bitdefender

GAMESAFE

Benutzerhandbuch

Copyright© 2008 BitDefender

BitDefender GameSafe
Benutzerhandbuch

Veröffentlicht 2008.06.12

Copyright© 2008 BitDefender

Rechtlicher Hinweis

Keine Bestandteile dieses Handbuches dürfen in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jeglicher anderer Form von Datenspeicherung oder Informationswiederbeschaffung, ohne die Zustimmung von BITDEFENDER. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt bzw. Dokument ist urheberrechtlich geschützt. Die inhaltlichen Informationen in diesem Dokument sind faktenbasiert und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für eventuell auftretende Schäden bzw. Datenverlust die direkt oder indirekt unter Verwendung dieses Dokumentes entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von BITDEFENDER erstellte Webseiten, die auch nicht von BITDEFENDER kontrolliert werden. Somit übernimmt BITDEFENDER auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. BITDEFENDER stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass BITDEFENDER in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

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


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.

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 KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN, DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test, etc.).

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

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

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

Ist oder wird eine Bestimmung dieses Vertrageswegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam 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 eingetrageneTitel und Marken von BITDEFENDER. Alle anderen Marken und Titel sind Eigentümer 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.

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

Vorwort

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

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

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

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

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

1.2. Warnungen

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

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

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

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

2. Struktur

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 GameSafe** 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 Konfiguration. Eine detaillierte Beschreibung der Sicherheitsfähigkeiten von BitDefender. Die Abschnitt beschreibt ausführlich alle Optionen der erweiterten Einstellungs-Konsole Ihnen wird beigebracht wie Sie die BitDefender Module einstellen und verwenden um Ihren Computer gegen alle Arten von Malware zu schützen (Virus, Spyware, Rootkits und so weiter).

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

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

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

3. Ihre Mithilfe

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

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

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

Installation

1. Installation von BitDefender GameSafe

Der Abschnitt **Installation von BitDefender GameSafe** beschreibt die folgenden Themen:

- Systemanforderungen
- Installationsschritte
- Der Regelassistent
- Upgrade von einer vorherigen Version
- Reparieren oder Entfernen von BitDefender

1.1. Systemanforderungen

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

- Betriebssysteme: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (oder höher)

Windows 2000

- 800 MHz oder schneller
- Mindestens 256 MB Arbeitsspeicher (512 MB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte

Windows XP

- 800 MHz oder schneller
- Mindestens 256 MB Arbeitsspeicher (1 GB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte

Windows Vista

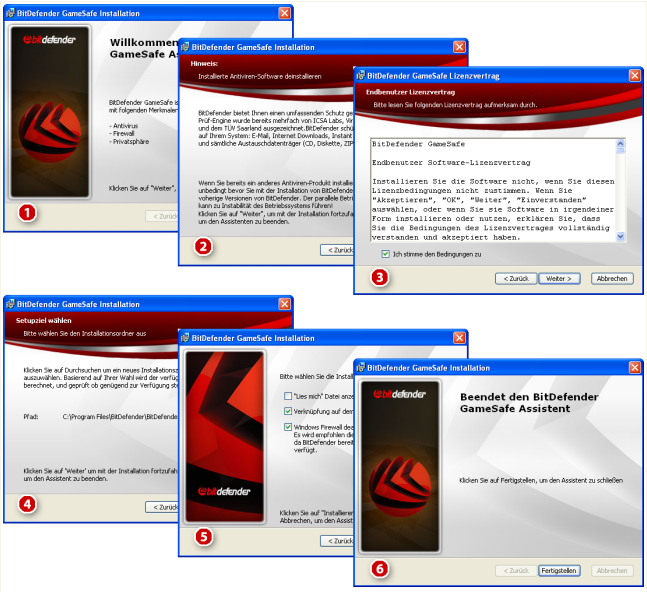
- 800 MHz oder schneller
- 512 MB Arbeitsspeicher (1 GB empfohlen)
- 60 MB freier Speicherplatz auf der Festplatte

BitDefender GameSafe kann als Testversion auf der Webseite von BitDefender heruntergeladen werden: http://www.bitdefender.de.

1.2. Installationsschritte

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 GameSafe zu installieren:

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

   BitDefender weist Sie daraufhin, falls Sie 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 Lizenzbedingungen, wählen Sie die Option **Ich stimme den Lizenzbedingungen zu**, und klicken Sie auf **Weiter**. Wenn Sie den Lizenzbestimmungen nicht zustimmen, klicken Sie auf **Abbrechen**. Der Installationsprozess wird abgebrochen und das Setup-Programm beendet.
4. Standardmäßig wird BitDefender GameSafe im Ordner `C:\Programme\BitDefender\BitDefender 2008` installiert. Wenn Sie den Installationpfad ändern möchten, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner in dem Sie den BitDefender GameSafe 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.
   - **Speichern eines Symbols auf Ihrem Desktop** - um ein Symbol am Ende der Installation auf Ihrem Desktop zu speichern.
   - **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 den window-seigene Firewall zu deaktivieren.

Wichtig
Wir empfehlen die windows-basierte Firewall zu deaktivieren. BitDefender GameSafe 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.

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

6. Klicken Sie auf **Fertigstellen**. Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setup-Assistent den Installationsprozess beenden kann. Das sollten Sie so schnell wie möglich tun.

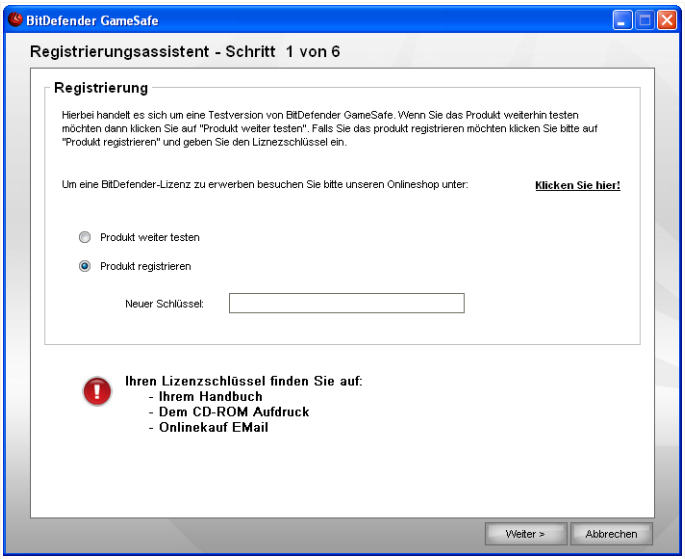
   Wenn Sie die Standardeinstellungen für den Installationspfad übernommen haben, so finden Sie unter `Programme/Dateien`einen neuen Ordner mit dem Namen `BitDefender` der den Unterordner `BitDefender 2008` beinhaltet.

1.3. Einrichtungs-Assistent

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

Den Assistenten abzuschließen ist nicht verpflichtend. Wie auch immer, Sie ich entscheiden.Wir empfehlen Ihnen das Abscließen, um Ihnen Zeit zu sparen und Ihr System zu sichern selbst bevor Sie BitDefender installiert haben.

1.3.1. Schritt 1/6 - BitDefender GameSafe registrieren



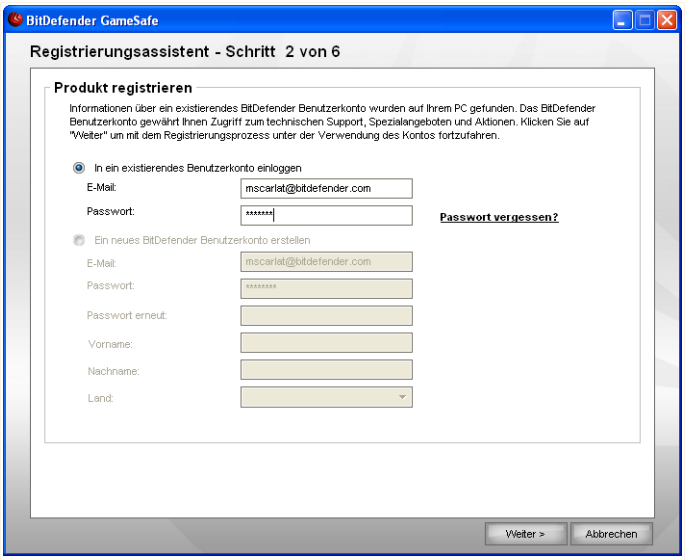
Registrierung

Wählen Sie **Produkt registrieren** , um **BitDefender GameSafe** zu registrieren. Tragen Sie den neuen Schlüssel in das Eingabefeld ein.

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

Klicken Sie auf **Weiter**.

1.3.2. Schritt 2/6 - BitDefender-Benutzerkonto erstellen



Kontoerstellung

Ich habe noch kein BitDefender-Benutzerkonto

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

Anmerkung
Wenn Sie dieses Konto später erstellen möchten, markieren Sie die entsprechenden Option.

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.

Anmerkung
Das Passwort sollte mindestens 4 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.

Klicken Sie auf **Weiter**.

Ich habe bereits ein BitDefender Nutzerkonto.

BitDefender weist Sie daraufhin, falls bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert wurde. In diesem Fall müssen Sie nur auf **Weiter** klicken.

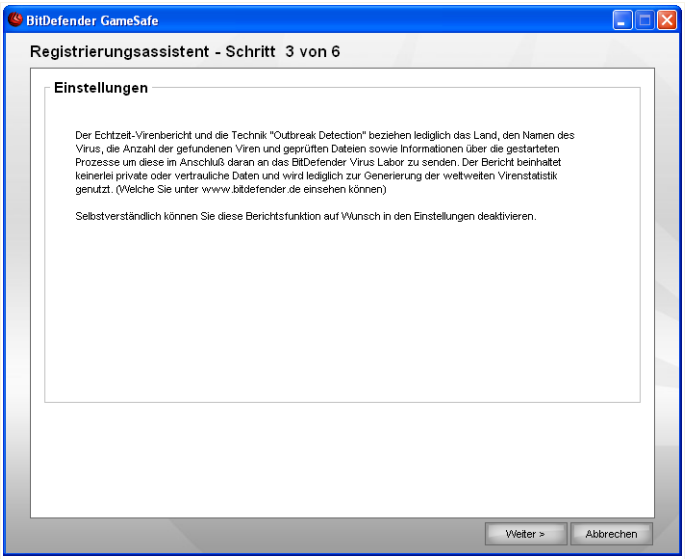
Wenn Sie bereits ein aktives Benutzerkonto besitzen, BitDefender es jedoch nicht entdeckt, wählen Sie **In ein bestehendes BitDefender-Benutzerkonto einloggen** und geben Sie die E-Mail Adresse und das Passwort Ihres Benutzerkontos ein.

Anmerkung
Wenn Sie ein falsches Passwort eingeben, so werden Sie dazu aufgefordert es erneut anzugeben sobald Sie auf **Weiter** klicken. Klicken Sie auf **Ok** um das Passwort erneut einzugeben. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

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

Klicken Sie auf **Weiter**.

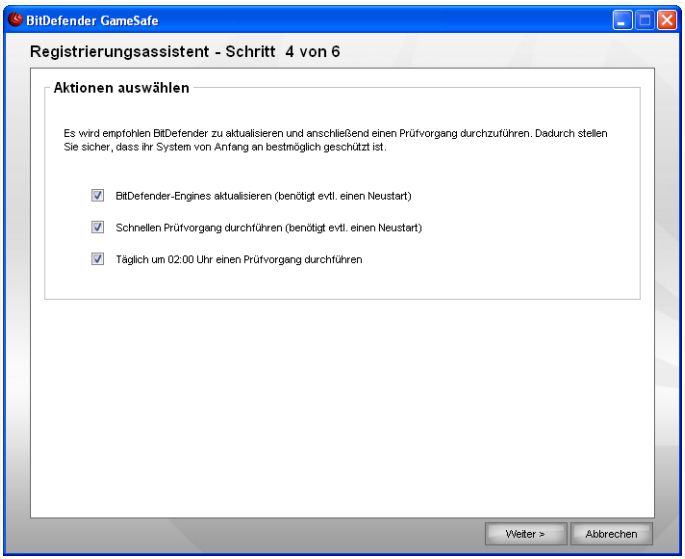
1.3.3. Schritt 3/6 - Informationen über RTVR



System-Informationen

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

1.3.4. Schritt 4/6 - Aufgaben



Auswahl für Aktionen

Nehmen Sie hier die BitDefender Sicherheitseinstellungen für Ihr System vor.

Folgende Optionen stehen zur Verfügung:

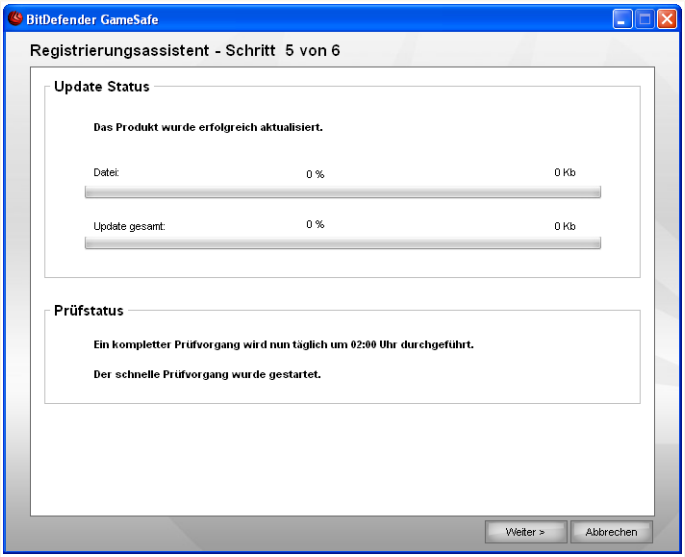
- **Update der BitDefender-Engine (möglicherweise mit Neustart)** - Beim nächsten Schritt wird ein Update der BitDefender-Engine durchgeführt, um Ihren Computer gegen aktuelle Gefahren zu schützen.
- **Schnelle Systemprüfung (erfordert möglicherweise einen Neustart)** - Während des nächsten Schrittes 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 Freitag zur angegebenen Uhrzeit einen Prüfvorgang aus.

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

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

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

1.3.5. Schritt 5/6 - Durchführen der Aufgaben

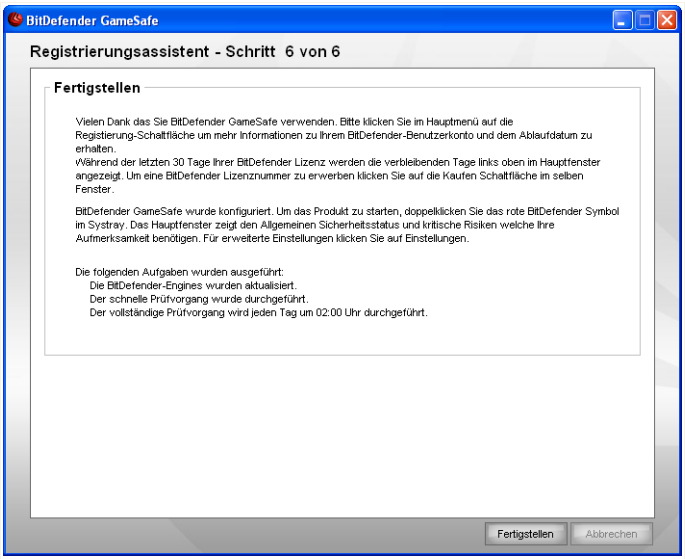


Status

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

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

1.3.6. Schritt 6/6 - Aufgabenübersicht



Fertigstellen

Dies ist der letzte Schritt des Einrichtungsassistenten.

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

1.4. Upgrade

Die Prozedur für das Upgrade kann über zwei Schritte erfolgen:

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

Deinstallieren Sie zunächst die Vorgängerversion. Starten Sie dann den Computer neu und installieren Sie die neue Version wie im Abschnitt „*Installationsschritte*“ (S. 3) beschrieben.

1.5. BitDefender reparieren oder entfernen

Wenn Sie das Programm **BitDefender GameSafe** reparieren oder entfernen möchten, gehen Sie über das Windows-Startmenü wie folgt vor: **Start** → **Programme** → **BitDefender 2008** → **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 GameSafe 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 des BitDefender GameSafe 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**.

Anmerkung
Nachdem die Deinstallation beendet wurde empfehlen wir Ihnen den Ordner `BitDefender` im Ordner `Programme` zu löschen.

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

2. Erste Schritte

Nachdem Sie BitDefender installiert haben ist Ihr PC geschützt. Sie können den BitDefender Sicherheitscenter jederzeit öffnen um den Sicherheitstatus zu prüfen, vorsorgliche Massnahmen durchzuführen oder das Produkt zu konfigurieren.

Sie erreichen den BitDefender Sicherheitscenter über das Windows-Startmenü: **Start → Programme → BitDefender 2008 → BitDefender GameSafe**. Schneller geht es jedoch mittels Doppelklick auf das **BitDefender Symbol** in der Systemleiste.

BitDefender Sicherheitscenter

Das BitDefender Sicherheitscenter enthält zwei Bereiche:

- Der **Sicherheitsstatus** Bereich: Enthält Informationen über Sicherheitsrisiken auf Ihrem Computer und hilft Ihnen diese zu beheben. Die Status-Zeile zeigt Ihnen wieviele Risiken Ihren Computer betreffen. Durch einen Klick auf die rote **Alle beheben** Schalftfläche werden die Risiken direkt behoben oder Sie werden zur Behebung geführt. Gleichzeitig sind vier Status-Schaltflächen für die unterschiedlichen Sicherheitsbereiche verfügbar. Eine grüne Status-Schaltfläche

steht für "keine Sicherheitsrisiken". Eine gelbe oder rote Schaltfläche steht für "mittlere oder hohe Sicherheitsrisiken". Um diese zu beheben klicken Sie auf die entsprechende Schaltfläche und dann auf die **Beheben** Schaltfläche. Einer nach dem anderen, oder alle zusammen durch klicken auf **Alle beheben**. Grau signalisiert ein nicht konfiguriertes Modul.

- Der **Schnellmaßnahmen** Bereich: Hilft Ihnen dabei ihr System sauber und geschützt zu halten.

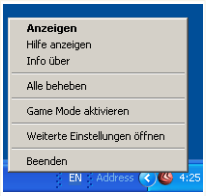
Ausserdem enthält der BitDefender Sicherheitscenter mehrere nutzliche Verknüpfungen.

Verweise	*Beschreibung*
Kaufen	Öffnet eine Seite wo Sie das Produkt erwerben können.
Benutzerkonto	Öffnet Ihr BitDefender Benutzerkonto.
Registrieren	Öffnet den Registrierungs-Assistenten.
Hilfe	Öffnet die Hilfedatei.
Support	Öffnet die BitDefender Support Webseite
Einstellungen	Öffnet die Einstellungen-Konsole
Ereignise	Öffnet ein Fenster mit den BitDefender Ereignisen

2.1. BitDefender-Symbol im System-Tray

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

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



BitDefender Symbol

- **Anzeigen** - Öffnet den BitDefender Sicherheitscenter.
- **Hilfe** - Öffnet die Hilfedatei.
- **Über** - Öffnet die BitDefender Webseite.
- **Alle beheben** - Hilft Ihnen bei der Behebung von Sicherheitsrisiken.
- **Spielmodus ein-/ausschalten** - aktiviert/deaktiviert den Spielmodus.
- **Weitere Einstellungen öffnen** - Öffnet die erweiterten Einstellungen.

- **Jetzt Aktualisieren** - ein Update wird unverzüglich durchgeführt. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.
- **Beenden** - Beendet BitDefender.

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.

2.2. Aktivitsänzeige

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

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

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

Aktivitäsanzeige

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

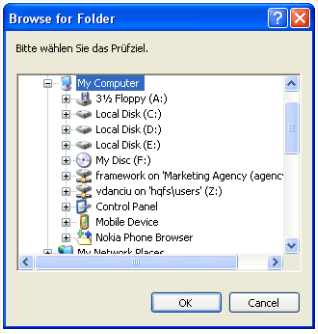
Sie können die **Aktivitätsanzeige** zum Prüfen von Objekten verwenden. Ziehen Sie die Objekte hierzu einfach mit der Maus auf die Anzeige und lassen Sie diese dann los. Für weitere Informationen fahren Sie bitte fort mit *„Prüfen per Drag & Drop“* (S. 66).

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**. Um das Fenster komplett verschwinden zu lassen klicken Sie in der **Einstellungskonsole** auf **Erweitert** und entfernen Sie das Häckchen bei **Aktivitätsanzeige**.

2.3. 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 2008 → 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 erscheint und führt Sie durch den Scanprozess.

2.4. Spielmodus

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:

- Alle BitDefender Alarme und Pop-ups werden deaktiviert.
- Der Echtzeit-Schutz wird auf **Tolerant** gestellt.
- Die BitDefender Firewall ist für den **Spielmodus** eingestellt.

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

2.4.1. 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 `Alt+G` (Standard-Tastenkombination)

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

2.4.2. Tastenkombination für Spielmodus ändern

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

1. Klicken Sie auf **Einstellungen** im BitDefender Security Center um das Einstellungsfenster zu öffnen.

   Anmerkung
   Sie können auch mit der rechten Maustaste auf das BitDefender-Symbol im System-Tray klicken und **Erweiterte Einstellungen öffnen** wählen.

