BitDefender 8
Professional Plus

Benutzerhandbuch

bitdefender
secure your every bit

Inhaltsverzeichnis

Table of contents

1

Bedingungen

Software-Lizenzierung

Die BitDefender-Software ist durch Urheberrechtsgesetze und internationale Urheberrechtsverträge ebenso geschützt wie durch andere Gesetze und Verträge zum Schutz des geistigen Eigentums. Die Urheberrechte und andere Gesetze zum Schutz des geistigen Eigentums schützen in vielen anderen Ländern die Rechte der Softwareeigentümer, indem ausschließlich ihnen Rechte, einschließlich des Rechts, das Softwareprodukt zu vervielfältigen und zu kopieren, eingeräumt werden. Das Kopieren des Softwareproduktes ohne die Zustimmung des Eigentümers stellt eine Urheberrechtsverletzung dar und wird strafrechtlich verfolgt.

Ein Softwareprodukt wird als kopiert betrachtet, wenn Sie:

- die Software in den Arbeitsspeicher Ihres Rechners laden, indem Sie diese von der Diskette, Festplatte, CD-ROM oder anderen Medien direkt ausführen;
- die Software auf ein anderes Medium, wie zum Beispiel eine Diskette oder eine Festplatte, kopieren;
- das Programm auf Ihrem Rechner von einem Netzwerkserver, auf dem sich die Software befindet, ausführen.

Fast jede gewerbliche Software wird direkt oder indirekt vom Urheberrechtseigentümer - dem Softwareentwickler - durch den so genannten Lizenzvertrag für die Endbenutzung lizenziert. Die Softwareprodukte können verschiedenartige Lizenzverträge haben.

Lizenzvertrag

WENN SIE NICHT MIT DEN NACHFOLGENDEN BEDINGUNGEN DES LIZENZVERTRAGES UND DEN GEWÄHRLEISTUNGSBESTIMMUNGEN EINVERSTANDEN SIND, SIND SIE NICHT ZUR INSTALLATION, BENUTZUNG UND WEITERGABE DER SOFTWARE BERECHTIGT! DURCH KLICKEN ODER BESTÄTIGEN VON "JA", "ICH STIMME ZU", "WEITER" ODER DURCH INSTALLATION ODER DURCH BENUTZUNG ERKLÄREN SIE, DASS SIE DEN FOLGENDEN VERTRAG VERSTANDEN HABEN UND DEM VERTRAG UND SEINEM INHALT VOLLSTÄNDIG ZUSTIMMEN.

Der Lizenzvertrag und die Gewährleistungsbestimmungen sind ein rechtsgültiger Vertrag zwischen Ihnen (einer natürlichen oder juristischen Person, im Folgenden Benutzer genannt) und der SOFTWIN zur Benutzung des oben und folgend genannten SOFTWIN-SOFTWAREPRODUKTES, welches außer dem eigentlichen SOFTWAREPRODUKT auch dazugehörige Medien, gedruckte Materialien und die Nutzung von Online- und anderen Medien 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 die Gewährleistungsbestimmungen gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrages und den Gewährleistungsbestimmungen nicht zustimmen, ist der Hersteller SOFTWIN nicht bereit, das SOFTWAREPRODUKT an Sie zu lizenzieren. In diesem Falle sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu verwenden oder zu kopieren. Die Rückgabe des Produktes kann nur innerhalb von 30 Tagen nach dem Kauf beim Verkäufer des SOFTWAREPRODUKTS unter voller Rückerstattung des Kaufpreises erfolgen. Ein rechtsgültiger Kaufbeleg ist dazu erforderlich.

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 Lizenz. Folgende Rechte werden Ihnen eingeräumt:

ANWENDUNGSSOFTWARE. Der Benutzer darf eine Kopie des SOFTWAREPRODUKTES auf einem Betriebssystem und einen Einzelplatzrechner installieren und benutzen. Der Benutzer, auf dessen Einzelplatzrechner das SOFTWAREPRODUKT installiert ist, darf eine weitere (zweite) Kopie zu seiner eigenen Benutzung auf einem tragbaren Rechner installieren.

NETZWERKBENUTZUNG. Der Benutzer darf eine Kopie des SOFTWAREPRODUKTES auf einem Speicherplatz innerhalb eines geschlossenen Netzwerkes speichern und installieren, um es von dort wiederum für einen Einzelplatzrechner zu nutzen. Für jeden weiteren Einzelplatzrechner, auf dem eine Kopie des SOFTWAREPRODUKTES installiert ist oder gestartet wird, muss der Benutzer eine weitere Lizenz erwerben und ausweisen. Eine einzelne Lizenz des SOFTWAREPRODUKTES darf nicht auf mehreren Einzelplatzrechnern oder gleichzeitig auf verschiedenen Rechnern genutzt werden. Falls der Benutzer eine mehrfache oder gleichzeitige Nutzung des SOFTWAREPRODUKTES wünscht, empfiehlt SOFTWIN den Erwerb einer Multilizenz.

MULTILIZENZ. Falls der Benutzer eine Multilizenz des SOFTWAREPRODUKTES erworben und diesen Lizenzvertrag dazu erhalten hat, darf er so viele Kopien installieren und benutzen, wie unter „Lizenzierte Kopien“ angegeben ist. Der Benutzer darf zusätzlich dieselbe Anzahl an

Kopien auf tragbaren Rechnern installieren und diese nach denselben Regeln wie unter „Anwendungssoftware“ beschrieben (also nicht gleichzeitig) nutzen.

LIZENZGÜLTIGKEIT. Der Lizenzvertrag über das SOFTWAREPRODUKT beginnt mit dem Tag der Installation, der Speicherung oder andererseits mit dem Tag der ersten Benutzung und behält seine Gültigkeit auf dem Einzelplatzrechner, auf dem es ursprünglich (zuerst) installiert wurde.

UPGRADES. Sollte das SOFTWAREPRODUKT mit der Bezeichnung „Upgrade“ gekennzeichnet sein, muss der Benutzer für eine berechtigte Nutzung ein gültiges, von SOFTWIN als berechtigt anerkanntes anderes SOFTWAREPRODUKT lizenziert haben. Das als „Upgrade“ gekennzeichnete SOFTWAREPRODUKT ersetzt und/oder ergänzt das zum Upgrade berechtigende SOFTWAREPRODUKT. Der Benutzer darf das aus dem Upgrade resultierende SOFTWAREPRODUKT nur nach dem hier vorliegenden Lizenzvertrag nutzen. Sollte das als „Upgrade“ gekennzeichnete SOFTWAREPRODUKT ein Upgrade für eine einzelne Komponente eines kompletten Softwarepaketes sein, darf das SOFTWAREPRODUKT auch nur als einzelner Bestandteil dieses Softwarepaketes genutzt und transferiert und nicht als separates Produkt auf mehr als einem Einzelplatzrechner genutzt werden.

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

EINGESCHRÄNKTE GEWÄHRLEISTUNG. SOFTWIN gewährleistet für einen Zeitraum von 30 Tagen, dass das Medium auf dem das SOFTWAREPRODUKT geliefert wird, frei von allen Defekten ist. Sollte dies nicht der Fall sein, wird SOFTWIN das Medium austauschen oder dem Benutzer den Betrag zurückerstatten, den der Benutzer für das SOFTWAREPRODUKT bezahlt hat. SOFTWIN gewährleistet weder die dauerhafte Verfügbarkeit noch die Fehlerfreiheit des SOFTWAREPRODUKTES noch dass Unzulänglichkeiten und Fehler des SOFTWAREPRODUKTES behoben werden. SOFTWIN gewährleistet ebenso nicht, dass das SOFTWAREPRODUKT den Anforderungen des Benutzers entspricht. SOFTWIN übernimmt ausdrücklich keinerlei Garantie jeder Art, ausdrücklich oder stillschweigend, einschließlich, jedoch nicht beschränkt auf die stillschweigenden Garantien der Eignung zum Verkauf, oder zu einem bestimmten Zweck, oder die Nichtverletzung von Rechten Dritter. Der Benutzer trägt das alleinige Risiko für die Verwendung und Leistung des SOFTWAREPRODUKTES. Diese Gewährleitung gibt dem Benutzer bestimmte Rechte, die von Land zu Land verschieden sein können.

BESCHRÄNKUNG DER HAFTUNG. Jeder Benutzer des SOFTWAREPRODUKTES, der dieses benutzt, testet oder auch nur ausprobiert, trägt alleinig das Risiko, das aus der Qualität und Performance des SOFTWAREPRODUKTES entsteht. In keinem Fall können SOFTWIN oder ihre Lieferanten auf irgendeine Weise für, durch Verwendung des SOFTWAREPRODUKTES, 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 des SOFTWAREPRODUKTES entstanden sind. Dies gilt auch dann, wenn SOFTWIN über existierende und/oder mögliche Schäden informiert wurde. IN KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN, DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test etc.).

WICHTIGE 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.

REGIERUNGSBEGRENZUNGESRECHTE/BEGRENZUNGSRECHTERKLÄRUNG. Benutzung, Vervielfältigung, Offenbarung durch die Regierung unterliegen den Einschränkungen, die in folgenden Subparagraphen festgesetzt sind: (c)(1)(ii) Rechte hinsichtlich der Technischen Daten und Computer Software DFARS 252.227-7013 oder den Subparagraphen (c)(1) und (2) der Anwendung der Klausel der begrenzten Rechte der Kommerziellen Computersoftware 48 CFR 52.227-19. Kontaktieren Sie SOFTWIN, Fabrica de Glucoza Str. 5, 72322-Sect.2, Bukarest, Rumänien, Tel. 0040-21-2330780 oder Fax:0040-21-2330763.

ALLGEMEIN. Dieser Vertrag unterliegt dem Recht von Rumänien. Diese Vereinbarung darf nur durch eine Ergänzung zum Lizenzvertrag und der Gewährleistungsbestimmung verändert werden. Diese Änderung muss in schriftlicher Form erfolgen und muss von SOFTWIN und dem Benutzer unterzeichnet sein. Dieser Vertrag wurde in deutscher Sprache geschrieben und kann nicht in eine andere Sprache übersetzt oder interpretiert werden. Preise, Kosten und Gebühren in Zusammenhang mit der Benutzung des SOFTWAREPRODUKTES können ohne weitere Ankündigung geändert werden. Ist oder wird eine Bestimmung dieses Vertrages wegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam oder wird sie für unwirksam erklärt, so wird hierdurch die Gültigkeit des übrigen, mit der unwirksamen Bestimmung nicht unmittelbar zusammenhängenden Vertragsteils nicht berührt. BitDefender und alle zugehörigen Logos sind eingetragene Titel und Marken von SOFTWIN. Alle anderen Marken und Titel sind Eigentum der jeweiligen Rechteinhaber.

2

BitDefender-Rescue-System

BitDefender 8 Professional wird mit einer bootfähigen CD (**BitDefender-Rescue-System** basierend auf LinuxDefender) ausgeliefert, welches in der Lage ist, alle existierenden Festplatten zu scannen und zu desinfizieren, bevor Sie Ihr Betriebssystem starten.

Sie sollten das **BitDefender-Rescue-System** immer dann nutzen, wenn Ihr Betriebssystem wegen eines Virenbefalls nicht korrekt arbeitet. Dies passiert dann, wenn Sie kein Antivirenprodukt im Einsatz haben.

Das Update der Virensignaturen geschieht automatisch immer dann, wenn der Nutzer das **BitDefender-Rescue-System** startet.

Systemvoraussetzungen

- Intel-kompatible CPU (Pentium 2/300MHz oder höher);
- 64 MB RAM für Textmodus, mindestens 256 MB für Grafikmodus mit KDE (512 MB empfohlen);
- Standard SVGA-kompatible Grafikkarte.

Wie gescannt wird

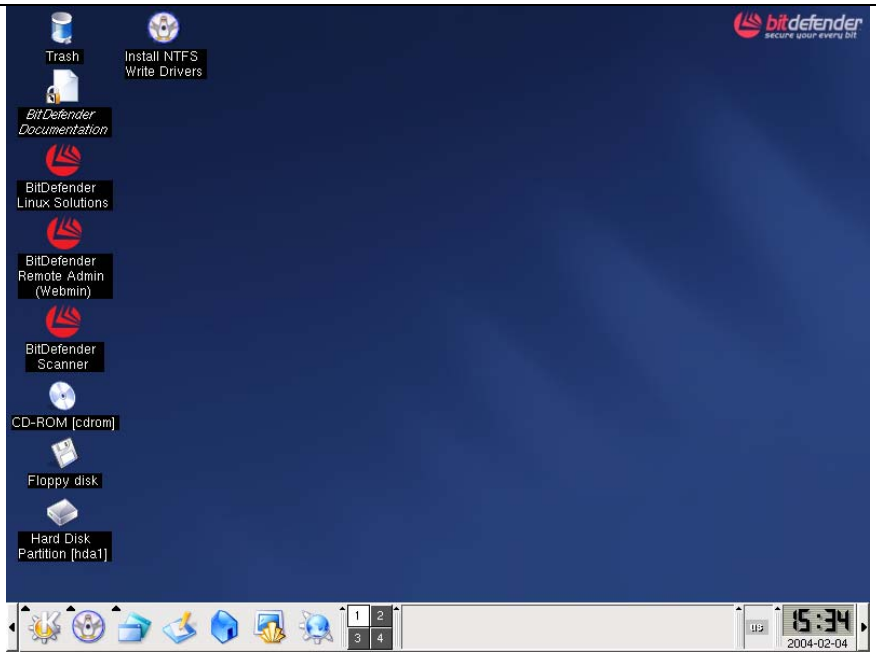
Folgen Sie diesen Schritten, um Ihren Computer auf Viren zu überprüfen:

Booten von CD

Legen Sie die BitDefender-Rescue-CD in Ihr CD-ROM-Laufwerk und starten Sie Ihren Computer neu.

Dann wird automatisch das **BitDefender-Rescue-System** gestartet (eventuell müssen Sie Ihr BIOS so einstellen, dass Ihr Computer von der CD booten kann).

Die grafische Oberfläche des **BitDefender-Rescue-Systems** erscheint:



Darstellung 1

Installieren der NTFS-Treiber

Klicken Sie mit der linken Maustaste auf das **Installieren NTFS Write Treiber**-Symbol. In dem darauf folgenden Fenster klicken Sie zweimal auf **Weiter**. Dann startet die NTFS-Treiber-Installation. **LinuxDefender** benötigt zwei Treiber (`ntoskrnl.exe` und `ntfs.sys`), um Zugriff auf Ihre Festplatte zu erhalten. Zurzeit werden nur Windows XP-Treiber unterstützt. Beachten Sie, dass Sie diese auch für Windows 2000/NT/2003 nutzen können.

Während der Installation werden Sie diese Nachricht erhalten:

`Cannot open target file "/var/lib/capative/ext2fsd.sys": Read-only file System`.

Bestätigen Sie dies mit **OK**.

Zum Abschluss klicken Sie auf **OK,** um die Installation zu beenden.

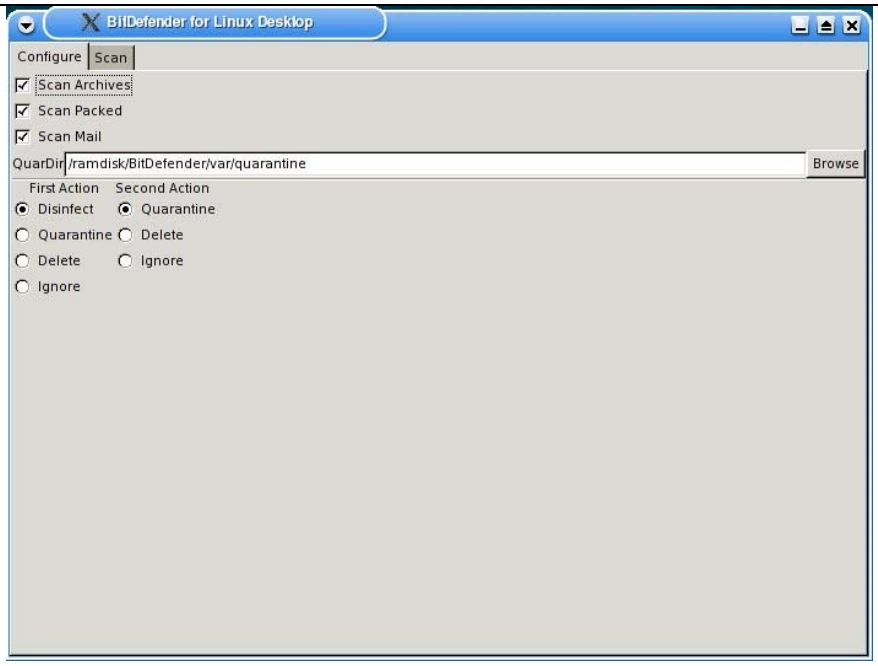
Sie erhalten diese Nachricht: `Although essential modules ….` Klicken Sie auf **OK**.

Überprüfen Ihrer Festplatte

Auf dem LinuxDefender-Desktop klicken Sie auf das **Hard Disk Partition [hda1]**-Symbol. Es öffnet sich ein Fenster, in dem Sie den Inhalt Ihrer Festplatte einsehen können. Schließen Sie dieses Fenster.

Auswahl der Scan-Optionen

Klicken Sie auf das **BitDefender-Scanner**-Symbol, um eine Auswahl der Scan-Optionen zu sehen. Das folgende Fenster öffnet sich:



Darstellung 2

Folgende Optionen sind möglich:

- **Scan Archives** – Scannen innerhalb von Archiven
- **Scan Packed** – Scannen in komprimierten Dateien
- **Scan Mail** – Scannen der Mail-Datenbank
- **QuarDir** – die Standardeinstellung für den Quarantäne-Ordner ist: `/ramdisk/BitDefender/var/quarantine`. Falls Sie den Quarantäne-Ordner verschieben wollen, klicken Sie auf **Durchsuchen** und wählen Sie einen anderen Ort (oder schreiben Sie in das **QuarDir**-Feld).

BitDefender wird versuchen, eine Aktion durchzuführen, wenn das Programm eine infizierte Datei findet. Sie können auswählen, welche Aktion durchgeführt wird. Wenn die erste Aktion aus irgendeinem Grund ausfällt, wird eine zweite Aktion durchgeführt.

TIPP: Wir empfehlen Ihnen, die erste Aktion: **Desinfizieren** zu benutzen, zweite Aktion: **Löschen**.

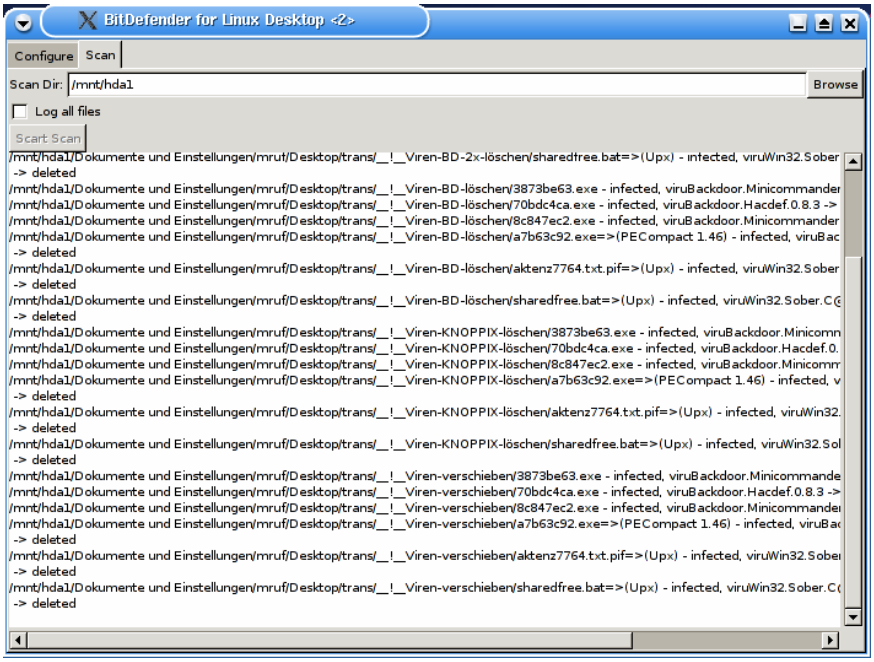
Sie können eine der folgenden Aktionen wählen:

Erste Aktion	Beschreibung
Desinfizieren	Die infizierte Datei wird desinfiziert.
Quarantäne	Die infizierte Datei wird in die Quarantäne verschoben. Wenn Sie LinuxDefender verlassen, wird der Quarantäne-Ordner gelöscht.
Löschen	Die infizierte Datei wird **ohne Warnung** gelöscht.
Ignorieren	Falls eine infizierte Datei gefunden wird, wird sie ignoriert.

Zweite Aktion	Beschreibung
Quarantäne	Die infizierte Datei wird in die Quarantäne verschoben.
Löschen	Löscht die infizierte Datei ohne Warnung.
Ignorieren	Falls eine infizierte Datei gefunden wird, wird sie ignoriert.

Starten des Scan-Prozesses

Klicken Sie auf den **Scan-**Reiter.



Darstellung 3

Im **Scan Dir**-Feld können Sie den Pfad der Festplatte angeben, die gescannt werden soll.

Beispiele:

Wenn Sie eine Festplatte mit drei Partitionen haben, muss jede einzelne gescannt werden.

- `/mnt/hda1` – für die erste Partition;
- `/mnt/hda2` – für die zweite Partition;
- `/mnt/hda3` – für die dritte Partition.

Wenn Sie eine zweite Festplatte haben, so ist der Inhalt:

- `/mnt/hdb1`– für die erste Partition;
- `/mnt/hdb2`– für die zweite Partition.

Wenn Sie SCSI-Festplatte mit zwei Partitionen haben, so ist der Inhalt:

- `/mnt/sda1`– für die erste Partition;
- `/mnt/sda2`– für die zweite Partition.

Die Option **Log all files** ist standardmäßig nicht aktiviert, weil sie die Scangeschwindigkeit stark verlangsamt.

Klicken Sie auf **Start Scan** und der Scan beginnt.

Findet BitDefender einen Virus, erscheint eine Nachricht im Hauptfenster.

Anmerkung

Lassen Sie bitte den Virenscan zweimal durchführen. Es besteht die Möglichkeit, dass ein Virus beim Scan einer NTFS-Partition beim ersten Mal nicht entfernt wird.

3

Produkt-Installation

Systemvoraussetzungen

Um eine korrekte Funktion des Produktes sicherzustellen, vergewissern Sie sich vor der Installation, dass folgende Systemvoraussetzungen gegeben sind:

Minimum Prozessor: Pentium 200 MHz
Minimum Festplattenspeicher: 40 MB
Minimum RAM-Speicher: 64 MB (128 MB empfohlen)
Betriebssystem: Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 4.0 (+)
Für eine Integration mit Outlook benötigen Sie: Outlook Express 5.0 oder später, Microsoft Outlook 2000 oder später

Installationsschritte

Doppelklicken Sie auf den Setup-Ordner. Damit starten Sie den Setup-Assistenten, der Ihnen bei der Installation hilft.

Darstellung 4

Installationsschritte:

1. Klicken Sie auf **Weiter**, um fortzufahren, oder auf **Abbrechen**, um die Installation zu beenden.
2. Klicken Sie auf **Weiter**, um fortzufahren oder auf **Zurück**, um wieder zum ersten Schritt zu kommen.
3. Bitte lesen Sie die **Lizenzvereinbarung** und wählen Sie **Ich stimme den Bedingungen zu**; klicken Sie dann auf **Weiter.** Wenn Sie den Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie verlassen das Setup.
4. Sie können zwischen verschiedenen Installationsarten wählen: Normal, Benutzerdefiniert oder Vollständig.
   - **Normal** – Das Programm wird mit den gebräuchlichsten Einstellungen installiert. Diese Option empfiehlt sich für die meisten Nutzer.
   - **Benutzerdefiniert** – Sie können die Komponenten wählen, die Sie installieren wollen. Diese Option wird für fortgeschrittene Nutzer empfohlen.
   - **Vollständig** – Alle Komponenten des Programms werden installiert.

   Wenn Sie **Normal** oder **Vollständig** gewählt haben, überspringen Sie Schritt 5.
5. Wenn Sie **Benutzerdefiniert** gewählt haben, öffnet sich ein Fenster mit allen BitDefender-Komponenten, so dass Sie aus einer Liste wählen können, was Sie installieren möchten.

   Wenn Sie auf eine Komponente klicken, erscheint eine kurze Beschreibung (inbegriffen das Minimum an Festplattenspeicher). Wenn Sie auf ein  klicken, erscheint ein neues Fenster und Sie können auswählen, welche Komponente Sie installieren wollen.

Sie können den Ordner wählen, in dem das Produkt installiert werden soll. Standardmäßig wird BitDefender im Ordner `C:\Programme Dateien\Softwin\BitDefender 8` installiert.

Falls Sie einen anderen Ordner wählen wollen, klicken Sie auf **Durchsuchen**. Ein neues Fenster wird geöffnet, in dem Sie einen Ordner auswählen können. Klicken Sie auf **Weiter**.

