bitdefender

FREE EDITION 2009

Benutzerhandbuch

bitdefender

BitDefender Free Edition 2009

Benutzerhandbuch

Veröffentlicht 2009.06.23

Rechtlicher Hinweis

bitdefender

Inhaltsverzeichnis

Endbenutzer Software Lizenzvertrag

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

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

Der Lizenzvertrag und die Gewährleistungsbestimmungen sind ein rechtsgültiger Vertrag zwischen Ihnen (einer natürlichen oder juristischen Person, im Folgenden Benutzer genannt) und BITDEFENDER zur Benutzung des oben und folgend genannten BITDEFENDER SOFTWAREPRODUKTES, welches außer dem eigentlichen SOFTWAREPRODUKT auch dazugehörige Medien, gedruckte Materialien und die Nutzung von Online- und anderen Medien oder elektronische Dokumentation (im Weiteren bezeichnet BitDefender)beinhaltet. Das SOFTWAREPRODUKT und die zugehörigen Materialien sind durch internationale Urheberrechtsverträge geschützt. Indem Sie das SOFTWAREPRODUKT installieren, kopieren, downloaden, darauf zugreifen oder es anderweitig verwenden, erklären Sie sich damit einverstanden, durch die Bestimmungen des Lizenzvertrages und der Gewährleistungsbestimmungen gebunden zu sein.

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

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

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

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

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

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

Upgrades: Wenn BitDefender als Upgrade ausgezeichnet ist, müssen Sie die erforderliche Lizenz besitzen, um das Produkt zu nutzen, dass BitDefender als Upgradefähig identifiziert hat. Ein als Upgrade gekennzeichnetes BitDefender Produkt, ersetzt und/oder erweitert das Produkt, welches die Basis Ihres Upgrades darstellte. Sie dürfen dieses upgraded Produkt alleine gemäß der Lizenzvereinbarung nutzen. Wenn BitDefender ein Update einer Komponente eines Software-Packets ist, das Sie bereits als einzelnes Produkt lizensiert haben, darf BitDefender nur als Teil des Packets genutzt werden und darf nur von der Anzahl Anwender genutzt werden, für die das Produkt lizensiert ist. Die Bestimmungen und Konditionen dieser Lizenz ersetzen vorherige Absprachen, die zwischen Ihnen und BitDefender, in Bezug auf das originale oder upgraded Produkt, existiert haben können.

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

EINGESCHRÄNKTE GEWÄHRLEISTUNG: BITDEFENDER gewährleistet für einen Zeitraum von 30 Tagen, dass das Medium auf dem BitDefender geliefert wird, frei von allen Defekten ist. Sollte dies nicht der Fall sein, wird BITDEFENDER das Medium

austauschen oder dem Benutzer den Betrag zurück erstatten, den der Benutzer für BitDefender bezahlt hat. BITDEFENDER gewährleistet weder die dauerhafte Verfügbarkeit, noch die Fehlerfreiheit von BitDefender, noch dass Unzulänglichkeiten und Fehler von BitDefender behoben werden. BITDEFENDER gewährleistet ebenso nicht, dass BitDefender den Anforderungen des Benutzers entspricht.

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

BESCHRÄNKUNG DER HAFTUNG: Jeder, der BitDefender benutzt, testet oder evaluiert, trägt alleinig das Risiko, das aus der Qualität und Performance von BitDefender entsteht. In keinem Fall können BITDEFENDER oder ihre Lieferanten auf irgendeine Weise für, durch Verwendung von BitDefender, entstandene Schäden jeder Art haftbar gemacht werden, einschließlich und ohne Beschränkung, direkter und indirekter, zufälliger und spezieller Schäden die aus der Verwendung, Performance oder der Verfügbarmachung von BitDefender entstanden sind. Dies gilt auch dann, wenn BITDEFENDER über existierende und / oder mögliche Schäden informiert wurde. IN KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN, DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test, etc.).

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

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

Die Nutzungslizenz für das BitDefender Produkt, kann ohne vorherige 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 BITDEFENDER. Alle anderen Marken und Titel sind Eigentum der jeweiligen Rechteinhaber.

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

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

Im Fall von Widersprüchen oder Unstimmigkeiten zwischen übersetztenFassungen der vorliegenden Bestimmungen gilt die von BITDEFENDER ausgegebene englische Fassung.

BITDEFENDER SRL Preciziei Boulevard, no. 24, West Gate Building H2, ground floor, 6th district, Bucharest, Romania

Vorwort

Diese Anleitung ist für alle Nutzer der BitDefender Free Edition 2009. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen, die gewohnt sind unter Windows zu arbeiten.

Dieses Handbuch wird Ihnen zeigen, wie BitDefender Free Edition 2009 installiert, Konfiguriert und benutzt wird. Sie werden lernen das Beste aus BitDefender heraus zu holen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

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

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

1.2. Symbole

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

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

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

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

2. Struktur

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

Installation. Schritt-für-Schritt Anleitung zur Installation von BitDefender auf einer Workstation. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender Free Edition 2009** und werden durch jeden Schritt begleitet. Zusätzlich wird beschreiben wie eine Deinstallation von BitDefender durchzuführen ist.

Grundkonfiguration. Beschreibung der Grundkonfiguration und Wartung von BitDefender.

Erweiterte Administration. Eine detaillierte Präsentation der BitDefender Advanced View Schnittstelle. Ihnen wird gezeigt, wie man Prüfvorgänge und Update-Einstellungen konfiguriert.

Wie man. Bietet Vorgehensweisen um die allgemeinsten Aufgaben in BitDefender schnell durchzuführen

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

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

3. Ihre Mithilfe

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

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

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

Installation

1. Systemanforderungen

Sie können BitDefender Free Edition 2009 nur auf Computern mit den folgenden Betriebssystemen installieren:

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

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

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

1.1. Hardware-Anforderungen

Für Windows XP

- 800 MHz Prozessor oder höher
- 256 MB Arbeitsspeicher (512 MB empfohlen)
- 300 MB freier Festplattenspeicher (350 MB empfohlen)

Für Windows Vista

- 800 MHz Prozessor oder höher
- Mindestens 512 MB Arbeitsspeicher (1 GB empfohlen)
- 300 MB freier Festplattenspeicher (350 MB empfohlen)

Für Windows Home Server

- 800 MHz Prozessor oder höher
- Mindestens 512 MB Arbeitsspeicher (1 GB empfohlen)
- 300 MB freier Festplattenspeicher (350 MB empfohlen)

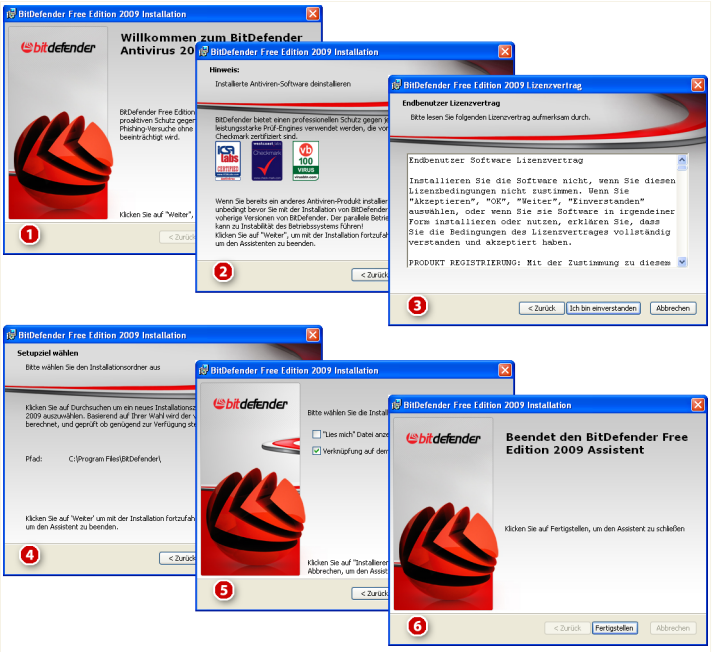
1.2. Software-Anforderungen

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

2. BitDefender installieren

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

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



Installationsschritte

Folgen Sie diesen Schritten, um BitDefender Free Edition 2009 zu installieren:

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

BitDefender Free Edition 2009 informiert Sie sofern weitere Antiviren-Produkte auf Ihrem Computer installiert sind. Klicken Sie auf **Entfernen**, um das betreffende Produkt zu deinstallieren. Sollten Sie fortfahren wollen ohne das entsprechende Produkt zu entfernen, dann klicken Sie auf **Weiter**.

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

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

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

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

   Klicken Sie auf **Weiter**.

5. Optionen bezüglich der Installation auswählen. Manche werden standardmäßig gewählt:
   - **Öffnen der Readme Datei** - öffnen der Readme Datei am Ende der Installation.
   - **Verknüpfung auf dem Desktop anlegen** - um am Ende der Installation eine Verküpfung zu BitDefender Free Edition 2009 auf Ihrem Desktop anzulegen.
   - **CD nach Installation auswerfen** - um die CD nach Beendigen der Installation auszuwerfen. Diese Option erscheint nur, wenn Sie von CD installieren.

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

   Bitte warten Sie bis der Installationsvorgang beendet wurde.

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

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

3. Upgrade zur Vollversion

Die Vollversionen von BitDefender schützen Ihren Computer in Echtzeit und stellen diverese andere Funktionen zum Schutz Ihres PCs und Ihrer Identität im Internet zur Verfügung.

Um von BitDefender Free Edition 2009 auf die Vollversion zu Upgraden, folgen Sie diesen Schritten:

1. Kaufen Sie ein BitDefender Produkt, welches Ihren Anforderungen entspricht. Sie können das BitDefender Produkt kaufen, indem Sie auf den **Upgrade** Link klicken, der sich unten auf der BitDefender Benutzeroberfläche befindet.
2. Installation der Vollversion von BitDefender: doppel-klicken Sie auf die Installationsdatei und folgen Sie dem Setup-Assistenten. Sie müssen BitDefender Free Edition 2009 nicht erst deinstallieren.

4. BitDefender reparieren oder entfernen

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

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

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

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

  Bitte starten Sie Ihren Computer neu, wenn Sie dazu aufgefordert werden. Klicken Sie anschliessend auf **Installieren** um BitDefender Free Edition 2009 neu zu installieren.

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

- **Entfernen** - dient zum Entfernen aller installierten Komponenten. Wir empfehlen die Option **Entfernen** zu verwenden um eine saubere Neuinstallation durchzuführen.

  Wenn Sie BitDefender entfernen wählen erscheint ein neues Fenster.

  Klicken Sie auf **Entfernen**, um BitDefender Free Edition 2009 vom Ihrem Computer zu entfernen.

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

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

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

Während dem Entfernen ist ein Fehler aufgetreten

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

Grundkonfiguration

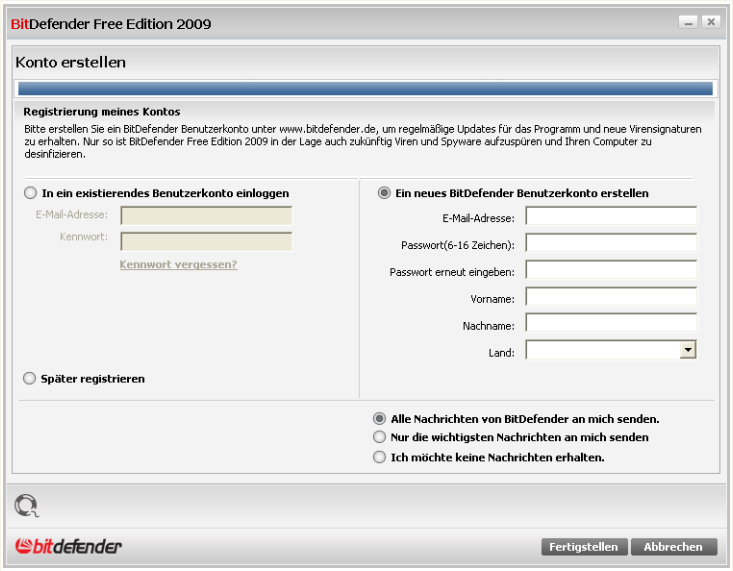
5. Erste Schritte

BitDefender Free Edition 2009 ist ein kostenloser Antivirus&Antispyware Scanner. Er sucht und entfernt Viren, Spyware und andere schädliche Software von Ihren PC.

BitDefender Free Edition 2009 ist bereits mit einem Lizenzschlüssel registriert, der ein Jahr ab Installationsdatum gültig ist. Sobald der Lizenzschlüssel abläuft, wird BitDefender seine Funktion einstellen.

5.1. BitDefender aktivieren

Beim Erst-Start nach der Installation, wird BitDefender Sie auffordern ein Benutzerkonto anzulegen. Das Benutzerkonto ist obligatorisch, um das Produkt zu aktivieren. You must create an account within 15 days after installing BitDefender. Otherwise, BitDefender will no longer update.



Konto erstellen

Wenn Sie zur Zeit kein BitDefender Benutzerkonto einrichten wollen, klicken Sie auf **später registrieren** und dann auf **Beenden**. Ansonsten wählen Sie:

- „Ich habe noch kein BitDefender-Benutzerkonto“ (S. 12)
- „Ich habe bereits ein BitDefender Benutzerkonto.“ (S. 13)

Anmerkung

BitDefender wird Sie benachrichtigen Ihr Produkt zu aktivieren und wird Sie dabei unterstützen dies zu bewerkstelligen. Für weitere Informationen lesen Sie bitte *„Alle beheben“* (S. 27).