2. Klicken Sie auf **Erweitert**.
3. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination für Spielmodus 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 für Spielmodus aktivieren** entfernen, wird die Tastenkombination deaktiviert.

3. Sicherheitsstatus

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

Es gibt vier Sicherheitsstatus-Schaltflächen:

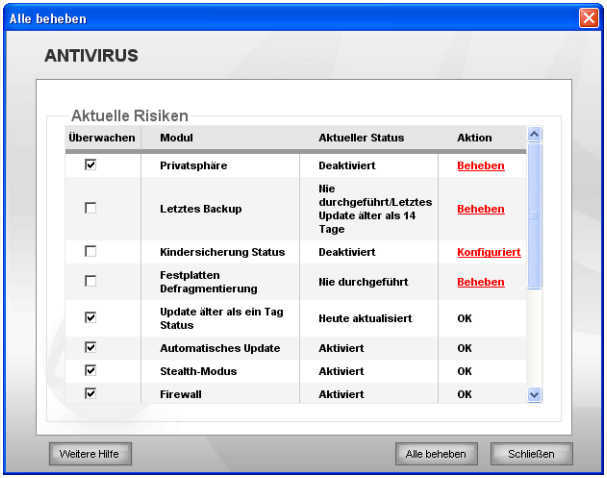
- **PC SICHERHEIT**
- **NETZWERKSICHERHEIT**
- **IDENTITÄTSKONTROLLE**

Links neben diesen zeigt Ihnen die Statuszeile die Anzahl von Risiken welche Ihr System betreffen und eine rote **Alle beheben** Schaltfläche.

Die vier Schaltflächen können je nach Sicherheitsstatus die Farben grün, gelb, rot oder grau annehmen.

- **Grün** steht für ein niedriges Sicherheitsrisiko für Ihren Computer.
- **Gelb** signalisiert ein mittleres Sicherheitsrisiko für Ihren Computer.
- **Rot** signalisiert ein hohes Sicherheitsrisiko für Ihren Computer.
- **Grau** signalisiert ein nicht konfiguriertes Modul.

Das Beheben von Sicherheitsrisiken bedarf keiner Anstrengung und kann durch einen einfachen Klick auf **Alle beheben** durchgeführt werden. Ein neues Fenster wird sich öffnen.



Sicherheitsrisiken

Sie werden eine Liste mit den Sicherheitsrisiken und einer Kurzbeschreibung angezeigt bekommen.

Um ein bestimmtes Risiko zu beheben klicken Sie auf die entsprechende **Beheben** Schaltfläche. Dies wird das Problem direkt beheben oder Ihnen die nötigen Schritte aufzeigen. Wenn Sie sich entscheiden alle Risiken zu beheben so klicken Sie auf **Alle beheben** und befolgen Sie die weiteren Anweisungen.

Wenn Sie weiterführende Hilfe benötigen, klicken Sie auf die Schaltfläche **Weitere Hilfe** die sich am unteren Rand des Fensters befindet. Es wird eine Kontexthilfe angezeigt, in der Sie detaillierte Informationen über ein Problem und seine Lösung erhalten.

Wichtig

Für jedes Sicherheitsrisiko existiert ein Auswahlfeld, welches standardmässig aktiviert ist. Wenn Sie ein bestimmtes Risiko nicht mehr angezeigt bekommen möchten dann entfernen Sie das entsprechende Häckchen. Bitte verwenden Sie diese Möglichkeit mit Vorsicht, da Sie dadurch nicht mehr über die entsprechenden Risiken informiert werden.

Um die Risiken später zu beheben, klicken Sie auf **Schließen**.

3.1. PC Sicherheit Status-Schaltfläche

Wenn die Sicherheitsstatus-Schaltfläche grün ist gibt es nichts um sich sorgen zu machen. Sollte die Schaltfläche gelb, rot oder grau sein ist Ihr Computer einem mittleren oder hohen Sicherheitsrisiko ausgesetzt.

Die Farbe der Sicherheitsstatus-Schaltfläche kann sich nicht nur durch das Ändern von Einstellungen verändern sondern auch durch das Unterlassen von wichtigen Vorgängen, wie z.B. wird die Schaltfläche gelb wenn Sie lange keinen Prüfvorgang mehr durchgeführt haben. Oder rot wenn Sie sehr lange keinen Prüfvorgang mehr durchgeführt haben.

Die Tabelle zeigt Ihnen Informationen zu den möglichen Sicherheitsrisiken.

Risiko	*Farbe*
Der letzte Prüfvorgang ist lange her	Gelb
Der letzte Prüfvorgang ist sehr lange her	Rot
Der Echtzeitvirenschutz ist deaktiviert	Rot
Der Echtzeitvirenschutz ist auf Tolerant eingestellt	Gelb
Das Automatische Update ist deaktiviert	Rot
Das letzte Update fand vor einem Tag statt	Rot

Um alle Risiken zu beheben befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Sicherheitsstatus-Schaltfläche.
2. Klicken Sie entweder auf die **Beheben**-Schaltflächeum ein Risiko nach dem anderen zu beheben oder verwenden Sie die Schaltfläche **Alle beheben** um alle auf einmal zu beheben.
3. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

3.2. Netzwerksicherheit-Status Schaltfläche

Wenn die Netzwerksicherheit-Status Schaltfläche grün ist gibt es nichts um sich sorgen zu machen. Sollte die Schaltfläche gelb, rot oder grau sein ist Ihr Computer einem mittleren oder hohen Sicherheitsrisiko ausgesetzt.

Die Tabelle zeigt Ihnen Informationen zu den möglichen Sicherheitsrisiken.

Risiko	Farbe
Die Firewall ist deaktiviert	Rot
Der Stealth Modus ist deaktiviert	Rot
Die Kabellose Verbindung ist nicht gesichert	Rot

Um alle Risiken zu beheben befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Netzwerksicherheit-Status Schaltfläche.
2. Klicken Sie entweder auf die **Beheben**-Schaltflächeum ein Risiko nach dem anderen zu beheben oder verwenden Sie die Schaltfläche **Alle beheben** um alle auf einmal zu beheben.
3. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

3.3. Identitätskontolle-Status Schaltfläche

Wenn die Identitätskontrolle-Status Schaltfläche grün ist gibt es nichts um sich sorgen zu machen. Sollte die Schaltfläche rot oder grau sein ist Ihr Computer einem hohen Sicherheitsrisiko ausgesetzt.

Die Tabelle zeigt Ihnen Informationen zu den möglichen Sicherheitsrisiken.

Risiko	Farbe
Der Privatsphäreschutz wurde konfiguriert und AKTIVIERT	Grün
Der Privatsphäreschutz wurde konfiguriert und DEAKTIVIERT	Rot
Der Privatsphäreschutz wurde nicht konfiguriert	Grau

Um alle Risiken zu beheben befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Privatsphäre-Status Schaltfläche.
2. Klicken Sie entweder auf die **Beheben**-Schaltflächeum ein Risiko nach dem anderen zu beheben oder verwenden Sie die Schaltfläche **Alle beheben** um alle auf einmal zu beheben.
3. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

4. Schnellmaßnahmen

Unterhalb der vier Status Schaltflächen finden Sie den **Schnellmaßnahmen** Bereich.

4.1. Sicherheit

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

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

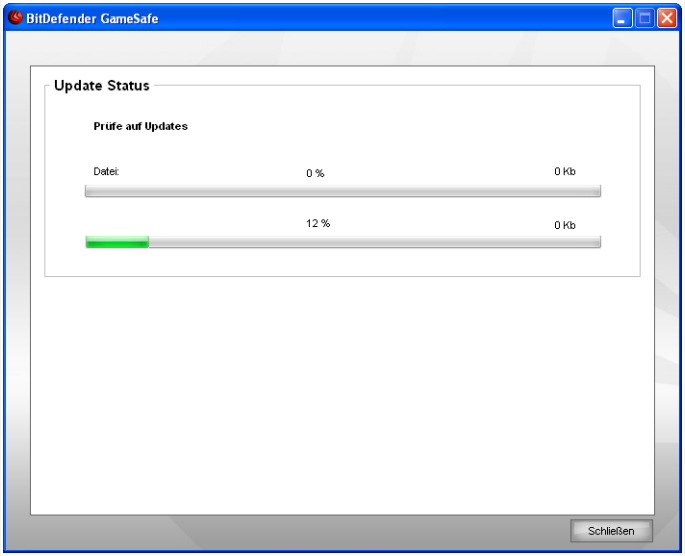
Folgende Aktionen stehen zur Verfügung:

- **Jetzt Aktualisieren** - ein sofortiges Update ird durchgeführt.
- **Eigene Dateien prüfen** - Führt eine schnelle Prüfung Ihrer Eigenen Dateien durch.
- **Tiefe Systemprüfung** - Prüft den gesamten Computer (inklusive Archiven)
- **Vollständige Systemprüfung** - Prüft den gesamten Computer (ohne Archive)

4.1.1. 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.

Als Standardeinstellung sucht BitDefender nach Updates, sobald Sie den Computer einschalten, und dann **jede Stunde** erneut. Wenn Sie den BitDefender aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren**. Der Update-Prozess wird gestartet und das folgende Fenster erscheint:



BitDefender Updaten

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

Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet 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 **Schließen**. Dadurch wird der Update-Prozess nicht gestoppt.

Anmerkung
Sollten Sie mit einer Einwahlverbindung mit dem Internet verbunden sein, so wird empfohlen regelmäßig ein manuelles Update durchzuführen.

Bitte starten Sie Ihren Computer neu wenn dies verlangt wird. Im Falle enes grundlegenden Updates werden Sie dazu aufgefordert den Computer neuzustarten. Wenn Sie nicht nochmals nach einem Neustart gefragt werden möchten dann wählen Sie **Auf Neustart warten und nicht nachfragen**. Somit wird das Produkt, beim nächsten Mal wenn ein Update einen Neustart erfordert, weiterhin mit den alten Dateien arbeiten, bis Sie das System selbst neustarten.

Klicken Sie auf **Neustarten** um Ihr System sofort neuzustarten.

Wenn Sie Ihr System später neustarten möchten, klicken Sie einfach auf **Ok**. Wir raten Ihnen Ihr System so bald wie möglich neuzustarten.

4.1.2. Scan mit BitDefender

Um Ihren Computer nach Malware zu durchsuchen, starten Sie einen Scanauftrag, inem Sie auf die entsprechende Schaltfläche klicken. Die folgende Tabelle zeigt Ihnen die verfügbaren Scanaufträge mit einer Kurzbeschreibung:

Auftrag	*Beschreibung*
Eigene Dateien prüfen	Nutzen Sie diesen Auftrag um die wichtigsten Ordner zu überprüfen: `Eigene Dateien`, `Desktop` und `StartUp`. Dies gewährleistet die Sicherheit Ihrer Dokumente, einen sicheren Arbeitsbereich und das korrekte Ausführen von Anwendungen.
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.

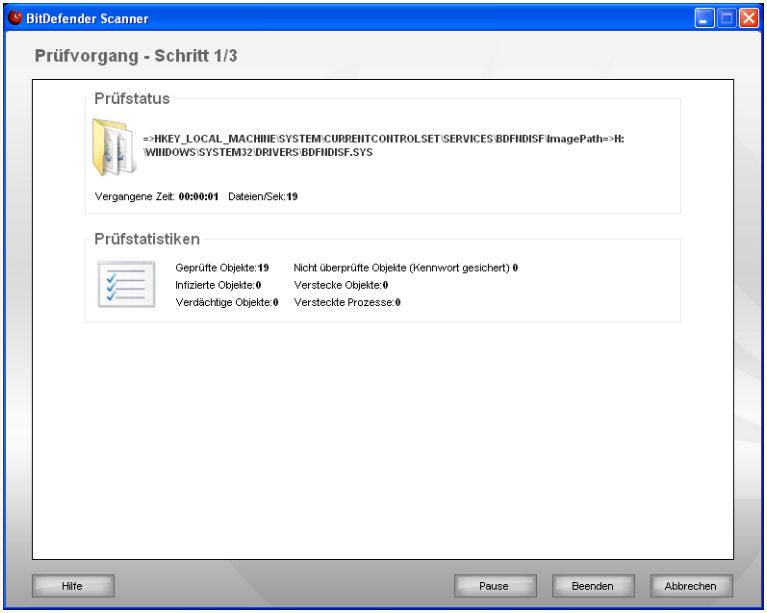
Anmerkung
Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

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.

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.

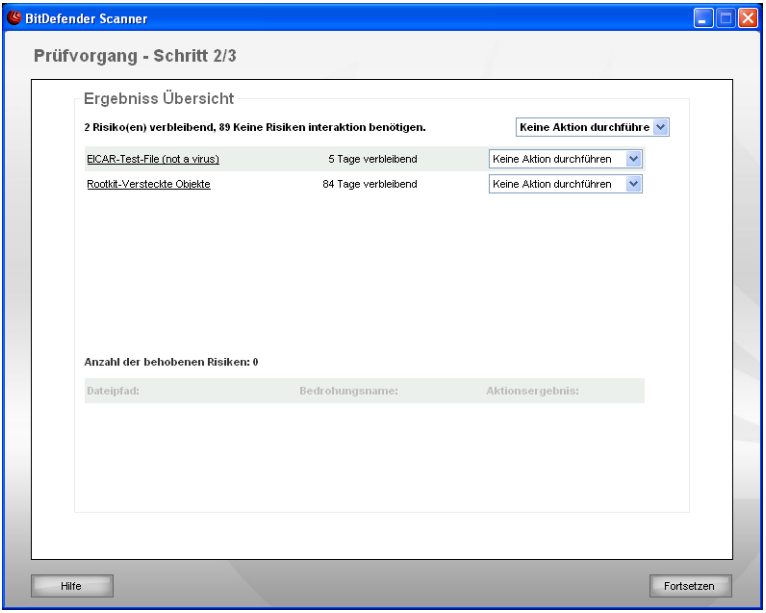
Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

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 der Malware mit der sie infiziert sind. Klicken Sie auf den Link, der sich auf die Gefährdung bezieht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine Globale Aktion für jede Gruppe auswählen oder Sie können für jedes Risiko eine eigene Aktion angeben.

Folgende Aktionen stehen zur Verfügung:

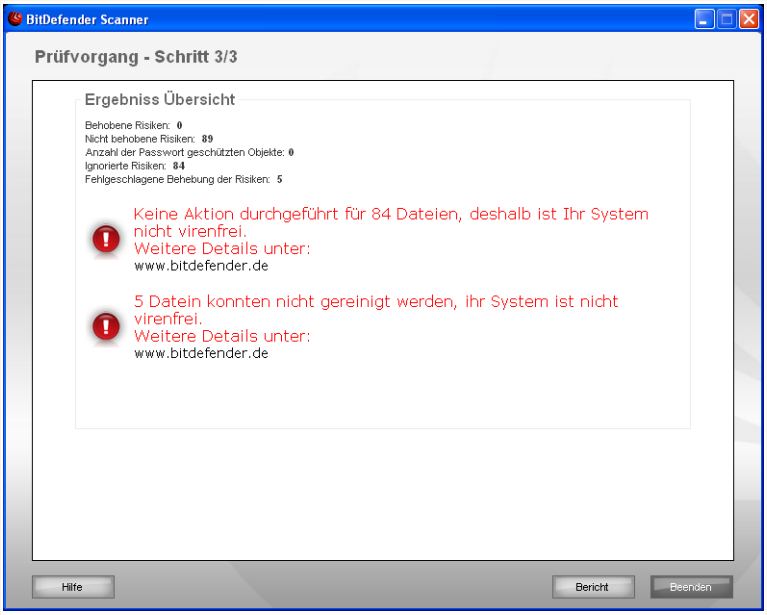
Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt.

Aktion	Beschreibung
Desinfizieren	Desinfiziert die infizierten Dateien.
Löschen	Löscht die infizierten Dateien.
Aufdecken	Macht versteckte Objekte sichtbar.

Klicken Sie auf **Weiter** um die festgelegten Aktionen durchzuführen.

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. Die Berichtsdatei wird automatisch im Abschnitt Berichte im Menüpunkt **Eigenschaften** des entsprechenden Prüfvorgangs gesichert.

Wichtig
Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu, um den Säuberungsprozess fertigzustellen.

Klicken Sie auf **Beenden**, um das Ergebnisfenster zu schließen.

BitDefender konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert BitDefender erfolgreich die entdeckten infizierten Dateien, oder es isoliert den Virus. Doch kann es zu Problemen kommen 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.

BitDefender Objekte, die durch ein Passwort geschützt werden

Die Kategorie Passwort-Schutz beinhaltet zwei Objektarten: Archive und Installer Solange diese Objekte keine infizierten Dateien beinhalten die ausgeführt werden, stellen Sie keine Gefahr für die Systemsicherheit dar.

Um Sicherzustellen dass diese Objekte nicht infiziert sind:

- Wenn das Objekt, das mit einem Passwort geschützt ist, ein Archiv ist, entpacken Sie die Dateien die es beinhaltet und überprüfen Sie diese einzeln. Die einfachste Art einen Scan durchzuführen besteht darin, die Dateien mit der rechten Maustaste anzuklicken und **BitDefender Antivirus 2008** in dem Menu zu wählen.
- Wann das Objekt, das mit einem Passwort geschützt ist, ein Installer ist, stellen Sie sicher, dass der Echtzeit-Schutz aktiviert ist, bevor Sie den Installer starten. Sollte der Installer infiziert sein, so wird BitDefender den Virus entdecken und isolieren.

Wenn Sie nicht möchten, dass diese Objekte weiterhin von BitDefender entdeckt werden, so müssen Sie sie als Ausnahmen in dem Scanprozess angeben. Um Ausnahmen anzugeben, klicken Sie auf **Einstellungen** um das Einstellungsfenster zu öffnen und öffenen Sie dann **Antivirus > Ausnahmen** . Beachten Sie für weitere Informationen: Vom Scan ausgeschlossene Objekte.

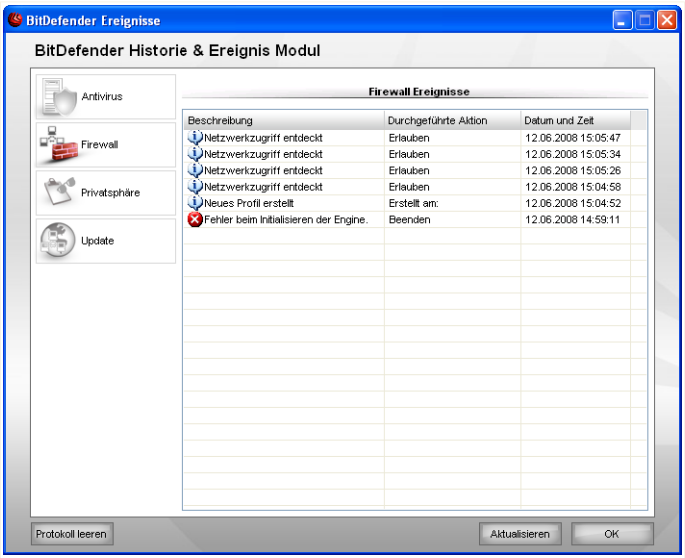
BitDefender Entdeckte Verdächtige Dateien

Verdächtige Dateien sind Dateien, die während der heuristischen Analyse als potentiell mit Malware infiziert entdeckt werden, da die Struktur derselben unbekannt ist.

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 für eine weitere Analyse an das BitDefender-Labor zu senden.

5. Ereignise

Durch einen Klick auf die Schaltfläche **Ereignise** im unteren Bereich des BitDefender Sicherheitscenters öffnet sich eine Übersicht über BitDefender Ereignise. Hier können Sie zum Beispiel problemlos einsehen wann ein Update durchgeführt wurde, ob Schädlinge gefunden wurden und so weiter.



Ereignise

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

- **Antivirus**
- **Firewall**
- **Privatsphäre**
- **Update**

Für jede Kategorie ist eine Liste von Ereignisen verfügbar. Jedes Ereignis enthält folgende Informationen: Eine Kurzbeschreibung, die von BitDefender durchgeführte

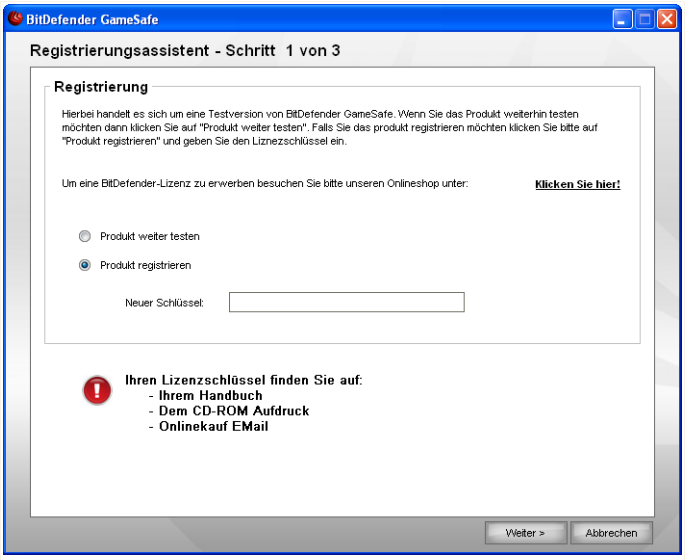
Aktion, sowie Datum und Zeitpunkt des Auftretens. Wenn Sie nähere Informationen zu einem Ereignis erhalten möchten dann klicken Sie doppelt auf selbiges.

