenn Sie mit dem Mauszeiger auf das Symbol gehen.

5.4. Scanaktivitsänzeige

Die **Scan Aktions-Anzeige** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.

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

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



Aktivitätsanzeige

Anmerkung

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

Sie können die **Aktivitätsanzeige** zum Prüfen von Objekten verwenden. Ziehen Sie die Objekte hierzu einfach mit der Maus auf die Anzeige und lassen Sie diese dann los. Für weitere Informationen fahren Sie bitte fort mit „*Prüfen per Drag & Drop*“ (S. 160).

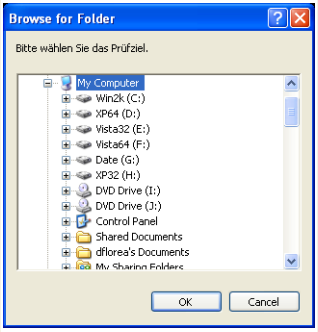
Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**. Um dieses Fenster vollständig zu verbergen, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Zu erweiterter Ansicht wechseln** (wenn Sie sich in der**Basisansicht** befinden).
2. Klicken Sie auf das Modul **Allgemein** in dem Menu auf der linken Seite.
3. Klicken Sie auf den Tab **Einstellungen**.
4. Deaktivieren Sie das Kontrollkästchen **Scanaktivitätsleiste aktivieren (Bildschirmgrafik der Produktaktivität)**.

5.5. BitDefender Manuelle Prüfung

Wenn Sie schnell einen bestimmten Ordner prüfen möchten können Sie den BitDefender Prüfvorgang verwenden.

Um die BitDefender Manuelle Prüfung zu starten, verwenden Sie das Startmenü: **Start → Programme → BitDefender 2009 → BitDefender Manuelle Prüfung** Das folgende Fenster wird erscheinen:



BitDefender Manuelle Prüfung

Alles was Sie tun müssen ist den gewünschten Ordner zu wählen und anschliessend auf **OK** zu klicken. Der BitDefender Scanner wird erscheinen und Sie durch den Prüfprozess führen.

5.6. Spiele-Modus

Der Spielmodus verändert die Schutzeinstellungen derart, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist. Wenn Sie den Spielmodus aktivieren werden folgende Einstellungen angewendet:

- Berechnungszeit & Speicherverbrauch minimieren
- Automatische Updates & Prüfungen hinausschieben
- Alle Benachrichtigungen und Pop-Ups deaktivieren
- Nur die wichtigsten Dateien prüfen

Wenn der Spielmodus aktiviert ist, sehen Sie den Buchstaben `G` über dem BitDefender Symbol.

5.6.1. Spielmodus benutzen

Sie können eine der folgenden Methoden wählen, um den Spielmodus zu aktivieren:

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

Wichtig
Vergessen Sie nicht den Spielmodus später wieder auszuschalten. Befolgen Sie dazu die selben Schritte wie zum Einschalten des Spielmodus.

5.6.2. Tastenkombination für Spielmodus ändern

Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Zu erweiterter Ansicht wechseln** (wenn Sie sich in der**Basisansicht** befinden).
2. Klicken Sie auf **Spiele/Laptop Modus** in dem Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Spiele-Modus**.
4. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**.
5. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :
   - Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination `Strg+Alt+D` benutzen möchten, markieren Sie `Strg` und `Alt` und geben Sie `D` ein.

Anmerkung
Wenn Sie die Markierung neben **Tastenkombination aktivieren** entfernen, wird die Tastenkombination deaktiviert.

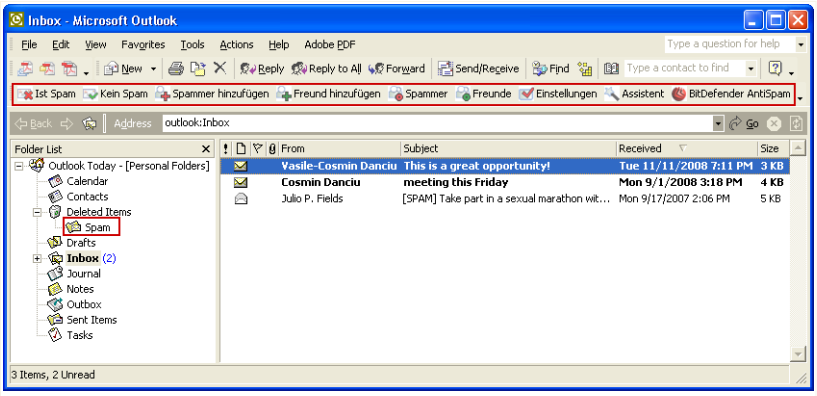
5.7. Integration in Mail Clients

BitDefender integriert sich über eine intuitive und einfach anzuwendende Leisten in die folgenden Mail Clients:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

5.7.1. Antispam Symbolleiste

Im oberen Bereich des Mail Clients können Sie die Antispamleiste sehen.



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.

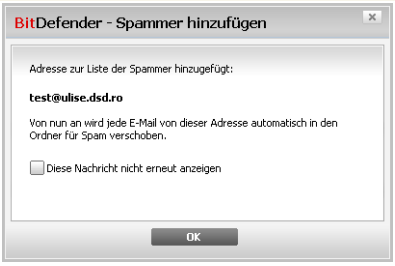
- **Kein Spam** - Klicken Sie auf diesen Button und das bayesianische Modul erkennt die ausgewählten Mails nicht als Spam. Sie werden nicht als **Spam** markiert und in den **Posteingang** verschoben.

  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 NachrichtIhrer **Spammerliste** hinzuzufügen.



Spammer hinzufügen

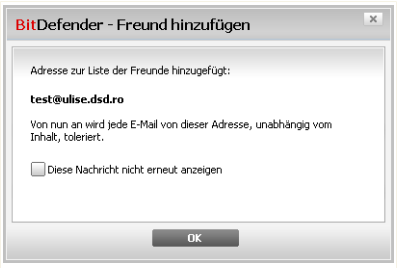
Wählen Sie **Diese Nachricht nicht erneut anzeigen**, um dieses Fenster nicht mehr zu sehen, wenn Sie eine neue Spam-Mail in die Liste aufnehmen.

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 dieserMail Ihrer **Freundesliste** hinzuzufügen.



Freund 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** - Öffnen Sie **Spammerliste**. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleichwelchen 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 **Windows Addressenbuch** / **Outlook Express Pfade** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail** zu impotieren, wählen Sie die adäqute Option aus **Importiere E-Mail Adressen aus** Menu.

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.

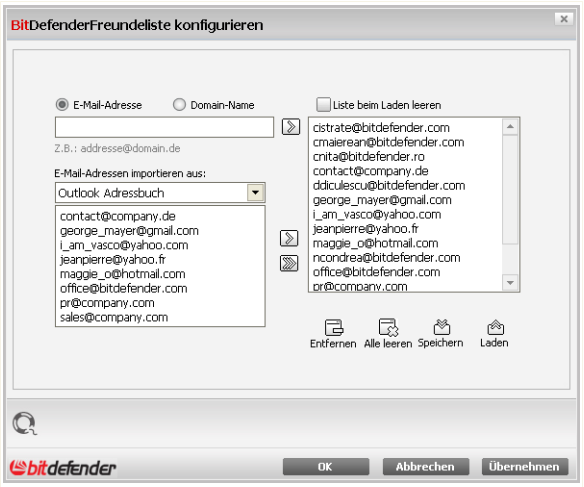
Benutzen Sie die **Speichern**/ **laden** Buttons, um **Spammerliste** zu speichern oder um zu laden. Die Datei wird die `.bwl` Endung haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Liste beim Laden leeren**.

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

- **Freunde** - Öffnen Sie **Freundenliste**. Sie enthält alle E-Mail-Adressen, von denen Sie immer Nachrichten erhalten wollen, gleichwelchen 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 **Windows Addressenbuch** / **Outlook Express Pfade** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail** zu impotieren, wählen Sie die adäqute Option aus **Importiere E-Mail Adressen aus** Menu.

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 **Freundenliste** zu speichern oder um zu laden. Die Datei wird die `.bwl` Endung haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Liste beim Laden 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

Die folgenden Optionen sind verfügbar:

- **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** - öffnet die BitDefender Benutzeroberfläche.

5.7.2. Konfigurationsassistent

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

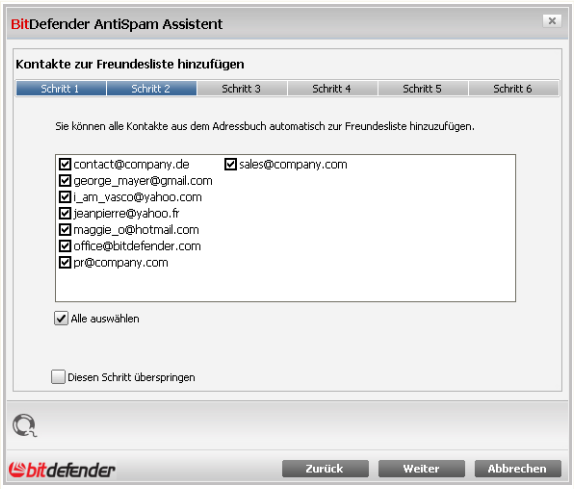
Anmerkung
Der Assistent kann jederzeit über die Schaltfläche **Assistent** in der Antispam-Toolbaraufgerufen werden.

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.

Um einen Kontakt zur Freundesliste hinzuzufügen klicken Sie auf **Alle auswählen**.

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

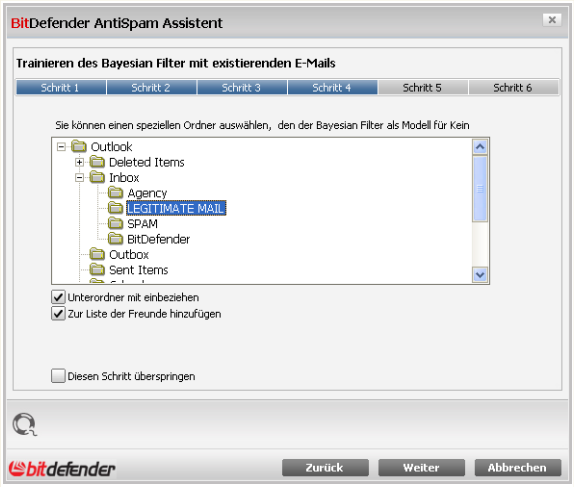
Sie finden heraus, dass Ihr Antispam-Filter an Effektivität verloren hat. Dies kann daher kommen, dass das Training nicht genau durchgeführt worden ist (z. B. haben Sie versehentlich eine Anzahl legitimer Mails als Spam markiert oder umgekehrt). Falls Ihr Filter sehr ungenau arbeitet, müssen Sie Ihre 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

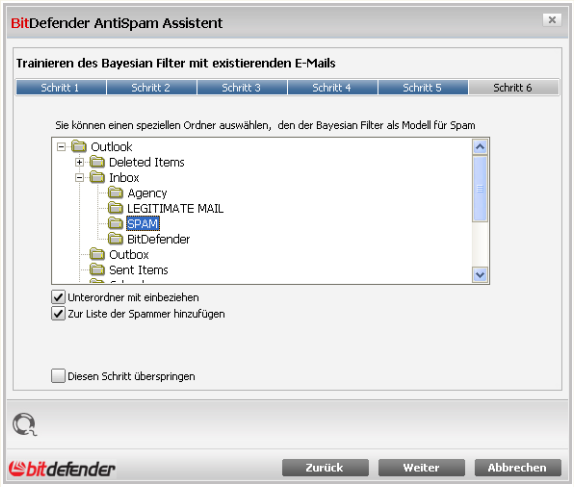
Bitte wählen Sie einen Ordner, der legitime E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam Filter zu trainieren.

Es gibt zwei weitere Optionen unter der Ordnerliste:

- **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.

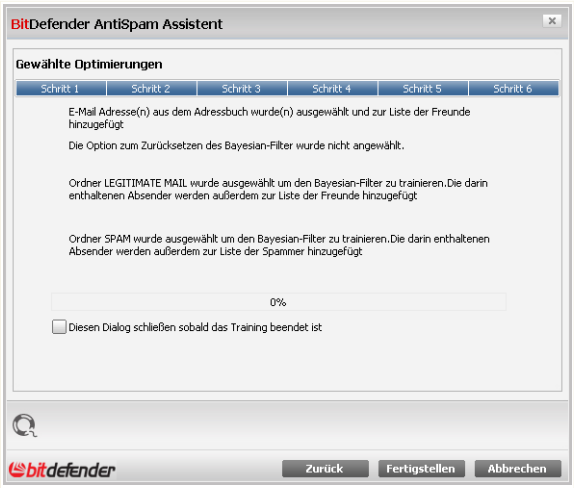
Wichtig
Bitte vergewissern Sie sich, dass der von Ihnen gewählte Ordner keine legitimen E-Mails enthält, ansonsten wird die Antispam-Leistung beträchtlich reduziert.

Es gibt zwei weitere Optionen unter der Ordnerliste:

- **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**.

5.8. Integration in Web-Browser

BitDefender schützt Sie während des Surfens vor Phishingversuchen. Er prüft die Webseiten auf welche Sie zugreifen und warnt Sie vor Phishingseiten. Eine Whitelist von Webseiten welche nicht durch BitDefender geprüft werden kann ebenfalls erstellt werden.

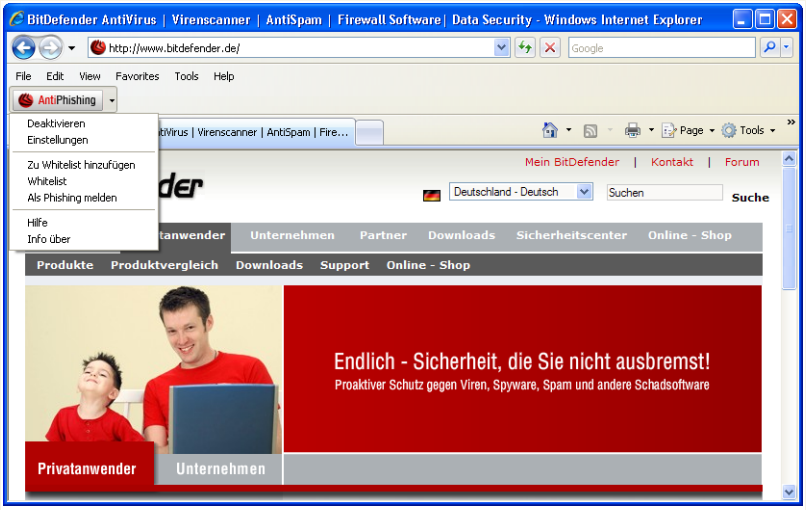
BitDefender integriert sich über eine intuitive und einfach anzuwendende Toolbar in die folgenden Web-Browser:

- Internet Explorer
- Mozilla Firefox

Sie können die Antiphishingeinstellungen und die Whitelist leicht und effizient über die BitDefender Antiphishingleiste in den oben genannten Browsern verwalten.

Die Antiphishingleiste, symbolisiert durch das **BitDefender Icon**, finden Sie im oberen Bereich des Browsers. Klicken Sie dieses an um die Leiste anzuzeigen.

Anmerkung
Sollten Sie die Leiste nicht sehen dann klicken Sie auf **Extras**, **Menüleiste** und wählen Sie **BitDefender Leiste**.



Antiphishingleiste

Folgende Aktionen stehen in der Leiste zur Verfügung:

- **Aktivieren/Deaktivieren** - Aktiviert/deaktiviert die BitDefender Antiphishingleiste.

  Anmerkung
  Wenn Sie die Antiphishingleiste beenden werden Sie nicht länger von Phishingversuchen geschützt.

- **Einstellungen** - Öffnet ein Fenster in welchem Sie Einstellungen zur Antiphishingleiste vornehmen können.

  Die folgenden Optionen sind verfügbar:

- **Prüfung aktivieren** - Aktiviert/deaktiviert die Antiphishingprüfung.
- **Vor dem Hinzufügen zur Whitelist fragen** - Frägt Sie bevor eine Webseite zur Whitelist hinzugefügt wird.

■ **Zu Whitelist hinzufügen** - Fügt die momentane Webseite zur Whitelist hinzu.

Anmerkung
Durch das hinzufügen zur Whitelist wird die Seite nicht mehr von BitDefender auf Phishing geprüft. Wir empfehlen Ihnen nur Seiten hinzuzufügen welchen Sie vollständig vertrauen.

■ **Whitelist zeigen** - Öffnet die Whitelist.

Sie können eine Liste der Webseiten sehen welche nicht von BitDefender Antiphishing geprüft werden.

Wenn Sie eine Webseite aus der Whitelist entfernen möchten, sodass die Webseite wieder auf Phishing geprüft wird, klicken Sie auf **Entfernen** neben dem gewünschten Eintrag.

Sie können Webseiten, welchen Sie vollständig vertrauen, zur Whitelist hinzufügen sodass diese nicht auf Phishing geprüft werden. Um eine Seite zur Whitelist hinzuzufügen geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Hinzufügen**.

■ **Hilfe** - Öffnet die Hilfedatei.
■ **Über** - Öffnet ein Fenster in welchem Sie Informationen über BitDefender erhalten und Hilfe finden falls etwas unvorhergesehenes geschied.

5.9. Integration in Messenger

Bitdefender bietet Verschlüsselungsmöglichkeiten um Ihre vertraulichen Dokumente und Ihre Unterhaltungen über Instant Messaging mit dem Yahoo Messenger und dem MSN Messenger zu schützen.

BitDefender verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

■ Ihr Chatpartner hat eine BitDefender Verison installiert, die die IM-Verschlüsselung unterstützt und die IM-Verschlüsselung ist für die Instant Messaging Anwendung aktiviert, die verwendet wird.

■ Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.

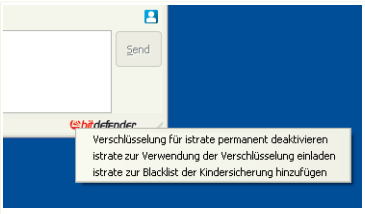
Wichtig

BitDefender verschlüsselt die Unterhaltung nicht, wenn ein Chatpartner eine webbasierte Chat-Anwendung verwendet, so wie Meebo, oder eine andere Anwendung die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt.

Sie können die IM-Verschlüsselung einfach mit der BitDefender Toolbar von dem Chat-Fenster aus konfigurieren.

Wenn Sie mit der rechten Maustaste auf die Toolbar von BitDefender klicken, erhalten Sie die folgenden Optionen:

- Verschlüsselung dauerhaft für bestimmte Chatpartner aktivieren / deaktivieren.
- Einen bestimmten Chatpartner dazu einladen, die Verschlüsselung zu nutzen
- Einen bestimmten Chatpartner von der Blacklist der Kindersicherung entfernen

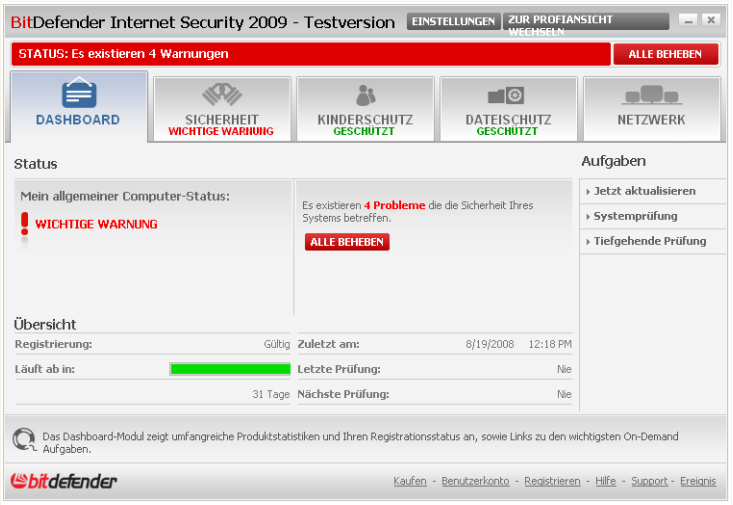


Instant Messaging Verschlüsselungsoptionen

Klicken Sie auf eine der oben genannten Optionen, um diese zu aktivieren.

6. Dashboard

Wenn Sie auf den Tab Dashboard klicken erhalten Sie umfangreiche Produktstatistiken und Informationen über Ihren Registrierungsstatus. Weiterhin werden Links zu den wichtigsten On-Demand Aufgaben angezeigt.



Dashboard

6.1. Übersicht

Hier können Sie eine Zusammenfassung der Statistiken bezüglich des Update-Status, des Status Ihres Benutzerkontos sowie Registrierungs- und Lizenzinformationen sehen.

Objekt	Beschreibung
Letztes Update	Zeigt das Datum an, zu dem Ihr BitDefender Produkt zuletzt aktualisiert wurde. Bitte führen Sie regelmäßig Updates durch, damit Ihr System vollständig geschützt ist.

Objekt	Beschreibung
Mein Benutzerkonto	Zeigt die E-Mail-Adresse an, die Sie benutzen können, um auf Ihr Online-Benutzerkonto zugreifen zu können, um Ihren Lizenzschlüssel zu erhalten und vom BitDefender Support und anderen Services profitieren zu können.
Registrierung	Zeigt Ihren Lizenzschlüssel und dessen Status an. Damit Ihr System sicher ist, müssen Sie BitDefender erneuern oder aktualisieren, wenn der Lizenzschlüssel abgelaufen ist.
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels.

Wenn Sie den BitDefender aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren** im Aufgabenbereich.

Um ein BitDefender Benutzerkonto zu erstellen oder sich in ein bestehendes einzuloggen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Link **Mein Benutzerkonto** im unteren Bereich des Fensters. Eine Webseite wird geöffnet.
2. Geben Sie Ihren Benutzernamen und das Passwort ein und klicken Sie auf **Login**.
3. Um ein BitDefender-Benutzerkonto zu erstellen, wählen Sie **Sie haben kein Benutzerkonto?** und geben Sie die benötigten Informationen ein.

Anmerkung
Die hier eingetragenen Daten bleiben vertraulich.

Um den BitDefender Internet Security 2009 zu registrieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf den Link **Mein Benutzerkonto** im unteren Bereich des Fensters. Ein Registrierungsassistent wird geöffnet.
2. Klicken Sie auf die Schaltfläche **Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren**.
3. Geben Sie den neuen Lizenzschlüssel in das entsprechende Feld ein.
4. Klicken Sie auf **Fertigstellen**.

Um einen neuen Lizenzschlüssel zu kaufen, befolgen Sie diese Schritte.

1. Klicken Sie auf den Link **Mein Benutzerkonto** im unteren Bereich des Fensters. Ein Registrierungsassistent wird geöffnet.

2. Klicken Sie auf den Link **Ihren BitDefender Lizenzschlüssel erneuern**. Eine Webseite wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Jetzt kaufen**.

6.2. Aufgaben

Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben: Vollständige Systemprüfung, tiefgehende Systemprüfung, jetzt Aktualisieren.

Folgende Aktionen stehen zur Verfügung:

- **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
- **Tiefgehende Systemprüfung** - Prüft den gesamten Computer (inklusive Archiven).
- **Jetzt Aktualisieren** - startet ein sofortiges Update.

6.2.1. Prüfen mit BitDefender

Um Ihren Computer auf Malware zu prüfen, führen Sie eine Scan-Aufgabe durch, indem Sie auf die entsprechende Schaltfläche klicken. Die folgende Tabelle zeigt Ihnen die verfügbaren San-Aufgaben mit einer Kurzbeschreibung:

Aufgabe	*Beschreibung*
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.

Anmerkung
Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

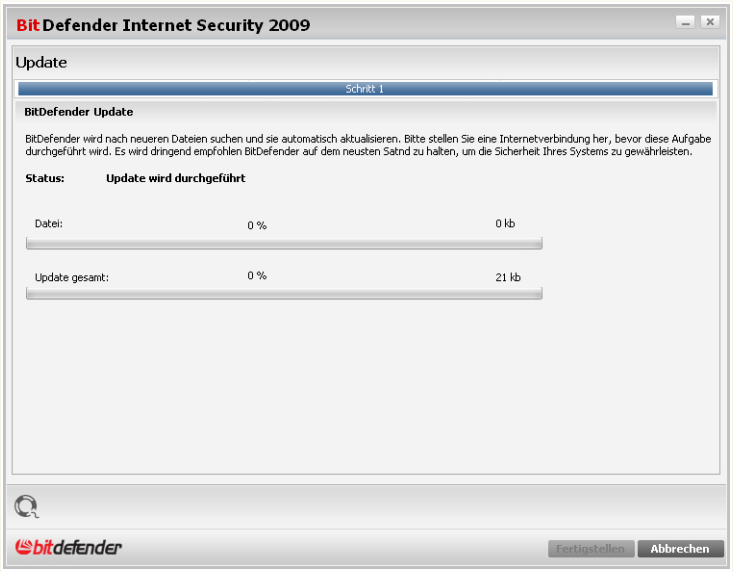
Wenn Sie einen Prüfvorgang, ob schneller oder kompletter Vorgang, starten wird der BitDefender Scanner geöffnet.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

6.2.2. BitDefender Updaten

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.

In der Standardeinstellung sucht BitDefender nach Updates wenn Sie Ihren Computer einschalten und dann **jede weitere Stunde** erneut. Wenn Sie BitDefender selbst aktualisieren möchten, klicken Sie auf **Jetzt Aktualisieren**. Der Update-Prozess wird gestartet und das folgende Fenster wird erscheinen:



BitDefender Updaten

In diesem Fenster können Sie den Status des Update-Prozesses sehen.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Wenn Sie dieses Fenster schließen möchten, klicken Sie einfach auf **Abbrechen**. Dies wird den Update-Prozess nicht anhalten.

Anmerkung
Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen.

Bitte starten Sie Ihren Computer neu, wenn dies verlangt wird. Im Falle von wichtigen Updates, werden Sie aufgefordert, Ihren Computer neu zu starten.

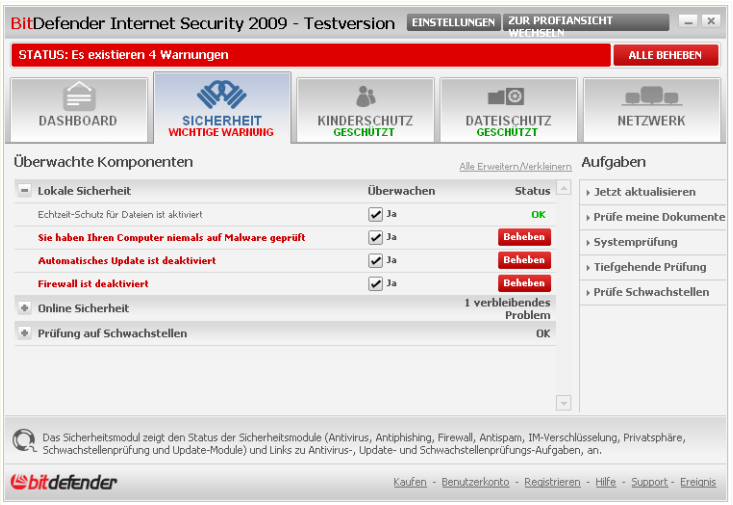
Klicken Sie auf **Neustart** um Ihr System unverzüglich neuzustarten.

Wenn Sie Ihr System später neustarten möchten, klicken Sie auf **OK**. Wir empfehlen Ihnen, das System so schnell wie möglich neuzustarten.

7. Sicherheit

BitDefender beinhaltet ein Sicherheitsmodul welches Ihr System virenfrei und aktuell hält.

Um die verfügbaren Aktionen anzuzeigen klicken Sie auf den Reiter **Sicherheit**



Sicherheit

Das Sicherheitsmodul besteht aus zwei Bereichen:

- **Überwachte Komponenten** - Hier sehen Sie die vollständige Liste der überwachten Komponenten für jedes Sicherheitsmodul. Sie können auswählen, welche Module überwacht werden sollen. Es wird empfohlen alle Komponenten zu überwachen.
- **Aufgaben** - Hier finden Sie die wichtigsten Sicherheitsaufgaben: Vollständige Systemprüfung, tiefgehende Systemprüfung, jetzt Aktualisieren.

7.1. Überwachte Komponenten

Die überwachten Komponenten sind in mehrere Kategorien unterteilt.

Kategorie	Beschreibung
Lokale Sicherheit	Hier können Sie den Status jedes Sicherheitsmoduls überprüfen, das Objekte auf Ihrem Computer schützt (Dateien, Registry, Speicher, usw).
Online-Sicherheit	Hier können Sie den Status jedes Sicherheitsmoduls überprüfen, das Ihre Online-Transaktionen und Ihren Computer schützt, während Sie im Internet sind.
Anfälligkeitsprüfung	Hier können Sie überprüfen, ob wichtige Software auf Ihrem PC auf dem neusten Stand ist. Passwörter von Windows Benutzerkonten werden nach den Sicherheitsregeln überprüft.

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

7.1.1. Lokale Sicherheit

Wir wissen dass es wichtig ist benachrichtigt zu werden, wann immer ein Problem die Sicherheit Ihres Computers beeinträchtigt. Durch das Anzeigen jedes Sicherheitsmoduls, informiert Sie BitDefender Internet Security 2009 nicht nur darüber wenn Sie Einstellungen verändern, die Einfluss auf die Sicherheit Ihres Computers haben könnten, sondern auch wenn Sie vergessen haben wichtige Aufgaben durchzuführen.

Diese Probleme bezüglich der lokalen Sicherheit, werden in expliziten Sätzen beschrieben. Wenn die Sicherheit Ihres Computers, in Übereinstimmung mit jedem Satz, irgendwie beeinträchtigt sein sollte, so werden Sie eine rote Statusfläche mit der Bezeichnung **Feststellen** sehen. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Echtzeit Dateischutz ist aktiviert	Alle Dateien werden bei Zugriff, durch Sie oder durch ein Programm auf dem System, geprüft.
Sie haben Ihren Computer heute auf Malware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.

Risiko	Beschreibung
Automatisches Update ist aktiviert	Bitte lassen Sie die automatischen Updates aktiviert, um sicherzustellen, dass die Malware-Signaturen Ihres BitDefender Produktes ständig aktualisiert werden.
Jetzt aktualisieren	Das Update des Produktes und für Malware-Signaturen wird durchgeführt.
Firewall ist aktiviert	Schützt Ihren Computer vor Hackern und schädlichen Angriffen von außen.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

7.1.2. Online Sicherheit

Die Angelegenheiten bezüglich der Online-Sicherheit werden in expliziten Sätzen beschrieben. In Übereinstimmung mit jedem Satz wird eine rote Statusfläche mit der Bezeichnung **Feststellen** angezeigt, wenn die Sicherheit Ihres Computers möglicherweise gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Antispam ist aktiviert	Gewährleistet, dass Ihre E-Mails auf Malware geprüft und nach Spams gefiltert werden.
Identitätskontrolle ist aktiviert	Hilft Ihnen vertrauliche Daten zu sichern, indem der Web- und Mail-Datenverkehr nach bestimmten Zeichenfolgen geprüft wird. Es wird empfohlen die Identitätskontrolle zu aktivieren, um Ihre vertraulichen Daten (E-Mail-Adressen, Benutzer IDs, Passwörter, Kreditkartennummern, usw) vor Diebstahl zu schützen.

Risiko	Beschreibung
Firefox Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.
Internet Explorer Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

7.1.3. Schwachstellen-Scan

Die Angelegenheiten bezüglich der Anfälligkeit werden in expliziten Sätzen beschrieben. In Übereinstimmung mit jedem Satz wird eine rote Statusfläche mit der Bezeichnung **Feststellen** angezeigt, wenn die Sicherheit Ihres Computers möglicherweise gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Anfälligkeitsprüfung ist aktiviert	Überwacht die Updates von Microsoft Windows und von Microsoft Windows Office sowie die Passwörter der Microsoft Windows Benutzerkonten, um sicherzustellen, dass Ihr Betriebssystem auf dem neusten Stand und nicht anfällig für Passwortumgehungen ist.
Wichtige Microsoft Updates	Installieren Sie wichtige Microsoft Updates.
Andere Microsoft Updates	Installieren Sie weniger wichtige Microsoft Updates.

Risiko	Beschreibung
Automatische Updates für Windows sind aktiviert	Installieren Sie neue Windows Sicherheits-Updates, sobald diese verfügbar sind.
Admin (Sicheres Passwort)	Zeigt die Passwortsicherheit für bestimmte Benutzer an.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

7.2. Aufgaben

Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben: Vollständige Systemprüfung, tiefgehende Systemprüfung, jetzt Aktualisieren.

Folgende Aktionen stehen zur Verfügung:

- **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
- **Tiefgehende Systemprüfung** - Prüft den gesamten Computer (inklusive Archiven).
- **Eigene Dateien prüfen** - Führt eine schnelle Prüfung Ihrer Eigenen Dateien durch.
- **Jetzt Aktualisieren** - startet ein sofortiges Update.
- **Prüfung auf Schwachstellen**

7.2.1. Prüfen mit BitDefender

Um Ihren Computer auf Malware zu prüfen, führen Sie eine Scan-Aufgabe durch, indem Sie auf die entsprechende Schaltfläche klicken. Die folgende Tabelle zeigt Ihnen die verfügbaren San-Aufgaben mit einer Kurzbeschreibung:

Aufgabe	Beschreibung
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Meine Dokumente prüfen	Verwenden Sie diese Aufgabe, um wichtige Ordner zu prüfen: `Meine Dokumente`, `Desktop` und `Autostart`. Das gewährleistet die Sicherheit Ihrer Dokumente, einen sicheren Arbeitsbereich und saubere Anwendungen die beim Start ausgeführt werden.

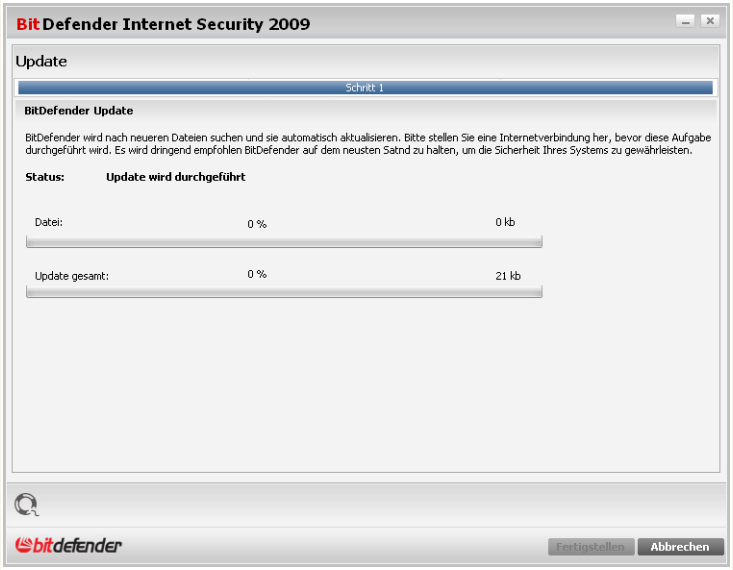
Anmerkung
Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

Wenn Sie einen Prüfvorgang, ob schneller oder kompletter Vorgang, starten wird der BitDefender Scanner geöffnet. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

7.2.2. BitDefender Updaten

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.

In der Standardeinstellung sucht BitDefender nach Updates wenn Sie Ihren Computer einschalten und dann **jede weitere Stunde** erneut. Wenn Sie BitDefender selbst aktualisieren möchten, klicken Sie auf **Jetzt Aktualisieren**. Der Update-Prozess wird gestartet und das folgende Fenster wird erscheinen:



BitDefender Updaten

In diesem Fenster können Sie den Status des Update-Prozesses sehen.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Wenn Sie dieses Fenster schließen möchten, klicken Sie einfach auf **Abbrechen**. Dies wird den Update-Prozess nicht anhalten.

Anmerkung
Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen.

Bitte starten Sie Ihren Computer neu, wenn dies verlangt wird. Im Falle von wichtigen Updates, werden Sie aufgefordert, Ihren Computer neu zu starten.

Klicken Sie auf **Neustart** um Ihr System unverzüglich neuzustarten.

Wenn Sie Ihr System später neustarten möchten, klicken Sie auf **OK**. Wir empfehlen Ihnen, das System so schnell wie möglich neuzustarten.

7.2.3. Prüfung auf Schwachstellen/Anfälligkeit

Die Prüfung auf Schwachstellen überprüft die Microsoft Windows Updates, Microsoft Windows Office Updates und die Passwörter Ihrer Microsoft Windows Benutzerkonten, um sicherzustellen, dass Ihr Betriebssystem auf dem neusten Stand ist und keine Anfälligkeit für eine Passwortumgehung besteht.

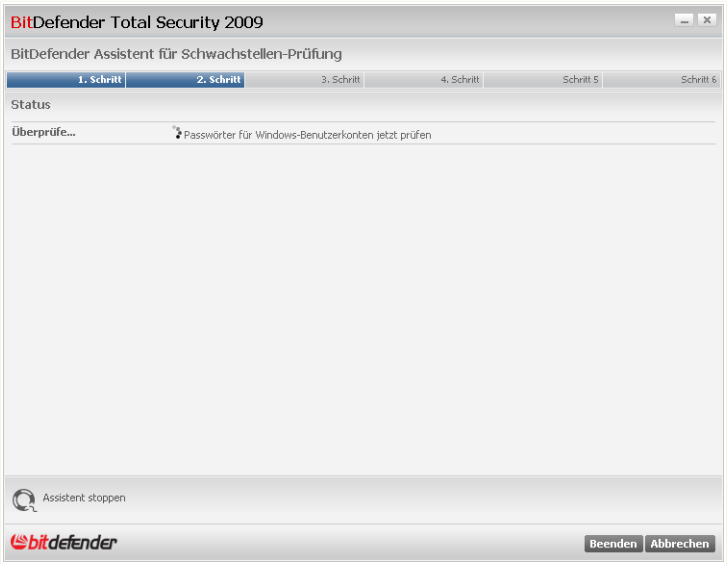
Um Ihren Computer auf Schwachstellen zu prüfen, klicken Sie auf **Prüfung auf Schwachstellen** und folgen Sie den Schritten des Assistenten.

Schritt 1/6 - Auswahl der zu prüfenden Schwachstellen

Schwachstellen

Klicken Sie auf **Weiter** um das System auf die ausgewählten Schwachstellen zu überprüfen.

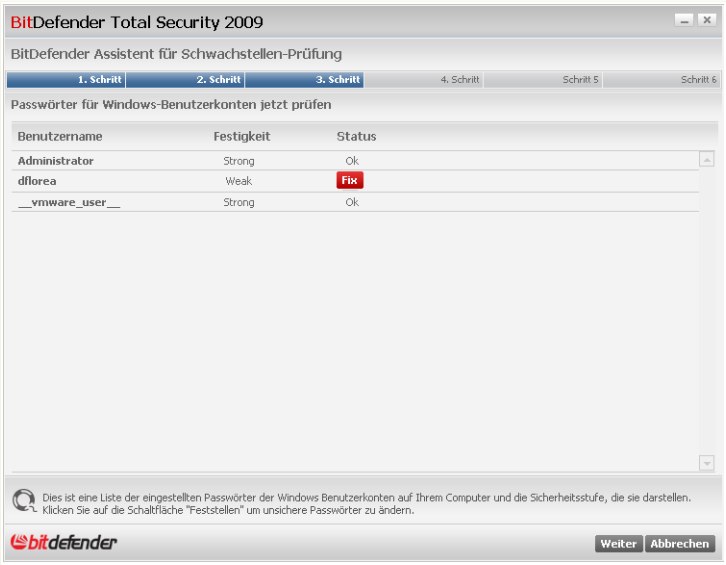
Schritt 2/6 - Nach Schwachstellen suchen



Prüfung auf Schwachstellen

Bitte warten Sie bis BitDefender die Prüfung auf Schwachstellen beendet hat.

Schritt 3/6 - Unsicheres Passwort ändern



Passwörter von Benutzern

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.

Klicken Sie auf **Beheben**, um unsichere Passwörter zu ändern. Ein neues Fenster wird sich öffnen.

Passwort ändern

Wählen Sie die Methode um ein Problem zu beheben:

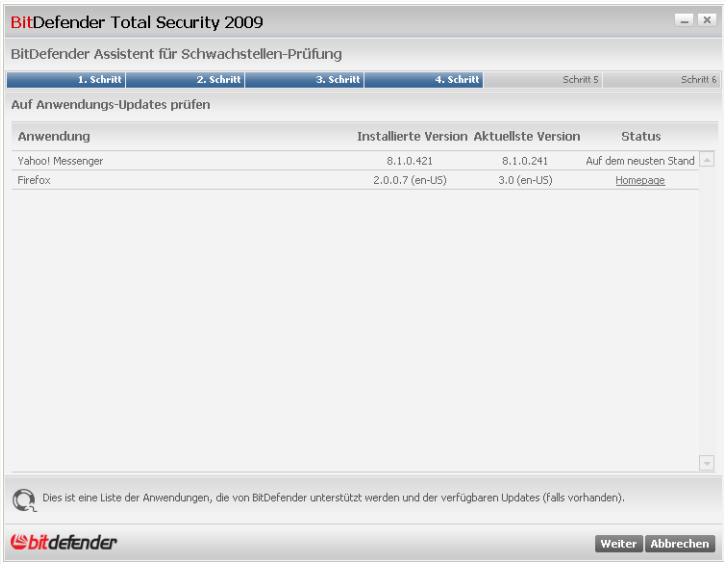
- **Den Benutzer zwingen das Passwort beim nächsten Login zu ändern.** Beim nächsten Windows-Login wird BitDefender den Benutzer dazu auffordern das Passwort zu ändern.
- **Benutzerpasswort ändern.** Geben Sie das neue Passwort in jedes der Editierfelder ein.

Anmerkung
Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

Klicken Sie auf **OK**, um das Passwort zu ändern.

Klicken Sie auf **Weiter**.

Schritt 4/6 - Anwendungen aktualisieren



Anwendungen

Sie können eine Liste der Anwendungen sehen, die von BitDefender geprüft wurden und ob diese auf dem neusten Stand sind. Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

Klicken Sie auf **Weiter**.

Schritt 5/6 - Windows aktualisieren

Windows Updates

Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zur Zeit nicht auf Ihrem Computer installiert sind. Klicken Sie auf **Alle System-Updates installieren**, um die verfügbaren Updates zu installieren.

Klicken Sie auf **Weiter**.

Schritt 6/6 - Ergebnisse betrachten

Ergebnisse

Klicken Sie auf **Schließen**.