6. Klicken Sie auf **Weiter**.
7. Sie haben vier Möglichkeiten:
   - ➔ **Update BitDefender** – um BitDefender nach der Installation upzudaten. Ihr System muss mit dem Internet verbunden sein.
   - ➔ **Durchführen eines kompletten Scans** – um nach dem Ende der Installation einen kompletten Virenscan auf Ihrem Computer durchzuführen.
   - ➔ **Öffnen der Readme-Datei** – öffnen der Readme-Datei am Ende der Installation.
   - ➔ **Speichern eines Symbols auf Ihrem Desktop** – um am Ende der Installation ein Symbol auf Ihrem Desktop zu speichern.

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

Anmerkung

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

Entfernen, Reparieren oder Modifizieren von BitDefender-Eigenschaften

Wenn Sie **BitDefender 8 Professional** modifizieren, reparieren oder entfernen wollen, verwenden Sie das Windows-Startmenü: **Start → Programme→ BitDefender 8 → Modifizieren, Reparieren oder Deinstallieren**.

Sie werden aufgefordert, Ihre Eingabe mit einem Klick auf **Weiter** zu bestätigen. Ein neues Fenster öffnet sich und Sie können wählen zwischen:

- **Modifizieren** – Auswahl neuer Programmkomponenten oder bereits installierter Komponenten.
- **Reparieren** – erneute Installation aller Komponenten.

  Bevor Sie das Produkt reparieren, empfehlen wir Ihnen, Ihre Freundes- und Spammerliste zu exportieren und erst nach dem Reparieren wieder zu importieren.

- **Entfernen** – entfernt alle installierten Komponenten.

Um mit dem Setup fortzufahren, wählen Sie bitte eine dieser drei aufgeführten Optionen. Wir empfehlen **Entfernen** für eine saubere Installation. Nach dem Deinstallieren löschen Sie am besten den Ordner **Softwin** aus dem Ordner **Programme**, um eine gute Neuinstallation zu gewährleisten.

4

Beschreibung und Eigenschaften

Beschreibung

Ein gutes Antivirenprogramm ist leider nicht genug in einer vernetzten Umgebung. Bedrohungen für Computer und Netzwerke stellen nicht nur Viren, sondern auch arglistige Individuen wie Hacker oder Spammer dar. Dem trägt das BitDefender-Produkt-Entwicklungsteam mit seiner Sicherheits-Software Rechnung.

BitDefender 8 Professional Plus bildet mit einem Antiviren-, Firewall-, Antispam- und einem Update-Modul ein umfassendes Sicherheitspaket, das sich an die Bedürfnisse aller Internetbenutzer in der ganzen Welt anpassen lässt.

Haupteigenschaften

BitDefender 8 Professional Plus beinhaltet 4 Schutzmodule: **Antivirus**, **Firewall**, **Antispam** und **Update**.

Antivirus

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

Permanenter Antivirenschutz

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

Peer-2-Peer-Applikationsschutz

Scannt nach Viren, die durch Instant Messaging und Filesharing-Software verteilt werden.

Innovativer Verhaltensblocker

Blockiert gefährliche Applikationen basierend auf einer Analyse des Verhaltens. Diese Methode stellt sicher, dass Sie geschützt sind vor neuen Viren, Trojanern, Internetwürmern und anderen gefährlichen Codes. Das Dateisystem, die Registry und die Internetaktivitäten werden permanent überwacht.

Quarantäne
Verdächtige/infizierte Dateien können optional in eine sichere Quarantäne-Umgebung hinterlegt werden, bevor Sie sie desinfizieren oder löschen. Der Inhalt dieser Quarantäne-Umgebung kann zwecks detaillierter Analyse an die BitDefender-Labore gesendet werden. Dateien, die bekanntermaßen sicher sind, können einfach aus der Quarantäne wieder an ihren alten Platz verschoben werden.

Kompletter E-Mail-Schutz
Diese Anwendung funktioniert unter dem POP3-Protokoll-Level und blockiert alle infizierten E-Mail-Inhalte, unabhängig vom genutzten E-Mail-Client (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat etc.) und ohne zusätzliche Anwendungskonfiguration.

Firewall

Das Firewall-Modul schützt Ihre Daten und Ihre Privatsphäre, indem es den eingehenden und ausgehenden Verkehr filtert und gefährliche Scripte und “XXX”-Einwahlprogramme blockiert.

Internet-Verkehrskontrolle
Definiert ganz genau, welche ein- und ausgehenden Verbindungen zugelassen oder abgelehnt werden. Definiert Regeln bezüglich spezieller Protokolle, Ports, Anwendungen und/oder Remote-Adressen.

Einwahlkontrolle
Ein konfigurierbarer Anti-Einwähler verhindert, dass sich gefährliche Anwendungen installieren und so hohe Telefonrechnungen verursachen.

Aktive Inhaltskontrolle
Blockiert proaktiv alle möglichen gefährlichen Anwendungen wie ActiveX, Java-Applets oder Java-Script-Codes.

Umfassende Privatsphären-Kontrolle
Die Firewall filtert ein- und ausgehende Cookies, schützt so Ihre Identität und verbirgt ihre Vorlieben, wenn Sie im Internet surfen.

Antispam

Sehr einfach handelt das BitDefender-AntiSpam-Modul das Problem der Spam-Mails, so dass Sie keine mehr erhalten.

Antispam-Arbeitsschemata

Hochentwickelter AntiSpam-Schutz
BitDefender-AntiSpam bezieht fünf Filter mit ein, die sicherstellen, dass Ihr Posteingang spam-frei bleibt: Weiße/Schwarze Listen, Sprach-Filter, URL-Filter, Heuristischer Filter und den Bayesianischen Filter.

Selbstlernender Filter
Der hoch entwickelte, selbstlernende Bayesianische Filter lässt Ihre Nachrichten mit einem einzigen Klick klassifizieren. Nach nur wenigen Malen werden Sie feststellen, dass es von Zeit zu Zeit immer leichter wird. Jede Markierung, die Sie hinzufügen, verbessert die Genauigkeit. Die Filtereinstellungen reichen von Hoch bis Niedrig.

Ohne Schwierigkeiten

Sie werden nur über den Eingang legitimer Nachrichten informiert. Spam wird lautlos in Ihren Spam-Ordner verschoben, wo er nach Ihren Bedürfnissen gelöscht oder bearbeitet werden kann.

Kompatibel mit allen E-Mail-Clients

BitDefender-AntiSpam arbeitet mit allen E-Mail-Clients zusammen und kann von der BitDefender-Management-Konsole aus konfiguriert werden. Darüber hinaus lässt es sich sofort einbinden in Microsoft Outlook/Outlook Express. Mit den AntiSpam-Filtern erlaubt es eine einfache, intuitive Zusammenarbeit.

Update

Dieses Modul versorgt das Produkt mit Updates, neuen Virensignaturen und Eigenschaften.

Schnelle, kostenlose Updates

Ohne dass der Nutzer eingreifen muss, werden neue, intelligente Updates zum Antivirenschutz heruntergeladen. Das Update kann über das Netzwerk, das Internet oder direkt über einen Proxy-Server ausgeführt werden. Lizenzierte BitDefender-Nutzer profitieren somit von den kostenlosen Virendefinitionen, Updates und Produktverbesserungen.

Selbstreparierend

Das Produkt ist in der Lage, sich bei Bedarf selbst zu reparieren. Dies geschieht durch Download beschädigter oder fehlender Dateien von den BitDefender-Servern.

Automatische Updates

Updates für Antivirus und Antispam sind kostenlos und voll automatisiert. Die Prüfung auf Updates kann geplant und sooft durchgeführt werden, wie Sie es für nötig halten.

Erweiterte Funktionen

Sachkundige Entscheidungen

Konfigurationsassistenten stehen Ihnen zur Seite, während Sie Ihr System sicher machen. Eine umfangreiche Datenbank beinhaltet Daten und Anwendungen, mit Hilfe derer Sie entscheiden können, ob eine Anwendung, die auf Ihr Netzwerk zugreift, vertrauenswürdig ist oder nicht.

Einfach zu installieren und zu nutzen

Eine einfache Schnittstelle macht es leichter für Sie, das Produkt zu installieren und zu nutzen. Durch die intuitive Datei-Zone/Netz-Zone können Sie einzelne Dateien durch Drag & Drop auf Viren scannen lassen.

Rund um die Uhr professioneller technischer Support

Qualifizierte Supportmitarbeiter geben Hilfestellung und online finden Sie eine Datenbank mit Antworten auf häufig gestellte Fragen (FAQ).

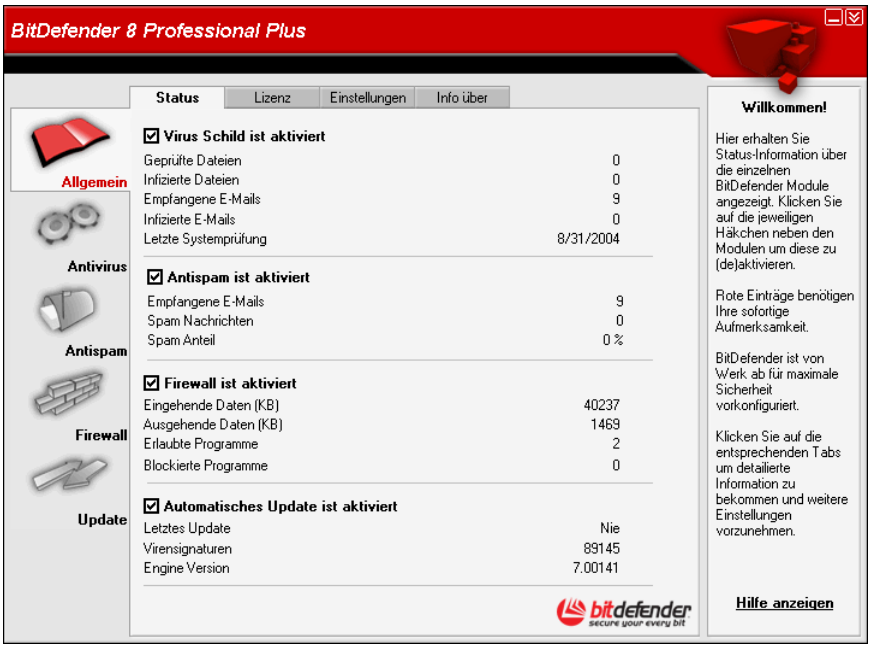
5

Die Management-Konsole

Überblick

BitDefender 8 Professional Plus enthält eine zentrale Management-Konsole, die es erlaubt, die Schutzfunktionen für alle BitDefender-Module zu konfigurieren. Mit anderen Worten: Es reicht aus, die Management-Konsole zu öffnen, um Zugriff auf alle Module zu haben (**Antivirus**, **Firewall**, **Antispam** und **Update**).

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start** → **Programme** → **BitDefender 8** → **BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol.



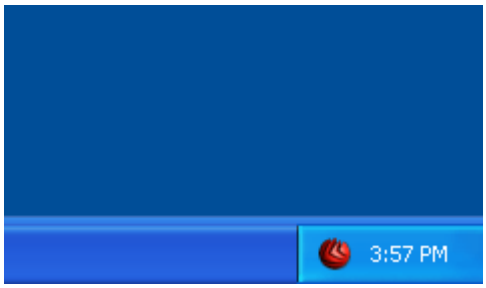
Darstellung 5

Auf der linken Seite der Management-Konsole sehen Sie die Modul-Auswahl:

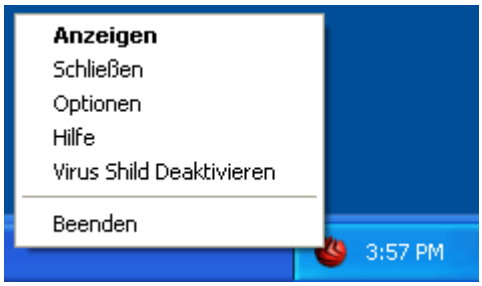
- Allgemein – Sie sehen eine Zusammenfassung aller BitDefender-Einstellungen, überdies Produktdetails und Kontaktinformationen. Hier können Sie auch das Produkt registrieren.
- Antivirus – das Antivirus-Konfigurationsfenster öffnet sich.
- Antispam – das Antispam-Konfigurationsfenster öffnet sich.
- Firewall – das Firewall-Konfigurationsfenster öffnet sich.
- Update – das Update-Konfigurationsfenster öffnet sich.

Die Option **Hilfe anzeigen,** platziert unten rechts, öffnet die Hilfe-Datei.

Wenn die Konsole minimiert ist, erscheint ein Symbol in derSystem-Ablage.



Darstellung 6



Darstellung 7

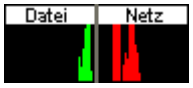
Wenn Sie auf das Symbol doppelklicken, öffnet sich die Management-Konsole.

Mit einem Rechtsklick auf das Symbol öffnet sich ein Popup-Menü, wie *Darstellung 7* zeigt:

- **Anzeigen** – öffnet die Management-Konsole.
- **Schließen** – minimiert das Programm.
- **Optionen** – öffnet ein Fenster mit Optionen für die Management-Konsole.
- **Hilfe** – öffnet die elektronische Dokumentation.
- **Virus-Schild Deaktivieren/Aktivieren** – Deaktiviert/Aktiviert Virus-Schild.
- **Beenden** – beendet die Anwendung. Bei Auswahl dieser Option verschwindet das Symbol aus der Systemablage. Um erneut Zugriff auf die Management-Konsole zu bekommen, starten Sie sie aus dem Startmenü.

Scan-Aktionsbalken

Viele von Ihnen haben wahrscheinlich schon das kleine graue Rechteck bemerkt, das man in jede Ecke des Bildschirms schieben kann.



Dieses Fenster zeigt eine graphische Visualisierung der Scan-Aktivität auf Ihrem System.

Darstellung 8

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.

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

Tipp: Wenn Sie die graphische Visualisierung völlig ausblenden möchten, deaktivieren Sie die Option „Show Scan Activity Bar“ (im Antivirus-Modul, Schild-Sektion).

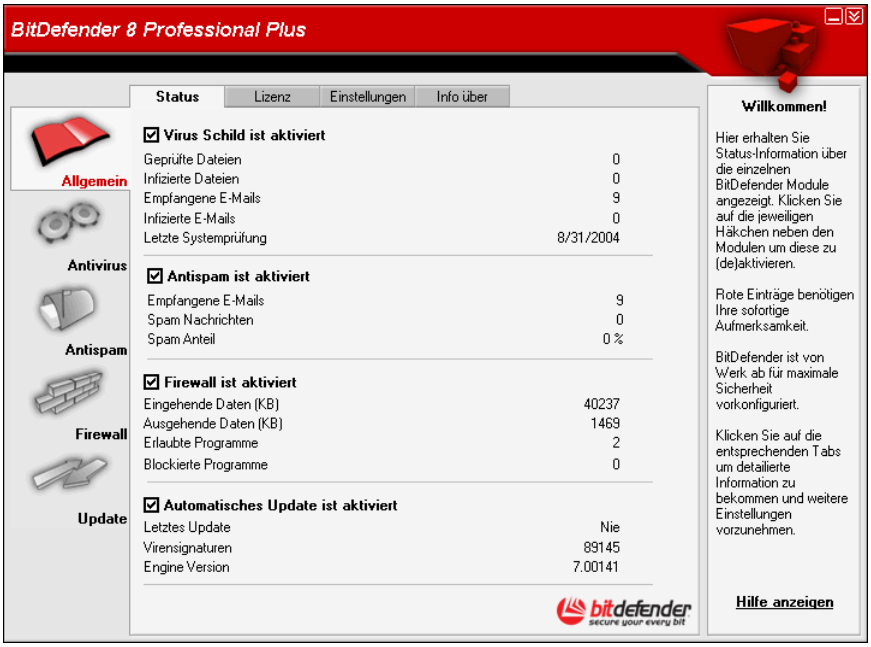
Allgemein-Modul

BitDefender verfügt über eine vollständige Konfiguration für maximale Sicherheit. Wesentliche Status-Informationen über alle BitDefender-Module werden im **Allgemein**-Modul angezeigt.

Das **Allgemein**-Modul beinhaltet vier verschiedene Sektionen: Status, Lizenz, Einstellungen und Info Über.

Status

Hier finden Sie eine Übersicht über den Produkt-Status.



Darstellung 9

Durch Setzen der entsprechenden Häkchen können Sie die Hauptmerkmale des BitDefenders aktivieren oder deaktivieren.

Optionen, die in Rot markiert sind, erfordern unbedingte Aufmerksamkeit.

Virus-Schild

Bietet einen Echtzeit-Schutz vor Viren und anderen gefährlichen Bedrohungen. Es zeigt die Anzahl der gescannten Dateien, der infizierten Dateien, der gescannten Nachrichten, der infizierten Nachrichten und das Datum des letzten System-Scans.

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

TIPP: Wir empfehlen dringend, einen kompletten Virenscan mindestens einmal in der Woche durchzuführen. Um einen kompletten Systemscan durchzuführen, aktivieren Sie das **Antiviren**-Modul, Sektion Virus Scan, wählen Sie die Lokalen Laufwerke aus und klicken Sie dann auf **Scan**.

Antispam

Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Spam-Mails kommen von überall in großer Zahl und in unterschiedlicher Größe. BitDefender-AntiSpam arbeitet mit allen E-Mail-Clients und kann von der Management-Konsole aus konfiguriert werden (Antispam-Sektion). Darüber hinaus lässt es sich sofort einbinden in Microsoft Outlook/Outlook Express. Die Antispam-Filter erlauben eine einfache, intuitive Zusammenarbeit.

Um zu verhindern, dass Spam in Ihren Posteingang gelangt, aktivieren Sie den **Antispam**-Filter.

Sehen Sie, wie BitDefender-AntiSpam arbeitet

Firewall

Die Personal Firewall schützt Sie vor Internetattacken. Die Firewall-Regeln verhindern, dass Hacker und gefährliche Software Zugriff auf Ihren Computer und Ihre persönlichen Daten erhalten. Die Darstellungen zeigen den Internet-Verkehr während der Sitzung, die Anzahl an zugelassenen Programmen, die Ihre Internetverbindung nutzen, und die Anzahl der blockierten Programme.

Um gegen Internetattacken geschützt zu sein, aktivieren Sie die **Firewall**.

Automatisches Update

Neue Viren werden jeden Tag gefunden und identifiziert. Daher ist es sehr wichtig, BitDefender mit den neuesten Virensignaturen zu aktualisieren. Das Datum des letzten Updates und die Anzahl der Viren, die entdeckt (und somit auch desinfiziert) werden können, werden angezeigt.

Damit Ihre wichtigen Daten stets geschützt sind, kann BitDefender ein automatisches Update durchführen. Lassen Sie daher am besten die Option „Automatisches Update“ aktiviert.

Produkt-Registrierung

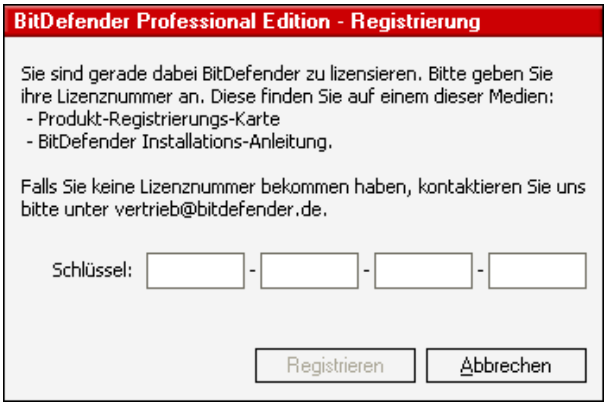
Dieses Register zeigt Informationen über den Status Ihrer BitDefender-Lizenzen. Hier können Sie das Produkt registrieren und das Ablaufdatum sehen.

Darstellung 10

Das Produkt wird mit einem Test-Registrierungsschlüssel ausgeliefert, welcher eine Gültigkeit von 30 Tagen hat. Wenn Sie am Ende der Testzeit das Produkt erwerben wollen, benötigen Sie einen neuen Lizenzschlüssel. Klicken Sie hierfür auf **Jetzt kaufen**, um diesen im BitDefender-Online-Shop zu erhalten.

Um Ihren standardmäßigen Lizenzschlüssel zu erneuern, klicken Sie auf **Lizenznummer ändern**.

Das folgende Fenster öffnet sich:



Darstellung 11

Tragen Sie Ihren **Schlüssel** in das entsprechende Feld ein. Klicken Sie auf **Registrieren**, um diesen Prozess abzuschließen.

Falls Sie sich verschreiben, werden Sie aufgefordert, Ihren Lizenzschlüssel erneut einzugeben.

Wenn Sie einen gültigen Lizenzschlüssel eingegeben haben, öffnet sich ein Bestätigungsfenster.

Nun können Sie in der Sektion „Registrierung“ das Ablaufdatum Ihrer Lizenz einsehen.

TIPP: Bitte aktivieren Sie alle Ihre BitDefender-Produkte, um vom BitDefender-Support und unseren freien Services profitieren zu können.

Einstellungen der Management-Konsole

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

Darstellung 12

Um eine Option auszuwählen, klicken Sie mit der Maus auf ein Auswahlfeld.

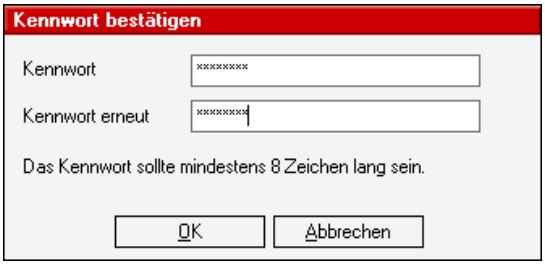
- **BitDefender beim Start von Windows laden** – automatisches Starten des BitDefenders beim Systemstart. Dies wird dringend empfohlen!
- **Minimiert starten** – minimiert die BitDefender-Management-Konsole, nachdem das System gestartet worden ist. Nur das BitDefender-Symbol erscheint in der Systemablage.
- **Schutz nach verlassen der Konsole beibehalten** – auch wenn die Management-Konsole geschlossen worden ist, beschützt Sie BitDefender permanent.
- **Sicherheits-Mitteilungen anzeigen** – von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Startbildschim anzeigen** – zeigt das Fenster, welches geöffnet wird, wenn Sie BitDefender starten.
- **Viren-Meldung an das BitDefender Virus Labor** – sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

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

- **Hinweise anzeigen** – Pop-up-Fenster anzeigen, die über den Produktstatus informieren.
- **Konsole per Kennwort schützen** – die Passwort-Einstellung aktivieren, um Ihre BitDefender-Einstellungen zu schützen.

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

Das folgende Fenster erscheint:



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

Darstellung 13

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

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

➔ Die Oberflächen-Datei erlaubt Ihnen, die Farbe der Management-Konsole zu wählen.

Abschließend klicken Sie auf **Übernehmen**.

Info über

In dieser Sektion finden Sie Kontaktinformationen und Produktdetails.

BitDefender™ bietet Sicherheitslösungen an, die den heutigen Computerumgebungen gerecht werden, und liefert effektives Gefahrenmanagement für über 38 Millionen Heimanwender und Unternehmen in mehr als 100 Länder.

BitDefender™ ist zertifiziert von allen größeren unabhängigen Kritikern - **ICSA Labs**, **CheckMark** und **Virus Bulletin** - und überdies das einzige Sicherheitsprodukt, das einen **Preis von IST** erhalten hat.

Antivirus-Modul

BitDefender schützt alle gängigen Einstiegspunkte auf Ihrem System: E-Mail, Internet-Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP, USB-Speicher).

Mehr Eigenschaften

Vom Antivirus-Modul aus haben Sie Zugriff auf alle BitDefender-Einstellungen und BitDefender-Eigenschaften.

Nach Aufforderung scannen und bei Bedarf scannen

Der Virenschutz ist unterteilt in zwei Kategorien:

- Bei Zugriff scannen: verhindert, dass neue Viren Ihr System befallen. Diese Option wird auch Viren-Schild genannt. Dateien werden gescannt, sobald der Nutzer Zugriff darauf hat. BitDefender zum Beispiel scannt ein Worddokument auf Viren, sobald Sie es öffnen, und E-Mails, sobald Sie sie erhalten. BitDefender scannt Ihre Dateien, sobald Sie sie nutzen.
- Nach Aufforderung scannen: entdeckt residente Viren auf Ihrem System. Das ist der klassische Virenscan, ausgelöst durch den Nutzer – Sie wählen ein Laufwerk aus, einen Ordner oder eine Datei aus und BitDefender scannt sie – nach Aufforderung.

Mehr detaillierte Erläuterungen finden Sie in den nachfolgenden Kapiteln.

Bei Zugriff scannen

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol.

In der Management-Konsole klicken Sie auf **Antivirus**.

Darstellung 14

Das **Virus-Schild** schützt Ihren Computer, indem es E-Mails, Downloads und andere Dateien scannt.

Um zu verhindern, dass Viren Ihren Computer befallen, aktivieren Sie das **Virus-Schild**.