Ich habe noch kein BitDefender-Benutzerkonto

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

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.
- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort muss zwischen 6 und 16 Zeichen lang sein
- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.
- **Land** - wählen Sie das Land Ihres Wohnsitzes aus.

Anmerkung

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

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

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

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

- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.

Ich habe bereits ein BitDefender Benutzerkonto.

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

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

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

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

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

Klicken Sie auf **Fertigstellen**.

5.2. BitDefender öffnen.

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

5.3. Ansichtmodus der Benutzeroberfläche

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

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

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

5.3.1. Basisansicht

Die Basisansicht ist eine einfache Bedienoberfläche welche Ihnen dabei hilft Sicherheitsrisiken zu überwachen und zu beheben, sowie vorbeugende Maßnahmen zum Schutz Ihres Rechners durchzuführen.

Basisansicht

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

Objekt	Beschreibung
Einstellungen	Öffnet ein Fenster in dem Sie wichtige Sicherheitsmodule einfach aktivieren oder deaktivieren können.
Zur erweiterten Ansicht wechseln	Öffnen Sie das "Erweiterte Ansicht" -Fenster. Hier können Sie jeden BitDefender Modul genau konfigurieren.

Objekt	Beschreibung
	BitDefender wird sich beim nächsten Öffnen der Benutzeroberfläche dieser Option erinnern.
Status	Beinhaltet Informationen und hilft Ihnen Anfälligkeiten der Sicherheit Ihres Computers zu beheben.

- In der Mitte des Fensters befinden sich zwei Tabs. Die Tabs sind im Einzelnen beschrieben im „*Basisansicht*“ (S. 29) Abschnitt.

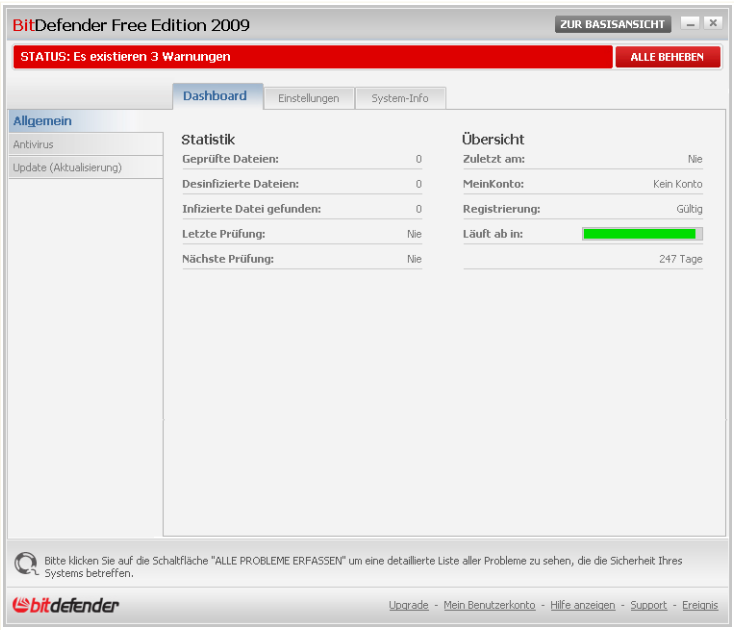
Tab	Beschreibung
Dashboard	Zeigt bedeutende Produktstatistiken und Links zu den wichtigsten On-Demand Aufgaben an.
Antivirus	Zeigt den Status des Antivirus-Moduls an, das Ihnen dabei hilft BitDefender auf dem neusten Stand und Ihren Computer virenfrei zu halten.

- Außerdem enthält die BitDefender Basisansicht mehrere nützliche Verknüpfungen.

Link	Beschreibung
Upgrade	Öffnet eine Webseite, auf der Sie BitDefender Produkte erwerben können. Die Vollversionen von BitDefender schützen Ihren Computer in Echtzeit und stellen diverese andere Funktionen zum Schutz Ihres PCs und Ihrer Identität im Internet zur Verfügung.
Mein Benutzerkonto	Öffnet eine Webseite von welcher Sie sich auf Ihr BitDefender Benutzerkonto einloggen können. Für weitere Informationen über den BitDefender Benuzterkonto, lesen Sie bitte „*BitDefender aktivieren*“ (S. 87).
Hilfe anzeigen	Öffnet die Hilfe-Datei, welche Ihnen zeigt, wie man BitDefender benutzt.
Support	Öffnet eine Webseite, die Ihnen Informationen zum technischen Support gibt.
Historie	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.

5.3.2. Fortgeschrittene Ansicht

Die Erweiterte Ansicht gibt Ihnen Zugriff jede einzelne Komponente von BitDefender. Hier können Sie BitDefender im Einzelnen konfigurieren.



Fortgeschrittene Ansicht

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

Objekt	Beschreibung
Zu Basisansicht wechseln	Öffnet das Basis Ansicht Fenster. BitDefender wird sich beim nächsten Öffnen der Benutzeroberfläche dieser Option erinnern.
Status	Beinhaltet Informationen und hilft Ihnen Anfälligkeiten der Sicherheit Ihres Computers zu beheben.

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

Anmerkung
Die Module der Erweiterten Ansicht werden im Einzelnen „Erweiterte Administration“ (S. 41) in diesem Abschnitt des Benutzerhandbuch vorgestellt.

Modul	*Beschreibung*
Allgemein	Hier haben Sie Zugriff zu den allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen betrachten.
Antivirus	Ermöglicht Ihnen die Prüfungsvorgänge und das Quarantäne Modul zu konfigurieren.
Update	Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.

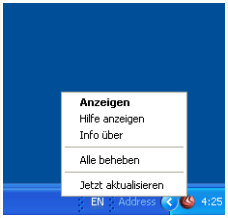
- Außerdem enthält die erweiterte Ansicht von BitDefender mehrere nutzliche Verknüpfungen.

Link	*Beschreibung*
Upgrade	Öffnet eine Webseite, auf der Sie BitDefender Produkte erwerben können. Die Vollversionen von BitDefender schützen Ihren Computer in Echtzeit und stellen diverese andere Funktionen zum Schutz Ihres PCs und Ihrer Identität im Internet zur Verfügung.
Mein Benutzerkonto	Öffnet eine Webseite von welcher Sie sich auf Ihr BitDefender Benutzerkonto einloggen können. Für weitere Informationen über den BitDefender Benuzterkonto, lesen Sie bitte *„BitDefender aktivieren“ (S. 87)*.
Hilfe anzeigen	Öffnet die Hilfe-Datei, welche Ihnen zeigt, wie man BitDefender benutzt.
Support	Öffnet eine Webseite, die Ihnen Informationen zum technischen Support gibt.
Historie	Zeigt Ihnen eine detaillierte Historie aller von BitDefender auf Ihrem System durchgeführten Aufgaben.

5.4. BitDefender Symbol im Infobereich der Taskleiste

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

Wenn Sie dieses Icon doppelklicken wird sich BitDefender öffnen. Zudem öffnen Sie durch einen Rechtsklick ein Untermenu welches Ihnen einen schnelles verwalten des BitDefender Produkts ermöglicht.



BitDefender Symbol

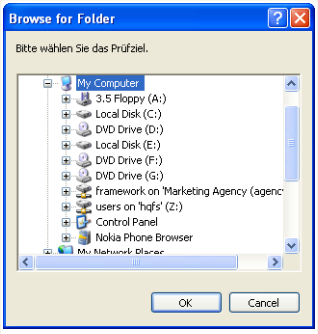
- **Show** - öffnet die Hauptbedienoberfläche des BitDefenders.
- **Hilfe** - öffnet die Hilfe-Datei, welche erklärt, wie man BitDefender Free Edition 2009 konfiguriert und benutzt.
- **Über** - Öffnet ein Fenster in welchem Sie Informationen über BitDefender erhalten und Hilfe finden falls etwas unvorhergesehenes geschied.
- **Alle Probleme beheben** - hilft bestehende Sicherheitsschwachstellen zu entfernen. Falls die Option nicht verfügbar ist, so gibt es keine zu behebenden Probleme. Für weitere Informationen lesen Sie bitte *„Alle beheben“* (S. 27).
- **Jetzt Aktualisieren** - ein Update wird unverzüglich durchgeführt. Ein neues Fenster wird erscheinen, in dem Sie Status des Updates sehen können.

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

5.5. BitDefender Manuelle Prüfung

BitDefender manuelle Prüfung lässt sie eine Prüfung eines bestimmten Ordners oder einer Festplattenpartition durchführen ohne das Erstellen einer Prüfaufgabe. Diese Funktion wurde implimentiert zur Verwendung im abgesicherten Modus von Windows. Falls Ihr System mit einem anpassungfähigen Virus infiziert wurde, so können Sie versuchen diesen zu entfernen indem Sie Windows im abgesicherten Modus starten und mit der manuellen Prüfung von BitDefender jede Festplattenpartition scannen.

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



BitDefender Manuelle Prüfung

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

Scanoptionen. Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Falls infizierte Dateien entdeckt werden wird BitDefender versuchen diese zu desinfizieren (den Mailwarecode entfernen). Wenn die Desinfizierung fehlschlagen sollte wird Ihnen der Antivirus Prüfassistent andere Möglichkeiten anbieten wie mit den infizierten Dateien verfahren werden kann. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

Was ist Abgesichertes Modus?

Der abgesicherte Modus ist eine Sonderfunktion von Windows, welche in den meisten Fällen zur Behebung von Problemen, die normale Operationen von Windows beeinflussen, verwendet wird. Solche Probleme reichen von Treiberkonflikten, bishin zu Viren welche Windows am normalen Starten hindern. Im abgesicherten Modus lädt Windows nur die nötigsten Betriebssystemkomponenten und Basistreiber. Nur wenige Anwendungen funktionieren im abgesicherten Modus. Das ist der Grund warum die meisten Viren im abgesicherten Modus inaktiv und somit einfach zu entfernen sind.

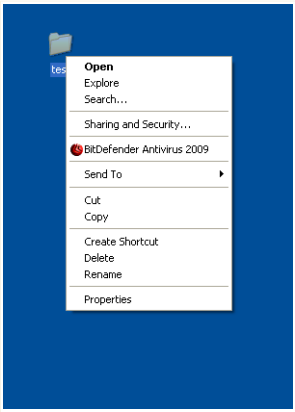
Um Windows im abgesicherten Modus zu starten, starten Sie ihren Rechner neu und drücken die `F8` Taste bis das Windows Erweiterte Optionen Menu erscheint. Sie können zwischen mehreren Optionen wählen. Sie können **abgesicherter Modus mit Netwerktreibern wählen** um auch Internetzugriff zu haben.

Anmerkung

Um mehrere Informationen über Abgesichertes Modus herauszufinden, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**). Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.

5.6. Integration in das Windows Kontextmenu

Das Kontextmenu erscheint wann immer Sie eine Datei oder einen Ordner auf Ihrem Computer oder Desktop rechtsklicken.



Windows Kontextmenu

BitDefender integriert sich in das Windows Kontextmenu um Ihnen zu helfen Dateien leichter prüfen zu können. Sie können die BitDefender Option im Kontextmenu schnell erkennen indem Sie nach dem BitDefender Symbol schauen.

- Prüfe mit BitDefender 2009

5.6.1. Mit BitDefender 2009 prüfen

Sie können das Kontextmenu verwenden um schnell und einfach Dateien, Ordner und sogar ganze Laufwerke prüfen zu lassen. Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Mit BitDefender 2009 prüfen** aus dem Menu aus. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Scanoptionen. Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Falls infizierte Dateien entdeckt werden wird BitDefender versuchen diese zu desinfizieren (den Mailwarecode entfernen). Wenn die Desinfizierung fehlschlagen sollte wird Ihnen der Antivirus Prüfassistent andere Möglichkeiten anbieten wie mit den infizierten Dateien verfahren werden kann.

Wenn Sie die Prüfoptionen ändern möchten, befolgen Sie die Schritte:

1. Bitdefender öffnen.
2. Wenn sich die Bedinoberfläche in der Basis Ansicht befindet**Wechseln Sie zur Profi Ansicht**indem Sie die Schaltfläche, die sich oben-rechts befindet, anklicken.
3. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
4. Klicken Sie auf den Tab **Virenscan**
5. Rechtsklicken Sie die **Untermenuprüfung** und wählen Sie **Öffnen**. Ein neues Fenster wird sich öffnen.
6. Klicken Sie**Anpassen** und konfigurieren Sie die Prüfoption wie gewünscht. Um herauszufinden was eine Option macht, halten Sie den Mauszeiger darüber und lesen die angezeigte Beschreibung im unteren Teil des Fensters.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern.
8. Klicken Sie **OK** um die neue Prüfoption zu bestätigen und anzuwenden.

Anmerkung
Sie sollten die Prüfoption dieser Prüfmethode nicht verändern, es sei den Sie haben einen triftigen Grund dazu.