8. Kindersicherung

BitDefender beinhaltet ein Kindersicherungsmodul welches Ihnen dabei hilft

Um das Kindersicherungsmodul zu öffnen, klicken Sie auf den Tab **Elternteil**

Kindersicherung

Das Kindersicherungsmodul besteht aus zwei Bereichen:

- **Überwachte Komponenten** - Hier sehen Sie die vollständige Liste der überwachten Komponenten für jedes Sicherheitsmodul. Sie können auswählen, welche Module überwacht werden sollen. Es wird empfohlen alle Komponenten zu überwachen.
- **Aufgaben** - Hier finden Sie die wichtigsten Sicherheitsaufgaben: Vollständige Systemprüfung, tiefgehende Systemprüfung, jetzt Aktualisieren.

8.1. Überwachte Komponenten

Die überwachte Komponente ist die folgende:

Kategorie	Beschreibung
Kindersicherung	Hier können Sie den Status Moduls Kindersicherung überprüfen, das Ihnen die Möglichkeit gibt, den Zugriff Ihrer Kinder auf das Internet oder bestimmte Anwendungen zu begrenzen.

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

8.1.1. Kindersicherung

Die Kindersicherung überwacht den Status der Module, die Ihnen die Möglichkeit geben den Zugang von Kindern zum Internet oder zu bestimmten Anwendung zu begrenzen.

Die Angelegenheiten bezüglich der Kindersicherung werden in expliziten Sätzen beschrieben. In Übereinstimmung mit jedem Satz wird eine rote Statusfläche mit der Bezeichnung **Feststellen** angezeigt, wenn ein Vorgang den Schutz Ihrer Kinder beeinträchtigt. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Kindersicherung ist nicht konfiguriert	Die Kindersicherung kann den Zugang zu unangemessenen Web-Seiten oder zum Internet für bestimmte Zeiträume blockieren und E-Mails, IM und den Web-Datenverkehr nach bestimmten Schlüsselwörtern usw filtern

Wenn die Statusfläche grün ist, können Ihre Kinder sicher das Internet benutzen. Um zu erreichen, dass diese Fläche grün ist, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

8.2. Aufgaben

Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben: Vollständige Systemprüfung, tiefgehende Systemprüfung, jetzt Aktualisieren.

Folgende Aktionen stehen zur Verfügung:

- **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
- **Tiefgehende Systemprüfung** - Prüft den gesamten Computer (inklusive Archiven).
- **Jetzt Aktualisieren** - startet ein sofortiges Update.

8.2.1. Prüfen mit BitDefender

Um Ihren Computer auf Malware zu prüfen, führen Sie eine Scan-Aufgabe durch, indem Sie auf die entsprechende Schaltfläche klicken. Die folgende Tabelle zeigt Ihnen die verfügbaren San-Aufgaben mit einer Kurzbeschreibung:

Aufgabe	Beschreibung
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.

Anmerkung

Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

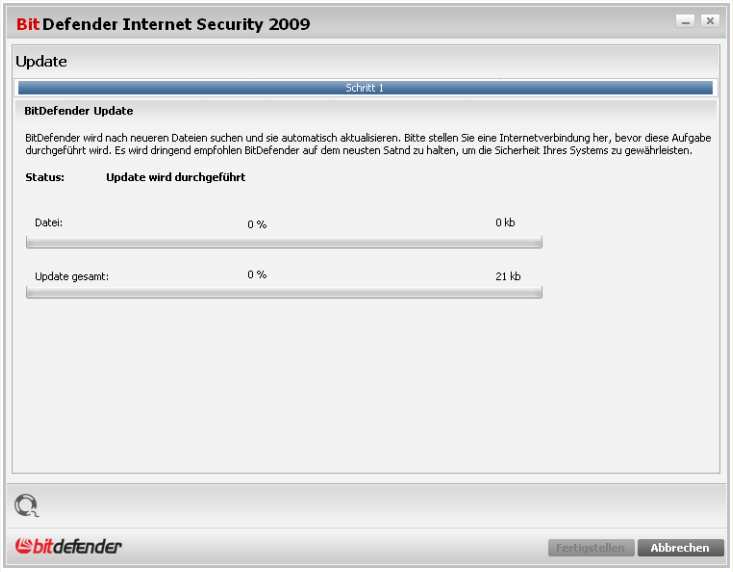
Wenn Sie einen Prüfvorgang, ob schneller oder kompletter Vorgang, starten wird der BitDefender Scanner geöffnet.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

8.2.2. BitDefender Updaten

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.

In der Standardeinstellung sucht BitDefender nach Updates wenn Sie Ihren Computer einschalten und dann **jede weitere Stunde** erneut. Wenn Sie BitDefender selbst aktualisieren möchten, klicken Sie auf **Jetzt Aktualisieren**. Der Update-Prozess wird gestartet und das folgende Fenster wird erscheinen:



BitDefender Updaten

In diesem Fenster können Sie den Status des Update-Prozesses sehen.

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet, dass die entsprechenden Dateien stufenweise aktualisiert werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Wenn Sie dieses Fenster schließen möchten, klicken Sie einfach auf **Abbrechen**. Dies wird den Update-Prozess nicht anhalten.

Anmerkung
Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen.

Bitte starten Sie Ihren Computer neu, wenn dies verlangt wird. Im Falle von wichtigen Updates, werden Sie aufgefordert, Ihren Computer neu zu starten.

Klicken Sie auf **Neustart** um Ihr System unverzüglich neuzustarten.

Wenn Sie Ihr System später neustarten möchten, klicken Sie auf **OK**. Wir empfehlen Ihnen, das System so schnell wie möglich neuzustarten.

9. Datentresor

BitDefender beinhaltet einen Dateischutz, der Ihnen dabei hilft Ihre Daten nicht nur sicher, sondern auch vertraulich aufzubewahren. Um dies durchzuführen, sichern Sie Ihre Dateien im Dateischutz.

Datentresor. Sie möchten sensible Dateien sicherlich vor neugierigen Augen schützen. Hier kommt der Dateischutz des Datei Managers zum Einsatz.

- Der Dateischutz ist ein sicherer Speicherplatz für persönliche Informationen oder sensible Dateien.
- Der Dateischutz ist eine verschlüsselte Datei auf Ihrem Computer mit der Endung `bvd`.
- Durch die Verschlüsselung sind die Daten innerhalb des Schutzes sicher vor Diebstahlversuchen oder Sicherheitsproblemen.
- Wenn Sie diese`bvd` Datei mounten, wird eine logische Partition (ein neues Laufwerk) erscheinen. Es wird leichter für Sie sein dieses Prozess zu verstehen, wenn Sie an einen ähnlichen denken: Ein ISO-Image als virtuelle CD zu mounten.

Öffnen Sie einfach den Arbeitsplatz und Sie werden ein neues Laufwerk sehen, das den Dateischutz darstellt. Sie können Dateiprozesse (kopieren, löschen, ändern, usw) auf diesem Laufwerk durchführen. Die Dateien sind geschützt, solange sie sich in diesem Laufwerk befinden (denn für das Mounten ist ein Passwort notwendig). Wenn Sie fertig sind, schließen Sie Ihren Schutz ab (unmount) um dessen Inhalt zu schützen.

Um den Datei-Manager zu öffnen klicken Sie auf den Tab **Dateischutz**.

Datentresor

- **Überwachte Komponenten** - Hier können Sie eine komplette Liste der überwachten Komponenten jedes Moduls sehen. Sie können auswählen welche Module überwacht werden sollen. Es wird empfohlen die Überwachung für alle Komponenten zu aktivieren.

9.1. Überwachte Komponenten

Die überwachte Komponente ist die folgende:

Kategorie	Beschreibung
Dateischutz	Es handelt sich um einen sicheren Speicherplatz für persönliche Informationen oder sensible Dateien. Er befindet sich lokal auf Ihrem Computer. Durch die Verschlüsselung sind die Daten innerhalb des Schutzes vor Diebstahlversuchen oder Sicherheitsproblemen geschützt.

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

9.1.1. Datentresor

Die Probleme die den Privatbereich Ihrer Daten betreffen sind in expliziten Sätzen beschrieben. Übereinstimmend mit jedem Satz werden Sie eine rote Statusfläche mit der Bezeichnung **Feststellen** sehen, wenn der Privatbereich Ihrer Daten gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Dateischutz ist aktiviert	Der Datentresor schützt Ihre Dokumente indem diese verschlüsselt werden.

Wenn die Statusflächen grün sind, ist das Sicherheitsrisiko Ihrer Daten gering. Damit diese Flächen grün werden, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

9.2. Aufgaben

Folgende Aktionen stehen zur Verfügung:

- **Datei zum Schutz hinzufügen** - Startet den Assistenten zum Speichern Ihrer wichtigen Dateien/Dokumente in verschlüsselten Schutzlaufwerken.
- **Dateien aus dem Schutz entfernen** - Startet den Assistenten zum Löschen von Daten im Dateischutz.
- **Schutz ansehen** - Startet den Assistenten mit dem Sie den Inhalt eines Dateischutzes betrachten können.
- **Schutz abschließen** - Startet den Assistenten mit dem Sie den Dateischutz abschließen können, um seinen Inhalt zu schützen.

9.2.1. Dateien zum Schutz hinzufügen

Der Dateischutz ist ein besonderer Ort, der dazu verwendet wird wichtige Daten sicher zu speichern. Die Dokumente des Dateischutzes werden verschlüsselt.

Durch klicken auf **Dateien zum Schutz hinzufügen** wird ein Assistent gestartet, der Ihnen bei der Erstellung eines Schutzes und dem Hinzufügen von Dateien hilft.

Schritt 1/6 - Ziel wählen

Hier können Sie auswählen welche Dateien und Ordner zum Schutz hinzugefügt werden sollen.

Ziel

Klicken Sie auf **Ziel hinzufügen**, wählen Sie dann die Dateien und Ordner die hinzugefügt werden sollen und wählen Sie **OK**. Der Pfad der ausgewählten Position wird in der Spalte **Pfad** angezeigt. Wenn Sie die ausgewählte Position ändern möchten, klicken Sie einfach auf die nebenstehende Schaltfläche **Entfernen**.

Anmerkung
Sie können eine oder auch mehrere Ziele auswählen.

Klicken Sie auf **Weiter**.

Schritt 2/6 - Schutz auswählen

Hier können Sie einen neuen Schutz erstellen oder einen existierenden auswählen.

Schutz auswählen

Wenn Sie **Nach Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 5 weitergeleitet, wenn der ausgewählte Schutz geöffnet ist (mounted) oder zu Schritt 4 wir wenn er verschlossen ist (unmounted).

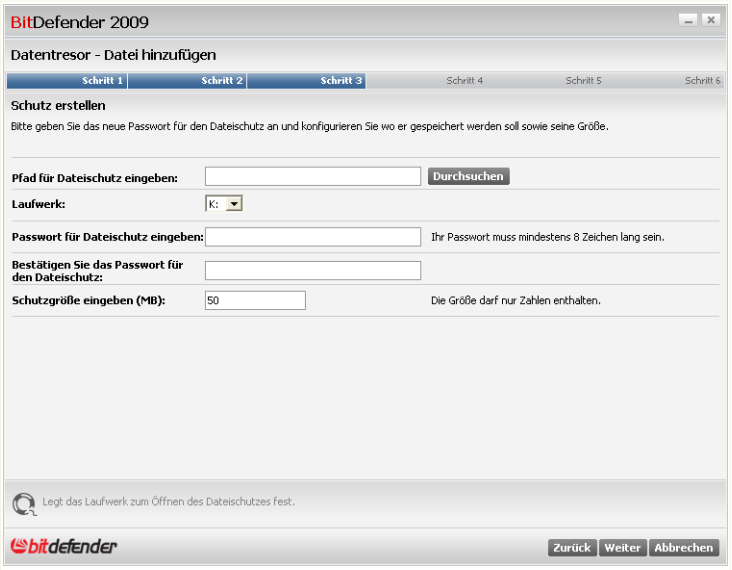
Wenn Sie **Einen bestehenden Dateischutz wählen** auswählen, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 5 weitergeleitet, wenn der ausgewählte Schutz geöffnet ist (mounted) oder zu Schritt 4 wir wenn er verschlossen ist (unmounted).

Wählen Sie **Neuen Dateischutz erstellen** wenn kein bestehender Schutz Ihren Bedürfnissen entspricht. Sie werden zu Schritt 3 weitergeleitet.

Klicken Sie auf **Weiter**.

Schritt 3/6 – Dateischutz erstellen

Hier können Sie genaue Informationen für den neuen Dateischutz angeben.



Schutz erstellen

Um die Informationen bezüglich des Dateischutzes anzugeben, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Durchsuchen** und wählen Sie einen Ort für die `bvd` Datei.

> ***Anmerkung***
> Bedenken Sie dass der Dateischutz eine verschlüsselte Datei auf Ihrem Computer mit der Endung `bvd` ist.

2. Wählen Sie einen Laufwerkbuchstaben für den neuen Dateischutz aus dem entsprechenden Menü.

> ***Anmerkung***
> Bedenken Sie, dass beim Mounten der `bvd` Datei eine neue logische Partition (ein neues Laufwerk) erscheinen wird.

3. Geben Sie ein Passwort für den Dateischutz in das dafür vorgesehene Feld ein.

   Anmerkung
   Ihr Passwort muss mindestens 8 Zeichen lang sein.

4. Geben Sie das Passwort erneut ein.
5. Legen Sie die Größe des Dateischutzes fest (in MB), indem Sie den entsprechenden Wert in das dazugehörige Eingabefeld eintragen.

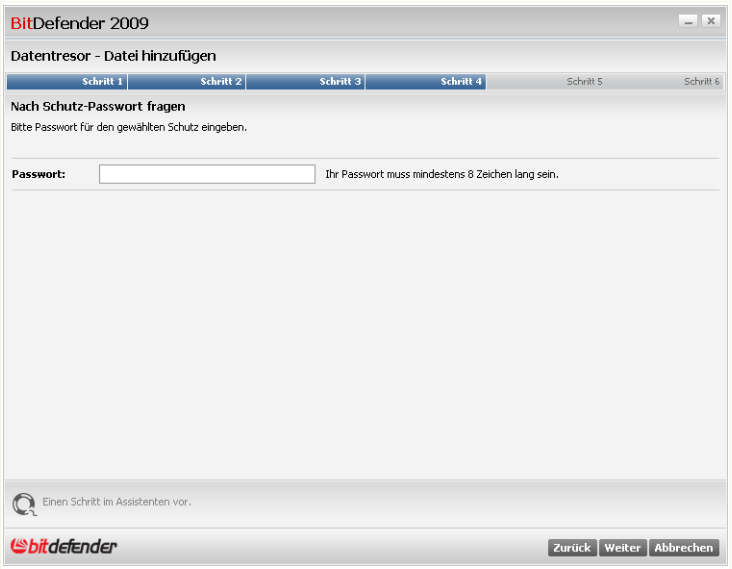
   Anmerkung
   Die Größe darf nur aus Zahlen bestehen.

Klicken Sie auf **Weiter**.

Sie werden zu Schritt 5 weitergeleitet.

Schritt 4/6 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.

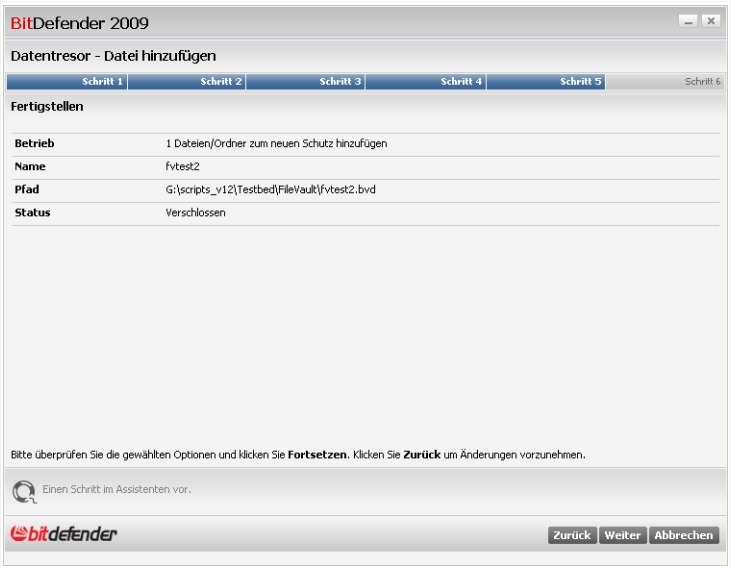


Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 5/6 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.



Übersicht

Klicken Sie auf **Weiter**.

Schritt 6/6 - Ergebnisse

Hier können Sie den Inhalt des Schutzes betrachten.

Ergebnisse

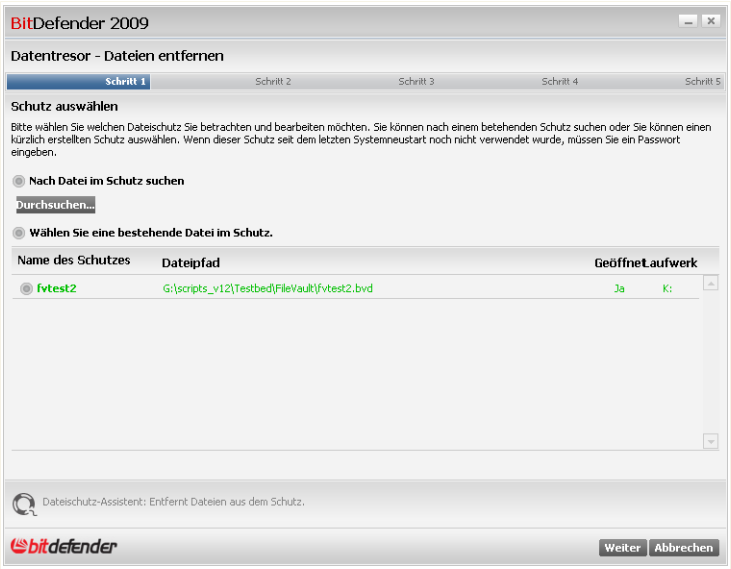
Klicken Sie auf **Fertigstellen**.

9.2.2. Dateien aus Schutz entfernen

Durch klicken auf **Dateien aus Schutz entfernen** wird ein Assistent gestartet welcher Ihnen bei dem Entfernen von Dateien aus einem bestimmten Schutz behilflich ist.

Schritt 1/5 - Schutz wählen

Hier können Sie den Schutz auswählen, aus dem die Dateien entfernt werden sollen.



Schutz auswählen

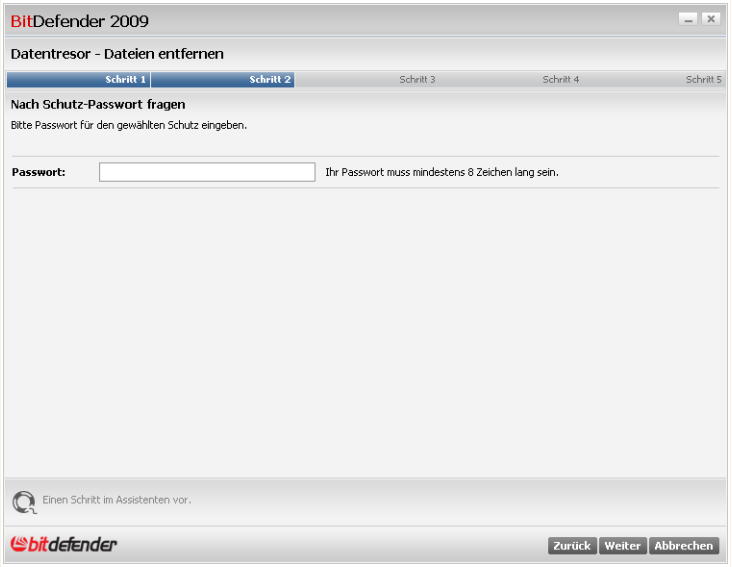
Wenn Sie **Nach einem Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Wenn Sie auf **Einen bestehenden Dateischutz auswählen** klicken, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Klicken Sie auf **Weiter**.

Schritt 2/5 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.



Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 3/5 – Dateien auswählen

Hier erhalten Sie die Liste der Dateien des zuvor ausgewählten Schutzes.

Dateien auswählen

Wählen Sie die Dateien die entfernt werden sollen und klicken Sie auf **Weiter**.

Schritt 4/5 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.

Übersicht

Klicken Sie auf **Weiter**.

Schritt 5/5 - Ergebnisse

Hier können Sie das Ergebnis der Operation sehen.

Ergebnisse

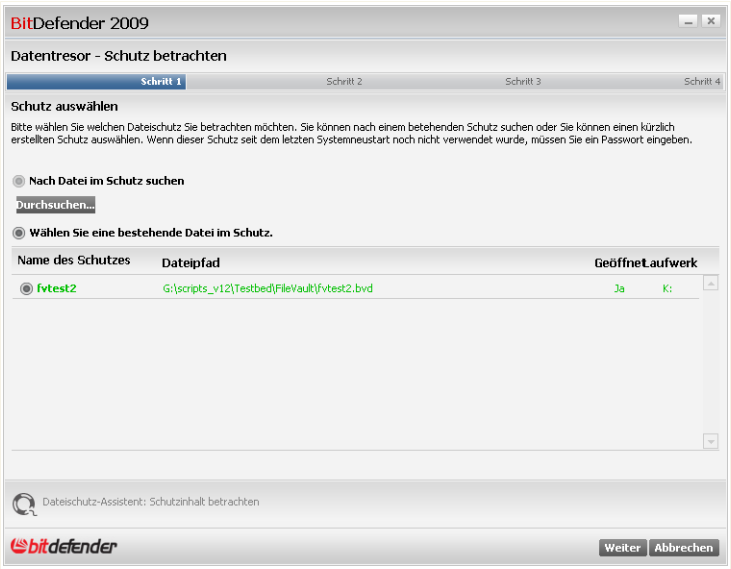
Klicken Sie auf **Fertigstellen**.

9.2.3. Dateien im Schutz betrachten

Durch klicken auf **Schutz ansehen** wird ein Assistent gestartet welcher Ihnen bei der Betrachtung der Daten eines speziellen Schutzes behilfich ist.

Schritt 1/4 - Schutz wählen

Hier können Sie auswählen von welchem Dateischutz die Dateien betrachtet werden sollen.



Schutz auswählen

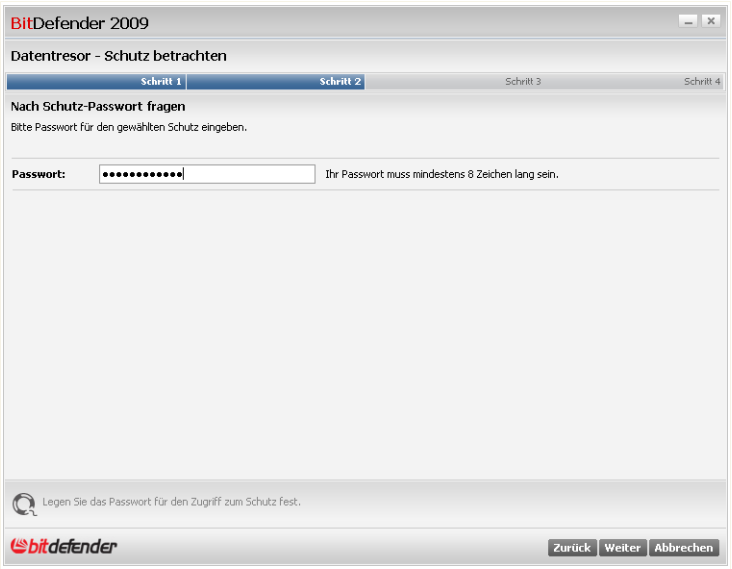
Wenn Sie **Nach einem Dateischutz suchen** auswählen, müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Wenn Sie auf **Einen bestehenden Dateischutz auswählen** klicken, müssen Sie auf den gewünschten Schutznamen klicken. Sie werden entweder zu Schritt 3 weitergeleitet wenn der Schutz geöffnet ist (mounted) oder zu Schritt 2 wenn er geschlossen ist (unmounted).

Klicken Sie auf **Weiter**.

Schritt 2/4 - Passwort

Hier werden Sie nach der Eingabe des Passwortes für den ausgewählten Dateischutz gefragt.



Passwort eingeben

Geben Sie das Passwort in das entsprechende Feld ein und klicken Sie auf **Weiter**.

Schritt 3/4 - Zusammenfassung

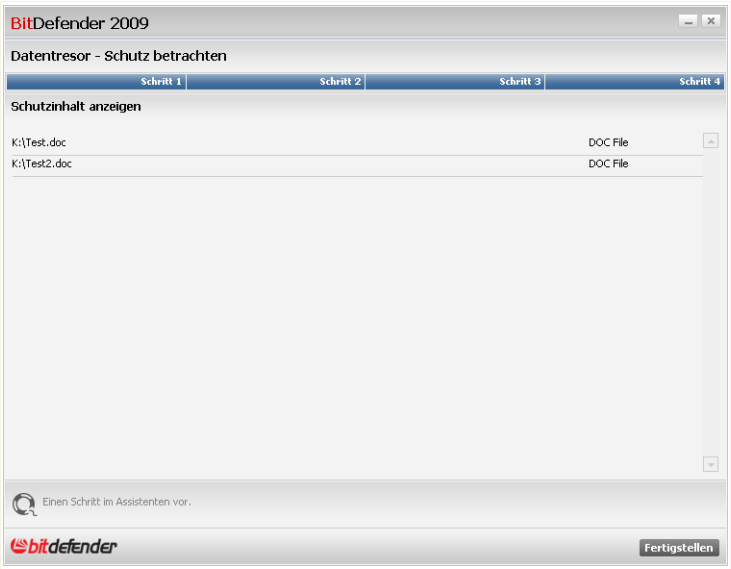
Hier können Sie die gewählten Prozesse noch einmal betrachten.

Übersicht

Klicken Sie auf **Weiter**.

Schritt 4/4 - Ergebnisse

Hier können Sie die Dateien des Schutzes sehen.



Ergebnisse

Klicken Sie auf **Fertigstellen**.

9.2.4. Schutz abschließen

Wie Sie bereits wissen ist ein Dateischutz eine verschlüsselte Datei auf Ihrem Computer mit der Endung `bvd`. Der Dateischutz kann geöffnet (mounted) oder abgeschlossen (unmounted) werden.

Um diesen Prozess besser zu verstehen, denken Sie an einen Banksafe - seine stabile Tür kann geschlossen oder geöffnet werden. Der Inhalt des Safes ist aber nur sicher, wenn der abgeschlossen ist. Gleichzeitig kann nur auf seinen Inhalt zugegriffen werden, wenn er geöffnet ist.

Durch klicken auf **Schutz abschließen** wird ein Assistent gestartet welcher Ihnen bei dem Abschließen (unmounten) eines bestimmten Schutzes behilfich ist.

Schritt 1/3 - Schutz wählen

Hier können Sie den Schutz auswählen der abgeschlossen werden soll.

Schutz auswählen

Wenn Sie **Nach einem Dateischutz suchen** auswählen müssen Sie auf **Durchsuchen** klicken und den Dateischutz auswählen.

Wenn Sie auf**Einen bestehenden Dateischutz wählen** klicken, dann müssen Sie den gewünschten Schutznamen anklicken.

Klicken Sie auf **Weiter**.

Schritt 2/3 - Zusammenfassung

Hier können Sie die gewählten Prozesse noch einmal betrachten.

Übersicht

Klicken Sie auf **Weiter**.

Schritt 3/3 - Ergebnisse

Hier können Sie das Ergebnis der Operation sehen.

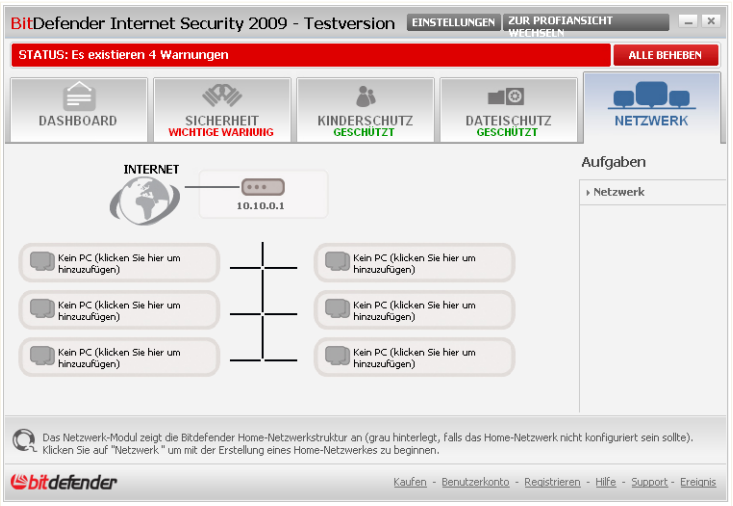
Ergebnisse

Klicken Sie auf **Fertigstellen**.

10. Netzwerk

Mit dem Netzwerk-Modul können Sie die BitDefender Produkte die auf den Computern in Ihrem Haushalt installiert sind von einem Computer aus verwalten.

Um das Netzwerk-Modul zu starten, klicken Sie auf den Tab **Datei Manager**.



Netzwerk

Um die BitDefender Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

1. Fügen Sie Ihren Computer dem BitDefender Home-Netzwerk hinzu. Das Hinzufügen zu einem Netzwerk besteht aus dem Konfigurieren eines administrativen Passworts für die Verwaltung des Home-Netzwerks.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).
3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

10.1. Aufgaben

Anfangs steht nur eine Schaltfläche zur Verfügung.

- **Netzwerk beitreten/erstellen** - bietet Ihnen die Möglichkeit ein Netzwerkpasswort einzustellen, um dem Netzwerk beizutreten.

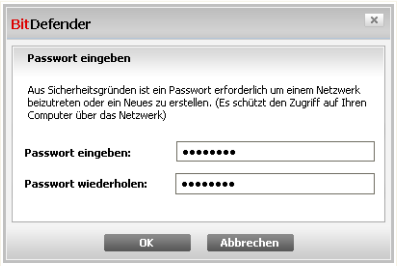
Nach dem Beitreten zum Netzwerk werden mehrere Schaltflächen erscheinen.

- **Netzwerk verlassen** - bietet Ihnen die Möglichkeit das Netzwerk zu verlassen.
- **Netzwerk verwalten** -bietet Ihnen die Möglichkeit Computer zum Netzwerk hinzuzufügen.
- **Alle prüfen** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu prüfen.
- **Alle aktualisieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu aktualisieren.
- **Alle registrieren** - bietet Ihnen die Möglichkeit alle verwalteten Computer gleichzeitig zu registrieren.

10.1.1. Dem BitDefender-Netzwerk beitreten

Um dem BitDefender Home-Netzwerk beizutreten, befolgen Sie diese Schritte:

1. Klicken Sie auf **Netzwerk beitreten/erstellen**. Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.



Passwort konfigurieren

2. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
3. Klicken Sie auf **OK**.

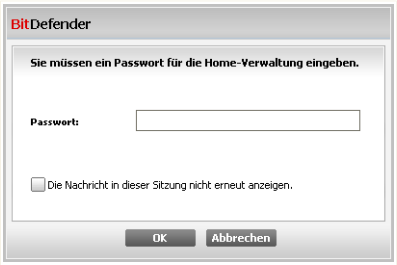
Sie sehen den Namen des Computers in der Netzwerkübersicht.

10.1.2. Computer zum BitDefender-Netzwerk hinzufügen

Um einen Computer zum BitDefender Home-Netzwerk hinzuzufügen, müssen Sie zuerst das Passwort der BitDefender Home-Verwaltung auf dem entsprechenden Computer konfigurieren.

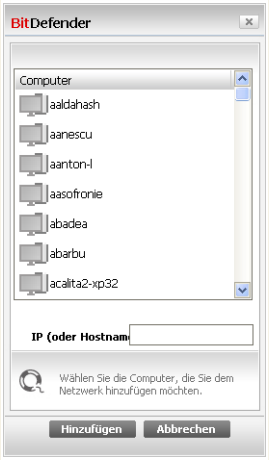
Um einen Computer zum BitDefender Home-Netzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Netzwerk verwalten**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**. Ein neues Fenster wird sich öffnen.

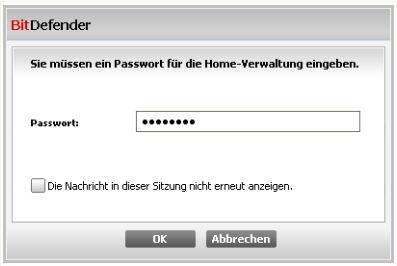


Computer hinzufügen

Sie können eine Liste der Computer im Netzwerk sehen. Die Bedeutung des Symbols ist wie folgt:

- Zeigt einen Online-Computer an, auf dem keine BitDefender-Produkte installiert sind.
- Zeigt einen Online-Computer an, auf dem BitDefender installiert ist.
- Zeigt einen Offline-Computer an, auf dem BitDefender installiert ist.

3. Sie können hierzu eine der folgenden Methoden wählen:
   - Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.
4. Klicken Sie auf **Hinzufügen**. Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.



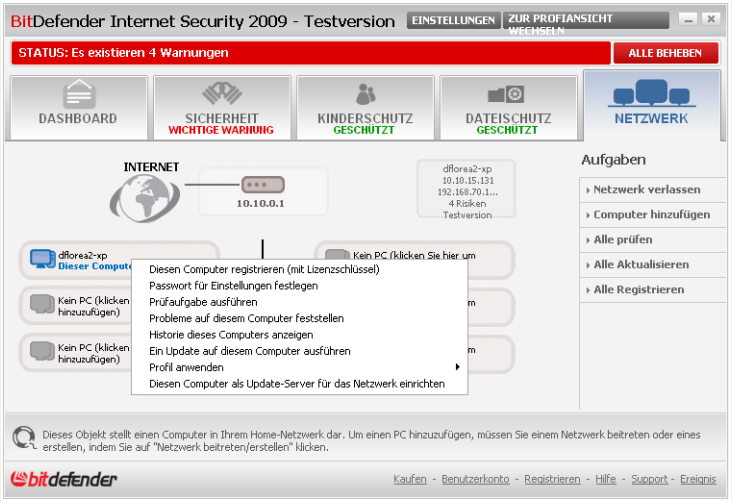
Authentifizieren

5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.
6. Klicken Sie auf **OK**. Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

Anmerkung
Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

10.1.3. Das BitDefender-Netzwerk verwalten

Wenn Sie das BitDefender Home-Netzwerk erstellt haben, können Sie alle BitDefender Produkte von einem Computer aus verwalten.



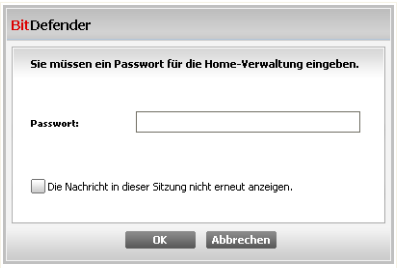
Netzwerkübersicht

Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Probleme die die Systemsicherheit betreffen, Registrierungsstatus von BitDefender).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **Diesen Computer registrieren**
- **Passwort für Einstellungen einstellen**
- **Prüf-Aufgabe ausführen**
- **Risiken auf diesem Computer feststellen**
- **Historie dieses Computers anzeigen**
- **Jetzt ein Update auf diesem Computer durchführen**
- **Profil anwenden**
- **Tuning-Aufgabe auf diesem Computer durchführen**
- **Diesen Computer als Update-Server für dieses Netzwerk festlegen**

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert das Passwort der lokalen Home-Verwaltung anzugeben.



Passwort eingeben

Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.

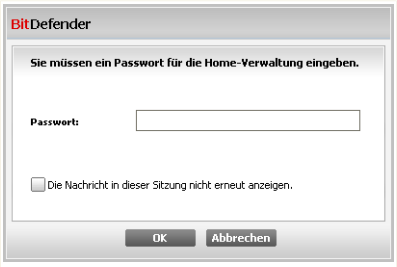
Anmerkung

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**. Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

10.1.4. Alle Computer prüfen

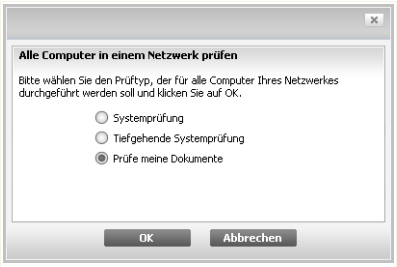
Um alle verwalteten Computer zu prüfen, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Alle prüfen**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Wählen Sie eine Prüfart.
   - **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
   - **Tiefgehende Systemprüfung** - Prüft den gesamten Computer (inklusive Archiven).
   - **Eigene Dateien prüfen** - Führt eine schnelle Prüfung Ihrer Eigenen Dateien durch.



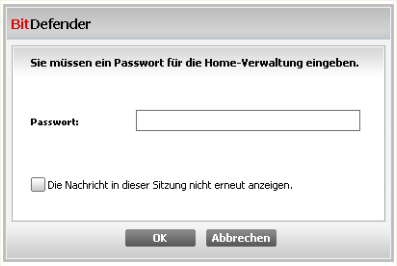
Prüfart wählen

3. Klicken Sie auf **OK**.

10.1.5. Alle Computer aktualisieren

Um alle verwalteten Computer zu aktualisieren, befolgen Sie folgende Schritte:

1. Klicken Sie auf**Alle aktualisieren** . Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



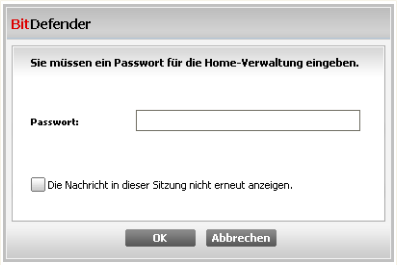
Passwort eingeben

2. Klicken Sie auf **OK**.

10.1.6. Alle Computer registrieren

Um alle verwalteten Computer zu registrieren, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Alle registrieren**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Geben Sie den Lizenzschlüssel zur Registrierung ein.

Alle Registrieren

3. Klicken Sie auf **OK**.

11. Basiseinstellungen

Unter den Basiseinstellungen können Sie einfach wichtige Sicherheitsmodule aktivieren/deaktivieren.

Um zu den Basiseinstellungen zu gelangen klicken Sie auf **Einstellungen** im oberen Bereich der Basisansicht.

Basiseinstellungen

Die verfügbaren Sicherheitsmodule wurden in mehrere Kategorien unterteilt.

Kategorie	*Beschreibung*
Lokale Sicherheit	Hier können Sie den Echtzeit-Schutz und das automatische Update (de)aktivieren.
Online-Sicherheit	Hier können Sie den Echtzeit-Mail- und Webschutz aktivieren/deaktivieren.
Kindersicherung Einstellungen	Hier können Sie die Kindersicherung aktivieren/deaktivieren.
Netzwerksicherheit	Hier können Sie die Firewall aktivieren/deaktivieren.

Kategorie	Beschreibung
Allgemeine Einstellungen	Hier können Sie den Spiele-Modus, Laptop-Modus, Paswörter, die Prüfaktivitätsleiste und mehr (de)aktivieren.

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

11.1. Lokale Sicherheit

Sie können die Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.

Sicherheitsmodul	Beschreibung
Echtzeit-Antivirus & Antispyware Dateischutz	Der Echtzeit-Dateischutz gewährleistet, dass alle Dateien geprüft werden, sobald auf sie zugegriffen wird, sei es durch Sie oder eine ausgeführte Anwendung
Automatisches Update	Das automatische Update gewährleistet, dass das aktuellste BitDefender Produkt und die Signaturdateien automatisch und regelmäßig heruntergeladen und installiert werden
Automatische Prüfung auf Schwachstellen	Die automatische Prüfung auf Schwachstellen gewährleistet, dass wichtige Software auf Ihrem PC stets auf dem neusten Stand ist.

11.2. Online Sicherheit

Sie können die Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.

Sicherheitsmodul	Beschreibung
Echtzeit Antivirus-, Antispam- & Antiphishing-Mail-Schutz	Der Echtzeit Mail-Schutz gewährleistet, dass Ihre E-Mails nach Spams gefiltert und auf Phishing-Versuche geprüft werden.
Echtzeit Antivirus- & Antipyware-Web-Schutz	Der Echtzeit Web-Schutz gewährleistet, dass alle über HTTP heruntergeladenen Dateien auf Viren und Spyware geprüft werden.

Sicherheitsmodul	Beschreibung
Echtzeit Antiphishing-Web-Schutz	Der Echtzeit Antiphishing-Web-Schutz gewährleistet, dass alle Dateien die über HTTP heruntergeladen werden auf Phishing-Versuche überprüft werden.
Identitätskontrolle	Die Identitätskontrolle hilft Ihnen dabei, vertrauliche Daten zu sichern, indem der gesamte Datenverkehr im Web und bei E-Mails nach bestimmten Zeichenfolgen geprüft wird.
IM-Verschlüsselung	Wenn Ihre IM-Kontakte BitDefender 2009 installiert haben, werden alle Gespräche über Yahoo! Messenger und Windows Live Messenger verschlüsselt.

11.3. Kindersicherung Einstellungen

Sie können die Kindersicherung mit einem Klick aktivieren/deaktivieren.

Die Kindersicherung kann den Zugang zu unangemessenen Webseiten oder zum Internet für einen bestimmten Zeitraum blockieren und Mail-, IM- und Web-Datenverkehr nach bestimmten Wörtern filtern.

11.4. Netzwerk Einstellungen

Sie können die Firewall mit einem Klick aktivieren/deaktivieren.

Die Firewall schützt Ihren Computer vor Hackern und schädlichen Angriffen.

11.5. Einstellungen Datentresor

Sie können den Dateischutz mit einem Klick aktivieren/deaktivieren.

Der Datentresor schützt Ihre Dokumente indem diese verschlüsselt werden.

11.6. Allgemeine Einstellungen

Sie können alle Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.