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

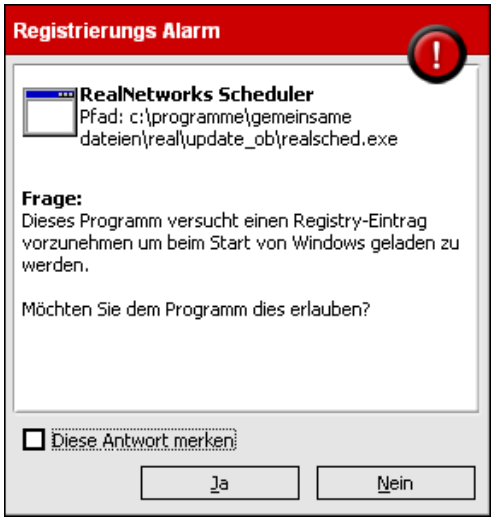
Mit diesen Einstellungen können Sie selbst vorgeben, was BitDefender auf Anforderung prüfen soll und wie das Programm reagiert, wenn es einen Virus findet.

Registry-Kontrolle

Ein sehr wichtiger Teil von Windows ist die **Registry**. Das ist der Ort, an dem 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.



Darstellung 15

Sie können die Änderung ablehnen, indem Sie auf **Nein** klicken, oder aber zulassen, indem Sie mit **Ja** bestätigen. Wenn Sie möchten, dass BitDefender Ihre Antwort speichern soll, wählen Sie die Option **Diese Antwort merken** aus.

Ihre Antworten sind die Grundlage der Richtlinien.

Wenn Sie die Registry-Einträge einsehen wollen, klicken Sie auf ››› entsprechend zur **Registrierung prüfen**.

Das folgende Fenster öffnet sich:

Darstellung 16

Für jede Anwendung wird ein kleines, erweiterbares Menü gebildet. Es beinhaltet alle Änderung der Registry.

Um einen Registry-Eintrag zu löschen, klicken Sie auf **Löschen**.

Um zeitweise einen Registry-Eintrag zu deaktivieren, ohne ihn zu löschen, entfernen Sie das Häkchen ☑, indem Sie darauf klicken. Wenn der Eintrag deaktiviert ist, sieht das so aus ☐.

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.

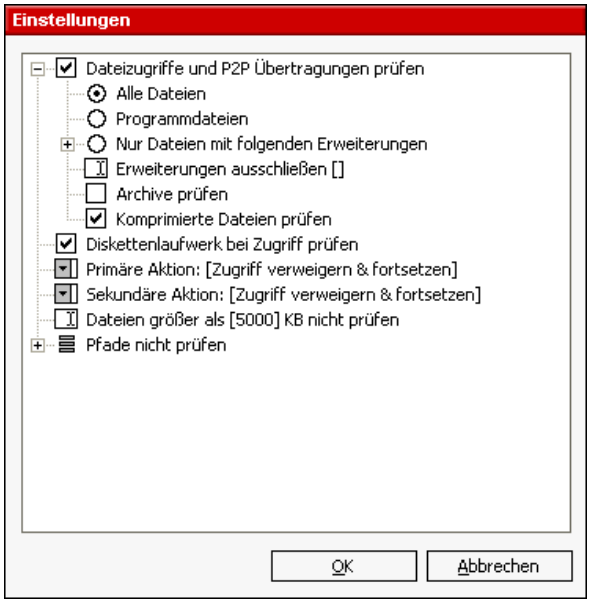
Auswahl der wichtigsten Einstellungen

Um eine Auswahl zu treffen, klicken Sie auf die entsprechende Box.

- **Eingehende E-Mails prüfen** – alle eingehenden E-Mails werden von BitDefender geprüft. Dies wird dringend empfohlen!
- **Dateizugriffe prüfen** – alle Dateien werden von BitDefender überprüft.
- **Datei- und Netzprüfmonitor anzeigen** – wählen Sie diese Option ab, wenn Sie die Aktivitätsleiste nicht mehr sehen wollen.
- **Warnen, wenn ein Virus entdeckt wurde** – ein Alarmfenster öffnet sich, sobald ein Virus gefunden wird. Für eine infizierte Datei zeigt das Alarmfenster den Virennamen an. Für eine infizierte E-Mail zeigt das Alarmfenster den Absender, den Empfänger und den Virennamen an.

Auswahl anderer Optionen

Klicken Sie auf **weitere Einstellungen**, um auszuwählen, wie Sie die infizierte Datei behandeln wollen. Das folgende Fenster öffnet sich:



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

Sie können sehen, dass einige Prüfoptionen sich 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.

Darstellung 17

- Wählen Sie **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.

  Die folgenden Optionen sind wählbar:

Optionen	Beschreibung
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; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pfd; msi; ini; csc; cmd; bas; eml; nws.
Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Archive prüfen	Auch der Inhalt von Archiven wird geprüft.
Komprimierte Dateien prüfen	Alle komprimierten Dateien werden überprüft.

➔ Wählen Sie **Diskettenlaufwerk bei Zugriff prüfen**, wenn Sie das Laufwerk prüfen wollen.

➔ Klicken Sie auf **Primäre Aktion** und wählen Sie aus der Liste die erste Aktion für infizierte Dateien.

BitDefender erlaubt im Falle eines Virenfundes zwei Aktionen. Die zweite Aktion ist nur dann möglich, wenn Sie Desinfizieren der Datei zuerst gewählt haben. Sie können folgende Möglichkeiten auswählen:

Aktion	Beschreibung
Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
Datei säubern	Die infizierte Datei wird desinfiziert.
Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben. Dort kann sie keinen Schaden mehr anrichten.

➔ Klicken Sie auf **Sekundäre Aktion** und wählen Sie aus der Liste die zweite Aktion für infizierte Dateien. Folgende Optionen sind wählbar:

Aktion	Beschreibung
Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
Datei säubern	Die infizierte Datei wird desinfiziert.
Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben. Dort kann sie keinen Schaden mehr anrichten.

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

➔ Klicken Sie auf "+" **Pfade nicht prüfen**, um einen Ordner auszuwählen, der nicht geprüft werden soll. Die Konsequenz ist, dass die Option ausgeweitet wird und **Neues Objekt** erscheint. Klicken Sie auf die dazu gehörende Box und wählen Sie aus dem Fenster die Datei aus, die nicht geprüft werden soll.

Auf Aufforderung prüfen

Die Mission 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 es ist eine sehr gute Idee, Ihren Computer auf residente Viren zu prüfen, nachdem Sie BitDefender installiert haben. Übrigens es ist auch eine gute Idee, Ihren Computer häufig auf Viren zu prüfen.

BitDefender ermöglicht vier Arten, auf Anforderung zu prüfen:

- Sofortiges Prüfen – folgen Sie den unten angegebenen Schritten, um Ihren Computer auf Viren zu prüfen;
- Kontextbezogenes Prüfen – Rechtsklick auf eine Datei oder einen Ordner und wählen Sie im Kontextmenü **BitDefender Antivirus v8** aus;
- Prüfen per Drag & Drop – verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitätsleiste;
- Prüfen mit BitDefender-Planer – die Systemüberprüfung wird periodisch oder zu bestimmten Zeitpunkten ausgeführt.

Sofortiges Prüfen

Um "auf Anforderung" zu prüfen, muss wie folgt vorgegangen werden:

1. Schließen Sie alle offenen Anwendungen

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).

2. Stellen Sie sicher, dass BitDefender auf dem aktuellen Stand ist

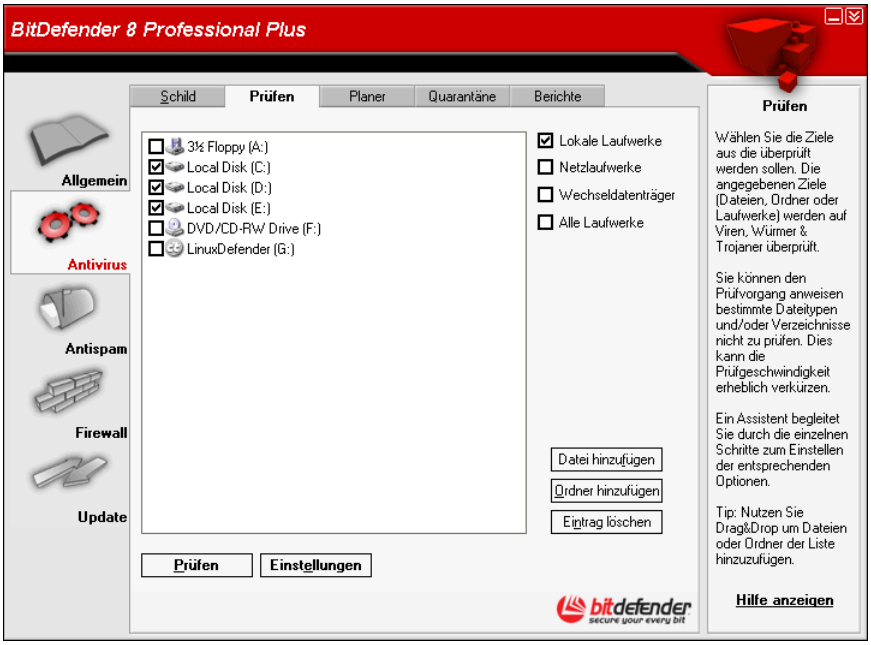
Da es täglich neue Bedrohungen durch Viren und Würmer gibt, sollten Sie, bevor Sie den Suchlauf starten, BitDefender mit Hilfe des Live-Update-Moduls aktualisieren.

Klicken Sie hierzu einfach auf **Update → Prüfen** in der BitDefender-Management-Konsole.

3. Zur Verwaltung der Dateien und Ordner, die geprüft werden

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol.

In der Management-Konsole klicken Sie auf **Antivirus → Prüfen**. Anfänglich enthält diese Sektion ein Abbild der Partitionsstruktur Ihres Systems. Außerdem sind einige Schaltflächen und Prüfoptionen sichtbar



Darstellung 18

Dieser Bereich enthält folgende Schaltflächen:

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

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

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

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

- **Einstellungen** – ermöglicht die Auswahl der zu prüfenden Dateien, die gewünschte Aktion, falls eine infizierte Datei gefunden wird, die Art der Berichterstattung sowie die Erstellung einer Berichtsdatei mit den Prüfungsergebnissen.
- **Prüfen** – startet den Prüfvorgang des Systems mit den ausgewählten Prüfoptionen.

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).
- **Alle Laufwerke** – prüft alle Laufwerke: lokale, entfernbare und verfügbare Netzwerklaufwerke.

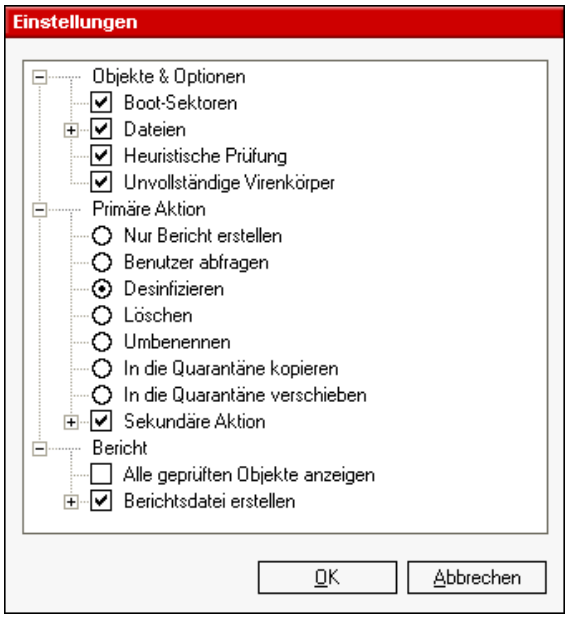
Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

Klicken Sie dann einfach auf den **Prüfen**-Button. BitDefender prüft ihren Computer nun unter Verwendung der Standard-Einstellungen.

4. Auswählen der Prüfoptionen – nur für fortgeschrittene Benutzer

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 auf **Einstellungen**, um mehr zu erfahren.



Darstellung 19

Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Sie werden in drei Kategorien eingeteilt:

- **Prüfoptionen**
- **Aktionsoptionen**
- **Berichtoptionen**

Um eine Option zu öffnen bzw. zu schließen, klicken Sie auf das Kästchen mit dem “+”- bzw. dem “-“-Zeichen.

Unter **Objekte & Optionen** können Sie die Art der zu prüfenden Objekte (Dateien, Speicher u. a.) festlegen und etwa auch, ob heuristisch gesucht werden soll (um unbekannte Viren zu entdecken). In der Kategorie **Prüfoptionen** gibt es folgende Einstellungsmöglichkeiten:

Einstellungen		Beschreibung
Boot-Sektoren		Prüft die Bootsektoren des Systems.
Dateien	Alle	Prüft alle vorhandenen Dateien, benötigt die meiste Zeit. Findet auch versteckte oder getarnte Viren.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pfd; msi; ini; csc; cmd; bas; eml; nws.`
	Nur Dateien mit folgenden Erweiterungen	Nur für fortgeschrittene Anwender. Prüft nur Dateien mit benutzerdefinierten Erweiterungen. Sie bestimmen, welche Daten geprüft werden sollen (Einschlussprinzip).
	Folgende Erweiterungen ausschließen	Nur für fortgeschrittene Anwender. Prüft alle Dateien, außer denen mit benutzerdefinierten Erweiterungen. Sie bestimmen, welche Daten nicht geprüft werden sollen (Ausschlussprinzip).
	Komprimierte Dateien	Prüft Dateien, die mit Packprogrammen, wie WinZip, WinRAR etc., komprimiert wurden.

Dateien prüfen	Archive	Prüft den Inhalt von eingepackten Archiven.
	Postfächer	Prüft den Inhalt von E-Mails und deren Attachments.
Heuristische Prüfung		Aktiviert den heuristischen Suchmodus. Mittels Heuristik können bisher unbekannte Viren auf Grundlage bestimmter Aktionsmuster und Verhaltensweisen, entdeckt werden. Dabei kann es auch zu Fehlalarmen kommen. Sollte eine verdächtige Datei auf Ihrem System gefunden werden, empfehlen wir, die Datei zur Überprüfung an das BitDefender-Virus-Labor zu schicken.
Unvollständige Virenkörper		Spürt unvollständige Virenkörper auf.

Mit der Auswahl der **Aktionsoptionen** bestimmen Sie die Aktion, die BitDefender im Falle einer entdeckten Infektion durchführen soll. Unter **Primäre Aktion** können Sie eine der folgenden Einstellungen auswählen:

Aktion	Beschreibung
Nur Bericht erstellen	Erstellt einen Bericht mit dem Namen des Virus, wenn eine infizierte Datei entdeckt wird.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne isolieren oder Löschen.
Desinfizieren	Reinigt die infizierte Datei von dem schädlichen Programmcode.
Löschen	Löscht die infizierte Datei.
Umbenennen	Ändert die Extension der infizierten Datei. Die neue Extension ist .vir. Durch die Umbenennung der infizierten Datei werden die Infektion des Systems und die weitere Verbreitung des Virus verhindert. Und die Datei steht für weitere Prüfung und Analyse zur Verfügung.
In die Quarantäne kopieren	Kopiert infizierte Dateien in die Quarantäne. Von dort aus können sie zur Analyse an das BitDefender-Viren-Labor gesendet werden. Dies bedeutet, dass eine infizierte Datei in die Quarantäne ***kopiert*** wird. Die Originaldatei bleibt infiziert im Originalverzeichnis bestehen. Es kann weiterhin auf sie zugegriffen und der schädliche Code ausgeführt werden.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Wenn das Virus in der Quarantäne ist, kann es keinen Zugriff mehr auf andere Dateien haben.
Sekundäre Aktion	Wählen Sie diese Einstellung, wenn Sie eine weitere Aktion konfigurieren möchten.

Wird eine Infektion festgestellt, können Sie neben den o. g. Optionen weitere Aktionen definieren. Setzen Sie einen Haken vor **Sekundäre Aktion** und klicken Sie auf das "+"-Zeichen. Folgende Optionen stehen zur Verfügung.

Aktion	Beschreibung
Nur Bericht erstellen	Erstellt einen Bericht mit dem Namen des Virus, wenn eine infizierte Datei entdeckt wird.

Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne isolieren oder Löschen.
Löschen	Löscht die infizierte Datei.
Umbenennen	Ändert die Extension der infizierten Datei. Die neue Extension ist .vir. Durch die Umbenennung der infizierten Datei werden die Infektion des Systems und die weitere Verbreitung des Virus verhindert. Und die Datei steht für weitere Prüfung und Analyse zur Verfügung.
In die Quarantäne kopieren	Kopiert infizierte Dateien in die Quarantäne. Von dort aus können sie zur Analyse an das BitDefender-Viren-Labor gesendet werden. Dies bedeutet, dass eine infizierte Datei in die Quarantäne ***kopiert wird*** wird. Die Originaldatei bleibt infiziert im Originalverzeichnischnis bestehen. Es kann weiterhin auf sie zugegriffen und der schädliche Code Code ausgeführt werden.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Wenn das Virus in der Quarantäne ist, kann es keinen Zugriff mehr auf andere Deteien haben.

Der nächste Schritt ist die Auswahl der **Berichtoptionen**. Klicken Sie auf das "+"-Zeichen. Nun können Sie Art und Form der Berichtdatei bestimmen.

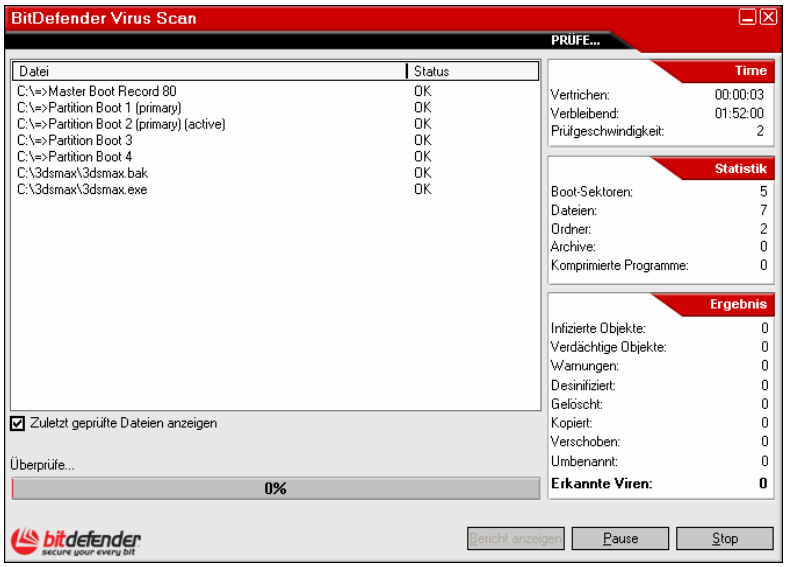
Optionen		Beschreibung
Alle geprüften Objekte anzeigen		Zeigt in einer Berichtdatei den Status und mögliche Infektionen aller geprüften Dateien an.
Create report file	Berichtdatei <vscan.log>	In diesem Feld können Sie den Namen der Berichtdatei festlegen. Klicken Sie auf die Beschreibung und geben Sie den neuen Dateinamen ein. Vorgabe ist vscan.log.
	Zum vorhandenen Bericht hinzufügen	Wählen sie diese Option aus, wenn Sie die Informationen über den neuen Prüfvorgang zu einer schon vorhandenen Berichtdatei hinzufügen möchten.
	Berichtdatei auf [1024] KB begrenzen	Im Laufe der Zeit können sich große Berichtdateien entwickeln. Klicken Sie, um die Größe der Berichtdatei zu begrenzen, auf das Kästchen und geben Sie in das angezeigte Feld die maximale Größe der Datei in KB ein.

Tipp: Sie können den Bericht im Register Bericht (im Antivirus-Modul) einsehen.

Klicken Sie auf **OK**, um das Fenster mit den Prüfeinstellungen zu schließen.

5. Prüfung starten

Nachdem Sie die Prüfoptionen bestimmt haben, müssen Sie nur noch den Prüfvorgang starten, indem Sie auf **Prüfen** klicken. Die Prüfung kann einige Zeit in Anspruch nehmen, abhängig von der Größe Ihres Festplattenlaufwerks!



BitDefender zeigt Ihnen während der Prüfung den Fortschritt und alarmiert Sie, wenn irgendwelche Viren gefunden werden.

Während des Prüfvorganges werden in einem 3-teiligen Fenster der Verlauf und die gefundenen Viren angezeigt.

Darstellung 20

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

Folgende Aktionen stehen Ihnen während des Prüfvorganges zur Verfügung:

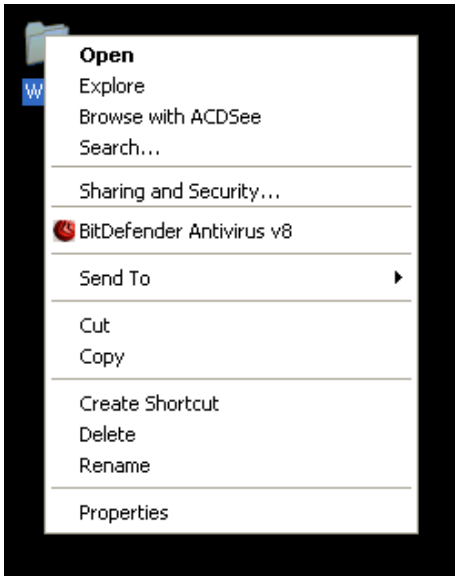
- **Stop** – Ein neues Fenster öffnet sich und Sie werden gefragt, ob Sie die Systemprüfung stoppen möchten. Wenn Sie sich entscheiden, den Suchvorgang abzubrechen, ändert sich die **Stop-**Schaltfläche in **Schließen**; ein Klick darauf schließt das Suchfenster.
- **Pause** – Hält den Prüfvorgang für eine bestimmte Zeit an; klicken Sie auf **Fortsetzen**, um ihn wieder zu starten.

TIPP: Wenn Sie beim Suchlauf die überprüften Dateien laufend angezeigt haben möchten, müssen Sie in den Prüfeinstellungen die Option **Zuletzt geprüfte Dateien anzeigen** aktivieren. Bitte beachten Sie, dass diese Option Ihren Computer während des Prüfvorgangs verlangsamt.

6. Weitere Scanmöglichkeiten

BitDefender bietet zwei weitere Möglichkeiten, einzelne Dateien oder Ordner direkt zu prüfen. Es gibt die Möglichkeit, über ein Kontextmenü zu scannen oder aber über die Drag & Drop-Funktion.

Scannen mit dem Kontextmenü



Darstellung 21

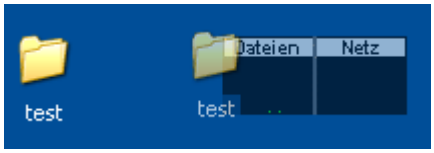
Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei. Wählen Sie **BitDefender Antivirus v8** aus.

Zusätzlich wird eine Berichtdatei erzeugt, welche im Modul **Antivirus → Berichte** eingesehen werden kann.

Prüfen per Drag & Drop

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

Darstellung 22

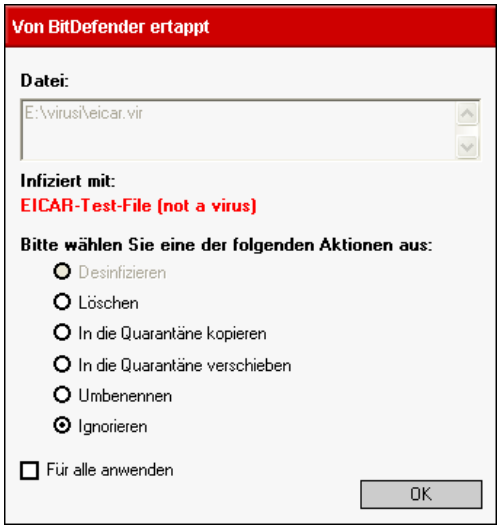


Darstellung 23

Zusätzlich wird eine Berichtdatei `activbar.log` erzeugt, welche unter **Antivirus → Berichte** eingesehen werden kann.

In einem neuen Fenster werden der Vorgang und das Ergebnis der Prüfung angezeigt.

Wird ein Virus gefunden, erscheint folgendes Fenster:



Darstellung 24

Hier sehen Sie den Namen der Datei und des Virus.

Nun können Sie eine der folgenden Möglichkeiten auswählen:

- **Desinfizieren** – reinigt die infizierten Dateien.
- **Löschen** – löscht automatisch alle infizierten Dateien, ohne eine Warnmeldung auszugeben. Wir empfehlen Ihnen, eine Kopie dieser Dateien anzulegen und sie nur dann zu löschen, wenn Sie sicher sind, dass sie nicht mehr benötigt werden.
- **In die Quarantäne kopieren** – kopiert infizierte Dateien in die Quarantäne.
- **In die Quarantäne verschieben** – verschiebt die infizierten Dateien in die Quarantäne.
- **Umbenennen** – benennt die infizierten Dateien um. Indem die infizierten Dateien umbenannt werden, vermeiden Sie, dass diese ausgeführt werden und sich weiter verbreiten können. Gleichzeitig können diese Dateien für weitere Untersuchungen gespeichert werden.
- **Ignorieren** – in diesem Fall wird die Infizierung ignoriert und keine Aktion ausgeführt. Nur der Standort der Datei wird angezeigt.

Wenn Sie wünschen, dass die ausgewählte Aktion für alle infizierten Dateien gilt, wählen Sie **Für alle anwenden** aus.