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

6. Registrierung

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

6.1. Schritt 1/3 - BitDefender GameSafe registrieren



Registrierung

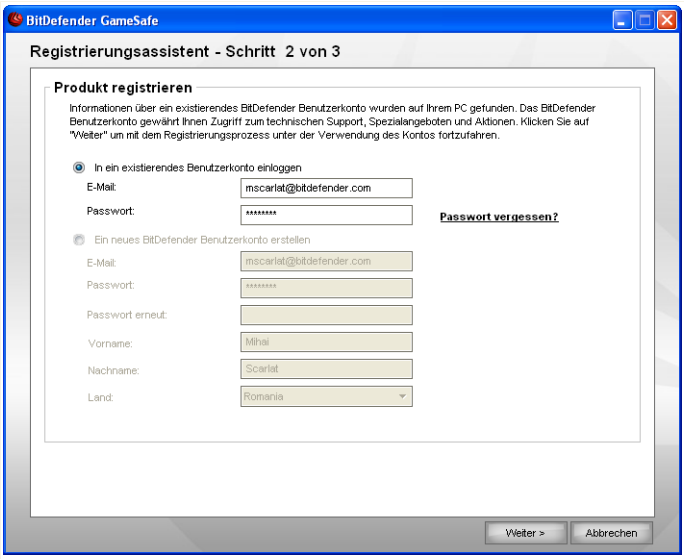
Wenn Sie keine Bitdefender-Lizenz besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Um BitDefender BitDefender GameSafe zu registrieren, wählen Sie **Produkt registrieren** Geben Sie im Feld **Neuer Schlüssel** den Lizenzschlüssel ein.

Um das Produkt weiter zu testen, und wenn der Testzeitraum noch nicht beendet ist, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**.

Klicken Sie auf **Weiter**.

6.2. Schritt 2/3 - BitDefender-Benutzerkonto erstellen



Kontoerstellung

Ich habe noch kein BitDefender-Benutzerkonto

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

Anmerkung
Wenn Sie dieses Konto später erstellen möchten, markieren Sie die entsprechenden Option.

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.

> ***Anmerkung***
> Das Passwort sollte mindestens 4 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.

Klicken Sie auf **Weiter**.

Ich habe bereits ein BitDefender Nutzerkonto.

BitDefender weist Sie daraufhin, falls bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert wurde. In diesem Fall müssen Sie nur auf **Weiter** klicken.

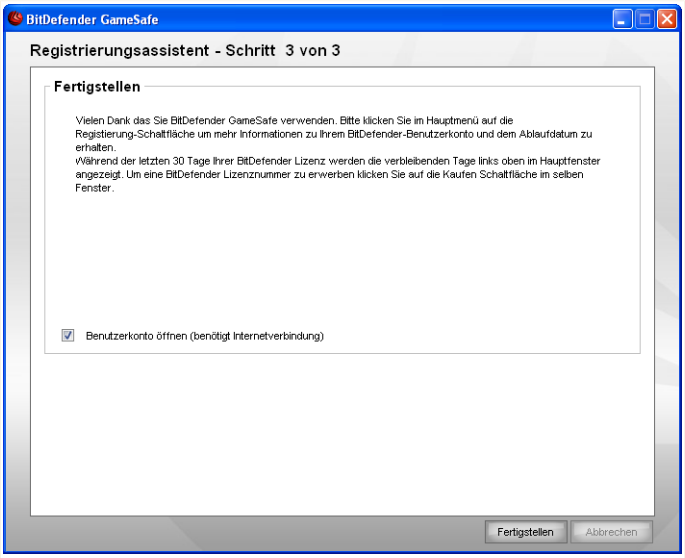
Wenn Sie bereits ein aktives Benutzerkonto besitzen, BitDefender es jedoch nicht entdeckt, wählen Sie **In ein bestehendes BitDefender-Benutzerkonto einloggen** und geben Sie die E-Mail Adresse und das Passwort Ihres Benutzerkontos ein.

> ***Anmerkung***
> Wenn Sie ein falsches Passwort eingeben, so werden Sie dazu aufgefordert es erneut anzugeben sobald Sie auf **Weiter** klicken. Klicken Sie auf **Ok** um das Passwort erneut einzugeben. Wenn Sie auf **Abbrechen** klicken, wird der Assistent beendet.

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

Klicken Sie auf **Weiter**.

6.3. Schritt 3/3 - BitDefender GameSafe registrieren



Übersicht

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

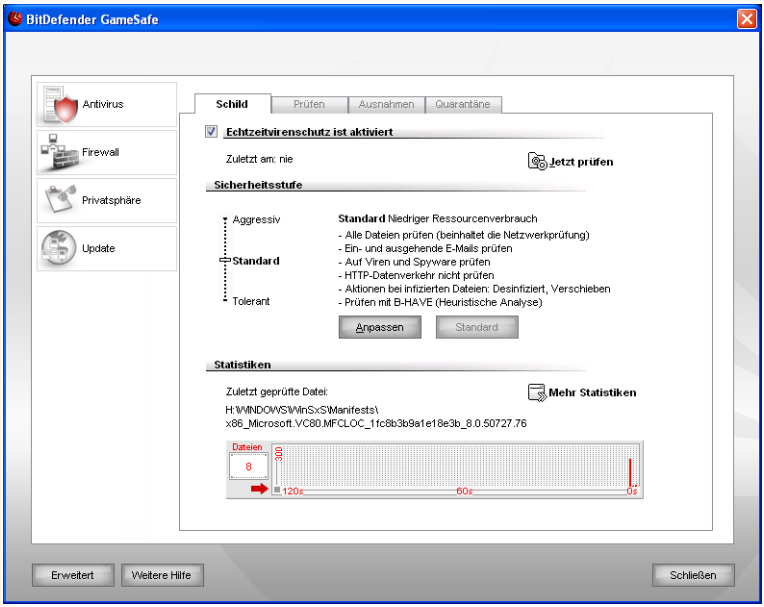
Klicken Sie auf **Beenden**, um dieses Fenster zu schließen.

Erweiterte Konfiguration

7. Einstellungskonsole

BitDefender GameSafe enthält eine zentrale Einstellungskonsole, welche Ihnen das konfigurieren und verwalten von allen BitDefender Einstellungen erlaubt.

Um zur Einstellungskonsole zu gelangen klicken Sie auf **Einstellungen** im unteren Bereich des BitDefender Sicherheitscenters.



Einstellungskonsole

Die Einstellungskonsole ist in verschiedene Module aufgeteilt: **Antivirus**, **Privatsphäre**, **Firewall** und **Update**. Dies erlaubt Ihnen das einfache Verwalten von BitDefender bezogen auf die verschiedenen Sicherheitsmodule.

Auf der linken Seite der Einstellungskonsole sehen Sie die Modulauswahl:

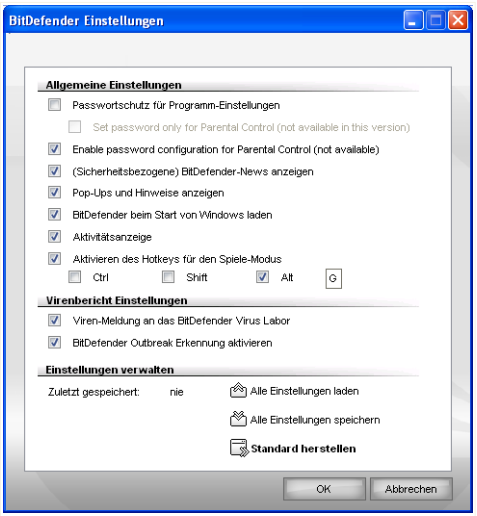
- Antivirus - In diesem Bereich können Sie das **AntiVirus**-Modul konfigurieren.
- Firewall - In diesem Bereich können Sie das **Firewall**-Modul konfigurieren.
- Privatsphäre - In diesem Bereich können Sie das Modul **Privatsphäre** konfigurieren.

- Update - In diesem Bereich können Sie **Updates** konfigurieren.

Wenn Sie weiterführende Hilfe benötigen, klicken Sie auf die Schaltfläche **Weitere Hilfe** die sich am unteren Rand des Fensters befindet. Es wird eine Kontexthilfe angezeigt, die Sie über den Abschnitt, in dem Sie sich befinden informiert.

7.1. Allgemeine Einstellungen vornehmen

Um die Allgemeinen Einstellungen von BitDefender zu konfigurieren klicken Sie in der Einstellungskonsole auf **Allgemein**. Ein neues Fenster wird sich öffnen.



Allgemeine Einstellungen

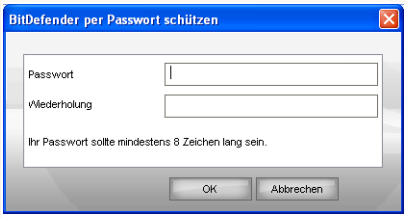
Hier können Sie die umfassenden Einstellungen von BitDefender einsehen. Standardmäßig wird BitDefender beim Windowsstart geladen und läuft dann im Hintergrund.

7.1.1. Allgemeine Einstellungen

- **Passwortschutz für Programmeinstellungen aktivieren** - aktiviert ein Passwort, 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 bestätigen

Schreiben Sie das Passwort in das **Passwort** Feld und wiederholen Sie es in dem Feld **Passwort erneut eingeben**. Danach klicken Sie auf **OK**.

Haben Sie einmal das Passwort eingestellt, so werden Sie stets danach gefragt werden, wenn Sie Änderungen in den BitDefender Einstellungen vornehmen möchten. Ein anderer Systemadministrator (falls vorhanden) wird ebenfalls dieses Passwort angeben müssen, um BitDefender Einstellungen ändern zu können.

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

- **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.
- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart. Dies wird dringend empfohlen.
- **Scanaktivitätsleiste aktivieren (zeigt Produktaktivität an)** - zeigt die Leiste der Scanaktivität an, wenn Sie Windows starten. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass die Scanaktivitätsleiste nicht weiter angezeigt wird.

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

- **Tastenkombination für Spielmodus aktivieren** -mit einer Tastenkombination kann der Spielmodus aktiviert/deaktiviert werden. Die Standardtastenkombination ist `Alt+G`.

  Um die Tastenkombination zu ändern, tun Sie Folgendes:

1. Wählen Sie zwischen folgenden Tasten: Steuerung (`Strg`), Shift (`Shift`) oder Alt (`Alt`).
2. Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

7.1.2. Einstellung Virenbericht

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

  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.

7.1.3. Update-Einstellungen

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

Wichtig
Nur Anwender mit Administratoren Rechten können die Einstellungen ändern.

Um die Werkseinstellungen zu laden, klicken Sie auf **Standard herstellen**.

8. Antivirus

BitDefender schützt Sie vor allen Arten von Schädlingen (Virus, Trojaner, Spyware, Rootkits und so weiter).

Neben dem klassischen Prüfvorgang mit Signaturen führt BitDefender einen Prüfvorgang per Heuristik durch. Mittels Heuristik können bisher unbekannte Viren auf Grundlage bestimmter Aktionsmuster und Verhaltensweisen, entdeckt werden. Dabei kann es auch zu Fehlalarmen kommen. Sollte eine verdächtige Datei auf Ihrem System gefunden werden, empfehlen wir, die Datei zur Überprüfung an das BitDefender-Virus-Labor zu schicken.

Der Virenschutz ist in zwei Kategorien aufgeteilt:

- **Echtzeitprüfung** - verhindert ein Eindringen neuer Viren in das System. Dies wird auch als Virenschutzschild bezeichnet - Dateien werden geprüft, sobald ein Benutzer auf sie zugreift. BitDefender wird z.B. ein Worddokument auf Schädlinge prüfen wenn Sie es öffnen, und eine EMailnachricht wenn Sie diese empfangen.
- **Prüfvorgang** - Erlaubt die Erkennung und Entfernung von Schädlingen welche Sich bereits auf Ihrem System befinden. 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.

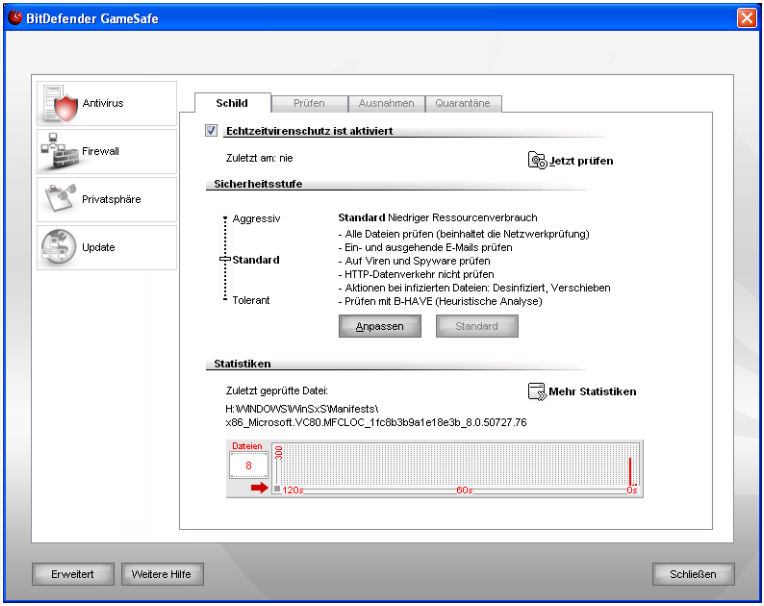
Der Abschnitt **AntiVirus** behandelt und erklärt folgende Themen:

- Bei Zugriff scannen
- Nach Aufforderung prüfen
- Vom Prüfen ausgeschlossene Objekte
- Quarantäne

8.1. Echtzeitprüfung

Die Echtzeitprüfung hält Ihren Computer durch das Prüfen von allen Dateien auf welche zugegriffen wird, E-Mailnachrichten und die Kommunikationen per Instant Messaging Software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) sicher.

Um die Echtzeitprüfung zu konfigurieren klicken Sie in der Einstellungskonsole auf **Antivirus>Schild**. Das folgende Fenster wird erscheinen:



Echtzeitschutz

Wichtig

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

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

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

8.1.1. Sicherheitsgrad 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:

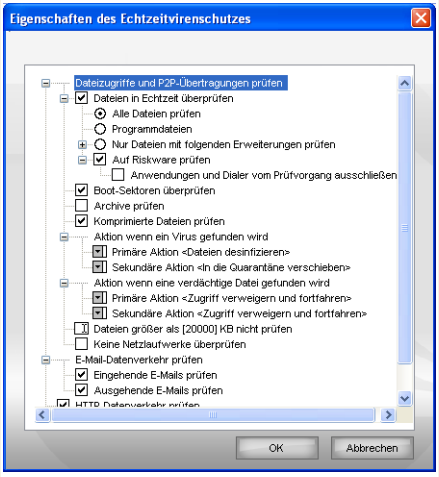
Sicherheitsstufe	Beschreibung
Tolerant	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. Programme und eingehende Nachrichten werden nur auf Viren hin geprüft. Neben den klassischen Signatur basierten Scans werden außerdem Heuristische Scans eingesetzt. Bei infizierten Dateien können 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**.

8.1.2. 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.

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



Einstellungen des Virus Schild

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

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.

Option		*Beschreibung*
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`;

Option		Beschreibung
		.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		**Zweite Aktion, falls die erste fehlschlägt** - Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.

Option		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		**Dateien größer als [x] nicht prüfen** - geben Sie die maximale Größe der zu prüfenden Datei ein. Falls die Größe 0 Kb ist, werden alle Dateien geprüft.
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.

  Folgende Optionen stehen zur Verfügung:

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

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

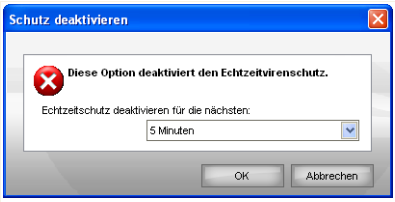
  Ist eine Datei infiziert wird eine Warnmeldung ausgegeben, die Hinweise über die Art des Schädlings beinhaltet. Bei infizierten E-Mails erhält der Empfänger eine Nachricht mit Hinweisen über die Art des Schädlings und Informationen über den Absender der Nachricht.

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

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

8.1.3. 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.

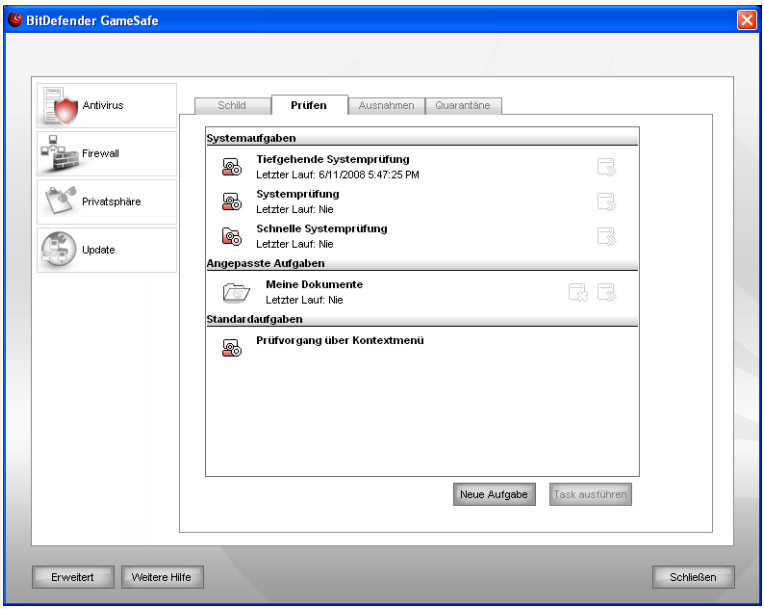
Warnung
Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist sind Sie nicht vor Schädlingen geschützt.

8.2. 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 Prüfvorgang zu konfigurieren oder zu starten klicken Sie in der Einstellungskonsole auf **Antivirus>Prüfen** Das folgende Fenster wird erscheinen:



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.

8.2.1. 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. 55).

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.

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.

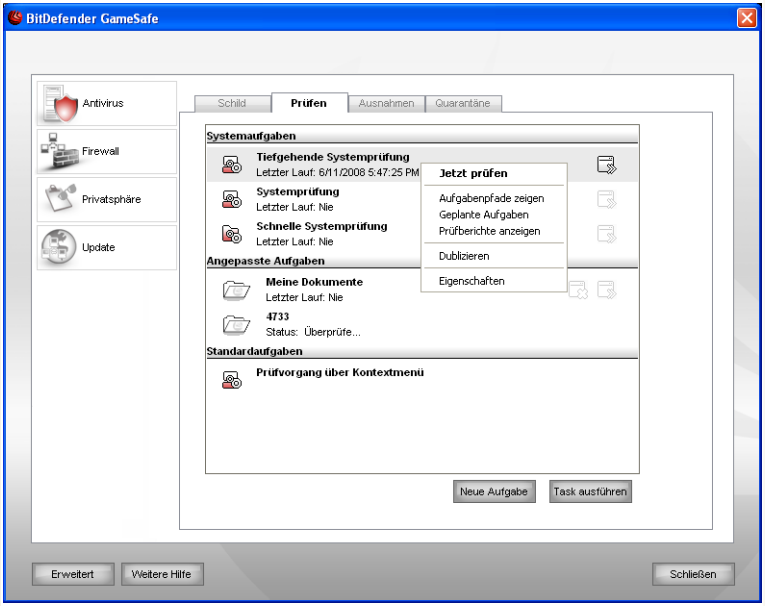
Anmerkung
Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

- **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.

8.2.2. Verwenden des Kontextmenüs

Für jede Aufgabe steht ein Shortcut Menü zur



Shortcut Menü

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.

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

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

- **Geplante Aufgaben** - Öffnet das Fenster **Eigenschaften** , **Planer**, wo Sie die ausgewählten Aufgaben planen können.
- **Prüfberichte anzeigen** - Öffnet das Fenster **Eigenschaften** , **Prüfberichte**, in welchem Sie die Berichte sehen, die nach dem Prüfungvorgang erstellt wurden.
- **Dublizieren** - wiederholt die ausgewählte Aufgabe.

Anmerkung
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.

- **Eigenschaften** - 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.

8.2.3. 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.

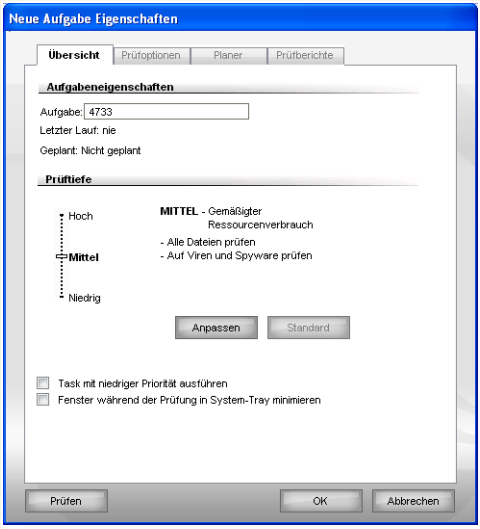
8.2.4. Konfiguration einer Prüfaufgabe

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. 72).

