

bitdefender



ANTIVIRUS₂₀₀₉

Benutzerhandbuch

 **bitdefender**



BitDefender Antivirus 2009

Benutzerhandbuch

Veröffentlicht 2009.01.30

Copyright© 2009 BitDefender

Rechtlicher Hinweis

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

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

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

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



BitDefender Antivirus 2009





Inhaltsverzeichnis

Endbenutzer Software Lizenzvertrag	ix
Vorwort	xiv
1. Verwendete Konventionen	xiv
1.1. Typografie	xiv
1.2. Symbole	xv
2. Struktur	xv
3. Ihre Mithilfe	xvi
Installation	1
1. Systemanforderungen	2
1.1. Hardware-Anforderungen	2
1.2. Software-Anforderungen	3
2. BitDefender installieren	4
2.1. Registrierungsassistent	6
2.1.1. Schritt 1/2 - BitDefender Antivirus 2009 registrieren	7
2.1.2. Schritt 2/2 - BitDefender-Benutzerkonto erstellen	8
2.2. Konfigurationsassistent	10
2.2.1. Schritt 1/8 - Begrüßungsfenster	11
2.2.2. Schritt 2/8 - Auswahl der Ansichtsmodi	12
2.2.3. Schritt 3/8 - Konfigurieren Sie das BitDefender Netzwerk	13
2.2.4. Schritt 4/8 - Identitätskontrolle konfigurieren	14
2.2.5. Schritt 5/8 - Virenberichte konfigurieren	18
2.2.6. Schritt 6/8 - Aufgabentyp	19
2.2.7. Schritt 7/8 - Warten bis Aufgaben vervollständigt wurden	20
2.2.8. Schritt 8/8 - Fertigstellen	21
3. Upgrade	22
4. BitDefender reparieren oder entfernen	23
Grundkonfiguration	25
5. Erste Schritte	26
5.1. BitDefender Antivirus 2009 starten	26
5.2. Ansichtmodus der Benutzeroberfläche	26
5.2.1. Basisansicht	26
5.2.2. Fortgeschrittene Ansicht	29
5.3. BitDefender Symbol im Infobereich der Taskleiste	31
5.4. Scanaktivitätsanzeige	32
5.5. BitDefender Manuelle Prüfung	33



5.6. Spiele-Modus	34
5.6.1. Spielmodus benutzen	34
5.6.2. Tastenkombination für Spielmodus ändern	34
5.7. Integration in Web-Browser	35
5.8. Integration in Messenger	37
6. Dashboard	39
6.1. Übersicht	86
6.2. Aufgaben	41
6.2.1. Prüfen mit BitDefender	41
6.2.2. BitDefender Updates	42
7. Antivirus	44
7.1. Überwachte Komponenten	44
7.1.1. Lokale Sicherheit	76
7.2. Aufgaben	46
7.2.1. Prüfen mit BitDefender	46
7.2.2. BitDefender Updates	47
8. Antiphishing	49
8.1. Überwachte Komponenten	49
8.1.1. Online Sicherheit	77
8.2. Aufgaben	51
8.2.1. Prüfen mit BitDefender	51
8.2.2. BitDefender Updates	52
9. Prüfung auf Schwachstellen	54
9.1. Überwachte Komponenten	54
9.1.1. Schwachstellen-Scan	78
9.2. Aufgaben	56
9.2.1. Prüfung auf Schwachstellen/Anfälligkeit	56
10. Netzwerk	64
10.1. Aufgaben	65
10.1.1. Dem BitDefender-Netzwerk beitreten	65
10.1.2. Computer zum BitDefender-Netzwerk hinzufügen	66
10.1.3. Das BitDefender-Netzwerk verwalten	68
10.1.4. Alle Computer prüfen	70
10.1.5. Alle Computer aktualisieren	71
10.1.6. Alle Computer registrieren	72
11. Basiseinstellungen	73
11.1. Lokale Sicherheit	74
11.2. Online Sicherheit	74
11.3. Allgemeine Einstellungen	74
12. Statusleiste	76
12.1. Lokale Sicherheit	76



12.2. Online Sicherheit	77
12.3. Schwachstellen-Scan	78
13. Registrierung	80
13.1. Schritt 1/1 - BitDefender Antivirus 2009 registrieren	80
14. Ereignis	82
<i>Erweiterte Administration</i>	<i>84</i>
15. Allgemein	85
15.1. Dashboard	85
15.1.1. Statistik	86
15.1.2. Übersicht	86
15.2. Einstellungen	87
15.2.1. Allgemeine Einstellungen	88
15.2.2. Virenbericht Einstellungen	89
15.3. System-Info	89
16. Antivirus	91
16.1. Echtzeitschutz	91
16.1.1. Sicherheitsstufe einstellen	92
16.1.2. Sicherheitsstufe anpassen	93
16.1.3. Konfigurieren Sie die Verhaltensprüfung	97
16.1.4. Echtzeitschutz deaktivieren	99
16.1.5. Antiphishingschutz konfigurieren	100
16.2. Prüfvorgang	101
16.2.1. Prüfaufgaben	102
16.2.2. Verwenden des Kontextmenüs	104
16.2.3. Erstellen von Zeitgesteuerten Aufgaben	105
16.2.4. Konfiguration einer Prüfaufgabe	106
16.2.5. Prüfoptionen	118
16.2.6. Prüfberichte anzeigen	124
16.3. Vom Prüfvorgang ausgeschlossene Objekte	126
16.3.1. Pfade vom Prüfen ausnehmen	128
16.3.2. Dateierweiterungen vom Prüfen ausnehmen	132
16.4. Quarantäne	136
16.4.1. Quarantäne-Dateien verwalten	138
16.4.2. Quarantäne-Einstellungen konfigurieren	138
17. Privatsphärekontrolle	140
17.1. Status der Privatsphärekontrolle:	140
17.1.1. Sicherheitsstufe einstellen	142
17.2. Antispyware/Identitätskontrolle	142
17.2.1. Erstellen von Privatsphäreregeln	144
17.2.2. Definition von Ausnahmen	148
17.2.3. Regeln bearbeiten	149



17.3. Registrierung prüfen	150
17.4. Cookie-Kontrolle	152
17.4.1. Konfigurationsfenster	155
17.5. Skript-Kontrolle	156
17.5.1. Konfigurationsfenster	158
18. Instant Messaging (IM) Verschlüsselung	160
18.1. Verschlüsselung für bestimmte Benutzer deaktivieren	162
19. Prüfung auf Schwachstellen	163
19.1. Status	163
19.1.1. Schwachstellen beheben	164
19.2. Einstellungen	171
20. Spiele-/Laptop-Modus	173
20.1. Spiele-Modus	173
20.1.1. Automatischer Spiele-Modus konfigurieren	174
20.1.2. Spieliste verwalten	175
20.1.3. Einstellungen des Spiele-Modus konfigurieren	177
20.1.4. Tastenkombination für Spielmodus ändern	177
20.2. Laptop-Modus	178
20.2.1. Einstellungen des Laptop-Modus konfigurieren	179
21. Netzwerk	181
21.1. Dem BitDefender-Netzwerk beitreten	182
21.2. Computer zum BitDefender-Netzwerk hinzufügen	182
21.3. Das BitDefender-Netzwerk verwalten	184
22. Update (Aktualisierung)	187
22.1. Automatisches Update	187
22.1.1. Benutzergesteuertes Update	189
22.1.2. Automatisches Update deaktivieren	189
22.2. Update-Einstellungen	190
22.2.1. Update-Adresse	191
22.2.2. Automatisches Update konfigurieren	191
22.2.3. Manuelle Update Einstellungen	192
22.2.4. Weitere Einstellungen konfigurieren	192
22.2.5. Proxyverwaltung	192
23. Registrierung	195
23.1. BitDefender Antivirus 2009 registrieren	196
23.2. Ein BitDefender Benutzerkonto erstellen	197
Hilfe erhalten	201
24. Support	202
24.1. BitDefender Knowledge Base	202



24.2. Nach Hilfe fragen	203
24.2.1. Zur Web-Selbstbedienung gehen	203
24.2.2. Ein Supportticket öffnen	203
24.3. Kontaktinformation	204
24.3.1. Kontaktadressen	204
24.3.2. Niederlassungen	204
BitDefender Notfall CD	207
25. Übersicht	208
25.1. Systemanforderungen	208
25.2. Integrierte Software	209
26. BitDefender Notfall CD Anleitung	212
26.1. BitDefender Notfall CD starten	212
26.2. BitDefender Notfall CD stoppen	213
26.3. Wie führe ich einen Prüfvorgang durch?	214
26.4. Wie kann ich die Internetverbindung konfigurieren?	215
26.5. Wie kann ich BitDefender aktualisieren?	217
26.5.1. Wie kann ich BitDefender über einen Proxy-Server aktualisieren?	217
26.6. Wie sichere ich meine Daten?	218
Glossar	221



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.