Wenn die Option „Desinfizieren“ nicht aktiviert ist, wird die Datei nicht desinfiziert. Verschieben Sie sie dann am besten in die Quarantäne, um sie uns für eine Analyse zuzusenden, oder löschen Sie sie.

Klicken Sie auf **OK**.

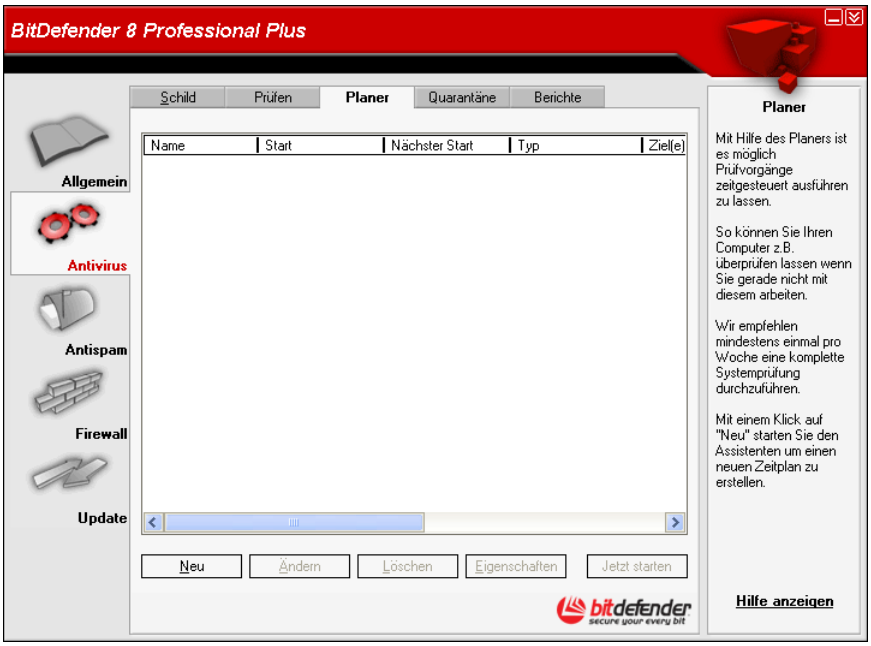
Prüfen mit dem BitDefender-Planer

Durch den BitDefender-Planer wird die Systemüberprüfung periodisch oder zu bestimmten Zeitpunkten ausgeführt, ohne dass der Benutzer eingreifen muss. Dazu wird vorher ein so genannter Task, eine Aufgabe oder ein Ereignis erstellt.

Das Prüfen wird mittels des **Planer**-Moduls durchgeführt. Es hat folgende Eigenschaften:

- Unterstützung durch einen Assistenten;
- Auswahl der Prüfwiederholungen;
- wählt Laufwerke und/oder Ordner aus;
- wählt Dateierweiterungen aus;
- hat verschiedene Konfigurationsmodule für jede Prüfaufgabe;
- ermöglicht das Prüfen von Netzlaufwerken;
- die infizierten oder verdächtigen Dateien werden automatisch in der Quarantäne isoliert;
- prüft im Hintergrund, ohne den Eingriff des Benutzers;
- fasst die Eigenschaften der geplanten Aufgabe zusammen;
- prüft Berichte, die in Berichtdateien generiert wurden.

Gehen Sie in der Management-Konsole zum **Antivirus**-Modul und klicken Sie auf das Register **Planer**.



Darstellung 25

Hier finden Sie einige Schaltflächen, die zur Verwaltung der Prüfaufgaben dienen:

- **Neu** – startet den Assistenten, der Sie bei der Erstellung eines neuen Prüf-Ereignisses unterstützt.
- **Ändern** – ändert die Eigenschaften eines vorher erstellten Ereignisses. Dabei wird ebenfalls der Assistent gestartet.

> Wenn Sie den Namen des Ereignisses ändern, wird ein neues Ereigniss unter dem neuen Namen erzeugt.

- **Löschen** – löscht ein ausgewähltes Ereignis.
- **Eigenschaften** – zeigt die Eigenschaften eines ausgewählten Ereignisses an.
- **Jetzt starten** – startet sofort die ausgewählte Aufgabe.

Die Benutzeroberfläche des **Planers** enthält ebenfalls eine Liste, in der die Prüfereignisse angezeigt werden. Diese enthält den Namen des Prüfereignisses, das Datum der ersten Ausführung, das Datum der nächsten Ausführung und die Prüfart (periodisch oder einmalig).

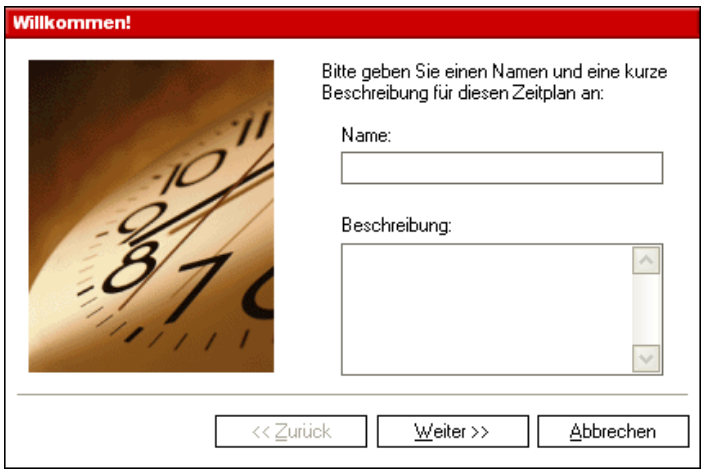
Weiterhin wird die Art und Weise der Erstellung eines Prüfereignisses erklärt. Der Planer enthält einen Assistenten, mit dem neue Aufgaben erstellt werden. Er wird Ihnen jedes Mal Hilfe leisten, wenn Sie ein neues Ereignis erstellen möchten oder ein schon vorhandenes ändern möchten.

Klicken Sie auf **Neu**. Damit starten Sie den Erstellungsassistent für Prüfaufgaben.

TIPP: Es wird empfohlen, dass Sie einen vollen System-Scan mindestens einmal wöchentlich festlegen.

1. Einführung

Zuerst muss der Name des neuen Tasks angegeben werden.



Geben Sie den Namen des neuen Ereignisses in das Feld **Name** ein und fügen Sie eine kurze Beschreibung in das Feld **Beschreibung** ein.

Klicken Sie auf **Weiter**, um fortzufahren.

Darstellung 26

Wenn Sie **Abbrechen** anklicken, öffnet sich ein Fenster, in dem Sie Ihre Entscheidung bestätigen: die Task-Erstellung abzubrechen oder fortzusetzen.

2. Einstellungen des Zeitplans/Datum anzeigen

Als Nächstes erscheint ein Fenster (siehe nachfolgende Abbildung), in dem Sie die Prüfart auswählen können.

Klicken Sie auf **Einmalig**, falls Sie eine einzige Prüfung planen möchten. Falls die Prüfung nach einer bestimmten Zeitspanne wiederholt werden soll, klicken Sie auf **Periodisch**.

Danach geben Sie in das Eingabe-Kästchen die Anzahl der Minuten/ Stunden/Tage/Wochen/Jahre ein und der Prozess wird nach dem Ablauf der angegebenen Zeitspanne wiederholt.

Darstellung 27

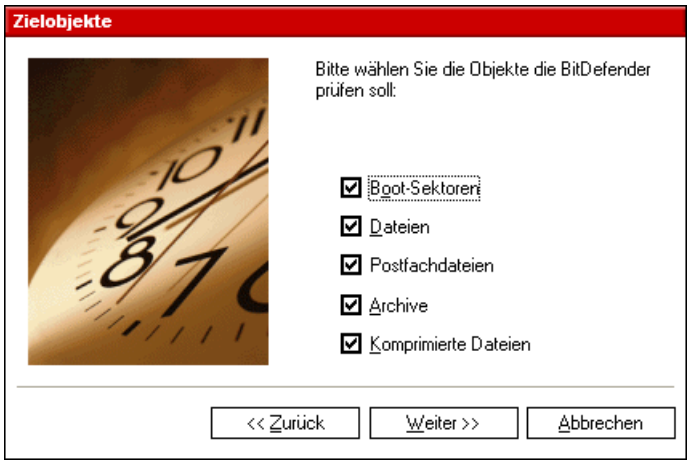
Sie können auf die Pfeile klicken, um die Minuten-/Stunden-/Tage-/Wochen-/Jahreszähler höher oder niedriger einzustellen. Legen Sie die Zeitspanne fest, nach der der Prüfvorgang wiederholt werden soll. Scrollen Sie die Liste hinunter und klicken Sie die gewünschte Zeiteinheit an.

Falls Sie die Option für ein wiederholtes Prüfen ausgewählt haben, ist der Prüfvorgang zeitlich unbegrenzt. Um dieses Ereignis zu verwerfen, muss es von der Ereignisliste aus dem Planerfenster gelöscht werden.

Nachdem Sie die Zeitspanne festgelegt haben, klicken Sie auf **Weiter**, um fortzufahren und die zu prüfenden Objekte auszuwählen. Falls Sie Ihre Aktion rückgängig machen möchten, klicken Sie auf **Zurück**.

3. Zielobjekte

Als Nächstes wählen Sie die zu prüfenden Objekte – Bootsektor, Arbeitsspeicher, Dateien, Archive und/oder komprimierte Dateien – aus.



Die Liste mit den vorhandenen Objekten wird in der nebenstehenden Abbildung gezeigt. Wählen Sie eines oder mehrere Zielobjekte aus, indem Sie diese(s) einfach anklicken. Die ausgewählten Objekte werden mit einem Haken im entsprechenden Kästchen angezeigt.

Darstellung 28

Sie können eines der folgenden Objekte auswählen:

- **Boot-Sektoren** – prüft den Bootsektor, um Bootviren zu erkennen;
- **Dateien** – prüft den Arbeitsspeicher des Systems, um im Arbeitsspeicher vorhandene Viren zu entdecken;
- **Postfachdateien** - prüft Mailarchive, um Mailviren zu entdecken;
- **Archive** – prüft Archivinhalte;
- **Komprimierte Dateien** – prüft komprimierte Dateien.

Klicken Sie anschließen auf **Weiter**.

4. Zielpfad auswählen

Weiterhin müssen Sie den Pfad des zu prüfenden Objektes, wie in der Abbildung dargestellt, auswählen. Dieser Schritt ist erforderlich, wenn Sie vorher die Option **Dateien prüfen** ausgewählt haben.

Nebenstehend wird das Explorerfenster angezeigt, aus dem Sie die zu prüfenden Partitionen, Ordner und Dateien auswählen können.

Wenn sich der Mauszeiger auf einer Datei befindet, wird der vollständige Pfad der Datei in dem Feld unter dem Explorer-fenster angezeigt.

Darstellung 29

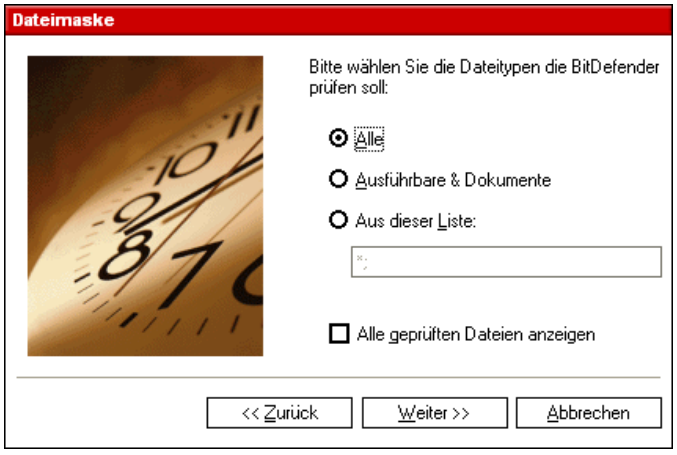
Um die zu prüfenden Adressen auszuwählen, können Sie auch die Schnellauswahl verwenden, die sich über dem Explorerfenster befindet:

- **Lokale Laufwerke** – prüft alle lokalen Laufwerke;
- **Netzlaufwerke** – prüft alle Netzwerklaufwerke.

Klicken Sie dann auf **Weiter**.

5. Dateimaske wählen

Weiterhin müssen Sie die Art der zu prüfenden Dateien auswählen. Dieser Schritt ist nur erforderlich, wenn Sie vorher die Option **Dateien** prüfen aktiviert haben.



Das nebenstehende Fenster zeigt die Liste mit den Datei-Kategorien an.

Darstellung 30

Sie müssen sich für eine einzige Kategorie entscheiden:

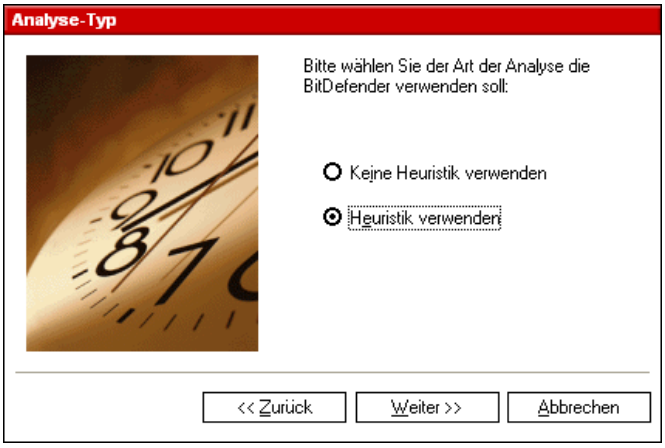
- **Alle** – prüft alle Dateitypen;
- **Ausführbare & Dokumente** – prüft Programmdateien und Dokumente;
- **Aus dieser Liste** – prüft nur die Dateien, deren Erweiterungen nicht in der Liste erscheinen. Diese Erweiterungen müssen durch ein Semikolon getrennt werden.

Falls Sie Informationen zu allen geprüften, infizierten oder nicht infizierten Dateien sehen möchten, wählen Sie die Option **Alle geprüften Dateien anzeigen**. Aber bedenken Sie, dass sich Ihre Computerleistung mit dieser Einstellung reduziert.

Klicken Sie dann auf **Weiter**.

6. Prüfart auswählen

Weiterhin müssen Sie die Prüfart auswählen.



Wie Sie in der nebenstehenden Abbildung sehen können, müssen Sie eine der beiden Prüfmöglichkeiten auswählen:

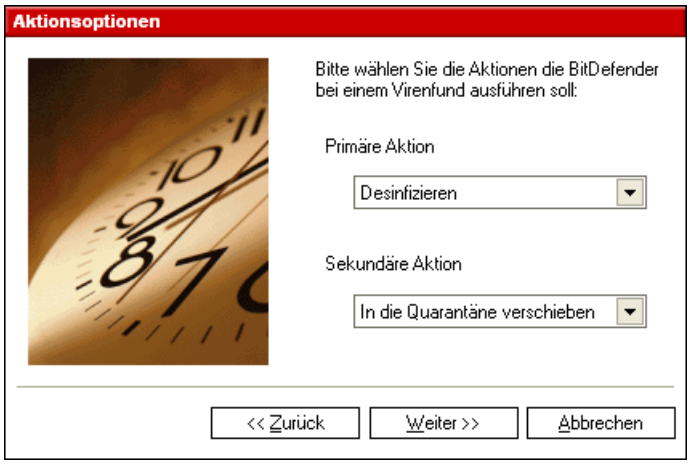
Darstellung 31

- Keine Heuristik verwenden - bedeutet, dass die Dateien anhand von Virensignaturen geprüft werden. Um diese Prüfart zu aktivieren, klicken Sie auf **Keine Heuristik verwenden**;
- Heuristik verwenden – stellt eine auf bestimmten Algorithmen basierende Methode dar. Sie dient dem Zweck, neue, noch unbekannte Viren zu entdecken. Gelegentlich können dadurch vermeintlich verdächtige Codes in normalen Programmen gemeldet werden (Fehlalarm). Um diese Prüfart zu aktivieren, klicken Sie auf **Heuristik verwenden**.

Klicken Sie auf **Weiter**.

7. Aktionsoptionen

Wählen Sie dann zwei Aktionen aus, die im Fall eines Virenfundes ausgeführt werden sollen.



Sie können sowohl die erste als auch die zweite Aktion auswählen.

Darstellung 32

Wir empfehlen Ihnen, **Desinfizieren** als erste und **In die Quarantäne verschieben** als zweite Aktion auszuwählen.

Für die erste Aktion haben Sie mehrere Optionen:

Erste Aktion	Beschreibung
Desinfizieren	Desinfizieren der Dateien.
Datei löschen	Löscht automatisch, ohne Warnung, alle infizierten Dateien. Nicht empfohlen!
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Somit kann auf die Datei nicht mehr zugegriffen werden.
Umbenennen	Ändert die Extension der infizierten Datei. Die neue Extension ist .vir. Durch die Umbenennung der infizierten Datei werden die Infektion des Systems und die weitere Verbreitung des Virus verhindert. Und die Datei steht für weitere Prüfung und Analyse zur Verfügung.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne isolieren oder Löschen.
Ignorieren	Die Infektion wird ignoriert und es wird keine Aktion durchgeführt. Es wird nur der Status berichtet.

Für die zweite Aktion haben Sie folgende Möglichkeiten:

Zweite Aktion	Beschreibung
Datei löschen	Löscht automatisch, ohne Warnung, alle infizierten Dateien. Nicht empfohlen!
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Somit kann auf die Datei nicht mehr zugegriffen werden.
Umbenennen	Ändert die Extension der infizierten Datei. Die neue Extension ist

	.vir. Durch die Umbenennung der infizierten Datei werden die Infektion des Systems und die weitere Verbreitung des Virus verhindert. Und die Datei steht für weitere Prüfung und Analyse zur Verfügung.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne isolieren oder Löschen.
Ignorieren	Die Infektion wird ignoriert und es wird keine Aktion durchgeführt. Es wird nur der Status berichtet.

Klicken Sie auf **Weiter**.

8. Bericht

Wählen Sie nun, ob und wie ein Prüfbericht erstellt werden soll.

Um einen Bericht zu erstellen, klicken Sie auf **Bericht erstellen**. Damit werden auch alle anderen Optionen für die Berichterstellung aktiviert.

Darstellung 33

Geben Sie den Namen des Berichts in das Feld **Dateiname** ein. Standardname ist `schedule.log`. Der Bericht beinhaltet Informationen über den Scanprozess: die Anzahl der entdeckten Viren, die Anzahl der geprüften Dateien, die Anzahl der desinfizierten und entfernten Viren.

Aktivieren Sie **An bestehenden Bericht anfügen**, wenn Sie die Informationen über eine neue Prüfung an einen alten Bericht anfügen möchten. So haben Sie nachher einen ausführlichen Bericht über alle Ereignisse der Vergangenheit.

Klicken Sie **Alten Bericht überschreiben** an, wenn Sie jedesmal einen neuen Bericht haben möchten. Auf diese Weise werden alle alten Informationen gelöscht.

Tipp: Sie können den Bericht im Register Bericht (im Antivirus-Modul) ansehen.

Klicken Sie auf **Weiter**.

9. Zusammenfassung

Damit haben Sie ein neues Prüfereignis erstellt. Es werden Ihnen alle Einstellungen noch einmal zusammenfassend gezeigt.

In der nebenstehenden Abbildung kann man sehen, dass alle Einstellungen eines Prüfereignisses angezeigt werden.

Darstellung 34

Sie können jede gewünschte Änderung vornehmen, indem sie Ihre Aktionen rückgängig machen. Klicken Sie dazu auf **Zurück**.

Falls Sie keine weiteren Änderungen vornehmen möchten, klicken Sie auf **Fertigstellen**. Das neue Ereignis wird nun im Planerfenster angezeigt.

Für jedes geplante Prüfereignis werden Name, Beschreibung, Startzeit, die Zeit der nächsten Ausführung, die Prüfart (periodisch oder einmalig), das Ziel, die Dateierweiterungen, die Analyseart und die auf infizierte Dateien anzuwendende Aktion angegeben.

Anmerkung

Wenn Sie ein Prüfereignis ändern möchten, müssen Sie die gleichen Schritte wie bei der Erstellung ausführen. Falls sich der Ereignisname ändert, wird ein neues Ereignis erstellt. Ein Beispiel: Sie haben ein Ereignis EV1 genannt und Sie ändern den Namen in EV2, dann wird EV1 nicht verloren gehen, sondern es wird ein neues Ereignis EV2 mit den gleichen Eigenschaften wie EV1 erstellt.

Wenn Sie mit der rechten Maustaste auf ein geplantes Ereignis klicken, erscheint ein Popup-Menü, so wie im angezeigten Bild:

Falls kein Ereignis ausgewählt wurde und Sie mit der rechten Maustaste in das Fenster klicken, wird nur die Option **Neu** aktiviert, alle anderen Optionen sind deaktiviert.

Darstellung 35

Tipp: Der Planer ermöglicht eine unbegrenzte Anzahl von geplanten Prüfereignissen.

Sie können auch mit der Tastatur durch die Scan-Ereignisse surfen: drücken Sie die **Löschtaste**, um das gewählte Scan-Ereignis zu löschen, drücken Sie die **Eingabetaste**, um die gewählten Ereigniseigenschaften anzusehen oder die **Inserttaste**, um ein neues Ereignis zu erstellen (der Planer-Assistent erscheint).

Drücken Sie die Pfeiltasten, um in der Ereignisliste zu navigieren.

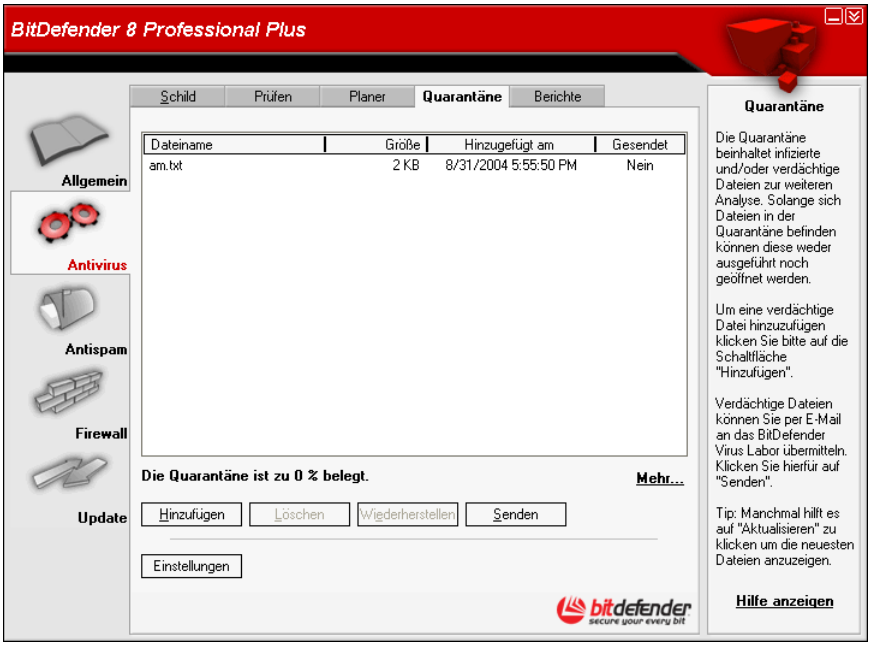
Isolation von infizierten Dateien

BitDefender 8 Professional Plus ermöglicht die Isolation von infizierten Dateien in einem sicheren Bereich, der so genannten Quarantäne. Durch die Isolation der infizierten Dateien in der Quarantäne reduziert sich das Risiko einer weiteren Infektion. Die infizierten Dateien können zur genaueren Analyse automatisch oder manuell an das BitDefender-Labor gesendet werden.

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

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol.

In der Management-Konsole wählen Sie das **Antivirus**-Modul und klicken auf das Register **Quarantäne**.



Darstellung 36

Wie Sie in der obigen Darstellung sehen können, enthält das Quarantäne-Fenster eine Liste mit allen infizierten Dateien, die isoliert wurden. Bei jeder Datei werden Name, Größe, Datum der letzten Änderung und der Name des Quarantäne-Ordners angezeigt. Wenn Sie mehr Informationen darüber sehen möchten, klicken Sie **Mehr Informationen** an.

Anmerkung

Wenn das Virus in der Quarantäne ist, kann auf die Datei nicht mehr zugegriffen werden.

Die Quarantäne-Oberfläche enthält folgende Buttons:

➔ **Hinzufügen** - Falls Sie wissen oder glauben, dass Sie eine infizierte Datei auf Ihrem Rechner haben, können Sie diese im Quarantäneordner isolieren. Ein neues Fenster öffnet sich und Sie können die Datei auswählen. Damit wird die Datei in die Quarantäne verschoben. Wenn Sie die Datei in die Quarantäne-Zone verschieben möchten, wählen Sie die Checkbox **Original-Datei(en) löschen** aus. Eine weitere Methode, infizierte Dateien in die Quarantäne zu verschieben, ist, sie per Drag & Drop in das Quarantäne-Feld zu ziehen.

➔ **Löschen** – entfernt die ausgewählte Datei.