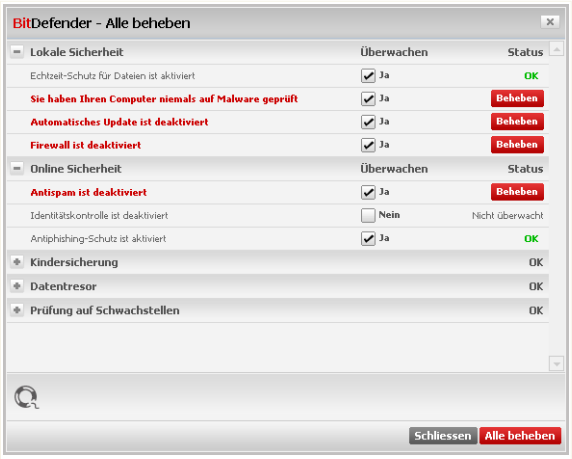
Objekt	Beschreibung
Spiele-Modus	Der Spiele-Modus verändert temporär die Einstellungen, so dass die Systemleistung während des Spielens so wenig wie möglich beeinträchtigt wird.
Laptop-Modus	Der Laptop-Modus verändert temporär die Einstellungen, so dass die Betriebsdauer des Laptopakkus so wenig wie möglich beeinträchtigt wird.
Passwort für Einstellungen	Dies gewährleistet, dass die Einstellungen von BitDefender nur von der Person verändert werden können, die das Passwort kennt.
Passwort für Kindersicherung	Indem Sie diese Option aktivieren, werden Sie die Einstellungen der Kindersicherung schützen. Dies gewährleistet, dass die Einstellungen der Kindersicherung nur von der Person geändert werden können, die das Passwort kennt.
BitDefender Neuigkeiten	Wenn Sie diese Option aktivieren, erhalten Sie von Bitdefender wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.
Produktbenachrichtigungen	Wenn Sie diese Option aktivieren, erhalten Sie Informationsbenachrichtigungen.
Aktivitätsleiste	Die Aktivitätsleiste ist eine kleine durchsichtige Leiste, die den Fortschritt der Prüfaktivität von BitDefender anzeigt. Die grüne fortlaufende Linie zeigt die Prüfaktivität von Bitdefender auf Ihrem lokalen System an. Die rote fortlaufende Linie zeigt die Prüfaktivität für Ihre Internetverbindung an.
BitDefender beim Start von Windows laden	Wenn Sie diese Option aktivieren, wird die Benutzeroberfläche von BitDefender beim Hochfahren des Computers geladen. Diese Option hat keinen Einfluss auf die Schutzstufe.
Virenbericht senden	Wenn Sie diese Option aktivieren, werden Virenberichte zum BitDefender Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.
Ausbruchentdeckung	Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch zum BitDefender Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre

Objekt	Beschreibung
	IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

12. Statusleiste

Wie Sie leicht erkennen können, befindet sich im oberen Bereich des Fensters von BitDefender Internet Security 2009 eine Statusleiste, die die Anzahl der ausstehenden Probleme anzeigt. Klicken Sie auf die Schaltfläche **Alle Probleme feststellen** um Bedrohungen für die Sicherheit Ihres Computers einfach zu entfernen. Ein Fenster für den Sicherheitsstatus wird erscheinen.

Der Sicherheitsstatus zeigt Ihnen eine, einfach zu konfigurierende, Liste von Sicherheitsrisiken auf Ihrem Computer. BitDefender Internet Security 2009 informiert Sie sobald ein Sicherheitsrisiko auftritt.



Statusleiste

12.1. Lokale Sicherheit

Wir wissen dass es wichtig ist benachrichtigt zu werden, wann immer ein Problem die Sicherheit Ihres Computers beeinträchtigt. Durch das Anzeigen jedes Sicherheitsmoduls, informiert Sie BitDefender Internet Security 2009 nicht nur darüber wenn Sie Einstellungen verändern, die Einfluss auf die Sicherheit Ihres Computers haben könnten, sondern auch wenn Sie vergessen haben wichtige Aufgaben durchzuführen.

Diese Probleme bezüglich der lokalen Sicherheit, werden in expliziten Sätzen beschrieben. Wenn die Sicherheit Ihres Computers, in Übereinstimmung mit jedem Satz, irgendwie beeinträchtigt sein sollte, so werden Sie eine rote Statusfläche mit der Bezeichnung **Feststellen** sehen. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	*Beschreibung*
Echtzeit Dateischutz ist aktiviert	Alle Dateien werden bei Zugriff, durch Sie oder durch ein Programm auf dem System, geprüft.
Sie haben Ihren Computer heute auf Malware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.
Automatisches Update ist aktiviert	Bitte lassen Sie die automatischen Updates aktiviert, um sicherzustellen, dass die Malware-Signaturen Ihres BitDefender Produktes ständig aktualisiert werden.
Jetzt aktualisieren	Das Update des Produktes und für Malware-Signaturen wird durchgeführt.
Firewall ist aktiviert	Schützt Ihren Computer vor Hackern und schädlichen Angriffen von außen.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

12.2. Online Sicherheit

Die Angelegenheiten bezüglich der Online-Sicherheit werden in expliziten Sätzen beschrieben. In Übereinstimmung mit jedem Satz wird eine rote Statusfläche mit der

Bezeichnung **Feststellen** angezeigt, wenn die Sicherheit Ihres Computers möglicherweise gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	*Beschreibung*
Antispam ist aktiviert	Gewährleistet, dass Ihre E-Mails auf Malware geprüft und nach Spams gefiltert werden.
Identitätskontrolle ist aktiviert	Hilft Ihnen vertrauliche Daten zu sichern, indem der Web- und Mail-Datenverkehr nach bestimmten Zeichenfolgen geprüft wird. Es wird empfohlen die Identitätskontrolle zu aktivieren, um Ihre vertraulichen Daten (E-Mail-Adressen, Benutzer IDs, Passwörter, Kreditkartennummern, usw) vor Diebstahl zu schützen.
Firefox Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.
Internet Explorer Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

12.3. Datentresor

Die Probleme die den Privatbereich Ihrer Daten betreffen sind in expliziten Sätzen beschrieben. Übereinstimmend mit jedem Satz werden Sie eine rote Statusfläche mit der Bezeichnung **Feststellen** sehen, wenn der Privatbereich Ihrer Daten gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Dateischutz ist aktiviert	Der Datentresor schützt Ihre Dokumente indem diese verschlüsselt werden.

Wenn die Statusflächen grün sind, ist das Sicherheitsrisiko Ihrer Daten gering. Damit diese Flächen grün werden, befolgen Sie diese Schritte:

1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

12.4. Schwachstellen-Scan

Die Angelegenheiten bezüglich der Anfälligkeit werden in expliziten Sätzen beschrieben. In Übereinstimmung mit jedem Satz wird eine rote Statusfläche mit der Bezeichnung **Feststellen** angezeigt, wenn die Sicherheit Ihres Computers möglicherweise gefährdet ist. Andernfalls wird eine grüne Statusfläche **OK** angezeigt.

Risiko	Beschreibung
Anfälligkeitsprüfung ist aktiviert	Überwacht die Updates von Microsoft Windows und von Microsoft Windows Office sowie die Passwörter der Microsoft Windows Benutzerkonten, um sicherzustellen, dass Ihr Betriebssystem auf dem neusten Stand und nicht anfällig für Passwortumgehungen ist.
Wichtige Microsoft Updates	Installieren Sie wichtige Microsoft Updates.
Andere Microsoft Updates	Installieren Sie weniger wichtige Microsoft Updates.
Automatische Updates für Windows sind aktiviert	Installieren Sie neue Windows Sicherheits-Updates, sobald diese verfügbar sind.

Risiko	Beschreibung
Admin (Sicheres Passwort)	Zeigt die Passwortsicherheit für bestimmte Benutzer an.

Wenn die Statusfläche grün ist, so ist das Sicherheitsrisiko für Ihr System gering. Um zu erreichen, dass diese Fläche grün wird, befolgen Sie diese Schritte:

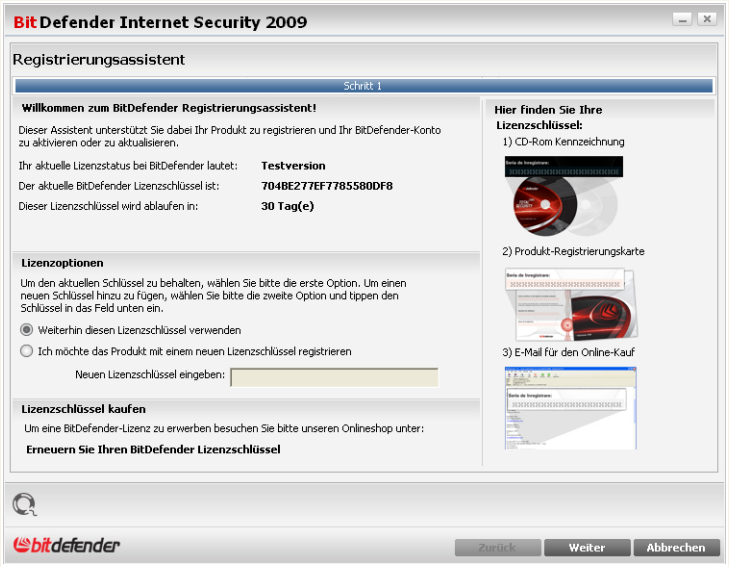
1. Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.
2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

Wenn Sie möchten, dass bestimmte Komponenten von der Überwachung ausgeschlossen werden, lassen Sie das Kontrollkästchen **Ja, diese Komponente überwachen** frei.

13. Registrierung

BitDefender Internet Security 2009 verfügt über eine 30-tägige Testversion Wenn Sie BitDefender Internet Security 2009 registrieren, den Lizenzschlüssel ändern oder ein BitDefender-Benutzerkonto erstellen möchten, klicken Sie auf den Link **Registrieren** der sich im unteren Bereich des Fensters von BitDefender befindet. Der Registrierungs-Assistent wird erscheinen.

13.1. Schritt 1/1 - BitDefender Internet Security 2009 registrieren



Registrierung

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

Um BitDefender Internet Security 2009 zu registrieren:

1. Klicken Sie auf die Schaltfläche **Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren**.
2. Geben Sie den Lizenzschlüssel in das Editierfeld ein.

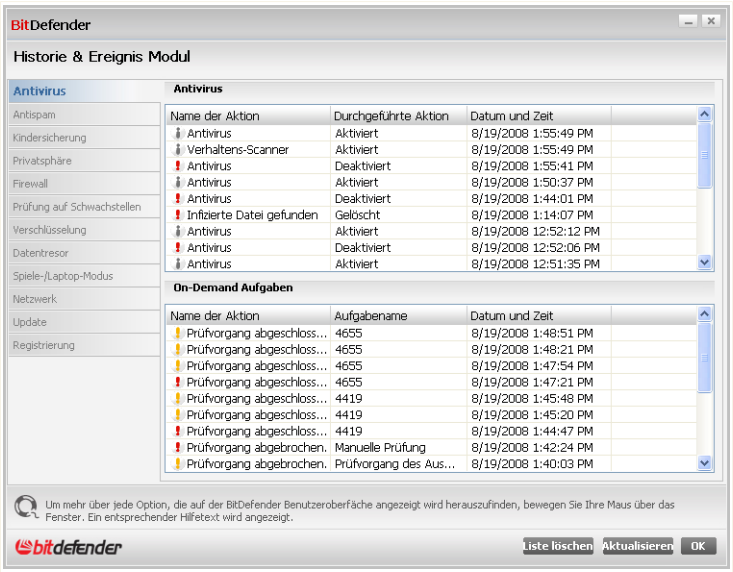
Anmerkung
Sie finden den Lizenzschlüssel:
- Auf dem CD-Aufdruck.
- Auf der Registrierungskarte des Produktes.
- In der E-Mail-Bestätigung des Online-Kaufs.

Wenn Sie keinen Bitdefender-Lizenzschlüssel besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Klicken Sie auf **Fertigstellen**.

14. Ereignis

Der Link **History** im unteren Bereich des Fensters des BitDefender Security Center öffnet ein anderes Fenster mit der BitDefender Historie & Ereignisse. Dieses Fenster bietet Ihnen einen Überblick über die Ereignisse bezüglich der Sicherheit. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.



Ereignisanzeige

Um eine gute Übersicht zu gewähren wurden die BitDefender Ereignise auf der linken Seite in verschiedene Gruppen aufgeteilt:

- **Antivirus**
- **Firewall**
- **Antispam**
- **Privatsphäre**
- **Kindersicherung**
- **Update**

- **Netzwerk**
- **Dateischutz**

Für jede Kategorie ist eine Liste von Ereignisen verfügbar. Jedes Ereignis enthält folgende Informationen: Eine Kurzbeschreibung, die von BitDefender durchgeführte Aktion, sowie Datum und Zeitpunkt des Auftretens. Wenn Sie nähere Informationen zu einem Ereignis erhalten möchten dann klicken Sie doppelt auf selbiges.

Klicken Sie auf **Zurücksetzen** wenn Sie die Einträge entfernen möchten oder auf **Aktualisieren** um sicherzustellen das die Anzeige aktuell ist.

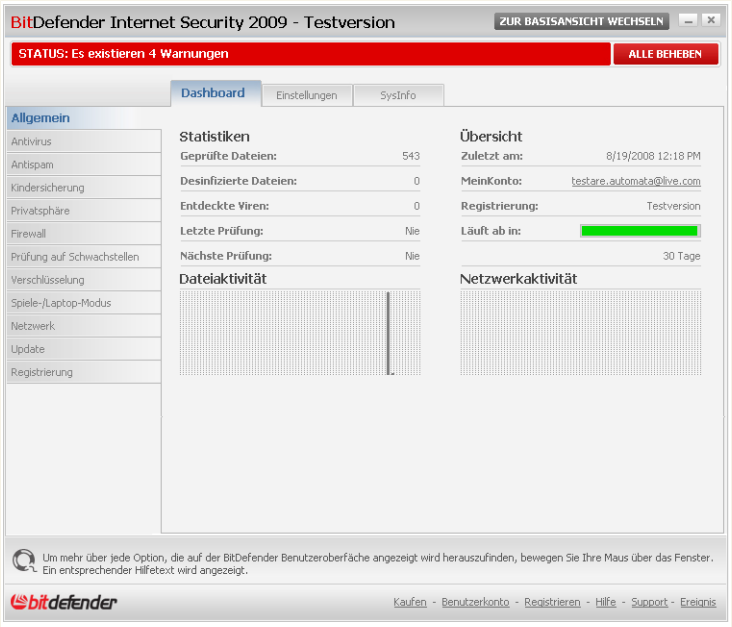
Erweiterte Administration

15. Allgemein

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

15.1. Dashboard

Um die Statistiken der Produktaktivität und Ihren Registrierungsstatus zu sehen, öffnen Sie das **Allgemeine>Dashboard** in der erweiterten Ansicht.



Dashboard

Das Dashboard besteht aus mehreren Bereichen:

- **Statistiken** - Zeigt wichtige Informationen bezüglich der Aktivität von BitDefender an.

- **Überblick** - Zeigt Ihnen den Update-Status sowie Registrierungs- und Lizenzinformationen an.
- **Dateibereich** - Zeigt die Entwicklung der Anzahl der Objekte an, die von BitDefender Antimalware geprüft wurden. Die Höhe der Leiste zeigt die Intensität des Datenverkehrs für diesen Zeitraum an.
- **Netzwerkbereich** - Zeigt die Entwicklung des Netzwerk-Datenverkehrs an, der von der BitDefender Firewall gefiltert wurde. Die Höhe der Leiste zeigt die Intensität des Datenverkehrs für diesen Zeitraum an.

15.1.1. Statistik

Wenn Sie die Aktivität von BitDefender überwachen möchten, können Sie das im Statistikbereich tun. Sie können folgende Objekte sehen:

Objekt	Beschreibung
Überprüfte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung auf Malware überprüft wurden.
Desinfizierte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung desinfiziert wurden.
Entdeckte Viren	Zeigt die Anzahl der Viren an, die während der letzten Prüfung auf Ihrem System gefunden wurden.
Blockierte Portprüfungen	Zeigt die Anzahl der Portprüfungen an, die von der BitDefender Firewall blockiert wurden. Portprüfungen werden häufig von Hackern verwendet, um offene Ports auf Ihrem Computer zu finden, um diese dann zu verwenden. Lassen Sie die Firewall und den Stealth-Modus aktiviert um gegen Portprüfungen geschützt zu sein.

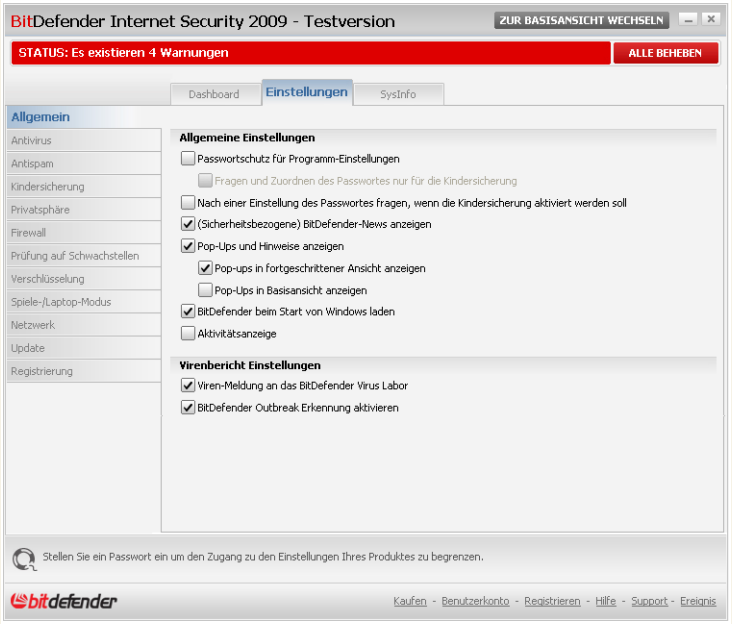
15.1.2. Übersicht

Hier können Sie eine Zusammenfassung der Statistiken bezüglich des Update-Status, des Status Ihres Benutzerkontos sowie Registrierungs- und Lizenzinformationen sehen.

Objekt	Beschreibung
Letztes Update	Zeigt das Datum an, zu dem Ihr BitDefender Produkt zuletzt aktualisiert wurde. Bitte führen Sie regelmäßig Updates durch, damit Ihr System vollständig geschützt ist.
Mein Benutzerkonto	Zeigt die E-Mail-Adresse an, die Sie benutzen können, um auf Ihr Online-Benutzerkonto zugreifen zu können, um Ihren Lizenzschlüssel zu erhalten und vom BitDefender Support und anderen Services profitieren zu können.
Registrierung	Zeigt Ihren Lizenzschlüssel und dessen Status an. Damit Ihr System sicher ist, müssen Sie BitDefender erneuern oder aktualisieren, wenn der Lizenzschlüssel abgelaufen ist.
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels.

15.2. Einstellungen

Um allgemeine Einstellungen für Bitdefender vorzunehmen und zu verwalten klicken Sie auf **Allgemeine>Einstellungen** in der erweiterten Ansicht.



Allgemeine Einstellungen

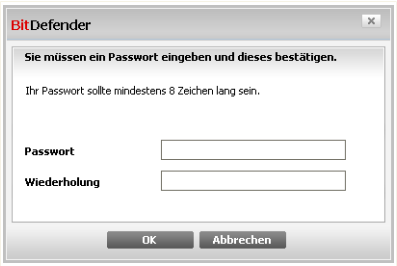
Hier können Sie die umfassenden Einstellungen von BitDefender einsehen. Standardmäßig wird BitDefender beim Windowsstart geladen und läuft dann im Hintergrund.

15.2.1. Allgemeine Einstellungen

- **Passwortschutz für Programm-Einstellung aktivieren** - 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:



Passwort eingeben

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

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

Wenn Sie nur während der Einstellung der Kindersicherung nach dem Passwort gefragt werden möchten, so aktivieren Sie auch **Passwort für Kindersicherung erfragen/anwenden**. Wenn ein Passwort nur für die Kindersicherung eingestellt wurde, und Sie diese Option nicht aktivieren, so wird das entsprechende Passwort bei der Einstellung jeder BitDefender-Option erfragt.

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

- **Bei Aktivierung der Kindersicherung fragen, ob ich das Passwort konfigurieren möchte** - wenn diese Option aktiviert ist und kein Passwort eingestellt wurde, werden Sie dazu aufgefordert ein Passwort einzustellen um die Kindersicherung zu aktivieren. Wenn Sie ein Passwort einstellen, können andere Benutzer mit administrativen Rechten die Einstellungen der Kindersicherung nicht verändern.
- **BitDefender-News anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Pop-Ups und Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren. Sie können BitDefender konfigurieren, damit die Pop-ups und Hinweise in der Basisansicht oder (bzw und) Profiansicht angezeigt werden.
- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart. Dies wird dringend empfohlen.
- **Aktivitsänzeige aktivieren (grafische Bildschirmanzeige der Produktaktivität)** - zeigt die Leiste der Scanaktivität an wenn Windows läuft. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass die Scanaktivitätsleiste angezeigt wird.

Anmerkung
Diese Option kann nur für das aktuelle Windows Benutzerkonto konfiguriert werden.

15.2.2. Virenbericht Einstellungen

- **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.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden für die Erstellung von Statistiken verwendet.

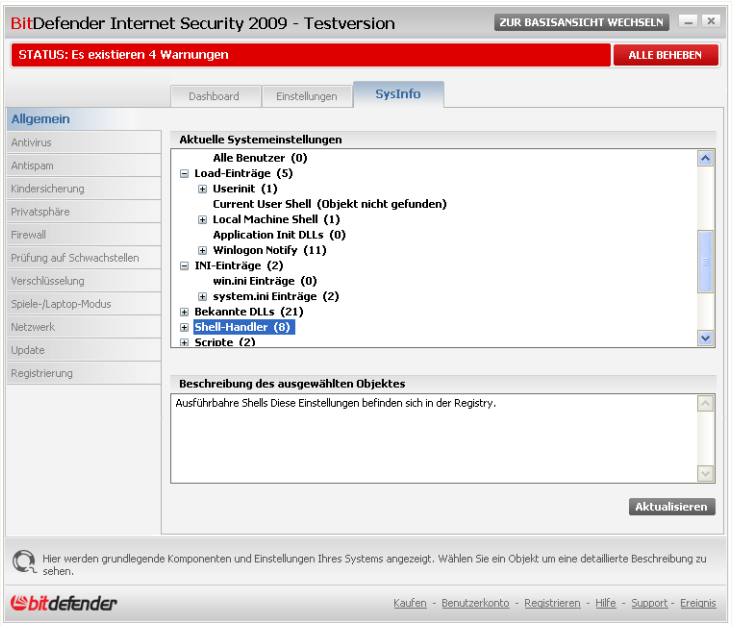
- **BitDefender Outbreak Erkennung aktivieren** - sendet Berichte über potentiele Virenausbrüche an das BitDefender Labor.

  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden nur für die Erkennung von neuen Viren verwendet.

15.3. System-Info

BitDefender erlaubt Ihnen in einer einzigen Übersicht alle Einstellungen und Programme welche beim Systemstart gestartet werden einzusehen.

Um diese Systeminformationen anzuzeigen klicken Sie auf **Allgemeine>Systeminformationen** in der erweiterten Ansicht.



System-Info

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:

- **Wiederherstellen** - stellt die ursprüngliche Dateiassoziation der aktuellen Datei wieder her. Nur für die Einstellungen **Dateiassoziationen** verfügbar!
- **Gehe zu** - öffnet ein Fenster mit der Pfadangabe für das Objekt (Zum Beispiel: **Eintragung**).

> ***Anmerkung***
> Je nach ausgewähltem Objekt wird die Schaltfläche **Gehe zu** nicht erscheinen.

- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.

16. Antivirus

BitDefender schützt Sie vor allen Arten von Schädlingen (Virus, Trojaner, Spyware, Rootkits und so weiter). Der Virenschutz ist in zwei Kategorien aufgeteilt:

- Echtzeitschutz - hält neue Malware-Bedrohungen davon ab, in Ihr System zu gelangen. BitDefender wird z.B. ein Worddokument auf Schädlinge prüfen wenn Sie es öffnen, und eine EMailnachricht wenn Sie diese empfangen.

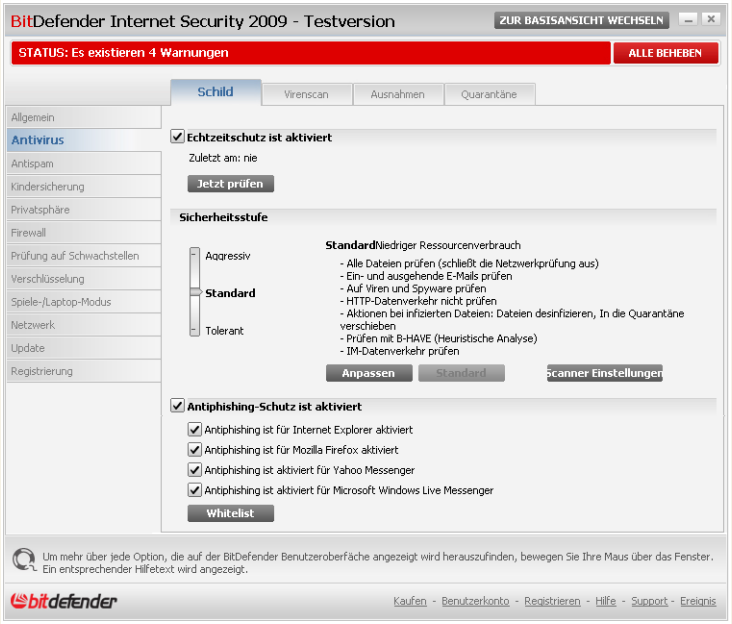
  Anmerkung
  Der Echtzeitschutz gilt auch für die Prüfung auf Zugriff (On-Access) - Dateien werden geprüft, sobald die Benutzer auf sie zugreifen.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um eine klassische , durch den Benutzer gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche BitDefender prüfen soll, und BitDefender prüft diese. Die Prüfaufgaben erlauben Ihnen die Prüfroutinen auf Ihre Bedürfnisse anzupassen und diese zu einem festgelegten Zeitpunkt zu starten.

16.1. Echtzeitschutz

BitDefender bietet einen dauerhaften Echtzeitschutz gegen verschiedene Malware, indem alle Dateien auf die zugegriffen wird sowie E-Mail-Nachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) geprüft werden. BitDefender Antiphishing gewährleistet einen sicheren Aufenthalt und den Schutz persönlicher Informationen im Internet. Der Benutzer wird über potentielle Phishing-Webseiten alarmiert.

Um den Echtzeitschutz und BitDefender Antiphishing zu konfigurieren klicken Sie auf **Antivirus>Schild** in der erweiterten Ansicht.



Echtzeitschutz

Sie können sehen ob der Echtzeitschutz aktiviert oder deaktiviert ist. Wenn Sie den Status des Echtzeitschutzes verändern möchten, markieren Sie das entsprechende Kontrollkästchen oder lassen Sie es frei.

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

Um eine schnelle Systemprüfung durchzuführen klicken Sie auf **Jetzt prüfen**.

16.1.1. Sicherheitsstufe einstellen

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

Es gibt 3 mögliche Einstellungen:

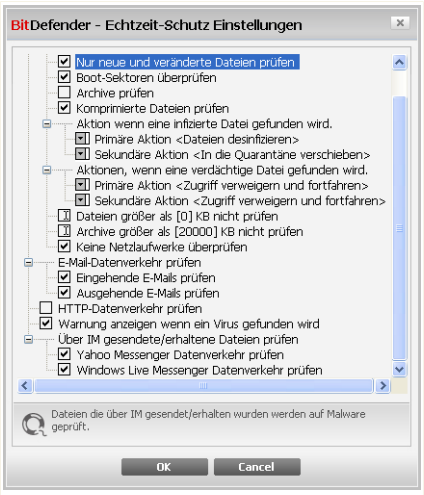
Sicherheitseinstellung	Beschreibung
Tolerant	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. Programme und eingehende Nachrichten werden nur auf Viren hin geprüft. Neben den klassischen Signatur basierten Scans werden außerdem Heuristische Scans eingesetzt. Bei infizierten Dateien können Sie wählen zwischen Datei bereinigen/Zugriff verweigern.
Standard	Gewährleistet Standard Sicherheit. Belastung 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.

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

16.1.2. Sicherheitsstufe anpassen

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.

Um die Echzeit-Sicherheitseinstellungen **anzupassen**, klicken Sie auf **Einstellung ändern**. Das folgende Fenster öffnet sich:



Einstellungen des Virus Schild

Die Prüfoptionen sind wie ein aufklappbares Windows-Explorermenü aufgebaut. Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Anmerkung
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.

Optionen		*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;`

Optionen		Beschreibung
		.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.
	Auf Spyware prüfen	Risikosoftware erkennen. Erkannte Dateien werden als infiziert behandelt. Software welche diese Dateien verwendet könnte Ihre Arbeit einstellen falls diese Option aktiviert ist. Wählen Sie **Dialer und Anwendungen vom Scan ausschließen**, wenn Sie diese Dateien vom Scan ausschließen wollen.
Bootsektor prüfen		Prüft die Bootsektoren des Systems.
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 verweigern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei säubern	Desinfiziert die infizierten Dateien.
	Datei löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.
Aktionsoptionen		Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.

Optionen		Beschreibung
	Zugriff verweigern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
	Datei löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
	In Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.
Dateien größer als (x) nicht prüfen		Geben Sie die maximale Dateigröße an, bis zu der Dateien gescannt werden sollen. Wenn Sie "0" eingeben werden alle Dateien unabhängig von Ihrer Größe geprüft.
Archive größer als [20000] Kb nicht prüfen		Geben Sie die maximale Größe (in Kilobytes/KB) von Archiven ein, die geprüft werden sollen. Wenn Sie alle Archive, unabhängig von deren Größe, prüfen möchten, geben Sie 0 ein.
Netzwerkfreigaben nicht prüfen		Wenn diese Option aktiviert ist wird BitDefender keine Netzwerkfreigaben prüfen um einen schnelleren Netzwerkzugriff zu erlauben. Wir empfehlen die Aktivierung dieser Option nur wenn auf den den anderen Netzwerkrechnern ebenfalls eine Antiviruslösung installiert ist.

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

  Die folgenden Optionen sind verfügbar:

Optionen	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.

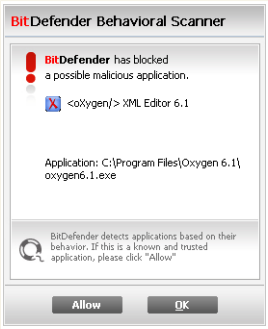
  Im Falle eines Verdachts kann ein Assistent aufgerufen werden der Ihnen dabei hilft, verdächtige Dateien zur weiteren Analyse an das BitDefender Virus Labor zu senden. Optional können Sie Ihre E-Mail-Adresse angeben, um weitere Informationen zur Analyse zu erhalten.
- **Dateien, die über IM erhalten/gesendet wurden prüfen.** Um Dateien zu prüfen, die Sie über Yahoo Messenger oder Windows Live Messenger erhalten oder senden, markieren Sie die entsprechenden Kontrollkästchen.

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

16.1.3. Konfigurieren Sie die Verhaltensprüfung.

Die Verhaltensprüfung bietet Schutz gegen neue Bedrohungen mit unbekannten Signaturen. Er überprüft und analysiert konstant das Verhalten der Anwendungen, die auf Ihrem Computer ausgeführt werden und benachrichtigt Sie, wenn eine Anwendung ein verdächtiges Verhalten aufweist.

Die Verhaltensprüfung benachrichtigt Sie, wenn eine Anwendung versucht eine potenziell schädliche Aktion durchzuführen und fordert Sie zum Handeln auf.

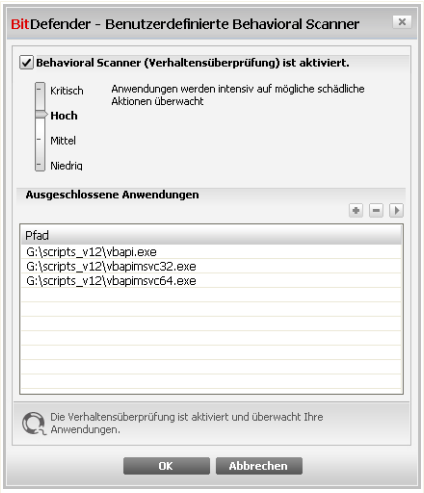


Benachrichtigung der Verhaltensprüfung

Wenn Sie die entdeckte Anwendung kennen und ihr vertrauen, klicken Sie auf **Erlauben**. Die Verhaltensprüfung wird diese Anwendung nicht weiter auf möglicherweise schädliches Verhalten prüfen.

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

Um die Verhaltensprüfung zu konfigurieren, klicken Sie auf **Prüfeinstellungen**.



Benutzerdefinierte Behavioral Scanner

Wenn Sie die Verhaltensprüfung deaktivieren möchten, lassen Sie das Kontrollkästchen **Verhaltensprüfung ist aktiviert** frei.

Wichtig
Lassen Sie die Verhaltensprüfung aktiviert, um gegen unbekannte Viren geschützt zu sein.

Sicherheitsgrad einstellen

Die Sicherheitsstufe der Verhaltensprüfung ändert sich automatisch, wenn Sie eine neue Stufe für den Echtzeitschutz einstellen. Wenn Sie mit der Standardeinstellung nicht zufrieden sein sollten, können Sie die Sicherheitsstufe manuell konfigurieren.

Anmerkung
Bitte denken Sie daran, dass bei der Änderung der aktuellen Sicherheitsstufe des Echtzeitschutzes, die Sicherheitsstufe der Verhaltensprüfung ebenfalls verändert wird.

Ziehen Sie den Schieber an der Skala entlang, um die Sicherheitsstufe an Ihre Bedürfnisse anzupassen.

Sicherheitseinstellung	Beschreibung
Wichtig	Anwendungen werden streng auf potenziell schädliche Aktionen überwacht.
Hoch	Anwendungen werden intensiv auf potenziell schädliche Aktionen überwacht.
Mittel	Anwendungen werden mittelmäßig auf potenziell schädliche Aktionen überwacht.
Niedrig	Anwendungen werden auf potenziell schädliche Aktionen überwacht.

Ausgeschlossene Anwendungen verwalten

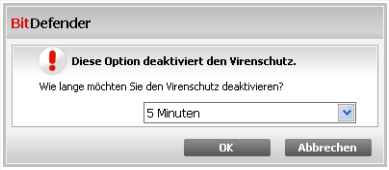
Sie können die Verhaltensprüfung so einstellen, dass bestimmte Anwendungen nicht überprüft werden. Die Anwendungen, die aktuell nicht von der Verhaltensprüfung überprüft werden, befinden sich in der Tabelle**Ausgeschlossene Anwendungen**.

Um die ausgeschlossenen Anwendungen zu verwalten, können Sie die Schaltflächen verwenden, die sich im oberen Bereich der Tabelle befineden:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.
- **Edit** - edit an application path.

16.1.4. Echtzeitschutz deaktivieren

Wenn Sie den Echtzeitschutz deaktivieren möchten erscheint ein Warnfenster.



Echtzeitschutz deaktivieren

Sie müssen die Deaktivierung bestätigen indem Sie wählen wie lange der Schutz deaktiviert werden soll. Zur Auswahl stehen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.

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

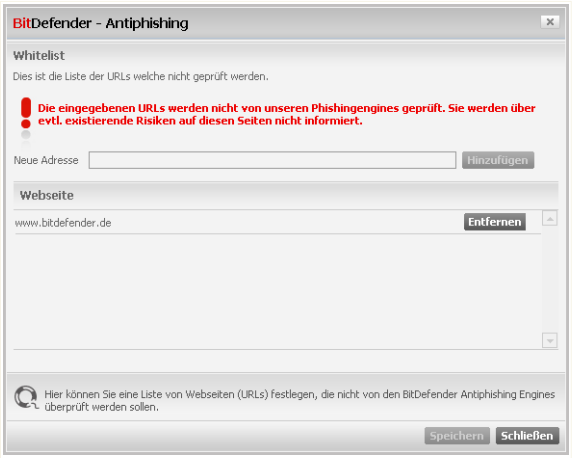
16.1.5. Antiphishingschutz konfigurieren

BitDefender bietet Antiphishingschutz in Echtzeit für:

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

Sie können den Antiphishingschutz für bestimmte Anwendungen oder komplett deaktivieren.

Sie können auf **Whitelist** klicken um eine Liste von Webseiten zu konfigurieren und verwalten, die nicht von den BitDefender Antiphishing-Engines überprüft werden sollen.



Antiphishing Whitelist

Sie können eine Liste der Webseiten sehen, die BitDefender aktuell nicht auf Phishinginhalte prüft.

Um eine neue Webseite zur Whitelist hinzuzufügen geben Sie die Adresse in das Feld **Neue Adresse** ein und klicken Sie dann auf **Hinzufügen**. Die Whitelist sollte nur Webseiten enthalten, denen Sie vollständig vertrauen. Fügen Sie beispielsweise Webseiten hinzu, auf denen Sie häufig einkaufen.

Anmerkung

Mit Hilfe der BitDefender Antiphishing-Toolbar in Ihrem Webbrowser können Sie ganz einfach Webseiten zu der Whitelist hinzufügen.

Um eine Webseite aus der Whitelist zu entfernen klicken Sie auf die entsprechende Schaltfläche **Entfernen**.

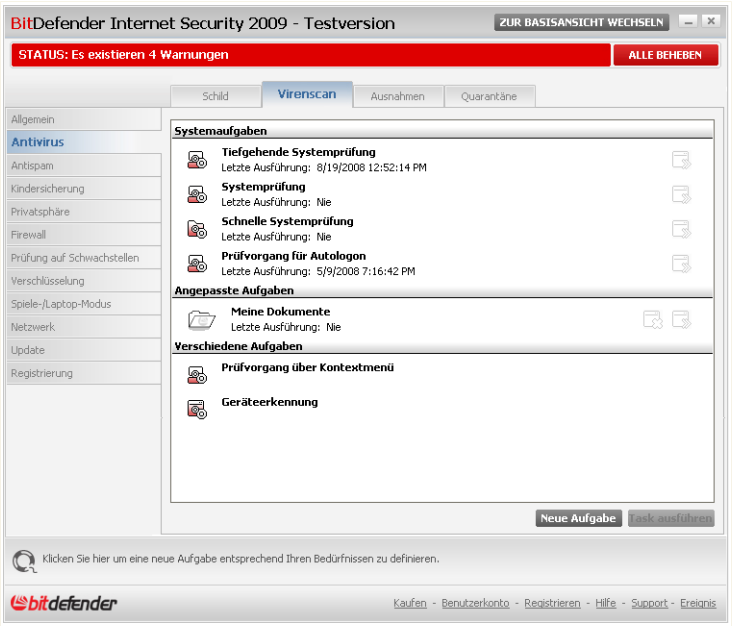
Klicken Sie auf **Schließen**, um die Änderungen zu speichern und das Fenster zu schließen.

16.2. Prüfvorgang

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.

Um einen On-Demand Prüfvorgang zu konfigurieren und zu starten klicken Sie auf **Antivirus>Prüfen** in der erweiterten Ansicht.



Prüfaufgaben

Der Prüfvorgang basiert auf Prüfaufgaben welche die Einstellungen zum Vorgang sowie die zu prüfenden Objekte beinhalten. Sie können einen Prüfvorgang einfach durch das Ausführen einer vordefinierten Aufgabe starten oder aber Sie erstellen sich selbst eine angepasste Aufgabe.

16.2.1. Prüfaufgaben

BitDefender enthält bereits eine große Zahl von vordefinierten Aufgaben für bestimmte Gegebenheiten.

Jede Aufgabe hat ein **Einstellungen** Fenster welches Ihnen erlaubt die Einstellungen einzustellen und die Prüfberichte zu betrachten. Weitere Informationen finden Sie unter „*Konfiguration einer Prüfaufgabe*“ (S. 147).

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

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

Standard Einstellungen	*Beschreibung*
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Schnelle Systemprüfung	Prüft die Ordner `Windows`, `Programme` und `All Users`. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.
Prüfung bei Login	Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet. Standardmäßig ist die Prüfung im Hintergrund deaktiviert. Um die Aufgabe zu benutzen, klicken Sie darauf mit der rechten Maustaste, wählen Sie **Planer** und setzen Sie die Ausführung der Aufgabe**beim Systemstart**. Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)

Anmerkung
Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

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

  Eine Aufgabe `Meine Dokumente` steht ebenfalls zur Verfügung. Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

- **Standardaufgaben** - 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:

- **Planer** - zeigt an ob die Aufgabe zu einen bestimmten Zeitpunkt durchgeführt werden soll. Klicken Sie auf die Schaltfläche um das **Einstellungen** Fenster zu öffnen, im Reiter Planer können Sie die Details einsehen und ändern.
- **Löschen** - löscht die ausgewählte Aufgabe.

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

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus, indem eine Sofortige Prüfung durchgeführt wird.

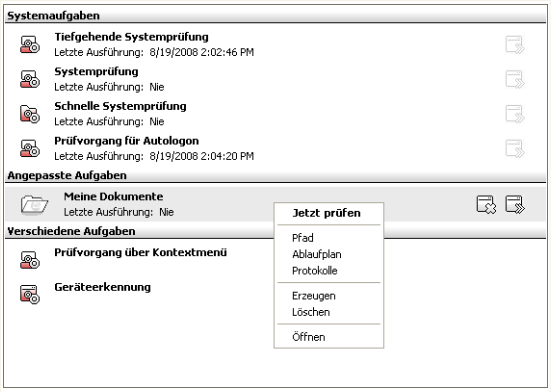
Jede Prüfung hat ihre eigenen **Eigenschaften** Fenster, in welchem Sie die Prüfoptionen konfigurieren, das Ziel der Prüfung festlegen,die Tasks planen oder die Berichte ansehen können.

16.2.2. Verwenden des Kontextmenüs

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

Folgende Aktionen stehen zur Verfügung:

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



Shortcut Menü

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

Anmerkung
Im Falle von Systemaufgaben wird diese Option durch **Aufgabenpfade anzeigen** ersetzt.

- **Ablaufplan** - Öffnet das Fenster **Eigenschaften** , Planer, wo Sie die ausgewählten Aufgaben planen können.
- **Prüfberichte** - Öffnet das Fenster **Eigenschaften**, Prüfberichte, wo Sie die Berichte sehen, die nach dem Prüfungvorgang erstellt wurden.
- **Dublizieren** - Kopiert die ausgewählte Aufgabe. Dies ist sinnvoll, wenn neue Aufgaben erstellt werden, weil die Einstellungen für die wiederholte Aufgabe geändert werden können.
- **Löschen** - löscht die ausgewählte Aufgabe.