5.7. Antivirus Prüfassistent

Wann immer Sie den On-Demand Scan einleiten (z.B, Rechtsklick auf einen Ordner und dor wählen **Prüfe mit BitDefender 2009**), wird der Antivirus Prüfassistent erscheinen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

Anmerkung
Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

5.7.1. Schritt 1/3 - Prüfvorgang

BitDefender prüft die gewählten Dateien und Ordner.

Prüfvorgänge durchführen

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

Bitte warten Sie bis BitDefender den Prüfvorgang beendet hat.

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

Passwortgeschützte Archive. Wenn BitDefender während des Prüfvorgangs ein passwortgeschütztes Archiv entdeckt und die Standartaktion ist **Frage nach Passwort**, Sie werden aufgefordert das Passwort anzugeben. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Ich möchte für dieses Objekt das Passwort eingeben.** Wenn Sie möchten das BitDefender Archive prüftt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.

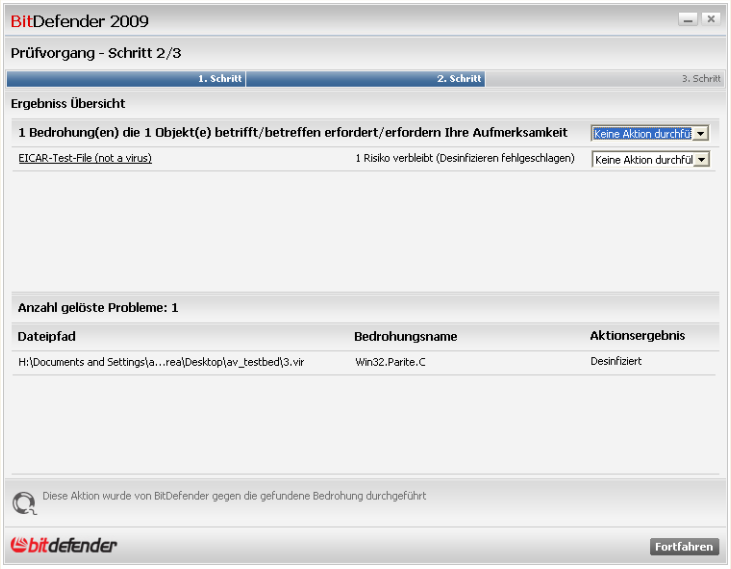
- **Ich möchte für dieses Objekt kein Passwort angeben (dieses Objekt überspringen).** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Ich möchte für kein Objekt ein Passwort angeben (alle passwortgeschützten Objekte überspringen).** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. BitDefender wird nicht in der Lage sein sie zu prüfen, jedoch wird eine Aufzeichnung im Prüflog eingetragen.

Klicken Sie auf **OK** um fortzufahren.

Stoppen oder pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

5.7.2. Schritt 2/3 - Aktionsauswahl

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



Aktionen

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

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

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

Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktion	*Beschreibung*
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.
Löschen	Löscht die infizierten Dateien.
In Quarantäne verschieben	Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa. Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits. Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

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

5.7.3. Schritt 3/3 - Zusammenfassung

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

Übersicht

Ihnen wird eine Zusammenfassung angezeigt. Falls Sie umfangreichere Informationen zum Prüfverlauf möchten, klicken Sie**Logdatei anzeigen**um die Logdatei einzusehen.

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

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

Von BitDefender entdeckte verdächtige Dateien

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

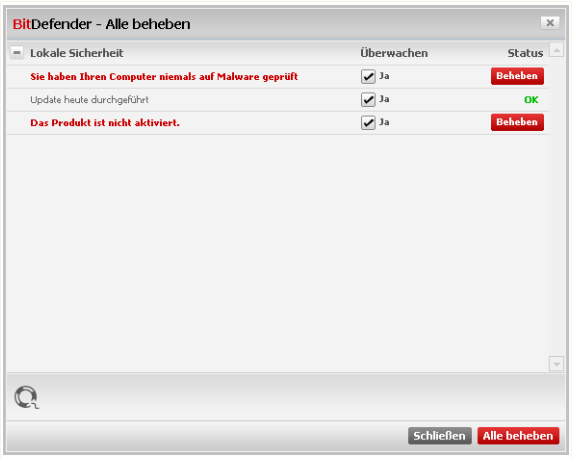
Falls verdächtige Dateien während des Prüfvorganges erkannt werden, werden Sie aufgefordert, diese Dateien zum BitDefender-Labor zu senden. Klicken Sie auf **OK** um diese Dateien zum BitDefender Lab für weitere Analysen zu senden.

6. Alle beheben

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

Im oberen Bereich des BitDefender Fensters, zeigt eine Statusleiste die Anzahl der offenen Punkte. Wähle **Alle Probleme lösen** oder **Dieses Problem lösen** um offene Probleme zu beheben. Ein Sicherheitsstatus-Fenster wird sich öffnen.

Anmerkung
Wenn kein Risiko die Sicherheit Ihres Systems beeinflusst ist die Statusleiste grün.



Statusleiste

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

Diese Probleme könnten erscheinen:

Risiko	*Beschreibung*
Sie haben Ihren Computer nie auf Maleware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.
Sie haben Ihren Computer seit x Tag(en) nicht auf Malware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.
Automatisches Update ist deaktiviert	Bitte lassen Sie die automatischen Updates aktiviert, um sicherzustellen, dass die Malware-Signaturen Ihres BitDefender Produktes ständig aktualisiert werden.
Das Update wurde seit x Tagen nicht durchgeführt	Bitte aktuallisieren Sie BitDefender umgehend. Ist BitDefender nicht auf dem aktuellsten Stand, wird es neue Malware nicht erkennen können, wenn Sie Ihren PC scannen.
Jetzt aktualisieren	Das Update des Produktes und für Malware-Signaturen wird durchgeführt.
Das Produkt ist nicht aktiviert	Um das Produkt zu aktivieren muss ein BitDefender Benutzerkonto erstellt werden.

Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.

Falls sie ein Risiko von der Überwachung ausschliessen möchten entfernen Sie einfach den entsprechenden Hacken aus der **Monitor** Spalte.

7. Basisansicht

Die Basisansicht ist eine einfache Bedienoberfläche welche Ihnen dabei hilft Sicherheitsrisiken zu überwachen und zu beheben, sowie vorbeugende Maßnahmen zum Schutz Ihres Rechners durchzuführen. Die Basisansicht ist unterteilt in zwei Tabs:

Tab	Beschreibung
Dashboard	Zeigt bedeutende Produktstatistiken und Links zu den wichtigsten On-Demand Aufgaben an.
Antivirus	Zeigt den Status des Antivirus-Moduls an, das Ihnen dabei hilft BitDefender auf dem neusten Stand und Ihren Computer virenfrei zu halten.

Auf der rechten Seite jedes Tabs, sehen Sie einen Aufgaben Bereich. Hier können Sie Links zu den standard On-Demand Aufgaben finden. Benutzen Sie diese Aufgaben, um Ihren PC zu scannen und um BitDefender auf dem neusten Stand zu halten.

7.1. Dashboard Tab

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

Dashboard

Das Dashboard besteht aus mehreren Bereichen:

- **Status** - Alamiert Sie sobald Risiken Ihren Computer gefährden und hilft Ihnen diese zu beheben. Wähle **Alle Probleme lösen** oder **Dieses Problem lösen** um offene Probleme zu beheben. Für weitere Informationen lesen Sie bitte *„Alle beheben“ (S. 27)*.
- **Overview** - Zeigt den Update Status, Registrierung und Lizenzinformationen.

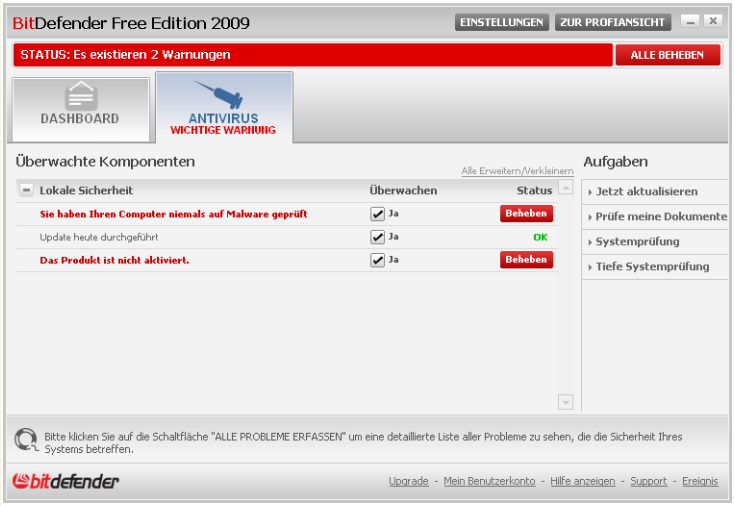
Objekt	*Beschreibung*
Registrierung	Ihr Produkt ist für ein Jahr ab dem Installationsdatum gültig.
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels.
Mein Benutzerkonto	Zeigt die Email Adresse Ihres BitDefender Benutzerkontos. Sie müssen ein BitDefender Benutzerkonto erstellen um das Produkt zu aktivieren. Für weitere Informationen über den BitDefender Benuzterkonto, lesen Sie bitte *„BitDefender aktivieren“ (S. 87)*.

Objekt	Beschreibung
Letztes Update	Zeigt an wann Ihr BitDefender Produkt zu letzt aktualisiert worden ist. Bitte führen Sie regelmäßige Aktualisiserungen durch, damit BitDefender auch die neusten Viren erkennen kann.
Letzte Prüfung	Zeigt an wann Ihr Computer zu letzt geprüft worden ist. Wenn die letzte Prüfung länger als eine Woche her ist, führen Sie bitte so bald wie möglich eine solche durch.

- **Aufgaben** - Stellt Links zu den wichtigsten Security Aufgaben zur Verfügung:
  - **Jetzt Aktualisieren** - startet ein sofortiges Update.
  - **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
  - **Tiefe Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (einschließlich Archive).

7.2. Antivirus Tab

BitDefender beinhaltet ein Antivirus-Modul welches Ihr System virenfrei und Ihren BitDefender auf dem neusten Stand hält. Um das Antivirus-Modul zu öffnen klicken Sie auf den Tab **Antivirus**.



Antivirus

Der Antivirus Tab ist in zwei Bereiche unterteilt:

- **Überwachte Komponenten** - Erlaubt es Ihnen die Liste aller überwachten Komponenten zu sehen. Sie können sich aussuchen welche der Komponenten überwacht werden sollen. Es ist empfohlen die Überwachungsfunktion für alle zu aktivieren.
- **Aufgaben** - Hier finden Sie Links zu den wichtigsten Sicherheitsaufgaben.
  - **Jetzt Aktualisieren** - startet ein sofortiges Update.
  - **Meine Dokumente prüfen** - startet eine schnelle Prüfung Ihrer Dokumente und Einstellungen.
  - **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
  - **Tiefe Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (einschließlich Archive).

7.2.1. Überwachte Komponenten

Wir wissen dass es wichtig ist benachrichtigt zu werden, wann immer ein Problem die Sicherheit Ihres Computers beeinträchtigt. Durch das Überwachen jedes

Sicherheitsmoduls, informiert Sie BitDefender nicht nur darüber wenn Sie Einstellungen verändern, die Einfluss auf die Sicherheit Ihres Computers haben könnten, sondern auch wenn vergessen wurde wichtige Aufgaben durchzuführen.

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

Risiko	*Beschreibung*
Sie haben Ihren Computer nie auf Maleware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.
Sie haben Ihren Computer seit x Tag(en) nicht auf Malware geprüft	Es wird dringend empfohlen eine On-Demand Prüfung so bald wie möglich durchzuführen, um zu überprüfen, ob die Dateien auf Ihrem Computer frei von Malware sind.
Automatisches Update ist deaktiviert	Bitte lassen Sie die automatischen Updates aktiviert, um sicherzustellen, dass die Malware-Signaturen Ihres BitDefender Produktes ständig aktualisiert werden.
Das Update wurde seit x Tagen nicht durchgeführt	Bitte aktuallisieren Sie BitDefender umgehend. Ist BitDefender nicht auf dem aktuellsten Stand, wird es neue Malware nicht erkennen können, wenn Sie Ihren PC scannen.
Jetzt aktualisieren	Das Update des Produktes und für Malware-Signaturen wird durchgeführt.
Das Produkt ist nicht aktiviert	Um das Produkt zu aktivieren muss ein BitDefender Benutzerkonto erstellt werden.

Klicken Sie auf **Feststellen** um alle Sicherheitsrisiken nacheinander festzustellen.

Falls sie ein Risiko von der Überwachung ausschliessen möchten entfernen Sie einfach den entsprechenden Hacken aus der **Monitor** Spalte.