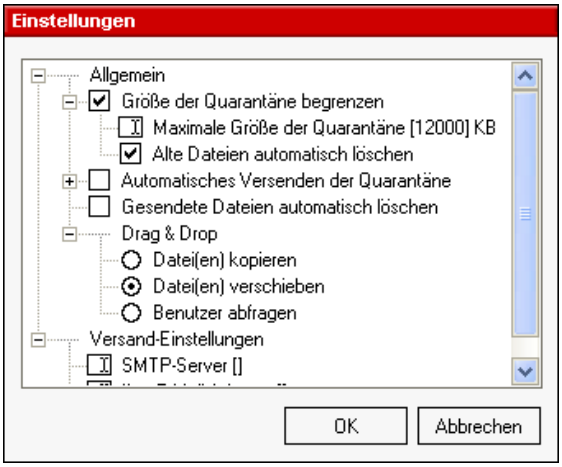
➔ **Wiederherstellen** – stellt markierte Dateien im Ursprungsverzeichnis wieder her.

➔ **Senden** - Sie können diese Dateien zur gründlichen Analyse an das BitDefender-Labor senden. Dazu müssen Sie vorher, wie weiter unten dargestellt, unter **Einstellungen** die entsprechenden **Versand-Einstellungen** eintragen.

Anmerkung

Standardmäßig werden alle Dateien zur gründlichen Analyse an das BitDefender-Labor gesendet. Wenn Sie die Dateien nicht an das BitDefender-Labor senden möchten, deaktivieren Sie **Automatisches Versenden der Quarantäne** in den Einstellungen.

➔ **Einstellungen** – öffnet ein Fenster für die Einstellungen des Quarantäne-Moduls:



Darstellung 37

Die Quarantäne-Einstellungen sind in zwei Kategorien unterteilt:

- **Quarantäne-Einstellungen**
- **Versand-Einstellungen**

Klicken Sie auf das Kästchen mit dem "+"-Zeichen, um eine Option zu öffnen, oder auf das "-"-Zeichen, um eine Option zu schließen.

Quarantäne-Einstellungen

➔ **Größe der Quarantäne begrenzen** – die Größe des Quarantäne-Ordners wird begrenzt auf 12000 KB. Sie können auch eine beliebige Größe im Feld **Maximale Größe der Quarantäne** angeben.

Wenn Sie die Funktion **Alte Dateien automatisch löschen** aktivieren, werden alte Dateien aus der Quarantäne gelöscht, sobald der Ordner voll ist.

➔ **Automatisches Versenden der Quarantäne** – sendet automatisch alle Dateien aus dem Quarantäne-Ordner zur Überprüfung an das BitDefender-Virenlabor. Sie können überdies in Minuten angeben, wie oft die Dateien in der Quarantäne versendet werden sollen.

➔ **Gesendete Dateien automatisch löschen** – löscht automatisch die aus der Quarantäne gesendeten Dateien.

➔ **Drag & Drop** – für die Drag & Drop-Funktion des Quarantäne-Ordners können Sie hier die Art des Drag & Drop einstellen: Kopieren der Dateien, Verschieben der Dateien, Bestätigung durch den Anwender.

Versand-Einstellungen

Sie müssen einige Einstellungen vornehmen, um die Dateien aus dem Quarantäne-Ordner an das BitDefender-Virenlabor zu senden.

➔ **SMTP-Server** – hier muss der Name und die Adresse des Post-Ausgangsservers eingegeben werden, den Sie zum Versenden Ihrer E-Mails verwenden.

Diese Angaben können Sie den Einstellungen Ihres E-Mail-Programms oder den Vorgaben Ihres Providers hinsichtlich Ihres E-Mail-Accounts entnehmen.

Anmerkung

Der SMTP-Server kann mit dem Namen (z. B. `server.company.com`) oder mit der IP-Adresse (z. B. 196.23.21.3) angegeben werden.

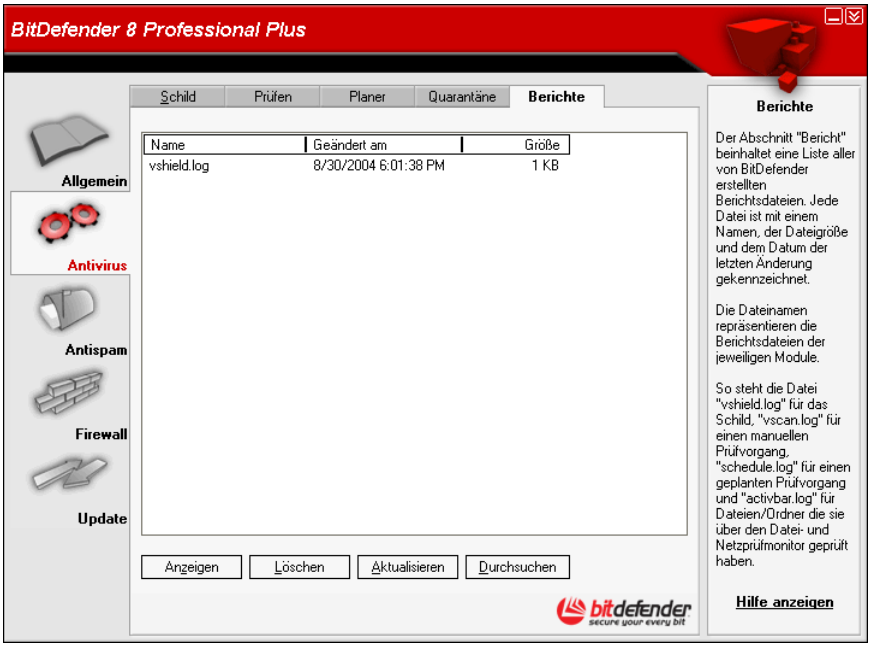
➔ **Ihre E-Maildresse** – geben Sie hier Ihre E-Mail-Adresse an, wenn Sie eine Antwort bezüglich der eingesendeten Dateien aus dem Virenlabor haben möchten.

Ansicht der Berichtdateien

Wenn eine Prüfung ausgeführt wird, kann der Benutzer die Optionen so konfigurieren, dass eine Berichtdatei erstellt und Informationen über den Prüfvorgang angezeigt werden. Diese Informationen kann der Benutzer direkt in der Management-Konsole betrachten.

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol.

In der Mangement-Konsole klicken Sie das **Antivirus**-Modul an und darin das Register **Berichte**.



Darstellung 38

BitDefender zeichnet alle seine Aktivitäten und Ergebnisse auf Ihrem Computer auf. Folgende Statistiken stehen Ihnen zur Verfügung:

- Vshield.log ist der Bericht, in dem BitDefender alle geprüften, infizierten, reparierten und verschobenen Dateien oder E-Mails vermerkt;
- Vscan.log wird geschrieben, wenn Sie eine manuelle Systemprüfung starten;
- Schedule.log enthält die Ergebnisse der geplanten Suchläufe, die Sie festgelegt haben;
- Activbar.log wird erstellt, wenn Sie mit Drag & Drop möglicherweise infizierte Dateien prüfen.

Der **Berichtbereich** enthält eine Liste aller Berichtdateien die bisher generiert wurden. Bei jeder Datei werden Name, Größe und Datum der letzten Änderung angezeigt.

Zur Verwaltung der Berichtdateien sind folgende Schaltflächen vorhanden:

- **Anzeigen** – öffnet die ausgewählte Berichtdatei.
- **Löschen** – löscht die ausgewählte Berichtdatei.
- **Aktualisieren** – Falls in der Management-Konsole das Register **Berichte** geöffnet ist und in der Zwischenzeit ein Prüfvorgang auf Ihrem Computer stattfindet, wird die neue Berichtdatei mit den Prüfergebnissen (wenn Sie die Option **Dateibericht erstellen** ausgewählt haben) nur dann angezeigt, wenn sie auf **Aktualisieren** klicken.
- **Durchsuchen** – öffnet ein Fenster, in dem Sie die Berichtdateien, die Sie sich ansehen wollen, auswählen können.

TIPP: Die Berichtdateien (die im Berichtbereich erscheinen) werden im selben Ordner gespeichert, in dem BitDefender installiert wurde. Wenn Sie die Berichtdateien in einem anderen Ordner gespeichert haben, klicken Sie auf **Durchsuchen**, um diese Dateien zu finden.

Die Entfernung eines entdeckten Virus

Viren sind viel einfacher zu stoppen, wenn sie lediglich versuchen auf Ihr System zuzugreifen, als wenn sie bereits Ihren Computer befallen haben.

Deshalb sollte der Virusschutz immer aktiviert und aktualisiert werden.

Wenn BitDefender einen residenten Virus entdeckt hat, wird empfohlen, ihn durch BitDefender entfernen zu lassen.

Dies kann auf verschiedene Art und Weise geschehen - die residenten Viren, die auf Ihrem System bereits aktiv sind, können sehr trickreich sein.

Wenn BitDefender einen Virus findet und nicht in der Lage ist, Ihr System zu desinfizieren, sollten Sie mit unsererem Unterstützungsteam support@bitdefender.de in Verbindung treten.

Das Geheimnis zum Entfernen eines Virus ist, alles über den Virus zu wissen. Sie finden zusätzliche Informationen über Viren auf unserer Website: www.bitdefender.de

Für die weitverbreitetsten Viren bieten wir spezielles Desinfizierungswerkzeug an.

Es ist immer eine gute Idee, im Internet nach allen Informationen zu suchen, die Sie über Viren finden können.

Wünschen Sie mehr Hilfe, treten Sie mit unserem Support in Verbindung:
support@bitdefender.de

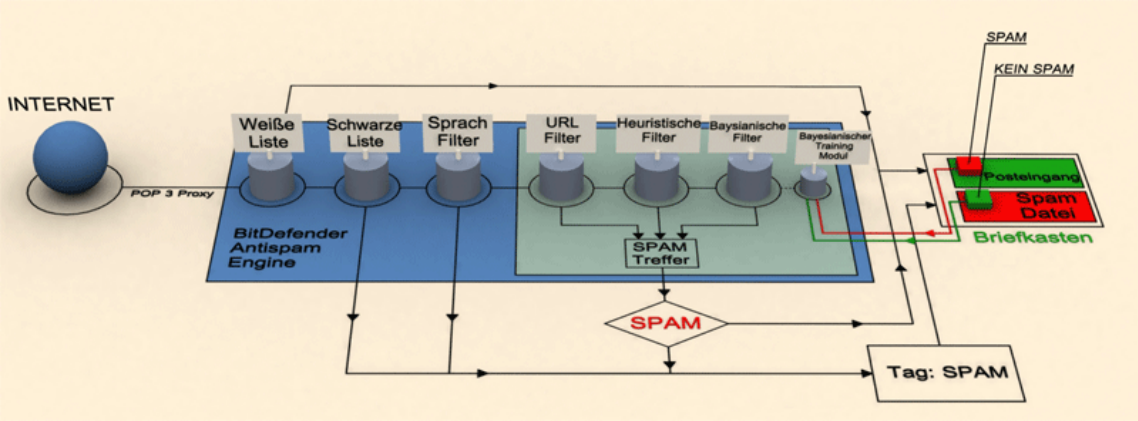
Antispam-Modul

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

Eigenschaften

Wie es arbeitet

Das unten abgebildete Schema zeigt, wie BitDefender arbeitet.



Darstellung 39

BitDefender-Antispam arbeitet mit sechs verschiedenen Filtern, die sicherstellen, dass Ihr Posteingang spamfrei bleibt: **Weiße Liste, Schwarze Liste**, **Sprach-Filter, URL-Filter, Heuristischer Filter** und **Bayesianischer Filter**.

Sie können jeden dieser Filter im Antispam-Modul in der **BitDefender-Management-Konsole** aktivieren/deaktivieren.

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

Anders der Filter **Schwarze Liste,** der überprüft, ob der Absender in dieser Liste steht. Falls nicht, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

Der Sprach-Filter überprüft, ob die E-Mail in Kyrillisch oder mit asiatischen Buchstaben geschrieben worden ist. Falls dem so ist, wird die Mail markiert und in den **Spam**-Ordner verschoben. Falls die E-Mail diese Merkmale nicht aufweist, wird sie mit dem URL-Filter überprüft.

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

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

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

Der Bayesianische Filter analysiert die Nachricht bezüglich statistischer Informationen in Bezug auf spezielle Wörter und vergleicht diese mit denen, die nicht als Spam klassifiziert sind.

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

Anmerkung

Falls Sie einen anderen E-Mail-Clienten als Microsoft Outlook oder Microsoft Outlook Express verwenden, sollten Sie Regeln entwickeln, um E-Mails, die als Spam markiert sind, in den BitDefender-Quarantäne- Ordner zu verschieben. BitDefender wird den E-Mails den Anhang SPAM hinzufügen.

Weiße Liste/Schwarze Liste

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine Freundes- und Spamliste geführt, so können Sie festlegen, welche E-Mails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

Weiße Liste/Schwarze Liste ist auch als **Freundes-Liste/Spammer-Liste** bekannt.

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

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

Sprach-Filter

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

URL-Filter

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

Immer dann, wenn Sie ein Update machen, werden dem URL-Filter neue Links hinzugefügt, um so die Effektivität des URL-Filters zu steigern.

Jeder URL-Link innerhalb einer E-Mail wird mit der Datenbank verglichen und bei einem Treffer wird die Mail der Spamliste hinzugefügt.

Heuristischer Filter

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

Entdeckt er E-Mails mit sexuellem Inhalt in der Bertreffzeile, werden diese Mails als Spam identifiziert.

Anmerkung

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

TIPP: Immer dann, wenn Sie ein Update durchführen, werden dem Heuristischen Filter neue Regeln hinzugefügt, somit wird die Effektivität des Antispam-Moduls verbessert. BitDefender kann automatische Updates durchführen. Lassen Sie daher das automatische Update aktiviert.

Bayesianischer Filter

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

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

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

Sie korrigieren das Modul, indem Sie die **Ist Spam**- und **Ist kein Spam**-Buttons in der BitDefender-Symbolleiste anklicken (zu finden in **Outlook** und **Outlook Express**).

Sie können diese Filter alle im Antispam-Modul in der **BitDefender-Management-Konsole** aktivieren/deaktivieren.

Konfigurieren des BitDefenders über die Management-Konsole

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü: **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: klicken Sie auf das BitDefender Symbol.

In der Management-Konsole klicken Sie auf **Antispam**.

Darstellung 40

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

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

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

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

Einstellen des aggressivsten Levels

Bewegen Sie den Schieberegler, um den Toleranzlevel einzustellen.

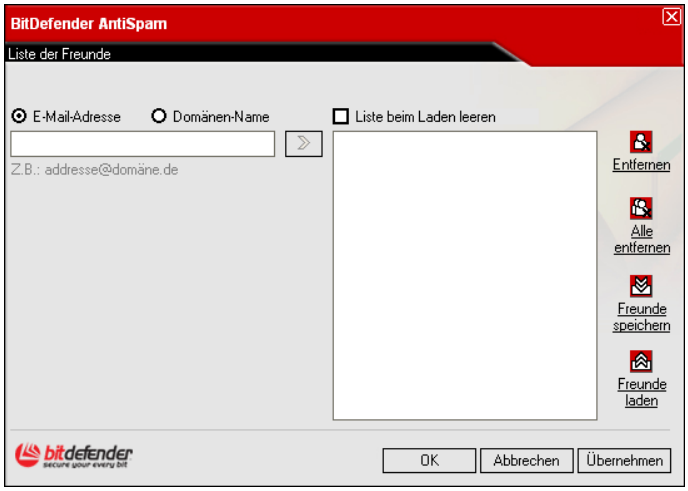
- **Tolerant** – bedeutet, dass Spam hereinkommen kann.
- **Aggressiv** – bedeutet, dass sehr wenig Spam hereinkommt, dass aber auch einige legitime Mails als Spam markiert werden können.

Ausfüllen der Adressliste

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

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

Um die Freundesliste zu handhaben, klicken Sie auf ››› (übereinstimmend mit Ihrer Freundesliste) oder klicken Sie auf den **Freunde**-Button in der BitDefender-Symbolleiste bei Outlook oder Outlook Express. Das folgende Fenster mit Informationen über Ihre Freunde erscheint:



Hier können Sie die Einträge Ihrer Freundesliste ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adressse**, tragen Sie sie ein und klicken Sie auf den »-Button.

Die Adresse wird Ihrer Freundesliste hinzugefügt.

Darstellung 41

Die Adresse muss so aussehen: `name@domain.com`

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

Die Domain muss folgendes Aussehen haben:

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

Anmerkung

Jede Mail mit einer Freundes-Adresse wird automatisch in Ihren Posteingang verschoben.

Um ein Objekt aus der Liste zu löschen, klicken Sie auf den **Entfernen**-Button. Sie können so viele Objekte auswählen, wie sie wollen, indem Sie die Umschalttaste oder Steuerung drücken. Wenn Sie den **Alle Entfernen**-Button klicken, werden alle Einträge aus der Liste gelöscht. Beachten Sie, dass eine Wiederherstellung nicht möglich ist.

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

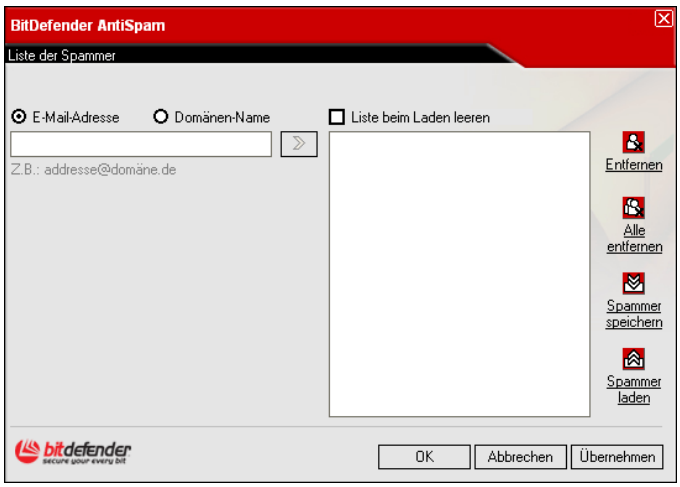
Anmerkung

Wir empfehlen, dass Sie Ihre Freundesnamen Ihrer Freundesliste hinzufügen. Somit stellen Sie sicher, dass nur legitime Nachrichten an Sie weitergeleitet werden.

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

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

Um die Spammer-Liste zu bearbeiten, klicken Sie auf >>> (übereinstimmend mit Ihrer Spammer-Liste) oder klicken Sie auf den **Spammer**-Button in der BitDefender-Symbolleiste bei **Outlook** oder **Outlook Express**. Das folgende Fenster öffnet sich:



Hier können Sie die Einträge Ihrer Spammerliste ändern.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die E-Mail-Adressse, tragen Sie sie ein und klicken Sie auf den »-Button.

Die Adresse wird Ihrer Spammerliste hinzugefügt.

Darstellung 42

Die Adresse muss so aussehen: `name@domain.com`

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

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

Anmerkung

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

Um ein Objekt zu löschen, klicken Sie auf den **Entfernen**-Button. Sie können so viele Objekte markieren, wie Sie möchten, indem Sie die Umschalttaste oder Steuerung drücken. Wenn Sie den **Alle Entfernen**-Button klicken, werden alle Einträge aus der Liste gelöscht. Beachten Sie, dass eine Wiederherstellung nicht möglich ist.

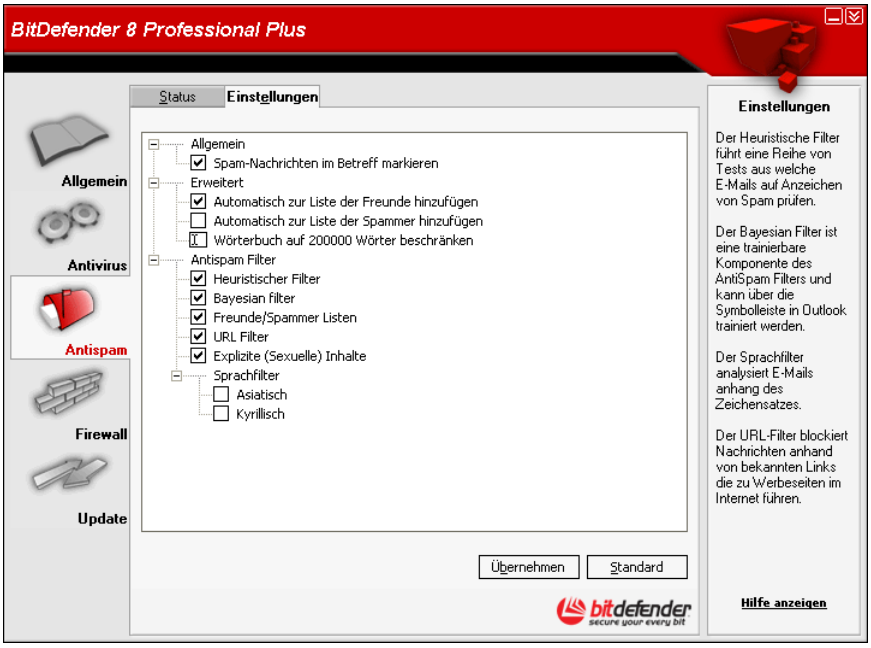
Benutzen Sie die **Spam speichern**/**Spam laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung `.bwl` haben.

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

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

Einstellung weiterer Optionen

Klicken Sie auf den Reiter **Einstellungen**, um diese einzusehen und um die erweiterten Einstellungen von Antispam zu bearbeiten.



Darstellung 43

Drei Kategorien von Einstellungen sind möglich (**Allgemein, Erweitert** und **Antispam Filter**).

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

1. Allgemein

➔ **Spam-Nachrichten im Betreff markieren** - wenn Sie diese Option auswählen, werden alle als Spam eingestuften Mails im Betreff als Spam markiert.

2. Erweitert

➔ **Automatisch zur Liste der Freunde hinzufügen** – wenn Sie diese Option gewählt haben, wird beim nächsten Klick auf den **Kein Spam**-Button in der BitDefender-Symbolleiste der Sender automatisch zu **Kein Spam** hinzugefügt.

➔ **Automatisch zur Liste der Spammer hinzufügen** – wenn Sie diese Option gewählt haben, wird beim nächsten Klick auf den **Ist Spam**-Button in der BitDefender-Symbolleiste der Sender automatisch zu **Ist Spam** hinzugefügt.

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

- **Wörterbuch auf 200.000 Wörter beschränken** – mit dieser Option können Sie die Größe des Bayesianischen Verzeichnisses begrenzen – kleiner ist schneller, größer ist akkurater. Die empfohlene Größe sind 200.000 Wörter.

3. Antispam Filter

- **Heuristischer Filter** – deaktiviert den Heuristischen Filter.
- **Bayesianischer Filter** – deaktiviert den Bayesianischen Filter.
- **Freundes / Spammer Listen** – deaktiviert die Freundes-/Spammerliste.
- **URL Filter** – deaktiviert den URL-Filter.
- **Explizite (Sexuelle) Inhalte** – deaktiviert den Filter für eindeutige Inhalte.
- **Sprachfilter** – Sie können Nachrichten blockieren, die in Kyrillisch und/oder Asiatisch geschrieben worden sind.

Um die Filter zu deaktivieren, entfernen Sie das Häkchen in den Boxen, indem Sie es anklicken ☑. Wenn der Filter deaktiviert ist, sieht die Box so aus: ☐

Konfigurieren von BitDefender-Antispam für Microsoft Outlook/Outlook Express

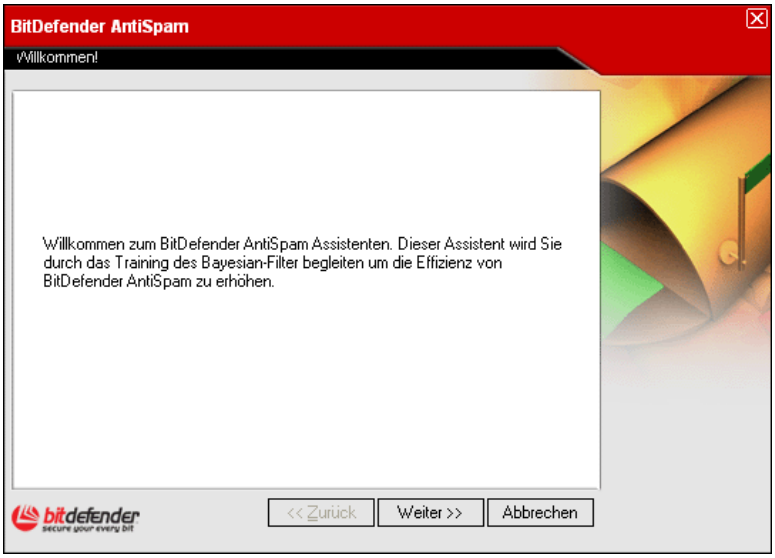
Nachdem der Installationsprozess abgeschlossen ist und Sie zum erstenmal Microsoft Outlook öffnen, erscheint ein Assistent, der Ihnen hilft, die Freundesliste zu konfigurieren und den Bayesianischen Filter zu trainieren.

Wenn Sie im Moment nicht konfigurieren möchten, können Sie das jederzeit nachholen, indem Sie den **Assistenten** anklicken.