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

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

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

16.2.3. Erstellen von Zeitgesteuerten Aufgaben

Um eine Prüfaufgabe zu erstellen verwenden Sie eine der folgenden Methoden:

- Dublizieren einer existierenden Regel, neu benennen und vornehmen der nötigen Änderungen im Fenster Eigenschaften.
- Klicken Sie auf **Neue Aufgabe** um eine neue Aufgabe zu erstellen und zu konfigurieren.

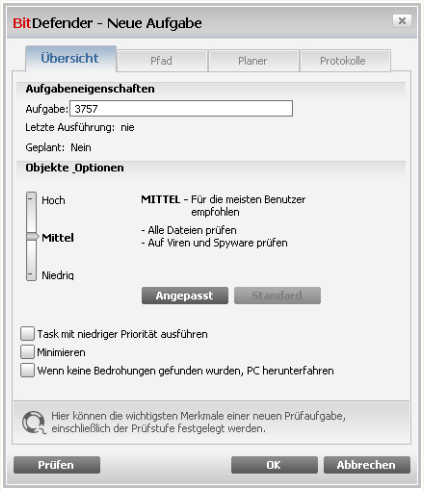
16.2.4. Konfiguration einer Prüfaufgabe

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. Um das Fenster zu öffnen klicken Sie auf die **Öffnen** Schaltfläche, auf der rechten Seite der Aufgabe (oder rechtsklicken Sie die Aufgabe und wählen Sie **Öffnen**).

Anmerkung
Weitere Inhalte und Einzelheiten zum Reiter **Prüfberichte** finden Sie in der Produktbeschreibung auf Seite „*Prüfberichte anzeigen*“ (S. 165).

Konfigurieren der Prüfoptionen

Um die Prüfoptionen einer Prüfaufgabe festzulegen klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Eigenschaften**. Das folgende Fenster wird erscheinen:



Übersicht

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

Prüftiefe festlegen

Sie können die Konfiguration einfach durch das wählen der Prüftiefe festlegen. 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.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel. Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
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.

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

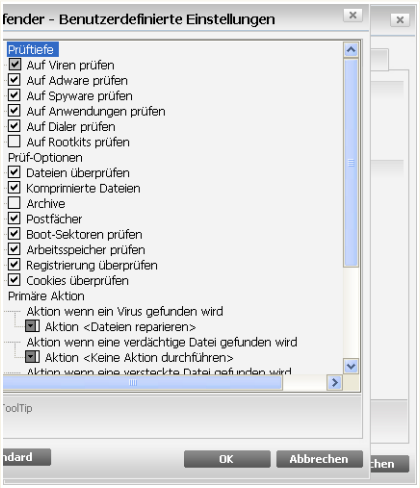
- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
- **Minimieren des Prüffensters beim Scan-Start.** Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das BitDefender - Logo in der Symbolleiste wieder geöffnet werden.
- **Herunterfahren des Computers nach erfolgtem Prüfvorgang und wenn keine Bedrohungen gefunden wurden**

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

Prüftiefe konfigurieren

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.

Klicken Sie bitte auf**Anpassen** - um Ihre eigenen Prüfoptionen zu setzen. Ein neues Fenster öffnet sich.



Auswahlfenster Einstellungen

Die Prüfoptionen sind wie ein aufklappbares Windows-Explorermenü aufgebaut. Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Die Prüfoptionen sind in 3 Kategorien unterteilt:

- **Prüftiefe.** Legen Sie fest nach welcher Art von Schädlingen BitDefender suchen soll indem Sie die entsprechende **Prüftiefe** aktivieren.

Optionen	*Beschreibung*
Dateien prüfen	Sucht nach bekannten Viren.

Optionen	Beschreibung
	BitDefender erkennt auch unvollständige Virenkörper, dadurch wird Ihr System zusätzlich geschützt.
Auf Adware prüfen	Sucht nach möglichen Adware-Anwendungen. Entsprechende Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.
Auf Spyware prüfen	Sucht nach bekannter Spyware. Entsprechende Dateien werden wie infizierte Dateien behandelt.
Programmdateien prüfen	Legitime Anwendungen prüfen, die als Spionage-Tool verwendet werden können, um schädliche Anwendungen oder andere Bedrohungen zu verbergen.
Auf Dialer prüfen	Prüft auf Anwendungen welcher kostenpflichtige Nummern wählen. Erkannte Dateien werden als infiziert behandelt. Dadurch ist es möglich das betroffene Anwendungen nicht mehr funktionsfähig sind.
Auf Rootkits prüfen	Prüft nach versteckten Objekten (Dateien und Prozesse), meist Rootkits genannt.

- **Prüfoptionen.** Geben Sie an, welche Arten von Objekten geprüft werden sollen (Dateitypen, Archive, usw.), indem Sie die entsprechenden Optionen in der Kategorie **Virenprüfoptionen** auswählen.

Optionen		Beschreibung
Dateien	**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`;

Optionen		Beschreibung
		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.
Komprimierte Dateien		Alle komprimierten Dateien werden überprüft.
Archive		Prüft den Inhalt von eingepackten Archiven. Die Prüfung archivierter Dateien verlängert die benötigte Zeit für die Prüfung und erfordert mehr Systemressourcen. Sie können auf **Begrenzung der Archivgröße** klicken und die maximale Größe der zu prüfenden Archive in Kilobytes (KB) eingeben.
Postfächer		Prüft den Inhalt von E-Mails und deren Attachments.
Boot-Sektoren		Prüft die Bootsektoren des Systems.
Speicher prüfen		Prüft den Speicher auf Viren und andere Malware.
Registry prüfen		Prüft Einträge in der Systemregistrierung.
Cookies prüfen		Prüft gespeicherte Cookies von Webseiten.

- **Aktionsoptionen.** Geben Sie die auszuführende Aktion für jede Kategorie entdeckter Dateien an, indem Sie die Optionen in der Kategorie **Aktionsoptionen** verwenden.

  Anmerkung
  Um eine neue Aktion auszuwählen, klicken Sie auf die aktuelle Aktion und wählen Sie die gewünschte Aktion aus dem Menu.

  - Wählen Sie die durchzuführende Aktion für die erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien können Sie in der Berichtsdatei einsehen.
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.
Dateien löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

- Wählen Sie die durchzuführende Aktion für die als verdächtig erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für verdächtige Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Dateien löschen	Die verdächtige Datei wird ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die verdächtige Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Anmerkung
Es wurden verdächtige Dateien gefunden. Wir empfehlen Ihnen diese Dateien zur Analyse an das BitDefender Labor zu senden.

- Wählen Sie die durchzuführende Aktion für die erkannten versteckten Dateien (Rootkits): Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für versteckte Dateien ausgeführt. Diese Dateien finden Sie in der Berichtsdatei.
In die Quarantäne verschieben	Verschiebt die versteckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Sichtbar machen	Deckt versteckte Dateien auf so das diese sichtbar werden.

- **Optionen für Aktionen für archivierte Dateien.** Die Prüfung und der Umgang mit Dateien in Archiven kann begrenzt sein. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Je nach Archivformat (Typ), kann BitDefender infizierte archivierte Dateien möglicherweise nicht desinfizieren, isolieren oder löschen. Konfigurieren Sie die Optionen, die für entdeckte archivierte Dateien ausgeführt werden sollen, indem Sie die entsprechenden Optionen aus der Kategorie**Aktionsoptionen für archivierte Dateien** auswählen.
  - Wählen Sie die durchzuführende Aktion für die erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Nur infizierte archivierte Dateien in das Prüfprotokoll aufnehmen. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
Dateien löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.

Aktion	Beschreibung
In die Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

- Wählen Sie die durchzuführende Aktion für die als verdächtig erkannten Dateien: Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Nur verdächtige archivierte Dateien in das Prüfprotokoll aufnehmen. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Dateien löschen	Die verdächtige Datei wird ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die verdächtige Datei in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

- Wählen Sie die durchzuführende Aktion für entdeckte Dateien mit Passwortschutz. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Als nicht geprüft protokollieren	Nur passwortgeschützte Dateien in das Prüfprotokoll aufnehmen. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Passwort erfragen	Wenn eine passwortgeschützte Datei entdeckt wird, den Benutzer dazu auffordern das Passwort anzugeben, damit die Datei geprüft werden kann.

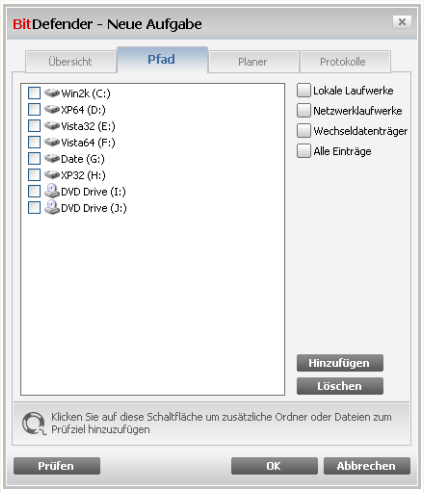
Anmerkung

Sollten Sie sich entschliessen die entdeckten Dateien zu ignorieren oder die gewählte Aktion fehlschlagen so müssen Sie im Prüfvorgangs-Assitenten eine Aktion auswählen.

Mit dem Klick auf **Standard** laden Sie die Grundeinstellungen. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Festlegen der Zielobjekte

Um das Zielobjekt einer Prüfaufgabe festzulegen rechtsklicken Sie auf diese und wählen Sie **Pfad**. Das folgende Fenster wird erscheinen:



Prüfziel

Sie können die Liste mit Lokalen, Netzwerk und Wechseldatenträgern sowie den Dateien und Ordnern einsehen. Alle markierten Objekte werden beim Prüfvorgang durchsucht.

Dieser Bereich enthält folgende Schaltflächen:

- **Hinzufügen** - Diese Schaltfläche ermöglicht das Hinzufügen von Dateien und Ordnern zur Prüfaufgabe.

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

- **Objekt(e) entfernen** - entfernt die Datei(en)/Ordner, die/der zuvor aus der Liste der zu prüfenden Objekte ausgewählt wurde(n).

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.

Prüfziel der Systemaufgaben anzeigen

Sie können das Prüfziel einer **Systemaufgabe** nicht ändern. Sie können nur ihr Prüfziel sehen.

Um das Zielobjekt einer bestimmten Prüfaufgabe zu sehen, klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie **Aufgabenpfade anzeigen**. Für eine **Vollständige Systemprüfung**, wird beispielsweise das folgende Fenster erscheinen:

Prüfziel der vollständigen Systemprüfung

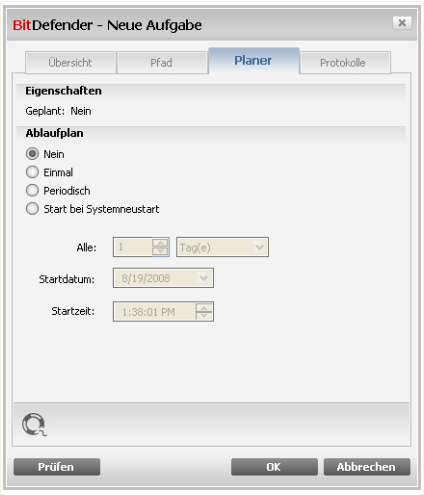
Vollständige Systemprüfung und **Tiefe Systemprüfung** werden alle lokalen Laufwerke prüfen, während**Schnelle Systemprüfung** nur die Ordner `Windows` und `Programme/Dateien` prüfen wird.

Klicken Sie auf **OK**, um dieses Fenster zu schließen. Um den Vorgang auszuführen, klicken Sie auf **Prüfen**.

Zeitgesteuerte Aufgaben festlegen

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.

Um eine Aufgabe zeitlich zu steuern rechtsklicken Sie auf diese und wählen Sie **Planer**. Das folgende Fenster wird erscheinen:



Planer

Hier können Sie die Einstellungen zum geplanten Prüfvorgang einsehen.

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**.
- **Bei Systemstart** - führt die Prüfung nach einer festgelegten Anzahl von Minuten durch, nachdem der Benutzer sich bei Windows angemeldet hat.

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

16.2.5. Prüfoptionen

Bevor Sie einen Prüfvorgang starten sollten Sie sich stellen das BitDefender aktuell ist. Die könnte dazu führen das BitDefender Viren nicht erkennt. Um sicherzustellen das BitDefender aktuell ist prüfen Sie die Sektion **Update>Update** in der Einstellungskonsole.

Anmerkung
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).

Prüfoptionen

BitDefender bietet vier Arten einen Prüfvorgang durchzuführen:

- Sofortiges Prüfen - Startet die von Ihnen gewählte Aufgabe umgehend
- Kontextbezogenes Prüfen - Rechtsklicken Sie auf eine Datei oder einen Ordner und wählen Sie im Kontextmenü BitDefender AntiVirus 2009 aus.
- Prüfen per Drag & Drop - verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitäts-Anzeige.
- Manuelle Prüfung - Verwenden Sie BitDefender Manuelle Prüfung um bestimmte Dateien und Ordner direkt zu prüfen.

Sofortiges Prüfen

Um Ihren Computer oder Teile Ihres Computers zu prüfen können Sie die Standardeinstellungen nutzen oder Ihre eigenen Aufgaben einrichten. Dies nennt sich Sofortiges Prüfen

Folgende Optionen sind wählbar:

- Doppelklick auf den gewünschten Prüfvorgang von der Liste.
- Klicken Sie **Jetzt Prüfen** für die entsprechende Aufgabe.
- Bitte wählen Sie die entsprechende Aufgabe und klicken Sie **Aufgabe ausführen**.

Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 161) in diesem Handbuch.

Scannen mit dem Kontextmenü

Um eine Datei oder einen Ordner zu prüfen ohne eine neue Aufgabe anzulegen können Sie die Kontextmenü-Prüfung verwenden. Dies nennt man Scannen mit dem Kontextmenü

Prüfvorgang über Kontextmenü

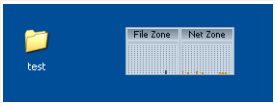
Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei oder Ordner und wählen Sie **BitDefender Antivirus 2009** aus.

Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel *„BitDefender Scanner“* (S. 161) in diesem Handbuch.

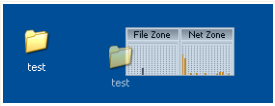
Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster **Eigenschaften** auf **Prüfen Kontext Menü** klicken.

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

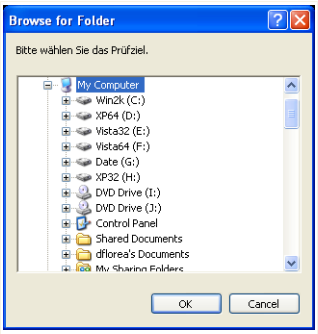
Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel *„BitDefender Scanner“* (S. 161) in diesem Handbuch.

Manuelle Prüfung

Die Manuelle Prüfung besteht daraus das zu prüfende Objekt direkt über die BitDefender Manuelle Prüfungsoption über den BitDefender Startmenüeintrag zu wählen.

Anmerkung
Die Manuelle Prüfung ist sehr hilfreich, da Sie diese auch im Abgesicherten Modus von Windows verwenden können.

Um das zu prüfende Objekt zu wählen verwenden Sie den Pfad: **Start → Programme → BitDefender 2009 → BitDefender Manuelle Prüfung**. Das folgende Fenster wird erscheinen:



Manuelle Prüfung

Wählen Sie das zu prüfende Objekt und klicken Sie auf **OK**.

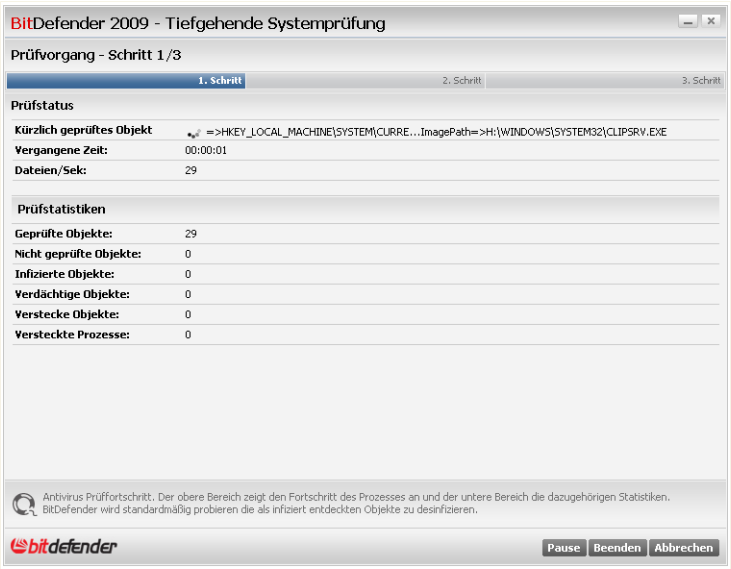
Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel *„BitDefender Scanner“* (S. 161) in diesem Handbuch.

BitDefender Scanner

Wenn Sie einen einen Prüfvorgang einleiten wird der BitDefender Scanner gestartet. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

Schritt 1/3 - Prüfvorgang

BitDefender prüft die gewählten Dateien und Ordner.



Prüfvorgänge durchführen

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

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

Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.

Bitte warten Sie bis BitDefender den Prüfvorgang beendet hat.

Schritt 2/3 - Aktionsauswahl

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

Aktionen

Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.

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

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.

Folgende Aktionen stehen zur Verfügung:

Aktion	*Beschreibung*
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt.
Desinfizieren	Desinfiziert die infizierten Dateien.
Löschen	Löscht die infizierten Dateien.
Aufdecken	Macht versteckte Objekte sichtbar.

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

Schritt 3/3 - Zusammenfassung

Wenn BitDefender das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet.

Übersicht

Ihnen wird eine Zusammenfassung angezeigt. Klicken Sie auf **Protokolldatei anzeigen** um das Prüfprotokoll zu sehen.

Wichtig
Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

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

BitDefender konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert BitDefender erfolgreich die infizierten Dateien, die er entdeckt hat, oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht gelöst werden können.

In diesen Fällen empfehlen wir Ihnen unser BitDefender Support Team unter www.bitdefender.de zu kontaktieren. Die Mitarbeiter unseres Supports werden Ihnen dabei helfen die entsprechenden Probleme zu lösen.

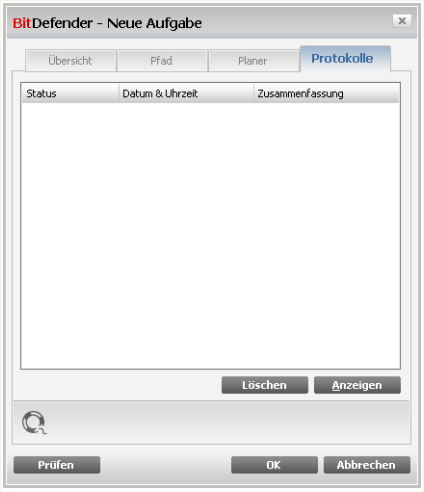
Von BitDefender entdeckte verdächtige Dateien

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

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

16.2.6. Prüfberichte anzeigen

Um die Prüfberichte nach dem beenden des Prüfvorgangs anzusehen, rechtsklicken Sie auf die Aufgabe und wählen Sie **Prüfberichte anzeigen**. Das folgende Fenster wird erscheinen:



Prüfberichte

Hier können Sie die Berichtdateien sehen, die immer dann erstellt werden wenn eine Aufgabe ausgeführt wurde. Jede Datei beinhaltet Informationen über den Status des Prüfprozesses, das Datum und die Zeit wann die Prüfung durchgeführt wurde und eine Zusammenfassung der Prüfergebnisse.

Zwei Schaltflächen sind verfügbar:

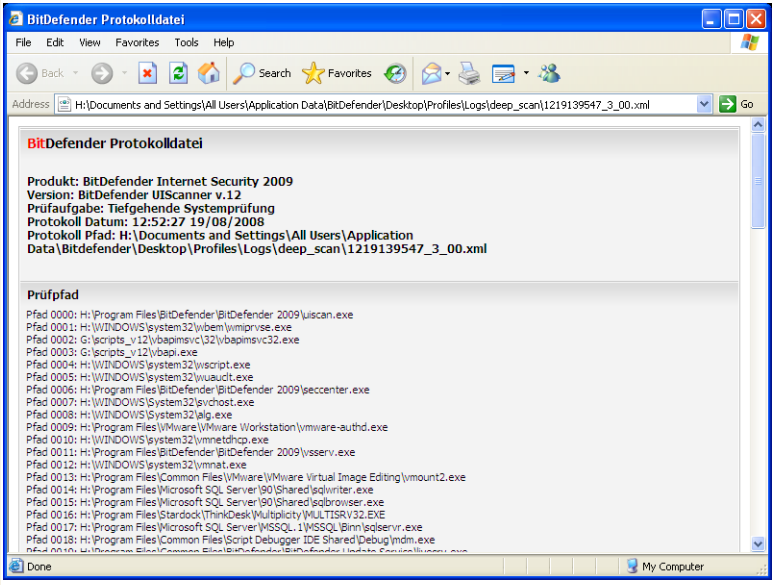
- **Löschen** - löscht die ausgewählte Berichtsdatei.
- **Anzeigen** - öffnet die ausgewählte Berichtsdatei. Die Berichtdatei wird in Ihrem Webbrowser geöffnet.

Anmerkung
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.

Beispiel Prüfbericht

Das folgende Bild zeigt ein Beispiel eines Prüfberichts:



Beispiel Prüfbericht

Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

16.3. Vom Prüfvorgang ausgeschlossene Objekte

In manchen Fällen wird es nötig sein bestimmte Dateien vom Prüfen auszunehmen. Zum Beispiel wenn Sie EICAR Testdateien von der Echtzeiprüfung ausschließen wollen, oder `.avi` Dateien nicht "on-demand" prüfen möchten.

BitDefender bietet die Möglichkeit Objekte vom Prüfvorgang, vom Echtzeitschutz oder von beidem auszunehmen. Dies dient dazu die Prüfgeschwindigkeit zu erhöhen oder Eingriffe bei der Arbeit zu verhindern.

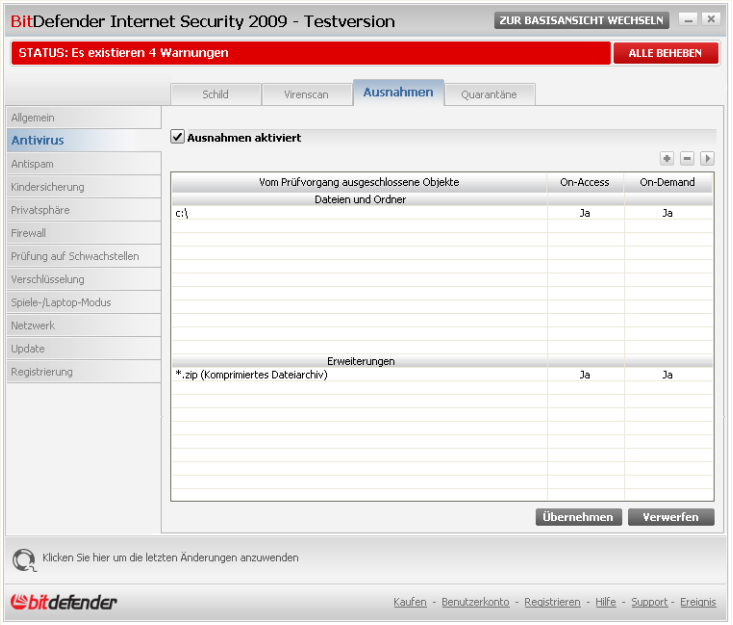
Zwei Arten von Objekten können vom Prüfen ausgenommen werden:

- **Pfade** - Die Datei oder der Ordner (inklusive der enthaltenen Objekte) werden nicht geprüft.

- **Erweiterungen** - Alle Dateien mit der festgelegten Erweiterung werden vom Prüfen ausgeschlossen.

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

Um die vom Prüfvorgang ausgeschlossenen Objekte zu sehen und verwalten klicken Sie auf **Antivirus>Ausnahmen** in der erweiterten Ansicht.



Ausnahmen

Sie können die Objekte (Dateien, Ordner, Erweiterungen) welche vom Prüfen ausgenommen sind einsehen. Für jedes Objekt ist ersichtlich ob es von der Echtzeitprüfung, dem Prüfvorgang oder beidem ausgenommen ist.

Anmerkung
Die vorgenommenen Ausnahmen werden bei der Kontextmenüprüfung NICHT berücksichtigt.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche

Um ein Objekt aus der Liste zu bearbeiten, klicken Sie auf die **Bearbeiten**-Schaltfläche. Ein neues Fenster erscheint in welchem Sie die Erweiterung, den Pfad und den Prüftyp der Ausnahme festlegen können. Wenn Sie die Änderungen vorgenommen haben klicken Sie auf **OK**.

Anmerkung
Sie können das Objekt auch mit der rechten Maustaste anklicken un es zu bearbeiten oder zu löschen.

Klicken Sie auf **Verwerfen** um die Änderungen welche Sie noch nicht mit **Übernehmen** bestätigt haben rückgängig zu machen.

16.3.1. Pfade vom Prüfen ausnehmen

Um einen Pfad vom Prüfen auszunehmen klicken Sie auf **Hinzufügen**. Sie werden vom Konfigurationsassistenten durch den Prozess des Ausnehmens geführt.

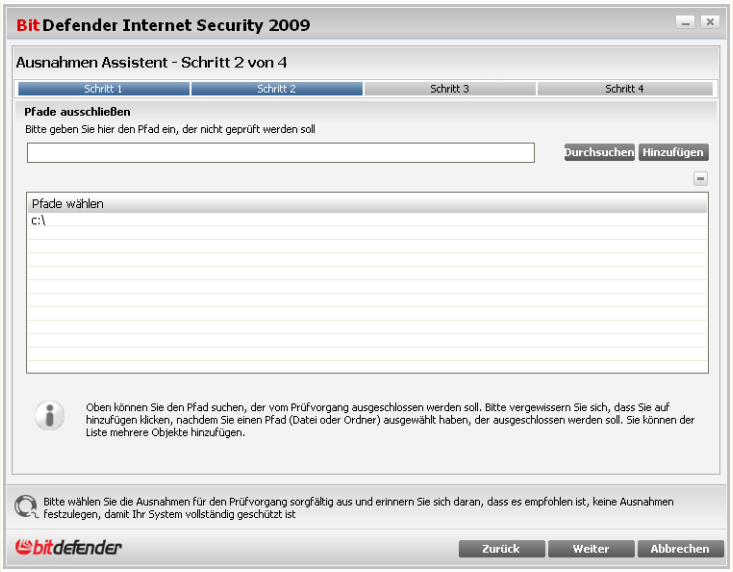
Schritt 1/4 - Wählen Sie die Objektart

Objektart

Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.

Klicken Sie auf **Weiter**.

Schritt 2/4 - Festlegen des Pfads



Ausgenommene Pfade

Um einen Pfad vom Prüfen auszuschliessen verwenden Sie eine von folgenden Methoden:

- Klicken Sie auf **Durchsuchen** und wählen Sie den gewünschten Ordner bzw. Datei, klicken Sie dann auf **Hinzufügen**.
- Geben Sie den Pfad welchen Sie vom Prüfen ausnehmen möchten direkt in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

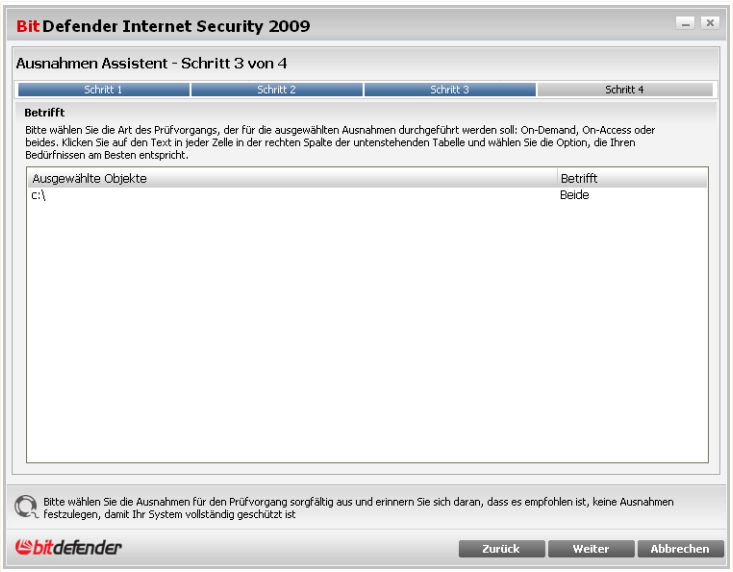
> ***Anmerkung***
> Sollte der eingegebene Pfad nicht existieren so erscheint eine Fehlermeldung. Klicken Sie auf **OK** und prüfen Sie den angegebenen Pfad.

Der Pfad erscheint in dem Moment in der Tabelle in welchem Sie ihn hinzufügen. Sie können so viele Pfade hinzufügen wie Sie wünschen.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp



Prüftyp

Sie bekommen angezeigt welche Pfade ausgenommen sind und von welchem Prüftyp.

Standardmässig sind die Pfade von beiden Prüftypen ausgenommen, Echtzeitschutz und Prüfvorgang. Um dies zu Ändern klicken Sie auf die entsprechende Anzeige und wählen Sie die gewünschte Option.

Klicken Sie auf **Weiter**.

Schritt 4/4 - Ausgeschlossene Dateien prüfen

Ausgeschlossene Dateien prüfen

Es wird dringend empfohlen die Dateien unter den festgelegten Pfaden zu prüfen, um sicherzustellen, dass diese nicht infiziert sind. Bitte markieren Sie das Kontrollkästchen um diese Dateien zu prüfen, bevor Sie von der Prüfung ausgeschlossen werden.

Klicken Sie auf **Fertigstellen**.

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

16.3.2. Dateierweiterungen vom Prüfen ausnehmen

Um Dateierweiterungen vom Prüfen auszunehmen klicken Sie auf die **Hinzufügen**-Schaltfläche. Der Ausnahmeassistent wird Sie durch den Vorgang begleiten.

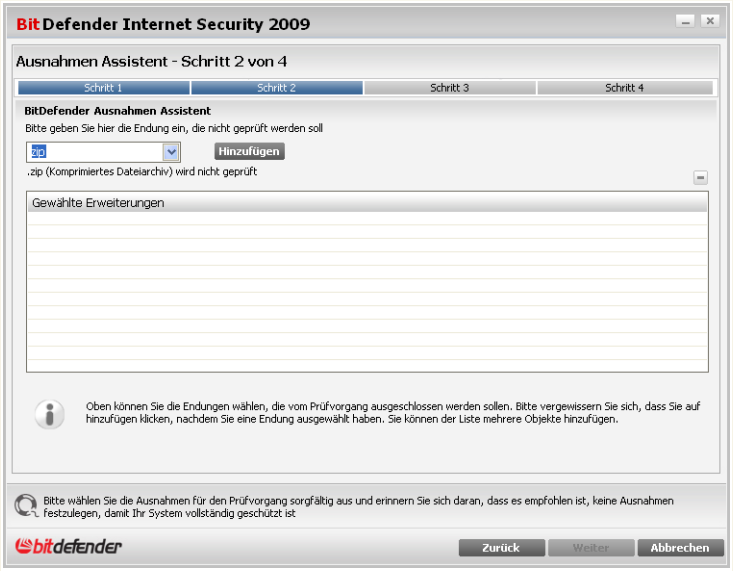
Schritt 1/4 - Wählen Sie die Objektart

Objektart

Wählen Sie die Option um eine Dateierweiterung vom Prüfen auszunehmen.

Klicken Sie auf **Weiter**.

Schritt 2/4 - Erweiterungen festlegen



Ausgenommene Erweiterungen

Um die auszunehmenden Erweiterungen festzulegen verwenden Sie eine der folgenden Methoden:

- Wählen Sie die gewünschte Erweiterung aus dem Menü aus und klicken Sie auf **Hinzufügen**.

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

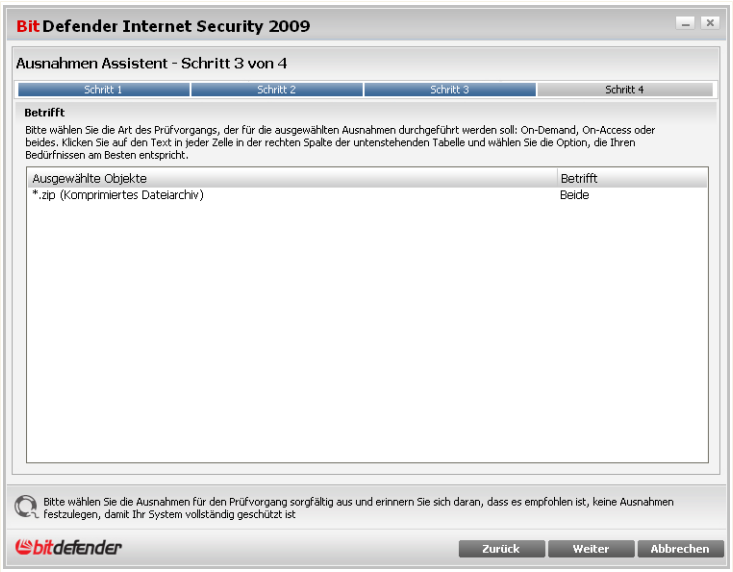
- Geben Sie die gewünschte Erweiterung in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

Die Erweiterungen erscheinen in der Tabelle sobald Sie diese hinzufügen. Sie können so viele Erweiterungen hinzufügen wie Sie wünschen.

Um ein Objekt aus der Liste zu entfernen markieren Sie es und klicken Sie dann auf die **Entfernen**-Schaltfläche

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp



Prüftyp

Ihnen wird eine Tabelle angezeigt in welche Sie die ausgenommenen Erweiterungen und den Prüftyp einsehen können.

Standardmässig werden die gewählten Erweiterungen von beiden Prüftypen ausgenommen (Echtzeitschutz und Prüfvorgang). Um dies zu klicken Sie auf die entsprechende Spalte und wählen Sie den gewünschten Eintrag.

Klicken Sie auf **Weiter**.

Schritt 4/4 - Wählen Sie den Prüftyp

Prüftyp

Es wird dringend empfohlen die Dateien mit den festgelegten Endungen zu prüfen, um sicherzustellen, dass sie nicht infiziert sind.

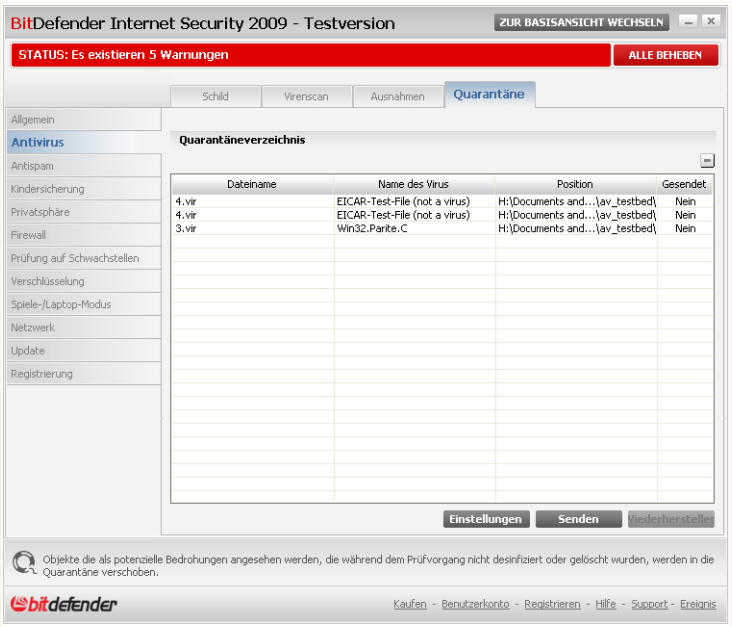
Klicken Sie auf **Fertigstellen**.

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

16.4. Quarantäne

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

Um die in die Quarantäne verschobenen Dateien zu sehen und Quarantäne-Einstellungen vorzunehmen klicken Sie in der erweiterten Ansicht auf **Antivirus>Quarantäne**.



Quarantäne

Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden. Zu jeder Datei die sich in der Quarantäne befindet sind die folgenden Informationen verfügbar: Name der Datei, Name des entdeckten Virus, der ursprüngliche Speicherort und das Übertragungsdatum.

Anmerkung

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

16.4.1. Quarantäne-Dateien verwalten

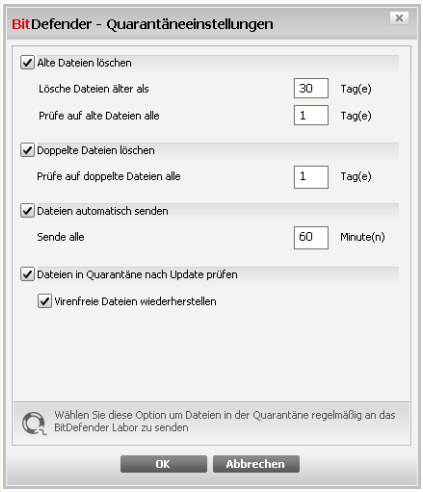
Um eine ausgewählte Datei aus der Quarantäne zu löschen klicken Sie **entfernen**. Wenn Sie eine infizierte Datei wiederherstellen wollen in ihrem original Speicherort klicken Sie **Wiederherstellen**.

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

Kontextmenü. Um die Quarantänedateien einfach zu verwalten steht ein Kontextmenü zur Verfügung. Hier stehen die selben Option wie zuvor genannt zur Verfügung. Klicken Sie auf **Aktualisieren** um die Ansicht zu erneuern.

16.4.2. Quarantäne-Einstellungen konfigurieren

Wenn Sie die Quarantäne-Einstellungen konfigurieren möchten klicken Sie auf **Einstellungen**. Ein neues Fenster wird sich öffnen.



Quarantäne Einstellungen

Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:

Alte Dateien löschen. Um alte Dateien in der Quarantäne automatisch zu löschen aktivieren Sie die entsprechende Option. Sie können festlegen nach wievielen Tagen alte Dateien gelöscht werden und wie oft BitDefender dies prüfen soll.

Anmerkung
In der Standardeinstellungen prüft BitDefender jeden Tag nach alten Dateien und löscht diese wenn Sie älter als 30 Tage sind.

Doppelte Dateien löschen. Um doppelte Dateien in der Quarantäne automatisch zu löschen aktivieren Sie die entsprechende Option. Geben Sie an wie oft eine Prüfung erfolgen soll.

Anmerkung
Standardmässig prüft BitDefender die Dateien in Quarantäne einmal täglich auf Dublikate.

Dateien automatisch senden. Um Dateien automatisch an das BitDefender Labor zu senden aktivieren Sie diese Option. Geben Sie an wie oft BitDefender die Dateien sendet.

Anmerkung
Standardmässig überträgt prüft BitDefender die Dateien in Quarantäne alle 60 Minuten.

Dateien in der Quarantäne nach einem Update nochmals prüfen. Um Dateien in der Quarantäne nach einem Update nochmals prüfen zu lassen aktivieren Sie die entsprechende Option. Sie können gereinigte Dateien automatisch an ihrem ursprünglichen Speicherort wiederherstellen, indem Sie **Saubere Dateien wiederherstellen** wählen.

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

17. AntiSpam

BitDefender Antispam verwendet aussergewöhnliche Technologische Innovationen und Standard-Antispam Filter um Spam auszusortieren bevor dieser im Posteingang landet.

17.1. Antispam Einblicke

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.

17.1.1. Antispam Filter

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

Anmerkung
Sie können jeden dieser Filter im der Reiter Einstellungen der **Antispam** Sektion aktivieren/deaktivieren.

Liste der Freunde/Liste der Spammer

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).

Sie können die Listen der Freunde/Spammer über die Erweiterte Ansicht oder in der Antispam Toolbar verwalten, die einige der meist benutzten Mail-Clients miteinbezieht.

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

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

Grafik-Filter

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

URL-Filter

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

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

NeuNet-Filter (Heuristik)

Der **Heuristischer Filter** führt eine Reihe von Tests mit allen Nachrichtinhalten durch (z. B. wird nicht nur die Betreffzeile, sondern auch der Nachrichtentext auf HTML-Text überprüft), hält Ausschau nach Wörtern, Phrasen, Links oder anderen Charakteristiken von Spam. Basierend auf dem Resultat der Analyse wird ein SPAM Wert hinzugefügt.

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

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

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 den bayesianischen Filter, indem Sie die **Ist Spam** und **Kein Spam**-Schaltflächen in der Antispam Toolbar benutzen.

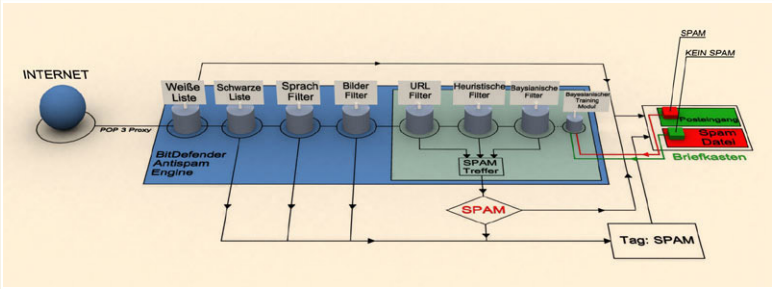
Anmerkung
Bei jedem durchgeführten Update werden:

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

17.1.2. Antispam Vorgang

Das unten abgebildete Schema zeigt, wie BitDefender arbeitet.



Antispam Vorgang

Die oben genannten Antispam-Filter(Freundesliste, Spammerlist, Charsetfilter, Bildfilter, URL-filter, NeuNet (Heuristischer) Filter and Bayesianischer Filter) werden zusammen mit der BitDefender Antispam Engine verwendet, um zu bestimmen ob bestimmte Mails in Ihren **Posteingang** gelangen oder nicht.

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

Der Filter 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.