7.3. Aufgaben

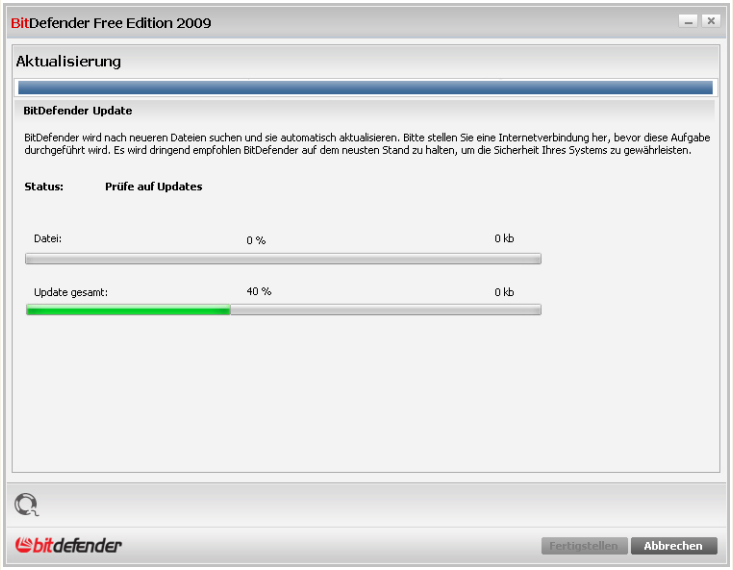
Auf der rechten Seite jedes Tabs, sehen Sie einen **Aufgaben** Bereich. Folgende Aktionen stehen zur Verfügung:

- **Jetzt Aktualisieren** - startet ein sofortiges Update.
- **Meine Dokumente prüfen** - startet eine schnelle Prüfung Ihrer Dokumente und Einstellungen. Diese Aufgabe steht nur auf dem **Antivirus** Tab zur Verfügung.
- **Vollständige Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (ohne Archive).
- **Tiefe Systemprüfung** - Führt einen Prüfvorgang für den gesamten Computer durch (einschließlich Archive).

7.3.1. BitDefender Updaten

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

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



BitDefender Updaten

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

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

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

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

Bitte starten Sie Ihren Computer neu, wenn dies verlangt wird. Im Falle von wichtigen Updates, werden Sie aufgefordert, Ihren Computer neu zu starten. Klicken Sie auf **Neustart** um Ihr System unverzüglich neuzustarten.

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

7.3.2. Prüfen mit BitDefender

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

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

Anmerkung

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

Sobald Sie eine Prüfung starten wird sich der Antivirus-Prüfassistent öffnen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 21).

8. Schnell-Aktivierung/-Deaktivierung der Einstellungen

Um schnell BitDefender Einstellungen zu aktivierern/deaktivieren, öffnen Sie Bitdefender, wechseln zur Standard-Ansicht und wählen **Einstellungen** in der oberen, rechten Ecke des Fensters.

Basiseinstellungen

Die Einstellungen sind in zwei gruppen unterteilt:

- Lokale Sicherheit
- Allgemeine Einstellungen

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

8.1. Lokale Sicherheit

Sie können die automatischen Updates mit einem Klick aktivieren/deaktivieren. Das automatische Update gewährleistet, dass das aktuellste BitDefender Produkt und die Signaturdateien automatisch und regelmäßig heruntergeladen und installiert werden

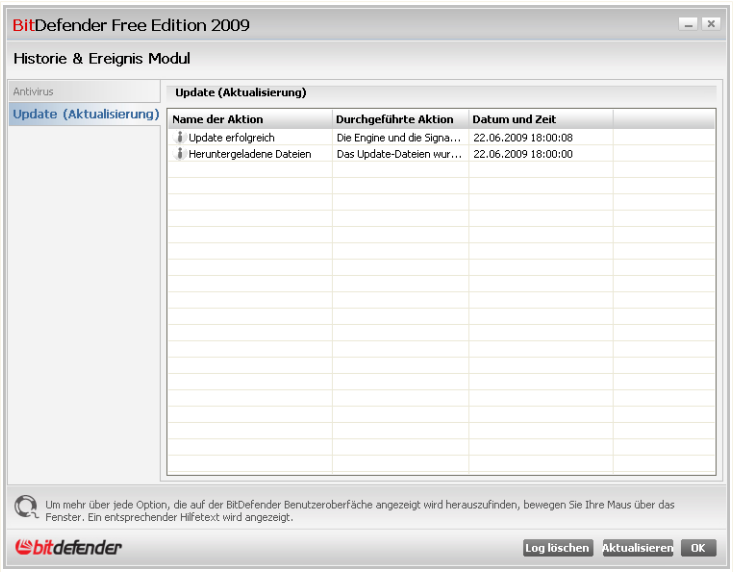
8.2. Allgemeine Einstellungen

Sie können die allgemeinen Einstellungen mit einem Klick aktvieren/deaktivieren.

Objekt	*Beschreibung*
BitDefender Neuigkeiten	Wenn Sie diese Option aktivieren, erhalten Sie von Bitdefender wichtige Firmenneuigkeiten, Produkt-Updates oder Informationen über die neusten Sicherheitsbedrohungen.
BitDefender beim Start von Windows laden	Durch Aktivierung dieser Option wird BitDefender beim PC-Start automatisch geladen. Dies wird dringend empfohlen.
Virenbericht senden	Wenn Sie diese Option aktivieren, werden Virenberichte zum BitDefender Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.
Ausbruchentdeckung	Wenn Sie diese Option aktivieren, werden Berichte über einen möglichen Virenausbruch zum BitDefender Labor für weitere Analysen gesendet. Bitte beachten Sie, dass diese Berichte keine vertraulichen Daten, wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.

9. Ereignis

Der **Ereignise** Link im unteren Bereich des BitDefender Sicherheitscenters öffnet ein anderes Fenster mit dem BitDefender Verlaufsereignissen. Dieses Fenster gibt Ihnen einen Überblick zu allen sicherheitsrelevanten Ereignissen. So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.



Ereignisanzeige

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

- **Antivirus**
- **Update**

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

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

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

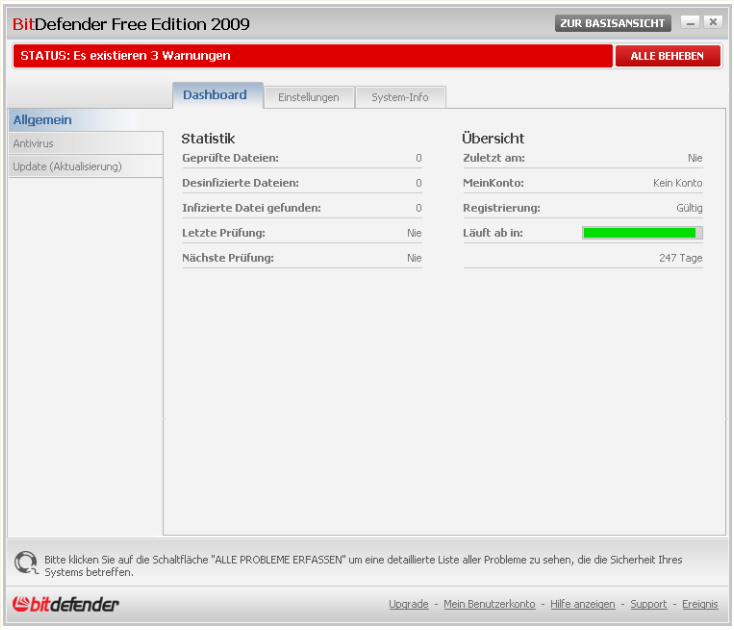
Erweiterte Administration

10. Oberfläche

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

10.1. Dashboard

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



Dashboard

Der Dashboard ist in zwei Bereiche unterteilt:

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

Objekt	Beschreibung
Geprüfte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung auf Malware überprüft wurden.
Desinfizierte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung desinfiziert wurden.
Infizierte Dateien entdeckt	Zeigt die Anzahl der Viren an, die während der letzten Prüfung auf Ihrem System gefunden wurden.
Letzte Prüfung	Zeigt an wann Ihr Computer zu letzt geprüft worden ist. Wenn die letzte Prüfung länger als eine Woche her ist, führen Sie bitte so bald wie möglich eine solche durch. Um den gesamten Computer prüfen zu lassen, gehen Sie zu **Antivirus**, Virenprüfung Tab, und starten Sie entweder eine vollständige- oder tiefgehende Systemprüfung.
Nächste Prüfung	Zeigt an wann die nächste Systemprüfung Ihres PC's ansteht. Um BitDefender so einzustellen, dass Ihr PC automatisch geprüft wird, bitte gehen Sie zu *„Wie man eine Systemprüfung einplant“* (S. 93).

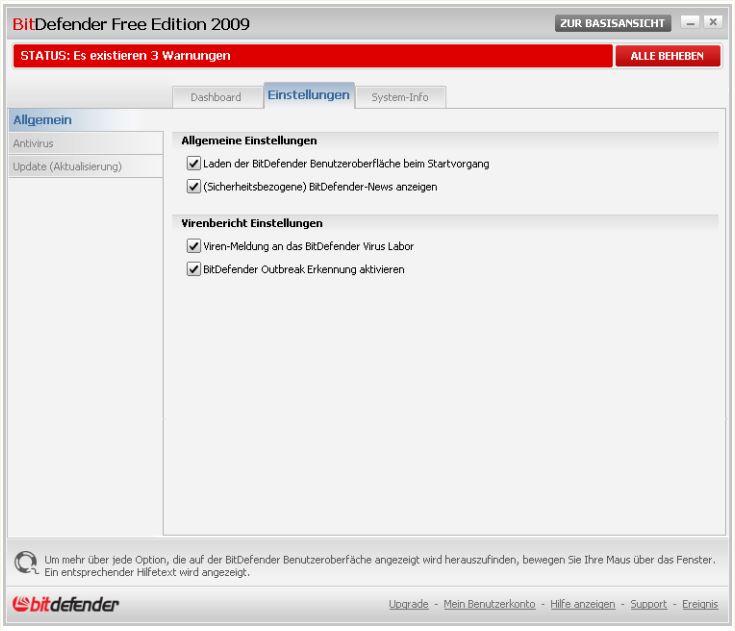
- **Überblick** - Zeigt Ihnen den Update-Status sowie Registrierungs- und Lizenzinformationen an.

Objekt	Beschreibung
Letztes Update	Zeigt an wann Ihr BitDefender Produkt zu letzt aktualisiert worden ist. Bitte führen Sie regelmäßige Aktualisiserungen durch, damit BitDefender auch die neusten Viren erkennen kann.
Mein Benutzerkonto	Zeigt die Email Adresse Ihres BitDefender Benutzerkontos. Sie müssen ein BitDefender Benutzerkonto erstellen um das Produkt zu aktivieren. Für weitere Informationen über den BitDefender Benuzterkonto, lesen Sie bitte *„BitDefender aktivieren“* (S. 87).
Registrierung	Ihr Produkt ist für ein Jahr ab dem Installationsdatum gültig.

Objekt	Beschreibung
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels.

10.2. Einstellungen

Um allgemeine Einstellungen für BitDefender vorzunehmen, klicken Sie auf **Allgemeine>Einstellungen** in der erweiterten Ansicht.



Allgemeine Einstellungen

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

10.2.1. Allgemeine Einstellungen

- **BitDefender Benutzeroberfläche beim Start von Windows laden** - startet BitDefender automatisch beim Systemstart. Dies wird dringend empfohlen.
- **BitDefender-News anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.

10.2.2. Virenbericht Einstellungen

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

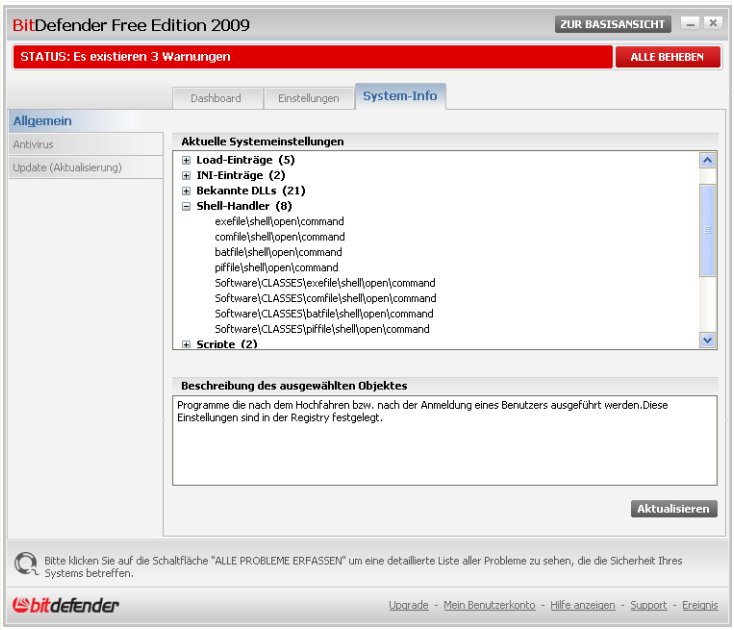
  Diese Meldungen beinhalten keine personifizierten Daten, wie Ihren Namen, IP-Adresse oder ähnliches. Diese werden nicht für kommerziele Zwecke verwendet. Die Meldungen beinhalten nur den Virennamen und werden für die Erstellung von Statistiken verwendet.
- **BitDefender Outbreak Erkennung aktivieren** - sendet Berichte über potentiele Virenausbrüche an das BitDefender Labor.