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

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

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

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



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

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

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

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

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

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

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

URHEBERRECHT: Alle Rechte und geistigen Eigentumsrechte an BitDefender(einschließlich, aber nicht beschränkt auf Logos, Bilder, Fotografien,



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

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

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



DOKUMENTEN, ANZEIGEN ODER ÄHNLICHEM, UNABHÄNGIG DAVON, OB DIES AUFGRUND GESETZLICHER ANFORDERUNGEN, DER GESCHÄFTSTÄTIGKEIT, DES GEWOHNHEITSRECHTS UND DER PRAXIS ODER DES HANDELSGEBRAUCHS ERFOLGT.

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

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

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

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

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



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

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

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

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

BitDefender und alle zugehörigen Logos sind eingetragene Titel und Marken von BITDEFENDER. Alle anderen Marken und Titel sind Eigentum der jeweiligen Rechteinhaber.

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

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

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

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



Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer vorgesehen, die sich für **BitDefender Antivirus 2009** als Sicherheitslösung entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

Dieses Handbuch beschreibt wie **BitDefender Antivirus 2009** zu handhaben ist, das Unternehmen und das Team, das es konzipiert hat, es wird Sie durch den Installationsprozess führen und Ihnen zeigen wie das Produkt zu konfigurieren ist. Sie lernen wie man **BitDefender Antivirus 2009** benutzt, wie Sie es aktualisieren, testen und anpassen können. So können Sie das Beste aus BitDefender herausholen.

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



Erscheinungsbild	Beschreibung
<code>sample code listing</code>	Beispielquelltexte werden in einer Schriftart mit fester Laufweite angegeben.

1.2. Symbole

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



Anmerkung

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



Wichtig

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



Warnung

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

2. Struktur

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

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

Grundkonfiguration. Beschreibung der Grundkonfiguration und Wartung von BitDefender.

Erweiterte Administration. Eine detaillierte Beschreibung der Sicherheitsfähigkeiten von BitDefender. Ihnen wird beigebracht wie Sie die BitDefender Module einstellen



und verwenden um Ihren Computer gegen alle Arten von Malware zu schützen (Virus, Spyware, Rootkits und so weiter).

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

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

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

3. Ihre Mithilfe

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

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



Wichtig

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



BitDefender Antivirus 2009

Installation



1. Systemanforderungen

Sie können BitDefender Antivirus 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 Betriebssystem und Ihre Hardware zu erhalten, klicken Sie mit der rechten Maustaste **Arbeitsplatz** auf dem Desktop und wählen Sie **Eigenschaften** aus dem Menu.

1.1. Hardware-Anforderungen

Für Windows XP

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

Für Windows Vista

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

Für Windows Home Server

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



1.2. Software-Anforderungen

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

Der Antiphishingschutz arbeitet nur für:

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

Instant Messaging (IM) Verschlüsselung arbeitet nur für:

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



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.

1 Willkommen zum BitDefender Antivirus 2009 Assistent. BitDefender Total Scan und andere Funktionen sind aktiviert. Klicken Sie auf "Weiter".

2 Bitte warten. BitDefender prüft, ob eine neuere Version des Installationspaketes verfügbar ist. Wenn Sie bereits ein anderes Antivirus-Produkt installiert haben, wird die Installation von BitDefender unterbrochen. Klicken Sie auf "Weiter", um die Installation fortzuführen, oder auf "Nein", um die Installation abzubrechen.

3 BitDefender Antivirus 2009 - BETA. Endbenutzer-Software-Lizenzvertrag. Installieren Sie die Software nicht, wenn Sie diesen Lizenzbedingungen nicht zustimmen. Klicken Sie auf "Akzeptieren", "OK", "Weiter", "Ich verstehe nicht", "Nein" oder "Abbrechen".

4 Bitte wählen Sie den Installationsort aus. Klicken Sie auf "Durchsuchen", um einen neuen Installationsort auszuwählen. Pfad: C:\Program Files\BitDefender. Klicken Sie auf "Weiter", um mit der Installation fortzuführen, oder auf "Abbrechen", um den Assistenten zu beenden.

5 Bitte wählen Sie die Installationsoptionen aus. "Lies mich" dabei anzeigen. Verknüpfung auf dem Desktop erstellen. Klicken Sie auf "Installieren", um die Installation abzubrechen, oder auf "Abbrechen", um den Assistenten zu beenden.

6 Beenden des BitDefender Antivirus 2009 Assistenten. Klicken Sie auf "Fertigstellen", um den Assistenten zu schließen.

Installationsschritte



Folgen Sie diesen Schritten, um BitDefender Antivirus 2009 auf Ihrem PC zu installieren:

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

BitDefender 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 Antivirus 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 erstellen** - um ein Symbol von BitDefender Antivirus 2009 am Ende der Installation auf Ihrem Desktop zu speichern.
 - **CD nach Installation auswerfen** - um die CD nach Beenden der Installation auszuwerfen. Diese Option erscheint nur, wenn Sie von CD installieren.
 - **Ausschalten von Windows-Defender** - um den Windows-Defender zu deaktivieren; diese Option erscheint nur bei Windows Vista.



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

Bitte warten Sie bis der Installationsvorgang beendet wurde.

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



Wichtig

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

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

2.1. Registrierungsassistent

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

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



Anmerkung

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



2.1.1. Schritt 1/2 - BitDefender Antivirus 2009 registrieren

BitDefender Antivirus 2009

BitDefender Registrierungsassistent - Schritt 1 von 2

Schritt 1

Willkommen zum BitDefender Registrierungsassistent!

Dieser Assistent unterstützt Sie dabei Ihr Produkt zu registrieren und Ihr BitDefender-Konto zu aktivieren oder zu aktualisieren.

Ihr aktuelle Lizenzstatus bei BitDefender lautet: **Testversion**

Der aktuelle BitDefender Lizenzschlüssel ist: **704BE277EF7785580DF8**

Dieser Lizenzschlüssel wird ablaufen in: **30 Tag(e)**

Lizenzoptionen

Um den aktuellen Schlüssel zu behalten, wählen Sie bitte die erste Option. Um einen neuen Schlüssel hinzu zu fügen, wählen Sie bitte die zweite Option und tippen den Schlüssel in das Feld unten ein.

Weiterhin diesen Lizenzschlüssel verwenden

Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren

Neuen Lizenzschlüssel eingeben:

Lizenzschlüssel kaufen

Um eine BitDefender-Lizenz zu erwerben besuchen Sie bitte unseren Onlineshop unter:

Erneuern Sie Ihren BitDefender Lizenzschlüssel

Schritt 2

Hier finden Sie Ihre Lizenzschlüssel:

1) CD-Rom Kennzeichnung

2) Produkt-Registrierungskarte

3) E-Mail für den Online-Kauf

bitdefender

Zurück Weiter Abbrechen

Registrierung

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

BitDefender Antivirus 2009 registrieren:

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



Anmerkung

Sie finden den Lizenzschlüssel:

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



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

Klicken Sie auf **Weiter**.

2.1.2. Schritt 2/2 - BitDefender-Benutzerkonto erstellen

BitDefender Antivirus 2009

BitDefender Registrierungsassistent - Schritt 2 von 2

Schritt 1 | Schritt 2

Registrierung meines Kontos

Informationen über ein existierendes BitDefender Benutzerkonto wurden auf Ihrem PC gefunden. Das BitDefender Benutzerkonto gewährt Ihnen Zugriff zum technischen Support, zu Spezialangeboten und Sonderaktionen. Wenn Sie Ihren Lizenzschlüssel für BitDefender verlieren, können Sie ihn wiedererhalten, indem Sie sich unter <http://myaccount.bitdefender.com> einloggen. Sie können sich in ein existierendes BitDefender Benutzerkonto einloggen oder ein Neues erstellen.