Konfigurations-Assistent

Dieser Assistent wird Sie während des Trainings für den Bayesianischen Filter begleiten, so dass die Effizienz des Antispam-Moduls bereits früh gegeben ist. Sie können auch Adressen aus Ihrem Adressbuch Ihrer Freundes-/Spammerliste hinzufügen.

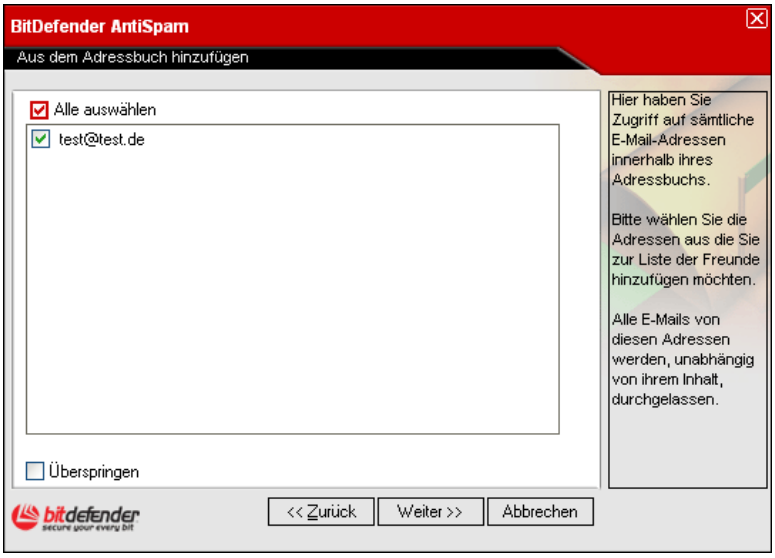
1. Willkommensfenster



Darstellung 44

Klicken Sie auf **Weiter**, um fortzufahren, oder auf **Abbrechen**, um den Assistenten zu beenden.

2. Hinzufügen von E-Mail-Adressen aus Ihrem Adressbuch



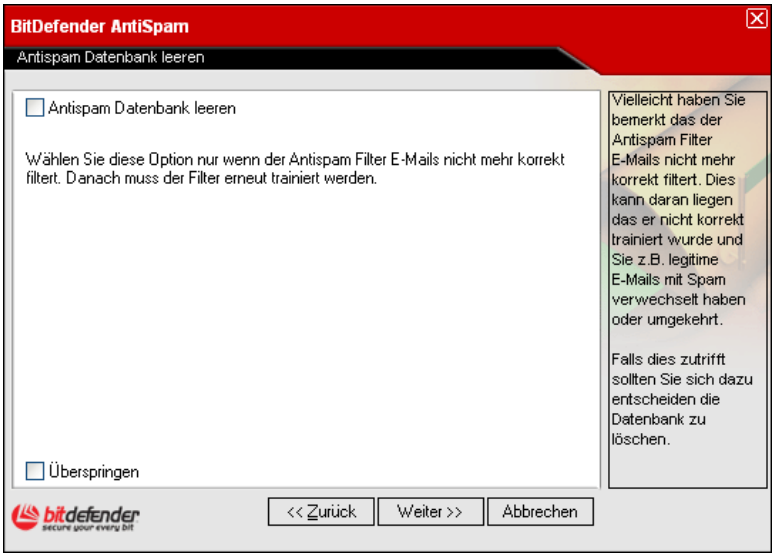
Darstellung 45

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

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht ausführen wollen.

Klicken Sie auf **Weiter**.

3. Bayesianische Daten löschen



Darstellung 46

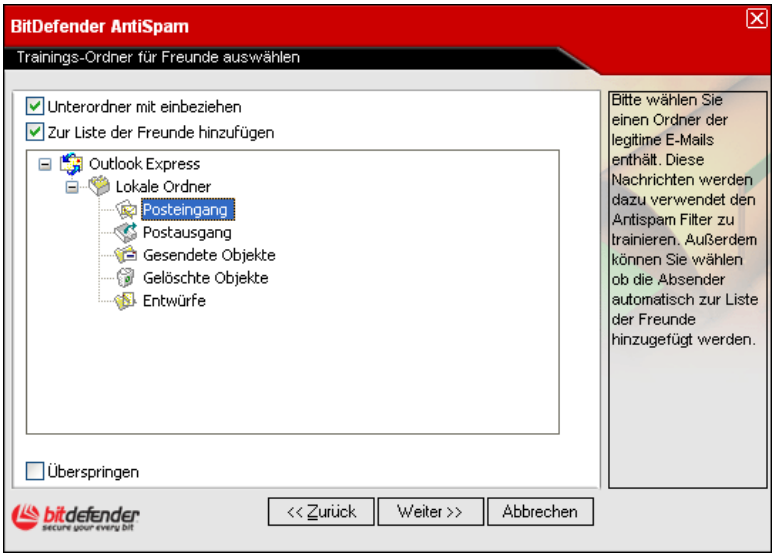
Sie finden heraus, dass Ihr Antispam-Filter an Effektivität verloren hat. Dies kann daher kommen, dass das Training nicht genau durchgeführt worden ist (z. B. haben Sie versehentlich eine Anzahl legitimer Mails als Spam markiert oder umgekehrt). Falls Ihr Filter sehr ungenau arbeitet, müssen Sie Ihre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

Wählen Sie **Antispam Datenbank Leeren**, wenn Sie die Bayesianische Datenbank neu starten wollen.

Wählen Sie **Überspringen**, wenn Sie diesen Schritt nicht durchführen möchten.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren.

4. Trainieren des Bayesianischen Filters mit legitimen E-Mails



Darstellung 47

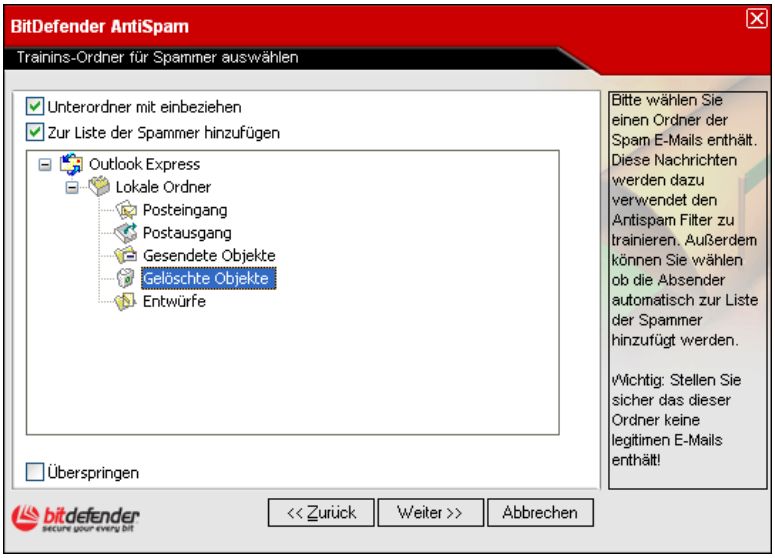
Bitte wählen Sie einen Ordner, der legitime E-Mails enthält. Diese Nachrichten werden genutzt, um den Antispam-Filter zu trainieren.

Im obigen Fenster sind zwei Optionen wählbar:

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

Sie können sich auch dazu entscheiden, diesen Schritt zu überspringen, indem Sie auf **Überspringen** klicken. Klicken Sie dann auf **Weiter**.

5. Trainieren des Bayesianischen Filters mit Spam-Mails



Darstellung 48

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

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

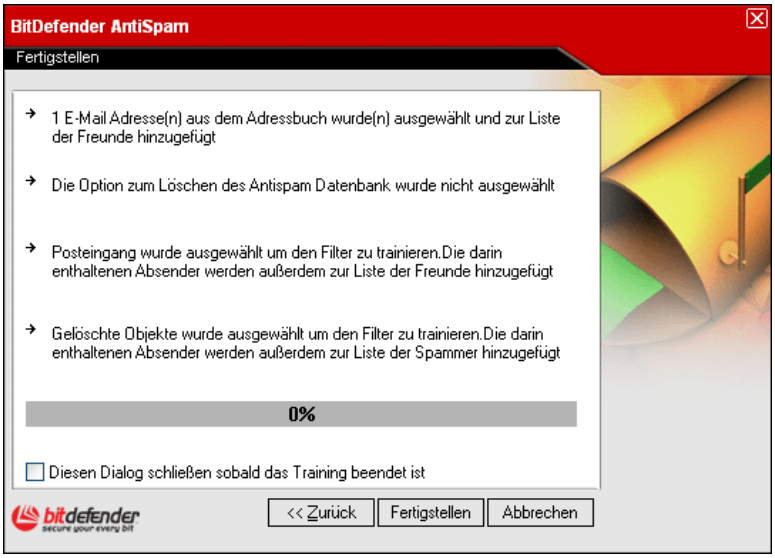
Im obigen Fenster sind zwei Optionen wählbar:

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

Sie können sich auch dazu entscheiden, diesen Schritt zu überspringen, indem Sie auf **Überspringen** klicken.

Klicken Sie dann auf **Weiter**.

6. Zusammenfassung



Darstellung 49

In diesem Fenster können Sie alle Einstellungen einsehen, die mit dem Konfigurations-assistenten durchgeführt worden sind. Sie können noch Änderungen vornehmen, indem Sie zum vorherigen Fenster zurückkehren.

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

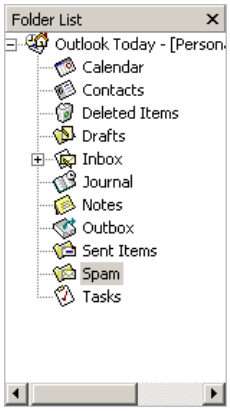
BitDefender-Symbolleiste

Auf der Oberseite von **Microsoft Outlook/Outlook Express** sehen Sie die BitDefender-Symbolleiste, die speziell entwickelt wurde, um Ihnen zu helfen, BitDefender zu konfigurieren.

Darstellung 50

Anmerkung

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



Darstellung 51

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

Jede Schaltfläche wird unten beschrieben:

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

Zukünftige Mails mit diesem Muster werden alle als Spam markiert.

TIPP: Sie können eine oder mehrere E-Mails markieren.

➔ **Not Spam** - **Kein Spam** - Klicken Sie auf diesen Button und das Bayesianische Modul erkennt die ausgewählten Mails nicht als Spam. Sie werden nicht als Spam markiert und in den Posteingang verschoben.

TIPP: Sie können eine oder mehrere E-Mails markieren.

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

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

➔ **Spammer hinzufügen** – Klicken Sie diesen Button, um die ausgewählte Nachricht Ihrer Spammerliste hinzuzufügen. Das folgende Fenster öffnet sich:

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

Darstellung 52

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

TIPP: Sie können einen oder mehrere Absender auswählen.

➔ **Zur Freundesliste hinzufügen** – Klicken Sie auf diesen Button, um den Absender dieser Mail Ihrer Freundesliste hinzuzufügen. Das folgende Fenster öffnet sich:

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

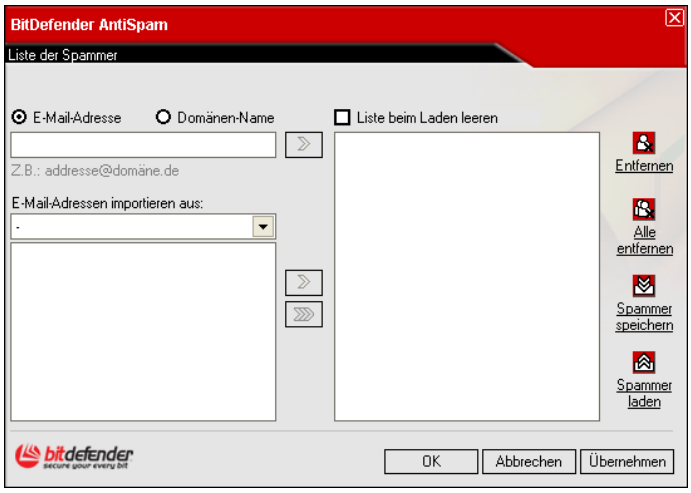
Darstellung 53

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

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

TIPP: Sie können einen oder mehrere Absender auswählen.

➔ **Spammer** – Klicken Sie auf diesen Button, um die Spammerliste zu öffnen. Sie enthält alle E-Mail-Adressen, von denen Sie keine Nachricht erhalten wollen, gleich welchen Inhalts. Ein Fenster, ähnlich der Management-Konsole, öffnet sich:



Hier können Sie Ihrer Spammerliste Einträge hinzufügen oder entfernen.

Falls Sie eine E-Mail-Adresse hinzufügen möchten, kontrollieren Sie die **E-Mail-Adressse**, tragen Sie sie ein und klicken Sie auf den -Button.

Die Adresse wird Ihrer Spammerliste hinzugefügt.

Darstellung 54

Die Adresse muss so aussehen: `name@domain.com`

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

Die Domäne wird Ihrer Spammerliste hinzugefügt:

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

Wenn Sie E-Mail-Adressen aus dem Adressbuch oder aus einem Ordner importieren möchten, klicken Sie den -Button an und wählen Sie **Windows Adressbuch** oder **Outlook Express Ordner** aus. Bei **Oulook Express Ordner** öffnet sich ein neues Fenster:

Wählen Sie den Ordner aus, der die E-Mail-Adressen enthält, die Sie in die Spammerliste aufnehmen möchten. Klicken Sie **Auswählen** an.

Darstellung 55

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

Anmerkung

Jede Mail von einer Adresse Ihrer Spammerliste wird automatisch in Ihren Papierkorb verschoben, ohne weitere Bearbeitung.

Um ein Objekt zu löschen, klicken Sie auf den **Entfernen**-Button. Sie können so viele Objekte markieren, wie Sie möchten, indem Sie die Umschalttaste oder Steuerung drücken. Wenn Sie den **Alle Entfernen**-Button anklicken, werden alle Einträge aus der Liste gelöscht. Beachten Sie, dass eine Wiederherstellung nicht möglich ist.

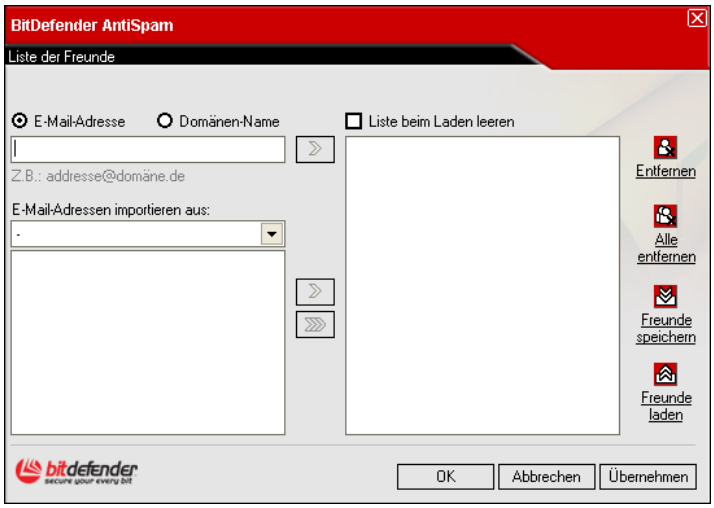
Benutzen Sie die **Spam speichern**-/**Spam laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung `.bwl` haben.

Wählen Sie das entsprechende Kontrollkästchen für **Wenn Laden, derzeitige Liste leeren**, wenn Sie die Spammerliste während des Ladens einer neuen Liste löschen möchten.

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

Nachdem Sie die **Spams** bearbeiten haben, klicken Sie auf **Übernehmen** und **OK**, um zu Outlook zurückzukehren.

➔ **Friends** - **Freunde** - Klicken Sie auf diesen Button, um die Freundesliste zu öffnen. Sie enthält alle E-Mail-Adressen, von denen Sie Nachrichten erhalten wollen, gleich welchen Inhalts. Ein Fenster, ähnlich der Management-Konsole, öffnet sich:



Hier können Sie Ihrer Freundesliste Einträge hinzufügen oder entfernen.

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

Die Adresse wird Ihrer Freundesliste hinzugefügt.

Darstellung 56

Die Adresse muss so aussehen: `name@domain.com`

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

Die Domain wird Ihrer Freundesliste hinzugefügt:

- `@domain.com`, `*domain.com` und `domain.com` – alle eingehenden Mails von `domain.com` werden in Ihren Posteingang verschoben;
- `*domain*` - alle eingehenden Mails von `domain` (egal welcher Endung) werden in Ihren Posteingang verschoben;

- *com – alle Mails mit dieser Endung com werden in Ihren Posteingang verschoben.

Wenn Sie E-Mail-Adressen aus dem Adressbuch oder aus einem Ordner importieren möchten, klicken Sie auf den -Button und wählen Sie **Windows Adressbuch** oder **Outlook Express Ordner** aus. Bei **Outlook Express Ordner** öffnet sich ein neues Fenster:

Darstellung 57

Wählen Sie den Ordner aus, der die E-Mail-Adressen enthält, die Sie der Freundesliste hinzufügen möchten. Klicken Sie auf **Auswählen**.

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

Anmerkung

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

Um ein Objekt zu löschen, klicken Sie auf den **Entfernen**-Button. Sie können so viele Objekte markieren, wie Sie möchten, indem Sie die Umschalttaste oder Steuerung drücken. Wenn Sie den **Alle Entfernen**-Button klicken, werden alle Einträge aus der Liste gelöscht. Beachten Sie, dass eine Wiederherstellung nicht möglich ist.

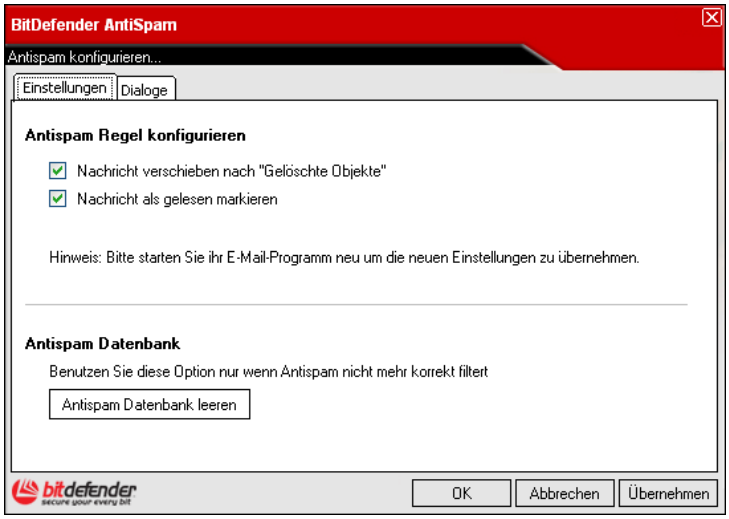
Benutzen Sie die **Freunde speichern**-/**Freunde laden**-Buttons, um zu speichern oder um zu laden. Die Datei wird die Endung .bwl haben.

Wählen Sie das entsprechende Kontrollkästchen für **Wenn Laden, derzeitige Liste leeren**, wenn Sie die Freundesliste während des Ladens einer neuen Liste löschen möchten.

Nachdem Sie die **Freundesliste** bearbeiten haben, klicken Sie auf **Übernehmen** und **OK**, um zu Outlook zurückzukehren.

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

➔ **Einstellungen** – klicken Sie auf diesen Button, um das Einstellungspanel zu öffnen.



Darstellung 58

Die folgenden Optionen sind wählbar:

- **Nachricht verschieben nach „Gelöschte Objekte“** – um die Spam-Mails zu löschen.
- **Nachricht als gelesen markieren** – um die Spam-Mails in den Papierkorb zu verschieben (nur für Microsoft Outlook Express).

Wenn Ihr Antispam-Filter ungenau arbeitet, sollten Sie die Filter-Datenbank löschen und den Bayesianischen Filter neu trainieren. Klicken Sie auf **Antispam Datenbank löschen**, um danach die Bayesianische Datenbank neu aufzubauen.

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

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

➔ **BitDefender-Antispam** - klicken Sie auf diesen Button, um die Management-Konsole zu öffnen.

Anmerkung

Wenn Sie die BitDefender-Symbolleiste nicht mehr sehen wollen, klicken Sie mit der rechten Maustaste die Microsoft Outlook-Symbolleiste an und wählen Sie die BitDefender-AntiSpam-Option ab.

Firewall-Modul

Die **Firewall** schützt Ihren Computer vor unberechtigten Zugriffen aus dem Internet.

Eigenschaften

Sie überwacht Ihre Internetverbindung und lässt Sie Regeln definieren, welche Verbindung erlaubt ist und welche geblockt werden soll.

Eine Firewall ist unabdingbar, wenn Sie eine permanente Verbindung zum Internet via Kabel oder DSL haben. Sie kann effektiv Trojaner oder Angriffe durch Hacker abwehren.

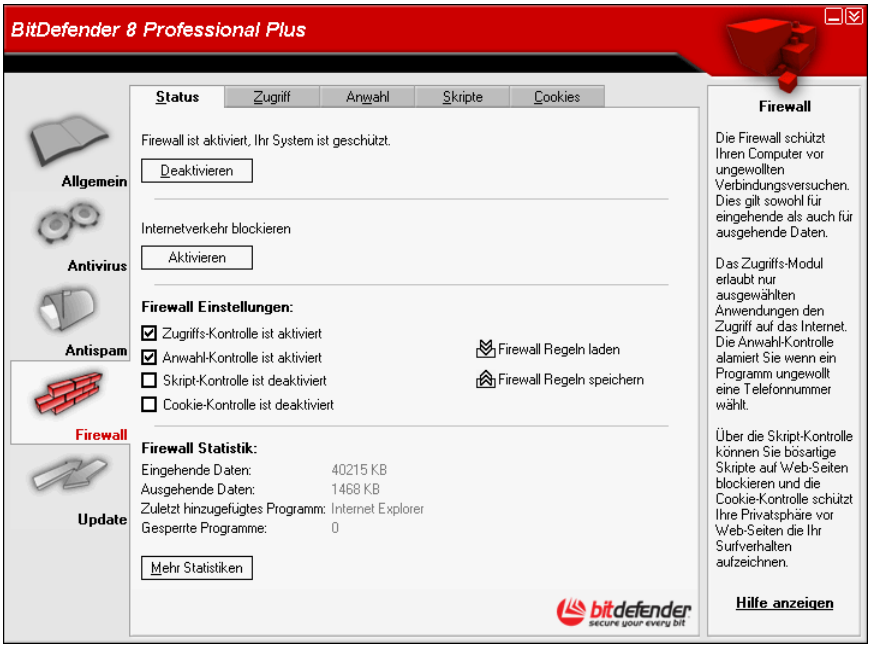
Die BitDefender-Firewall besteht aus vier Teilen:

- **Zugriff** ist der wichtigste Bestandteil. Er überwacht Programme, die Zugriff auf das Internet haben möchten, und ist äußerst wichtig hinsichtlich der Blockade von Trojanern.
- **Anwahl** warnt Sie, falls ein Programm versucht eine andere Telefonnummer anzuwählen.
- **Skripte** verhindert die Ausführung von Skripten aus unsicheren, nicht verlässlichen Quellen.
- **Cookies** filtert die ein- und ausgehenden Cookies und verschleiert damit Ihre Identität und Ihr Surfverhalten.

Detaillierte Erklärungen dieser Firewall-Bestandteile finden Sie weiter unten.

Überblick

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender-Symbol. Klicken Sie in der Management-Konsole auf **Firewall**.



Darstellung 59

Klicken Sie auf **Deaktivieren**, falls Sie den Firewall-Schutz deaktivieren wollen, oder klicken Sie auf **Aktivieren**, um den Internet-Verkehr zu blockieren.

TIPP: Falls Sie nicht die einzige Person sein sollten, die Ihren Computer benutzt, wird Ihnen empfohlen, Ihre BitDefender-Einstellungen mit einem Passwort zu sichern. Um den **Kennwortschutz** zu nutzen, gehen Sie auf **Allgemein**, öffnen Sie die Einstellungen und wählen Sie **Konsole per Kennwort schützen**.

In der Sektion **Firewall-Einstellungen** können Sie die Schutzoptionen, die Ihnen das Firewall-Modul bietet (**Zugriffs-Kontrolle**, **Anwahl-Kontrolle**, **Skript-Kontrolle**, **Cookie-Kontrolle**) aktivieren oder deaktivieren. Ein Schutz besteht nur dann, wenn die entsprechende Option ausgewählt ist.

Benutzen Sie **Firewall Regeln Speichern**-/**Firewall Regeln laden**-Buttons, wenn Sie die Regeln an einer bestimmte Stelle speichern bzw. von einer bestimmten Stelle laden möchten.

TIPP: Wenn Sie BitDefender erneut installieren möchten, empfiehlt es sich, diese Regeln vorher zu sichern und sie nach dem Neuinstallieren wieder zu importieren.

Auf der unteren Seite der Sektion können Sie die BitDefender-Statistiken über den Internet-Verkehr und hinzugefügte Programme sehen. Klicken Sie **Mehr Statistiken** an, wenn Sie ein Fenster mit mehr Informationen über diese Statistiken sehen möchten.

Zugriffs-Kontrolle

Die **Zugriffs-Kontrolle** ist der wichtigste Teil Ihrer Firewall. Sie überwacht, welche Programme versuchen, sich mit dem Internet zu verbinden. Dies ist besonders wichtig, um Trojaner zu blockieren.