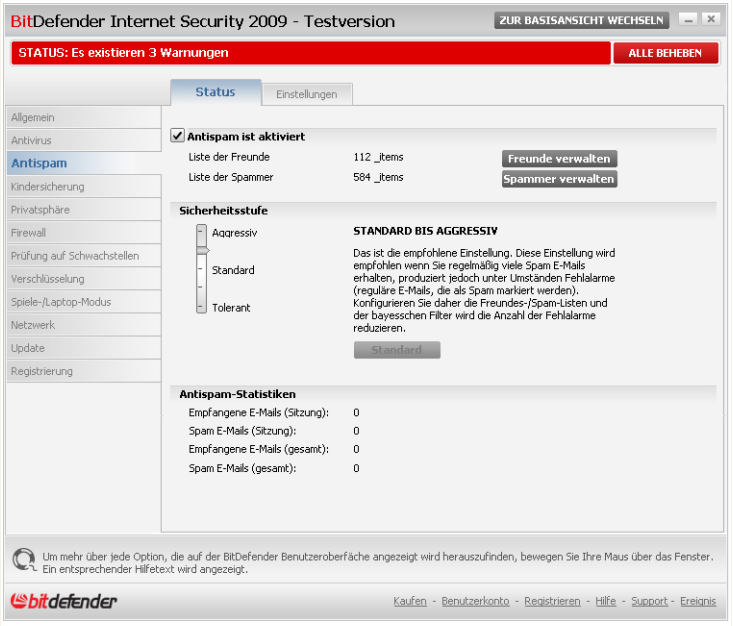
Wichtig

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.

17.2. Status

Um den Antispam-Schutz zu konfigurieren wählen Sie **Antispam>Status** in der erweiterten Ansicht.



Antispam-Status

Sie können sehen ob Antispam aktiviert oder deaktiviert ist. Wenn Sie den Antispam-Status verändern möchten, markieren Sie die entsprechende Option oder lassen Sie sie frei.

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.

17.2.1. Sicherheitsstufe anpassen

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

Es gibt 5 Sicherheitsstufen:

Sicherheitseinstellung	*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)
Tolerant bis Mittel	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. 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.

Sicherheitseinstellung	Beschreibung
	Fügen Sie Ihre Kontakte zur **Freundesliste** hinzu, um die Anzahl an Fehlalarmen zu reduzieren.

Sie können das Level für den gewünschten Schutz einstellen. (**Moderat zu Aggressiv**)Klicken Sie **Level anpassen**.

17.2.2. Freundesliste konfigurieren

Liste der Freunde – die Liste aller E-Mail-Adressen, von denen Sie immer Mails erhalten wollen, egal welchen Inhalts diese sind. Nachrichten Ihrer Freunde werden nicht als Spam deklariert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.

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

Um die Freundesliste zu konfigurieren, klicken Sie auf **Freunde verwalten** (oder klicken Sie auf die Schaltfläche **Freunde** in der Antispam Toolbar).

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 **Freundenliste** zu speichern oder um zu laden. Die Datei wird die `.bwl` Endung haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Liste beim Laden 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.

17.2.3. Konfigurieren der Spammerliste

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 Spammerliste zu konfigurieren, klicken Sie auf **Spammer verwalten** (oder klicken Sie auf die Schaltfläche **Spammer** in der Antispam Toolbar).

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 **Spammerliste** zu speichern oder um zu laden. Die Datei wird die `.bwl` Endung haben.

Um den Inhalt einer aktuellen Liste zurückzusetzen während Sie den Inhalt einer zuvor gespeicherten Liste laden wählen Sie **Liste beim Laden 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.

17.3. Einstellungen

Um die Antispam Einstellungen und Filter zu konfigurieren klicken Sie auf **Antispam>Einstellungen** in der erweiterten Ansicht.

Antispam Einstellungen

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.

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

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

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

17.3.1. 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.

17.3.2. Grundlegende Antispam Filter

- **Freundes-/Spammerlisten** - E-Mail-Nachrichten mit den Freundes-/Spammerlisten filtern.
  - **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 Toolbar den Sender automatisch zu Liste der Freunde hinzufügen.
  - **Automatisch zur Liste der Spammer hinzufügen** - wird beim nächsten Klick auf den **Ist Spam**-Button in der Antispam Toolbar den Sender automatisch zu Liste der Spammer hinzufügen.

Anmerkung
Die **Kein Spam** und **Ist Spam**- trainieren den Bayesian Filter.

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

17.3.3. Erweiterte 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.

18. Kindersicherung

Die BitDefender Kindersicherung gibt Ihnen die Möglichkeit den Zugriff auf das Internet und auf bestimmte Programme für jeden Benutzer mit einem Benutzerkonto auf dem System zu kontrollieren.

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

- Unangemessene Webseiten.
- Den Internetzugang zu bestimmten Zeiten (beispielsweise während dem Unterricht).
- Web-Seiten, Mails und Sofortnachrichten mit bestimmten Schlüsselwörtern.
- Anwendungen wie Spiele, Chat, Filesharing-Programme oder Andere.
- Sofortnachrichten, die von nicht erlaubten IM-Kontakten gesendet werden.

Wichtig

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

Um die Kindersicherung erfolgreich zu verwenden, um die Online- und Computeraktivität Ihrer Kinder zu begrenzen, müssen Sie diese wichtigsten Aufgaben fertigstellen:

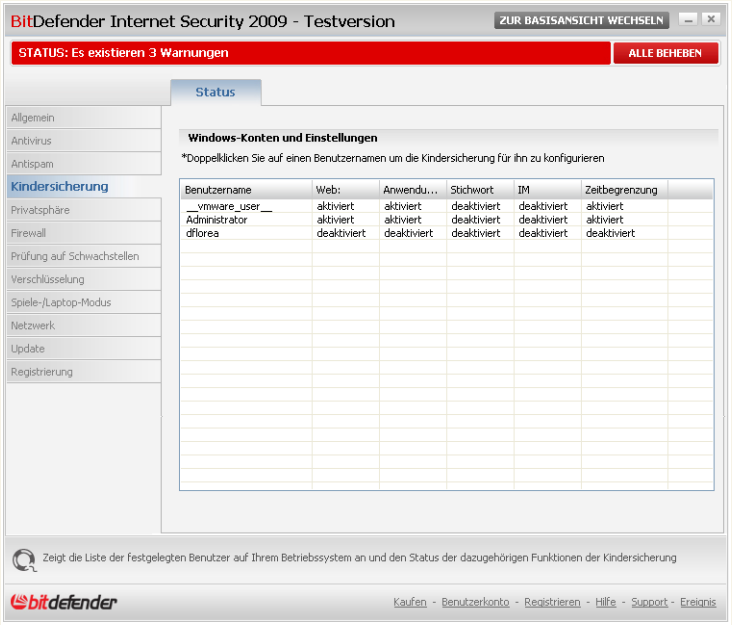
1. Erstellen Sie begrenzte (standard) Windows-Benutzerkonten für Ihre Kinder.

Anmerkung

Um herauszufinden wie Sie Windows-Benutzerkonten erstellen können, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**).

2. Konfigurieren Sie die Kindersicherung für die Windows-Benutzerkonten Ihrer Kinder.

Um die Kindersicherung zu konfigurieren klicken Sie in der erweiterten Ansicht auf **Kindersicherung**.



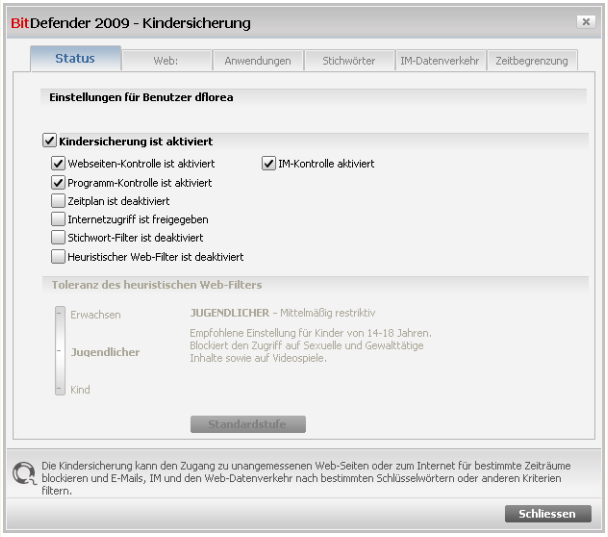
Kindersicherung

Sie können den Status der Funktionen der Kindersicherung sehen, die für jedes Windows Benutzerkonto konfiguriert wurden. Doppelklicken Sie auf einen Benutzernamen um das Fenster zu öffnen, in dem Sie die Kindersicherung für das entsprechende Benutzerkonto konfigurieren können.

Die folgenden Abschnitte in diesem Kapitel beschreiben detailliert die Funktionen der Kindersicherung und wie Sie sie verwenden können.

18.1. Status pro Benutzer einstellen

Um die Kindersicherung für einen bestimmten Benutzer zu konfigurieren doppelklicken Sie den entsprechenden Tab des Benutzers und klicken Sie dann auf den Tab **Status**



Status der Kindersicherung

Um die Kindersicherung für dieses Benutzerkonto zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Aktivieren Sie die Kindersicherung für dieses Benutzerkonto, indem Sie das Kontrollkästchen neben **Kindersicherung** markieren.

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

2. Stellen Sie ein Passwort ein, um Ihre Einstellungen für die Kindersicherung zu schützen. Für weitereInformationen besuchen Sie bitte *„Kindersicherung Einstellungen“* (S. 197).

3. Wählen Sie die Kontrollkästchen die den Kontrollmechanismen entsprechen, die Sie benutzen möchten:

   - **Web-Kontrolle** - um die Web-Navigation gemäß der von Ihnen festgelegten Regeln in dem Bereich Web zu filtern.

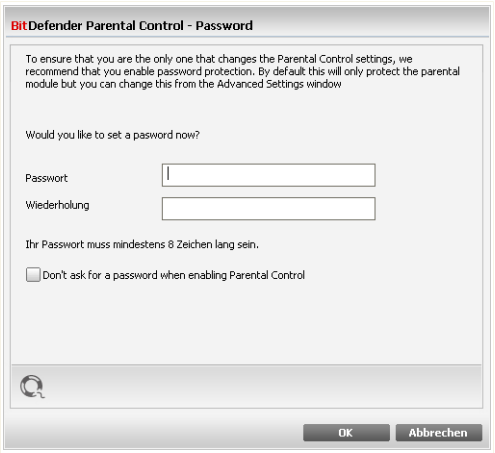
- **Programm-Kontrolle** - blockiert den Zugang zu Programmen, die Sie in dem Abschnitt Programme festgelegt haben.
- **Instant Messaging-Kontrolle** - um den Chat mit IM-Kontakten, entsprechend der von Ihnen im Abschnitt IM-Datenverkehr festgelegten Regeln zu erlauben oder zu verweigern.
- **Webzeitbegrenzung** - um den Zugang zum Internet zeitlich einzugrenzen, wie Sie es im Abschnitt Zeitbegrenzung festgelegt haben.
- **Internetzugriff** - um alle Verbindungen zu Webseiten zu blockieren (nicht nur die in dem Abschnitt Web festgelegten).
- **Stichwort-Filter** - um den Web-, Mail- und Instant Messaging-Zugriff nach den Regeln zu filtern, die Sie im Abschnitt Stichwörter festgelegt haben.
- **Heuristischer Web-Filter** - um den Internetzugang nach eingestellten Regeln zu filtern, die auf dem Alter der Anwender basieren.

4. Um vollständig von den enthaltenen Modulen profitieren zu können müssen die einzelnen Module konfiguriert werden. Um zu lernen wie Sie diese konfigurieren können, beachten Sie bitte die folgenden Inhalte in diesem Kapitel.

18.1.1. Kindersicherung Einstellungen

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

BitDefender wird Sie nach der Einstellung eines Passwortes fragen, wenn Sie die Kindersicherung aktivieren.



BitDefender per Passwort schützen

Um den Passwortschutz einzustellen, befolgen Sie die folgenden Schritte:

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

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

Anmerkung
Dieses Passwort wird nicht die anderen Einstellungen von BitDefender schützen.

Wenn Sie kein Passwort einstellen, und nicht möchten, dass dieses Fenster erneut erscheint, aktivieren Sie **Nicht nach Passwort fragen wenn die Kindersicherung aktiviert wird**.

18.1.2. Konfiguration des Heuristischen Web Filters

Der Heuristische Web Filter analysiert Webseiten und blockiert solche welche einen potenziel unangebrachten Inhalt enthalten.

Stellen Sie eine bestimmte Toleranzstufe ein, um den Internetzugang entsprechend vordefinierten altersbasierenden Regeln zu filtern. Ziehen Sie den Zeiger an der Scala entlang um die Stufe für den gewünschten Schutz einzustellen, den Sie für den Anwender für angemessen halten.

Es stehen 3 Toleranzstufen zur Verfügung:

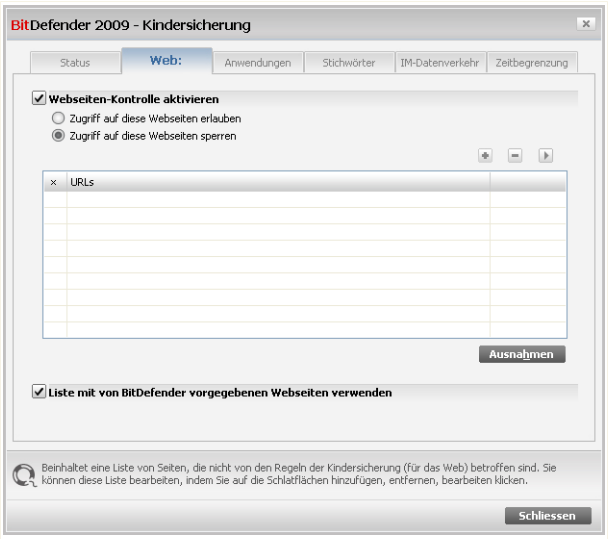
Toleranzeinstellung	Beschreibung
Kind	Bietet eingeschränkten Zugriff auf das Internet, gemäß den Empfehlungen für Anwender unter 14 Jahren. Internet Seiten mit möglicherweise schädlichen Inhalten für Kinder (Porno Seiten, Sex Seiten etc.) werden blockiert.
Jugendlicher	Bietet eingeschränkten Zugriff 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.

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

18.2. Web Kontrolle

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

Um die Web-Kontrolle für einen bestimmten Benutzer festzulegen doppelklicken Sie auf den entsprechenden Benutzer und klicken Sie dann auf den Tab **Web**.



Web Kontrolle

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

Wählen Sie **Zugriff auf diese Webseiten erlauben/Zugriff auf diese Webseiten sperren** um die erlaubte/blockierte Webseiten aufzulisten. Klicken Sie auf **Ausnahmen...** um auf die ergänzende Liste in einem Fenster anzusehen.

Die Maßstäbe müssen manuell eingestezt werden. Wählen Sie **Zugriff auf diese Webseiten erlauben/Zugriff auf diese Webseiten sperren** um Zugriffe zu erlauben oder zu verweigern. Danach, Klicken Sie auf **Einfügen...** um den Konfigurationsassistant zu starten.

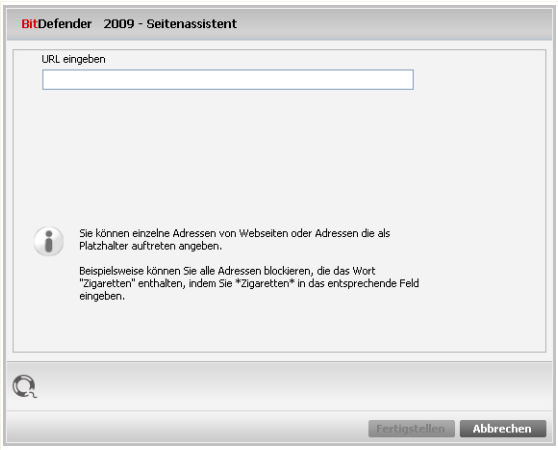
Um eine regel zu löschen, wählen Sie diese aus und klicken Sie **Löschen**. Um eine Regel zu modifizieren, wählen Sie diese aus und klicken Sie **Bearbeiten...** oder Doppelklicken Sie. Um eine Regel zeitlich begrenzt zu deaktivieren, ohne sie zu löschen, löschen die entsprechende Prüfbox.

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

18.2.1. Konfigurationsassistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 – Definieren der Webseiten



Definieren von Webseiten

Geben Sie den Namen der Webseite ein, auf die die Regeln ausgeführt werden sollen. Danach klicken Sie bitte **Beenden**.

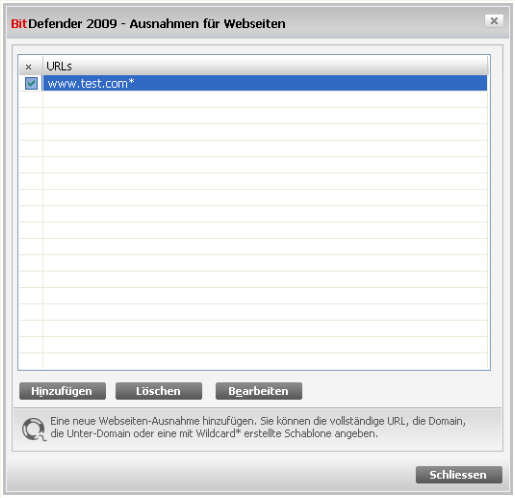
Wichtig
Syntax:

- `*.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;

18.2.2. 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.

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.

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

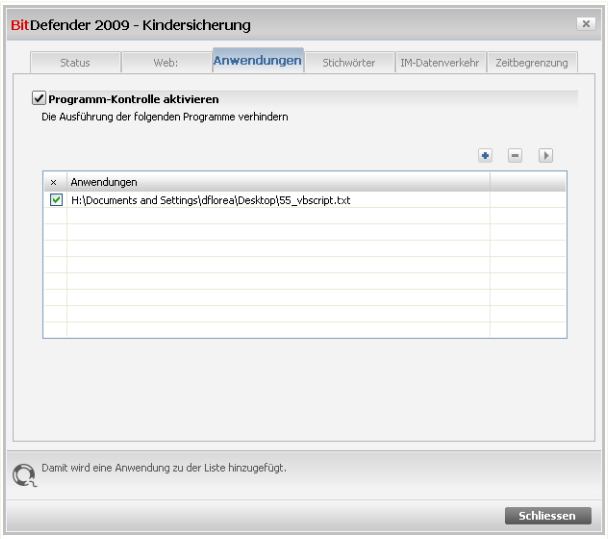
18.2.3. BitDefender Schwarze Liste Internet

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**.

18.3. Programmkontrolle

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 die Programmkontrolle für einen bestimmten Benutzer zu konfigurieren, doppelklicken Sie auf den entsprechenden Benutzer und klicken Sie dann auf den Tab **Anwendungen**.



Programmkontrolle

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.

Um eine regel zu löschen, wählen Sie diese aus und klicken Sie **Löschen**. Um eine Regel zu modifizieren, wählen Sie diese aus und klicken Sie **Bearbeiten...** oder Doppelklicken Sie. Um eine Regel zeitlich begrenzt zu deaktivieren, ohne sie zu löschen, löschen die entsprechende Prüfbox.

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

18.3.1. Konfigurationsassistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 – Auswahl der zu sperrenden Anwendung

Auswahl der zu sperrenden Anwendung

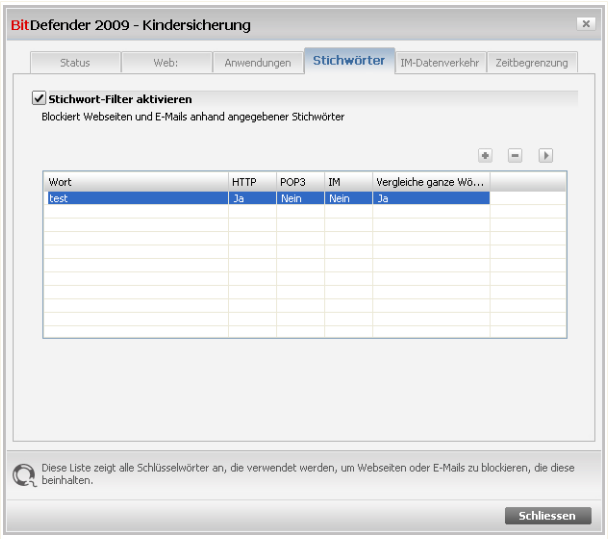
Klicken Sie bitte **Durchsuchen**, und wählen Sie dann die zu sperrende Anwendung. Danach klicken Sie **Beenden**.

18.4. Schlüsselwort-Filter

Mit der Schlüsselwortfilterung können Sie den Zugang zu E-Mail Nachrichten, Webseiten und Sofortnachrichten, die bestimmte Wörter enthalten, blockieren. Mit der Schlüsselwortfilterung können Sie verhindern, dass Ihre Kinder unangemessene Wörter oder Sätze sehen, wenn sie online sind.

Anmerkung
Die Schlüsselwortfilterung für Instant Messaging ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Um die Schlüsselwortfilterung für einen bestimmten Benutzer zu konfigurieren, doppelklicken Sie auf den entsprechenden Benutzer und klicken Sie dann auf den Tab **Schlüsselwörter**.



Schlüsselwort-Filter

Markieren Sie das Kontrollkästchen **Schlüsselwortfilterung aktivieren**, wenn Sie diese Funktion verwenden wollen.

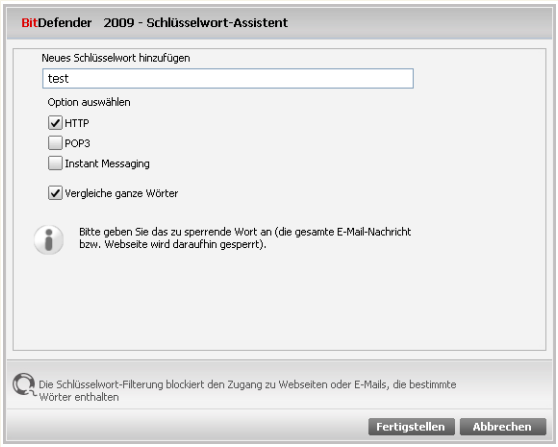
Sie müssen Regeln hinzufügen, um die Schlüsselwörter festzulegen, die blockiert werden sollen. Um eine Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und konfigurieren Sie die Regelparameter in dem Konfigurationsfenster.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Um eine bestehende Regel zu bearbeiten, doppelklicken Sie auf die Regel oder klicken Sie auf die Schaltfläche **Bearbeiten** und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

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

18.4.1. Konfigurationsfenster

Wenn Sie Regeln hinzufügen oder bearbeiten, wird ein Konfigurationsfenster erscheinen.



Passwort 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.

Optionen	Beschreibung
POP3	E-Mail Nachrichten, die das Schlüsselwort enthalten werden blockiert.
HTTP	Internet Seiten, die Schlüsselwörter enthalten, werden geblockt.
Instant Messaging	Sofortnachrichten, die das Schlüsselwort enthalten werden blockiert.

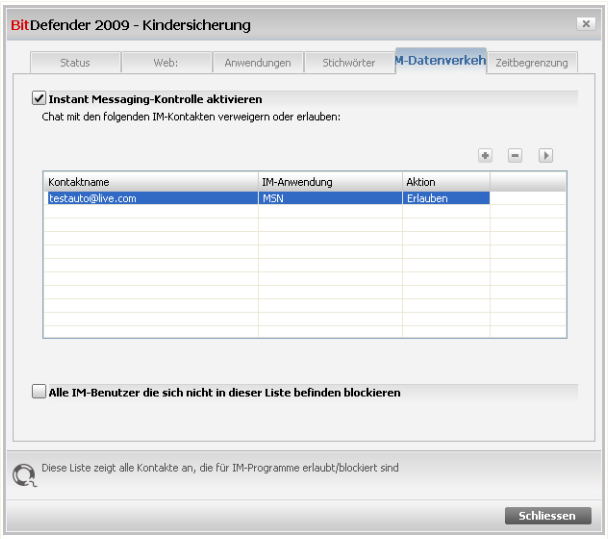
Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

18.5. Instant Messaging (IM) Kontrolle

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

Anmerkung
Die IM-Kontrolle ist nur für Yahoo Messenger und Windows Live (MSN) Messenger verfügbar.

Um die IM-Kontrolle für ein bestimmtes Benutzerkonto zu konfigurieren, doppelklicken Sie auf den entsprechenden Benutzer und klicken Sie dann auf den Tab **IM-Datenverkehr**.



Instant Messenger Kontrollassistent

Markieren Sie das Kontrollkästchen **Instant Messaging Kontrolle aktivieren** wenn Sie diese Kontrollfunktion verwenden möchten.

Sie müssen Regeln hinzufügen, um die IM-Kontakte festzulegen mit denen der Benutzer chatten darf oder nicht. Um eine Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und konfigurieren Sie die Regelparameter in dem Konfigurationsfenster.

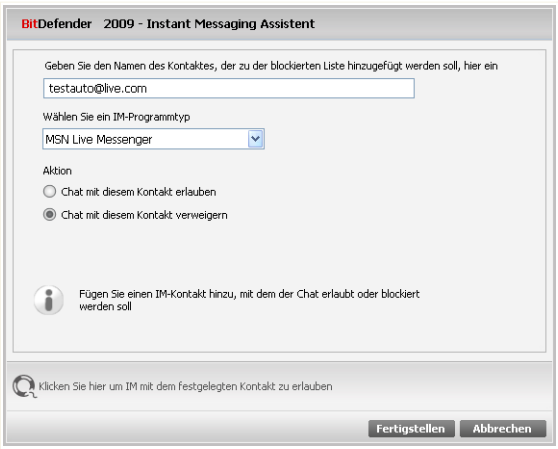
Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Um eine bestehende Regel zu bearbeiten, doppelklicken Sie auf die Regel oder klicken Sie auf die Schaltfläche **Bearbeiten** und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

Wenn Sie alle IM-Kontakte festgelegt haben, mit denen der Benutzer chatten darf, wählen Sie **Alle IM-Benutzer, die sich nicht in der Liste befinden blockieren**. Auf diese Art können nur die IM-Kontakte Sofortnachrichten an den Benutzer senden, denen dies explizit erlaubt wurde.

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

18.5.1. Konfigurationsfenster

Wenn Sie Regeln hinzufügen oder bearbeiten, wird ein Konfigurationsfenster erscheinen.



Fügen Sie einen IM-Kontakt hinzu

Gehen Sie wie folgt vor:

1. Geben Sie den Benutzernamen (ID) des IM-Kontakts ein.
2. Wählen Sie das Chatprogramm das der Kontakt verwendet.
3. Wählen Sie die Aktion der Regel:
   - **Chat mit diesem Kontakt verweigern**
   - **Chat mit diesem Kontakt erlauben**
4. Klicken Sie auf **Beenden** um die Regel hinzuzufügen.

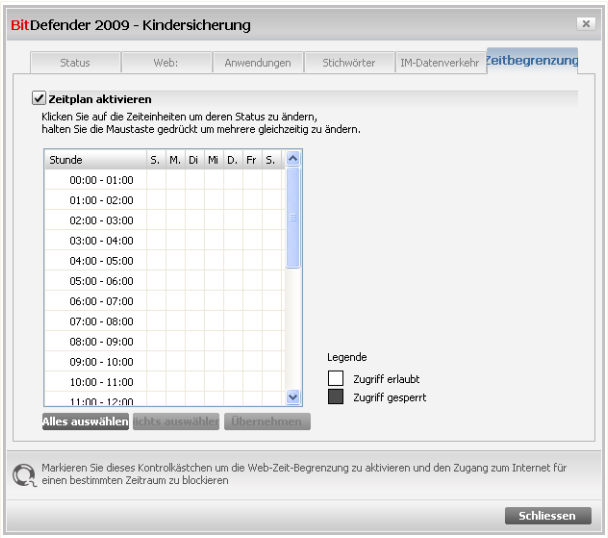
18.6. Zeitplan

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

Anmerkung

BitDefender wird Aktualisierungen jede Stunde unabhängig von der Einstellungen vom **Webzeitbegrenzer** durchführen.

Um die Web-Zeitbegrenzung für einen bestimmten Benutzer zu konfigurieren, doppelklicken Sie auf den entsprechenden Benutzer und klicken Sie dann auf den Tab **Zeitbegrenzung**.



Zeitplan

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.

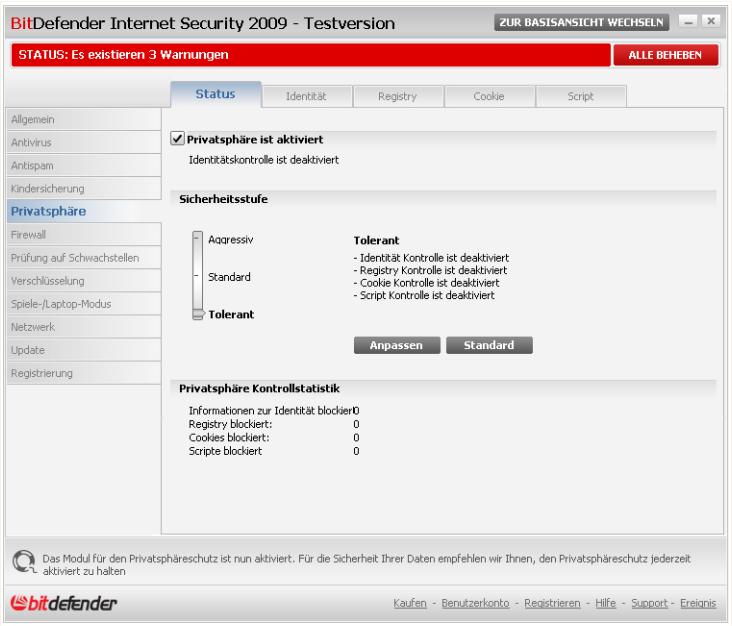
Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

19. Privatsphärekontrolle

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.

19.1. Status der Privatsphärekontrolle:

Um die Privatsphäre zu konfigurieren und Informationen dazu zu erhalten klicken Sie auf **Privatsphäre>Status** in der erweiterten Ansicht.



Status der Privatsphärekontrolle:

Sie können ob die Privatssphäre aktiviert ist oder nicht. Wenn Sie den Status der Privatssphäre ändern möchten, markieren Sie die entsprechende Option, oder lassen Sie sie frei.

Wichtig
Um Datendiebstahl vorzubeugen und private Daten zu schützen, lassen Sie die **Privatsphäre** aktiviert.

Die Privatsphäre schützt Ihren Computer mit diesen wichtigen Kontrollmechanismen:

- Identitätskontrolle - schützt Ihre vertrauenswürdigen Daten indem der gesamte ausgehende HTTP- und SMTP- (Web/E-Mail) sowie der Instant Messaging-Datenverkehr gemäß den Regeln, die Sie in dem Abschnitt Identität festgelegt haben, gefiltert wird.
- Registry-Kontrolle - fragt um Erlaubnis immer wenn ein Programm versucht die Registry zu ändern um beim Windows Neustart ausgeführt zu werden.

- Cookie-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine neue Webseite einen Cookie auf Ihrem Rechner installieren will.
- Skript-Kontrolle- fragt nach Ihrer Einwilligung, sobald eine Webseite versucht, ein Skript oder andere aktive Inhalte zu aktivieren.

Im unteren Bereich können Sie die **Privatsphäre Statistiken** einsehen.

19.1.1. Sicherheitsstufe einstellen

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
Tolerant	**Registrierung** aktiviert.
Standard	**Registry Kontrolle** und **Indentität** sind aktiviert.
Aggressiv	**Registry Kontrolle**, **Identität** und **Script Kontrolle** sind aktiviert.

Sie können die Sicherheitsstufe für den gewünschten Schutz einstellen. Klicken Sie hierfür auf**Stufe anpassen**. Wählen Sie in dem Fenster das sich öffnet die gewünschten Sicherheitsstufen und klicken Sie auf **OK**.

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

19.2. Antispyware/Identitätskontrolle

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.

Die Identitätskontrolle schützt Sie gegen den Diebstahl wichtiger Daten, wenn Sie online sind. Basierend auf Regeln, die von Ihnen erstellt wurden, prüft die Identitätskontrolle den Web-, Mail und IM-Datenverkehr auf spezielle Zeichenfolgen

(zum Beispiel Ihre Kreditkartennummer). Wenn eine Übereinstimmung mit einer Webseite, E-Mail Adresse oder IM-Nachricht gefunden wird, werden diese sofort geblockt.

Sie können Regeln erstellen, um jegliche Information zu schützen, die Sie als persönlich oder vertraulich betrachten, von Ihrer Telefonnummer oder E-Mail-Adresse bis hin zu Ihren Bankkontoangaben. Es wird eine Multiuser Unterstützung zur Verfügung gestellt, wodurch Benutzer die sich in verschiedene Windows-Benutzerkonten einloggen Ihre eigenen Regeln zur Identitätskontrolle konfigurieren können. Die Regeln die Sie erstellen werden nur angewendet und es kann nur auf sie zugegriffen werden, wenn Sie in Ihrem Windows-Benutzerkonto eingeloggt sind.

Warum sollten Sie die Identitätskontrolle verwenden?

- Die Identitätskontrolle kann Keylogger-Spyware effektiv blockieren. Diese schädlichen Anwendungen speichern Ihre eingegebenen Tastenfolgen und senden sie über das Internet zu Hackern. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.

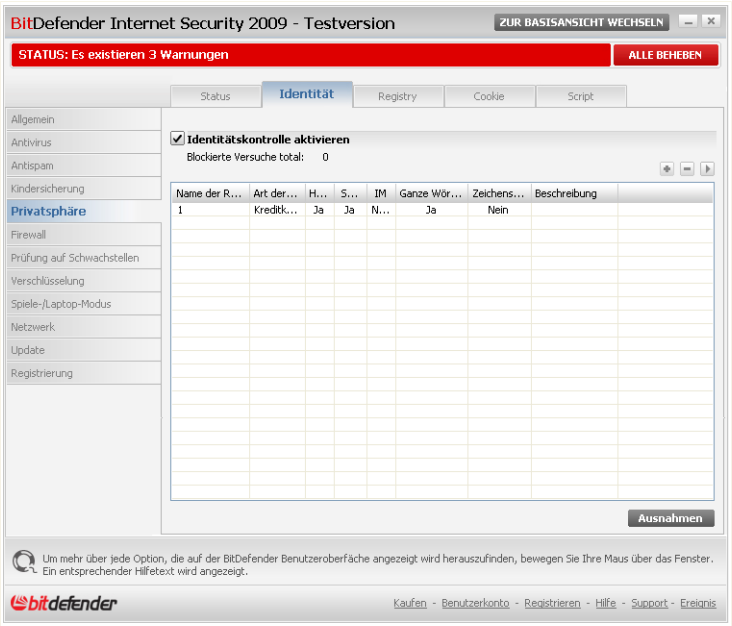
  Auch wenn eine solche Anwendung es schafft die Antivirus-Entdeckung zu umgehen, kann es die gestohlenen Daten nicht über E-Mail, das Internet oder Chatprogramme senden, wenn Sie entsprechende Regeln für die Identitätskontrolle eingestellt haben.

- Die Identitätskontrolle kann Sie vor Phishing schützen (Versuche, persönliche Daten zu stehlen). Die meisten Phishing-Versuche verwenden eine betrügerische E-Mail, um Sie dazu zu bringen persönliche Daten an eine gefälschte Webseite zu senden.

  So können Sie beispielsweise eine E-Mail erhalten, die behauptet von Ihrer Bank zu kommen und Sie dazu auffordert, Ihre Bankangaben dringend zu aktualisieren. In der E-Mail befindet sich ein Link zu einer Webseite, auf der Sie Ihre persönlichen Daten angeben sollen. Auch wenn dies alles echt erscheint, sind sowohl die E-Mail als auch die genannte Webseite Fälschungen. Wenn Sie auf den Link in der Mail klicken und Ihre persönlichen Daten an die Webseite senden, werden Sie diese Informationen an Hacker weiterleiten, die diesen Phishing-Versuch erstellt haben.

  Wenn entsprechende Regeln für die Identitätskontrolle eingestellt sind, können Sie die persönlichen Daten (so wie Ihre Kreditkartennummer) nicht an eine Webseite senden, außer wenn Sie die entsprechende Seite explizit als Ausnahme festgelegt haben.

Um die Identitätskontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Identität** in der erweiterten Ansicht.



Antispyware/Identitätskontrolle

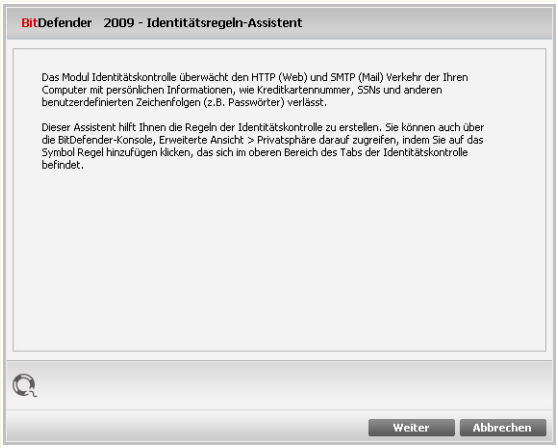
Wenn Sie die Identitätskontrolle verwenden möchten, befolgen Sie folgende Schritte:

1. Markieren Sie das Kontrollkästchen **Identitätskontrolle**.
2. Erstellen Sie Regeln um wichtige Daten zu schützen. Für weitere Informationen lesen Sie bitte *„Erstellen von Privatssphäreregeln“* (S. 216).
3. Erstellen Sie, wenn nötig, spezielle Ausnahmen zu den Regeln, die Sie erstellt haben. Für weitere Informationen lesen Sie bitte *„Definition von Ausnahmen“* (S. 220).

19.2.1. Erstellen von Privatssphäreregeln

Um eine Regel für die Identitätskontrolle zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und befolgen Sie die Schritte des Konfigurationsassistenten.

Schritt 1/4 - Willkommensfenster



Begrüßungsfenster

Klicken Sie auf **Weiter**.

Schritt 2/4 - Typ und Daten der Regel auswählen

Typ und Richtung auswählen

Hier können Sie die Parameter auswählen:

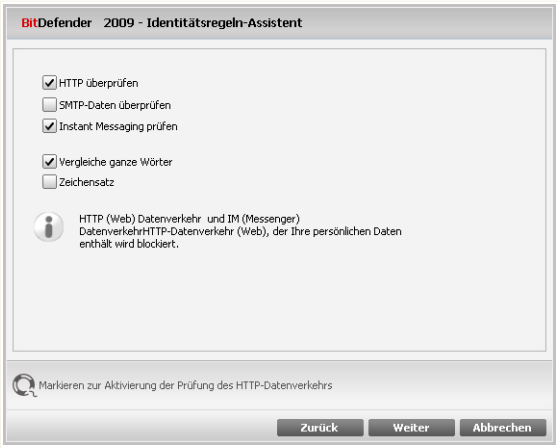
- **Name der Regel** - Geben Sie einen Namen für die Regel in dieses Editierfeld ein.
- **Art der Regel** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- Geben Sie in das Feld **Daten der Regel** die Daten ein, die geschützt werden sollen. Wenn Sie zum Beispiel Ihre Kreditkartennummer schützen wollen, geben Sie sie zum Teil oder ganz ein.

> ***Anmerkung***
> Wenn Sie weniger als drei Zeichen angeben werden Sie aufgefordert die Daten zu überprüfen. Wir empfehlen die Eingabe von mindestens drei Zeichen um ein versehentliches blockieren von Nachrichten oder Webseiten zu verhindern.

Alle 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 3/4 - Datenverkehr auswählen



Datenverkehr auswählen

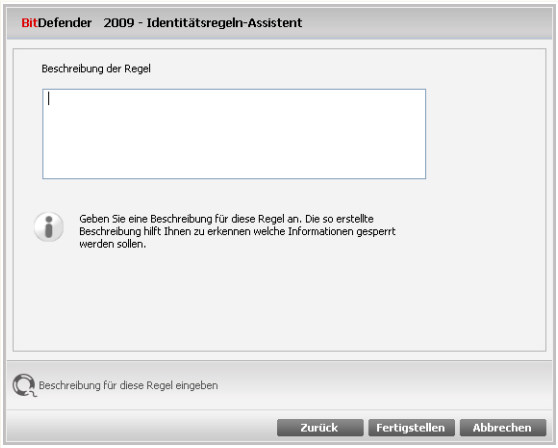
Bitte wählen sie den Datenverkehrstyp welchen BitDefender prüfen soll. Die folgenden Optionen sind verfügbar:

- **HTTP-Daten überprüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **SMTP-Daten überprüfen** - prüft alle ausgehenden E-Mail-Nachrichten.
- **Instant Messaging überprüfen** - prüft den Instant Messaging Datenverkehr und blockiert ausgehende Nachrichten, die die Regeldaten enthalten.

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

Klicken Sie auf **Weiter**.

Schritt 4/4 - Regel beschreiben



Beschreibung der Regel

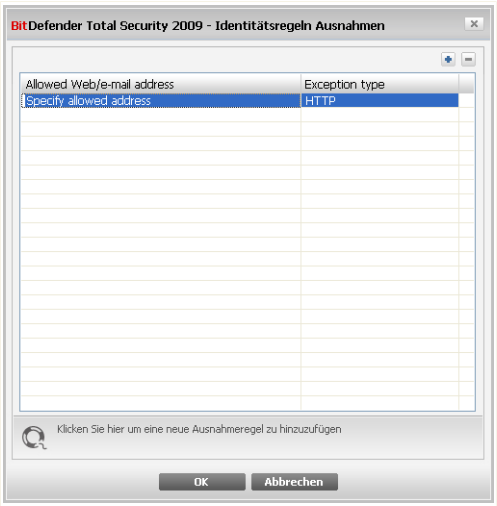
Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein. Da die blockierten Daten (Zeichenfolgen) nicht als ein vollständiger Text angezeigt werden wenn auf die Regel zugegriffen wird, sollte Ihnen die Beschreibung dabei helfen sie einfach zu identifizieren.

Klicken Sie auf **Fertigstellen**. Die Regel wird in der Tabelle erscheinen.

19.2.2. Definition von Ausnahmen

In manchen Fällen wird es nötig sein Ausnahmen für bestimmte Identitätsregeln zu erstellen. In manchen Fällen ist es nötig Ausnahmen für bestimmte Regeln zu erstellen. Zum Beispiel haben Sie eine Regeln angelegt welche verhindert das Ihre Kreditkartennummer per HTTP übertragen wird. Nun möchten Sie sich aber z.B. Schuhe auf einer bestimmten Webseite per Kreditkarte kaufen. In diesem Fall müssten Sie eine Ausnahme definieren um dies möglich zu machen.

Um eine solche Ausnahme zu erstellen klicken Sie auf die **Ausnahmen**-Schaltfläche.