In ein existierendes Benutzerkonto einloggen

E-Mail-Adresse:

Passwort:

[Passwort vergessen?](#)

Ein neues BitDefender Benutzerkonto erstellen

E-Mail-Adresse:

Passwort:

Passwort erneut eingeben:

Vorname:

Nachname:

Land:

Registrierung überspringen

Bitte senden Sie mir alle BitDefender Nachrichten

Bitte senden Sie mir die wichtigsten BitDefender Nachrichten

Ich möchte keine Nachrichten erhalten

Kontoerstellung

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

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



Wichtig

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

Ich habe noch kein BitDefender-Benutzerkonto

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

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

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

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

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

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

Klicken Sie auf **Fertigstellen**.

Ich habe bereits ein BitDefender Nutzerkonto.

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



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

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

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

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

Klicken Sie auf **Fertigstellen**.

2.2. Konfigurationsassistent

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

Ist ist nicht erforderlich den Assistenten abzuschließen. Dennoch empfehlen wir es Ihnen um Zeit zu sparen und um Ihr System zu sichern noch bevor BitDefender Antivirus 2009 vollständig installiert wurde.



Anmerkung

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



2.2.1. Schritt 1/8 - Begrüßungsfenster



Klicken Sie auf **Weiter**.



2.2.2. Schritt 2/8 - Auswahl der Ansichtmodi

BitDefender Antivirus 2009

BitDefender Konfigurationsassistent - Schritt 2 von 8

Schritt 1 Schritt 2 Schritt 3 Schritt 4 Schritt 5 Schritt 6 Schritt 7 Schritt 8

Ansichtmodus der Benutzeroberfläche

Sie können zwischen der der Basisansicht und der Profiansicht für BitDefender wählen, je nach Erfahrung die Sie mit unserem Produkt besitzen.

Basisansicht
Eine einfache Benutzeroberfläche mit der Sie einen Basiszugang zu allen Modulen haben. Sie können alle Angelegenheiten sehen, die die Sicherheit Ihres Systems betreffen.

Fortgeschrittene Ansicht
Eine erweiterte Benutzeroberfläche mit der Sie Zugriff auf jede einzelne Komponente des BitDefender Produktes haben. Sie werden fortgeschrittene Einstellungen so wird weitere Funktionen vornehmen können

Sie können jederzeit, während Sie BitDefender benutzen zwischen diesen Ansichten Wechslen

Klicken Sie hier um die Benutzeroberfläche von BitDefender auf Basisansicht einzustellen.

bitdefender Zurück Weiter Abbrechen

Ansichtmodi

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

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

Klicken Sie auf **Weiter**.



2.2.3. Schritt 3/8 - Konfigurieren Sie das BitDefender Netzwerk

BitDefender Antivirus 2009

BitDefender Konfigurationsassistent - Schritt 3 von 8

Schritt 1 Schritt 2 **Schritt 3** Schritt 4 Schritt 5 Schritt 6 Schritt 7 Schritt 8

Konfiguration der Home-Verwaltung

BitDefender 2009 beinhaltet eine neue Komponente, die Home-Verwaltung, mit der Sie ein virtuelles Netzwerk aus allen Computern in Ihrem Haushalt erstellen und alle BitDefender Produkte, die in diesem Netzwerk integriert sind, verwalten können. Sie können als Administrator eines Netzwerkes handeln, das Sie erstellen oder Sie können Teil eines Netzwerkes werden, das von einem anderen Computer erstellt und verwaltet wird.

Klicken Sie auf das untere Kontrollkästchen wenn Sie Teil des BitDefender Home-Netzwerkes werden wollen. Sie werden dazu aufgefordert ein Passwort für die Home-Verwaltung einzugeben, wodurch der Administrator des Netzwerkes die Möglichkeit erhält, die Einstellungen und Aktionen für BitDefender auf diesem Computer ferngesteuert zu kontrollieren.

Ich möchte ein Teil der BitDefender Home-Netzwerkes sein

Passwort für die Home-Verwaltung:

Passwort erneut eingeben:

Um mehr über jede Option, die auf der BitDefender Benutzeroberfläche angezeigt wird herauszufinden, bewegen Sie Ihre Maus über das Fenster. Ein entsprechender Hilfetext wird angezeigt.

Zurück **Weiter** **Abbrechen**

BitDefender Netzwerkkonfiguration

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

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

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



Wichtig

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

Klicken Sie auf **Weiter**.



Klicken Sie auf **Weiter**.

Erstellen von Regeln für die Identitätskontrolle

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

Identitätsregel hinzufügen

Name der Regel HTTP überprüfen

Art der Regel SMTP-Daten überprüfen

Daten der Regel Vergleiche ganze Wörter

Kasus vergleichen

Instant Messaging prüfen



Identitätskontrolle Regel

Hier können Sie die Parameter auswählen:

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



Anmerkung

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

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



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

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

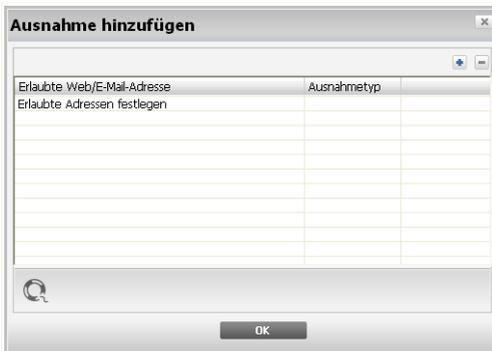
- **HTTP-Daten überprüfen** - prüft den HTTP (web) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
- **SMTP-Daten überprüfen** - prüft alle ausgehenden E-Mail-Nachrichten.
- **Instant Messaging überprüfen** - prüft den Instant Messaging Datenverkehr und blockiert ausgehende Nachrichten,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

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

Erstellen von Ausnahmen der Identitätskontrolle

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

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



Ausnahmen der Identitätskontrolle

Um eine Ausnahme zu erstellen befolgen Sie die folgenden Schritte:



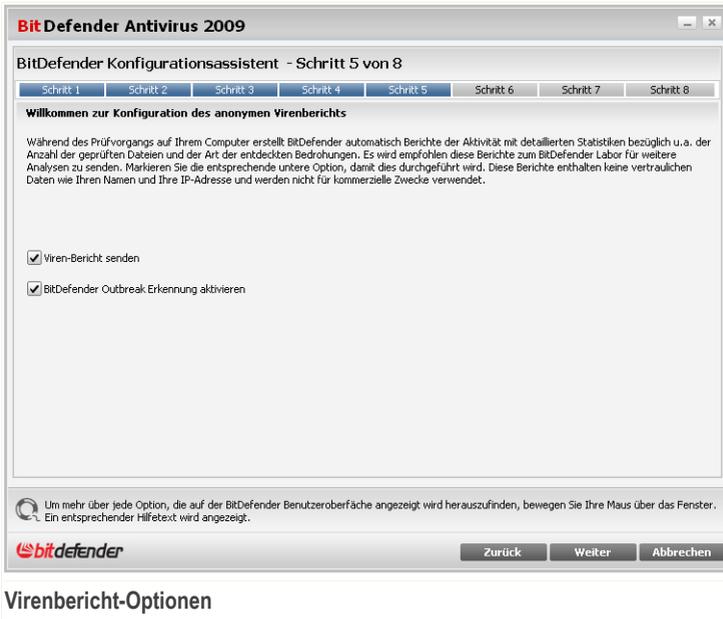
1. Klicken Sie auf die Schaltfläche  **Hinzufügen** um einen neuen Eintrag in die Tabelle hinzuzufügen.
2. Doppelklicken Sie auf **Entsprechende Ausnahme eingeben** und geben Sie die gewünschte Adresse zum Ausnehmen ein.
3. Doppelklicken Sie dann auf **Typ wählen** und wählen Sie den gewünschten Eintrag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

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

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



2.2.5. Schritt 5/8 - Virenberichte konfigurieren



Virenbericht-Optionen

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

Folgende Optionen können konfiguriert werden:

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



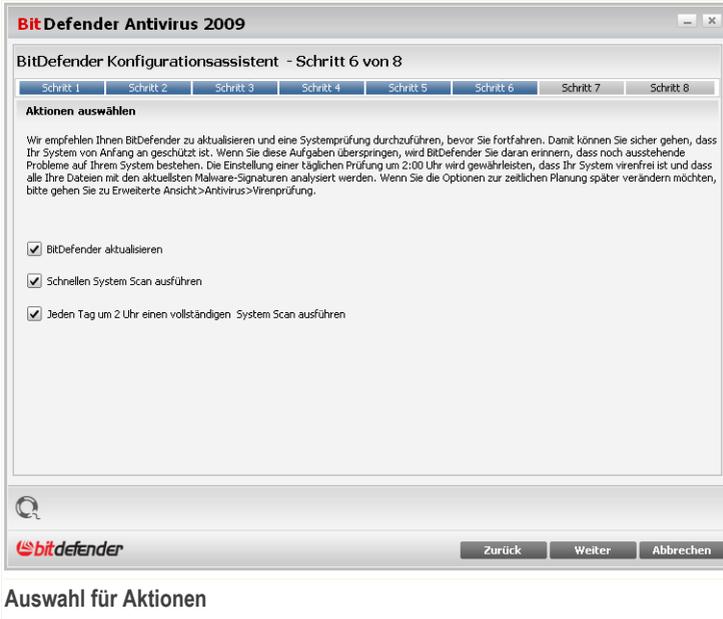
Anmerkung

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

Klicken Sie auf **Weiter**.