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

10.3. System-Info

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

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



System-Info

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

Drei Schaltflächen sind verfügbar:

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

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

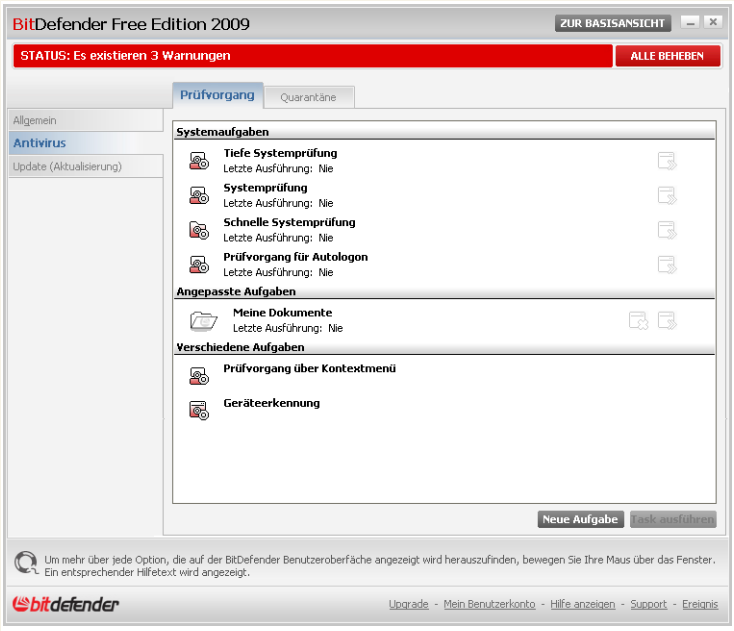
- **Aktualisieren** - öffnet erneut die das Menü **System-Info**.

11. Antivirus

Das Antivirus-Modul ermöglicht Ihnen die Prüfungsvorgänge und das Quarantäne Modul zu konfigurieren.

11.1. Prüfvorgang

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



Prüfaufgaben

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

11.1.1. Prüfaufgaben

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

Jede Aufgabe hat ein **Einstellungen** Fenster welches Ihnen erlaubt die Einstellungen einzustellen und die Prüfberichte zu betrachten. Weitere Informationen finden Sie unter „*Konfiguration einer Prüfaufgabe*“ (S. 51).

Es gibt drei verschiedene Einstellungen der Prüfoptionen:

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

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

Anmerkung
Dadurch das die Prüfvorgänge **Tiefgehende Systemprüfung** und **Systemprüfung** alle Dateien prüfen kann der Vorgang einige Zeit in Anspruch nehmen. Daher

empfehlen wir Ihnen die Aufgabe mit niedriger Priotität durchzuführen oder wenn Sie das System nicht verwenden.

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

  Eine Aufgabe `Meine Dokumente` steht ebenfalls zur Verfügung. Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.
- **Standardaufgaben** - enthält eine Liste verschiedener Prüfoptionen. Diese Optionen weisen auf andere Prüfoptionen hin, die in diesem Fenster nicht ausgeführt werden können. Sie können nur die Einstellungen ändern oder die Prüfberichte ansehen.

Drei Schaltflächen sind verfügbar:

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

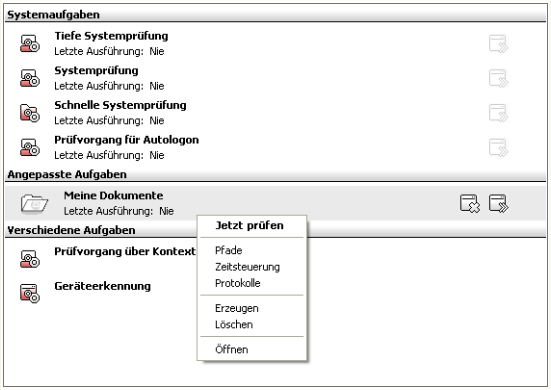
  Anmerkung
  Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

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

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

11.1.2. Verwenden des Kontextmenüs

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



Shortcut Menü

Folgende Aktionen stehen zur Verfügung:

- **Jetzt prüfen** - führt die ausgewählte Aufgabe aus und startet eine sofortige Prüfung.
- **Pfad** - Öffnet das **Eigenschaften** Fenster, Reiter Pfad,wo Sie das Prüfziel für die ausgewählte Aufgabe ändern können.

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

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

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

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

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

11.1.3. Erstellen von Zeitgesteuerten Aufgaben

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

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

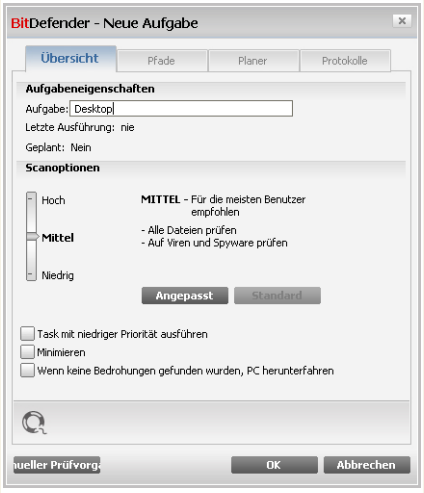
11.1.4. Konfiguration einer Prüfaufgabe

Jede Prüfung hat ihre eigenen **Eigenschaften** ein Fenster indem Sie die prüfoptionen konfigurieren können, das Ziel der Prüfung festlegen,die Tasks planen oder die Berichte ansehen. Um das Fenster zu öffnen klicken Sie auf die **Öffnen** Schaltfläche, auf der rechten Seite der Aufgabe (oder rechtsklicken Sie die Aufgabe und wählen Sie **Öffnen**).

Anmerkung
Weitere Inhalte und Einzelheiten zum Reiter **Prüfberichte** finden Sie in der Produktbeschreibung auf Seite „*Prüfberichte anzeigen*“ (S. 72).

Konfigurieren der Prüfoptionen

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



Übersicht

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

Prüftiefe festlegen

Sie können die Konfiguration einfach durch das wählen der Prüftiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie das gewünschte Level erreicht haben.

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	*Beschreibung*
Niedrig	Bietet ausreichende Entdeckung. Belastung der Ressourcen ist niedrig. Die Programme werden nur auf Viren hin geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel. Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.

Sicherheitseinstellung	Beschreibung
Hoch	Bietet eine hohe Entdeckung. Belastung der Ressourcen ist hoch. Alle Dateien und Archive werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.

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

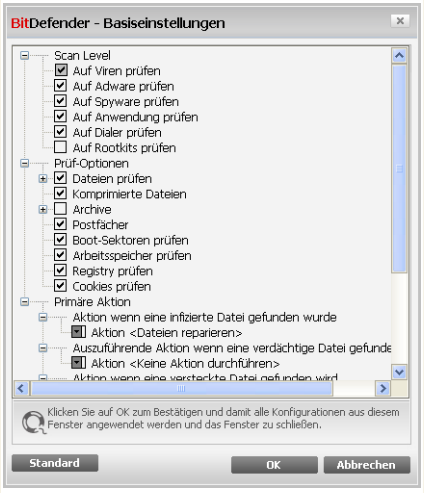
- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
- **In Systemtray minimieren.** Es verkleinert das Prüffenster beim Prüfvorgang in die untere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

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

Prüftiefe konfigurieren

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

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



Auswahlfenster Einstellungen

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

Die Prüfoptionen sind in 3 Kategorien unterteilt:

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

Optionen	*Beschreibung*
Dateien prüfen	Sucht nach bekannten Viren. BitDefender erkennt auch unvollständige Virenkörper, dadurch wird Ihr System zusätzlich geschützt.
Auf Adware prüfen	Sucht nach möglichen Adware-Anwendungen. Entsprechende Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.
Auf Spyware prüfen	Sucht nach bekannter Spyware. Entsprechende Dateien werden wie infizierte Dateien behandelt.

Optionen	Beschreibung
Programmdateien prüfen	Legitime Anwendungen prüfen, die als Spionage-Tool verwendet werden können, um schädliche Anwendungen oder andere Bedrohungen zu verbergen.
Auf Dialer prüfen	Prüft auf Anwendungen welcher kostenpflichtige Nummern wählen. Erkannte Dateien werden als infiziert behandelt. Dadurch ist es möglich das betroffene Anwendungen nicht mehr funktionsfähig sind.
Auf Rootkits prüfen	Prüft nach versteckten Objekten (Dateien und Prozesse), meist Rootkits genannt.

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

Optionen		Beschreibung
Dateien	**Alle Dateien prüfen**	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` und `nws`.
	Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Komprimierte Dateien		Alle komprimierten Dateien werden überprüft.
Archive		Prüfe innerhalb normaler Archive, so wie `.zip`, `.rar`, `.ace`, `.iso` und Andere. Wenn Sie alle Arten von Archiven prüfen wollen (einschließlich Installer und chm Dateien)

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

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

Anmerkung

Um eine neue Aktion auszuwählen, klicken Sie auf die aktuelle Aktion und wählen Sie die gewünschte Aktion aus dem Menu. Sollten Sie sich entschliessen die entdeckten Dateien zu ignorieren oder die gewählte Aktion fehlschlagen so müssen Sie im Prüfvorgangs-Assitenten eine Aktion auswählen.

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

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien können Sie in der Berichtsdatei einsehen.

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

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

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

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

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

Aktion	Beschreibung
Keine Aktion durchführen	Es wird keine Aktion für versteckte Dateien ausgeführt. Diese Dateien finden Sie in der Berichtsdatei.

Aktion	Beschreibung
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa.
In die Quarantäne verschieben	Verschiebt die versteckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Anmerkung

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

- **Option der Vorgehnsweise für passwortgeschützte und verschlüsselte Dateien.** Von Windows verschlüsselten Dateien sind womöglich wichtig für Sie. Deshalb können Sie verschieden Aktionen für infizierte und verdächtige Dateien, die von Windows verschlüsselt sind, konfigurieren. Eine andere Dateikathegorie welche besondere Vorgehensweisen verlangt sind passwortgeschützte Dateien. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Verwenden Sie diese Optionen um festzulegen welche Aktionen für passwortgeschützte Archive und Windows-verschlüsselte Dateien vorzunehmen sind.
  - **Aktion wenn ein Virus in eine verschlüsselte Datei gefunden wird.** Wählen Sie die anzuwendende Aktion bei von Windows verschlüsselten, infizierten Dateien. Die folgenden Optionen sind verfügbar:

Aktion	Beschreibung
Keine Aktion durchführen	Zeichne nur infizierte, von Windows verschlüsselte Dateien auf. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.

Aktion	Beschreibung
Dateien reparieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
Dateien löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.
In die Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

- **Aktion wenn eine verdächtige verschlüsselte Datei gefunden wird.** Wählen Sie die anzuwendende Aktion bei von Windows verschlüsselten, verdächtigen Dateien. Die folgenden Optionen sind verfügbar:

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

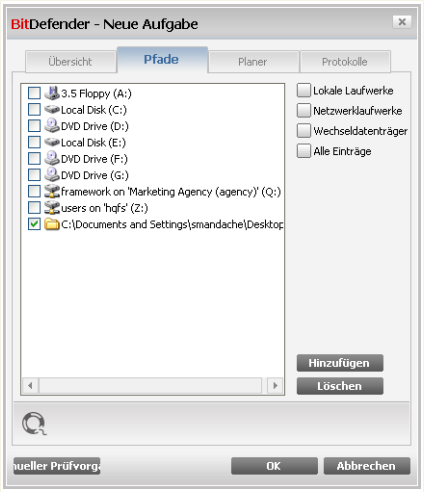
- **Aktion wenn eine passwortgeschützte Datei gefunden wird.** Wählen Sie die durchzuführende Aktion für entdeckte Dateien mit Passwortschutz. Die folgenden Optionen sind verfügbar:

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

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

Festlegen der Zielobjekte

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



Prüfziel

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

Dieser Bereich enthält folgende Schaltflächen:

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

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

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

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

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

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

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

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

Prüfziel der Systemaufgaben anzeigen

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

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

Prüfziel der vollständigen Systemprüfung

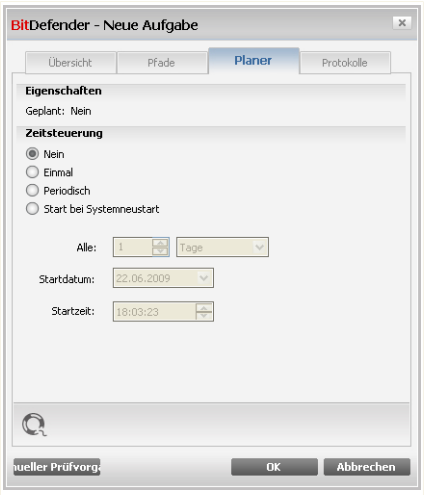
Vollständige Systemprüfung und **Tiefe Systemprüfung** werden alle lokalen Laufwerke prüfen, während**Schnelle Systemprüfung** nur die Ordner `Windows` und `Programme/Dateien` prüfen wird.

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

Zeitgesteuerte Aufgaben festlegen

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

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



Planer

Hier können Sie die Einstellungen zum geplanten Prüfvorgang einsehen.

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

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

  Wenn der Scanvorgang nach einem bestimmten Zeitraum wiederholt werden soll, aktivieren Sie das Kontrollkästchen **Regelmäßig**, und geben Sie in das Textfeld **Alle** die entsprechende Anzahl von Minuten/Stunden/Tage/Wochen/Monate/Jahre ein, nach der die Wiederholung erfolgen soll. Definieren Sie den Startzeitpunkt im Feld **Start Datum/Zeit**.
- **Bei Systemstart** - führt die Prüfung nach einer festgelegten Anzahl von Minuten durch, nachdem der Benutzer sich bei Windows angemeldet hat.