Ausnahmen

Um eine Ausnahme zu erstellen befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Hinzufügen** um einen neuen Eintrag in der Tabelle zu erstellen.
2. Doppelklicken Sie auf **Erlaubte Adresse angeben** und geben Sie die Webseite, E-Mail-Adresse oder den IM-Kontakt an, die/den Sie als Ausnahme hinzufügen möchten.
3. Doppelklicken Sie dann auf **Typ wählen** und wählen Sie den gewünschten Eintrag aus dem Menü aus.
   - Wenn Sie eine Webseite eingegeben haben dann wählen Sie **HTTP**.
   - Wenn Sie eine E-Mail Adresse eingegeben haben dann wählen Sie **SMTP**.
   - Wenn Sie einen IM-Kontakt eingegeben haben dann wählen Sie **IM**.

Um eine Ausnahme aus der Liste zu entfernen markieren Sie diese und klicken Sie dann auf **Entfernen**.

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

19.2.3. Regeln bearbeiten

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

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

Regel editieren

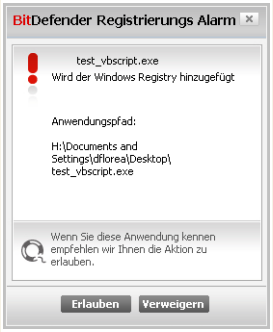
Hier können Sie Namen, Beschreibungen und Parameter der Regel ändern. (Typ, Daten und Datenverkehr). Klicken Sie **OK** um die Änderungen zu speichern.

19.3. Registrierung prüfen

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.



Registrierungsalarm

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

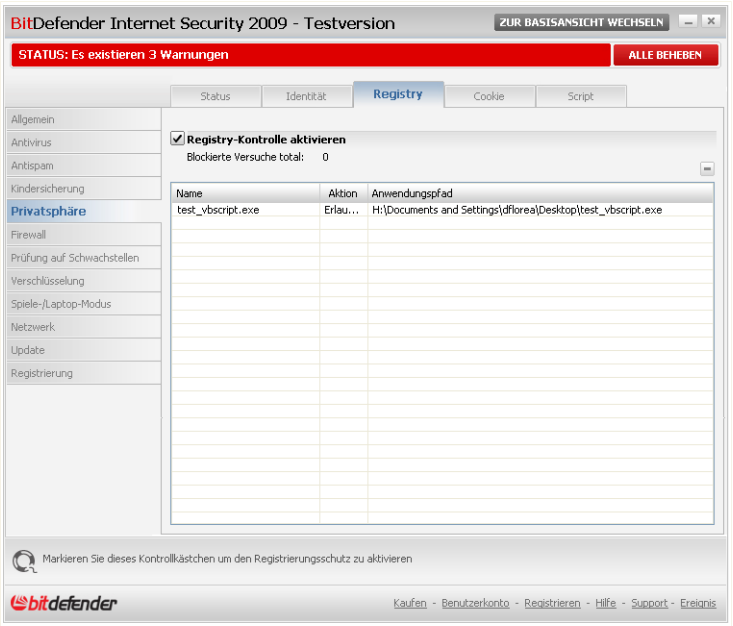
Wenn Sie das Programm nicht kennen und es Ihnen verdächtig erscheint, klicken Sie auf **Blockieren** um es davon abzuhalten die Windows-Registry zu verändern. Klicken Sie andererseits auf **Erlauben** um die Veränderung zu erlauben.

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

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.

Um die Registry-Kontrolle zu konfigurieren klicken auf **Privatssphäre>Registry** in der erweiterten Ansicht.



Registrierung prüfen

Sie können eine Liste der Regeln in der Aufstellung ansehen.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

19.4. Cookie-Kontrolle

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

Generell erleichtern Cookies das tägliche 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.

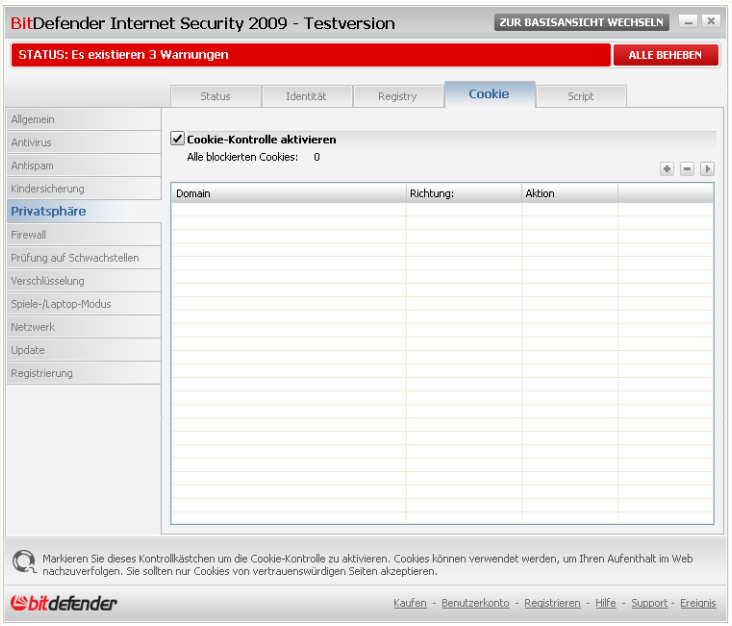
Wählen Sie **Diese Antwort merken** und klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in der Regelliste aufgenommen. Sie werden dann nicht wieder informiert, wenn Sie das nächste Mal mit derselben Seite in Verbindung treten.

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.

Um die Cookie-Kontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Cookie** in der erweiterten Ansicht.



Cookie-Kontrolle

Sie können eine Liste der Regeln in der Aufstellung ansehen.

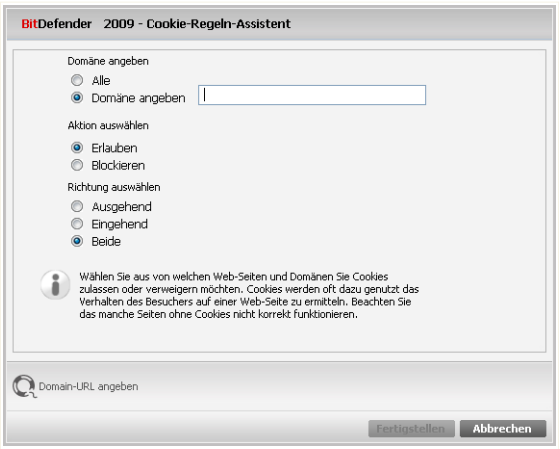
Wichtig
Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Um die Regelparameter zu ändern, doppelklicken Sie auf die Regel und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

Um eine Regel manuell hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

19.4.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



Adresse, Aktion und Richtung 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.

Typ	Beschreibung
Eingehend	Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden.
Beide	Die Regeln finden in beide Richtungen Anwendung.

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

Klicken Sie auf **Fertigstellen**.

19.5. 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.

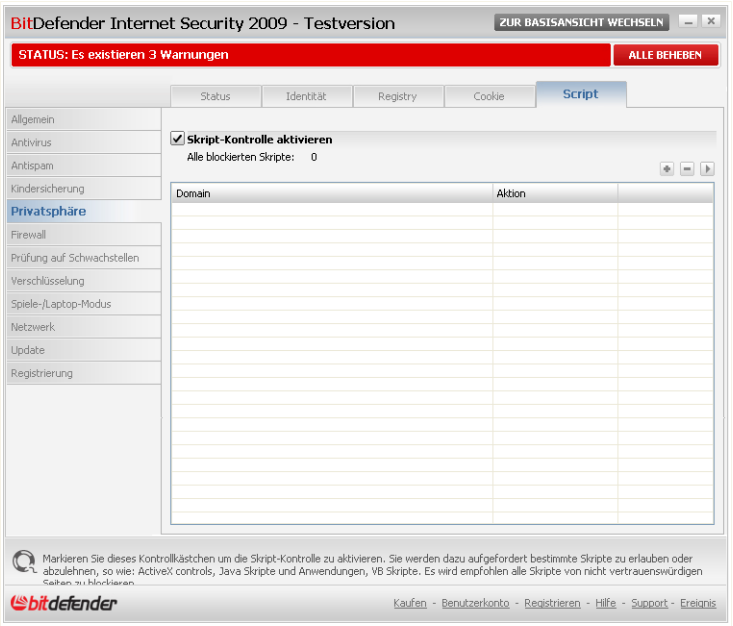
Mit der **Skript Kontrolle** entscheiden Sie, welche Webseiten Sie als zuverlässig erachten und welche nicht. BitDefender wird immer Ihr Einverständnis abfragen, wenn eine Webseite ein Skript oder einen anderen aktiven Inhalt aktivieren will:

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.

Um die Skript-Kontrolle zu konfigurieren klicken Sie auf **Privatssphäre>Skript** in der erweiterten Ansicht.



Skript-Kontrolle

Sie können eine Liste der Regeln in der Aufstellung ansehen.

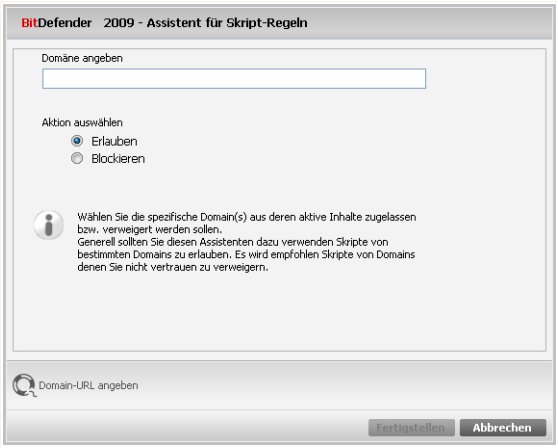
Wichtig
Die Regeln sind nach Prioritäten gelistet. Dies bedeutet die erste Regel besitzt die höchste Priorität in der Liste. Per Drag & Drop können die einzelnen Regeln gemäß der gewünschten Priorität verschoben werden.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Um die Regelparameter zu ändern, doppelklicken Sie auf die Regel und führen Sie die gewünschten Änderungen in dem Konfigurationsfenster durch.

Um eine Regel manuell zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.

19.5.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



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**.

20. Firewall

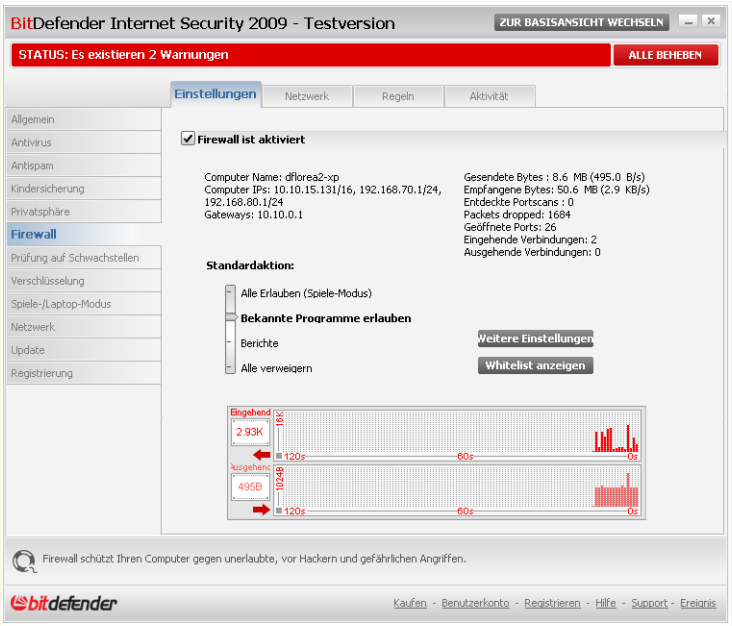
Die Firewall schützt Ihren Computer vor unberechtigten eigehenden und ausgehenden Zugriffen. Sie überwacht Ihre Verbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.

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

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.

20.1. Einstellungen

Um die Firewall zu konfigurieren klicken Sie auf **Firewall>Einstellungen** in der erweiterten Ansicht.



Firewall-Einstellungen

Sie können sehen ob ob die BitDefender Firewall aktiviert oder deaktiviert ist. Wenn Sie den Status der Firewall ändern möchten, markieren Sie das entsprechende Kontrollkästchen oder lassen Sie es frei.

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

Es gibt zwei verschiedene Informationskategorien:

- **Netzwerkkonfiguration.** Sie können den Namen Ihres Computers, seine IP-Adresse und die Standard-Schnittstelle sehen. Wenn Sie mehr als einen Netzwerkadapter haben (dies bedeutet, dass Sie mit mehreren Netzwerken verbunden sind), so sehen Sie die für jeden Adapter konfigurierte IP-Adresse und Schnittstelle.
- **Statistik.** Sie können verschiedene Statistiken zu der Aktivität der Firewall sehen:

- Anzahl der gesendeten Bytes.
- Anzahl der empfangenen Bytes.
- Anzahl der Portscans, die von BitDefender entdeckt und blockiert wurden. Portprüfungen werden häufig von Hackern verwendet, um offene Ports auf Ihrem Computer zu finden, um diese dann zu verwenden.
- Anzahl der abgenommenen Datenpakete.
- Anzahl der offenen Ports.
- Anzahl der aktiven Verbindungen mit eingehendem Datenverkehr.
- Anzahl der aktiven Verbindungen mit ausgehendem Datenverkehr.

Um die aktiven Verbindungen und die offenen Ports zu sehen, klicken Sie auf den Tab Aktivität.

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**.

20.1.1. Standardaktion einstellen

Standardmäßig erlaubt BitDefender automatisch allen Programmen der Whitelist eine Verbindung zum Netzwerk und dem Internet herzustellen. Für alle anderen Programme fordert Sie BitDefender über ein Benachrichtigungsfenster dazu auf, die durchzuführende Aktion festzulegen. Die von Ihnen festgelgte Aktion wird dann immer durchgeführt, wenn das entsprechende Programm versucht auf das Netzwerk/Internet zuzugreifen.

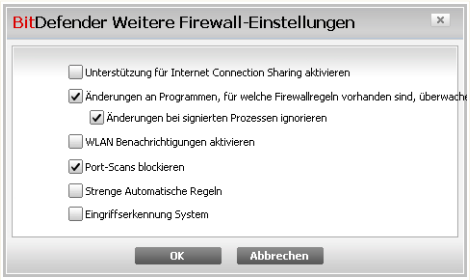
Ziehen Sie den Zeiger an der Skala entlang um die Standardaktion einzustellen, die durchgeführt werden soll, wenn das Programm versucht auf das Netzwerk/Internet zuzugreifen. Folgende Standardaktionen stehen zur Verfügung:

Standardaktion	Beschreibung
Alle erlauben	Verwendet die momentanen Regeln und erlaubt alle Anfragen welche nicht den Regeln entsprechen ohne Nachfrage. Diese Einstellung kann für Netzwerkadministratoren und Gamer hilfreich sein.

Standardaktion	Beschreibung
Bekannte Programme erlauben	Wendet die aktuellen Regeln an und erlaubt, ohne vorher zu fragen, alle ausgehenden Verbindungsversuche von Programmen, die in der Whitelist vorhanden sind. Bei anderen Anwendungen werden Sie um Erlaubnis gefragt. 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.
Berichte	Verwendet die momentanen Regeln und frägt Sie bei alle Anfragen welche nicht den Regeln entsprechen.
Alle verweigern	Wendet die aktuellen Regeln an und verweigert alle Verbindungsversuche, wenn diese nicht mit den aktuellen Regeln übereinstimmen.

20.1.2. Weitere Einstellungen der Firewall konfigurieren

Sie können auf **Erweitert** klicken, um die erweiterten Firewall-Einstellungen zu konfigurieren.



Eweiterte Firewall Einstellungen

Die folgenden Optionen sind verfügbar:

- **Unterstützung für Internet Connection Sharing aktivieren** - Erlaubt die Unterstützung von Internet Connection Sharing (ICS).

Anmerkung
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 es Anwendern in lokalen Netzwerken von ihrem Computer aus auf das Internet zuzugreifen. Dies ist sinnvoll wenn Sie eine spezielle/bestimmte Internet Verbindung(z.B. Drahtlose Anbindung) nutzen und diese mit anderen Mitgliedern im Netzwerk teilen wollen.

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).

- **Änderungen an Programmen, für welche Firewallregeln vorhanden sind, prüfen** - Prüft ob das Programm für welches eine Regel erstellt wurde verändert wurde und frägt gegebenenfalls ab ob der Zugriff erlaubt werden soll.

  Normalerweise werden Anwendungen durch Updates verändert, es kann aber auch sein das eine Anwendung durch einen Schädling verändert wird um Ihren Computer zu infizieren.

  Anmerkung
  Wir empfehlen Ihnen die Option aktiviert zu lassen und nur Anwendungen Zugriff zu gewähren bei welchen Sie erwarten das diese Zugriff zum Internet benötigen.

  Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad. Signierte Anwendungen haben einen höheren Sicherheitsfaktor. Sie können diesen Anwendungen den Zugriff erlauben auch wenn diese verändert wurden. Aktivieren Sie hierzu die Option **Änderungen bei signierten Prozessen ignorieren**.

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

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

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

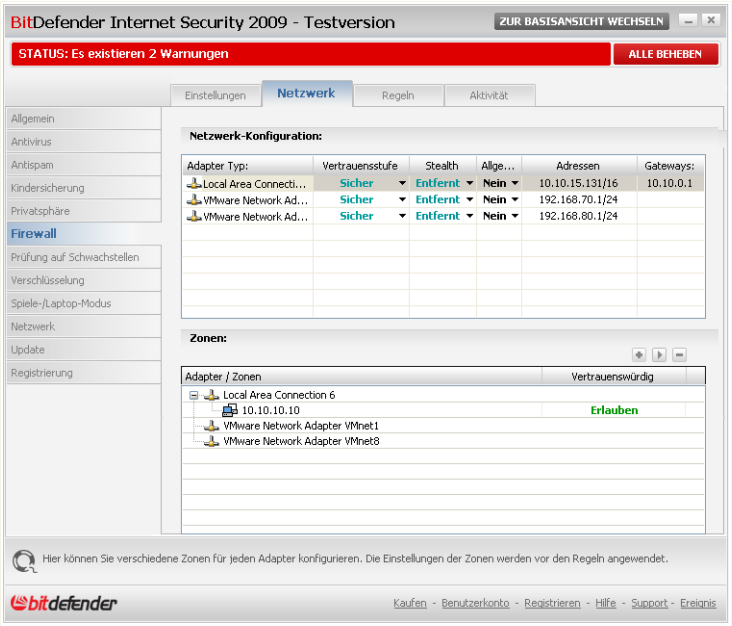
- **Genaue automatische Regeln** -erstellt genaue Regeln bezüglich der Verwendung des Benachrichtigungsfensters der Firewall. Wenn diese Option ausgewählt ist, wird BitDefender Sie dazu auffordern für jede Anwendung, die versucht auf das

Netzwerk oder das Internet zuzugreifen, eine Aktion durchzuführen und Regeln zu erstellen.

- **Intrusion detection system (IDS)** - aktiviert die heuristische Überwachung von Anwendungen, die versuchen auf das Netzwerk oder das Internet zuzugreifen.

20.2. Netzwerk

Um die Firewall-Einstellungen zu konfigurieren klicken Sie auf **Firewall>Netzwerk** in der erweiterten Ansicht.



Netzwerk

Die Spalten in der Tabelle **Netzwerkkonfiguration** bieten Ihnen detaillierte Informationen über das Netzwerk mit dem Sie verbunden sind:

- **Adapter** - Der Netzwerkadapter, den Ihr Computer verwendet, um eine Verbindung mit dem Netzwerk oder dem Internet herzustellen.

- **Typ** - Die Vertrauensstufe, die dem Netzwerkadapter zugewiesen ist. Entsprechend der Netzwerkadapterkonfiguration wird BitDefender dem Adapter automatisch eine Vertauensstufe zuweisen oder Sie nach weiteren Angaben fragen.
- **Verdeckt** - Ob Sie von anderen Computern entdeckt werden können.
- **Generisch** - Ob für diese Verbindung generische Regeln angewendet werden.
- **Adressen** - die für den Adapter konfigurierte IP-Adresse.
- **Schnittstellen** - Die IP-Adresse die Ihr Computer verwendet um eine Verbindung mit dem Internet herzustellen.

20.2.1. Vertrauensstufe ändern

BitDefender weist jedem Netzwerkadapter eine Vertrauensstufe zu. Die Vertrauensstufe, die einem Adapter zugewiesen ist zeigt an, wie vertrauenswürdig das entsprechende Netzwerk ist.

Basierend auf der Vertrauensstufe werden verschiedene Reglen für den Adapter erstellt, bezüglich des Umgangs von BitDefender und des Systems mit dem Zugang zum Netzwerk oder Internet.

Sie können die für jeden Adapter konfigurierte Vertrauensstufe in der Tabelle **Netzwerkkonfiguration** in der Spalte **Typ** sehen. Um die Vertrauensstufe zu ändern, klicken Sie auf den Pfeil der Spalte **Typ** und wählen Sie die gewünschte Stufe.

Vertrauensstufe	*Beschreibung*
Vollkommen vertrauenswürdig	Deaktiviert die Firewall für den entsprechenden Adapter.
Lokal vertrauenswürdig	Erlaubt den Datenverkehr zwischen Ihrem Computer und den Computern im lokalen Netzwerk.
Sicher	Erlaubt das gemeinsame Verwenden von Ressourcen mit Computern im lokalen Netzwerk. Diese Stufe ist für lokale Netzwerke (im Haushalt oder Büro) automatisch eingestellt.
Unsicher	Netzwerk- oder Internet-Computer können keine Verbindung mit Ihrem Computer herstellen. Diese Stufe ist für öffentliche Netzwerke (wenn Sie eine IP-Adresse von einem Internet Service Provider erhalten haben) automatisch eingestellt.
Lokal blockieren	Blockiert jeglichen Datenverkehr zwischen Ihrem Computer und Computern im lokalen Netzwerk, während der

Vertrauensstufe	Beschreibung
	Internetzugang bestehen bleibt. Diese Vertrauensstufe ist automatisch für unsichere (offene) WLAN-Netzwerke eingestellt.
Blockiert	Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.

20.2.2. Den Stealth-Modus konfigurieren

Der Stealth-Modus macht Ihren Computer unsichtbar für schädliche Software und Hacker im Netzwerk oder Internet. Um den Stealth-Modus zu konfigurieren, klicken Sie auf den Pfeil ▾ in der Spalte **Verdeckt** und wählen Sie die gewünschte Option.

Stealth-Option	Beschreibung
Einschalten	Stealth-Modus ist aktiviert. Ihr Computer ist weder im lokalen Netzwerk noch im Internet sichtbar.
Ausschalten	Stealth-Modus ist deaktiviert. Jeder Benutzer im lokalen Netzwerk oder im Internet kann Ihren Computer entdecken.
Klicken Sie auf **Remote**.	Ihr Computer kann nicht im Internet entdeckt werden. Benutzer im lokalen Netzwerk können Ihren Computer entdecken

20.2.3. Generische Einstellungen vornehmen

Wenn sich die IP-Adresse eines Netzwerkadapters geändert hat, verändert BitDefender die Vertrauensstufe entsprechend. Wenn Sie die selbe Vertrauensstufe beibehalten möchten, klicken Sie auf den Pfeil ▾ in der Spalte **Generisch** und wählen Sie **Ja**.

20.2.4. Netzwerk-Zonen

Sie können erlaubte oder blockierte Computer für einen bestimmten Adpater hinzufügen.

Ein vertrauenswürdiger Bereich ist ein Computer, dem Sie vollständig vertrauen. Zwischen Ihrem Computer und den Computern, denen Sie vertrauen, ist jeglicher Datenaustausch erlaubt. Um Ressourcen mit speziellen Computern in ungesicherten WLAN-Netzwerken zu teilen, fügen Sie sie als erlaubte Computer hinzu.

Ein blockierter Bereich ist ein Computer, mit dem Ihr Computer in keiner Weise kommunizieren soll.

Die Tabelle **Bereiche** zeigt die aktuellen Netzwerkbereiche für jeden Adampter an.

Um einen Bereich hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.

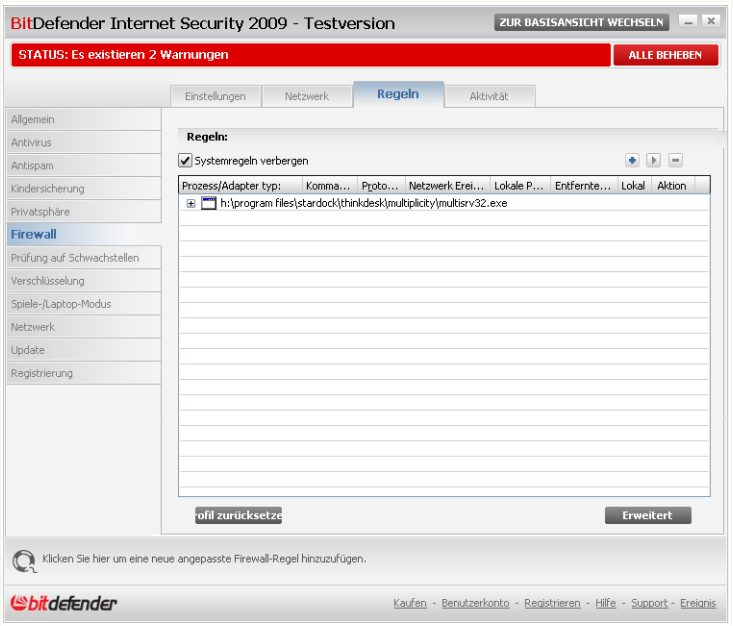
Bereich hinzufügen

Gehen Sie wie folgt vor:

1. Wählen Sie die IP-Adresse des Computers der hinzugefügt werden soll.
2. Wählen Sie eine Aktion:
   - **Erlauben** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird erlaubt.
   - **Verweigern** - jeglicher Datenverkehr zwischen Ihrem Computer und dem ausgewählten Computer wird blockiert.
3. Klicken Sie auf **OK**.

20.3. Regeln

Um die Firewall Regeln, die den Netzwerk- und Internetzugriff von Programmen kontrollieren zu konfigurieren, klicken Sie auf **Firewall>Regeln** in der erweiterten Ansicht.



Firewall-Regeln

Sie können die Programme (Prozesse) sehen, für die die Firewall-Regel erstellt wurde. Lassen Sie das Kontrollkästchen **Systemregeln verbergen** frei, wenn Sie ebenfalls die Regeln bezüglich des Systems oder von BitDefender Prozessen zu sehen.

Um die Regeln zu sehen, die für eine bestimmte Anwendung erstellt wurden, klicken Sie auf das + Kästchen neben der entsprechenden Anwendung. Sie können detaillierte Informationen für jede Regel sehen, so wie sie in den Spalten der Tabelle dargestellt sind:

- **Prozess/Adapter-Typen** - der Prozess und die Netzwerkadaptertypen für die die Regel angewendet wird. Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern. Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).

- **Befehlszeile** - der Befehl in der Windows Befehlszeile der verwendet wird um den Prozess zu starten (**cmd**).
- **Protokoll** - das IP-Protokoll für das die Regel angewendet wird. Sie werden eines der Folgenden sehen:

Protokoll:	*Beschreibung*
Alle	Beinhaltet alle IP-Protokolle.
TCP	Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle am Datenaustausch beteiligten Computer kennen diese Vereinbarungen und befolgen sie. Es ist damit ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Computernetzwerken. Es ist Teil der TCP/IP-Protokollfamilie. Entwickelt wurde TCP von Robert E. Kahn und Vinton G. Cerf. Ihre Forschungsarbeit, die sie im Jahre 1973 begannen, dauerte mehrere Jahre. Die erste Standardisierung von TCP erfolgte deshalb erst im Jahre 1981 als RFC 793. TCP stellt einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung (Sockets) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Referenzmodells angesiedelt.
UDP	User Datagram Protocol (UDP) ist ein minimales, verbindungsloses Netzprotokoll. Es gehört zur Transportschicht der TCP/IP-Protokollfamilie und ist im Gegensatz zu TCP nicht auf Zuverlässigkeit ausgelegt. UDP erfüllt im Wesentlichen den Zweck, die durch die IP-Schicht hergestellte Endsystemverbindung um eine Anwendungsschnittstelle (Ports) zu erweitern. Die Qualität der darunter liegenden Dienste, insbesondere die Zuverlässigkeit der Übertragung, erhöht UDP hingegen nicht.
Eine Nummer	Stellt ein besonderes IP-Protokoll dar (anders als TCP und UDP). Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter www.iana.org/assignments/protocol-numbers.

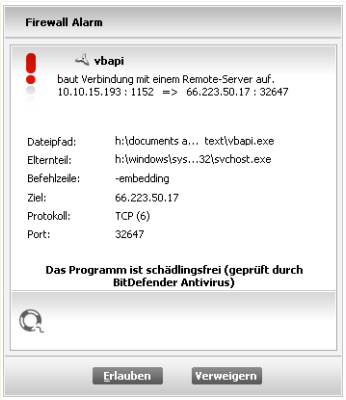
- **Netzwerkereignisse** - die Netzwerkereignisse für die die Regel angewendet wird. Folgende Ereignisse können auftreten:

Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen. Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Überwachen	Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Lokale Ports** - die Ports auf Ihrem Computer, für die die Regel angewendet wird.
- **Remote-Ports** - die Ports auf den Remote-Computern, für die die Regel angewendet wird.
- **Lokal** - ob die Regel nur für Computer im lokalen Netzwerk angewendet wird.
- **Aktion** - ob der Anwendung unter den festgelegten Umständen der Zugriff auf das Netzwerk/Internet erlaubt oder verweigert wird.

20.3.1. Regeln automatisch hinzufügen

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



Firewall Alarm

Sie können folgendes sehen: Die Anwendung, die versucht, auf das Internet, den Pfad zur Anwendungsdatei, dem Bestimmungsort, das Protokoll verwendet und Port , auf dem die Anwendung versucht in Verbindung zu stehen.

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

Bassierend auf Ihrer Wahl wird eine Regel erstellt. Das nächste Mal wenn die Anwendung versucht eine Verbindung herzustellen wird die Regeln direkt angewand.

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

20.3.2. Regeln löschen

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche. Sie können eine oder auch mehrere Regeln auswählen und löschen.

Wenn Sie alle Regeln die für eine bestimmte Anwendung erstellt wurden löschen möchten, wählen Sie die Anwendung aus der Liste und klicken Sie auf die **Regel löschen**-Schaltfläche.

20.3.3. Regeln erstellen und bearbeiten

Durch das Konfigurieren der Regelparameter im Konfigurationsfenster können neue Regeln erstellt und bestehende Regeln bearbeitet werden.

Regeln erstellen. Um eine Regel manuell zu erstellen, befolgen Sie folgende Schritte:

1. Klicken Sie auf die **Regel hinzufügen** -Schaltfläche. Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.

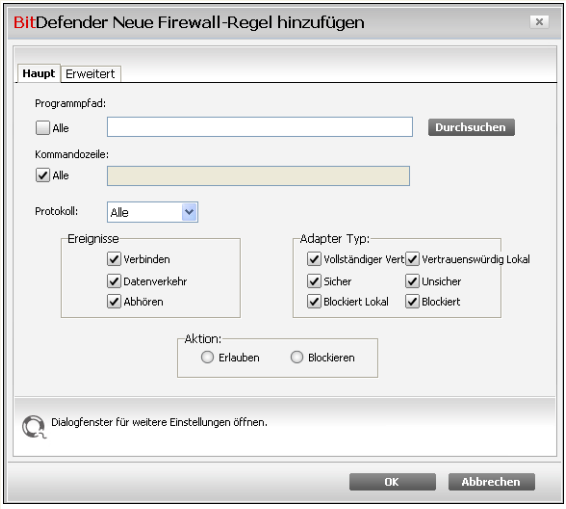
3. Klicken Sie auf **OK** um die neue Regel hinzuzufügen.

Regeln bearbeiten. Um eine bestehende Regel zu bearbeiten, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Regel bearbeiten** oder doppelklicken Sie auf die Regel. Das Konfigurationsfenster wird erscheinen.
2. Knofigurieren Sie die wichtigsten und erweiterten Parameter wie benötigt.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Allgemeine Parameter konfigurieren

Der Tab **Allgemein** des Konfigurationsfensters bietet Ihnen die Möglichkeit die allgemeinen Regelparameter zu verwalten.



Allgemeine Parameter

Folgende Parameter können konfiguriert werden:

- **Programmpfad.** Klicken Sie auf **Durchsuchen** und wählen Sie das Programm für das die Regel angewendet wird. Wenn Sie möchten, dass die Regel für alle Programme angewendet wird, wählen Sie **Alle**.

- **Befehlszeile.** Wenn Sie möchten, dass die Regel nur angewendet wird, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Befehlszeile von Windows geöffnet wird, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie den entsprechenden Befehl in das Editierfeld ein.
- **Protokoll:** Wählen Sie aus dem Menu das IP-Protokoll für das die Regel angewendet wird.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für ein bestimmtes Protokoll angewendet wird, wählen Sie **Andere**. Ein Editierfeld wird erscheinen. Geben Sie die dem Protokoll, das gefiltert werden soll, zugewiesene Nummer in das Editierfeld ein.

Anmerkung

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

- **Ereignisanzeige.** Wählen Sie je nach ausgewähltem Protokoll die Netzwerkereignisse, für die die Regel angewendet werden soll. Folgende Ereignisse können auftreten:

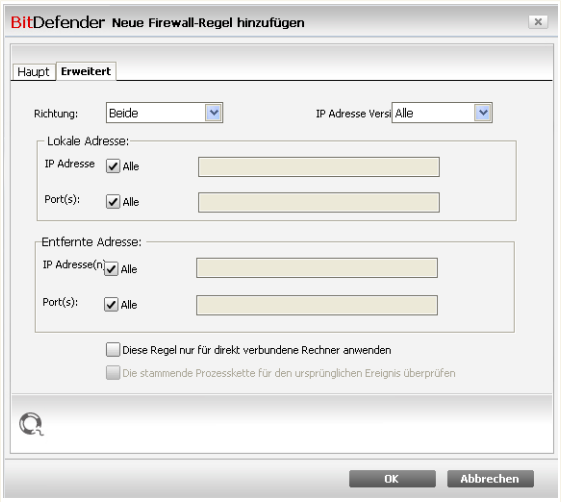
Ereignis	Beschreibung
Verbinden	Vorausgehender Austausch von Standardnachrichten, die von Verbindungsprotokollen (wie TCP) verwendet werden, um eine Verbindung herzustellen. Mit Verbindungsprotokollen entsteht ein Datenverkehr zwischen zwei Computern nur nachdem eine Verbindung hergestellt wurde.
Datenverkehr	Datenfluss zwischen zwei Computern.
Überwachen	Status in dem eine Anwendung das Netzwerk überwacht, das eine Verbindung herstellen oder Informationen über eine Peer-Anwendung erhalten möchte.

- **Vertrauensstufe.** Wählen Sie die Vertrauensstufen, für die die Regel angewendet wird.
- **Aktion.** Folgende Aktionen sind wählbar:

Aktion	Beschreibung
Erlauben	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

Erweiterte Parameter konfigurieren

Der Tab **Erweitert** des Konfigurationsfensters gibt Ihnen die Möglichkeit erweiterte Regelparameter zu konfigurieren.



Erweiterte Parameter

Folgende erweiterte Parameter können konfiguriert werden:

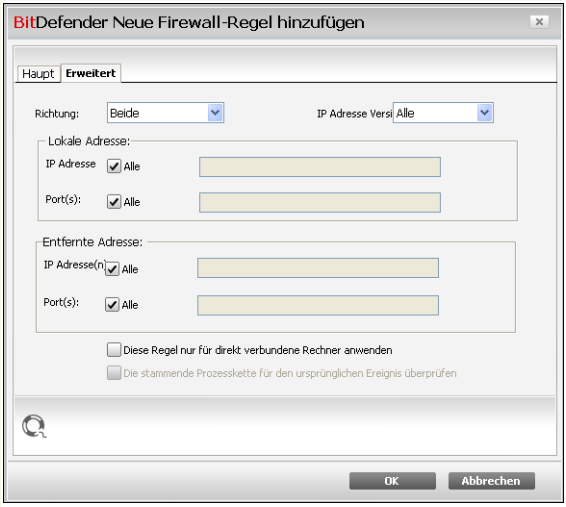
- **Richtung.** Wählen Sie aus dem Menu die Richtung des Datenverkehrs, für den die Regel angewendet wird.

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

- **IP-Version.** Wählen Sie aus dem Menu die IP-Version (IPv4, IPv6 oder andere), für die die Regel angewendet werden soll.
- **Lokale Adresse.** Bestimmen Sie die lokale IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - Wenn Sie mehr als einen Netzwerkadapter haben, können Sie das Kontrollkästchen **Alle** freilassen und eine bestimmte IP-Addresse eingeben.
  - Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Entfernte Adresse.** Bestimmen Sie die Remote-IP-Adresse und den Port, für die die Regel angewendet werden soll, wie folgt:
  - Um den Datenverkehr zwischen Ihrem Computer und einem bestimmten Computer zu filtern, lassen Sie das Kontrollkästchen **Alle** frei und geben Sie dessen IP-Adresse an.
  - Falls Sie TCP oder UDP als Protokoll ausgewählt haben, können Sie spezielle Ports in der Bandbreite von 0 und 65535 auswählen. Wenn Sie die definierten Regeln für alle Ports auswählen möchten, wählen Sie bitte **Alle**.
- **Diese Regel nur für direkt verbundene Computer anwenden.** Wählen Sie diese Option, wenn Sie möchten dass diese Regel nur für den lokalen Datenverkehr angewendet werden soll.
- **Den Ablauf überprüfen um das ursprüngliche Ereignis festzustellen.** Sie können diesen Parameter nur verändern, wenn Sie **Genaue automatische Regeln** ausgewählt haben (öffnen Sie den Tab Einstellungen und klicken Sie auf **Erweiterte Einstellungen**). Genaue Regeln bedeuten, dass BitDefender Sie auffordert eine Aktion durchzuführen, wenn eine Anwendung versucht eine Verbindung mit dem Netzwerk/Internet herzustellen, wenn der vorangegangene Prozess ein anderer war.

20.3.4. Erweiterte Regelverwaltung

Wenn Sie eine erweiterte Kontrolle über die Firewall-Regeln benötigen, klicken Sie auf **Erweitert**. Ein neues Fenster wird sich öffnen.



Erweiterte Regelverwaltung

Sie können eine Liste der Firewall-Regeln, nach dem Datum der Erstellung geordnet, sehen. Die Spalten der Tabelle geben nützliche Informationenzu jeder Regel.

Anmerkung

Wenn ein Verbindungsversuch ausgeführt wurde (sowohl eingehend als auch ausgehend), wendet BitDefender die Aktion der ersten Regel an, die auf die entsprechende Verbindung zutrifft. Deshalb ist die Reihenfolge der Regeln sehr wichtig.

Um eine Regel zu löschen, selektieren Sie diese und klicken Sie die **Löschen** Schaltfläche.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken Sie auf **Bearbeiten**.

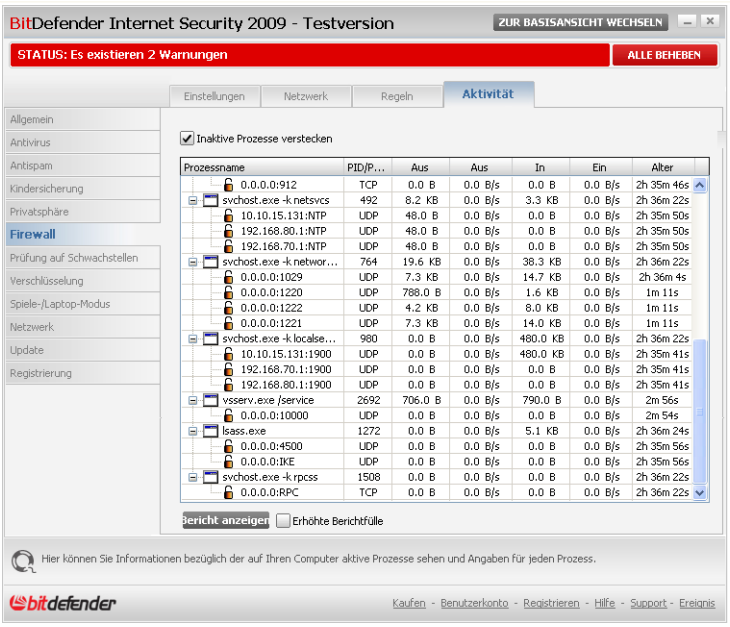
Sie können die Priorität einer Regel erhöhen oder heruntersetzen. Klicken Sie **In der Liste hochsetzen** um die ausgewählte Regel um ein Level nach oben zu setzen.

Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herunterzusetzen. Um einer Regel die höchste Priorität zu geben klicken Sie auf die **Als erste**-Schaltfläche. Um einer Regel die niedrigste Priotität zu zuweisen klicken Sie auf die **Als letzte**-Schaltfläche.

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

20.4. Aktivitätsanzeige

Um die aktuellen Netzwerk/Internetaktivitäten, die von der Anwendung sortiert wurden zu verfolgen (TCP und UDP) und um den Firewall-Bericht einzusehen klicken Sie auf **Firewall>Aktivität** in der erweiterten Ansicht.



Aktivitätsanzeige

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

Wenn Sie ebenfalls inaktive Prozesse sehen wollen, lassen Sie das Kontrollkästchen **Inaktive Prozesse verbergen** frei.

Die Bedeutung der Symbole ist wie folgt:

- Zeigt ein offene Verbindung auf Ihrem Computer an.
- Zeigt einen offenen Port auf Ihrem Computer an.

Das Fenster zeigt die aktuellen Netzwerk/Internetaktivitäten in Echtzeit. Wenn einzelne Verbindungen oder Ports geschlossen werden können Sie sehen wie diese ausgrauen, und evtl. verschwinden. Das selbe kann auch mit Anwendungen im Fenster geschehen welche geschlossen werden.

Für eine umfangreiche Ereignisliste bezüglich der Verwendung des Firewall-Moduls (Firewall aktivieren/deaktivieren, Datenverkehr blockieren, Einstellungen verändern) oder die durch die von diesem Modul entdeckten Aktivitäten erstellt wurden (Portprüfung, Verbindungsversuche oder Datenverkehr entsprechend den Regeln blockieren), betrachten Sie das BitDefender Firewall-Protokoll indem Sie auf **Protokoll anzeigen** klicken. Die Datei befindet sich im Ordner Gemeinsame Dateien des aktuellen Windows-Benutzers unter dem folgenden Pfad: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Wenn Sie möchten, dass das Protokoll noch mehr Informationen enthält, wählen Sie **Protokollumfang erweitern**.