2.2.6. Schritt 6/8 - Aufgabentyp



Auswahl für Aktionen

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

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



Wichtig

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

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

Klicken Sie auf **Weiter**.

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

BitDefender Antivirus 2009

BitDefender Konfigurationsassistent - Schritt 7 von 8

Schritt 1 Schritt 2 Schritt 3 Schritt 4 Schritt 5 Schritt 6 Schritt 7 Schritt 8

BitDefender Update

BitDefender wird die während dem letzten Schritt ausgewählte Aufgabe durchführen. Unten können Sie den Status des Update-Prozesses beobachten. Sobald der Update-Prozess beendet ist, wird eine On-Demand-Prüfung starten. Sie können auf Weiter klicken, um den Assistenten zu beenden (Die Prüfaufgabe wird im Hintergrund ausgeführt)

Status: Update erfolgreich

Datei: 0 % 0 kb

Update gesamt: 0 % 0 kb

Zurück Weiter Abbrechen

Status

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

Klicken Sie auf **Weiter**.



2.2.8. Schritt 8/8 - Fertigstellen

BitDefender Antivirus 2009

BitDefender Konfigurationsassistent - Schritt 8 von 8

Schritt 1 Schritt 2 Schritt 3 Schritt 4 Schritt 5 Schritt 6 Schritt 7 Schritt 8

Fertigstellen

Vielen Dank das Sie BitDefender 2009 verwenden. Bitte klicken Sie im Hauptmenü auf die Registrierung-Schaltfläche um mehr Informationen zu Ihrem BitDefender-Benutzerkonto und dem Ablaufdatum Ihres aktuellen Lizenzschlüssels zu erhalten.

Während der letzten 30 Tage Ihrer BitDefender Lizenz werden die verbleibenden Tage im Dashboard im Hauptfenster angezeigt. Um eine neue BitDefender Lizenznummer zu erwerben klicken Sie auf die Kaufen-Schaltfläche im selben Fenster.

BitDefender Total Security 2009 wurde konfiguriert. Um das Produkt zu starten, doppelklicken Sie auf das rote BitDefender-Symbol in der Taskleiste. Im Modus Basisansicht, zeigt das Dashboard im Hauptfenster den allgemeinen Schutzstatus an sowie kritische Punkte, die Ihre Aufmerksamkeit erfordern. Für weitere Optionen, klicken Sie auf "Zu Erweiterter Ansicht wechseln" im gleichen Fenster.

Benutzerkonto öffnen (benötigt Internetverbindung)

Markieren Sie dieses Kontrollkästchen wenn Sie Ihr BitDefender Benutzerkonto nach der Fertigstellung des Assistenten öffnen möchten. Bitte beachten Sie, dass Sie Ihr Benutzerkonto bestätigen müssen, indem Sie die Bestätigungsmail öffnen, die zu Ihrer Adresse gesendet wurde.

bitdefender Zurück Fertigstellen Abbrechen

Fertigstellen

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

Klicken Sie auf **Fertigstellen**.



3. Upgrade

Um ein Upgrade auf BitDefender Antivirus 2009 durchzuführen, befolgen Sie die folgenden Schritte:

1. Wir empfehlen eine ältere Version von BitDefender zu entfernen. Für weitere Informationen benutzen Sie die Hilfedatei oder das Handbuch des Produktes.
2. Bitte starten Sie Ihren Computer neu.
3. Installieren Sie den BitDefender Antivirus 2009 wie es hier beschrieben ist: *„BitDefender installieren“ (S. 4).*



4. BitDefender reparieren oder entfernen

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

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

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

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

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

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

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



Anmerkung

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

Wenn Sie BitDefender entfernen wählen erscheint ein neues Fenster.



Wichtig

Nur Windows Vista! Nach dem entfernen von BitDefender sind Sie nicht länger vor Schädlingen wie z.B. Viren und Spyware geschützt. Wenn Sie Windows Defender nach der Deinstallation von BitDefender wieder aktivieren möchten selektieren Sie bitte die entsprechende Auswahl.

Klicken Sie auf **Entfernen** um BitDefender Antivirus 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**.

Während dem Entfernen ist ein Fehler aufgetreten

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



Grundkonfiguration



5. Erste Schritte

Sobald Sie BitDefender installiert haben ist Ihr Computer geschützt.

5.1. BitDefender Antivirus 2009 starten

Der erste Schritt besteht in dem Starten von BitDefender.

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

5.2. Ansichtmodus der Benutzeroberfläche

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

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



Anmerkung

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

5.2.1. Basisansicht

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



- 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	Öffnet das Fenster der erweiterten Ansicht. Hier können Sie die vollständige Liste der Module sehen und jede Komponente bis ins Detail konfigurieren. BitDefender wird Sie an diese Option erinnern, wenn Sie das nächste Mal die Benutzeroberfläche öffnen.
Status	Beinhaltet Informationen und hilft Ihnen Anfälligkeiten der Sicherheit Ihres Computers zu beheben.

- In der Mitte des Fensters befinden sich fünf Tabs.



Tab	Beschreibung
Dashboard	Zeigt wichtige Produktstatistiken und Ihren Registrierungsstatus an sowie Links zu den wichtigsten On-Demand Aufgaben.
Antivirus	Zeigt den Status des Antivirus-Moduls an, das Ihnen dabei hilft BitDefender auf dem neusten Stand und Ihren Computer virenfrei zu halten.
Antiphishing	Zeigt den Status des Antiphishing-Moduls an, das gewährleistet, dass alle Internetseiten, auf die Sie mit dem Internet Explorer oder Mozilla Firefox zugreifen sicher sind.
Schwachstellen	Zeigt den Status des Moduls Schwachstellen/Anfälligkeit an, das Ihnen dabei hilft die wichtigste Software auf Ihrem PC stets auf dem neusten Stand zu halten.
Netzwerk	Zeigt die Struktur des BitDefender Home-Netzwerkes an.

- Außerdem enthält die BitDefender Basisansicht mehrere nützliche Verknüpfungen.

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



5.2.2. Fortgeschrittene Ansicht

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

The screenshot shows the BitDefender Antivirus 2009 - Testversion interface. At the top, there is a red status bar with the text "STATUS: Es existieren 2 Warnungen" and a button "ALLE BEHEBEN". Below this, there are tabs for "Dashboard", "Einstellungen", and "SysInfo". The "Dashboard" tab is active, displaying a sidebar with navigation options like "Allgemein", "Antivirus", "Privatsphäre", etc. The main area is divided into sections: "Statistiken" (Statistics) showing "Geprüfte Dateien: 586", "Desinfizierte Dateien: 0", "Entdeckte Viren: 0", "Letzte Prüfung: Nie", and "Nächste Prüfung: Nie"; "Übersicht" (Overview) showing "Zuletzt am: 8/18/2008 8:31 PM", "Mein Konto: testare.automata@live.com", "Registrierung: Testversion", and "Läuft ab in: 30 Tage" with a progress bar; and "Dateiaktivität" (File Activity) with a grid chart. At the bottom, there is a note about the network module and a footer with the BitDefender logo and links like "Kaufen", "Benutzerkonto", "Registrieren", "Hilfe", "Support", "Ereignis".