Ist die **Zugriffs-Kontrolle** aktiviert, wird BitDefender jedes Mal Ihre diesbezügliche Freigabe abfragen, falls ein neues Programm Informationen senden oder aus dem Internet empfangen will:

Darstellung 60

Sie erhalten die folgenden Informationen: Den Namen der Anwendung, die Zugriff auf das Internet haben will, die IP-Adresse und den Port, den die Anwendung ansteuert.

Markieren Sie **Diese Antwort merken**, wählen sie **Ja** oder **Nein** und eine Regel wird erstellt und in Ihrer Regelliste vermerkt.

Bei einer Wiederholung des gleichen Zugriffes werden Sie dann nicht mehr informiert.

TIPP: Wann immer BitDefender ein legitimes Programm erkennt, das versucht, Zugriff auf das Internet aufzubauen, sollten Sie ihm die Verbindung erlauben.

Lassen Sie nur Verbindungen zu IP-Adressen oder Domains zu, die Sie kennen.

Klicken Sie auf **Zugriff** im **Firewall**-Menü, um die Regelliste der Zugriffs-Kontrolle aufzurufen. Das folgende Fenster erscheint:

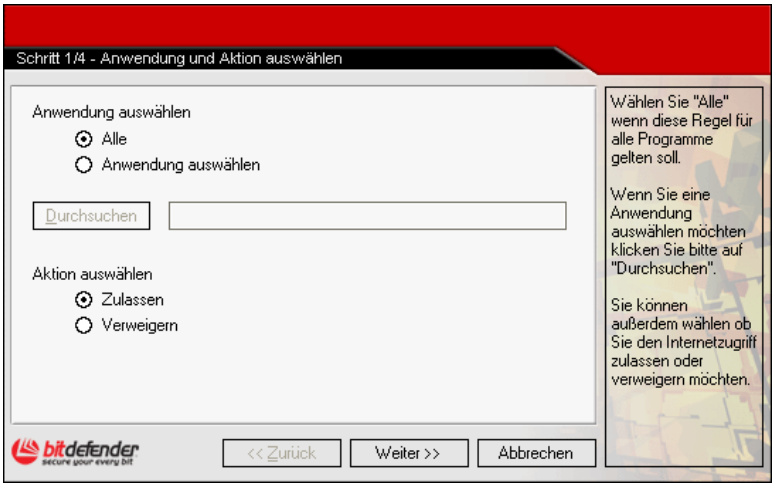
Darstellung 61

Regeln werden in diese Liste aufgenommen, sobald Sie die Frage von BitDefender hinsichtlich des Zugriffs eines neuen Programms auf das Internet beantwortet haben.

Die Priorität der Regeln ist von unten nach oben aufsteigend. Das bedeutet, die zuletzt erstellte Regel hat die höchste Priorität.

Regeln können automatisch (durch ein Warnfenster) oder manuell (klicken Sie auf **Neue Regel** und wählen Sie die Parameter für diese Regel) erstellt werden. Der erste Schritt des Konfigurationsassistenten erscheint:

Anwendung und Aktion auswählen



Darstellung 62

Sie können die folgenden Parameter wählen:

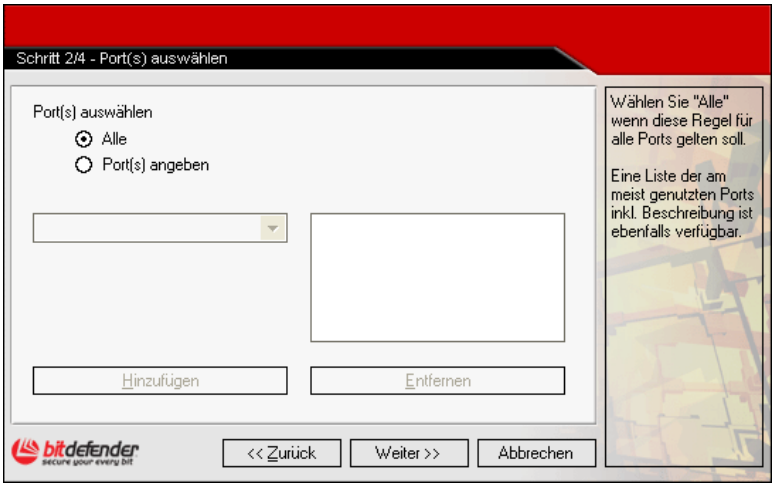
- **Anwendung** – wählen Sie die Anwendung für die Regel. Sie können eine bestimmte Anwendung wählen (klicken Sie **Anwendung auswählen**, **Durchsuchen** und wählen Sie eine bestimmte Anwendung) oder alle Anwendungen (markieren Sie **Alle**).

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

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

Klicken Sie auf **Weiter**, um fortzufahren.

Port(s) auswählen



Darstellung 63

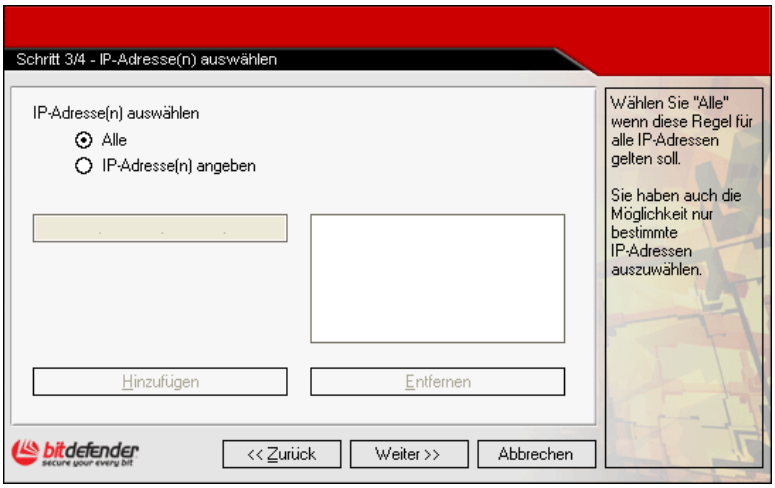
Eine Liste mit den gebräuchlichsten Ports und einer kurzen Beschreibung ist vorhanden, um Sie bei der Wahl von spezifischen Ports zu unterstützen.

➔ **Port(s) auswählen** – Markieren Sie **Port(s) angeben** und wählen Sie die Ports, auf die die Regel angewendet werden soll. Klicken Sie auf **Hinzufügen**.

Wenn Sie in der Auswahl **Alle** markieren, werden alle Ports ausgewählt. Falls Sie einen Port löschen möchten, wählen Sie **Entfernen**.

Klicken Sie auf **Weiter**, um fortzufahren.

IP-Adresse(n) auswählen



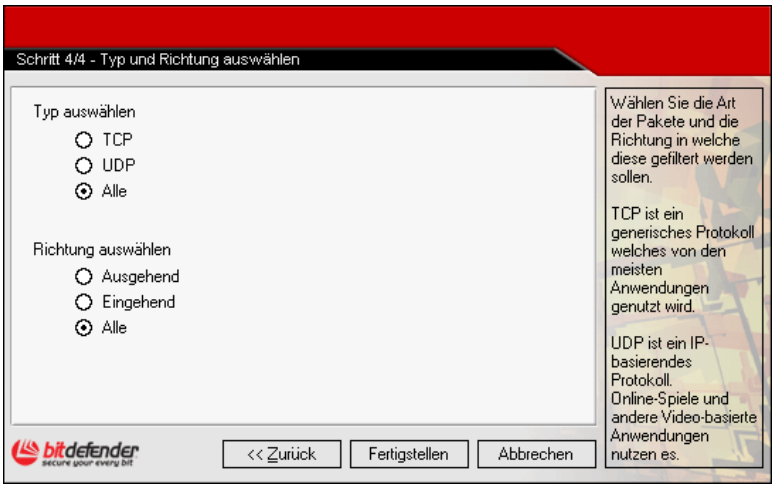
Darstellung 64

➔ **IP-Adresse(n) auswählen** – wählen Sie **IP-Adresse(n)** angeben und geben Sie die gewünschte IP-Adresse, auf die die Regel angewendet werden soll, im darunterliegenden Feld ein. Klicken Sie auf **Hinzufügen**.

Wenn Sie in der Auswahl **Alle** markieren, werden alle IP-Adressen ausgewählt. Um IP-Adressen zu löschen, wählen Sie diese aus und klicken Sie auf **Entfernen**.

Klicken Sie auf **Weiter**, um fortzufahren.

Typ und Richtung auswählen



Darstellung 65

Setzten Sie die Parameter:

➔ **Protokolltyp** – wählen Sie die Protokolle TCP, UDP oder beide aus.

Typ	Beschreibung
TCP	Transmission Control Protocol - TCP ermöglicht zwei Rechnern eine Verbindung herzustellen und Daten auszutauschen. TCP sichert die Datenübermittlung, wobei die Pakete in der gleichen Reihenfolge, in der sie abgeschickt wurden, übermittelt werden.
UDP	User Datagram Protocol - UDP ist eine IP-basierende Datenübermittlung, die für Verbindungen mit hohem Datenvolumen entworfen wurde. Spiele und andere video-basierende Anwendungen benutzen UDP.
TCP/UDP	Transmission Control Protocol und User Datagram Protocol.

➔ **Richtung** - wählt die Richtung des Datenverkehrs aus.

Richtung	Beschreibung
Ausgehend	Die Regel wird nur auf die ausgehenden Daten angewandt.
Eingehend	Die Regel wird nur auf die eingehenden Daten angewandt.
Alle	Die Regel wird in beide Richtungen angewandt.

Klicken Sie auf **Fertigstellen**.

Jede erstellte Regel kann später über die **Zugriffs-**Funktion aufgerufen und weiter bearbeitet werden.

Um eine Regel zeitweise zu deaktivieren, ohne sie zu löschen, entfernen Sie die Markierung aus dem nebenstehenden Kästchen ☑ durch Anklicken. Ein leeres Kästchen ☐ zeigt, dass die Regel deaktiviert ist.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Entfernen**. Um eine Regel anzupassen, doppelklicken Sie auf diese.

TIPP: Vergessen Sie nicht, **Fertigstellen** zu wählen, nachdem Sie eine Regel geändert haben.

Anwahl-Kontrolle

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

Mit der **Anwahl**-Kontrolle entscheiden Sie, welche Verbindung mit welcher Telefonnummer Sie zulassen oder unterbinden wollen.

Die Anwahl-Kontrolle überwacht alle Dialer, die auf ein Computer-Modem zugreifen wollen, warnt den Benutzer unmittelbar und verlangt die Ablehnung oder Zustimmung zu solch einer Operation:

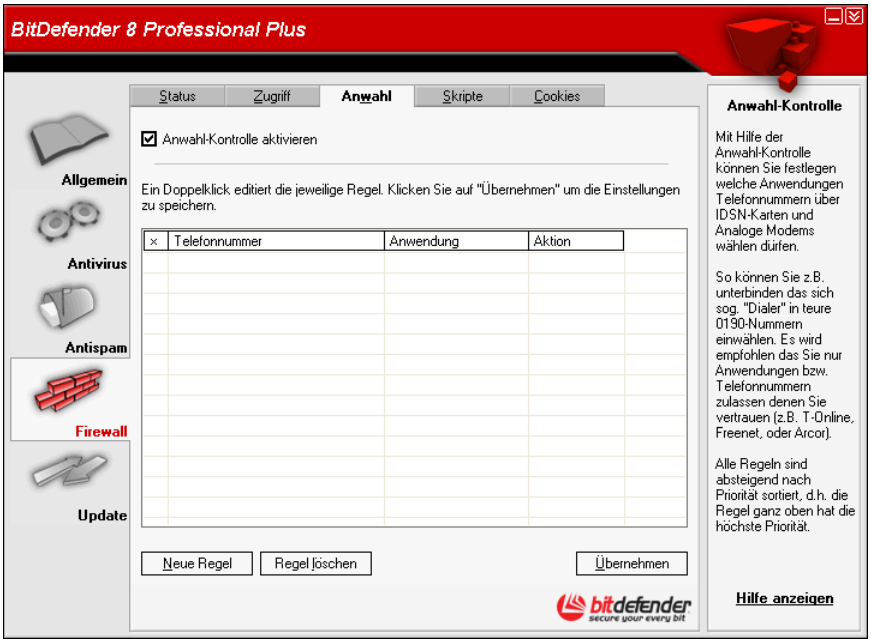
Darstellung 66

Sie sehen den Namen der Anwendung und die vorgesehene Telefonnummer.

Wählen Sie **Diese Antwort merken**, klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in die Regelliste aufgenommen.

Bei einer Wiederholung dieser Anwahl werden Sie nicht mehr informiert.

Klicken Sie auf den **Anwahl**-Reiter unter **Firewall**, um zur Regelliste der Anwahl-Kontrolle zu gelangen. Das folgende Bild erscheint:

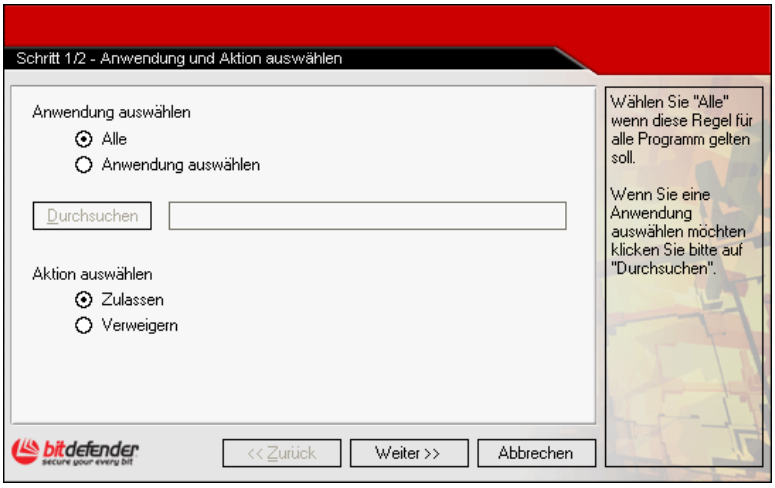


Darstellung 67

Die Priorität der Regeln ist von unten nach oben aufsteigend. Das bedeutet, die zuletzt erstellte Regel hat die höchste Priorität.

Die Regeln können automatisch hinzugefügt werden (durch ein Warnfenster) oder manuell (klicken Sie auf **Neue Regel** und wählen Sie die Parameter für diese Regel).
Der Konfigurationsassistent wird gestartet:

Anwendung und Aktion auswählen



Darstellung 68

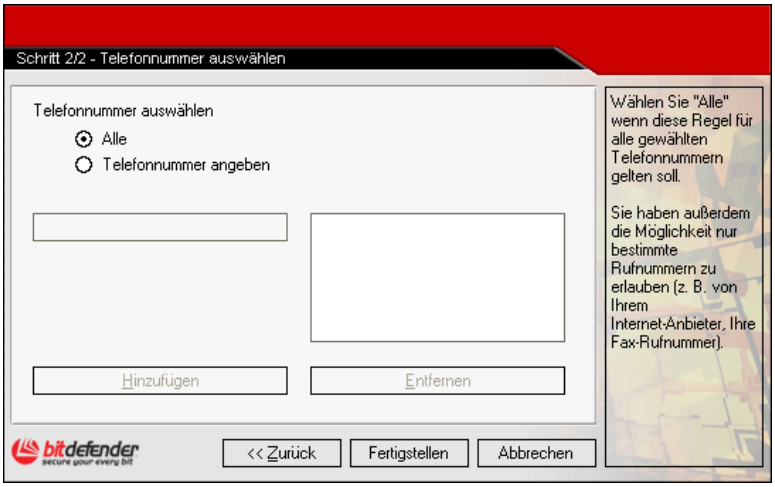
Sie können die folgenden Parameter wählen:

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

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

Klicken Sie auf **Weiter**.

Telefonnummer auswählen



Darstellung 69

Sie können die folgenden Parameter wählen:

➔ **Telefonnummer auswählen** – Markieren Sie **Telefonnummer angeben** und geben Sie die Telefonnummer, für die die Regel erstellt werden soll, in das darunterliegende Feld ein. Klicken Sie auf **Hinzufügen**.

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

Anmerkung

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

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

Wählen Sie **Fertigstellen**.

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

Um eine Regel zeitweise zu deaktivieren, ohne sie zu löschen, entfernen Sie die Markierung aus dem nebenstehenden Kästchen ☑ durch Anklicken. Ein leeres Kästchen ☐ zeigt, dass die Regel deaktiviert ist.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Entfernen**. Um eine Regel anzupassen, doppelklicken Sie auf diese.

TIPP: Vergessen Sie nicht, **Fertigstellen** zu wählen, nachdem Sie eine Regel geändert haben.

Skript-Kontrolle

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

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:

Darstellung 70

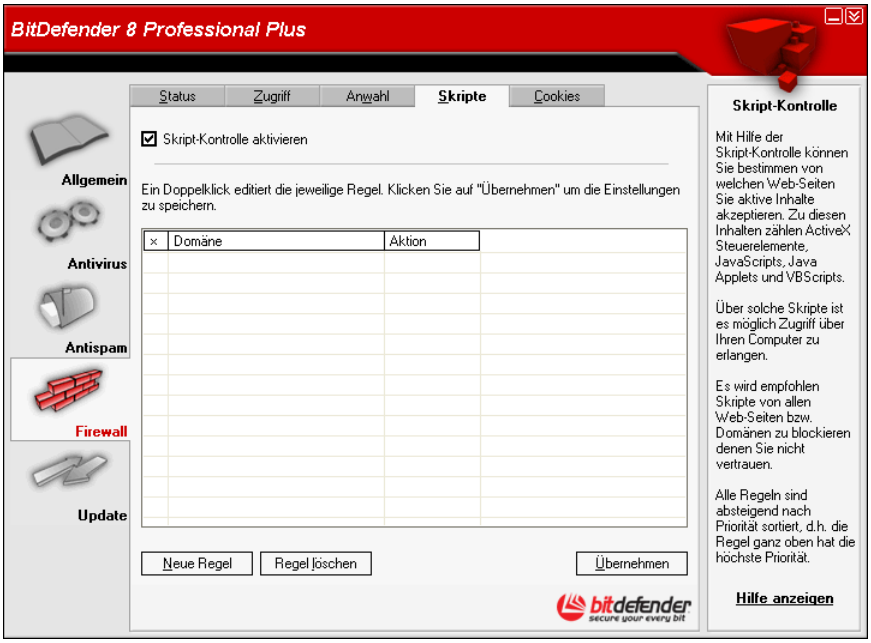
Der Namen der Quelle wird Ihnen angezeigt.

Wählen Sie **Diese Antwort merken**, klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in die Regelliste aufgenommen.

Falls die gleiche Seite erneut Ihren aktiven Inhalt versenden will, werden Sie nicht wieder informiert.

TIPP: Bösartige Skripts können Ihr System gefährden. Deswegen wird empfohlen, dass Sie die Skripts von allen Bereichen blockieren, denen Sie nicht vertrauen.

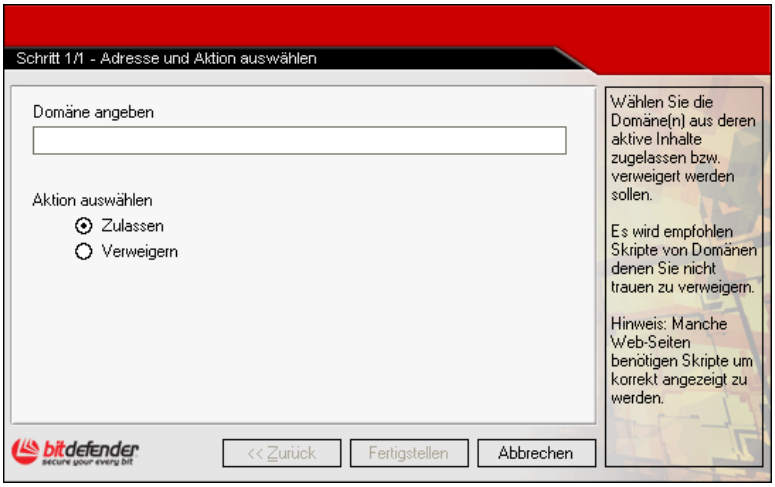
Wählen Sie den Reiter **Skripte** in Ihrem **Firewall**-Menü, um die Regellisten der **Skript-Kontrolle** anzuzeigen. Das folgende Fenster erscheint:



Darstellung 71

Die Priorität der Regeln ist von unten nach oben aufsteigend. Das bedeutet, die zuletzt erstellte Regel hat die höchste Priorität.

Regeln können automatisch (durch ein Warnfenster) oder manuell (klicken Sie auf **Neue Regel** und wählen Sie die Parameter für diese Regel) erstellt werden. Das folgende Bild erscheint:



Darstellung 72

Sie können folgende Parameter angeben:

- **Domäne angeben** – schreiben Sie die Domäne, auf die die Regel angewendet werden soll, in das darunterstehende Feld.
- **Aktion auswählen** – wählen Sie die Aktion der Regel.

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

Klicken Sie auf **Fertigstellen**.

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

Um eine Regel zeitweise zu deaktivieren, ohne sie zu löschen, entfernen Sie die Markierung aus dem nebenstehenden Kästchen ☑ durch Anklicken. Ein leeres Kästchen ☐ zeigt, dass die Regel deaktiviert ist.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Entfernen**. Um eine Regel anzupassen, doppelklicken Sie auf diese.

TIPP: Vergessen Sie nicht, **Fertigstellen** zu wählen, nachdem Sie eine Regel geändert haben.

Cookie-Kontrolle

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

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

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

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

Darstellung 73

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

Wählen Sie **Diese Antwort merken**, klicken Sie auf **Ja** oder **Nein** und eine Regel wird erstellt, angewendet und in die Regelliste aufgenommen.

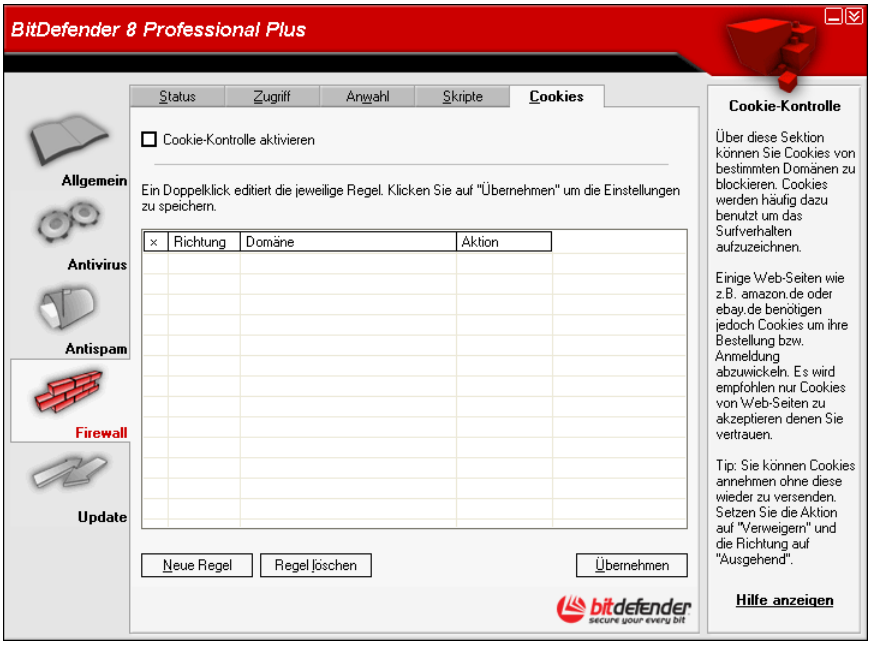
Sie werden dann nicht wieder informiert, wenn Sie das nächste Mal mit derselben Seite in Verbindung treten.

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

Die Anzahl der Abfragen wird sich reduzieren!

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.

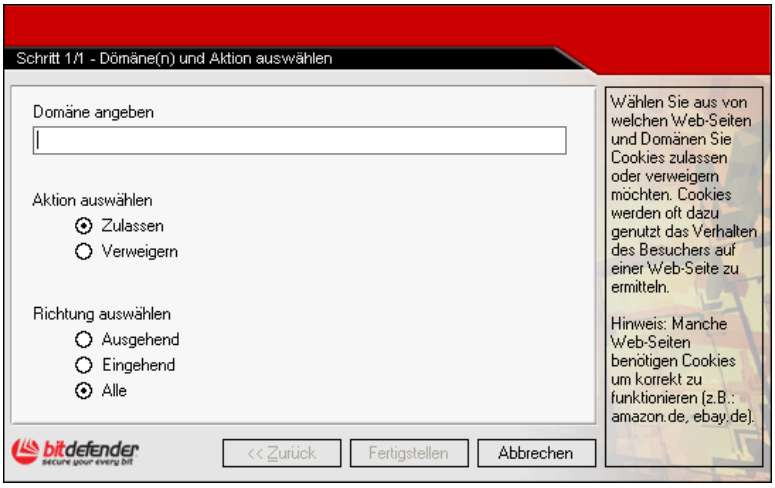
Wählen Sie den Reiter **Cookies** in Ihrem **Firewall**-Menü, um die Regellisten der **Cookie-Kontrolle** anzuzeigen. Das folgende Fenster erscheint:



Darstellung 74

Die Priorität der Regeln ist von unten nach oben aufsteigend. Das bedeutet, die zuletzt erstellte Regel hat die höchste Priorität.