21. Verschlüsseln

Bitdefender bietet Verschlüsselungsmöglichkeiten um Ihre vertraulichen Dokumente und Ihre Unterhaltungen über Instant Messaging mit dem Yahoo Messenger und dem MSN Messenger zu schützen.

21.1. Instant Messaging (IM) Verschlüsselung

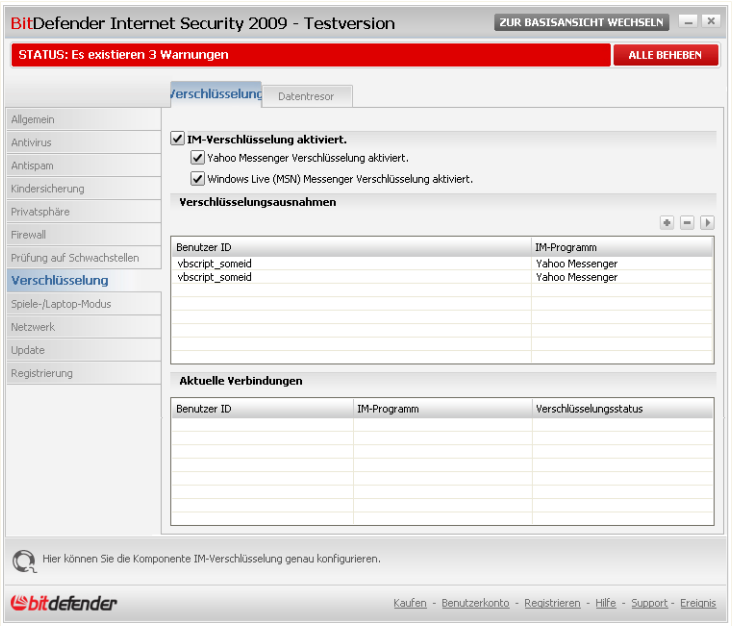
BitDefender verschlüsselt standardmäßig alle Ihre Unterhaltungen über IM-Chats, vorausgesetzt dass:

- Ihr Chatpartner hat eine BitDefender Verison installiert, die die IM-Verschlüsselung unterstützt und die IM-Verschlüsselung ist für die Instant Messaging Anwendung aktiviert, die verwendet wird.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.

Wichtig
BitDefender verschlüsselt die Unterhaltung nicht, wenn ein Chatpartner eine webbasierte Chat-Anwendung verwendet, so wie Meebo, oder eine andere Anwendung die Yahoo Messenger oder Windows Live (MSN) Messenger unterstützt.

Um die IM-Verschlüsselung zu konfigurieren klicken Sie auf **Verschlüsselung>IM-Verschlüsselung** in der erweiterten Ansicht.

Anmerkung
Sie können die IM-Verschlüsselung einfach mit der BitDefender Toolbar von dem Chat-Fenster aus konfigurieren. Für weitere Informationen lesen Sie bitte „*Integration in Messenger*“ (S. 53).



Instant Messenger Verschlüsselung

Die IM-Verschlüsselung ist standardmäßig für Yahoo Messenger und Windows Live (MSN) Messenger aktiviert. Sie können die IM-Verschlüsselung für eine bestimmte Anwendung oder komplett deaktivieren.

Zwei Tabellen werden angezeigt:

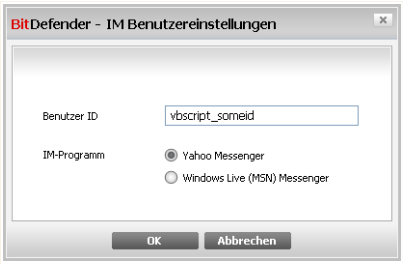
- **Verschlüsselungsausnahmen** - listet die Benutzer-IDs und das entsprechende IM-Programm auf, für den die Verschlüsselung deaktiviert ist. Um einen Kontakt aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Aktuelle Verbindungen** - listet die aktuellen Instant Messaging Verbindungen auf (Benutzer ID und entsprechendes IM-Programm) und zeigt an, ob diese verschlüsselt sind oder nicht. Eine Verbindung kann aus folgenden Gründen nicht verschlüsselt sein:
  - Sie haben die Verschlüsselung für den entsprechenden Kontakt deaktiviert.

- Ihr Kontakt hat keine BitDefender Version installiert, die eine IM-Verschlüsselung unterstützt.

21.1.1. Verschlüsselung für bestimmte Benutzer deaktivieren

Um die Verschlüsselung für einen bestimmten Benutzer zu deaktivieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um das Konfigurationsfenster zu öffnen.



Kontakte hinzufügen

2. Geben Sie die Benutzer-ID Ihres Kontaktes in das Editierfeld ein.
3. Wählen Sie die Chat-Anwendung des Kontaktes.
4. Klicken Sie auf **OK**.

21.2. Datentresor

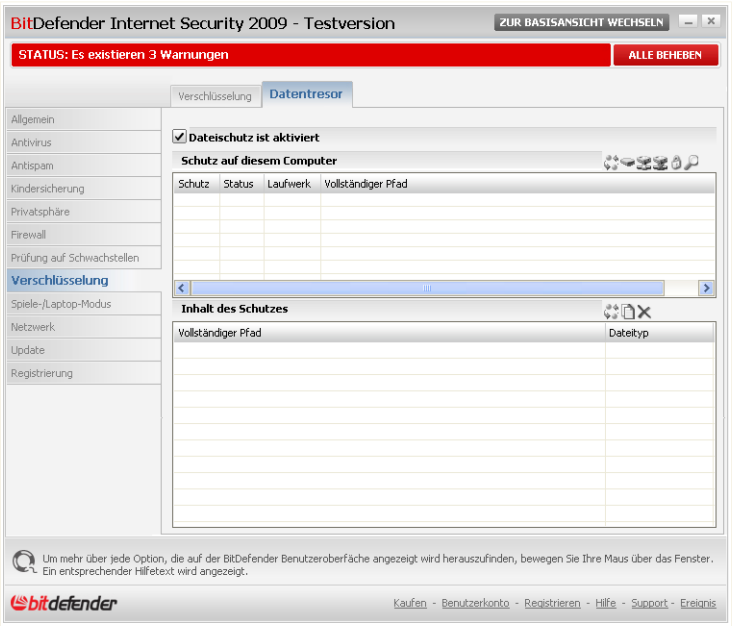
Der BitDefender Dateischutz gibt Ihnen die Möglichkeit verschlüsselte, passwortgeschützte logische Laufwerke (oder einen Schutz) auf Ihrem Computer zu erstellen, in denen Sie sicher Ihre wichtigen und vertraulichen Daten speichern können. Die Daten, die im Schutz gespeichert sind, können nur von der Person gesehen werden, die das Passwort kennt.

Mit dem Passwort können Sie einen Schutz öffnen, Daten speichern und den Schutz abschließen, wobei dieser sicher bleibt. Wenn ein Schutz geöffnet ist, können Sie neue Dateien hinzufügen, auf aktuelle Dateien zugreifen oder diese verändern.

Der Dateischutz ist eine verschlüsselte Datei auf Ihrer Festplatte mit der Endung `bvd`. Auch wenn die Dateien, die den Dateischutz darstellen von anderen Betriebssystemen

gelesen werden können, (beispielsweise Linux), können die sich darin befindenen Informationen nicht gelesen werden, weil sie verschlüsselt sind.

Um den Dateischutz auf Ihrem Computer zu verwalten klicken Sie auf **Verschlüsselung>Dateischutz** in der erweiterten Ansicht.



Datentresor

Um den Dateischutz zu deaktivieren, lassen Sie das Kontrollkästchen **Dateischutz ist aktiviert** frei und klicken Sie auf **Ja** um zu bestätigen. Wenn Sie den Dateischutz deaktivieren, wird jeder Dateischutz abgeschlossen und Sie haben keinen Zugriff mehr auf die sich darin befindenden Dateien.

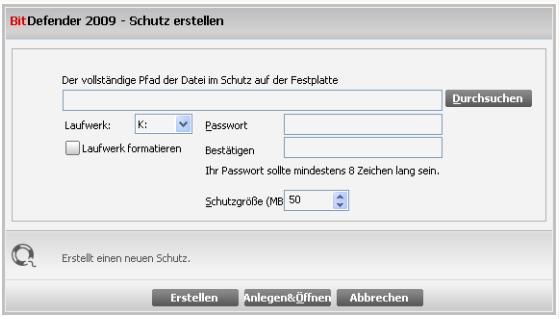
Die obere Tabelle zeigt den Dateischutz auf Ihrem Computer an. Sie können den Namen, den Status (offen/geschlossen), den Laufwerkbuchstaben und den vollständigen Pfad des Schutzes sehen. Die untere Tabelle zeigt den Inhalt des ausgewählten Schutzes an.

21.2.1. Einen Dateischutz erstellen

Um einen Dateischutz zu erstellen verwenden Sie eine der folgenden Methoden:

- Klicken Sie auf **Schutz erstellen**.
- Klicken Sie mit der rechten Maustaste auf die Schutztabelle und wählen Sie **Erstellen**.
- Klicken Sie mit der rechten Maustaste auf Ihren Desktop oder in einem Ordner auf Ihrem Computer, wählen Sie **BitDefender Dateischutz** und wählen Sie dann **Erstellen**.

Ein neues Fenster wird sich öffnen.



Datentresor erstellen

Gehen Sie wie folgt vor:

1. Geben Sie den Speicherort und den Namen des Dateischutzes an.
   - Klicken Sie auf **Durchsuchen** um den gewünschten Speicherort auszuwählen und den Dateischutz unter dem gewünschten Namen zu speichern.
   - Geben Sie den vollen Pfad des Dateischutzes auf der Festplatte ein.
2. Wählen Sie einen Laufwerkbuchstaben aus dem Menu. Wenn Sie einen Schutz öffnen, wird ein virtuelles Laufwerk mit dem gewählten Laufwerkbuchstaben unter Arbeitsplatz erscheinen.
3. Geben Sie das Schutz-Passwort in das Feld **Passwort** ein. Jeder, der den Schutz öffnen und auf die Dateien zugreifen möchte muss zuerst das Passwort angeben.

4. Wählen **Laufwerk formatieren** um das virtuelle Laufwerk des Dateischutzes zu formatieren.
5. Wenn Sie die Standardgröße (50 MB) des Schutzes ändern möchten geben Sie den gewünschten Wert in das Feld **Schutzgröße** ein.
6. Klicken Sie auf **Erstellen** wenn Sie den Schutz unter dem gewünschten Speicherort ersetllen möchten. Um den Schutz als ein virtuelles Laufwerk unter Arbeitsplatz zu erstellen und anzuzeigen, klicken Sie auf **Erstelen&Öffnen**

21.2.2. Einen Schutz öffnen

Um auf die Dateien in einem Schutz zugreifen und mit ihnen arbeiten zu können, muss der Schutz geöffnet werden. Wenn Sie einen Schutz öffnen, erscheint ein virtuelles Laufwerk unter Arbeitsplatz. Das Laufwerk hat den Laufwerkbuchstaben, der dem Schutz zugewiesen wurde.

Um einen Schutz zu öffnen verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Schutz öffnen**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Öffnen**.
- Klicken Sie mit der rechten Maustaste auf den Dateischutz unter Arbeitsplatz, gehen Sie auf **BitDefender Dateischutz** und wählen Sie **Öffnen**.

Ein neues Fenster wird sich öffnen.

Dateischutz öffnen

Gehen Sie wie folgt vor:

1. Wählen Sie einen Laufwerkbuchstaben aus dem Menu.
2. Geben Sie das Schutz-Passwort in das Feld **Passwort** ein.
3. Klicken Sie auf **Öffnen**.

21.2.3. Schutz abschließen

Wenn Sie mit Ihrer Arbeit im Schutz fertig sind, müssen Sie diesen abschließen um Ihre Daten zu schützen.

Um den Dateischutz abzuschließen verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Schutz abschließen**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Abschließen**.
- Klicken Sie mit der rechten Maustaste auf den Dateischutz unter Arbeitsplatz, gehen Sie auf **BitDefender Dateischutz** und wählen Sie **Abschließen**.
- Klicken Sie mit der rechten Maustaste auf das entsprechende virtuelle Laufwerk unter Arbeitsplatz, gehen Sie auf **BitDefender Dateischutz** und wählen Sie **Abschließen**.

21.2.4. Passwort für Schutz ändern

Um das Passwort für einen Schutz zu ändern, verwenden Sie bitte folgende Methoden:

- Wählen Sie den Schutz aus der Tabelle und klicken Sie auf **Passwort ändern**.
- Klicken Sie mit der rechten Maustaste auf den Schutz in der Tabelle und wählen Sie **Passwort ändern**.
- Klicken Sie mit der rechten Maustaste auf den Dateischutz unter Arbeitsplatz, gehen Sie auf **BitDefender Dateischutz** und wählen Sie **Passwort ändern**.

Ein neues Fenster wird sich öffnen.

Passwort für Schutz ändern

Gehen Sie wie folgt vor:

1. Geben Sie das aktuelle Passwort des Schutzes in das Feld **Altes Passwort** ein.
2. Geben Sie das neue Passwort des Schutzes in die Felder **Neues Passwort** und **Neues Passwort bestätigen** ein.

   Anmerkung

   Ihr Passwort muss mindestens 8 Zeichen lang sein. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

3. Klicken Sie auf **OK**, um das Passwort zu ändern.

21.2.5. Dateien zu einem Schutz hinzufügen

Um Dateien zu einem Schutz hinzuzufügen, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Datei hinzufügen**. Ein neues Fenster wird sich öffnen.
2. Wählen Sie welche Dateien / Ordner zum Schutz hinzugefügt werden sollen.
3. Klicken Sie auf **OK** um die ausgewählten Objekte in den Schutz zu kopieren.

Anmerkung

System- oder Programmdateien können nicht zum Schutz hinzugefügt werden.

21.2.6. Dateien aus einem Schutz entfernen

Um eine Datei aus einem Schutz zu entfernen, befolgen Sie folgende Schritte:

1. Wählen Sie aus der Schutztabelle den Schutz, der die Dateien enthält, die Sie entfernen möchten.
2. Wählen Sie die zu entfernende Datei aus der Tabelle, die den Schutzinhalt anzeigt.
3. Klicken Sie auf ✕ **Datei entfernen**.

Anmerkung
Wenn der Schutz geöffnet ist, können Sie Dateien direkt aus dem virtuellen Laufwerk, dem der Schutz zugewiesen ist, entfernen.

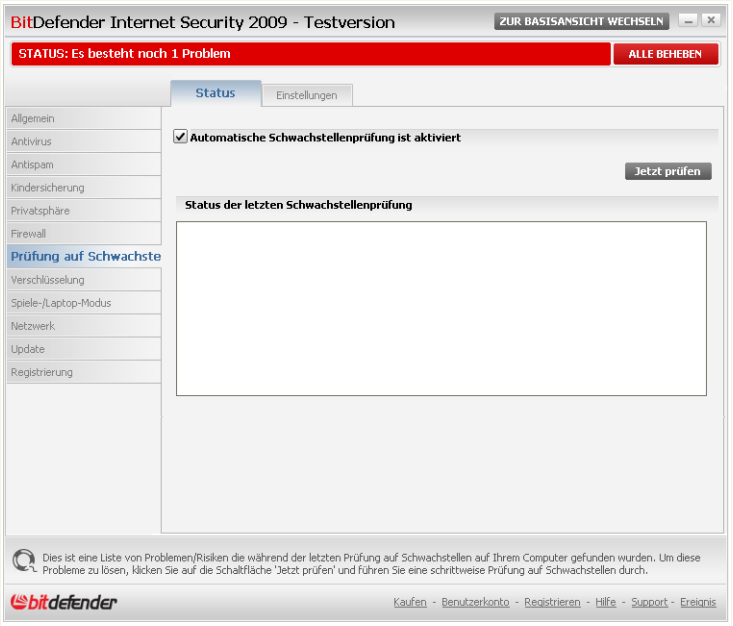
22. Prüfung auf Schwachstellen

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

BitDefender überprüft Ihr System regelmäßig auf Schwachstellen und benachrichtigt Sie über bestehende Probleme oder Risiken.

22.1. Status

Um die automatische Prüfung auf Schwachstellen zu konfigurieren oder eine Prüfung auf Schwachstellen auszuführen, klicken Sie auf **Schwachstellen>Status** in der erweiterten Ansicht.



Status der Schwachstellen Prüfung

Jede Tabelle zeigt die gelöste Objekte aus der letzten Schwachstellen Prüfung und deren aktuellen Status an. Hier können Sie sehen, welche Aktion Sie durchführen sollen, um jede Schwachstelle zu beheben, falls welche vorhanden. Wenn die Aktion**Keine** ist, dann wird diese Angelegenheit keine Schwachstelle darstellen.

Wichtig
Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die **Automatische Prüfung auf Schwachstellen** aktiviert.

22.1.1. Schwachstellen beheben

Um eine bestimmte Schwachstelle zu beheben, klicken Sie doppelt darauf und von der Situation abhängig, fahren Sie folgenderweise fort:

- Klicken Sie auf **Alle System-Updates installieren**, um die verfügbaren Windows Updates zu installieren.
- Wenn eine Anwendung nicht auf dem neusten Stand ist, Nutzen Sie den auf der Webseite **verfügbaren**) Link um die aktuellste Version herunterzuladen und zu installieren.
- Falls ein Windowskonto ein schwaches Passwort hat, fordern Sie den Benutzer beim nächsten Windows-Login auf das Passwort zu ändern oder ändern Sie es selbst.

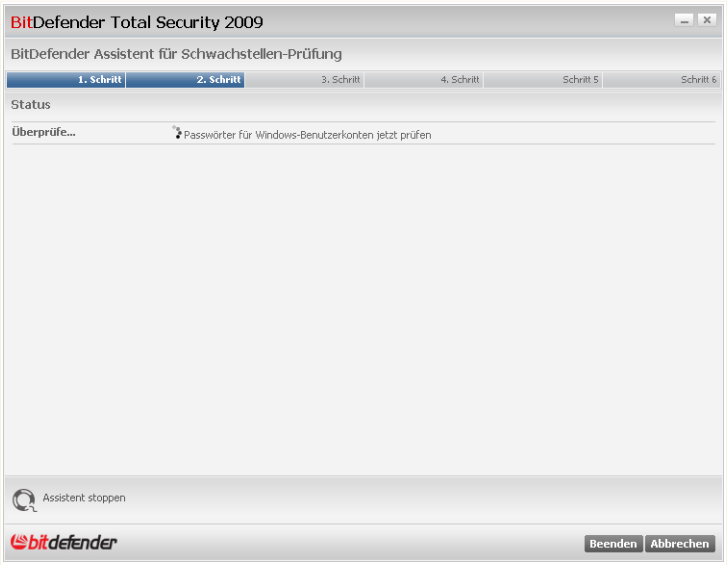
Um Ihren Computer auf Schwachstellen zu prüfen, klicken Sie auf **Jetzt prüfen** und folgen Sie den Schritten des Assistenten um die Schwachstellen zu beheben.

Schritt 1/6 - Auswahl der zu prüfenden Schwachstellen

Schwachstellen

Klicken Sie auf **Weiter** um das System auf die ausgewählten Schwachstellen zu überprüfen.

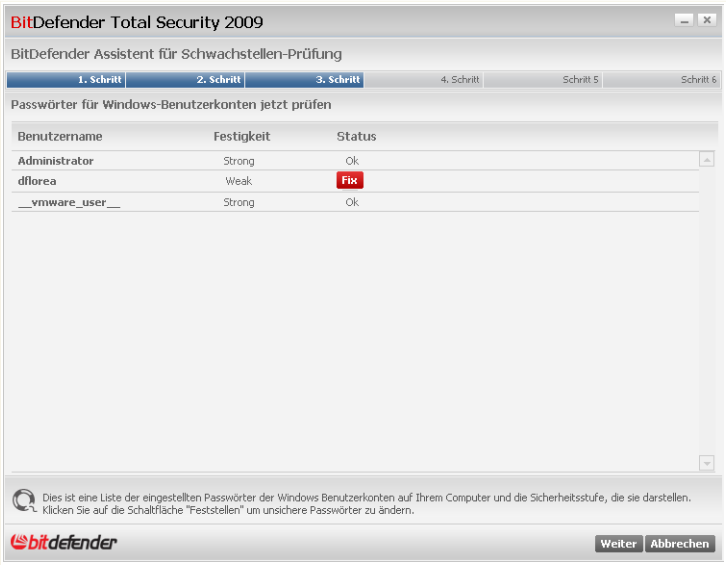
Schritt 2/6 - Nach Schwachstellen suchen



Prüfung auf Schwachstellen

Bitte warten Sie bis BitDefender die Prüfung auf Schwachstellen beendet hat.

Schritt 3/6 - Unsicheres Passwort ändern



Passwörter von Benutzern

Sie können die Liste der auf Ihrem Computer konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet.

Klicken Sie auf **Beheben**, um unsichere Passwörter zu ändern. Ein neues Fenster wird sich öffnen.

Passwort ändern

Wählen Sie die Methode um ein Problem zu beheben:

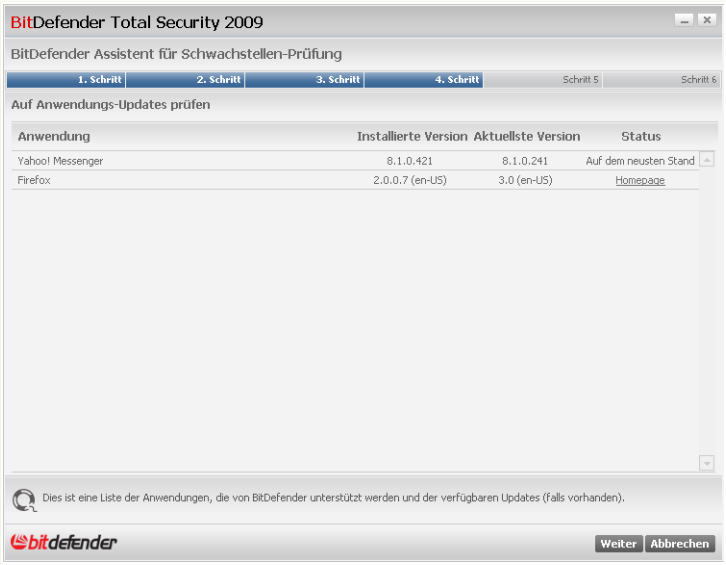
- **Den Benutzer zwingen das Passwort beim nächsten Login zu ändern.** Beim nächsten Windows-Login wird BitDefender den Benutzer dazu auffordern das Passwort zu ändern.
- **Benutzerpasswort ändern.** Geben Sie das neue Passwort in jedes der Editierfelder ein.

Anmerkung
Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (so wie #, $ or @).

Klicken Sie auf **OK**, um das Passwort zu ändern.

Klicken Sie auf **Weiter**.

Schritt 4/6 - Anwendungen aktualisieren



Anwendungen

Sie können eine Liste der Anwendungen sehen, die von BitDefender geprüft wurden und ob diese auf dem neusten Stand sind. Wenn eine Anwendung nicht auf dem neusten Stand ist, klicken Sie auf den zur Verfügung stehenden Link um die aktuellste Version herunterzuladen.

Klicken Sie auf **Weiter**.

Schritt 5/6 - Windows aktualisieren

Windows Updates

Sie können die Liste der wichtigen und weniger wichtigen Windows-Updates sehen, die zur Zeit nicht auf Ihrem Computer installiert sind. Klicken Sie auf **Alle System-Updates installieren**, um die verfügbaren Updates zu installieren.

Klicken Sie auf **Weiter**.

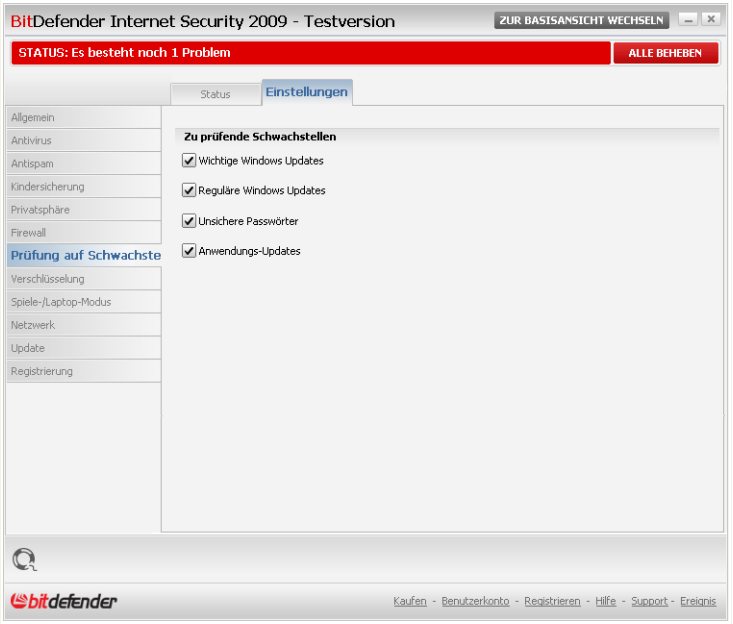
Schritt 6/6 - Ergebnisse betrachten

Ergebnisse

Klicken Sie auf **Schließen**.

22.2. Einstellungen

Um die Einstellungen für die automatische Prüfung auf Schwachstellen zu verwalten, klicken Sie auf **Schwachstellen>Einstellungen** in der erweiterten Ansicht.



Einstellungen der automatischen Prüfung auf Schwachstellen

Markieren Sie die Kontrollkästchen der entsprechenden Systemschwachstellen die regelmäßig überprüft werden sollen.

- **Wichtige Windows Updates**
- **Normale Windows Updates**
- **Unsichere Passwörter**
- **Anwendungs-Updates**

Anmerkung
Wenn Sie das Kontrollkästchen für eine bestimmte Schwachstelle freilassen, wird Bitdefender Sie nicht über die entsprechenden Probleme und Risiken informieren.

23. Spiele-/Laptop-Modus

Das Modul Spiele-/Laptop-Modus gibt ihnen die Möglichkeit spezielle Betriebsmodi von BitDefender zu konfigurieren.

- Der Spiele-Modus verändert die Schutzeinstellungen zeitweise derart, dass ihr Einfluss auf die Leistungsfähigkeit des Systems während Sie spielen so gering wie möglich ist.
- Der Laptop-Modus stoppt voreingestellte Aufgaben wenn der Laptop über einen Akku betrieben wird, um dessen Laufzeit zu verlängern.

23.1. Spiele-Modus

Der Spielmodus verändert die Schutzeinstellungen zeitweise derart, dass ihr Einfluss auf die Leistungsfähigkeit des Systems so gering wie möglich ist. Wenn Sie den Spielmodus aktivieren werden folgende Einstellungen angewendet:

- Alle BitDefender Alarme und Pop-ups werden deaktiviert.
- Der Echtzeit-Schutz wird auf **Tolerant** gestellt.
- Die BitDefender Firewall ist auf**Alle erlauben** eingestellt. Das bedeutet, dass alle neuen Verbindungen (eingehend und ausgehend) automatisch erlaubt werden, unabhängig vom verwendeten Port oder Protokoll.
- Updates werden nicht standardmäßig durchgeführt.

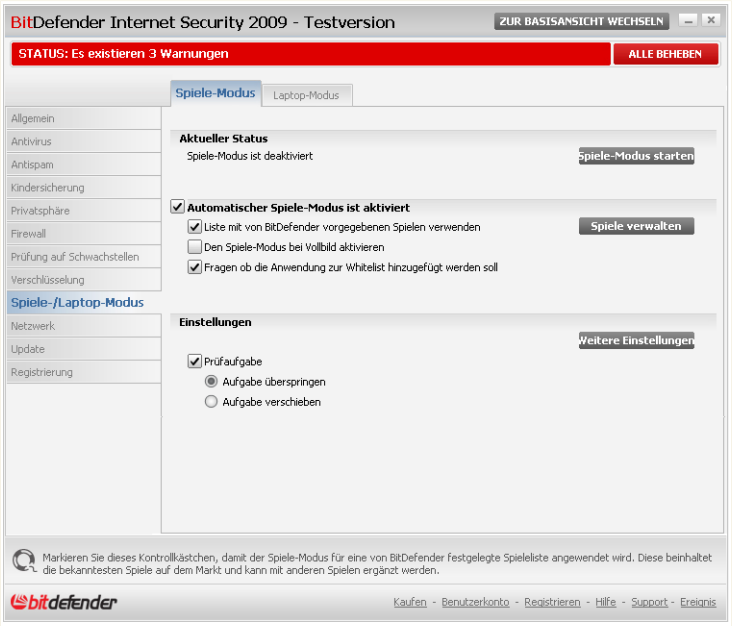
  Anmerkung
  Um diese Einstellung zu ändern, gehen Sie zu Update>Einstellungen und lassen Sie das Kontrollkästchen **Kein Update im Spiele-Modus** frei.

- Voreingestellte Prüfaufgaben sind standardmäßig deaktiviert.

BitDefender startet den Spiele-Modus standardmäßig wenn Sie ein Spiel starten, das sich auf der Liste der bekannten Spiele von BitDefender befindet, oder wenn eine Anwendung auf dem ganzen Bildschirm ausgeführt wird. Mit dem Tastenkürzel `Strg+Alt+Shift+G` können Sie den Spiele-Modus manuell starten. Es wird dringend empfohlen dass Sie den Spiele-Modus verlassen, wenn Sie mit dem Spielen fertig sind (Sie können dafür das selbe Tastenkürzel verwenden `Ctrl+Alt+Shift+G`).

Anmerkung
Wenn der Spielmodus aktiviert ist, sehen Sie den Buchstaben G über dem BitDefender Symbol.

Um den Spiele-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Spiele-Modus** in der Profiansicht.



Spiele-Modus

Im oberen Bereich des Abschnitts können Sie den Status des Spiele-Modus sehen. Sie können auf**Spiele-Modus starten** oder **Spiele-Modus beenden** klicken um den aktuellen Status zu verändern.

23.1.1. Automatischer Spiele-Modus konfigurieren

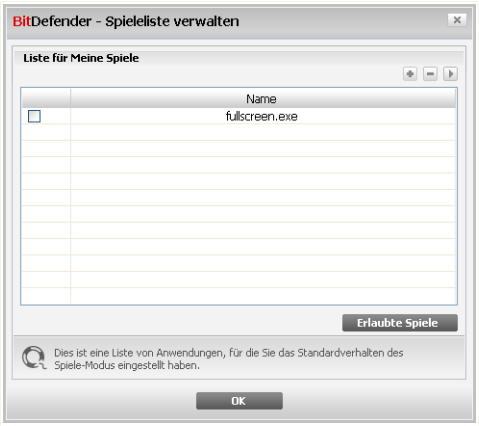
Mit dem automatischen Spiele-Modus kann BitDefender automatisch den Spiele-Modus starten, wenn ein Spiel entdeckt wird. Folgende Optionen können konfiguriert werden:

- **Von BitDefender zur Verfügung gestellte Spieleliste verwenden** - wenn Sie ein Spiel der Liste der bekannten Spiele starten, startet BitDefender automatisch den Spiele-Modus. Um diese Liste zu sehen, klicken Sie auf **Spiele verwalten** und dann **Erlaubte Spiele ansehen**.
- **Spiele-Modus bei Vollbild starten** -wenn eine Anwendung auf dem gesamten Bildschirm ausgeführt wird startet der Spiele-Modus automatisch.
- **Anwendung zur Spieleliste hinzufügen?** - um aufgefordert zu werden, eine neue Anwendung zur Spieleliste hinzuzufügen wenn Sie das Vollbild verlassen. Indem Sie eine neue Anwendung zur Spieleliste hinzufügen, wird BitDefender den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

Anmerkung
Wenn Sie nicht möchten, dass BitDefender den Spielemodus automatisch startet, lassen Sie das Kontrollkästchen **Automatischer Spiele-Modus** frei.

23.1.2. Spieleliste verwalten

BitDefender startet den Spiele-Modus automatisch, wenn eine Anwendung gestartet wird die sich auf der Spieleliste befindet. Um die Spieleliste zu sehen und zu verwalten, klicken Sie auf**Spiele verwalten**. Ein neues Fenster wird sich öffnen.



Spieleliste

Neue Anwendungen werden automatisch zur Liste hinzugefügt, wenn:

- Sie ein Spiel starten das Bitdefender bekannt ist. Um diese Liste zu sehen, klicken Sie auf **Erlaubte Spiele betrachten**.
- Nachdem Sie das Vollbild beendet haben, können Sie das Spiel über das Aufforderungsfenster zur Spieleliste hinzufügen.

Wenn Sie den automatischen Spiele-Modus für eine bestimmte Anwendung von der Liste deaktivieren möchten, lassen Sie das entsprechende Kontrollkästchen frei. Sie sollten den automatischen Spiele-Modus für reguläre Anwendungen die den gesamten Bildschirm verwenden deaktiviert lassen, so wie Web-Browser und Mediaplayer.

Um die Spiele-Liste zu verwalten, können Sie die Schaltflächen verwenden, die sich im oberen Bereich der Tabelle befineden:

- Klicken Sie auf **Hinzufügen** um eine neue Anwendung zu der Spieleliste hinzufügen.
- **Entfernen** - dient zum Entfernen einer Anwendung von der Spieleliste.
- Klicken Sie auf **OK** um den Eintrag aus der Spieleliste zu editieren.

Spiele hinzufügen oder bearbeiten

Wenn Sie einen Eintag der Spiele-Liste hinzufügen oder bearbeiten, wird folgendes Fenster erscheinen:

Spiel hinzufügen

Klicken Sie auf **Durchsuchen** um die Anwendung auszuwählen oder geben Sie den vollständigen Pfad der Anwendung in das Editierfeld ein.

Wenn Sie nicht möchten, dass der Spiele-Modus automatisch gestartet wird, wenn die ausgewählte Anwendung gestartet wurde, wählen Sie **Deaktivieren**.

Klicken Sie auf **OK** um den Eintrag zu der Spieleliste hinzuzufügen.

23.1.3. Einstellungen des Spiele-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Prüfaufgabe** - um zu verhindern, dass voreingestellte Prüfaufgaben im Spielemodus ausgeführt werden. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die voreingestellte Aufgabe wird sofort ausgeführt, sobald der Spiele-Modus beendet wird.

Um die BitDefender Firewall automatisch zu deaktivieren, wenn der Spiele-Modus ausgeführt wird, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Weitere Einstellungen**. Ein neues Fenster wird sich öffnen.
2. Markieren Sie das Kontrollkästchen **Firewall nicht verwenden**.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

23.1.4. Tastenkombination für Spielmodus ändern

Mit dem Tastenkürzel `Strg+Alt+Shift+G` können Sie den Spiele-Modus manuell starten. Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Weitere Einstellungen**. Ein neues Fenster wird sich öffnen.

Mehr Einstellungen

2. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :
   - Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).
   - Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

   Wenn Sie beispielsweise die Tastenkombination `Strg+Alt+D` benutzen möchten, markieren Sie `Strg` und `Alt` und geben Sie `D` ein.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Anmerkung
Wenn Sie die Markierung neben **Tastenkombination** entfernen, wird die Tastenkombination deaktiviert.

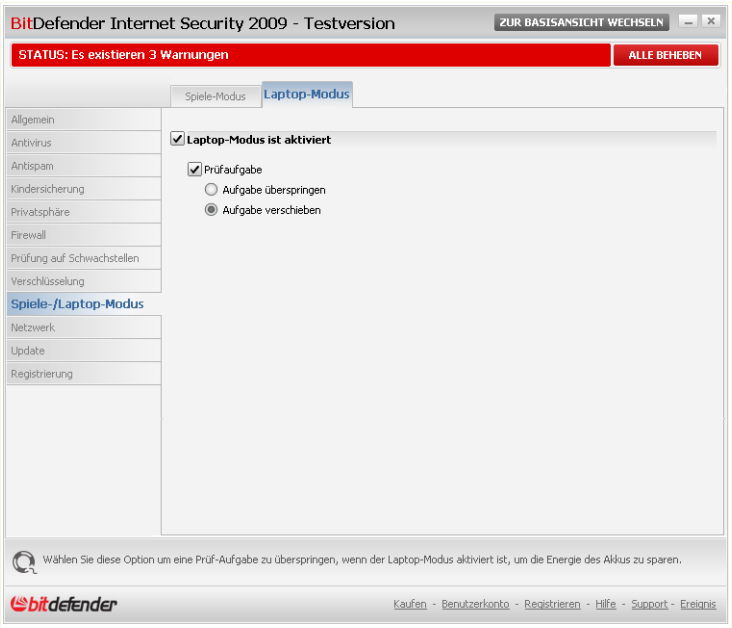
23.2. Laptop-Modus

Der Laptop-Modus wurde für Nutzer von Laptops und Notebooks konzipiert. Er soll den Energieverbrauch von BitDefender so gering wie möglich halten um den Einfluss auf die Akkulaufzeit zu minimieren.

Während der Laptop-Modus ausgeführt wird, werden voreingestellte Aufgaben standardmäßig nicht durchgeführt.

BitDefender erkennt wenn Ihr Laptop über ein Akku läuft und startet den Laptop-Modus automatisch. Ebenso beendet BitDefender automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Um den Laptop-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Laptop-Modus** in der Profiansicht.



Laptop-Modus

Sie können sehen ob der Laptop-Modus aktiviert ist oder nicht. Wenn der Laptop-Modus aktiviert ist, wird BitDefender die konfigurierten Einstellungen anwenden, wenn der Laptop über einen Akku betrieben wird.

23.2.1. Einstellungen des Laptop-Modus konfigurieren

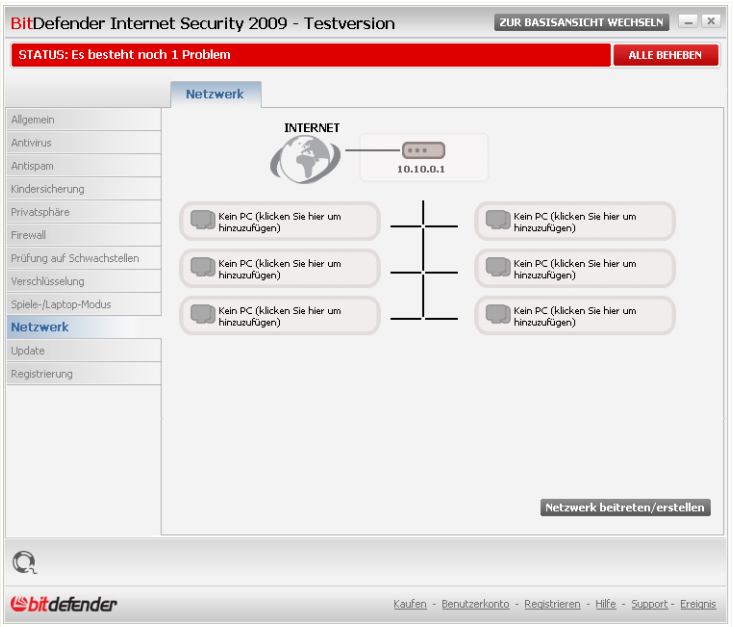
Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Prüfaufgabe** - um zu verhindern, dass Prüfaufgaben durchgeführt werden, wenn der Laptop-Modus ausgeführt wird. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die Aufgabe wird sofort durchgeführt, sobald der Laptop-Modus beendet wird.

24. Netzwerk

Mit dem Netzwerk-Modul können Sie die BitDefender Produkte die auf den Computern in Ihrem Haushalt installiert sind von einem Computer aus verwalten.



Netzwerkübersicht

Um die BitDefender Produkte, die auf den Computern in Ihrem Haushalt installiert sind verwalten zu können, befolgen Sie diese Schritte:

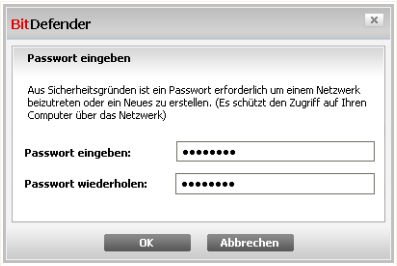
1. Fügen Sie Ihren Computer dem BitDefender Home-Netzwerk hinzu. Das Hinzufügen zu einem Netzwerk besteht aus dem Konfigurieren eines administrativen Passworts für die Verwaltung des Home-Netzwerks.
2. Fügen Sie jeden Computer, den Sie verwalten möchten dem Home-Netzwerk hinzu (Passwort einstellen).

3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

24.1. Dem BitDefender-Netzwerk beitreten

Um dem BitDefender Home-Netzwerk beizutreten, befolgen Sie diese Schritte:

1. Klicken Sie auf **Netzwerk beitreten/erstellen**. Sie werden dazu aufgefordert, das Passwort für die Home-Verwaltung zu konfigurieren.



Passwort konfigurieren

2. Geben Sie das selbe Passwort in jedes der Editierfelder ein.
3. Klicken Sie auf **OK**.

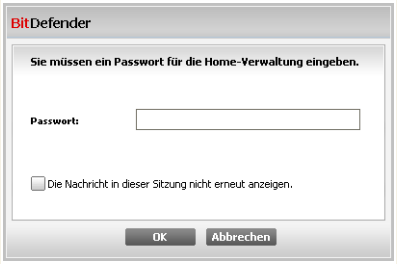
Sie sehen den Namen des Computers in der Netzwerkübersicht.

24.2. Computer zum BitDefender-Netzwerk hinzufügen

Um einen Computer zum BitDefender Home-Netzwerk hinzuzufügen, müssen Sie zuerst das Passwort der BitDefender Home-Verwaltung auf dem entsprechenden Computer konfigurieren.

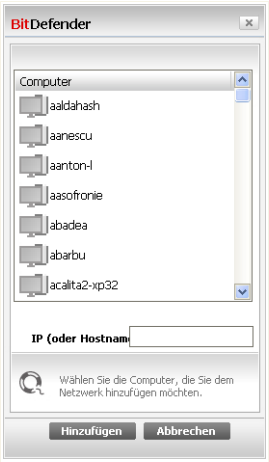
Um einen Computer zum BitDefender Home-Netzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf **Netzwerk verwalten**. Sie werden dazu aufgefordert, das Passwort für die lokale Home-Verwaltung anzugeben.



Passwort eingeben

2. Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**. Ein neues Fenster wird sich öffnen.