Fortgeschrittene Ansicht

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

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



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

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

Modul	Beschreibung
Allgemein	Hier haben Sie Zugriff zu den allgemeinen Einstellungen. Sie können hier auch das Dashboard und detaillierte Systeminformationen betrachten.
Antivirus	Bietet Ihnen die Möglichkeit Ihr Virus-Schild und Prüfprozesse zu konfigurieren, Ausnahmen festzulegen und das Quarantäne-Modul zu konfigurieren.
Privatsphäre-Kontrolle	Bietet Ihnen die Möglichkeit Datendiebstahl von Ihrem Computer vorzubeugen und Ihre Privatsphäre zu schützen während Sie online sind.
Verschlüsselung	Bietet Ihnen die Möglichkeit Unterhaltungen über Yahoo und Windows Live (MSN) Messenger zu verschlüsseln.
Schwachstellen	Bietet Ihnen die Möglichkeit wichtige Software auf Ihrem PC stets auf dem neusten Stand zu halten.
Spiele-/Laptop-Modus	Bietet Ihnen die Möglichkeit voreingestellte Prüfaufgaben, während Ihr Laptop über einen Akku betrieben wird. Weiterhin können Pop-ups und Benachrichtigungen vermieden werden während Sie spielen.
Netzwerk	Bietet Ihnen die Möglichkeit mehrere Computer in Ihrem Haushalt zu verwalten und konfigurieren.
Update	Bietet Ihnen die Möglichkeit die neusten Updates zu erhalten, das Produkt zu aktualisieren und den Update-Prozess genau zu konfigurieren.



Modul	Beschreibung
Registrierung	Bietet Ihnen die Möglichkeit BitDefender Antivirus 2009 zu registrieren, einen Lizenzschlüssel zu wechseln oder ein BitDefender Benutzerkonto zu erstellen.

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

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

5.3. BitDefender Symbol im Infobereich der Taskleiste

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



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

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



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

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

5.4. Scanaktivitätsanzeige

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

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



Anmerkung

Die Aktivitätsanzeige benachrichtigt Sie wenn der Echtzeitschutz deaktiviert ist dadurch das in der **Dateizone** ein rotes Kreuz erscheint.



Sie können die **Aktivitätsanzeige** zum Prüfen von Objekten verwenden. Ziehen Sie die Objekte hierzu einfach mit der Maus auf die Anzeige und lassen Sie diese dann



los. Für weitere Informationen fahren Sie bitte fort mit „Prüfen per Drag & Drop“ (S. 119).

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

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

5.5. BitDefender Manuelle Prüfung

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

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



BitDefender Manuelle Prüfung

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



5.6. Spiele-Modus

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

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

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

5.6.1. Spielmodus benutzen

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

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



Wichtig

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

5.6.2. Tastenkombination für Spielmodus ändern

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

1. Klicken Sie auf **Zu erweiterter Ansicht wechseln** (wenn Sie sich in der **Basisansicht** befinden).
2. Klicken Sie auf **Spiele/Laptop Modus** in dem Menü auf der linken Seite.
3. Klicken Sie auf den Tab **Spiele-Modus**.
4. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**.
5. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :



- Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (`Strg`), Shift (`Shift`) oder Alt-Taste (`Alt`).
- Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

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



Anmerkung

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

5.7. Integration in Web-Browser

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

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

- Internet Explorer
- Mozilla Firefox

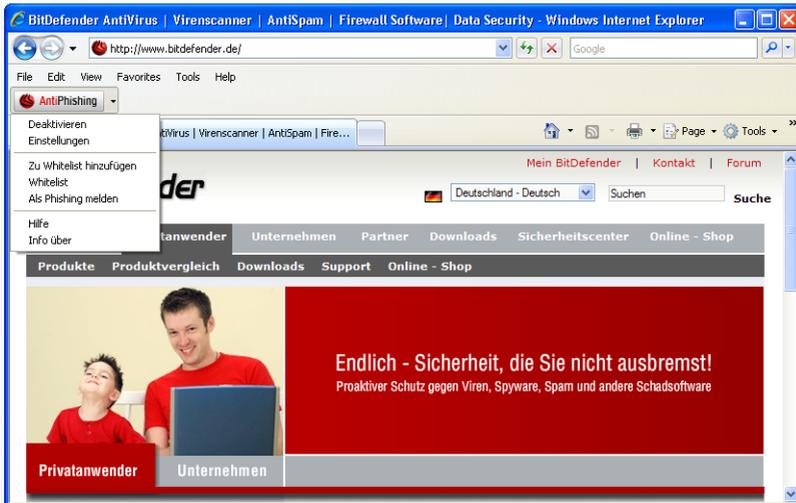
Sie können die Antiphishingeinstellungen und die Whitelist leicht und effizient über die BitDefender Antiphishingleiste in den oben genannten Browsern verwalten.

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



Anmerkung

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



Antiphishingleiste

Folgende Aktionen stehen in der Leiste zur Verfügung:

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



Anmerkung

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

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

Die folgenden Optionen sind verfügbar:

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



Anmerkung

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



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

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

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

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

■ **Hilfe** - Öffnet die Hilfedatei.

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

5.8. Integration in Messenger

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

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

- Ihr Chatpartner hat eine BitDefender Verison installiert, die die IM-Verschlüsselung unterstützt und die IM-Verschlüsselung ist für die Instant Messaging Anwendung aktiviert, die verwendet wird.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.



Wichtig

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

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

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



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



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



6. Dashboard

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

BitDefender Antivirus 2009 - Testversion EINSTELLUNGEN ZUR PROFIANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

DASHBOARD ANTIVIRUS **WICHTIGE WARNUNG** ANTIPHISHING **GESCHÜTZT** ANFÄLLIGKEIT **GESCHÜTZT** NETZWERK

Status

Mein allgemeiner Computer-Status:
WICHTIGE WARNUNG
 Es existieren **2 Probleme** die die Sicherheit Ihres Systems betreffen.
 ALLE BEHEBEN

Aufgaben

- Jetzt aktualisieren
- Systemprüfung
- Tiefgehende Prüfung

Übersicht

Registrierung:	Testversion	Zuletzt am:	8/18/2008	8:31 PM
Läuft ab in:	<div style="width: 100%; height: 10px; background-color: green;"></div>	Letzte Prüfung:	Nie	
	30 Tage	Nächste Prüfung:	Nie	

Das Dashboard-Modul zeigt umfangreiche Produktstatistiken und Ihren Registrierungsstatus an, sowie Links zu den wichtigsten On-Demand Aufgaben.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Dashboard

6.1. Übersicht

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

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



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

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

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

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



Anmerkung

Die hier eingetragenen Daten bleiben vertraulich.

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

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

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

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



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

6.2. Aufgaben

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

Folgende Aktionen stehen zur Verfügung:

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

6.2.1. Prüfen mit BitDefender

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

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



Anmerkung

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

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

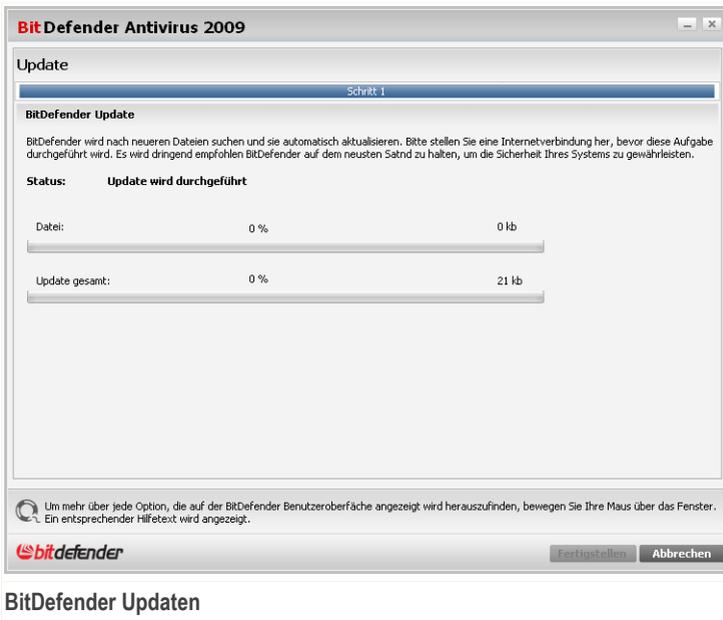


Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

6.2.2. BitDefender Updates

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:



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. Antivirus

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**.