Regeln können automatisch (durch ein Warnfenster) oder manuell (klicken Sie auf **Neue Regel** und wählen Sie die Parameter für diese Regel) erstellt werden. Das folgende Bild erscheint:



Darstellung 75

Sie können die folgenden Parameter angeben:

- **Domäne angeben** – schreiben Sie die Domäne, auf die die Regel angewendet werden soll, in das darunterliegende Feld.
- **Aktion auswählen** – wählen Sie die Aktion der Regel.

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

- **Richtung auswählen** – wählen Sie die Richtung der Verbindung.

Aktion	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf Cookies, die von der verbundenen Seite versendet werden
Eingehend	Die Regel bezieht sich nur auf Cookies, die an die verbundene Seite versendet werden.
Alle	Die Regel wird in beiden Fällen angewandt.

Klicken Sie auf **Fertigstellen**.

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

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

Um eine Regel zeitweise zu deaktivieren, ohne sie zu löschen, entfernen Sie die Markierung aus dem nebenstehenden Kästchen ☑ durch Anklicken. Ein leeres Kästchen ☐ zeigt, dass die Regel deaktiviert ist.

Um eine Regel zu löschen, wählen Sie diese aus und klicken Sie auf **Entfernen**. Um eine Regel anzupassen, doppelklicken Sie auf diese.

TIPP: Vergessen Sie nicht, **Fertigstellen** zu wählen, nachdem Sie eine Regel geändert haben.

Update-Modul

Da ständig neue Viren in relativ kurzen Abständen auftreten, ist es sehr wichtig, dass Sie Ihr Antiviren-Produkt täglich aktualisieren.

Eigenschaften

Es gibt zwei Arten von Updates:

- **Antispam-Update** – Um den Spamschutz zu verbessern, werden neue Regeln zur Heuristik und zum URL-Filter hinzugefügt. Diesen Vorgang nennt man **Antispam-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, wird das **Produkt-Update** genannt;
- **Antiviren-Schutz** – Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virus-Definitions-Update**.

Dem Anwender stehen zur Aktualisierung zwei Möglichkeiten zur Verfügung:

- **Manuelles Update** – Der Benutzer entscheidet, wann BitDefender nach einem Update sucht.
- **Automatisches Update** – BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind.

Wenn Sie über Kabel, Netzwerk oder DSL ständig mit dem Internet verbunden sind, sucht BitDefender nach dem Einschalten des Computers und dann in der Standardeinstellung alle 3 Stunden nach verfügbaren Updates.

TIPP: Wenn Sie mit einer Wählverbindung (Modem oder ISDN) mit dem Internet verbunden sind, empfiehlt es sich, das BitDefender-Update manuell durchzuführen.

Manuelles Update

Um Zugriff auf die Management-Konsole zu erhalten, folgen Sie dem Windows-Startmenü **Start → Programme → BitDefender 8 → BitDefender 8 Professional** oder schneller: Doppelklick auf das BitDefender Symbol.

Klicken Sie in der Management-Konsole auf **Update**.

Darstellung 76

Das manuelle Update kann jederzeit durchgeführt werden, auch wenn das Produkt vorher auf automatisches Update festgelegt wurde. Um ein manuelles Produktupdate durchzuführen, unternehmen Sie folgende Schritte:

- Klicken Sie auf **Prüfen**. Update verbindet sich sofort mit dem BitDefender-Update-Server und prüft, ob ein Update existiert.
- Wenn ein Update gefunden wird, werden sein Name und seine Größe angezeigt. Klicken Sie auf **Update**, um den Aktualisierungsprozess zu starten.

  TIPP: Wenn Sie sehen möchten, welche Dateien aktualisiert wurden, klicken Sie **Details** an.

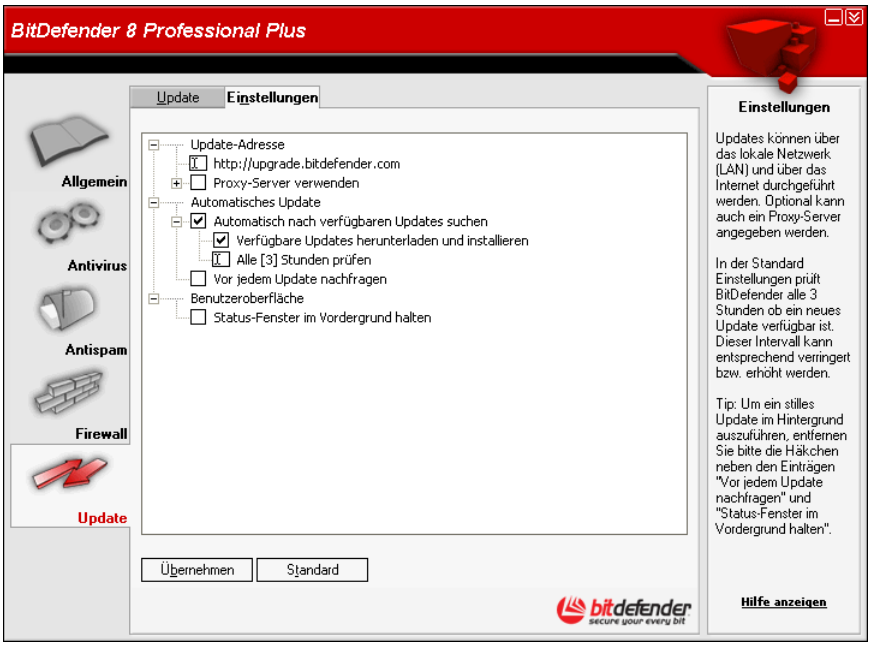
  Wenn es kein Update gibt, werden Sie darauf hingewiesen.

Anmerkung

Manchmal ist es nötig, den Computer neu zu starten, um das Update zu vervollständigen. Wenn ein Systemneustart verlangt wird, sollten Sie ihn so schnell wie möglich durchführen.

Automatisches Update

Wenn Sie ein fortgeschrittener Benutzer sind, klicken Sie auf den Reiter **Einstellungen**, um das Update-Modul zu konfigurieren.



Darstellung 77

Updates können vom lokalen Netz, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden.

Das Fenster mit den Update-Einstellungen enthält drei aufklappbare Optionskategorien, (**Updateadresse**, **Automatisches Update** und **Benutzeroberfläche**), ähnlich wie in den Windowsmenüs.

Klicken Sie auf das Kästchen mit dem "+"-Zeichen, um eine Option zu öffnen, oder auf das "-"-Zeichen, um eine Option zu schließen.

Update-Adresse

➔ Wählen Sie die Update-Adresse und die Proxy-Einstellungen aus, falls Sie einen Proxy verwenden. Die voreingestellte Adresse ist: http://upgrade.bitdefender.com

➔ **Proxy-Einstellungen** – falls Sie einen Proxy-Server einsetzen, muss die entsprechende Markierung gesetzt werden. Nehmen Sie dann folgende Einstellungen vor.

- **Adresse** - Geben Sie die IP-Adresse oder den Namen des Proxy-Servers ein.

  Syntax: `name:port` or `ip:port`.

- **Benutzername** - Geben Sie den Benutzernamen ein, wenn der Proxy-Server eine Anmeldung erfordert.

  Syntax: `domain\user`.

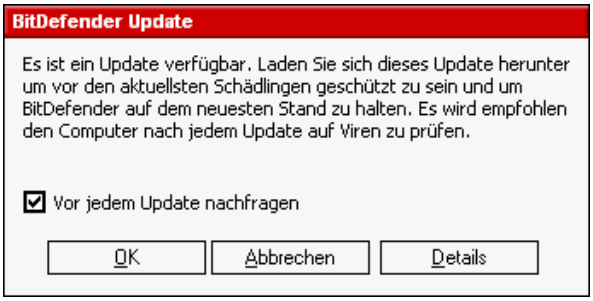
- **Kennwort –** Geben Sie das Kennwort ein, wenn der Proxy-Server eine Anmeldung mit Kennwort erfordert.

Einstellungen für das automatische Update

➔ **Automatisches Update** – BitDefender verbindet sich automatisch mit dem BitDefender-Update-Server und prüft, ob neue Updates vorhanden sind.

- **Verfügbare Updates herunterladen und installieren** – wenn neue Updates verfügbar sind, werden diese automatisch heruntergeladen und installiert.
- **Alle <x> Stunden prüfen** – Definiert, wie oft auf verfügbare Updates geprüft werden soll. Standard ist <3> Stunden.

➔ **Vor jedem Update nachfragen** – Sie werden vor jedem Update gefragt, ob es installiert werden soll.



Klicken Sie auf die **OK-**Schaltfläche, um den Updatevorgang zu starten, oder auf **Abbrechen**, um später ein Update durchzuführen.

Darstellung 78

Wenn Sie auf **Details** klicken, sehen Sie, welche Dateien aktualisiert werden.

Benutzeroberfläche

➔ Standardmäßig wird das Update im Vordergrund durchgeführt, dabei wird ein Fenster mit dem Verlauf des Updates sichtbar angezeigt. Falls das Update im Hintergrund stattfinden soll, erweitern Sie die Optionen der **Benutzeroberfläche** und entfernen Sie die Markierung bei **Downloadfenster immer im Vordergrund halten**.

Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, oder klicken auf **Standard**, um auf die Standardeinstellungen zurücksetzen.

Tipps

Antivirus

So sichern Sie Ihren Computer vor Bedrohungen aus dem Internet:

1. Nachdem der Installations-Prozess abgeschlossen ist, registrieren Sie bitte Ihr Produkt wie im Abschnitt Produkt-Registrierung beschrieben.
2. Führen Sie ein manuelles Update durch. Klicken Sie in der Management-Konsole auf **Update**. Klicken Sie auf den Reiter **Update** und dann auf **Prüfen.**
3. Führen Sie einen vollen Scan Ihres Systems durch (wie beschrieben im Abschnitt Sofortiges Prüfen).
4. In der Sektion Status des **Allgemein**-Moduls aktivieren Sie die wichtigsten Eigenschaften von BitDefender: Virus Schild, Firewall und Automatisches Update.
5. Programmieren Sie BitDefender mittels des Planer-Moduls, die Systemüberprüfung mindestens einmal wöchentlich durchzuführen.

TIPP: Das Planer-Modul erlaubt Ihnen, komplette System-/Laufwerküberprüfungen festzulegen, ohne dass Sie daran denken müssen.

Falls Sie nicht die einzige Person sein sollten, die Ihren Computer benutzt, wird Ihnen empfohlen, Ihre BitDefender-Einstellungen mit einem Kennwort zu sichern (nutzen Sie die Option **Konsole per Kennwort schützen** im Reiter Einstellungen des Allgemein-Moduls).

Antispam

Um mit BitDefender-Antispam Ihr Postfach vor lästigem Spam zu schützen, gehen Sie bitte folgendermaßen vor:

1. Falls Sie **Microsoft Outlook** oder **Microsoft Outlook Express** benutzen, verwenden Sie den Konfigurationsmanager, der sich öffnet, wenn Sie Ihr E-Mail-Konto aufrufen. Sie können ihn ebenfalls über die BitDefender-Antispam-Symbolleiste durch Klicken auf das **Wizard**-Symbol starten.
2. **Fügen Sie die Adressen** von Personen, deren E-Mails Sie immer empfangen wollen, **in die** Freundesliste ein. **BitDefender** wird Nachrichten von Personen dieser Liste nicht blockieren, die Aufnahme von Personen in die Freundesliste gewährleistet also den Erhalt von gewünschten Nachrichten.
3. **Trainieren Sie den Bayesianischen Filter.** Falls Sie E-Mails als Spam einstufen, die BitDefender nicht erkannt hat, wählen Sie diese bitte aus und klicken Sie auf der BitDefender-Antispam-Symbolleiste auf den **Ist Spam**-Button. Weitere E-Mails mit demselben Muster werden dann als Spam erkannt.

Der Bayesianische Filter wird erst aktiv, wenn Sie 60 und mehr E-Mails als „Ist Spam“ markiert haben. Verwenden Sie den Konfigurationsassistenten.

4. **Halten Sie Ihr BitDefender-Programm auf dem aktuellen Stand.** Immer wenn Sie ein Update vornehmen, werden dem Heuristischen Filter neue Regeln und dem URL-Filter neue Links hinzugefügt. Dies hilft Ihnen, die Effektivität Ihres **Antispam-**Systems zu steigern.
5. **Konfigurieren Sie den Sprachfilter.** Viele Spam-Nachrichten sind in kyrillischen oder asiatischen Schriftzeichen geschrieben. Richten Sie diesen Filter ein, wenn Sie alle E-Mails, die in diesen Schriften verfasst sind, ablehnen möchten.

TIPP: In der **Bitdefender-Management-Konsole** können Sie im **Antispam**-Modul, Reiter Einstellungen, jeden Antispam-Filter aktivieren oder deaktivieren.

7

Häufig gestellte Fragen

Allgemein

1. **F:** Wie kann ich überprüfen, ob BitDefender aktiviert ist?
   A: Klicken Sie auf **Allgemein** und dort auf den Reiter Status. Sie sehen, welche Module von BitDefender aktiviert sind und welche nicht.

2. **F:** Welche Anforderungen an das System stellt BitDefender?
   A: Sie können die Systemanforderungen im Abschnitt Systemvoraussetzungen einsehen.

3. **F:** Wie deinstalliere ich BitDefender?
   A: Klicken Sie auf: **Start** → **Programme** → **BitDefender 8** → **Ändern, Reparieren, Deinstallation** und folgen Sie den Anweisungen des Assistenten, um mit der Deinstallation zu beginnen.

4. **F:** Wo gebe ich meine Lizenznummer ein?
   A: Klicken Sie auf **Allgemein** und dort auf den Reiter Lizenz. Klicken Sie nun auf **Lizenznummer ändern** und geben Sie Ihre Lizenznummer ein.

Antivirus

5. **F:** Wie kann ich einen Prüfvorgang starten?
   A: Klicken Sie auf **Antivirus** und wählen Sie dort den Reiter Prüfen. Wählen Sie **Lokale Laufwerke** und klicken Sie nun auf **Prüfen**.

6. **F:** Wie oft sollte ich meinem Computer prüfen?
   A: Wir empfehlen den Computer mindestens einmal pro Woche zu prüfen.

7. **F:** Wie kann ich heruntergeladene Dateien automatisch prüfen?
   A: BitDefender überprüft sämtliche Dateien in Echtzeit. Alles, was Sie tun müssen, ist das Virus-Schild aktiviert zu lassen.

8. **F:** Wie kann ich BitDefender anweisen, periodische Prüfungen durchzuführen?
   A: Klicken Sie auf **Antivirus** und dort auf den Reiter Planer. Klicken Sie nun auf **Neu** und folgen Sie dem Assistenten.

9. **F:** Was kann ich mit Dateien innerhalb der Quarantäne tun?
   A: Sie können diese Dateien an das BitDefender-Virus-Labor übersenden, zuvor müssen Sie jedoch die E-Mail-Einstellungen definieren, indem Sie im Reiter Quarantäne auf **Einstellungen** klicken.

Antispam

10. **F:** Was ist Spam?
    A: Bei Spam handelt es sich um unerwünschte Werbung per E-Mail.

11. **F:** Wie funktioniert BitDefender-Antispam?
    A: Bitte sehen Sie hierzu das Arbeitsschema an.

12. **F:** Wohin werden als Spam eingestufte E-Mails verschoben?
    A: Wenn Sie **Microsoft Outlook/Outlook Express** benutzen, werden bereits erkannte Spam-E-Mails in den Ordner Spam/Gelöschte Objekte verschoben.

    TIPP: Wenn Sie einen anderen E-Mail-Client nutzen, sollten Sie eine Regel erstellen, welche sämtliche E-Mails mit "[spam]" im Betreff in einen entsprechenden Ordner verschiebt.

13. **F:** Weshalb bekomme ich nach wie vor E-Mails von einer bestimmten E-Mail-Adresse, obwohl ich sie blockiert habe?
    A: Stellen Sie zunächst sicher, dass sich die blockierte E-Mail-Adresse nicht in der Liste der Freunde befindet. Diese hat Vorrang vor der Liste der Spammer und wird somit zuerst behandelt.

14. **F:** Was ist die Liste der Freunde?
    A: Diese Liste beinhaltet Adressen, von denen Sie immer E-Mails erhalten, unabhängig von deren Inhalt.

15. **F:** Was ist die Liste der Spammer?
    A: Diese Liste beinhaltet Adressen, von denen Sie keine E-Mails mehr erhalten möchten, unabhängig von deren Inhalt.

16. **F:** Was ist der Sprachfilter?
    A: Der Sprachfilter erlaubt es, E-Mails, die in Asiatisch bzw. Kyrillisch verfasst wurden, zu blockieren.

17. **F:** Was ist der URL-Filter?
    A: Der URL-Filter überprüft E-Mails auf Links zu bekannten Web-Seiten mit Werbeinhalten im Internet.

18. **F:** Was ist der Heuristische Filter?
    A: Dieser Filter führt eine Reihe von Tests durch, um zu bestimmen, ob es sich bei einer E-Mail um Spam handelt oder nicht. Hierbei werden alle Komponenten einer E-Mail getestet.

19. **F:** Was ist der Bayesianische Filter?
    A: Dieser Filter klassifiziert E-Mails anhand von statistischen Werten, wie oft bestimmte Wörter in einer E-Mail vorkommen, und vergleicht diese Daten mit bereits als Spam erkannten E-Mails.

Firewall

20. F: Wie kann ich sämtlichen Internetverkehr blockieren?
A: Klicken Sie auf **Firewall** und im Reiter Status unter **Internetverkehr blockieren** auf **Aktivieren**.

21. F: Wieso sollte ich meine Firewall-Regeln abspeichern?
A: Nutzen Sie diese Funktion, wenn Sie vorhaben, eine Reparatur von BitDefender durchzuführen, da bei der Reparatur sämtliche Einstellungen auf die Standard-Werte zurückgesetzt werden.

22. F: Wozu dient die **Zugriffs-Kontrolle**?
A: Die **Zugriffs-Kontrolle** kontrolliert sämtliche Programme auf einen Internetzugriff und dient primär dazu, so genannte Trojanische Pferde zu blockieren.

23. F: Wozu dient die **Anwahl-Kontrolle**?
A: Die **Anwahl-Kontrolle** überwacht sämtliche Programme, die über das Modem eine Telefonverbindung aufbauen. Dies dient primär zur Erkennung von so genannten Dialern, also Programmen, die kostenpflichtige 0190er-Rufnummern anwählen.

24. F: Wozu dient die **Skript-Kontrolle**?
A: Die **Skript-Kontrolle** überprüft Web-Seiten auf gefährliche Skripte in Form von ActiveX, Java Scripts bzw. Applets und blockiert diese, wenn verdächtige Aktivitäten erkannt werden.

25. F: Wozu dient die **Cookie-Kontrolle**?
A: Die **Cookie-Kontrolle** schützt Ihre Privatsphäre, indem Sie selbst bestimmen können, welche Cookies angenommen bzw. versendet werden.

Update

26. F: Wieso ist es notwendig, BitDefender zu aktualisieren?
A: Jedesmal, wenn Sie ein Update ausführen, werden neue Virensignaturen, Heuristik-Regeln und URL-Filter hinzugefügt. Diese verbessern die Erkennung von Viren und Spam-E-Mails.

27. F: Wie kann ich BitDefender aktualisieren?
A: BitDefender prüft in der Standard-Einstellung alle 3 Stunden auf verfügbare Updates. Dieses Intervall können Sie unter Update, Reiter **Einstellungen**, verändern oder auch ein manuelles Update durchführen.

Wörterbuch

ActiveX	AktiveX ist ein Programm-Muster, das von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die AktiveX-Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit AktiveX können die Benutzer z. B. Fragen stellen oder beantworten, Buttons verwenden oder verschiedenartige Interaktionen mit der Webseite herstellen. AktiveX Controls werden oft in Visual Basic geschrieben. Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.
Arbeitsspeicher	Beim Arbeitsspeicher, auch RAM genannt, handelt es sich um kleine – in spezielle Speicherbänke auf der Hauptplatine – eingesteckte Module mit Speicherchips. Darin werden Anwendungsprogramme abgelegt und von der CPU bearbeitete Daten gespeichert. Beim Ausschalten des Computers geht der Inhalt des Arbeitsspeichers verloren. Die Gesamtleistung eines Computers wird maßgeblich von der Größe seines Arbeitsspeichers beeinflusst.
Archive	(1) Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/Backup erzeugt wurden. (2) Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.
Backdoor	Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.
Befehlszeile	Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen, die sich aus einzelnen Buchstabenfolgen zusammensetzen, statt. 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.

Berichtdatei	Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit den geprüften Pfaden, Ordnern und der Archivanzahl, aber auch den geprüften, infizierten oder verdächtigen Dateien.
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 wiedergeben, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.
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 das aber ein zweischneidiges Schwert. Einerseits ist es praktisch, wenn man nur Anzeigen, an denen man interessiert ist, ansehen kann, anderseits werden dafür Benutzerdaten gesammelt, so dass das Surfverhalten eines Nutzers genau nachverfolgbar ist. Von daher sind, was das Thema Datenschutz angeht, Cookies ein umstrittenes Thema.
Dateierweiterung	Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind. Viele Betriebssysteme benutzen Dateierweiterungen, z. B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen). Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.
Download	Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online-Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.
E-Mail	Elektronische Post. Ein Dienst, der Nachrichten an andere

	Rechner über ein lokales oder ein globales Netzwerk übermittelt.
Events (Ereignisse)	Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks und Tastatureingaben, oder System-ereignisse, wie zum Beispiel ungenügender Speicher, sein. Planer (Aufgabenplaner) ist ein Dienstprogramm, mit dessen Hilfe Ereignisse programmiert werden können.
Fehlalarm	Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.
Heuristisch	(Heureka, griech. für: etwas durch eigene Überlegung finden) Eine Methode, um neue Viren zu identifizieren. Diese Prüf-methode beruht nicht auf spezifischen Virussignaturen. Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann. Manchmal kann auch ein verdächtiger Code in einem normalen Programm gemeldet werden, indem der so genannte Fehlalarm generiert wird.
IP	**Internet Protokoll** - 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.
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 ist ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.
Laufwerk	Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann. Ein **Festplatten-Laufwerk** liest und beschreibt Festplatten. Ein **Disketten-Laufwerk** liest und beschreibt Disketten. Ein **CD-ROM-Laufwerk** kann Compact Discs (CD's) lesen. Laufwerke können sowohl interner (im Rechner eingebaut) als

	auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.
Mail Client	Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.
Makrovirus	Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen. Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird. Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.
Nicht heuristisch	Diese Prüfmethode beruht auf einer spezifischen Virussignatur. Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann und dass dieser keinen falschen Alarm auslöst.
Pfad	1. 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 (falls sie eine hat), z. B.: `c:\jobscompany\resume.doc`. 2. Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.
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.
Port	(1) 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. (2) In TCP/IP- und UDP-Netzwerken ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel wird die Schnittstelle 80 wird für http-Traffic verwendet.
Skript	Ein anderer Begriff für Makro - oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.
Startup-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.

System Tray	Der System Tray 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 wird eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden. Das TCP/IP-Protokoll bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.
Trojaner	Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt. 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 Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenken. Aber nachdem die Trojaner das Pferd in ihre durch Mauern gesicherte Stadt gebracht haben, schleichen sich die griechischen Soldaten, die sich in der Bauchhöhle des Holzpferdes verstecken, heraus, öffnen die Stadttore und ermöglichen so ihren Landsmännern 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 auf Updates ermöglicht.
Virus	Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat, und dass sich allein ausführt. Resultat von Virenbefall 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 überwinden.
Virus-Definition	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.

Kontaktinformationen

Die SOFTWIN GmbH als zertifizierter Dienstleister möchte ihren Kunden einen schnellen und leistungsfähigen Support auf hohem Niveau anbieten. Das unten angeführte Supportcenter wird daher laufend mit den neuesten Virendefinitionen und allen weiteren relevanten Informationen versorgt und beantwortet umgehend Ihre auftretenden Fragen, so dass Ihnen jederzeit schnellstens weitergeholfen werden kann.

Für SOFTWIN ist es sehr wichtig, mit den wertvollen Ressourcen unserer Kunden, wie Zeit und Geld, sparsam umzugehen, indem von uns technologisch fortschrittliche Produkte zu angemessenen Preisen angeboten werden. Unsere Überzeugung ist zudem, dass ein erfolgreiches Geschäft sowohl eine gute Kommunikation als auch die Zufriedenheit der Kunden mit dem Support voraussetzt.

Vertrieb: vertrieb@bitdefender.com

http://buy.bitdefender.de/

Technischer Support: support@bitdefender.de

Telefon: 49 (0) 7542 - 94 44 44
Fax: 49 (0) 7542 - 94 44 99

www.bitdefender.de

Einen lokalen Händler finden Sie unter: www.bitdefender.com/partner_list/