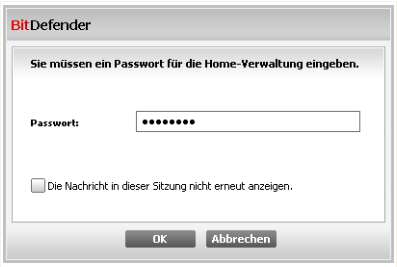
Computer hinzufügen

Sie können eine Liste der Computer im Netzwerk sehen. Die Bedeutung des Symbols ist wie folgt:

- Zeigt einen Online-Computer an, auf dem keine BitDefender-Produkte installiert sind.
- Zeigt einen Online-Computer an, auf dem BitDefender installiert ist.

- Zeigt einen Offline-Computer an, auf dem BitDefender installiert ist.

3. Sie können hierzu eine der folgenden Methoden wählen:
   - Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
   - Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.
4. Klicken Sie auf **Hinzufügen**. Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.



Authentifizieren

5. Geben Sie das Passwort für die Home-Verwaltung ein, das auf dem entsprechenden Computer konfiguriert wurde.
6. Klicken Sie auf **OK**. Wenn Sie das korrekt Passwort angegeben haben, wird der ausgewählte Computername in der Netzwerkübersicht erscheinen.

Anmerkung
Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

24.3. Das BitDefender-Netzwerk verwalten

Wenn Sie das BitDefender Home-Netzwerk erstellt haben, können Sie alle BitDefender Produkte von einem Computer aus verwalten.

Netzwerkübersicht

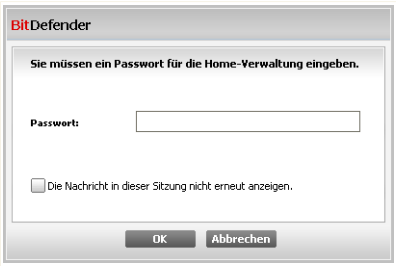
Wenn Sie den Mauszeiger auf einen Computer der Netzwerkübersicht bewegen, können Sie einige Informationen über diesen sehen (Name, IP-Adresse, Anzahl der Probleme die die Systemsicherheit betreffen, Registrierungsstatus von BitDefender).

Wenn Sie mit der rechten Mautaste auf einen Computernamen im Netzwerk klicken, können Sie alle administrativen Aufgaben sehen, die Sie auf dem Remote-Computer ausführen können.

- **Diesen Computer registrieren**
- **Passwort für Einstellungen einstellen**
- **Prüf-Aufgabe ausführen**
- **Risiken auf diesem Computer feststellen**
- **Historie dieses Computers anzeigen**
- **Jetzt ein Update auf diesem Computer durchführen**

- **Profil anwenden**
- **Tuning-Aufgabe auf diesem Computer durchführen**
- **Diesen Computer als Update-Server für dieses Netzwerk festlegen**

Bevor Sie eine Aufgabe auf einem bestimmten Computer ausführen können, werden Sie dazu aufgefordert das Passwort der lokalen Home-Verwaltung anzugeben.



Passwort eingeben

Geben Sie das Passwort für die Home-Verwaltung ein und klicken Sie auf **OK**.

Anmerkung

Wenn Sie mehrere Aufgaben durchführen möchten, dann wählen Sie **In dieser Sitzung nicht nochmals fragen**. Wenn Sie diese Option wählen, werden Sie während der laufenden Sitzung nicht nochmals nach einem Passwort gefragt.

25. Update (Aktualisierung)

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm BitDefender stets mit den neuesten Virensignaturen betreiben.

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

Wenn ein Update entdeckt wird, können Sie um eine Bestätigung für das Update gebeten werden oder das Update wird automatisch durchgeführt, je nach den Einstellungen für das automatische Update.

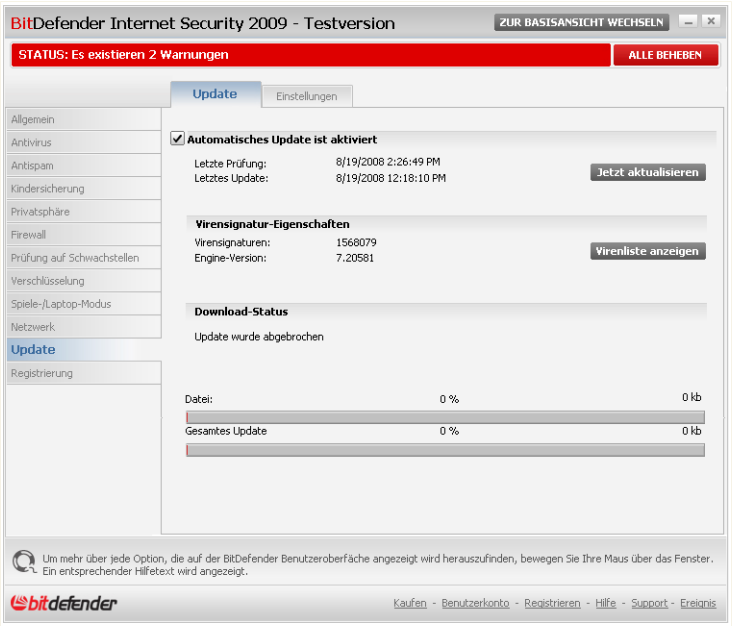
Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise geupdated werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die AntiViren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **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**.

25.1. Automatisches Update

Um Informationen zum Update zu erhalten und automatische Updates auszuführen, klicken Sie auf **Update>Update** in der erweiterten Ansicht.



Automatisches Update

Hier können Sie sehen wann das letzte Update durchgeführt wurde und wann zuletzt eine Prüfung nach Update stattgefunden hat. (und ob das Update erfolgreich war) Ausserdem werden Informationen zur momentanen Engineversion und zur Virensignatur angezeigt.

Wenn Sie das Updatemodul während eines Updates öffnen können Sie den aktuellen Status in Echtzeit einsehen.

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

Sie können Malware-Signaturen für Ihren BitDefender erhalten, indem Sie auf **Virenliste anzeigen** klicken. Eine HTML-Datei, die alle verfügbaren Signaturen enthält wird erstellt und in einem Webbrowser geöffnet. Sie können die Datenbank nach einer bestimmten Signatur durchsuchen oder auf **BitDefender Virenliste** klicken, um auf die Online-Signaturdatenbank von BitDefender zuzugreifen.

25.1.1. Benutzergesteuertes Update

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

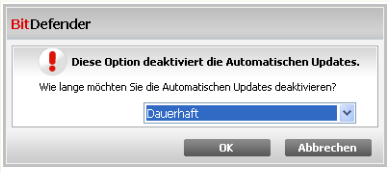
Das **Update** Modul verbindet Ihren Computer automatisch mit dem BitDefender Update Server und benachrichtigt Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt ob das Update erfolgen soll, oder das Update erfolgt automatisch.

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

Anmerkung
Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen.

25.1.2. Automatisches Update deaktivieren

Wenn Sie das Automatische Update deaktivieren erscheint ein Warnfenster.



Automatisches Update deaktivieren

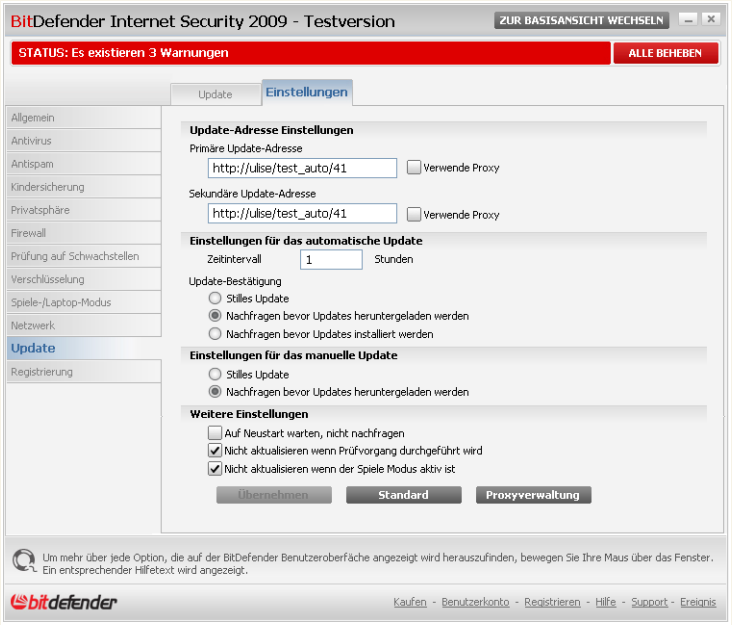
Sie müssen Ihre Einstellung bestätigen indem Sie definieren wie lange das Automatisch Update deaktiviert werden soll. Zur Verfügung stehen die Optionen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.

Warnung
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen die Deaktivierungszeit so gering wie möglich zu halten da BitDefender Sie nur gegen die neusten Bedrohungen schützen kann wenn dieser aktuell ist.

25.2. Update-Einstellungen

Updates können vom lokalen Netz, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden. Standardmässig prüft BitDefender jede Stunde auf neue Updates und installiert diese ohne Ihr zutun.

Um Updateeinstellungen vorzunehmen und Proxys zu konfigurieren klicken auf **Update>Einstellungen** in der erweiterten Ansicht.



Update-Einstellungen

Das Fenster mit den Update-Einstellungen enthält vier aufklappbare Optionskategorien (**Update-Adresse**, **Einstellungen für das Automatische Update**, **Einstellungen für das manuelle Update** und **Weitere Einstellungen**). Jede Kategorie wird seperat beschrieben.

25.2.1. Update-Adresse

Um eine Update-Adresse festzulegen verwenden Sie die Optionen der **Update-Adresse** Kategorie.

Anmerkung
Ändern Sie diese Einstellungn nur wenn Sie mit einem lokalen Updateserver verbunden sind oder wenn das Update über einen Proxy erfolgt.

Für ein zuverlässigeres und schnelleres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Standardmässig stimmen diese beiden Adressen überein: `http://upgrade.bitdefender.com`.

Um die Update-Adresse zu ändern geben Sie die Adresse des lokalen Servers in das gewünschte **URL** Feld ein.

Anmerkung
Wir empfehlen den Primären Updateserver auf den lokalen Server zu ändern und den sekundären Server unverändert zu belassen sodass im Falle eines lokalen Serverausfalls dennoch Updates durchgeführt werden können.

Wenn Sie für den Zugang zum Internet einen Proxy verwenden, wählen Sie die Option **Proxy verwenden**, und klicken Sie dann auf **Proxyverwaltung** um diese zu konfigurieren. Weitere Informationen finden Sie unter „*Proxyverwaltung*“ (S. 290)

25.2.2. Automatisches Update konfigurieren

Um die Optionen des Automatischen Updates einzustellen verwenden Sie die Optionen unter **Einstellungen für das Automatische Update**.

Sie können die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen im Feld **Zeitinterval** festlegen. Standardmässig ist dieses auf eine Stunde eingestellt.

Um festzulegen wie das automatische Update durchgeführt werden soll können Sie zwischen den folgenden Optionen wählen:

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.
- **Nachfragen bevor Updates installiert werden** - BitDefender frägt den Benutzer bevor ein Update installiert wird.

25.2.3. Manuelle Update Einstellungen

Um festzulegen wie ein manuelles Update durchgeführt wird wählen Sie ein der folgenden Optionen in der Kategorie **Einstellungen für das manuelle Update**:

- **Stilles Update** - BitDefender führt Updates, ohne Benutzereingriff, komplett selbständig im Hintergrund durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.

25.2.4. Weitere Einstellungen konfigurieren

Um sicherzustellen das Sie bei der Arbeit nicht vom Updatevorgang gestört werden haben Sie folgende Optionen in der Kategorie **Weitere Einstellungen** zur Verfügung:

- **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.

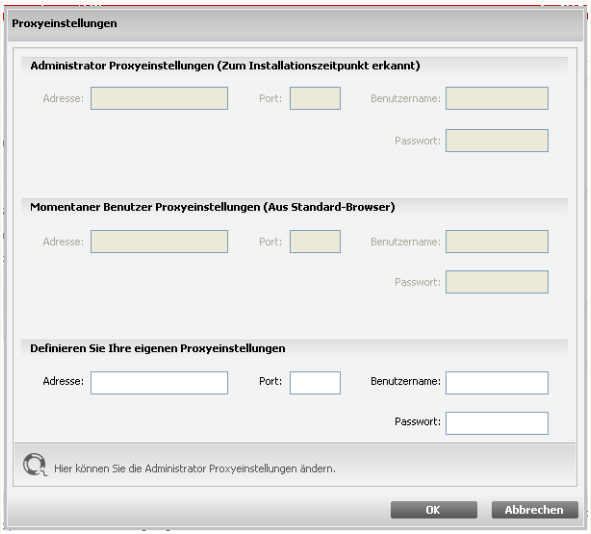
- **Nicht aktualisieren wenn der Spiele Modus aktiv ist** - Wenn der Spiele Modus aktiviert ist wird BitDefender kein Update durchführen. Durch diese Option können Sie den Einfluss der Anwendung, auf die Geschindigkeit während des Spielens minimieren.

25.2.5. Proxyverwaltung

Falls Ihre Firma einen Proxy verwendet um eine Internetverbindung herzustellen müssen Sie diese in BitDefender konfigurieren um sicherzustellen das ein Update möglich ist. Anderenfalls werden die Proxyeinstellungen des Administrators welcher das Produkt installiert hat, oder die momentanen Proxyeinstellungen des Standard-Browsers verwendet.

Anmerkung
Proxyeinstellungen können nur von Administratoren oder Hauptbenutzern (welche über das nötige Passwort verfügen) vorgenommen werden.

Um Proxyeinstellungen vorzunehmen klicken Sie auf **Proxyverwaltung**. Die **Proxyverwaltung** wird geöffnet.



Proxyverwaltung

Es bestehen drei mögliche Proxyeinstellungen:

- **Proxyeinstellungen des Administrators** - Diese Einstellungen wurden zum Zeitpunkt der Installation von BitDefender erkannt. Diese können nur von eben diesem Administratorkonto verändert werden. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.
- **Proxyeinstellungen der momentanen Benutzers** - Die Einstellungen des vom momentan eingeloggten Benutzers verwendeten Browser werden übernommen. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

Anmerkung
Die unterstützen Browser sind hierbei der Internet Explorer, Mozilla Firefox und Opera. Sollten Sie einen anderen Browser verwenden wird BitDefender nicht in der Lage sein die Einstellungen zu übernehmen.

- **Eigene Proxyeinstellungen** - Hier können Sie selbst Proxyeinstellungen vornehmen wenn Sie als Adminstrator eingeloggt sind.

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

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

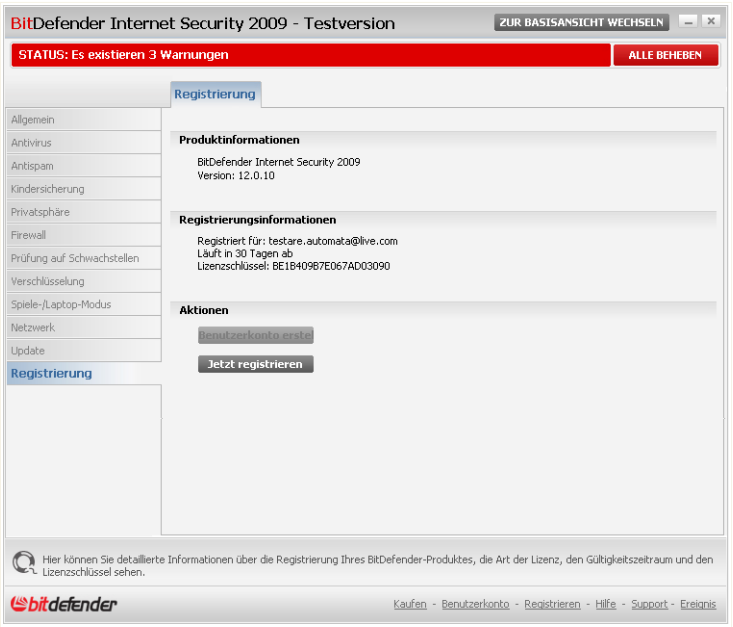
Zuerst wird versucht ein Update über die eigenen Proxyeinstellungen vorzunehmen. Als nächstes werden die Proxyeinstellungen des Administrators verwenden. Wenn auch dies nicht zum erfolgt führt wird ein Update über die Einstellungen des momentanen Benutzers durchgeführt.

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

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

26. Registrierung

Um komplette Informationen über Ihr Bitdefender-Produkt und den Registrierungsstatus zu erhalten, klicken Sie auf **Registrierung** in der erweiterten Ansicht.



Registrierung

In diesem Abschnitt werden folgende Bereiche angezeigt:

- **Produktinformation**: Das BitDefender-Produkt und die Version.
- **Registrierungsinformationen**: Die E-Mail-Adresse die verwendet wurde um Ihr BitDefender Benutzerkonto (falls konfiguriert) zu erstellen, der aktuelle Lizenzschlüssel und wie viele Tage verbleiben bis die Lizenz abläuft.

26.1. BitDefender Internet Security 2009 registrieren

Klicken Sie auf **Jetzt registrieren** um das Fenster für die Produktregistrierung zu öffnen.

Registrierung

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

Um BitDefender Internet Security 2009 zu registrieren:

1. Klicken Sie auf die Schaltfläche **Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren**.
2. Geben Sie den Lizenzschlüssel in das Editierfeld ein.

Anmerkung

Sie finden den Lizenzschlüssel:

- Auf dem CD-Aufdruck.
- Auf der Registrierungskarte des Produktes.

- In der E-Mail-Bestätigung des Online-Kaufs.

Wenn Sie keinen Bitdefender-Lizenzschlüssel besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Klicken Sie auf **Fertigstellen**.

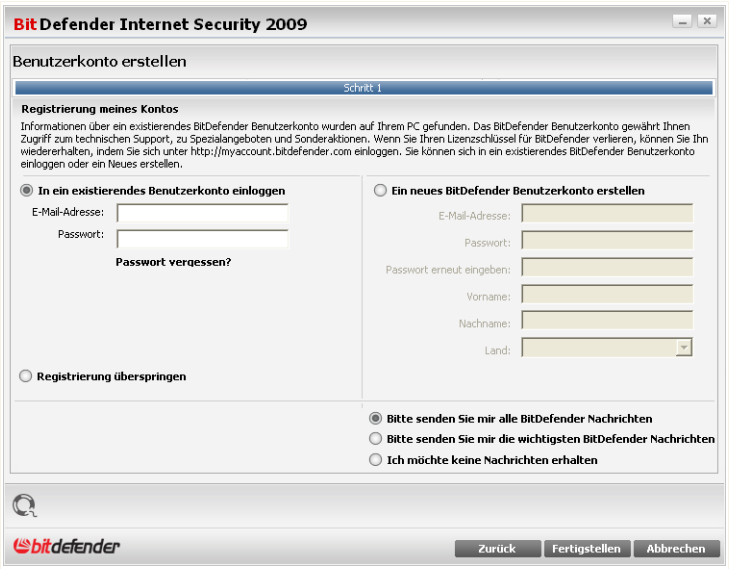
26.2. Ein BitDefender Benutzerkonto erstellen

Als Teil der Registrierung, sollen Sie ein BitDefender Konto erstellen. Mit dem BitDefender Benutzerkonto haben Sie Zugang zu BitDefender Updates, zu kostenfreien technischen Support und Sonderangeboten und -Aktionen. Wenn Sie Ihren BitDefender Lizenzschlüssel verlieren, können Sie sich unter http://myaccount.bitdefender.com in Ihr Konto einloggen, um ihn wieder zu erhalten.

Wichtig

Sie müssen innerhalb von 15 Tagen (Test-Version) bzw. 30 Tagen (lizensierte Version) nach Installation des BitDefender ein Benutzerkonto erstellen. Ansonsten, BitDefender wird keine automatische Updates erhalten.

Wenn Sie noch kein BitDefender-Benutzerkonto erstellt haben, klicken Sie auf **Ein Benutzerkonto erstellen** um das Fenster für die Benutzerkontoregistrierung zu öffnen.



Kontoerstellung

Wenn Sie zur Zeit kein BitDefender Benutzerkonto einrichten wollen, klicken Sie auf **Registrierung überspringen** und dann auf **Beenden**. Andererseits gehen Sie je nach Ihren Wünschen wie folgt vor:

- „Ich habe noch kein BitDefender-Benutzerkonto“ (S. 296)
- „Ich habe bereits ein BitDefender Nutzerkonto.“ (S. 297)

Ich habe noch kein BitDefender-Benutzerkonto

Um ein BitDefender-Benutzerkonto zu erstellen, wählen Sie **Ein neues BitDefender Benutzerkonto erstellen** und geben Sie die benötigten Informationen ein. Die hier eingetragenen Daten bleiben vertraulich.

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.
- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort sollte mindestens 6 Zeichen haben.

- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.
- **Land** - wählen Sie das Land Ihres Wohnsitzes aus.

Anmerkung
Benutzen Sie die angegebene E-Mail Adresse und das Passwort um sich in Ihr Benutzerkonto unter folgendem Link einzuloggen: http://myaccount.bitdefender.com.

Um erfolgreich ein Benutzerkonto einzurichten müssen Sie zunächst Ihre E-Mail Adresse aktivieren. Überprüfen Sie hierzu Ihre E-Mails der angegebenen Adresse und folgen Sie den Instruktionen, die Sie vom BitDefender Registrierungsservice zugesandt bekommen haben.

Auf Wunsch wird BitDefender Sie über die E-Mail-Adresse Ihres Benutzerkontos über Sonderangebote informieren. Wählen Sie eine der zur Verfügung stehenden Optionen:

- **Senden Sie mir alle BitDefender-Nachrichten**
- **Senden Sie mir nur die wichtigsten Nachrichten**
- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.

Ich habe bereits ein BitDefender Nutzerkonto.

BitDefender weist Sie daraufhin, falls bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert wurde. Geben Sie in diesem Fall das Passwort Ihres Benutzerkontos an.

Wenn Sie bereits ein aktives Benutzerkonto besitzen, BitDefender es jedoch nicht entdeckt, wählen Sie **In ein bestehendes BitDefender-Benutzerkonto einloggen** und geben Sie die E-Mail Adresse und das Passwort Ihres Benutzerkontos ein.

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

Auf Wunsch wird BitDefender Sie über die E-Mail-Adresse Ihres Benutzerkontos über Sonderangebote informieren. Wählen Sie eine der zur Verfügung stehenden Optionen:

- **Senden Sie mir alle BitDefender-Nachrichten**
- **Senden Sie mir nur die wichtigsten Nachrichten**

- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.

Hilfe erhalten

27. Support

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 BITDEFENDER 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.

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 +49 2301 91 84 555 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.

27.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen rund um Bitdefender 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 Bitdefender Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Knowledge Base ist jederzeit unter der Internet Adresse http://kb.bitdefender.de erreichbar.

27.2. Nach Hilfe fragen

27.2.1. Zur Web-Selbstbedienung gehen

Fragen zur Installation? Montags bis Freitags von 08.00 Uhr bis 20.00 Uhr stehen Ihnen unsere deutschsprachigen Techniker kostenfrei gerne zur Verfügung.

Bitte folgen Sie den Links:

Deutsch

http://www.bitdefender.com/de/KnowledgeBase/

Englisch

http://www.bitdefender.com/site/KnowledgeBase/

Französisch

http://www.bitdefender.com/fr/KnowledgeBase/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/

27.2.2. Ein Supportticket öffnen

Wenn Sie ein Supportticket und Hilfe per EMail erhalten möchten, folgen Sie einem der folgenden Links:

Deutsch: http://www.bitdefender.de/site/Main/contact/1/
English: http://www.bitdefender.com/site/Main/contact/1/
French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

27.3. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell.Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

27.3.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Technische Unterstützung: support@bitdefender.de
Dokumentationdocumentation@bitdefender.com
Partner Proogramm: vertrieb@bitdefender.de
Marketing: marketing@bitdefender.de
Media Relationspresse@bitdefender.de
Jobs: jobs@bitdefender.de
Virus Einsendungen: virus_submission@bitdefender.com
Spam Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Produkt Webseite: http://www.bitdefender.de
Produkt ftp Archive: http://www.bitdefender.de
Local distributors: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.de

27.3.2. 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

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Hotline: +49 2301 91 84 555

Technische Beratung: support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: http://www.bitdefender.de

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Telefon: 1-954-776-6262
Web: http://www.bitdefender.com

Technischer Support (Nur registrierte Benutzer):
- E-mail: support@bitdefender.de
- Telefon (gebührenfrei):
  - USA: 1-888-868-1873
  - Kanada: 1-866-947-1873

Kundenservice (Nur registrierte Benutzer):
- E-mail: customerservice@bitdefender.com
- Telefon (gebührenfrei):
  - USA: 1-888-868-1873
  - Kanada: 1-866-947-1873

Großbritannien und Irland

Business Center 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Tel: +40 21 - 233 07 80
Emailsupport@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: http://www.bitdefender.co.uk
Technische Unterstützung: 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
Tel: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street
Tettnang
Technische Unterstützung: support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Tel.: +40 21 3001226; +40 21 3001227; +40 21 3001228; +40 21 3001229
Fax: +40 21 2641799
Produkt Webseite: http://www.bitdefender.de

BitDefender Notfall CD

28. Übersicht

BitDefender Internet Security 2009 verfügt über eine bootfähige CD-ROM (BitDefender Notfall CD) 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.

Die BitDefender Notfall CD 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. Ausserdem kann er verwendet werden um Daten wiederherzustellen wenn Windows nicht mehr startet.

Anmerkung
Die BitDefender Rescue CD kann unter folgendem Link heruntergeladen werden: http://download.bitdefender.com/rescue_cd/

28.1. Systemanforderungen

Bevor Sie die BitDefender Notfall CD 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
512 MB Arbeitsspeicher (1 GB empfohlen)

CD-ROM
CD-Rom-Laufwerk und die BIOS-Einstellungen, um von CD zu booten.

Internetverbindung
Obwohl die BitDefender Notfall CD 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
Standard SVGA-kompatible Grafikkarte.

28.2. Integrierte Software

Die Bitdefender Notfall CD enthält die folgenden Software-Pakete.

Xedit
Dies ist ein Texteditor.

Vim
Hierbei handelt es sich um einen mächtigen Texteditor mit Syntax hervorhebung, GUI und vielem mehr. Für mehr Informationen besuchen Sie die Vim Webseite.

Xcalc
Ist ein Taschenrechner.

RoxFiler
RoxFiler ist ein schneller grafischer Dateimanager.

Für weitere Informationen besuchen Sie die RoxFiler Webseite.

MidnightCommander
GNU Midnight Commander (mc) ist ein textbasierender Dateimanager.

Für mehr Informationen besuchen Sie die MC Webseite.

Pstree
Pstree zeigt die laufenden Prozesse an.

Top
Top zeigt die Linux Tasks an.

Xkill
Xkill beendet einen Client nach seinen X-Quellen.

Partition Image
Partition Image hilft Ihnen dabei EXT2, Reiserfs, NTFS, HPFS, FAT16, und FAT32 Dateisysteme in Imagedateien zu sichern. Dieses Programm kann für Backupzwecke sinnvoll sein.

Für weitere Informationen besuchen Sie die Partimage Webseite.

GtkRecover

GtkRecover ist eine grafische Version des Konsolenprogramms Recover. Es hilft Ihnen beim Sichern von Dateien.

Für mehr Informationen besuchen Sie die GtkRecover Webseite.

ChkRootKit

ChkRootKit ist ein Programm welches Ihnen bei der Suche nach Rootkits hilft.

Für mehr Informationen besuchen Sie die ChkRootKit Webseite.

Nessus Network Scanner

Nessus ist ein Remote-Sicherheitsscanner für Linux, Solaris, FreeBSD, und Mac OS X.

Für weitere Informationen besuchen Sie die Nessus Webseite.

Iptraf

Iptraf ist eine IP Netzwerk-Monitoring Software.

Für weitere Informationen besuchen Sie dieIptraf Webseite.

Iftop

Iftop zeigt die verwendete Bandbreite für eine Schnittstelle an.

Für mehr Informationen besuchen Sie die Iftop Webseite.

MTR

MTR ist ein Netzwerkdiagnose-Tool.

Für weitere Informationen besuchen Sie dieMTR Webseite.

PPPStatus

PPPStatus zeigt Statistiken zum ein- und ausgehenden TCP/IP Verkehr.

Für weitere Informationen besuchen Sie die PPPStatus Webseite.

Wavemon

Wavemon ist eine Montoring-Anwendung für Kabellose Netzwerke.

Für mehr Informationen besuchen Sie die Wavemon Webseite.

USBView

USBView zeigt Informationen über angeschlossene USB Geräte.

Für mehr Informationen besuchen Sie die USBView Webseite.

Pppconfig

Pppconfig hilft bei der automatischen Erstellung einer PPP-Wahlverbindung.

DSL/PPPoe

DSL/PPPoe konfiguriert eine PPPoE (ADSL) Verbindung.

I810rotate

I810rotate aktiviert den Video Output auf i810 Hardware unter Verwendung von i810switch(1).

Für weitere Informationen besuchen Sie die I810rotate Webseite.

Mutt

Mutt ist ein mächtiger textbasierender MIME Mail Client.

Für weitere Informationen besuchen Sie die Mutt Webseite.

Mozilla Firefox

Mozilla Firefox ist ein bekannter Internet Browser.

Für weitere Informationen besuchen Sie die Mozilla Firefox Webseite.

Elinks

Elinks ist ein textbasierter Internet Browser.

Für weitere Informationen besuchen Sie die Elinks Webseite.

29. BitDefender Notfall CD Anleitung

Dieses Kapitel enhält Informationen darüber wie Sie die BitDefender Notfall CD starten und stoppen, zum Prüfen auf Schädlinge sowie zum Sichern von Daten verwenden können. Mit den in der BitDefender Notfall CD enthaltenen Programmen erhalten Sie mächtige Werkzeuge auf welche wir leider nicht alle eingehen können.

29.1. BitDefender Notfall CD 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 BitDefender Notfall CD Startbildschirm angezeigt. Folgen Sie nun bitte den auf dem Bildschirm angegebenen Schritten.

Anmerkung
Wählen Sie aus der Liste die Sprache die Sie für die Notfall CD verwenden möchten

LinuxDefender Startbildschirm

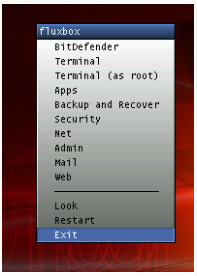
Nach dem Starten wird automatisch ein Virensignaturupdate durchgeführt. Dieser Vorgang kann einen gewissen Zeitraum in Anspruch nehmen.

Sobald der Bootvorgang abgeschlossen wurde, wird der Desktop angezeigt. Sie können nun damit beginnen die BitDefender Notfall CD zu verwenden.

Der LinuxDefender Desktop

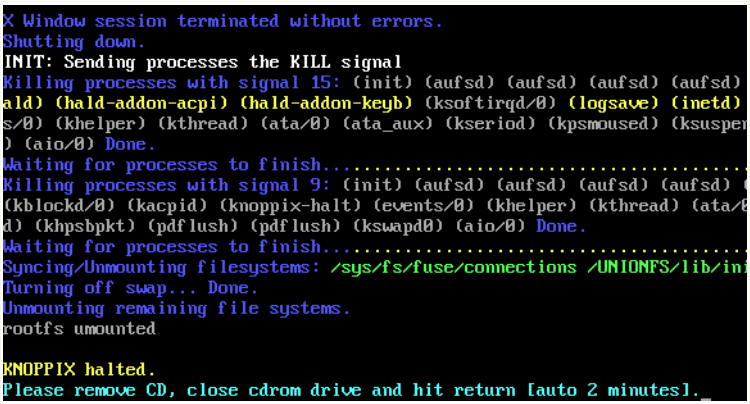
29.2. BitDefender Notfall CD stoppen

Sie können der Computer sicher herunterfahren indem Sie den Menüpunkt **Exit** im Kontextmenü (Rechtsklick) wählen. Alternativ verwenden Sie das **halt** Kommando im Terminal.



Wählen Sie "EXIT"

Sobald die BitDefender Notfall CD alle Programme beendet hat, bekommen Sie das folgende Bild angezeigt. Sobald dieses angezeigt wird, können Sie die CD aus dem Laufwerk entfernen, den Einschub schließen und den Computer neu starten.



Warten auf diese Nachricht, wenn der Rechner heruntergefahren wird

29.3. Wie führe ich einen Prüfvorgang durch?

Nachdem der Rechner gestartet wurde wird ein Assistent geöffnet welcher Ihnen hilft einen vollständigen Prüfvorgang Ihres Rechners durchzuführen. Alles was Sie tun müssen ist auf die **Start** Schaltfläche zu klicken.

Anmerkung
Wenn Ihre Bildschirmauflösung nicht hoch genug ist werden Sie gefragt ob Sie im Textmodus starten möchten.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

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

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

2. Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.

   Die Risiken werden in Gruppen angezeigt. Klicken Sie auf "+", um eine Gruppe zu öffnen, und auf "-", um diese wieder zu schließen.

Sie können eine Globale Aktion für jede Gruppe auswählen oder Sie können für jedes Risiko eine eigene Aktion angeben.

3. Ihnen wird eine Zusammenfassung angezeigt.

Wenn Sie ein bestimmtes Verzeichniss prüfen möchten dann befolgen Sie die folgenden Schritte:

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**.

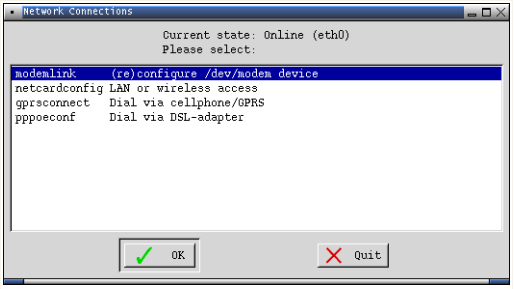
Oder Sie können den folgenden Befehl als Root von einem Terminal ausgeben. Der **BitDefender Antivirus-Scanner** beginnt mit der ausgewählten Datei oder Pfad als Default-Position zu scannen.

```
# bdscan /path/to/scan/
```

29.4. Wie kann ich die 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. Doppelklicken Sie auf die Verknüpfung für Netzwerkverbindungen auf Ihrem Arbeitsplatz. Das folgende Fenster erscheint.



Netzwerkverbindungen

2. Wählen Sie die Verbindung, die Sie verwenden und klicken Sie auf OK.

Verbindung	Beschreibung
modemlink	Wählen Sie diese Verbindung, wenn Sie ein Modem und eine Telefonleitung verwenden um eine Verbindung zum Internet herzustellen.
netcardconfig	Wählen Sie diese Verbindung, wenn Sie über ein LAN-Netzwerk die Verbindung zu dem Internet herstellen. Dies gilt auch für drahtlose Verbindungen.
gprsconnect	Wählen Sie diese Verbindung, wenn Sie über ein Handynetzwerk unter Verwendung eines GPRS (General Packet Radio Service) Protokolls eine Verbindung zu dem Internet herstellen. Sie können auch ein GPRS-Modem anstelle eines Handys verwenden.
pppoeconf	Wählen Sie diese Verbindung, wenn Sie über ein DSL-Modem eine Verbindung mit dem Internet herstellen.

3. Folgen Sie den Instruktionen auf dem Bildschirm. Wenn Sie nicht sicher sein sollten was Sie schreiben sollen, konsultieren Sie Ihren Netzwerkadministrator.

Wichtig
Bitte achten Sie darauf, dass Sie nur mit den oben genannten Optionen das Modem aktivieren. Um die Netzwerkverbindung zu konfigurieren, befolgen Sie diese Schritte.

1. Klicken Sie mit der rechten Maustaste auf den Desktop. Das Kontextmenu der BitDefender Rescue CD erscheint.
2. Wählen Sie **Terminal (als Root)**.
3. Geben Sie die folgenden Befehle ein:

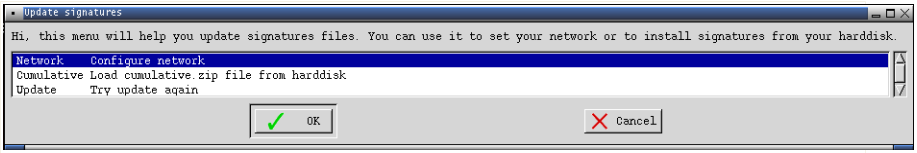
```
# pppconfig
```

4. Folgen Sie den Instruktionen auf dem Bildschirm. Wenn Sie nicht sicher sein sollten was Sie schreiben sollen, konsultieren Sie Ihren Netzwerkadministrator.

29.5. Wie kann ich BitDefender aktualisieren?

Nach dem Starten wird automatisch ein Virensignaturupdate durchgeführt. Wenn Sie diesen Schritt jedoch übersprungen haben, können Sie hier erfahren wie BitDefender aktualisiert werden kann.

1. Doppelklicken sie auf die Verknüpfung für Signatur-Updates auf dem Arbeitsplatz. Das folgende Fenster erscheint.



Signatur-Updates

2. Sie können hierzu eine der folgenden Methoden wählen:
   - Klicken Sie auf **Gesammelt** um Signaturen zu installieren die sich bereits auf Ihrer Festplatte befinden, indem Sie Ihren Computer durchsuchen und die Datei`cumulative.zip` laden.
   - Wählen Sie **Update** um eine sofortige Verbindung mit dem Internet herzustellen und die aktuellsten Virensignaturen herunterzuladen.
3. Klicken Sie auf **OK**.

29.5.1. Wie kann ich BitDefender über einen Proxy-Server aktualisieren?

Wenn ein Proxy-Server zwischen Ihrem Computer und dem Internet besteht, müssen einige Einstellungen vorgenommen werden, um die Erkennung von Virenstrukturen zu aktualisieren.

Um BitDefender über einen Proxy-Server zu aktualisieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie mit der rechten Maustaste auf den Desktop. Das Kontextmenu der BitDefender Rescue CD erscheint.
2. Wählen Sie **Terminal (als Root)**.
3. Geben Sie folgenden Befehl ein: **cd /ramdisk/BitDefender-scanner/etc**.
4. Geben Sie folgenden Befehl ein: **mcedit bdscan.conf** to edit this file by using GNU Midnight Commander (mc).

5. Kommentieren Sie die folgende Zeile aus: `#HttpProxy =` (löschen Sie nur das Zeichen `#`), und geben Sie die Domain, den Benutzernamen, das Passwort und den Server-Port des Proxy-Servers ein. Die entsprechende Zeile muss beispielsweise so aussehen:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Drücken Sie **F2** um die aktuelle Datei zu speichern und drücken Sie dann **F10** um Sie zu schließen.
7. Geben Sie folgenden Befehl ein: **bdscan update**.

29.6. Wie sichere ich meine Daten?

Nehmen wir einmal an das Sie Ihre Betriebssystem aus unbekannten Gründen nicht mehr starten können. Sie jedoch dringend wichtigen Daten von Ihrem Computer benötigen. Hier kann Ihnen die BitDefender Notfall CD behilflich sein.

Um Ihre Daten von Ihrem Computer auf einen Wechseldatenträger, wie z.B. einen USB Stick zu sichern befolgen Sie die folgenden Schritte:

1. Legen Sie die BitDefender Notfall CD in das CD-Laufwerk, stecken Sie den USB Stick ein und starten Sie dann Ihren Computer neu.

   Anmerkung
   Wenn Sie den USB Stick später verbinden müssen Sie das externe Gerät mit den folgenden Schritte mounten:
   a. Klicken Sie auf die Verknüpfung Terminal Emulator auf dem Arbeitsplatz.
   b. Geben Sie den folgenden Befehl ein:

   ```
   # mount  /media/sdb1
   ```

   Bitte beachten Sie, dass dies je nach Ihrer Computerkonfiguration `sda1` anstelle von `sdb1` sein kann.

2. Warten Sie bis die BitDefender Notfall CD gestartet wurde. Das folgende Fenster erscheint.

Der Desktop

3. Doppelklicken Sie die Partition auf welcher die Daten gespeichert sind (z.B. `[sda3]`).

Anmerkung

Wenn Sie mit der BitDefender Notfall CD arbeiten werden Sie mit Linux-Partitionsnamen in Kontakt kommen. So kann `[sda1]` zum Beispiel für Laufwerk `(C:)` Ihrer Windows Partition stehen, `[sda3]` für `(F:)`, und `[sdb1]` für den USB Stick.

Wichtig

Wenn der Computer nicht ordnungsgemäß heruntergefahren wurde, kann es sein, dass bestimmte Partitionen nicht automatisch gemountet wurden. Um eine Partition zu mounten, befolgen Sie diese Schritte.

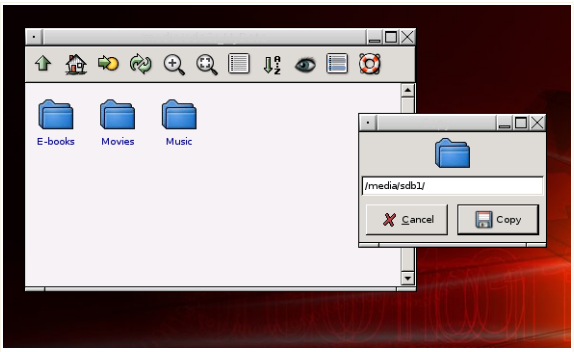
a. Klicken Sie auf die Verknüpfung Terminal Emulator auf dem Arbeitsplatz.

b. Geben Sie den folgenden Befehl ein:

```
# mount /media/partition_name
```

4. Durchsuchen Sie die Partitionen nach den gewünschten Dateien und Ordnern. Für Instanz, `Meine Daten` enthält `Filme`, `Musik` und `E-books` Sub-Datenverzeichnisse.

5. Rechtsklicken Sie den gewünschten Ordner und wählen Sie **Copy**. Das folgende Fenster erscheint.



Daten speichern

6. Tippen Sie `/media/sdb1/` in das vorgesehene Feld und klicken Sie dann auf **Copy**.

   Bitte beachten Sie, dass dies je nach Ihrer Computerkonfiguration `sda1` anstelle von `sdb1` sein kann.

Glossar

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

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.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

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

Backdoor (Hintertür)

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

Bootsektor

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

Bootvirus

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

Durchsuchen

Kurzform für Web-Browser, eine 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

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.

Ereignisanzeige

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

Fehlalarm

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.

Script

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

Spam

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

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten 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.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet).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.