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

11.1.5. Dateien und Ordner prüfen

Bevor Sie einen Prüfvorgang einleiten sollten Sie sich versichern dass BitDefender auf dem neuesten Stand der Maileware-Signaturen ist. Ihren Computer unter Verwendung einer veralteten Signaturendatenbank zu prüfen, kann BitDefender daran hindern neue Maleware, welche seit dem letzten Update gefunden wurde, zu erkennen. Überprüfen Sie wann das letzte Update durchgeführt wurde, gehen Sie zu **Update>Update** in Erweiterte Ansicht.

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

Prüftips

Hier sind noch einige Prüftips welche Sie vielleicht nützlich finden:

- Je nach Festplattengrösse kann das Durchführen einer umfassenden Systemprüfung (wie tiefgehende oder vollständige Systemprüfung) einige Zeit in Anspruch nehmen (bis zu einer Stunde oder sogar mehr). Aus diesem Grund sollten Sie derartige Prüfungen nur durchführen wenn Sie den Computer für eine längere Zeit nicht nutzen (z.B. die Nacht über).

  Sie können die Prüfung planen zu einem günstigen Zeitpunkt zu starten. Stellen Sie sicher den Computer laufen zu lassen. Stellen Sie mit Windows Vista sicher das sich Ihr Rechner nicht im Schlafmodus befindet im Moment der geplanten Aufgabe.

- Falls Sie regelmässig Dateien aus dem Netz in einen bestimmten Ordner herunterladen, erstellen Sie eine neue Prüfaufgabe und legen den Ordner als Prüfziel fest.. Planen sie die Aufgabe ein täglich oder häufiger zu laufen.

- Es gibt eine Malewareart welche sich, durch das Ändern der Windows-Einstellungen, konfiguriert beim Systemstart ausgeführt zu werden. Um Ihren Computer vor solch Maleware zu schützen, planen Sie eine**Autologon Prüfung** beim Systemstart zu laufen. Bitte beachten Sie das Autologon prüfen die Systemleistung für kurze Zeit nach dem Starten beeinflussen kann.

Prüfoptionen

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

- Sofortiges Prüfen - Startet die von Ihnen gewählte Aufgabe umgehend
- Kontext Prüfen - Rechtsklicken Sie auf eine Datei oder einen Ordner und wählen Sie **Prüfe mit BitDefender 2009 aus**.
- Manuelle Prüfung - Verwenden Sie BitDefender Manuelle Prüfung um bestimmte Dateien und Ordner direkt zu prüfen.

Sofortiges Prüfen

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

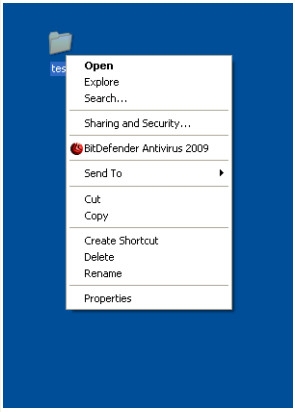
Folgende Optionen sind wählbar:

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

Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Scannen mit dem Kontextmenü

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



Prüfvorgang über Kontextmenü

Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei oder Ordner und wählen Sie **Prüfe mit BitDefender 2009** aus. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

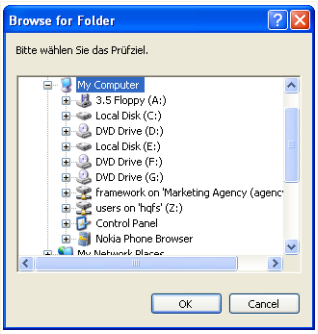
Sie können die Prüfoptionen ändern und die Berichtsdatei einsehen, wenn Sie im Fenster **Eigenschaften** auf **Prüfen Kontext Menü** klicken.

Manuelle Prüfung

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

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

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



Manuelle Prüfung

Wählen Sie das zu prüfende Objekt und klicken Sie auf **OK**. Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.

Antivirus Prüfassistent

Sobald Sie eine On-Demand-Prüfung starten wird sich der Antivirus-Prüfassistent öffnen. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

Anmerkung

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen. Sehen Sie nach dem Prüffortschritticon im Systemtray. Sie können dieses Objekt anklicken um das Prüffenster zu öffnen und so den Prüffortschritt zu sehen.

Schritt 1/3 - Prüfvorgang

BitDefender prüft die gewählten Dateien und Ordner.

Prüfvorgänge durchführen

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

Bitte warten Sie bis BitDefender den Prüfvorgang beendet hat.

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

Passwortgeschützte Archive. Wenn BitDefender während des Prüfvorgangs ein passwortgeschütztes Archiv entdeckt und die Standartaktion ist **Frage nach Passwort**, Sie werden aufgefordert das Passwort anzugeben. Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben. Die folgenden Optionen sind verfügbar:

- **Ich möchte für dieses Objekt das Passwort eingeben.** Wenn Sie möchten das BitDefender Archive prüftt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.

- **Ich möchte für dieses Objekt kein Passwort angeben (dieses Objekt überspringen).** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Ich möchte für kein Objekt ein Passwort angeben (alle passwortgeschützten Objekte überspringen).** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. BitDefender wird nicht in der Lage sein sie zu prüfen, jedoch wird eine Aufzeichnung im Prüflog eingetragen.

Klicken Sie auf **OK** um fortzufahren.

Stoppen oder pausieren der Prüfung. Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Schritt 2/3 - Aktionsauswahl

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

Aktionen

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

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

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

Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktion	*Beschreibung*
Keine Aktion durchführen	Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.
Löschen	Löscht die infizierten Dateien.
In Quarantäne verschieben	Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Dateien umbenennen	Die neue Erweiterung der versteckten Dateien wird `.bd.ren` sein. Infolgedessen werden Sie im Stande sein, zu suchen und solche Dateien auf Ihrem Computer zu finden, falls etwa. Bitte beachten Sie das es sich bei den versteckten Dateien nicht um die absichtlich von Windows verborgenen Dateien handelt. Die relevanten sind die von speziellen Programmen versteckten, bekannt als Rootkits. Rootkits sind nicht grundsätzlich schädlich. Jedoch werden Sie allgemein dazu benutzt Viren oder Spyware vor normalen Antivirenprogrammen zu tarnen.

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

Schritt 3/3 - Zusammenfassung

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

Übersicht

Ihnen wird eine Zusammenfassung angezeigt. Falls Sie umfangreichere Informationen zum Prüfverlauf möchten, klicken Sie**Logdatei anzeigen**um die Logdatei einzusehen.

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

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

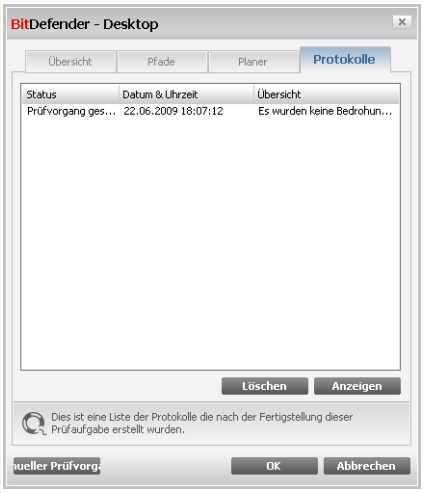
Von BitDefender entdeckte verdächtige Dateien

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

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

11.1.6. Prüfberichte anzeigen

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



Prüfberichte

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

Zwei Schaltflächen sind verfügbar:

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

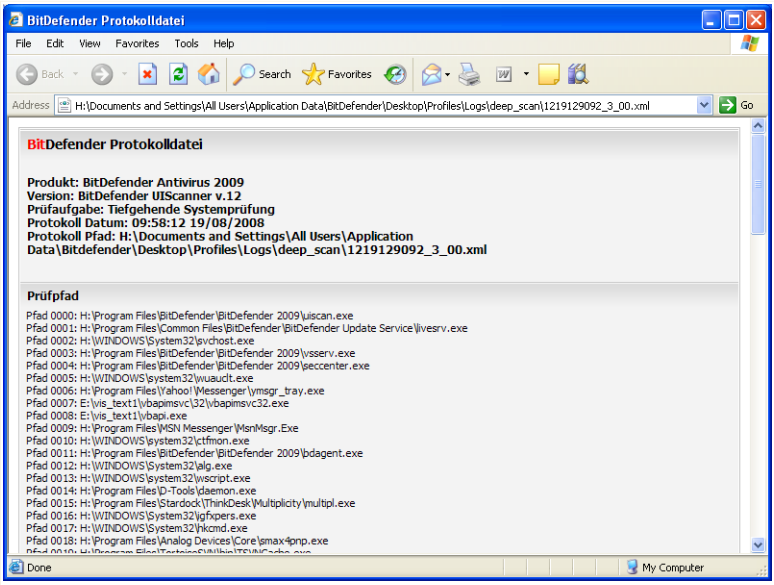
Anmerkung

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

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

Beispiel Prüfbericht

Das folgende Bild zeigt ein Beispiel eines Prüfberichts:



Beispiel Prüfbericht

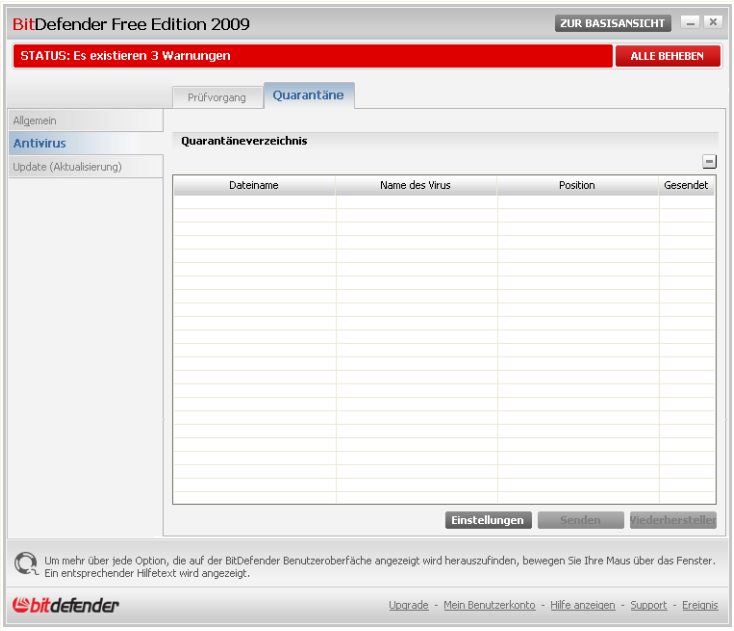
Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

11.2. Quarantäne

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

Zudem prüft BitDefender nach jedem Malewaresignaturen Update die Datein der Quarantäne. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

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



Quarantäne

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

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

11.2.1. Quarantäne-Dateien verwalten

Sie können jede ausgewählte Datei aus der Quarantäne in das BitDefender labor senden in dem Sie **Senden** klicken. Standardmässig überträgt prüft BitDefender die Dateien in Quarantäne alle 60 Minuten.

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

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

11.2.2. Quarantäne-Einstellungen konfigurieren

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

Quarantäne Einstellungen

Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:

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

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

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

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

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

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

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

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

12. Aktualisierung

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

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

Wenn ein Update entdeckt wird, können Sie um eine Bestätigung für das Update gebeten werden oder das Update wird automatisch durchgeführt, je nach den Einstellungen für das automatische Update.

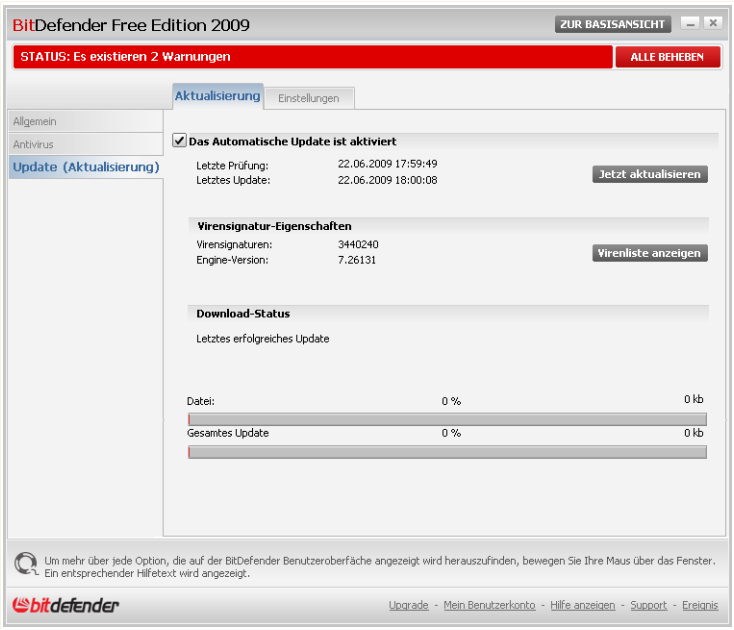
Der Updatevorgang wird "on the fly" durchgeführt, das bedeutet die entsprechenden Dateien stufenweise geupdated werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die AntiViren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur BitDefender Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.

12.1. Automatisches Update

Um Informationen zum Update zu erhalten und automatische Updates auszuführen, klicken Sie auf **Update>Update** in der erweiterten Ansicht.