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:



Überblick

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:

Sicherheitsstufe	*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:

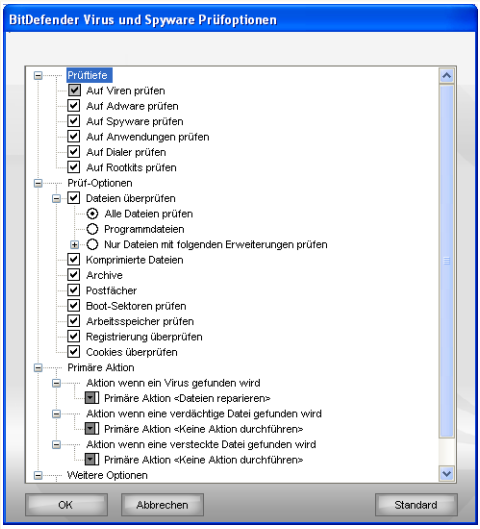
Option	*Beschreibung*
Aufgaben mit niedriger Priorität ausführen	Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
Minimieren des Prüffensters beim Scan-Start	Es verkleinert das Prüffenster beim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

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

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 Prüfeinstellungen 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 vier Kategorien unterteilt:

- **Prüftiefe**
- **Prüfoptionen**
- **Aktionsoptionen**
- **Weitere Optionen**

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

  Folgende Optionen stehen zur Verfügung:

Option	Beschreibung
Dateien prüfen	Sucht nach bekannten Viren. 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	Prüft Programmdateien (`.exe` und `.dll` Dateien.
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.

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

  Folgende Optionen stehen zur Verfügung:

Option		Beschreibung
Dateien prüfen	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`;

Option		Beschreibung
		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.
Komprimierte Dateien		Alle komprimierten Dateien werden überprüft.
Archive		Prüft den Inhalt von eingepackten Archiven.
Postfächer		Prüft den Inhalt von E-Mails und deren Attachments.
Boot-Sektoren prüfen		Prüft die Bootsektoren des Systems.
Speicher prüfen		Prüft den Speicher auf Viren und andere Malware.
Systemregistrierung prüfen		Prüft Einträge in der Systemregistrierung.
Cookies prüfen		Prüft gespeicherte Cookies von Webseiten.

- Wählen Sie die Aktionen für infizierte, verdächtige oder versteckte Dateien aus. Öffnen Sie den **Aktionsbereich**, um alle möglichen Aktionen für diese Dateien anzeigen zu lassen.
  - Wählen Sie die durchzuführende Aktion für die erkannten Dateien: Folgende Optionen stehen zur Verfügung:

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien können Sie in der Berichtsdatei einsehen.
Dateien reparieren	Desinfiziert die infizierten Dateien.
Dateien löschen	Infizierte Dateien werden ohne Warnung sofort gelöscht.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.

- Wählen Sie die durchzuführende Aktion für die als verdächtig erkannten Dateien: Folgende Optionen stehen zur Verfügung:

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.

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): Folgende Optionen stehen zur Verfügung:

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.
Sichtbar machen	Deckt versteckte Dateien auf so das diese sichtbar werden.

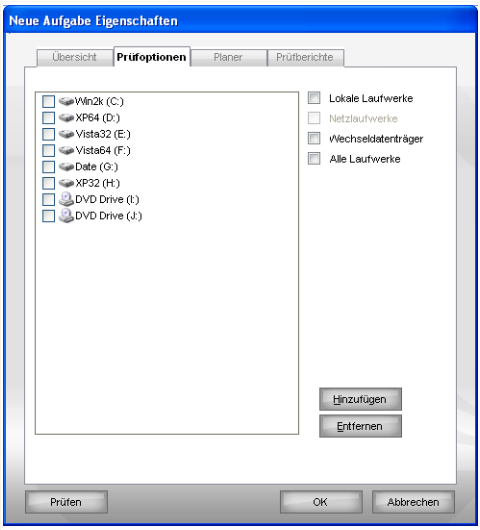
Anmerkung
Sollten Sie sich entschliessen die entdeckten Dateien zu ignorieren oder die gewählte Aktion fehlschlagen so müssen Sie im Prüfvorgangs-Assitenten eine Aktion auswählen.

■ Um alle verdächtigen Dateien nach dem Prüfvorgang an das BitDefender Labor zu senden markieren Sie die Option **Dateien an das BitDefender Labor senden**.

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

Festlegen der Zielobjekte

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



Prüfen der Zielobjekte

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** - Löscht die Datei/den Ordner, die/der zuvor aus der Liste der zu prüfenden Objekte ausgewählt wurde.

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

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

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

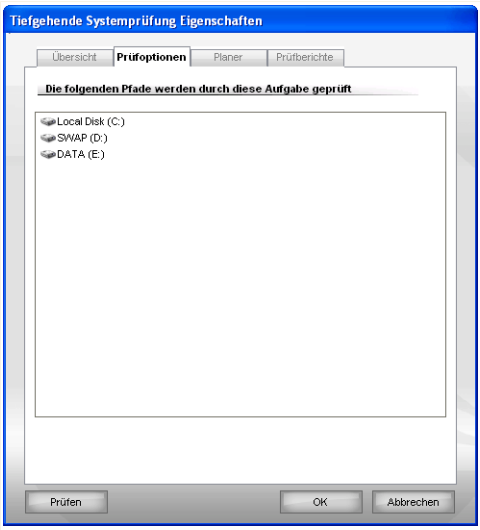
Anmerkung
Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

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

Prüfziel der Systemaugaben anzeigen

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

Um das Prüfziel einer speziellen Systemprüfaufgabe zu sehen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Aufgabenpfade anzeigen**. So wird beispielsweise für**Vollständige Systemprüfung** das folgende Fenster erscheinen:



Prüfziel der Vollständigen Systemprüfung

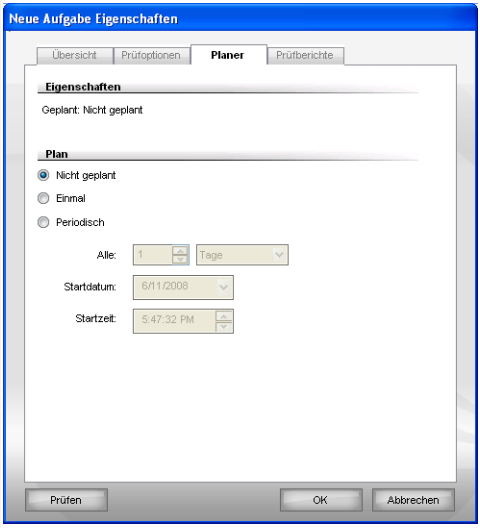
Vollständige Systemprüfung und **Tiefe Systemprüfung** überprüfen alle lokalen Laufwerke, während **Schnelle Systemprüfung** nur die Ordner `Windows` und `Programme/Dateien` überprüfen wird.

Klicken Sie auf **OK**, um dieses Fenster zu schließen. Wenn Sie die Aufgabe starten möchten, klicken Sie auf **Scan**.

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:



Zeitgesteuertes Starten von Prüfvorgängen

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**.

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

8.2.5. 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 2008 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

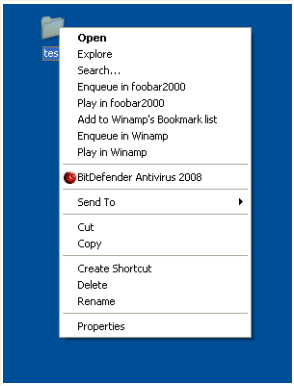
Folgende Optionen sind wählbar:

- 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. 67) 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



Kontextmenü

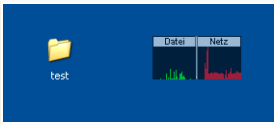
Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei oder Ordner und wählen Sie **BitDefender Antivirus 2008** aus.

Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel *„BitDefender Scanner“* (S. 67) in diesem Handbuch.

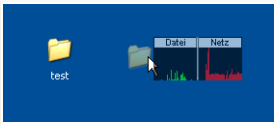
Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster **Eigenschaften** auf **Prüfen Kontext Menü** klicken.

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. 67) in diesem Handbuch.

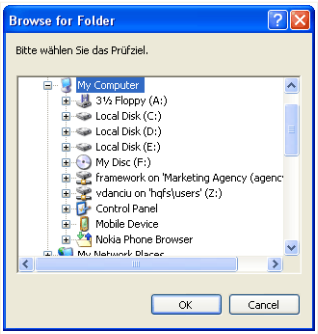
Manuelle Prüfung

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 2008 → BitDefender Manuelle Prüfung**.

Das folgende Fenster wird erscheinen:



Manuelle Prüfung

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

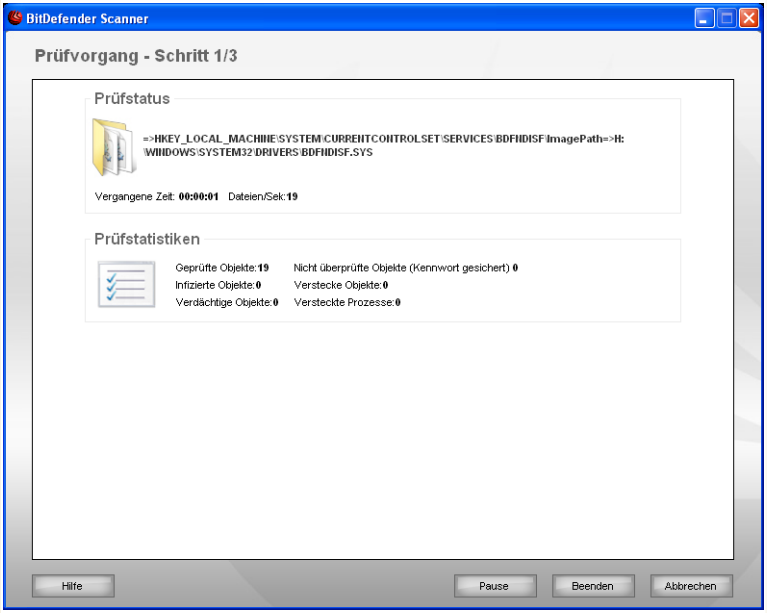
Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 67) in diesem Handbuch.

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.

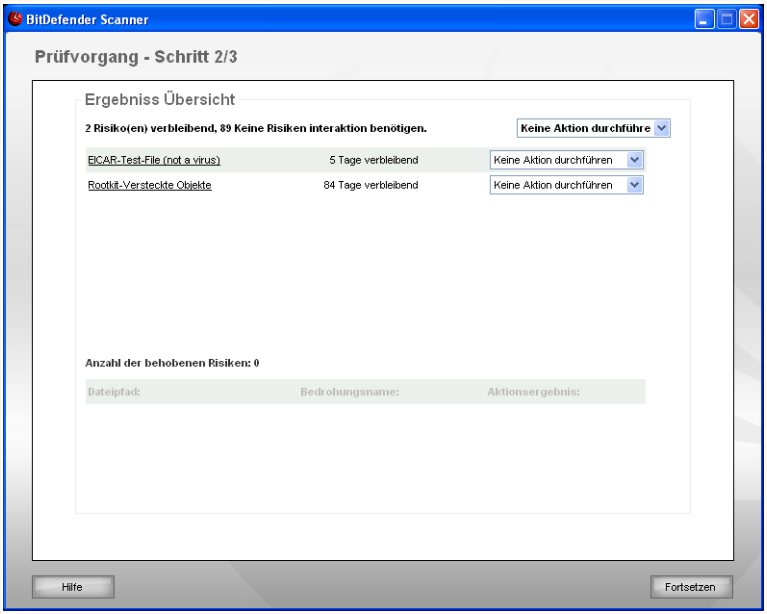
Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

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 der Malware mit der sie infiziert sind. Klicken Sie auf den Link, der sich auf die Gefährdung bezieht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine Globale Aktion für jede Gruppe auswählen oder Sie können für jedes Risiko eine eigene Aktion angeben.

Folgende Aktionen stehen zur Verfügung:

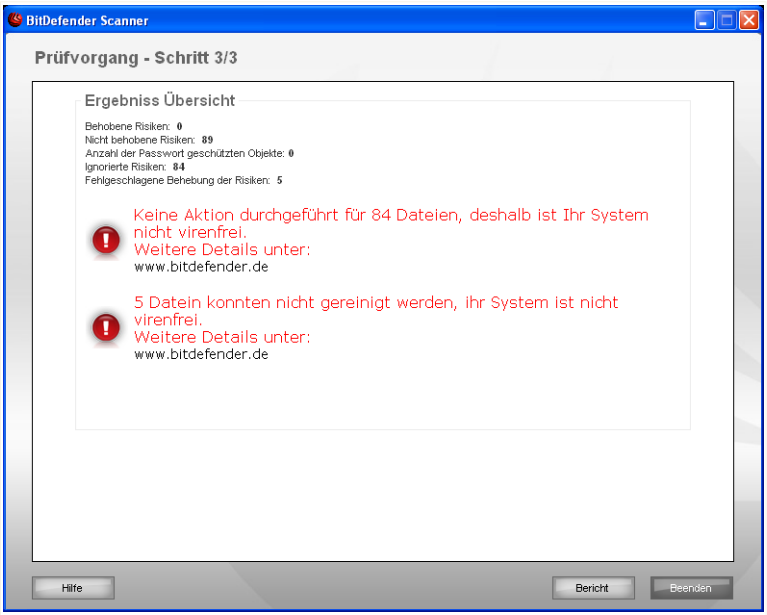
Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt.

Aktion	Beschreibung
Desinfizieren	Desinfiziert die infizierten Dateien.
Löschen	Löscht die infizierten Dateien.
Aufdecken	Macht versteckte Objekte sichtbar.

Klicken Sie auf **Weiter** um die festgelegten Aktionen durchzuführen.

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. Die Berichtsdatei wird automatisch im Abschnitt Berichte im Menüpunkt **Eigenschaften** des entsprechenden Prüfvorgangs gesichert.

Wichtig
Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu, um den Säuberungsprozess fertigzustellen.

Klicken Sie auf **Beenden**, um das Ergebnisfenster zu schließen.

BitDefender konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert BitDefender erfolgreich die entdeckten infizierten Dateien, oder es isoliert den Virus. Doch kann es zu Problemen kommen 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.

BitDefender Objekte, die durch ein Passwort geschützt werden

Die Kategorie Passwort-Schutz beinhaltet zwei Objektarten: Archive und Installer Solange diese Objekte keine infizierten Dateien beinhalten die ausgeführt werden, stellen Sie keine Gefahr für die Systemsicherheit dar.

Um Sicherzustellen dass diese Objekte nicht infiziert sind:

- Wenn das Objekt, das mit einem Passwort geschützt ist, ein Archiv ist, entpacken Sie die Dateien die es beinhaltet und überprüfen Sie diese einzeln. Die einfachste Art einen Scan durchzuführen besteht darin, die Dateien mit der rechten Maustaste anzuklicken und **BitDefender Antivirus 2008** in dem Menu zu wählen.
- Wann das Objekt, das mit einem Passwort geschützt ist, ein Installer ist, stellen Sie sicher, dass der Echtzeit-Schutz aktiviert ist, bevor Sie den Installer starten. Sollte der Installer infiziert sein, so wird BitDefender den Virus entdecken und isolieren.

Wenn Sie nicht möchten, dass diese Objekte weiterhin von BitDefender entdeckt werden, so müssen Sie sie als Ausnahmen in dem Scanprozess angeben. Um Ausnahmen anzugeben, klicken Sie auf **Einstellungen** um das Einstellungsfenster zu öffnen und öffenen Sie dann **Antivirus > Ausnahmen** . Beachten Sie für weitere Informationen: Vom Scan ausgeschlossene Objekte.

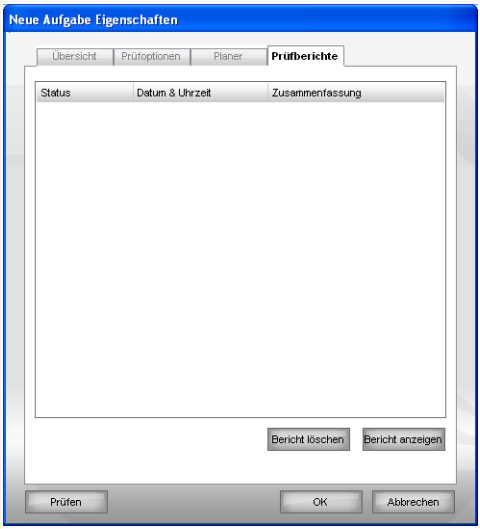
BitDefender Entdeckte Verdächtige Dateien

Verdächtige Dateien sind Dateien, die während der heuristischen Analyse als potentiell mit Malware infiziert entdeckt werden, da die Struktur derselben unbekannt ist.

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 für eine weitere Analyse an das BitDefender-Labor zu senden.

8.2.6. 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 nach jedem Scan erstellt werden.

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:

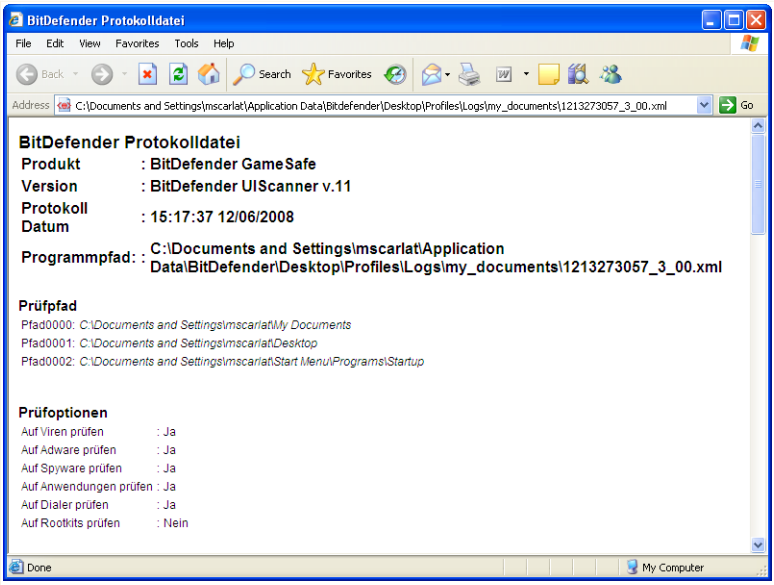
- **Bericht löschen** - löscht die ausgewählte Berichtsdatei.
- **Bericht anzeigen** - öffnet die ausgewählte Berichtsdatei. Die Berichtdatei wird in Ihrem Web-Browser geöffnet.

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.

Prüfbericht Beispiel

Die folgende Abbildung zeigt ein Beispiel eines Prüfberichts :



Prüfbericht Beispiel

Der Prüfbericht enthält detaillierte Informationen über den Scanprozess, wie Prüfoptionen, das Prüfziel, entdeckte Gefährdungen und die entsprechend ausgeführten Optionen.

8.3. Vom Prüfvorgang ausgeschlossene Objekte

In manchen Fällen wird es nötig sein bestimmte Dateien vom Prüfen auszunehmen. Zum Beispiel wenn Sie den Testvirus EICAR nicht prüfen möchten.

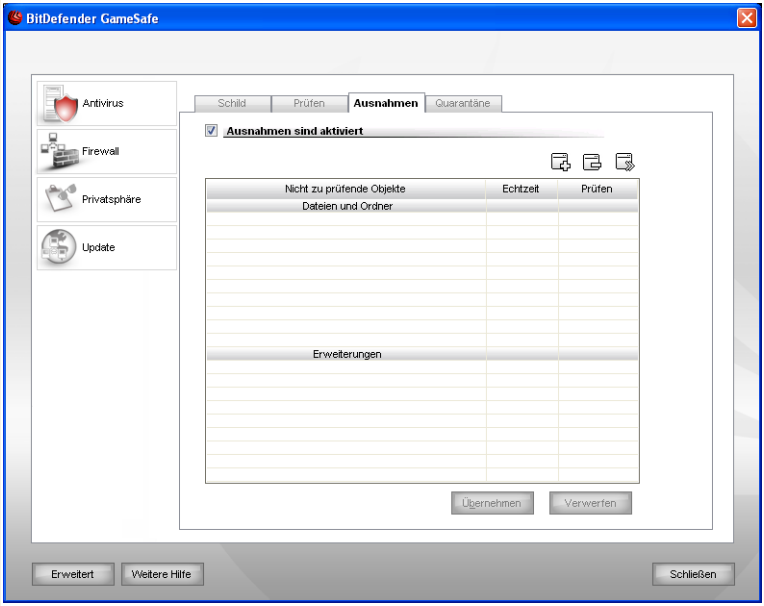
BitDefender bietet die Möglichkeit Objekte vom Prüfvorgang, vom Echtzeitschutz oder von beidem auszunehmen. Dies dient dazu die Prüfgeschwindigkeit zu erhöhen oder Eingriffe bei der Arbeit zu verhindern.

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 ausgenommenen Objekte zu verwalten klicken Sie auf **Antivirus>Ausnahmen** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



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**.

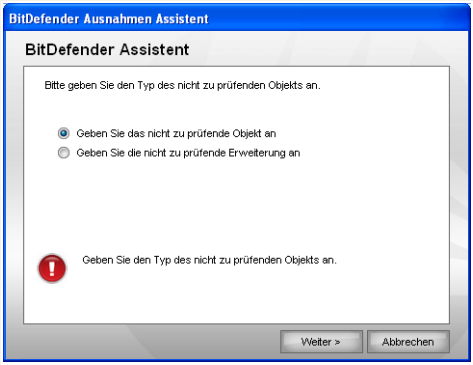
Anmerkung
Sie können das Objekt auch mit der rechten Maustaste anklicken un es zu bearbeiten oder zu löschen.