BitDefender Antivirus 2009 - Testversion

EINSTELLUNGEN ZUR PROFIANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

DASHBOARD ANTIVIRUS WICHTIGE WARUNG ANTIIPHISHING GESCHÜTZT ANFÄLLIGKEIT GESCHÜTZT NETZWERK

Überwachte Komponenten Alle Erweitern/Verkleinern Aufgaben

	Überwachen	Status
Lokale Sicherheit		
Echtzeit-Schutz für Dateien ist aktiviert	<input checked="" type="checkbox"/> Ja	OK
Sie haben Ihren Computer niemals auf Malware geprüft	<input checked="" type="checkbox"/> Ja	Beheben
Automatisches Update ist deaktiviert	<input checked="" type="checkbox"/> Ja	Beheben

→ Jetzt aktualisieren
→ Prüfe meine Dokumente
→ Systemprüfung
→ Tiefgehende Prüfung

Diese Komponente zeigt den Status des Antivirus-Schutzes auf Ihrem System an, sowie Links zu wichtigsten Prüfaufgaben.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Antivirus

Das Antivirus-Modul besteht aus zwei Bereichen:

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

7.1. Überwachte Komponenten

Die überwachte Komponente ist die folgende:



Kategorie	Beschreibung
Lokale Sicherheit	Hier können Sie den Status jedes Sicherheitsmoduls überprüfen, das Objekte auf Ihrem Computer schützt (Dateien, Registry, Speicher, usw).

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

7.1.1. Lokale Sicherheit

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

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

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

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



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

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

7.2. Aufgaben

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

Folgende Aktionen stehen zur Verfügung:

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

7.2.1. Prüfen mit BitDefender

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

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



Aufgabe	Beschreibung
	sicheren Arbeitsbereich und saubere Anwendungen die beim Start ausgeführt werden.



Anmerkung

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

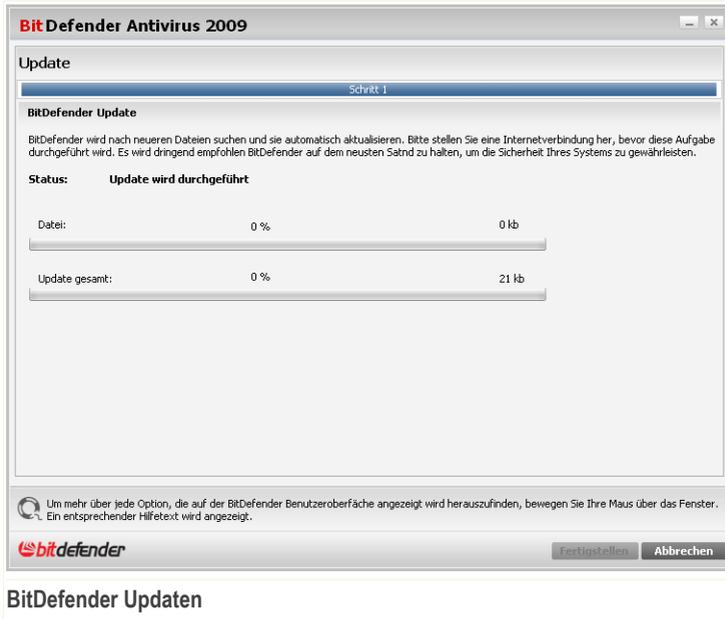
Wenn Sie einen Prüfvorgang, ob schneller oder kompletter Vorgang, starten wird der BitDefender Scanner geöffnet.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

7.2.2. BitDefender Updaten

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

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



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.



8. Antiphishing

BitDefender verfügt über ein Antiphishing-Modul, das gewährleistet, dass alle Internetseiten, auf die über den Internet Explorer oder Firefox zugegriffen wird sicher sind.

Um das Antiphishing-Modul zu aktivieren, klicken Sie auf den Tab **Antiphishing**.

The screenshot shows the BitDefender Antivirus 2009 - Testversion interface. At the top, there is a red status bar indicating "STATUS: Es existieren 2 Warnungen" and a button "ALLE BEHEBEN". Below this, there are five main tabs: DASHBOARD, ANTIVIRUS (with a red "WICHTIGE WARUNG" label), ANTIPHISHING (with a green "GESCHÜTZT" label), ANFÄLLIGKEIT (with a green "GESCHÜTZT" label), and NETZWERK. The ANTIPHISHING tab is selected. The main area is divided into "Überwachte Komponenten" and "Aufgaben". Under "Überwachte Komponenten", there is a list with "Online Sicherheit" selected. Under "Aufgaben", there are buttons for "Jetzt aktualisieren", "Systemprüfung", and "Tiefgehende Prüfung". At the bottom, there is a note: "Diese Komponente zeigt den Status des Antiphishing-Schutzes auf Ihrem System an, der den HTTP und IM-Datenverkehr auf Phishingversuche filtert." and the BitDefender logo with links for "Kaufen", "Benutzerkonto", "Registrieren", "Hilfe", "Support", and "Ereignis".

Das Antiphishing-Modul besteht aus zwei Bereichen:

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

8.1. Überwachte Komponenten

Die überwachte Komponente ist die folgende:



Kategorie	Beschreibung
Online-Sicherheit	Hier können Sie den Status jedes Sicherheitsmoduls überprüfen, das Ihre Online-Transaktionen und Ihren Computer schützt, während Sie im Internet sind.

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

8.1.1. Online Sicherheit

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

Risiko	Beschreibung
Gesprächverschlüsselung für IM ist aktiviert	Wenn Ihre IM-Kontakte BitDefender 2009 installiert haben, so werden alle IM-Unterhaltungen über Yahoo! Messenger und Windows Live Messenger verschlüsselt. Es wird empfohlen die Unterhaltung über IM zu verschlüsseln, damit diese privat bleiben.
Firefox Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.
Internet Explorer Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.

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

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

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



8.2. Aufgaben

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

Folgende Aktionen stehen zur Verfügung:

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

8.2.1. Prüfen mit BitDefender

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

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



Anmerkung

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



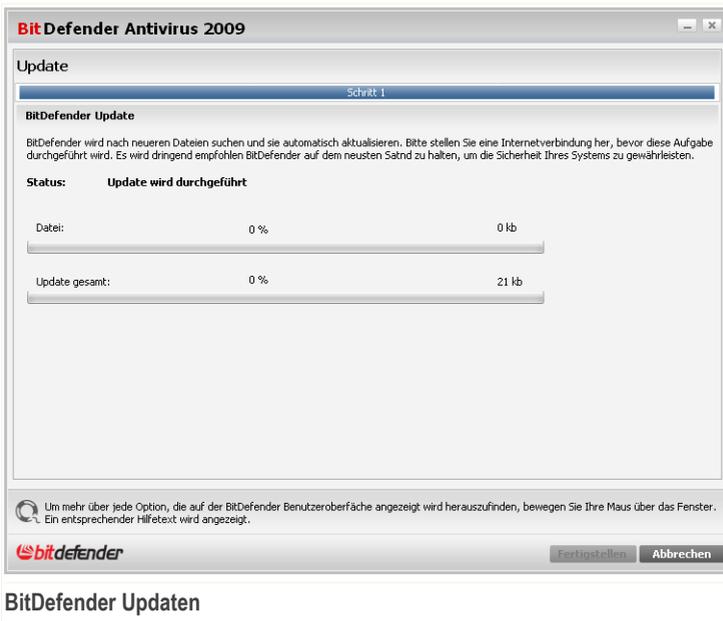
Wenn Sie einen Prüfvorgang, ob schneller oder kompletter Vorgang, starten wird der BitDefender Scanner geöffnet.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

8.2.2. BitDefender Updates

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:



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



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

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



Anmerkung

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

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

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

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



9. Prüfung auf Schwachstellen

BitDefender beinhaltet ein Schwachstellen-Modul, das Ihnen dabei hilft, wichtige Daten auf Ihrem Computer auf dem neusten Stand zu halten.

Um Schwachstellen-Modul zu öffnen, klicken Sie auf den Tab **Schwachstellen**

The screenshot shows the BitDefender Antivirus 2009 interface. At the top, there is a status bar indicating 'STATUS: Es existieren 2 Warnungen' (Status: There are 2 warnings) and a button 'ALLE BEHEBEN' (Fix all). Below this are several navigation tabs: DASHBOARD, ANTIVIRUS (with a 'WICHTIGE WARUNG' - Important warning), ANTIPHISHING (with 'GESCHÜTZT' - Protected), ANFÄLLIGKEIT (with 'GESCHÜTZT' - Protected), and NETZWERK (Network). The main area is divided into 'Überwachte Komponenten' (Monitored components) and 'Aufgaben' (Tasks). Under 'Überwachte Komponenten', the 'Prüfung auf Schwachstellen' (Vulnerability Check) component is selected, showing an 'OK' status. A description below states: 'Diese Komponente zeigt den Status der Anfälligkeit an, damit Sie überprüfen können ob wichtige Anwendungen auf Ihrem Computer auf dem neusten Stand sind.' (This component shows the status of vulnerability so you can check if important applications on your computer are up to date). At the bottom, there is a footer with the BitDefender logo and links for 'Kaufen' (Buy), 'Benutzerkonto' (User account), 'Registrieren' (Register), 'Hilfe' (Help), 'Support', and 'Ereignis' (Event).