Automatisches Update

Hier können Sie sehen wann das letzte Update durchgeführt wurde und wann zuletzt eine Prüfung nach Update stattgefunden hat. (und ob das Update erfolgreich war) Ausserdem werden Informationen zur momentanen Engineversion und zur Virensignatur angezeigt.

Wenn Sie das Updatemodul während eines Updates öffnen können Sie den aktuellen Status in Echtzeit einsehen.

Wichtig

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

Sie können Malware-Signaturen für Ihren BitDefender erhalten, indem Sie auf **Virenliste anzeigen** klicken. Eine HTML-Datei, die alle verfügbaren Signaturen enthält wird erstellt und in einem Webbrowser geöffnet. Sie können die Datenbank nach einer

bestimmten Signatur durchsuchen oder auf **BitDefender Virenliste** klicken, um auf die Online-Signaturdatenbank von BitDefender zuzugreifen.

12.1.1. Benutzergesteuertes Update

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

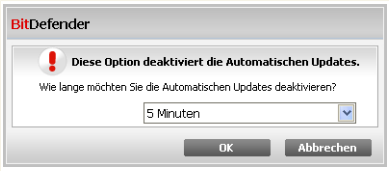
Das **Update** Modul verbindet Ihren Computer automatisch mit dem BitDefender Update Server und benachrichtigt Sie bei einem verfügbaren Update. Wenn ein neues Update verfügbar ist, wird je nach vorgenommener Einstellung entweder abgefragt ob das Update erfolgen soll, oder das Update erfolgt automatisch.

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

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

12.1.2. Automatisches Update deaktivieren

Wenn Sie das Automatische Update deaktivieren erscheint ein Warnfenster.



Automatisches Update deaktivieren

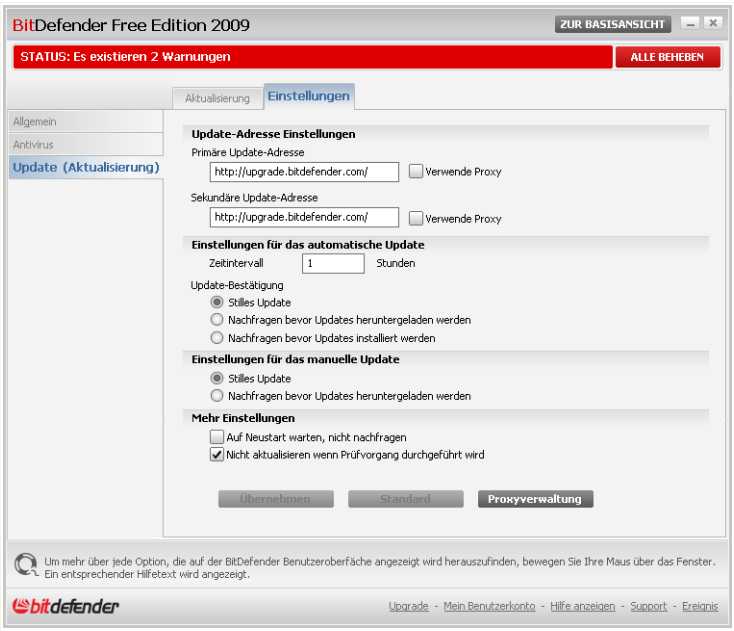
Sie müssen Ihre Einstellung bestätigen indem Sie definieren wie lange das Automatisch Update deaktiviert werden soll. Zur Verfügung stehen die Optionen 5, 15 oder 30 Minuten, eine Stunde, permanent oder bis zum nächsten Systemstart.

Wichtig
Ist BitDefender nicht auf dem aktuellsten Stand, wird es neue Malware nicht erkennen können, wenn Sie Ihren PC scannen.

12.2. Update-Einstellungen

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

Um Updateeinstellungen vorzunehmen und Proxys zu konfigurieren klicken auf **Update>Einstellungen** in der erweiterten Ansicht.



Update-Einstellungen

Das Fenster mit den Update-Einstellungen enthält vier aufklappbare Optionskategorien (**Update-Adresse**, **Einstellungen für das Automatische Update**, **Einstellungen für das manuelle Update** und **Weitere Einstellungen**). Jede Kategorie wird seperat beschrieben.

12.2.1. Update-Adresse

Um eine Update-Adresse festzulegen verwenden Sie die Optionen der **Update-Adresse** Kategorie.

Anmerkung
Ändern Sie diese Einstellungn nur wenn Sie mit einem lokalen Updateserver verbunden sind oder wenn das Update über einen Proxy erfolgt.

Für ein zuverlässigeres und schnelleres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Standardmässig stimmen diese beiden Adressen überein: `http://upgrade.bitdefender.com`.

Um die Update-Adresse zu ändern geben Sie die Adresse des lokalen Servers in das gewünschte **URL** Feld ein.

Anmerkung
Wir empfehlen den Primären Updateserver auf den lokalen Server zu ändern und den sekundären Server unverändert zu belassen sodass im Falle eines lokalen Serverausfalls dennoch Updates durchgeführt werden können.

Wenn Sie für den Zugang zum Internet einen Proxy verwenden, wählen Sie die Option **Proxy verwenden**, und klicken Sie dann auf **Proxyverwaltung** um diese zu konfigurieren. Weitere Informationen finden Sie unter „*Proxyverwaltung*“ (S. 83)

12.2.2. Automatisches Update konfigurieren

Um die Optionen des Automatischen Updates einzustellen verwenden Sie die Optionen unter **Einstellungen für das Automatische Update**.

Sie können die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen im Feld **Zeitinterval** festlegen. Standardmässig ist dieses auf eine Stunde eingestellt.

Um festzulegen wie das automatische Update durchgeführt werden soll können Sie zwischen den folgenden Optionen wählen:

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.
- **Nachfragen bevor Updates installiert werden** - BitDefender frägt den Benutzer bevor ein Update installiert wird.

12.2.3. Manuelle Update Einstellungen

Um festzulegen wie ein manuelles Update durchgeführt wird wählen Sie ein der folgenden Optionen in der Kategorie **Einstellungen für das manuelle Update**:

- **Stilles Update** - BitDefender führt Updates, ohne Benutzereingriff, komplett selbständig im Hintergrund durch.
- **Nachfragen bevor Update heruntergeladen werden** - Immer wenn ein Update verfügbar ist werden Sie gefragt ob dieser heruntergeladen werden soll.

12.2.4. Weitere Einstellungen konfigurieren

Um sicherzustellen das Sie bei der Arbeit nicht vom Updatevorgang gestört werden haben Sie folgende Optionen in der Kategorie **Weitere Einstellungen** zur Verfügung:

- **Auf Neustart warten, nicht nachfragen** - Mit der Aktivierung dieser Einstellung wird der Benutzer nicht gefragt, ob ein Update durch Neustart durchgeführt werden soll. Somit wird der Benutzer während der Arbeit nicht durch BitDefender unterbrochen. Ohne Aktivierung teilt BitDefender mit, dass ein Update den Neustart des Computers benötigt und fragt den Benutzer ob der Neustart nun durchgeführt werden soll.
- **Nicht aktualisieren wenn Prüfvorgang durchgeführt wird** - BitDefender kann während des Prüfvorganges kein Update durchführen. Auf diese Weise kann der Update-Vorgang den Prüfvorgang nicht beeinflussen.

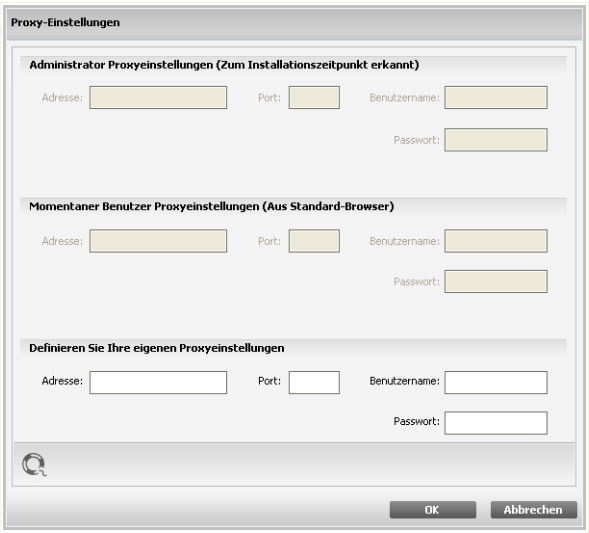
Anmerkung
Sollte BitDefender während eines Prüfvorganges aktualisiert werden, wird der Prüfvorgang abgebrochen.

12.2.5. Proxyverwaltung

Falls Ihre Firma einen Proxy verwendet um eine Internetverbindung herzustellen müssen Sie diese in BitDefender konfigurieren um sicherzustellen das ein Update möglich ist. Anderenfalls werden die Proxyeinstellungen des Administrators welcher das Produkt installiert hat, oder die momentanen Proxyeinstellungen des Standard-Browsers verwendet.

Anmerkung
Proxyeinstellungen können nur von Administratoren oder Hauptbenutzern (welche über das nötige Passwort verfügen) vorgenommen werden.

Um Proxyeinstellungen vorzunehmen klicken Sie auf **Proxyverwaltung**. Die **Proxyverwaltung** wird geöffnet.



Proxyverwaltung

Es bestehen drei mögliche Proxyeinstellungen:

- **Proxyeinstellungen des Administrators** - Diese Einstellungen wurden zum Zeitpunkt der Installation von BitDefender erkannt. Diese können nur von eben diesem Administratorkonto verändert werden. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.
- **Proxyeinstellungen der momentanen Benutzers** - Die Einstellungen des vom momentan eingeloggten Benutzers verwendeten Browser werden übernommen. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.

Anmerkung
Die unterstützen Browser sind hierbei der Internet Explorer, Mozilla Firefox und Opera. Sollten Sie einen anderen Browser verwenden wird BitDefender nicht in der Lage sein die Einstellungen zu übernehmen.

- **Eigene Proxyeinstellungen** - Hier können Sie selbst Proxyeinstellungen vornehmen wenn Sie als Adminstrator eingeloggt sind.

  Die folgenden Einstellungen müssen angegeben werden:
  - **Adresse** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - **Port** - Geben Sie den Port ein, über den BitDefender die Verbindung zum Proxy-Server herstellt.
  - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Bei einem Updateversuch werden alle Proxyeinstellung nacheinander verwendet bis ein Update möglich ist.

Zuerst wird versucht ein Update über die eigenen Proxyeinstellungen vorzunehmen. Als nächstes werden die Proxyeinstellungen des Administrators verwenden. Wenn auch dies nicht zum erfolgt führt wird ein Update über die Einstellungen des momentanen Benutzers durchgeführt.

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

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

Wie man

13. BitDefender aktivieren

Um das Produkt zu aktivieren muss ein BitDefender Benutzerkonto erstellt werden. BitDefender wird Sie, beim ersten Neustart nach der Installation, auffordern ein Benutzerkonto anzulegen. Erstellen Sie zu diesem Zeitpunkt kein Benutzerkonto, müssen Sie BitDefender später, wie folgt, aktivieren:

1. Bitdefender öffnen. Entweder Sie verwenden Windows Start, durch folgen des Pfads**Start → Programme → BitDefender 2009 → BitDefender Free Edition**, oder doppelklicken Sie das BitDefender Ikon im Systray.
2. Klicke **Alle Probleme beheben/Dieses Problem beheben**. Ein neues Fenster wird sich öffnen.
3. Klicke **Beheben**, um das Problem **Das Produkt ist nicht aktiviert** zu lösen.
4. Klicken Sie auf **Ja**. Ein neues Fenster wird sich öffnen.
5. Markieren Sie **Ein neues BitDefender Benutzerkonto erstellen** und geben Sie die benötigten Informationen ein. Die hier eingetragenen Daten bleiben vertraulich.
   - **E-Mail Adresse** - geben Sie Ihre E-Mail Adresse ein. Sobald Ihr Benutzerkonto erstellt ist wird an die angegebene E-Mail Adresse eine Bestätigungs E-Mail gesandt werden.
   - **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort muss zwischen 6 und 16 Zeichen lang sein
   - **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
   - **Vorname** - geben Sie Ihren Vornamen ein.
   - **Name** - Geben Sie Ihren Namen ein.
   - **Land** - wählen Sie das Land Ihres Wohnsitzes aus.
6. Auf Wunsch wird BitDefender Sie über die E-Mail-Adresse Ihres Benutzerkontos zu Sonderangeboten informieren. Wählen Sie eine der zur Verfügung stehenden Optionen:
   - **Senden Sie mir alle BitDefender-Nachrichten**
   - **Senden Sie mir nur die wichtigsten Nachrichten**
   - **Senden Sie mir keine Nachrichten**
7. Klicken Sie **Beenden** um die angegebenen Informationen zu bestätigen und Ihr Benutzerkonto zu erstellen.

8. Klicken Sie **OK** um die Aktivierung des Kontos zu bestätigen.
9. **Aktivieren Sie Ihr Benutzerkonto.** Sie müssen Ihr Benutzerkonto aktivieren bevor Sie es nutzen können. Sobald Sie die vom BitDefender Registrationsdienst gesandte Mail erhalten haben, folgen Sie den darin enthaltennen Anweisungen.