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

8.3.1. 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 1/3 - Wählen Sie die Objektart

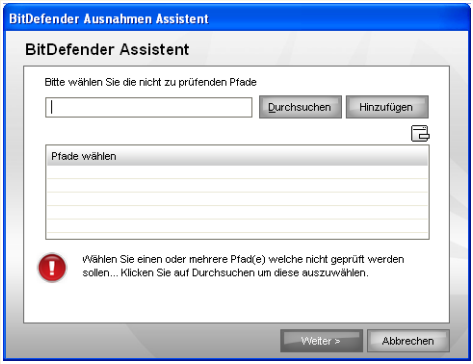


Objektart

Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.

Klicken Sie auf **Weiter**.

Schritt 2/3 - 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**.

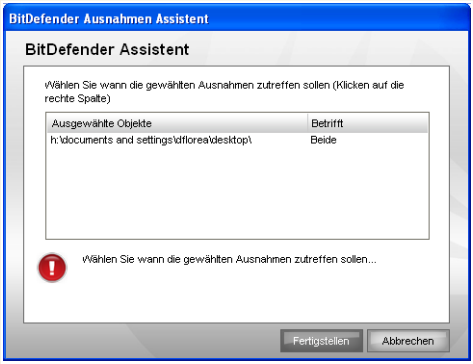
Anmerkung
Sollte der eingegebene Pfad nicht existieren so erscheint eine Fehlermeldung. Klicken Sie auf **OK** und prüfen Sie den angegebenen Pfad.

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 3/3 - 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.

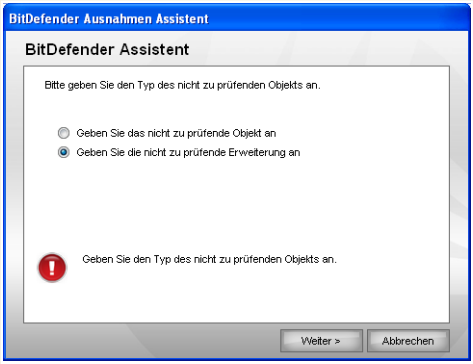
Klicken Sie auf **Fertigstellen**.

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

8.3.2. Dateierweiterungen vom Prüfen ausnehmen

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

Schritt 1/3 - Wählen Sie die Objektart

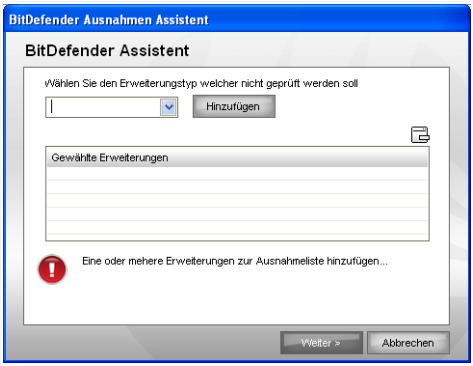


Objektart

Wählen Sie die Option um eine Dateierweiterung vom Prüfen auszunehmen.

Klicken Sie auf **Weiter**.

Schritt 2/3 - 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.

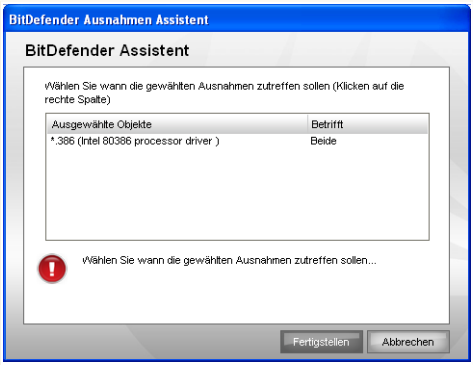
- Geben Sie die gewünschte Erweiterung in das Eingabefeld ein und klicken Sie auf **Hinzufügen**.

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 3/3 - 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.

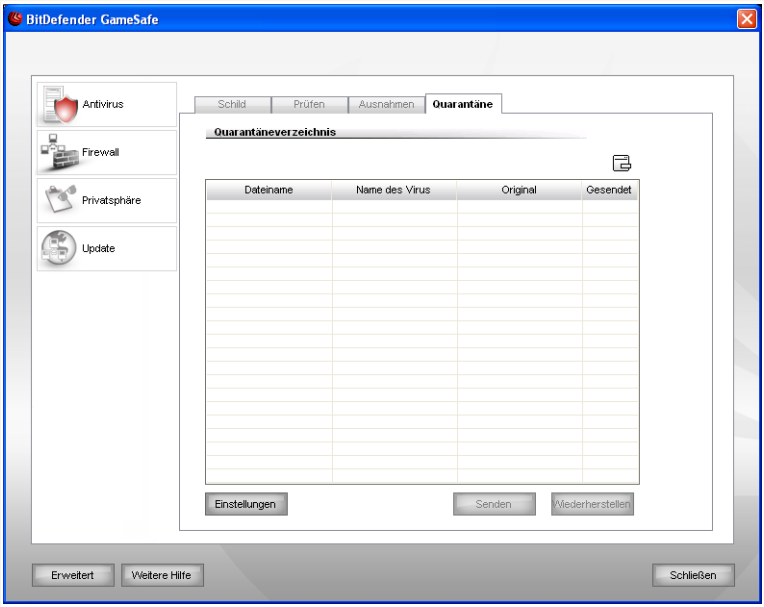
Klicken Sie auf **Fertigstellen**.

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

8.4. Quarantäne

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

Um die in Quarantäne verschobenen Dateien einzusehen und Einstellungen vorzunehmen klicken Sie in der Einstellungskonsole auf **Antivirus>Quarantäne**



Quarantäne

8.4.1. Quarantäne-Dateien verwalten

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

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

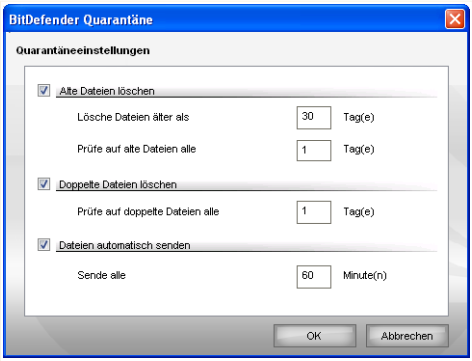
Um eine ausgewählte Datei aus der Quarantäne zu löschen klicken Sie **entfernen**. Wenn Sie eine infizierte Datei wiederherstellen wollen in ihrem original Speicherort klicken Sie **Wiederherstellen**.

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.

8.4.2. 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 10 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.

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

9. 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.

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

- Firewall Einblicke
- Status der Personal-Firewall
- Firewallregeln
- Weitere Einstellungen
- Aktivitätsanzeige
- Netzwerkzonen

9.1. Firewall Einblicke

Die BitDefender Firewall wurde konzipiert um Ihnen den bestmöglichen Schutz für Ihre Netzwerk / Internetverbindung zu gewähren ohne das Sie diese konfigurieren müssen. Egal über welche Art von Netzwerk Sie die Verbindung herstellen, BitDefender wird sich automatisch auf die Gegebenheiten anpassen.

Standardmässig erstellt BitDefender automatisch ein grundlegendes Firewall Profil sobald eine Netzwerkkonfiguration gefunden wurde. Ausserdem werden weitere gefundene Netzwerke automatisch hinzugefügt.

9.1.1. Was sind Firewall Profile?

Ein Firewall Profil ist eine Sammlung von Regeln welche den Zugang zum Netzwerk bzw. Internet regeln.

Abhängig von Ihrer Netwerkkonfiguration erstellt BitDefender automatisch ein für dieses Netwerk spezifisches Profil. Das Basis Profil enthält die elementarsten Regel angepasst auf den Netzwerktyp.

Anmerkung
Für jedes gefundene Netzwerk wird ein eigenes Profil erstellt, unabhängig davon mit wievielen Netzwerken Sie verbunden sind.

Es gibt 3 Arten von Basis Profilen:

Profile	*Beschreibung*
Direktverbindung	Enthält die grundlegenden Regeln für eine Direktverbindung zum Internet. Dieser Regeln erlaubt keinen Netzwerkzugriff auf Ihrem Computer.
Nicht Vertrauenswürdig	Enthält die grundlegenden Regeln für eine Verbindung zu einem unsicheren Netzwerk. Diese Regeln erlaubt Ihnen den Netzwerkzugriff, verhindert jedoch den Zugriff auf Ihren Computer.
Vertrauenswürdig	Enthält die grundlegenden Regeln für eine Verbindung zu einem sicheren Netzwerk. Es werden keine Einschränkungen des Netzwerkzugriffs vorgenommen. Das bedeutet Sie haben Zugriff auf Netzwerkdrucker, Freigaben usw. Ausserdem ist der Zugriff vom Netzwerk auf Ihren Computer gewährt.

Wenn Anwendungen versuchen eine Verbindung herzustellen werden entsprechende Regeln zum Profil hinzugefügt. Sie können festlegen das Sie jeweils gefragt werden ob eine Anwendung zugriff erhalten soll, oder das Programme welche in der Whitelist enthalten sind automatisch Zugriff erhalten und alle anderen weiterhin abgefragt werden.

Anmerkung
Um festzulegen wie Anwendung beim ersten Versuch des Verbindungsaufbaus behandelt werden öffnen Sie den Menüpunkt Status und legen Sie die Sicherheitsstufe fest. Um ein existierendes Profil zu bearbeiten, wechseln Sie zum Reiter Datenverkehr und klicken Sie auf **Profil bearbeiten**.

9.1.2. Was sind Netzwerkbereiche?

Ein Netzwerkbereich repräsentiert einen Computer innerhalb eines Netzwerks oder ein komplettes Netzwerk das von Ihrem Computer abgeschottet ist, oder gegenteilig, ein Computer der auf Ihren Computer verbinden kann.

Standardmässig fügt BitDefender automatisch bestimmte Zonen für bestimmte Netzwerkkonfigurationen hinzu. Eine Zone wird durch das hinzufügen einer zugehörigen Netzwerkzugriffsregel erstellt, anwendbar auf das komplette Netzwerk, im momentanen Profil.

Es gibt zwei Arten von Zonen:

Zonentyp	Beschreibung
Vertrauenswürdig	Computer einer Vertrauenswürdigen Zone können auf Ihrem Computer verbinden und Sie auf den anderen Computer. Alle Verbindungsanfragen von der Zone zu Ihrem Computer werden erlaubt, ebenso alle Anfragen von Ihnen zur Zone. Wenn ein Netzwerk als Vertrauenswürdige Zone hinzugefügt wird haben Sie uneingeschränkten Zugriff auf Netzwerkfreigaben, Durcker und andere Netzwerkquellen. Ebenso können Netzwerkmitglieder auf Ihrem Computer verbinden.
Nicht vertrauenswürdig	Computer einer nicht Vertrauenswürdigen Zone können nicht auf Ihrem Computer zugreifen, ebenso können Sie nicht auf das Netzwerk zugreifen. Alle Verbindungsanfragen von der Zone zu Ihrem Computer werden verweigert, ebenso alle Anfragen von Ihnen zur Zone. Wenn Sie den ICMP Traffic verweigern und den Stealth Modus aktivieren ist ihr Computer praktisch unsichtbar.

Anmerkung

Um eine Zone zu bearbeiten wechseln Sie zum Reiter Zonen. Um eine zu einer Zone gehörige Regeln zu bearbeiten, wechseln Sie zum Reiter Datenverkehr und klicken Sie auf **Profil bearbeiten**.

9.1.3. Bedienen der Firewall

Wenn Sie das System nach der Installation neu starten erkennt BitDefender automatisch Ihre Netzwerkeinstellungen, erstellt ein passendes Basis Profil und fügt eine dem Netzwerk entsprechende Zone hinzu.

Anmerkung

Wenn Sie per Direktverbindung mit dem Internet verbunden sind wird keine Zone erstellt. Wenn Sie mit meheren Netzwerken verbunden sind werden Zonen entsprechend der Netzwerke erstellt.

Jedes Mal wenn sich Ihre Netzwerkkonfiguration ändert, z.B. wenn Sie zu einem anderen Netzwerk verbinden oder eine Verbindung trennen wird automatisch ein neues Firewall Profil erstellt. Gleichzeitig werden die Zonen angepasst.

Wenn ein neues Firewall Profil erstellt wird, wird das alte Profil gespeichert, sodass es lediglich wieder geladen werden muss wenn Sie sich wieder mit dem Netzwerk verbinden.

Entsprechend der Netzwerkkonfiguration wird BitDefender sich automatisch konfigurieren. Folgendermaßen ist die BitDefender Firewall standardmässig konfiguriert:

- Sollten Sie über eine Direktverbindung mit dem Internet verbunden sein dann wird ein Direktverbindungs-Profil erstellt. Unabhängig davon ob Sie ausserdem mit einem weiteren Netzwerk verbunden sind.

  Anmerkung

  Um kein Sicherheitsrisiko einzugehen werden Vertrauenswürdige Netzwerke nicht standardmässig erstellt. Um ein Vertrauenswürdiges Profil zu erstellen müssen Sie das aktuelle Profil bearbeiten. Lesen Sie hierzu bitte „*Profil zurücksetzen*“ (S. 99).

- Zonen werden anhand der Netzwerkkonfiguration erstellt.

Zonentyp	*Netzwerkkonfiguration*
Vertrauenswürdig	**Private IP ohne Gateway** - Der Computer ist Teil eines lokalen Netzwerks (LAN) und stellt keine direkte Verbindung zum Internet her. Ein Beispiel hierfür wäre ein Heimnetzwerk welches erstellt wurde um Familienmitgliedern den Zugriff auf Freigaben, Drucker und ähnliches zu gewähren.

Zonentyp	Netzwerkkonfiguration
	Private IP mit Domaincontroller - Der Computer ist Teil eines Netzwerkes und mit einer Domain verbunden. Ein Beispiel hierfür ist ein Firmennetzwerk welches den Benutzern erlaubt Daten und anderen Ressourcen in der Domain zu verteilen. Das vorhandensein einer Domain setzt bestimmte Regeln vorraus.
Nicht vertrauenswürdig	**Offenes (nicht geschütztes) WLAN** - Der Computer ist Teil eines WLAN (wireless local area network). Ein Beispiel hierfür ist wenn Sie über einen öffentlichen Access-Point auf das Internet zugreifen.

Anmerkung

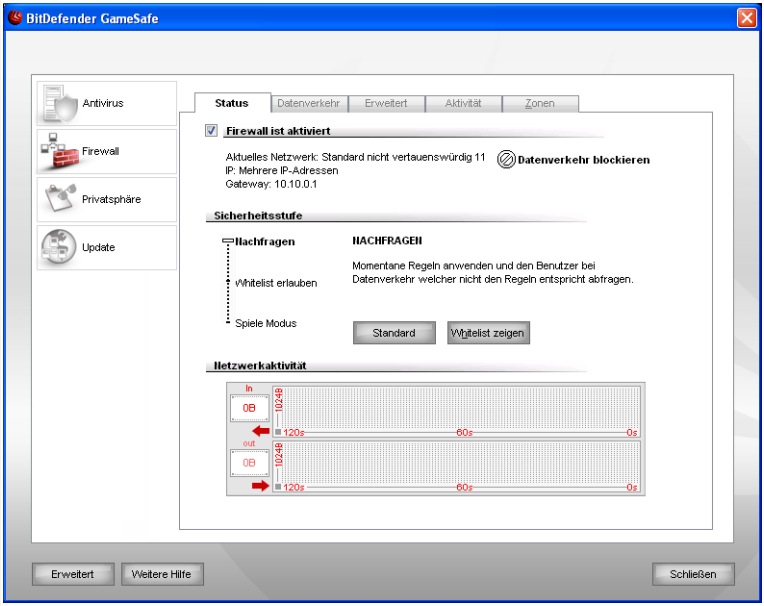
Zonen werden nicht für alle Typen von Netzwerkkonfigurationen erstellt, wie z.B.:

- **Öffentliche (routebare) IP** - Der Computer ist direkt mit dem Internet verbunden.
- **Private IP mit Gateway, aber ohne Domain** - Der Computer ist Teil eines LAN, ohne mit einer Domain verbunden zu sein und verbindet sich über einen Gateway mit dem Internet. Ein Beispiel hierfür ist ein Universitäts-Netzwerk in welchem es erlaubt ist Daten zu verteilen.

- Stealth-Modus ist aktiviert.
- VPN und Remoteverbindungen sind erlaubt.
- Internet Connection Sharing (ICS) ist für nicht vertrauenswürdige Zonen nicht erlaubt.
- Programme welche in der Whitelist vorhanden sind wird der Zugriff automatisch erlaubt, bei anderen werden Sie gefragt.

9.2. Status der Firewall

Um die Firewall zu konfigurieren klicken Sie bitte auf **Firewall>Status** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



Status der Firewall

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

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

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

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

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

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

9.2.1. Sicherheitsgrad einstellen

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

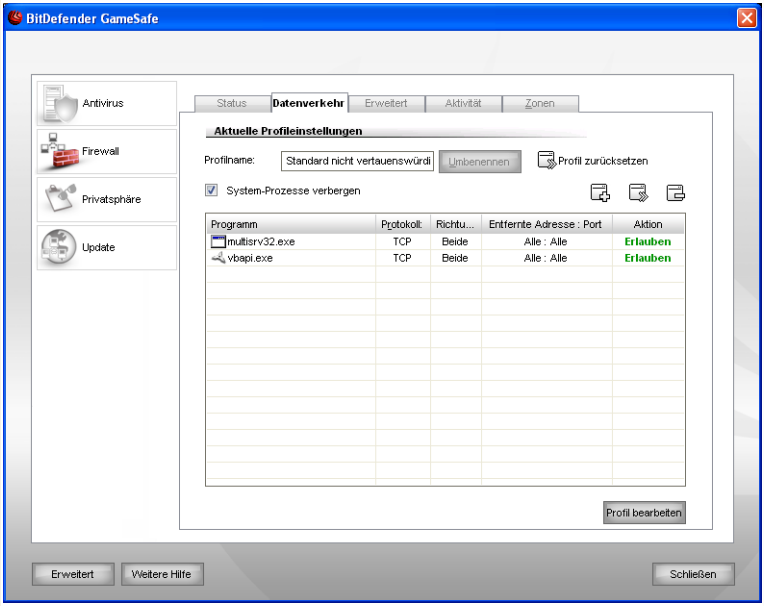
Es gibt 3 mögliche Einstellungen:

Sicherheitsstufe	*Beschreibung*
Spiele Modus	Verwendet die momentanen Regeln und erlaubt alle Anfragen welche nicht den Regeln entsprechen ohne Nachfrage. Diese Einstellung kann für Netzwerkadministratoren und Gamer hilfreich sein.
Whitelist erlauben	Erlaubt alle ausgehenden Verbindungsversuche von Programmen, die in der Whitelist vorhanden sind. Bei anderen Anwendungen werden Sie um Erlaubniss gefragt. Sie können die Regeln sehen wie Sie in dem Abschnitt Datenverkehr stehen. Programme mit Freundleslisten sind die am weitesten verbreiteten Programme weltweit. Sie beinhalten die bekanntesten Web Browsers, audio&video Players, Chat und Filesharing Programme, ebenso wie Server Clients und Betriebssystem Anwendungen. Wenn Sie sehen möchten welche Programme sich auf der Whitelist befinden, klicken Sie auf **Whitelist zeigen**.
Nachfragen	Verwendet die momentanen Regeln und frägt Sie bei alle Anfragen welche nicht den Regeln entsprechen.

Klicken Sie auf **Standard** um die Standardregel (**Empfohlene erlauben**) wiederherzustellen.

9.3. Firewall Regeln

Um die Firewall Regeln des momentanen Profils zu bearbeiten klicken Sie auf **Firewall>Datenverkehr** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



Firewall Regeln

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

Die Regeln können automatisch erstellt werden (durch das Alarm-Fenster) oder manuell (Klicken Sie **Hinzufügen** und wählen Sie die Parameter für die Regelerstellung.)

9.3.1. Regeln automatisch hinzufügen

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

Firewall Alarm

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

Wählen Sie **Erlauben** um allen Datenverkehr für diese Anwendung über das eingestellt Protokol 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.

9.3.2. Regeln manuell hinzufügen

Klicken Sie **Regel hinzufügen** und wäheln Sie die Parameter für die Regelerstellung. Das folgende Fenster wird erscheinen:

Regel hinzufügen

Um eine neue Regel hinzuzufügen befolgen Sie folgende Schritte:

1. Wählen Sie die Anwendung für welche die Regel erstellt werden soll.

   Um eine Anwendung hinzuzufügen klicken Sie auf **Durchsuchen**, wählen Sie die Anwendung aus und klicken Sie auf **OK**.

   Wenn die Regel für alle Anwendungen gelten so dann setzen Sie ein Häckchen bei **Diese Regel für alle Anwendungen verwenden**.
2. Wählen Sie das gewünschte Protokol.