Das Schwachstellen-Modul besteht aus zwei Bereichen:

- **Überwachte Komponenten** - Hier sehen Sie die vollständige Liste der überwachten Komponenten für jedes Sicherheitsmodul. Sie können auswählen, welche Module überwacht werden sollen. Es wird empfohlen alle Komponenten zu überwachen.
- **Aufgaben** - Hier finden Sie einen Link zu einem der wichtigsten Sicherheitsaufgaben.

9.1. Überwachte Komponenten

Die überwachte Komponente ist die folgende:



Kategorie	Beschreibung
Anfälligkeitsprüfung	Hier können Sie überprüfen, ob wichtige Software auf Ihrem PC auf dem neusten Stand ist. Passwörter von Windows Benutzerkonten werden nach den Sicherheitsregeln überprüft.

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

9.1.1. Schwachstellen-Scan

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

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

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

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



2. Sollte ein Problem nicht direkt behoben werden so folgen Sie den Anweisungen auf dem Bildschirm.

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

9.2. Aufgaben

Hier finden Sie einen Link zu einer der wichtigsten Sicherheitsaufgaben.

Die folgende Schaltfläche steht zur Verfügung:

- **Prüfung auf Schwachstellen**

9.2.1. Prüfung auf Schwachstellen/Anfälligkeit

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

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



Schritt 1/6 - Auswahl der zu prüfenden Schwachstellen

BitDefender Total Security 2009

BitDefender Assistent für Schwachstellen-Prüfung

1. Schritt 2. Schritt 3. Schritt 4. Schritt Schritt 5 Schritt 6

Aufgaben auswählen

Dieser Assistent wird Sie durch die erforderlichen Aktionen führen um Anwendungen zu erkennen die nicht mehr auf dem neusten Stand sind und Windows-Benutzerkonten mit einem schwachen Passwort. Bitte wählen Sie aus der unteren Liste, welche Objekte auf Schwachstellen geprüft werden sollen.

- Passwörter für Windows-Benutzerkonten jetzt prüfen
- Auf Anwendungs-Updates prüfen
- Auf wichtige Windows-Updates prüfen
- Auf optionale Windows-Updates prüfen

 Markieren Sie dieses Kontrollkästchen, damit BitDefender die Passwörter der Windows Benutzerkonten auf Ihrem Computer überprüft: Diese Passwörter sollten Buchstaben, Zahlen und Zeichen enthalten, um einen ausreichenden Schutz zu bieten.

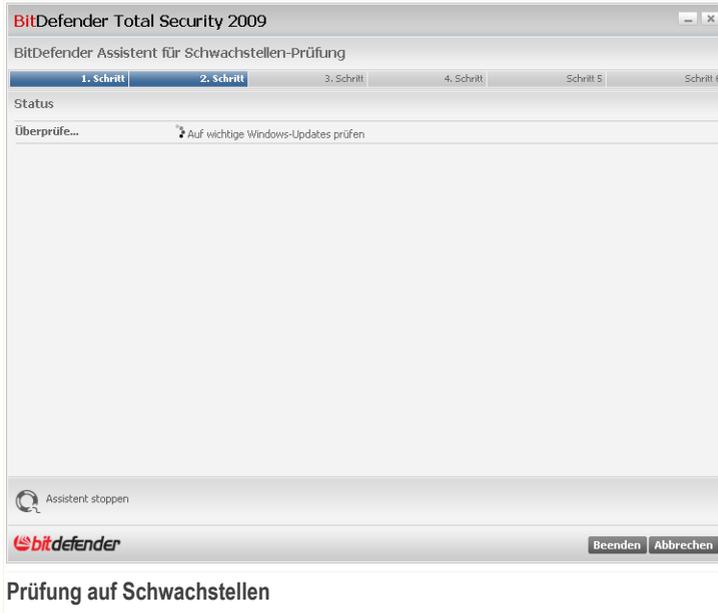
 Weiter Abbrechen

Schwachstellen

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



Schritt 2/6 - Nach Schwachstellen suchen



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



Schritt 3/6 - Unsicheres Passwort ändern

BitDefender Total Security 2009

BitDefender Assistent für Schwachstellen-Prüfung

1. Schritt | 2. Schritt | 3. Schritt | 4. Schritt | Schritt 5 | Schritt 6

Passwörter für Windows-Benutzerkonten jetzt prüfen

Benutzername	Festigkeit	Status
Administrator	Strong	Ok
amirea	Strong	Ok

Dies ist eine Liste der eingestellten Passwörter der Windows Benutzerkonten auf Ihrem Computer und die Sicherheitsstufe, die sie darstellen. Klicken Sie auf die Schaltfläche "Feststellen" um unsichere Passwörter zu ändern.

bitdefender

Weiter Abbrechen

Passwörter von Benutzern

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

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

BitDefender

Choose method to fix:

Force user to change password at next login

Change user password

Type password:

Confirm password:

OK Close

Passwort ändern



Wählen Sie die Methode um ein Problem zu beheben:

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



Anmerkung

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

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

Klicken Sie auf **Weiter**.



Schritt 4/6 - Anwendungen aktualisieren

The screenshot shows the BitDefender Total Security 2009 interface during a vulnerability check. The window title is "BitDefender Total Security 2009" and the subtitle is "BitDefender Assistent für Schwachstellen-Prüfung". The progress bar indicates "4. Schritt" (Step 4) is active, with other steps labeled "1. Schritt", "2. Schritt", "3. Schritt", "Schritt 5", and "Schritt 6".

The main content area is titled "Auf Anwendungs-Updates prüfen" (Check for application updates) and contains a table with the following data:

Anwendung	Installierte Version	Aktuellste Version	Status
Adobe Reader	8.1.2	8.1.2	Auf dem neusten Stand
Yahoo! Messenger	8.1.0.421	8.1.0.241	Auf dem neusten Stand
Firefox	3.0 (en-US)	3.0 (en-US)	Auf dem neusten Stand

Below the table, there is a search icon and the text: "Dies ist eine Liste der Anwendungen, die von BitDefender unterstützt werden und der verfügbaren Updates (falls vorhanden)." At the bottom of the window, there is the BitDefender logo and two buttons: "Weiter" (Next) and "Abbrechen" (Cancel).

Anwendungen

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

Klicken Sie auf **Weiter**.



Schritt 5/6 - Windows aktualisieren

The screenshot shows the BitDefender Total Security 2009 interface during a vulnerability check. The window title is "BitDefender Total Security 2009" and the subtitle is "BitDefender Assistent für Schwachstellen-Prüfung". The progress bar indicates "Schritt 5" of 6 steps. The main content area is titled "Windows Updates" and contains a list of updates under the heading "Auf wichtige Windows-Updates prüfen". The list includes updates for Windows XP, Microsoft XML Core Services, .NET Framework, and Outlook Express. At the bottom of the list, there is a button labeled "Alle System-Updates installieren". Below the list, there is a search icon and the text "Dies ist eine Liste der wichtigen und weniger wichtigen Updates für Windows-Anwendungen". The BitDefender logo is visible in the bottom left corner, and "Weiter" and "Abbrechen" buttons are in the bottom right corner.

Windows Updates

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

Klicken Sie auf **Weiter**.



Schritt 6/6 - Ergebnisse betrachten

The screenshot shows a window titled "BitDefender Total Security 2009" with a subtitle "BitDefender Assistent für Schwachstellen-Prüfung". The window has a progress bar at the top with six steps: "1. Schritt", "2. Schritt", "3. Schritt", "4. Schritt", "Schritt 5", and "Schritt 6". The "Schritt 6" tab is active. The main content area displays a message: "Die Prüfung auf Schwachstellen wurde abgeschlossen, doch keine Updates wurden installiert. Es ist wichtig, dass alle Anwendungen stets auf dem neusten Stand sind." Below this message is a small circular icon with a magnifying glass and the text: "Die Prüfung auf Schwachstellen wurde abgeschlossen, doch keine Updates wurden installiert. Es ist wichtig, dass alle Anwendungen stets auf dem neusten Stand sind." At the bottom left of the window is the BitDefender logo, and at the bottom right is a button labeled "Schliessen".