Nach der Aktivierung, klicken Sie auf den **My Account** Link um sich in Ihr Benutzerkonto einzuloggen. Den Link finden Sie in der rechten unteren Ecke der BitDefender Benutzeroberfläche.

Wichtig

You must create an account within 15 days after installing BitDefender. If you do not create a BitDefender account in due time, BitDefender will no longer receive its regular malware signature updates. If the malware signatures are outdated, BitDefender may not be able to detect new malware.

14. Wie man Datein und Ordner prüft

Prüfen mit BitDefender ist einfach und flexibel. Es gibt 3 Arten, BitDefender Dateien und Ordner auf Viren und andere Malware prüfen zu lassen.

- Unter Verwendung des Windows Kontext Menus
- Unter Verwendung von Prüfaufgaben
- Unter Verwenung der manuellen Prüfung

Sobald Sie die Prüfung eingeleitet haben wird der Antivirus Prüfassistent erscheinen und Sie durch den Handlungsprozess leiten. Weitere Informationen zu diesem Assistenten finden Sie unter *„Antivirus Prüfassistent“* (S. 21).

14.1. Unter Verwendung des Windows Kontext Menus

Dies ist der einfachste und empfohlene Weg eine Datei oder Ordner auf Ihrem Computer zu prüfen. Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Mit BitDefender 2009 prüfen** aus dem Menu aus. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Typische Situationen in welchen Sie diese Prüfmethode verwenden würden schliessen das Folgende ein:

- Sie verdächtigen eine bestimmte Datei oder Ordner infiziert zu sein.
- Wann immer Sie vom Internet Dateien herunterladen von denen Sie glauben infiziert zu sein.
- Prüfen Sie einen freigegebnen Ordner bevor Sie von ihm Dateien auf Ihren Rechner kopieren.

14.2. Unter Verwendung von Prüfaufgaben

Wenn Sie Ihren Computer oder bestimmte Ordner regelmässig prüfen lassen möchten, so sollten Sie in Betracht ziehen hierfür eine Prüfaufgabe zu verwenden. Prüfaufgaben weisen BitDefender an wo zu prüfen und welche Option und Aktion zu tätigen ist. Ausserdem, können Sieplanen sie auf geregelter Basis oder zu einer bestimmten Zeit laufen zu lassen.

Um Ihren Computer unter Verwendung von Prüfaufgaben prüfen zu lassen, öffnen Sie die BitDefender Benutzeroberfläche und starten dort die gewünschte Prüfaufgabe. Je nach gewählter Benutzeroberfläche (Basisansicht oder Erweiterte Ansicht), ist verschieden Schritten zu folgen um eine Prüfaufgabe zu starten.

Starten von Prüfaufgaben in der Basisansicht

In der Basisansicht lassen sich nur eine gewisse Anzahl von vorkonfigurierten Prüfaufgaben starten. Folgen Sie den Schritten um eine Prüfaufgabe in der Basisansicht zu starten:

1. Klicken Sie das**Antivirus** Tab.
2. Auf der rechten Seite**Aufgaben** -Bereich, klicken Sie auf die Prüfaufgabe welche Sie durchführen möchten. Dieses sind die verfügbaren Prüfaufgaben:

Prüfaufgabe	*Beschreibung*
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Meine Dokumente prüfen	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

3. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Starten von Prüfaufgaben in der Erweiterten Ansicht

In der Erweiterten Ansicht können Sie alle vorkonfigurierten Prüfaufgaben durchführen und deren Prüfoptionen ändern. Ausserdem können Sie dort Prüfaufgaben selbst erstellen wenn Sie an bestimmten Stellen Ihres Computers prüfen möchten. Folgen Sie den Schritten um eine Prüfaufgabe in der Erweiterten Ansicht zu starten:

1. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
2. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen. Dies sind die Standartprüfaufgeben welche Sie verwenden können:

Standard Einstellungen	*Beschreibung*
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Schnelle Systemprüfung	Prüft die`Windows` und `Programme` Ordner. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.
Meine Dokumente	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

3. Doppelklicken Sie die Prüfaufgabe die Sie zu starten wünschen.
4. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

14.3. Verwende BitDefender Manuelle Prüfung

BitDefender manuelle Prüfung lässt sie eine Prüfung eines bestimmten Ordners oder einer Festplattenpartition durchführen ohne das Erstellen einer Prüfaufgabe. Diese Funktion wurde implimentiert zur Verwendung im abgesicherten Modus von Windows. Falls Ihr System mit einem anpassungfähigen Virus infiziert wurde, so können Sie versuchen diesen zu entfernen indem Sie Windows im abgesicherten Modus starten und mit der manuellen Prüfung von BitDefender jede Festplattenpartition scannen.

Um Ihren Computer unter Verwendung der manuellen Prüfung zu prüfen, folgen Sie den Schritten:

1. Im  Windows Start Menu, folgen Sie dem Pfad**Start** → **Programme** → **BitDefender 2009** → **BitDefender manuelle Prüfung**. Ein neues Fenster wird sich öffnen.
2. Wähle Sie das Prüfziel:
   - Um Ihr Desktop zu prüfen, wählen sie einfach **Desktop**.
   - Um eine komplette Festplattenpartition prüfen zu lassen, wählen Sie sie unter Arbeitsplatz aus.
   - Um einen bestimmten Ordner zu prüfen, suchen Sie ihn heraus und wählen ihn aus.
3. Klicken Sie auf **OK** um die Prüfung zu starten.
4. Folgen Sie dem Antivirus Prüfassistenten um die Prüfung abzuschliessen.

Was ist Abgesichertes Modus?
Der abgesicherte Modus ist eine Sonderfunktion von Windows, welche in den meisten Fällen zur Behebung von Problemen, die normale Operationen von Windows beeinflussen, verwendet wird. Solche Probleme reichen von Treiberkonflikten, bis hin zu Viren welche Windows am normalen Starten hindern. Im abgesicherten Modus lädt Windows nur die nötigsten Betriebssystemkomponenten und Basistreiber. Nur wenige Anwendungen funktionieren im abgesicherten Modus. Das ist der Grund warum die meisten Viren im abgesicherten Modus inaktiv und somit einfach zu entfernen sind.
Um Windows im abgesicherten Modus zu starten, starten Sie ihren Rechner neu und drücken die `F8` Taste bis das Windows Erweiterte Optionen Menu erscheint. Sie können zwischen mehreren Optionen wählen. Sie können **abgesicherter Modus mit Netwerktreibern wählen** um auch Internetzugriff zu haben.

Anmerkung

Um mehrere Informationen über Abgesichertes Modus herauszufinden, öffnen Sie die Windows Hilfe/Support (Klicken Sie im Startmenu auf **Hilfe und Support**). Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.

15. Wie man eine Systemprüfung einplant

Ihren Computer regelmässig prüfen zu lassen ist die beste Art ihn frei von Maleware zu halten. BitDefender gibt Ihnen die Möglichkeit Prüfaufgaben einzuplanen so das Sie Ihren Computer automatisch prüfen lassen können.

Um BitDefender eine geplante Prüfaufgabe durchführen zu lassen folgen Sie den Schritten:

1. Bitdefender öffnen. Entweder Sie verwenden start Windows Start, durch folgen des Pfads**Start → Programme → BitDefender 2009 → BitDefender Free Edition**, oder doppelklicken Sie das BitDefender Ikon im Systray.
2. Wenn sich die Bedinoberfläche in der Basis Ansicht befindet**Wechseln Sie zur Profi Ansicht**indem Sie die Schaltfläche, die sich oben-rechts befindet, anklicken.
3. Klicken Sie auf **Antivirus** in dem Menü auf der linken Seite.
4. Klicken Sie auf den Tab **Virenscan** Hier finden Sie eine Reihe von Standartprüfaufgaben und Sie können hier Ihre eigenen Prüfaufgaben erstellen.
   - Systemaufgaben sind verfügbar und können unter jedem Windows Benutzerkonto gestartet werden.
   - Benutzeraufgaben sind ausschliesslich für den Benutzer verfügbar der sie erstellt hat und können auch nur von diesem gestartet werden.

   Dies sind die Standartprüfaufgeben welche Sie einplanen können:

Standard Einstellungen	*Beschreibung*
Tiefgehende Systemprüfung	Prüft das komplette System In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Systemprüfung	Prüft alle Dateien mit Ausnahme von Archiven. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, wie z.B. Viren, Spyware, Adware, Rootkits und so weiter.
Schnelle Systemprüfung	Prüft die`Windows` und `Programme` Ordner. In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitspeicher, die Registy und Cookies nicht geprüft.

Standard Einstellungen	Beschreibung
Prüfung bei Login	Prüft die Objekte, die ausgeführt werden, wenn ein Benutzer sich bei Windows anmeldet. Um diese Aufgabe zu nutzen, muss sie eingeplant werden beim Systemstart zu laufen. Standardmäßig ist die Prüfung im Hintergrund deaktiviert.
Meine Dokumente	Verwenden Sie diese um die folgenden für den jeweiligen Benutzer wichtigen Ordner zu prüfen: `Eigene Dateien`, `Desktop` und `Autostart`. Dies stellt sicher das Ihre Eigenen Dateien, Ihr Desktop und die beim Starten von Windows geladenen Programme schädlingsfrei sind.

Falls keine der Prüfaufgaben Ihren Bedürfnissen entspricht können Sie eine neue Prüfaufgabe erstellen, welche Sie dann wiederum so einplanen können wie Sie wünschen.

5. Rechtsklicken Sie die gewünschte Prüfaufgabe und wählen Sie**Eingeplant**. Ein neues Fenster wird sich öffnen.
6. Planen Sie die Aufgabe ein wie erforderlich:
   - Um die Aufgabe einmalig durchzuführen, wählen Sie **Einmalig** und bestimmen Sie das Startdatum und die Zeit.
   - Um die Prüfaufgabe nach dem Systemstart, wählen Sie **Beim Systemstart**. Geben Sie an wie lange nach dem Systemstart die Aufgabe gestartet sein wird.(Minuten)
   - Um die Aufgabe auf regulärer Basis laufen zu lassen, wählen Sie **Periodisch** und bestimmen Sie die Häufigkeit, das Startdatum und die Zeit.

Anmerkung

Als Beispiel, um Ihren Computer jeden Samstag um 2:00Uhr prüfen zu lassen, müssen Sie wie folgt einplanen:

a. Wählen Sie **Periodisch**.

b. Im **Täglich** Feld, geben Sie 1 ein und wählen dann**Wochen** im Menu. Auf diese Art wird die Aufgabe einmal wöchentlich laufen.

c. Legen Sie als Startdatum den kommenden Samstag fest.

d. Legen Sie als Startzeit `2:00:00 Uhr`fest.

7. Klicken Sie **OK** um die Planung zu speichern. Die Prüfaufgabe wird automatisch, gemäß der definierten Planung, ablaufen. Falls der Computer im Moment der geplanten Aufgabe abgeschaltet ist, so wird die Aufgabe beim nächsten Computerstart starten.

Kontakt

16. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell.Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

16.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Dokumentationdocumentation@bitdefender.com
Partner Proogramm: vertrieb@bitdefender.de
Marketing: marketing@bitdefender.de
Media Relationspresse@bitdefender.de
Jobs: jobs@bitdefender.de
Virus Einsendungen: virus_submission@bitdefender.com
Spam Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Produkt Webseite: http://www.bitdefender.de
Produkt ftp Archive: http://www.bitdefender.de
Lokale Großhändler: http://www.bitdefender.com/site/Partnership/list/
BitDefender Knowledge Base: http://kb.bitdefender.de

16.2. BitDefender Geschäftsstellen

The BitDefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

16.2.1. U.S.A

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (Geschäftsstelle& Vertrieb): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com

16.2.2. Deutschland

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Geschäftsstelle: +49 2301 91 84 222
Sales: vertrieb@bitdefender.de
Web: http://www.bitdefender.de

16.2.3. Großbritannien und Irland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-Mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096
Sales: sales@bitdefender.co.uk
Web: http://www.bitdefender.co.uk

16.2.4. Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
Fax: +34 932179128
Telefon: +34 902190765
Sales: comercial@bitdefender.es
Webseite: http://www.bitdefender.es

16.2.5. Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon Vertrieb: +40 21 2063470
Vertrieb E-Mail: sales@bitdefender.ro
Webseite: http://www.bitdefender.ro

Glossar

AktiveX

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

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

Adware

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

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

Archive

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

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

Backdoor (Hintertür)

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

Bootsektor

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

Bootvirus

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

Durchsuchen

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

Befehlszeile

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

Cookie

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

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

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

Download

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

E-Mail

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

Ereignisanzeige

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

Fehlalarm

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

Dateierweiterung

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

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

Heuristik

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

IP

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

Java Applet

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

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

Makrovirus

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

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

E-Mail Client

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

Arbeitsspeicher

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

Nicht heuristisch

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

Komprimierte Programme

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

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

Pfad

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

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

Phishing

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

Polymorpher Virus

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

Schnittstelle

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

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

Logdatei (Berichtsdatei)

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

Rootkit

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

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

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

Script

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

Spam

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

Spyware

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

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

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

Startup Objekt (Autostart-Objekt)

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

Symbolleiste

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

TCP/IP

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

Trojaner

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

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

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

Aktualisierung

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

BitDefender hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet.Es kann sich nicht an andere Programme anhängen.