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

   Die folgende Liste zeigt Ihnen die verfügbaren Protokole mit einer Kurzbeschreibung:

Protokoll	Beschreibung
ICMP	Internet Control Message Protocol (ICMP) benutzt wie TCP und UDP das Internet Protocol IP, ist also ein Teil der Internet-Protokoll-Familie. Es dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen. Obwohl ICMP eine Ebene über IP angeordnet ist, ist es in IP integriert. Es wird von jedem

Protokoll	Beschreibung
	Router und PC erwartet, ICM-Protokoll zu sprechen. Die meisten ICMP-Pakete enthalten Diagnose-Informationen, sie werden vom Router zur Quelle (engl. source) zurückgeschickt, wenn der Router Pakete verwirft, z.B. weil das Ziel (engl. destination) nicht erreichbar ist, die TTL abgelaufen ist, usw. Es gilt der Grundsatz, dass ein ICMP-Paket niemals ein anderes ICMP-Paket auslöst, d.h. die Tatsache, dass ein ICMP Paket nicht zugestellt werden konnte wird nicht durch ein Weiteres signalisiert. Eine Ausnahme zu diesem Grundsatz bildet die Echo-Funktion. Echo-ICMP-Pakete werden z.B. durch das Programm Ping verschickt. ICMP-Nachrichten werden beim Versand im Datenteil von IP-Datagrammen eingekapselt. Dabei sind im IP-Header der Servicetyp immer 0 und die Protokollnummer immer 1.
TCP	Transmission Control Protocol (TCP) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen. Alle am Datenaustausch beteiligten Computer kennen diese Vereinbarungen und befolgen sie. Es ist damit ein zuverlässiges, verbindungsorientiertes Transportprotokoll 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.

3. Wählen Sie die gewünschte Aktion aus dem entsprechenden Menü.

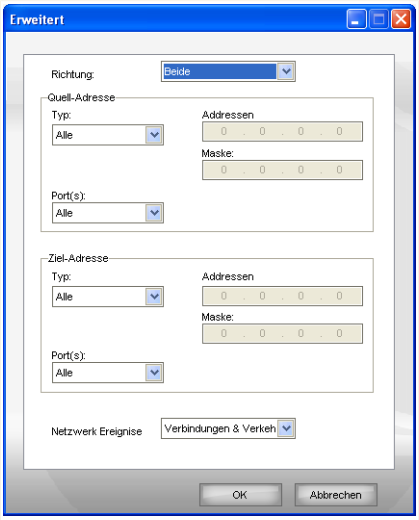
Aktion	Beschreibung
Erlauben	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

4. Wenn das zuvor gewählte Protokol TCP oder UDP ist, können Sie nun wählen ob das ein Zugriff von aussen auf die Anwendung möglich sein soll wenn diese als Server agiert.

   Setzen Sie ein Häckchen bei **Anderen Computern den Zugriff auf die Anwendung erlauben** um der Anwendung zu erlauben/verweigern Ports zu öffnen.

   Wenn Sie wünschen die Aktion nur für Datenverkehr & für UDP beziehungsweise für TCP zu erstellen dann entfernen Sie das entsprechende Häckchen.

Wenn Sie weitere Einstellungen zur Regeln definieren möchten dann klicken Sie auf **Erweitert**. Ein neues Fenster wird geöffnet.



Erweiterte Regeleinstellungen

Folgende Optionen können konfiguriert werden:

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

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

- **Quelladresse** - Legen Sie die Quelladresse fest.

  Um die Quelladresse festzulegen, wählen Sie den Adresstyp aus dem Menü und ergänzen Sie die benötigten Daten. Folgende Optionen stehen zur Verfügung:

Typ	Beschreibung
Alle	Die Regel betrifft alle Quelladressen.
Host	Die Regel betrifft nur einen festgelegten Host. Sie müssen die IP-Adresse des Host eingeben.
Netzwerk	Die Regel betrifft nur das festgelegte Netzwerk. Sie müssen die IP-Adresse oder Subnetmaske des Netzwerks eingeben.
Lokaler Host	Die Regel betrifft nur den lokalen Host als Quelle. Wenn Sie über mehr als eine Netwerkverbindung verfügen dann wählen Sie die Verbindung auf welche die Regeln angewand werden soll. Wenn Sie möchten das die Regel für alle Verbindungen verwendet wird dann wählen Sie **Alle**.
Lokales Netzwerk	Die Regel betrifft nur das lokale Netzwerk als Quelle. Wenn Sie mit mehreren Netzwerken verbunden sind dann wählen Sie im Menü die gewünschte Verbindung. Wenn Sie möchten das die Regel auf alle lokalen Netzwerke zutrifft wählen Sie **Alle**.

  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**.
- **Zieladresse** - Legen Sie die Zieladresse fest.

Um die Zieladresse festzulegen, wählen Sie den Adresstyp und ergänzen Sie die benötigten Daten. Folgende Optionen stehen zur Verfügung:

Typ	Beschreibung
Alle	Die Regel betrifft alle Zieladressen.
Host	Die Regel betrifft nur den festgelegten Host als Ziel. Sie müssen die IP-Adresse des Host eingeben.
Netzwerk	Die Regel betrifft nur das festgelegte Netzwerk als Ziel. Sie müssen die IP-Adresse oder Subnetmaske des Netzwerks eingeben.
Lokaler Host	Die Regel betrifft nur den lokalen Host als Ziel. Wenn Sie über mehr als eine Netwerkverbindung verfügen dann wählen Sie die Verbindung auf welche die Regeln angewand werden soll. Wenn Sie möchten das die Regel für alle Verbindungen verwendet wird dann wählen Sie **Alle**.
Lokales Netzwerk	Die Regel betrifft nur das lokale Netzwerk als Ziel. Wenn Sie mit mehreren Netzwerken verbunden sind dann wählen Sie im Menü die gewünschte Verbindung. Wenn Sie möchten das die Regel auf alle lokalen Netzwerke zutrifft wählen Sie **Alle**.

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**.

- **Netzwerk Ereignis** - Wenn Sie TCP oder UDP als Protokol gewählt haben können Sie auswählen auf welche Netzwerkereignise die Regel zutreffen soll.

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

Klicken Sie auf **Hinzufügen** um eine neue Firewall Regel zu erstellen.

9.3.3. Regeln bearbeiten

Sie können eine Liste der Regeln in der Auflistung ansehen.

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

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

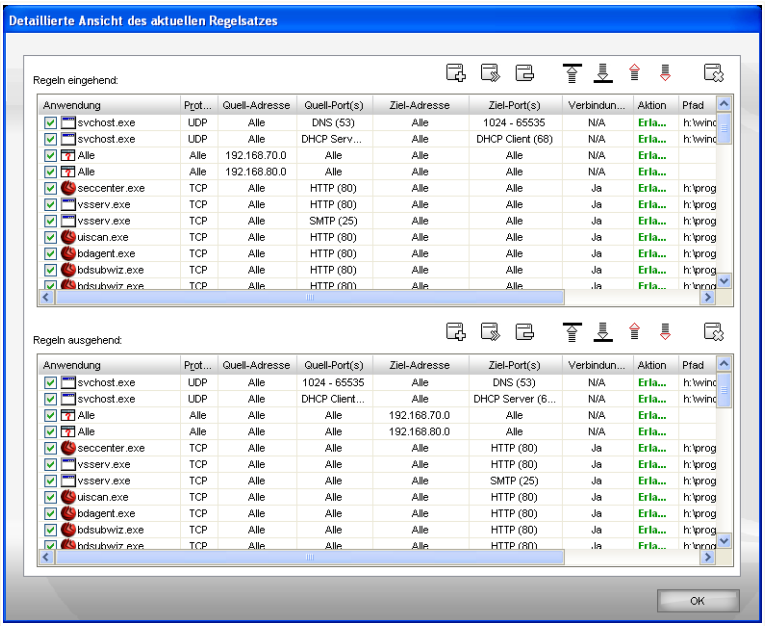
Um ein Objekt aus der Liste zu löschen, klicken Sie auf die **Entfernen**-Schaltfläche.

Um eine Regel zu bearbeiten wählen Sie die Regel aus und klicken Sie auf **Bearbeiten**.

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

9.3.4. Profile ändern

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



Detaillierte Ansicht

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

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

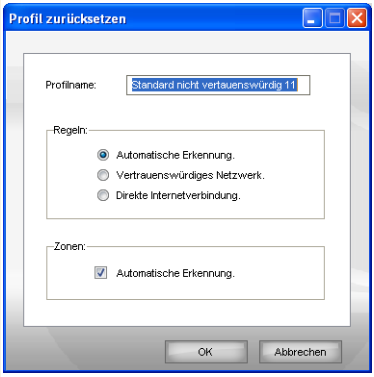
Sie können die Priorität einer Regel erhöhen oder heruntersetzen. Klicken Sie **In der Liste hochsetzen** um die ausgewählte Regel um ein Level nach oben zu setzen. Oder klicken Sie **In Liste heruntersetzen** um die Priorität der ausgewählten Regel herunterzusetzen. Um einer Regel die höchste Priorität zu geben klicken Sie auf die **Als erste**-Schaltfläche. Um einer Regel die niedrigste Priotität zu zuweisen klicken Sie auf die **Als letzte**-Schaltfläche.

Anmerkung
Ein Kontextmenü ist ebenfalls verfügbar und es enthält die folgenden Optionen: **Regel hinzufügen**, **Regel bearbeiten**, **Regel löschen**, **Nach oben**, **Nach unten** und **Alle löschen**.

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

9.3.5. Profil zurücksetzen

Fortgeschrittene Anwender möchten eventuell Ihre Firewall Profile zurücksetzen um den Schutz zu verbessern oder Anpassungen vorzunehmen. Sie können das Profil zurückzusetzen indem Sie auf Sie auf **Profil zurücksetzen** klicken. Das folgende Fenster wird erscheinen:



Profil zurücksetzen

Folgende Optionen können konfiguriert werden:

- **Profilname** - Geben Sie einen neuen Namen für das Profil ein.
- **Regeln** - Legen Sie bitte den Regeltyp für das Profil fest.

  Folgende Optionen stehen zur Verfügung:

Option	*Beschreibung*
Automatisch erkennen	Lässt BitDefender das Netzwerk erkennen und ein passendes Profil erstellen.
Vertrauenswürdiges LAN	Erstellt die grundlegenden Regeln für ein vertrauenswürdiges Netzwerk.
Direktverbindung	Erstellt die grundlegenden Regeln für eine Direktverbindung.

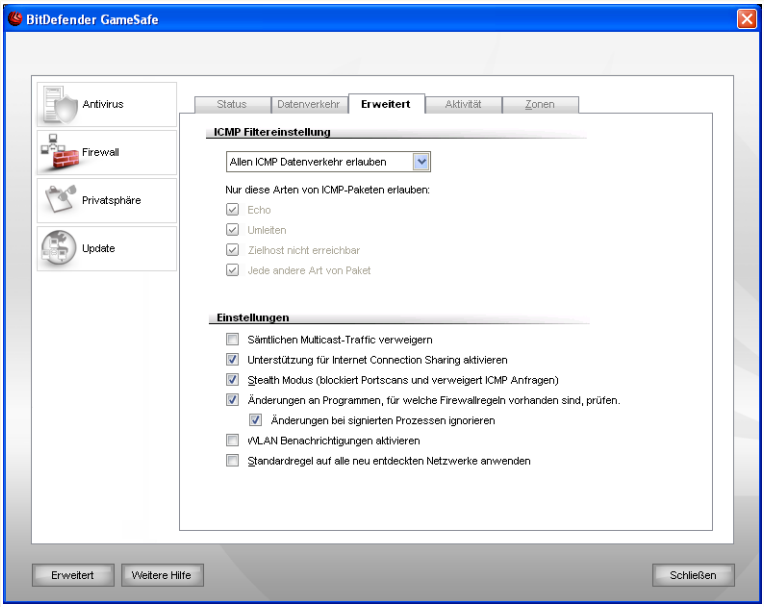
- **Zonen** - Wählen Sie **Automatische Erkennung** um BitDefender die passenden Zonen automatisch erstellen zu lassen.

Klicken Sie auf **OK**, um dieses Fenster zu schließen und das Profil zurück zu setzen.

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

9.4. Weitere Einstellungen

Um die erweiterten Einstellungen der BitDefender Firewall zu bearbeiten klicken Sie auf **Firewall>Erweitert** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



Weitere Einstellungen

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

9.4.1. ICMP Filter Einstellungen konfigurieren

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

- Klicken Sie auf **Gesamten ICMP Verkehr erlauben** wenn Sie sämtlichen ICMP Datenverkehr erlauben möchten.
- Klicken Sie auf **Gesamten ICMP Verkehr blockieren** wenn Sie sämtlichen ICMP Datenverkehr unterbinden möchten.
- **Eigene ICMP Filtereinstellungen** - Hier können Sie die Filtereinstellungen bearbeiten. Dies macht möglich die Typen von ICMP-Traffic selbst festzulegen.

  Folgende Optionen stehen zur Verfügung:

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

Option	Beschreibung
	wird die Nachricht nicht gesendet, obwohl eine bessere Verbindung besteht.
Zielhost nicht erreichbar	Dies ist eine Nachricht des ICMP Protokolls, die durch den Router generiert wird und mitteilt, dass das E-Mail Programm den Empfänger nicht erreichen kann, es sein denn, der Datensatz hat eine Mulitcast Adresse. Gründe dafür sind, dass die physikalische Adresse zum Host nicht existiert (die Distanz ist unerheblich), das angesprochene Protokoll oder der Port nicht aktiv sind oder die Daten fragmentiertwerden müssen und der Befehl „nicht fragmentieren“ist aktiviert.
Jede andere Art von Paket	Wenn Sie diese Option frei geschaltet ist, werden alle anderen Pakete außer **Echo**, **Zielhost nicht erreichbar** oder **Umleiten** durchgelassen.

9.4.2. Weitere Einstellungen der Firewall konfigurieren

Folgende Aktionen stehen zur Verfügung:

- **Sämtlichen Multicast-Traffic verweigern** - Mit dieser frei geschalteten Option werden alle erhaltenene Multicast Pakete fallengelassen.

  Multicast Datenverkehr ist auf eine spezielle Gruppe innerhalb eines Netzwerkes ausgerichtet. Pakete werden an eine spezielle Adresse gesendet von der aus der Multicast Clients sie empfangen kann, wenn er es erlaubt.

  Wenn zum Beispiel ein Mitglied im Netzwerk, der einen TV-Tuner zur Verfügung hat, an alle Mitglieder im Netzwerk oder per Multicast an spezielle Adressen einen Video Stream aussendet, können die Computer mit der Multicast Adresse dieses Paket akzeptieren oder ablehnen. Wenn das Paket akzeptiert wird, kann der Stream mit den Multicast Clients angesehen werden.

  Große Mengen an Multicast Datenverkehr benötigen sehr viel Bandbreite und Ressourcen. Wenn Sie diese Option auswählen wird jedes empfangene Multicast Paket abgelehnt. Wie auch immer, es wird nicht empfohlen diese Option auszuwählen.
- **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).

- **Stealth-Modus** - Macht Ihren Computer unsichtbar für schädliche Software und Hacker.

  Ein einfacher Weg um herauszufinden, ob Ihr Computer angreifbar ist, ist es die Ports zu verbinden und zu sehen, ob eine Antwort erfolgt. Das ist ein sogenannter Port Scan.

  Personen oder Software mit betrügerischer Absicht sollten keinesfalls erfahren, dass Ihr Computer überhaupt existiert, geschweige denn mit dem Netzwerk Daten austauscht. Der **Stealth-Modus** verhindert, dass Ihr Computer auf Zugriffsversuche reagiert, die versuchen, an Informationen über offene Ports und deren Herkunft zu gelangen.
- **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.

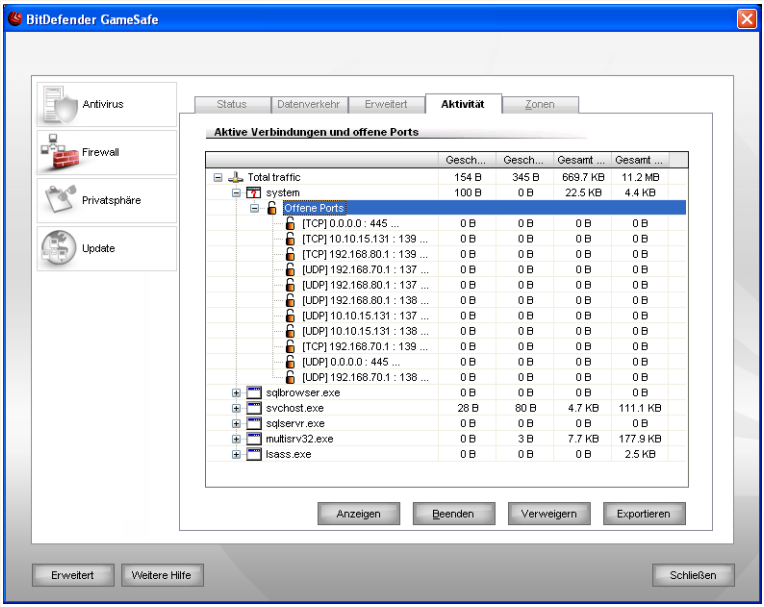
  Anmerkung
  Wir empfehlen Ihnen die Option aktiviert zu lassen und nur Anwendungen Zugriff zu gewähren bei welchen Sie erwarten das diese Zugriff zum Internet benötigen.

  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** - Aktiviert/deaktiviert die WLAN Benachrichtigungen
- **Das gleiche (allgemeine) Profil für alle neuen Netzwerke anwenden** - erstellt ein Standard (allgemeines) Firewall- Profil, mit dem Namen `Allgemeines Netzwerk`, und wendet es an, sobald eine neue Netzwerkkonfiguration entdeckt wird. Wenn Sie zu einer ehemaligen Netzwerkkonfiguration zurückkehren, für die bereits ein Firewall-Profil existiert, so wird das entsprechende Firewall-Profil geladen und nicht das Allgemeine.

9.5. Verbindungskontrolle

Um die aktuellen Netzwerk/Internetaktivitäten zu verfolgen (TCP und UDP) und um den Firewall-Bericht einzusehen klicken Sie in der Einstellungskonsole auf **Firewall>Aktivität**. Das folgende Fenster wird erscheinen:



Verbindungskontrolle

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.

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.

Klicken Sie auf **Verweigern**, um eine Regeln zu erstellen, die den Datenverkehr für ausgewählte Anwendungen, Ports oder Verbindungen einschränken. Sie werden aufgefordert Ihre Auswahl zu bestätigen. Die Regeln können unter dem Link Datenverkehr für weitere Feineinstellungen eingesehen werden.

Anmerkung
Um eine Anwendung, einen Port oder eine Verbinfung zu sperren, so können Sie auch mit der rechten Maustaste darauf klicken und **Sperren** wählen.

Klicken Sie auf **Stopp** um alle Instanzen eines ausgewählten Prozesses zu beenden. Sie werden aufgefordert Ihre Entscheidung zu bestätigen.

Anmerkung
Um einen Prozess zu stoppen, können Sie auch mit der rechten Maustaste darauf klicken und **Stopp** wählen.

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

Außerdem kann eine Liste generiert werden, die Aufschluss über Aktivitäten gibt (geprüfte Ports, Verweigern von Zugriffsversuchen, Tarnkappenmodus oder Datenverkehr gemäß den Einstellungen). Für diese detaillierte Liste klicken Sie bitte auf **Log anzeigen**. Diese Datei finden Sie alternativ auch im Anwendungsdaten-Ordner des angemeldeten Benutzers im Verzeichnis: `... Bitdefender\BitDefender Firewall\bdfirewall.txt` auf Ihrer lokalen Festplatte.

9.6. Netzwerk-Zonen

Eine Zone ist eine IP-Adresse oder ein Bereich von UP-Adressen für welche eine spezielle Regel innerhalb des Profils angelegt wurde. Diese Zonen können den Netzwerkzugriff entweder erlauben (vertrauenswürdige Zone) oder aber verweigern (nicht vertrauenswürdige Zone).

Standardmässig erkennt BitDefender das Netzwerk mit welchem Sie verbunden sind automatisch und fügt dieses entsprechend den Netzwerk-Zonen hinzu.

Anmerkung
Wenn Sie mit meheren Netzwerken verbunden sind, können entsprechend der Konfiguration, mehrere Zonen hinzugefügt werden.

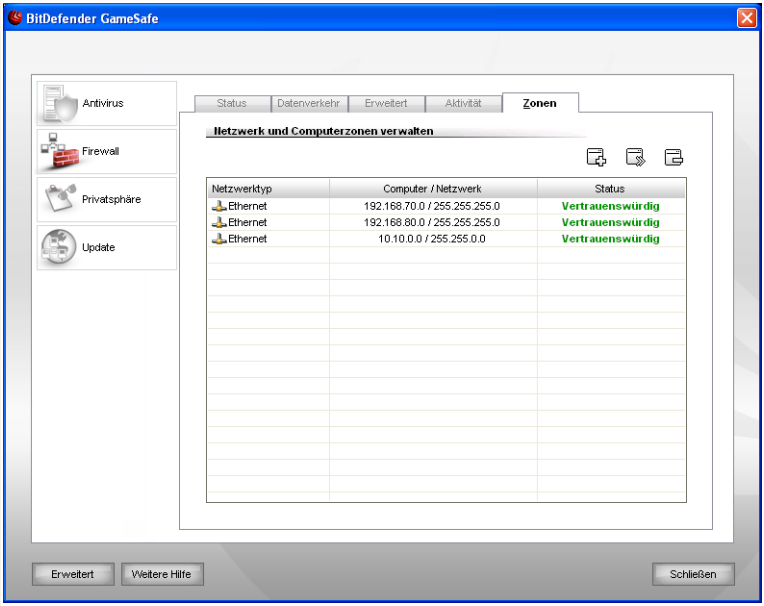
Vertrauenswürdige Zonen werden standardmässig bei folgenden Netzwerkkonfigurationen hinzugefügt:

- **Private IP ohne Gateway** - Der Computer ist Teil eines lokalen Netzwerks (LAN) und ist nicht direkt mit dem Internet verbunden.
- **Private IP mit Domaincontroller** - Der Computer ist Teil eines Netzwerkes und mit einer Domain verbunden.

Nicht vertrauenswürdige Zonen werden standardmässig bei folgenden Netzwerkkonfigurationen hinzugefügt:

- **Offenes (nicht geschütztes) WLAN** - Der Computer ist Teil eines WLAN (wireless local area network).

Um die Netzwerk-Zonen zu verwalten klicken Sie in der Einstellungskonsole auf **Firewall>Zonen**. Das folgende Fenster wird erscheinen:



Netzwerk-Zonen

Hier können Sie einsehen welches Zonen momentan im Profil vorhanden sind. Für jede Zone können Sie den Netzwerktyp (Ethernet, Wireless, PPP und so weiter), den Computer oder das Netzwerk welches die Zone darstellt, sowie ob es sich um eine vertauenswürdige Zone handelt oder nicht einsehen.

Um eine Zone zu bearbeiten markieren Sie diese und klicken Sie auf **Zone bearbeiten** oder doppelklicken Sie auf diese.

Anmerkung

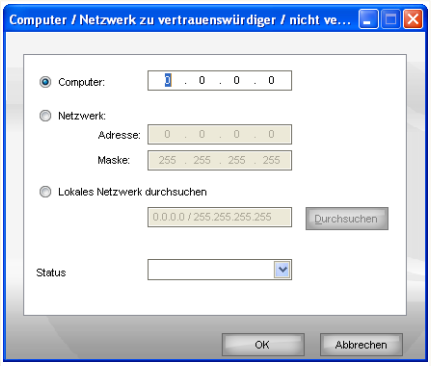
Standardmässig fügt BitDefender Wireless Netzwerke als nicht vertrauenswürdige Zonen ein. Sollten Sie zu einem Ad-hoc Wireless Netzwerk mit vertrauenswürdigen Computern verbunden sein, dann wünschen Sie evtl. die gewählte Zone zu bearbeiten um einen Datenaustausch mit anderen Geräten zu gewährleisten. Hierzu müssen Sie die Zone auf vertrauenswürdig umstellen.

Um eine Zone aus der Liste zu löschen, klicken Sie auf die **Zone löschen**-Schaltfläche.

9.6.1. Zone hinzufügen

Sie können Zonen manuell hinzufügen. Dies erlaubt Ihnen, z.B. in einem offenen Wireless Netzwerk, Dateien nur mit Ihrem Freunden auszutauschen (indem Sie die Computer der Freunde als vertrauenswürdige Zone angeben) oder um einem Computer in einer vertrauenswürdigen Umgebung den Zugriff zu verweigern. (indem Sie diesen als nicht vertrauenswürdig hinzufügen)

Um eine neue Zonen hinzuzufügen klicken Sie auf die **Zone hinzufügen** -Schaltfläche. Das folgende Fenster wird erscheinen:



Zone hinzufügen

Um eine Zone hinzuzufügen befolgen Sie folgende Schritte:

1. Legen Sie fest ob Sie einen Computer des Netzwerks oder das komplette Netzwerk als Zone hinzufügen möchten. Sie können hierzu eine der folgenden Methoden wählen:
   - Um einen bestimmten Computer hinzuzufügen wählen Sie **Computer** und geben Sie desen IP-Adresse an.
   - Um ein bestimmtes Netzwerk hinzuzufügen wählen Sie **Netzwerk** und geben Sie dessen IP-Adresse und Subnetzmaske ein.
   - Das lokale Netzwerk durchsuchen um einen Computer oder ein Netzwerk hinzuzufügen.

     Um das lokale Netzwerk zu durchsuchen klicken Sie auf **Netzwerk durchsuchen** und dann auf **Durchsuchen**. Ein neues Fenster erscheint in welchem Sie die gewünschten Computer oder Netzwerke auswählen können.

Wählen Sie den gewünschten Computer oder Netzwerke aus und klicken Sie auf **OK** um diese hinzuzufügen.

2. Wählen Sie aus dem Menü welchen Typ von Zone Sie erstellen möchten (Vertrauenswürdig oder nicht vertrauenswürdig).
3. Klicken Sie auf **OK** um die Zone hinzuzufügen.

10. Privatsphäre

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.

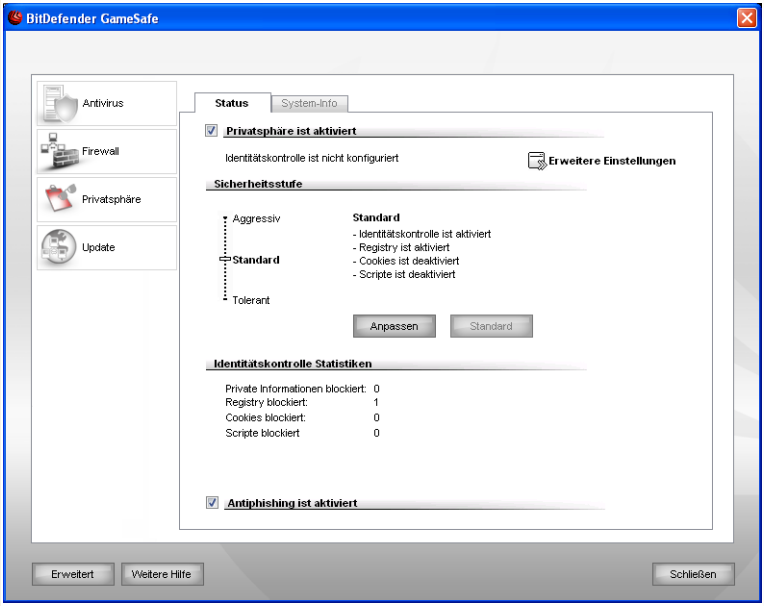
BitDefender prüft auch die von Ihnen besuchten Webseiten und warnt Sie sobald ein Phisingversuch entdeckt wird.

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

- Privatsphäre Status
- Weitere Einstellungen - Identität
- Weitere Einstellungen - Registrierung
- Weitere Einstellungen - Cookie
- Weitere Einstellungen - Skript
- System-Informationen
- Antiphishingleiste

10.1. Privatsphäre Status

Um die Privatsphäre zu konfigurieren und Informationen dazu zu erhalten klicken Sie auf **Privatsphäre>Status** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



Privatsphäre Status

10.1.1. Privatsphäre

Wichtig
Um Datendiebstahl und den Schutz der Privatsphäre zu gewährleisten, lassen Sie die **Privatsphäre** bitte immer aktiviert.

Die **Privatsphäre** schützt Ihren Computer durch 5 wichtige Kontrollmechanismen:

- Identität - schützt Ihre vertraulichen Daten indem jeglicher ausgehender HTTP und SMTP Datenverkehr aufgrund der erstellten Regeln unter Identität geprüft wird.

Anmerkung
Im unteren Bereich können Sie die **Antispyware Statistiken** einsehen.

- 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.

Um diese Einstellungen zu konfigurieren klicken Sie Weitere Einstellungen.

Sicherheitsgrad 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:

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

Sie können die Ebene für den gewünschten Schutz einstellen. Klicken Sie auf **Ebene anpassen**. Wählen Sie in dem sich öffnenden Fenster die Schutzkontrollen, die Sie aktivieren möchten und klicken Sie auf **OK**.

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

10.1.2. Antiphishingschutz

Phising ist eine kriminelle Aktivität im Internet durch welche versucht wird Leute mit Tricks dazu zu bringen Private Informationen herauszugeben.

Meist werden Phisingversuche durch das senden von Massenemails bewerkstelligt. Hierbei hoffen die Sender das die gesendete Nachricht auf einige der Empfänger zutrifft und diese private Informationen herausgeben.

Im Normalfall versucht eine Phisingnachricht an Daten zu einem Onlinekonto zu gelangen. Meist wird hierbei eine legitime Seite kopiert und der Benutzer aufgefordert die Daten einzugeben. Z.B. könnten Sie gebeten werden Ihre Zugangsdaten zu

bestätigen, oder Ihre Bankdaten anzugeben. Manchmal wird auch vorgegeben das Ihr Zugang gespeert wird wenn Sie den angegebenen Link nicht verwenden.

Ausserdem verwendet Spyware oftmals auch Trojaner als Keylogger um Ihre Daten direkt von Ihrem Computer zu stehlen.

Die häufigsten Ziele von Phishing sind Kunden von Online-Zahldiensten, wie z.B. Ebay und Paypal sowie Kunden von Banken welche Onlinedienste anbieten. Oftmals werden Benutzer von Online-Kommunikationsseiten Phishingziele zum Zweck von Identitäts-Diebstahl.

Um den Schutz vor Phishing aus dem Internet zu gewährleisten, halten Sie die **Antiphishing** Funktion jederzeit aktiviert. Dann ist BitDefender in der Lage jede Webseite welche Sie besuchen zu prüfen um sicherzustellen das es sich nicht um eine Phishingseite handelt. Eine Whitelist von Webseiten welche nicht durch BitDefender geprüft werden kann ebenfalls erstellt werden.

Um den Antiphsihingschutz und die Whitelist zu konfigurieren verwenden Sie am besten die BitDefender Antiphishingleiste im Internet Explorer. Für weitere Informationen besuchen Sie bitte „*Antiphishingleiste*“ (S. 130).

10.2. Weitere Einstellungen - Identität

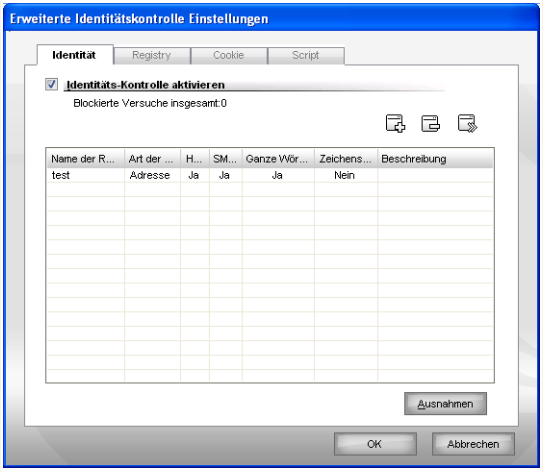
Vertrauliche Daten zu sichern ist für alle Anwender äußerst wichtig. Datenklau hat mit der Entwicklung der Internet Kommunikation standgehalten und wendet immer wieder neue Methoden an um Anwender zu täuschen und private Informationen zu erhalten.

Identitätskontrolle hilft Ihre privaten Daten zu sichern. Sie prüft den HTTP oder SMTP Datenverkehr, oder beides, auf spezielle Strings, welche Sie definieren. Wenn eine Übereinstimmung mit einer Webseite oder einer E-Mail Adresse gefunden wird, werden diese sofort geblockt.

BitDefender enthält eine Multiuser Unterstützung wodurch kein anderer Benutzer Ihre Regeln einsehen kann.

Privatsphäreregeln können in der Sektion **Identität** konfiguriert werden. Um diese Sektion zu öffnen klicken Sie bitte auf **Weitere Einstellungen** und wählen Sie den Reiter **Identität**.

Anmerkung
Um das **Weitere Einstellungen** Fenster zu öffnen, klicken Sie auf **Privatsphäre>Status** in der Einstellungskonsole und klicken Sie auf **Weitere Einstellungen**.



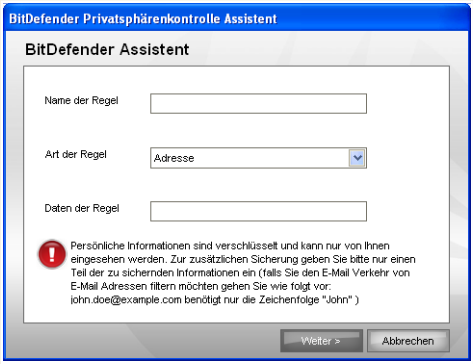
Antispyware

10.2.1. Erstellen von Privatssphäreregeln

Die Regeln müssen manuell eingegeben werden (klicken Sie **Hinzufügen** und wählen Sie die entsprechenden Parameter für die Regel). Der Regel-Assistent erscheint.

Der Konfigurationsassistent wird in 3 Schritten eingestellt.

Schritt 1/3 - Typ und Richtung auswählen



Typ und Richtung auswählen

Geben Sie den Namen der Regel im Bearbeitungsfeld ein.

Hier können Sie die Parameter auswählen:

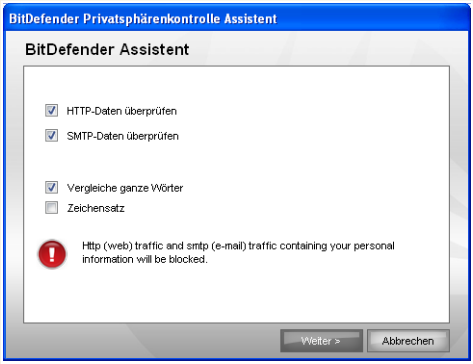
- **Regeltyp** - wählen Sie die Regel aus (Adresse, Name, Kreditkartennummer, PIN, TAN etc).
- **Daten der Regel** - Geben Sie die Regel für Daten ein.

> ***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 2/3 - Datenverkehr auswählen



Datenverkehr auswählen

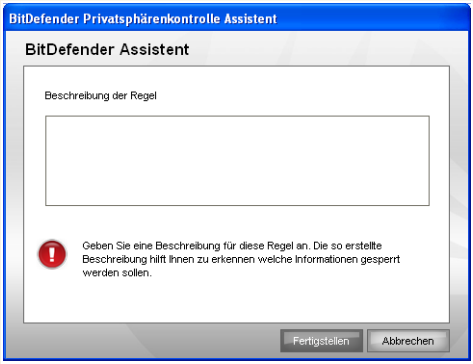
Bitte wählen sie den Datenverkehrstyp welchen BitDefender prüfen soll. Folgende Optionen stehen zur Verfügung:

- **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.

Sie können wählen ob die Regeln nur zutrifft wenn die Regeldaten wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

Klicken Sie auf **Weiter**.

Schritt 3/3 - Beschreibung der Regel



Beschreibung der Regel

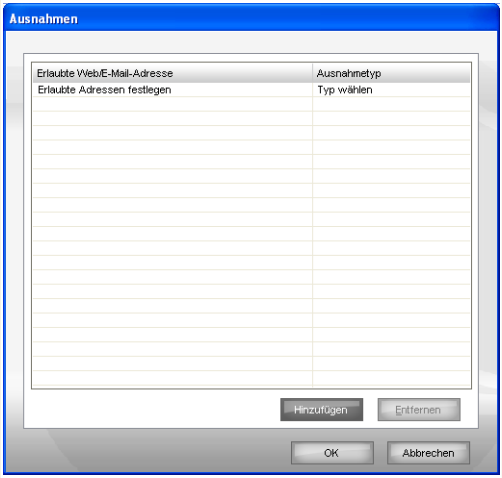
Geben Sie eine kurze Beschreibung der Regel im Eingabefeld ein.

Klicken Sie auf **Fertigstellen**.

10.2.2. 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 **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 EMailadresse eingegeben haben dann wählen Sie **SMTP**.

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

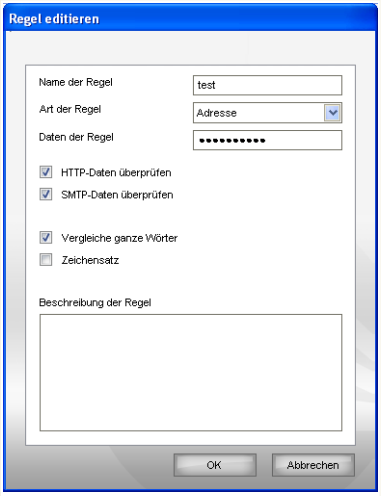
Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.2.3. Regeln bearbeiten

Sie können eine Liste der Regeln in der Aufstellung ansehen.

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

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



Regel bearbeiten

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

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

10.3. Weitere Einstellungen - Registrierung

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

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

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

Registry Alarm

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

Wenn Sie möchten, dass BitDefender Ihre Antwort speichert, wählen Sie die Option **Immer diese Aktion für diese Anwendung ausführen**. Dadurch wird eine Regel erstellt wodurch die selbe Aktion nochmals ausgeführt wird wenn die Anwendung versucht einen Registryeintrag zu ändern.

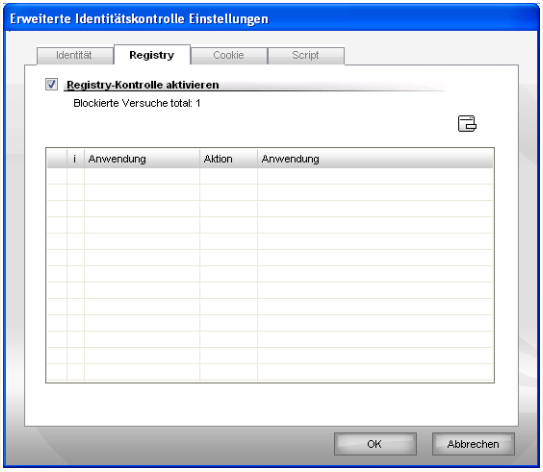
Anmerkung

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.

Jede gemerkte Regel kann im Reiter **Registry** für weitere Einstellungen eingesehen werden. Um diese Sektion zu öffnen klicken Sie bitte auf **Weitere Einstellungen** und wählen Sie den Reiter **Registry**.

Anmerkung

Um das **Weitere Einstellungen** Fenster zu öffnen, klicken Sie auf **Privatsphäre>Status** in der Einstellungskonsole und klicken Sie auf **Weitere Einstellungen**.



Registry Kontrolle

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 vorrübergehend zu deaktivieren, ohne diese zu löschen, entfernen Sie das entsprechende Häckchen vor der Regel.

Um die Aktion für eine Regel zu ändern doppelklicken Sie auf das Aktionsfeld und wählen Sie die gewünschte Aktion aus der Liste.

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

10.4. Weitere Einstellungen - Cookie

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

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

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

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

Cookie Alarm

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

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

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

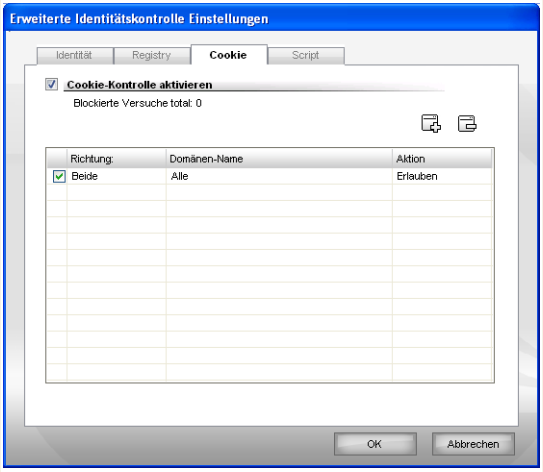
Anmerkung

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

Jede erstellte Regel kann später über den Reiter **Cookies** aufgerufen und weiter bearbeitet werden. Um diese Sektion zu öffnen klicken Sie bitte auf **Weitere Einstellungen** und wählen Sie den Reiter **Anwahl**.

Anmerkung

Um das **Weitere Einstellungen** Fenster zu öffnen, klicken Sie auf **Privatsphäre>Status** in der Einstellungskonsole und klicken Sie auf **Weitere Einstellungen**.



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.

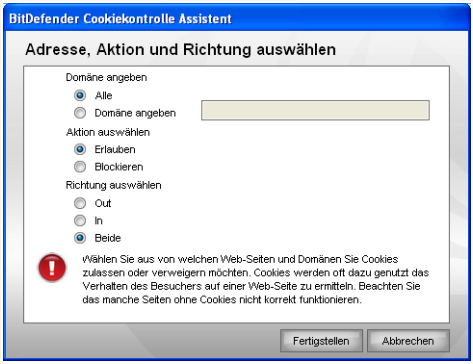
Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Alarm-Fenster) oder manuell (klicken Sie **Hinzufügen** und wählen Sie die Parameter für die Regel). Der Regelassistent erscheint.

10.4.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

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



Domäne(n) und Aktion auswählen

Hier können Sie die Parameter auswählen:

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

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

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

Typ	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf Cookies, welche von der verbundenen Seite versendet werden.
Eingehend	Die Regel bezieht sich nur auf Cookies welche an die verbundene Seite versendet werden.
Beide	Die Regeln finden in beide Richtungen Anwendung.

Klicken Sie auf **Fertigstellen**.

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

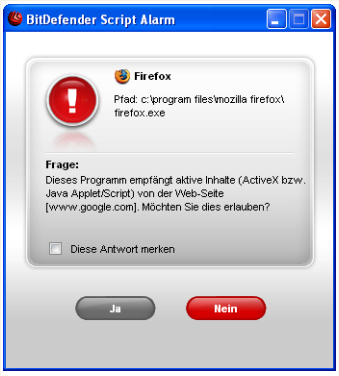
Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.5. Weitere Einstellungen - Script

Skripte und andere Programmierungen, wie z. B. ActiveX und Java applets, die für interaktive Webseiten verwendet werden, können verheerende Schäden verursachen. ActiveX-Elemente können zum Beispiel Zugriff auf Ihre Daten erlangen und sie auslesen, Daten von Ihrem Computer löschen, Passwörter auslesen und Nachrichten versenden, wenn Sie online sind. Sie sollten daher solche aktiven Elemente nur von Ihnen bekannten und zuverlässigen Seiten akzeptieren.

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

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



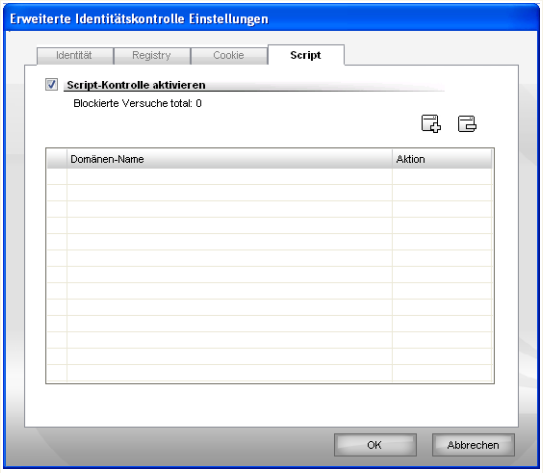
Skript Alarm

Der Namen der Quelle wird Ihnen angezeigt.

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

Jede erstellte Regel kann später über den Reiter **Skripte** aufgerufen und weiter bearbeitet werden. Um diese Sektion zu öffnen klicken Sie bitte auf **Weitere Einstellungen** und wählen Sie den Reiter **Script**.

Anmerkung
Um das **Weitere Einstellungen** Fenster zu öffnen, klicken Sie auf **Privatsphäre>Status** in der Einstellungskonsole und klicken Sie auf **Weitere Einstellungen**.



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.

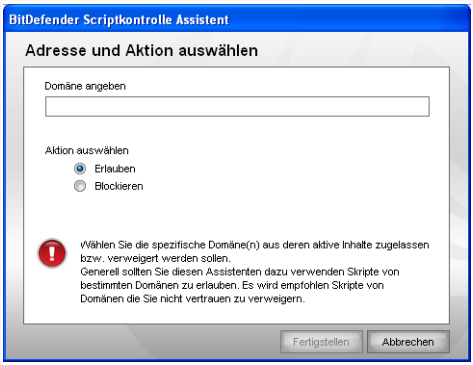
Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Regel löschen**. Um eine Regel anzupassen doppelklicken Sie auf diese. Um eine Regel zeitweise zu deaktivieren ohne diese zu löschen, entfernen Sie die Markierung aus dem nebenstehende Kästchen durch anklicken.

Die Regeln können automatisch (durch das Alarm-Fenster) oder manuell (klicken Sie **Hinzufügen** und wählen Sie die Parameter für die Regel). Der Regelassistent erscheint.

10.5.1. Konfigurations-Assistent

Der Konfigurations-Assistent besteht aus einem einzelnen Schritt.

Schritt 1/1 - Adresse und Aktion auswählen



Adresse und Aktion auswählen

Hier können Sie die Parameter auswählen:

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

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

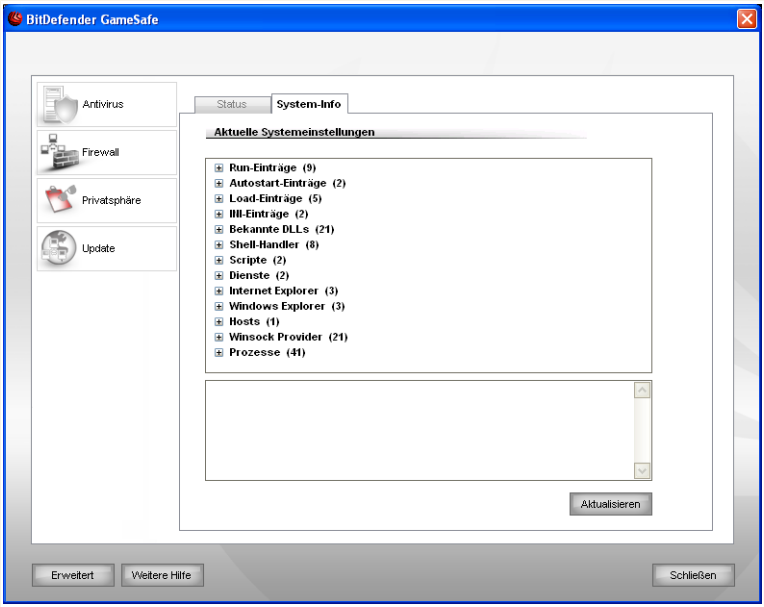
Klicken Sie auf **Fertigstellen**.

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

10.6. System-Informationen

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

Um diese Informationen anzuzeigen klicken Sie auf **Privatsphäre>System Info** in der Einstellungskonsole. Das folgende Fenster wird erscheinen:



System-Informationen

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:

- **Entfernen** - löscht das ausgewählte Objekt. Klicken Sie auf **Ja** um Ihre Einstellung zu bestätigen.

Anmerkung
Wenn Sie während der aktuellen Sitzung nicht nochmals gefragt werden möchten dann wählen Sie **Diese Sitzung nicht nochmals fragen**.

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

Anmerkung
Je nach ausgewähltem Objekt wird eine der Schaltflächen **Entfernen** oder **Gehe zu**, oder beide, nicht erscheinen.

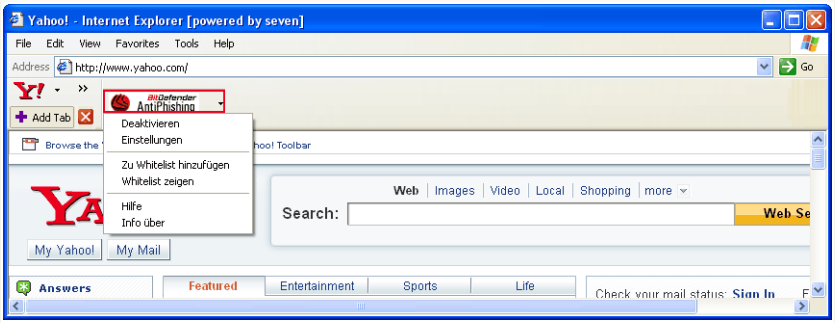
10.7. Antiphishingleiste

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.

Sie können die Antiphishingeinstellungen und die Whitelist leicht über die BitDefender Antiphishingleiste im Internet Exlorer konfigurieren.

Die Antiphishingleiste, symbolisiert durch das **BitDefender Icon**, finden Sie im oberen Bereich des Internet Explorers. 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.

  Folgende Optionen stehen zur Verfügung:
  - **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.

11. Update

Jeden Tag werden neue Viren entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie das Programm BitDefender stets mit den neuesten Virensignaturen betreiben.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung verfügen, arbeitet 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 verfügbar ist wird dieses je nach Einstellungen unter Update Einstellungen entweder auf Nachfrage oder automatisch geupdatet.

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:

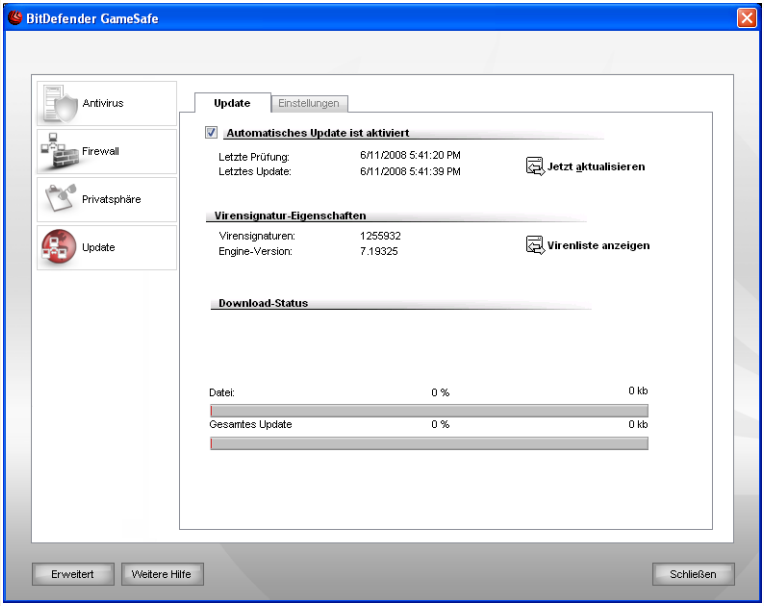
- **Updates für die Antivirus-Module** - wenn neue Bedrohungen auftreten, müssen die Dateien, in den die Virensignaturen enthalten sind, aktualisiert werden, damit ein kontinuierlicher und aktueller Schutz auch vor den neuen Gefahren gewährleistet ist. Diese Update-Art wird auch als **Virendefinitions-Update** bezeichnet.
- **Updates für die 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**.

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

- Automatisches Update
- Update-Einstellungen

11.1. Automatisches Update

Um Informationen zum Update und den Einstellungen hierzu zu erhalten klicken Sie in der Einstellungskonsole auf **Update>Update**. Das folgende Fenster wird erscheinen:



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.

Klicken Sie auf **Virenliste anzeigen** um eine HTML-Liste mit allen verfügbaren Virensignaturen anzuzeigen. Sie können die Datenbank auf spezifische Signatur hin durchsuchen oder klicken Sie **BitDefender Virus Liste** um auf die BitDefender Online Signatur Datenbank zuzugreifen.

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.

11.1.1. Benutzergesteuertes Update

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

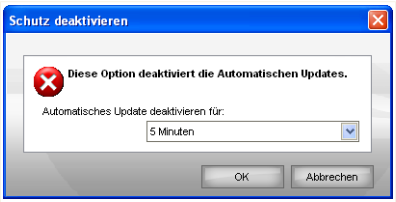
Das **Update** Modul verbindet Ihren Computer automatisch mit dem BitDefender Update Server und benachrichtigt Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt ob das Update erfolgen soll, oder das Update erfolgt automatisch.

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

Anmerkung
Sollten Sie mit einer Einwahlverbindung mit dem Internet verbunden sein, so wird empfohlen regelmäßig ein manuelles Update durchzuführen.

11.1.2. Automatisches Update deaktivieren

Wenn Sie das Automatische Update deaktivieren erscheint ein Warnfenster.



Automatisches Update deaktivieren

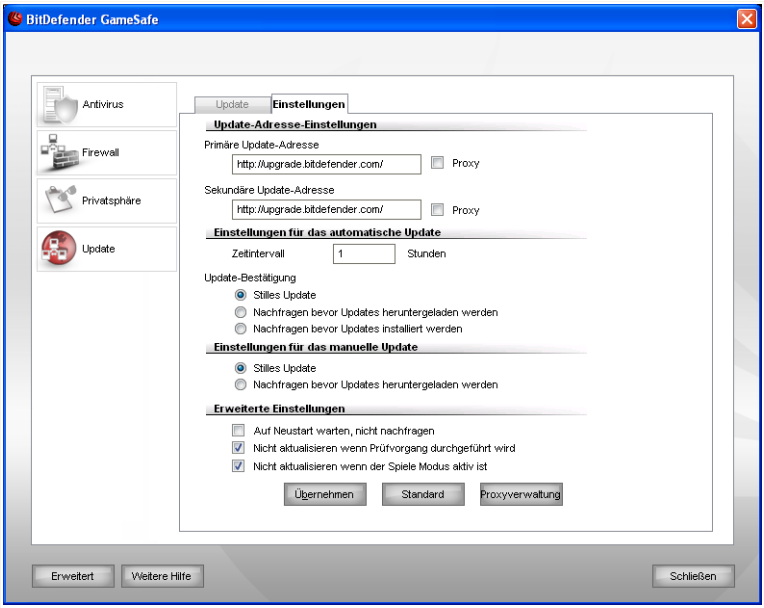
Sie müssen Ihre Einstellung bestätigen indem Sie definieren wie lange das Automatisch Update deaktiviert werden soll. Zur Verfügung stehen die Optionen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.

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.

11.2. Update-Einstellungen

Die Updates können im lokalen Netzwerk, über das Internet, direkt oder über einen Proxy-Server durchgeführt werden. Standardmässig prüft BitDefender jede Stunde auf neue Updates und installiert diese ohne Ihr zutun.

Um Updateeinstellungen vorzunehmen und evtl Proxys zu konfigurieren klicken Sie in der Einstellungskonsole auf **Update>Einstellungen**. Das folgende Fenster wird erscheinen:



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.

11.2.1. 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.

Anmerkung
Weitere Informationen finden Sie unter „*Proxyverwaltung*“ (S. 138)

11.2.2. 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.

Anmerkung
Sie werden gefragt bevor das Update heruntergeladen wird, auch wenn Sie den Sicherheitcenter gerade nicht geöffnet haben.

- **Nachfragen bevor Updates installiert werden** - BitDefender frägt den Benutzer bevor ein Update installiert wird.

Anmerkung
Sie werden gefragt bevor das Update installiert wird, auch wenn Sie den Sicherheitcenter gerade nicht geöffnet haben.

11.2.3. 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.

Anmerkung
Sie werden gefragt bevor das Update heruntergeladen wird, auch wenn Sie den Sicherheitcenter gerade nicht geöffnet haben.

11.2.4. 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.

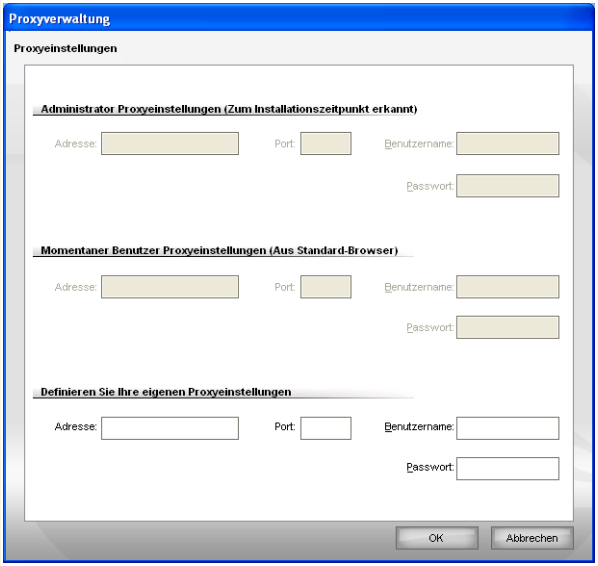
- **Nicht aktualisieren wenn der Spiele Modus aktiv ist** - Wenn der Spiele Modus aktiviert ist wird BitDefender kein Update durchführen. Durch diese Option können Sie den Einfluss der Anwendung, auf die Geschindigkeit während des Spielens minimieren.

11.2.5. 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.

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

BitDefender Notfall CD

12. Überblick

BitDefender GameSafe 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/

12.1. 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.

12.2. 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.

13. 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.

13.1. 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.

LinuxDefender Startbildschirm

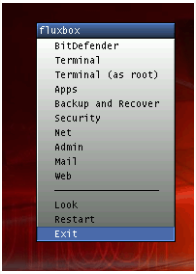
Nach dem Starten wird automatisch ein Virensignaturupdate durchgeführt. Dieser Vorgang keine einen gewissen Zeitraum in Anspruch nehmen.

Sobald der Bootvorgang abgeschlossen wurde, wird der Desktop angezeigt. Sie können nun damit beginnen die BitDefender Notfall CD zu verwenden.

Der LinuxDefender Desktop

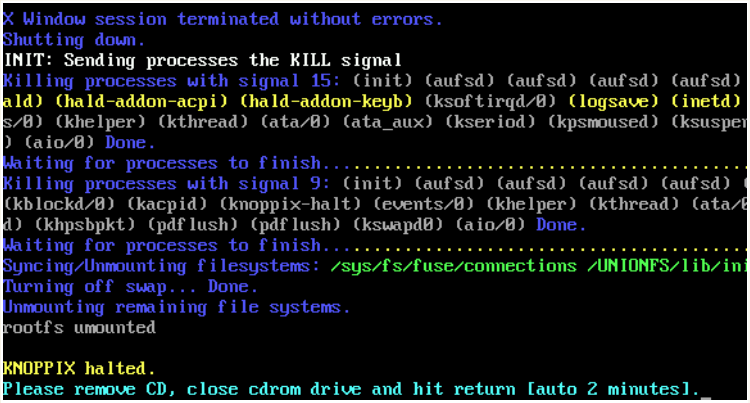
13.2. BitDefender Notfall CD stoppen

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

13.3. 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**.

Alternativ kann der Prüfvorgang auch mit Rechten des Benutzers root über den Terminal durchgeführt werden. Geben Sie dazu den folgenden Befehl im Terminal ein und bestätigen Sie mit der Taste ENTER.

```
# bdscan /path/to/scan/
```

13.4. 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**.

13.5. 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:

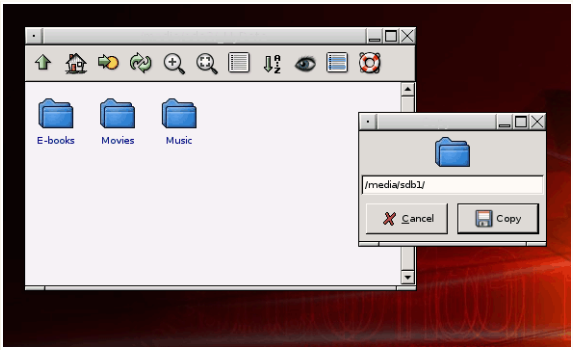
1. Legen Sie die BitDefender Notfall CD in das CD-Laufwerk, stecken Sie den USB Stick ein und starten Sie dann Ihren Computer neu.
2. Warten Sie bis die BitDefender Notfall CD gestartet wurde. Das folgende Fenster erscheint.

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.

4. Durchsuchen Sie die Partitionen nach den gewünschten Dateien und Ordnern.
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**.

Hilfe erhalten

14. 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.Es ist jedoch leider nicht vollkommen auszuschließen, dass es bei der Bearbeitung Ihrer Anfragen zu Engpässen kommen kann und bitten diesbezüglich um Nachsicht.

Wir freuen uns auf die Kontaktaufnahme zu unseren technischen Support und stehen Ihnen mit Rat und Tat zur Seite. Nutzen Sie hierfür einfach unseren E-Mail Kontakt support@bitdefender.de oder rufen Sie uns Werktags unter (075 42) 94 44-60 an.Falls Sie den Weg über E-Mail bevorzugen, teilen Sie uns bitte mit, welches Produkt und Betriebssystem Sie verwenden und beschreiben Sie das aufgetretene Problem so detailliert als möglich.

14.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen und hilfreichen Tipps & Tricks rund um die Produkte.In leicht verständlicher Form bietet die Knowledge Base Informationen, Anleitungen und Berichte über neue Patches und behobene Probleme.Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar.Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Knowledge Base ist jederzeit unter der Internet-Adresse http://kb.bitdefender.de erreichbar.

14.2. Nach Hilfe fragen

14.2.1. 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.

Webseite: www.bitdefender.com/gamesafe

14.3. Kontaktinformationen

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.

14.3.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Technische Beratung: support@bitdefender.de
Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren.
Vertrieb: vertrieb@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
presse@bitdefender.de
Jobs: jobs@bitdefender.com
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Viren melden: abuse@bitdefender.com
Webseite: http://www.bitdefender.de
Webseite: http://www.bitdefender.de
Lokale Anbieter: http://www.bitdefender.de
BitDefender Knowledge-Base: http://kb.bitdefender.de

14.3.2. 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.

U.S.A.

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Web: http://www.bitdefender.de
Technical support:

- E-Mail: support@bitdefender.com
- Telefon:
  - 1-888-868-1873 (Nur registrierte Nutzer; nur in den USA)
  - 1-954-776-6262 (Nur registrierte Nutzer)

Kundenservice:

- E-Mail: customerservice@bitdefender.com
- Telefon:
  - 1-888-868-1873 (Nur registrierte Nutzer; nur in den USA)
  - 1-954-776-6262 (Nur registrierte Nutzer)

Deutschland

BitDefender GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Deutschland
Tel: +49 7542 9444 60
Fax: +49 (0)75 42 - 94 44 99
support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: http://www.bitdefender.de
Technische Beratung: support@bitdefender.de

Großbritannien und Irland

One Victoria Square
Birmingham

B1 1BD
Phone: +44 207 153 9959
Fax: +40 21 - 233 07 63
support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: http://www.bitdefender.de
Technische Beratung: support@bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender-es.com
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Technische Beratung: support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Telefon: +40 21 4085600
Fax: +40 21 2330763
Webseite: http://www.bitdefender.de

Glossar

ActiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

Adware

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

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

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

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

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Bootsektor

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

Bootvirus

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

Browser

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird. Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer. Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download (Herunterladen)

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post.Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignise

Ereignise oder Erscheinungen, die in einem Programm vorkommen. Ereignise können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignise, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Prüfmethode beruht nicht auf spezifische Virussignaturen. Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann. Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

IP

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

Java Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner. Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips. Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur. Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt. Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen. Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen. Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN’s oder PIN’s preiszugeben. Dies soll aus Gründen der Aktualisierung geschehen. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

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

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten überwacht und über seine Internetverbindung abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Systemleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert. Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd

schenkten. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

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.