Ergebnisse

Klicken Sie auf **Schließen**.



10. Netzwerk

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

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

BitDefender Antivirus 2009 - Testversion

EINSTELLUNGEN ZUR PROFIANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

DASHBOARD ANTIVIRUS WICHTIGE WARUNG ANTIPHISHING GESCHÜTZT ANFÄLLIGKEIT GESCHÜTZT NETZWERK

INTERNET 10.10.0.1

Aufgaben

→ Netzwerk

Kein PC (Klicken Sie hier um hinzuzufügen)

Das Netzwerk-Modul zeigt die BitDefender Home-Netzwerkstruktur an (grau hinterlegt, falls das Home-Netzwerk nicht konfiguriert sein sollte). Klicken Sie auf "Netzwerk" um mit der Erstellung eines Home-Netzwerkes zu beginnen.

bitdefender

Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Netzwerk

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

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



10.1. Aufgaben

Anfangs steht nur eine Schaltfläche zur Verfügung.

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

Nach dem Beitreten zum Netzwerk werden mehrere Schaltflächen erscheinen.

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

10.1.1. Dem BitDefender-Netzwerk beitreten

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

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

BitDefender

Passwort eingeben

Aus Sicherheitsgründen ist ein Passwort erforderlich um einem Netzwerk beizutreten oder ein Neues zu erstellen. (Es schützt den Zugriff auf Ihren Computer über das Netzwerk)

Passwort eingeben:

Passwort wiederholen:

OK Abbrechen

Passwort konfigurieren

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



Sie sehen den Namen des Computers in der Netzwerkübersicht.

10.1.2. Computer zum BitDefender-Netzwerk hinzufügen

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

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

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

The screenshot shows a dialog box titled "BitDefender". The main text reads "Sie müssen ein Passwort für die Home-Verwaltung eingeben." Below this is a label "Passwort:" followed by a text input field. At the bottom left, there is a checkbox with the text "Die Nachricht in dieser Sitzung nicht erneut anzeigen." At the bottom right, there are two buttons: "OK" and "Abbrechen".

Passwort eingeben

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



Computer hinzufügen

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

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

3. Sie können hierzu eine der folgenden Methoden wählen:

- Wählen Sie aus der Liste den Namen des Computers der hinzugefügt werden soll:
- Geben Sie die IP-Adresse oder den Namen des Computers, der hinzugefügt werden soll in das dafür vorgesehene Feld ein.

4. Klicken Sie auf **Hinzufügen**. Sie werden dazu aufgefordert, das Passwort der Home-Verwaltung für den entsprechenden Computer einzugeben.



The screenshot shows a dialog box titled "BitDefender". The main text reads "Sie müssen ein Passwort für die Home-Verwaltung eingeben." Below this is a text input field labeled "Passwort:". Underneath the input field is a checkbox with the text "Die Nachricht in dieser Sitzung nicht erneut anzeigen." At the bottom of the dialog are two buttons: "OK" and "Abbrechen". Below the dialog box, the word "Authentifizieren" is written in a bold font.

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



Anmerkung

Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

10.1.3. Das BitDefender-Netzwerk verwalten

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



Netzwerkübersicht

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

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

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



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

The screenshot shows a dialog box titled "BitDefender". The main text reads "Sie müssen ein Passwort für die Home-Verwaltung eingeben." Below this is a label "Passwort:" followed by a text input field. At the bottom left, there is a checkbox with the text "Die Nachricht in dieser Sitzung nicht erneut anzeigen." At the bottom right, there are two buttons: "OK" and "Abbrechen".

Passwort eingeben

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



Anmerkung

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

10.1.4. Alle Computer prüfen

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

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

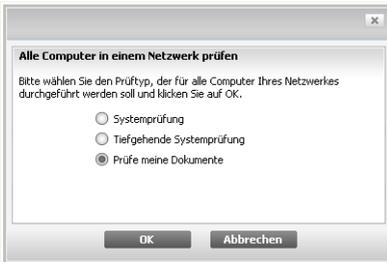
This is an identical screenshot to the one above, showing the BitDefender password prompt dialog box with the text "Sie müssen ein Passwort für die Home-Verwaltung eingeben.", a password input field, a checkbox for "Die Nachricht in dieser Sitzung nicht erneut anzeigen.", and "OK" and "Abbrechen" buttons.

Passwort eingeben



2. Wählen Sie eine Prüfarm.

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



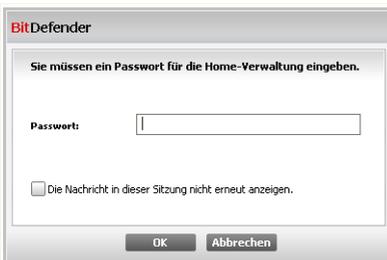
Prüfarm wählen

3. Klicken Sie auf **OK**.

10.1.5. Alle Computer aktualisieren

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

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



Passwort eingeben



2. Klicken Sie auf **OK**.

10.1.6. Alle Computer registrieren

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

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

The screenshot shows a dialog box titled "BitDefender". The main text reads "Sie müssen ein Passwort für die Home-Verwaltung eingeben." Below this is a label "Passwort:" followed by a text input field. At the bottom left, there is a checkbox with the text "Die Nachricht in dieser Sitzung nicht erneut anzeigen." At the bottom right, there are two buttons: "OK" and "Abbrechen".

Passwort eingeben

2. Geben Sie den Lizenzschlüssel zur Registrierung ein.

The screenshot shows a dialog box titled "Computer registrieren". The main text reads "Geben Sie den Lizenzschlüssel ein, mit dem Sie sich registrieren möchten". Below this is a label "Ihr Lizenzschlüssel:" followed by a text input field. At the bottom, there are two buttons: "OK" and "Abbrechen".

Alle Registrieren

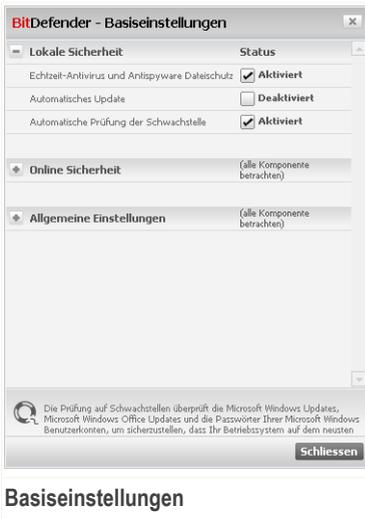
3. Klicken Sie auf **OK**.



11. Basiseinstellungen

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

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



Basiseinstellungen

Die verfügbaren Sicherheitsmodule wurden in mehrere Kategorien unterteilt.

Kategorie	Beschreibung
Lokale Sicherheit	Hier können Sie den Echtzeit-Schutz und das automatische Update (de)aktivieren.
Online-Sicherheit	Hier können Sie den Echtzeit-Mail- und Webschutz aktivieren/deaktivieren.
Allgemeine Einstellungen	Hier können Sie den Spiele-Modus, Laptop-Modus, Paswörter, die Prüfkativitätsleiste und mehr (de)aktivieren.

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



11.1. Lokale Sicherheit

Sie können die Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.

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

11.2. Online Sicherheit

Sie können die Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.

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

11.3. Allgemeine Einstellungen

Sie können alle Sicherheitsmodule mit einem Klick aktivieren/deaktivieren.



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



12. Statusleiste

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

Der Sicherheitsstatus zeigt Ihnen eine systematisch organisierte Liste von Sicherheitsrisiken auf Ihrem Computer. BitDefender Antivirus 2009 wird Ihnen mitteilen wenn ein Sicherheitsrisiko auftreten könnte.



Statusleiste

12.1. Lokale Sicherheit

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



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

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

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

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

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

12.2. Online Sicherheit

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



Risiko	Beschreibung
Gesprächsverschlüsselung für IM ist aktiviert	Wenn Ihre IM-Kontakte BitDefender 2009 installiert haben, so werden alle IM-Unterhaltungen über Yahoo! Messenger und Windows Live Messenger verschlüsselt. Es wird empfohlen die Unterhaltung über IM zu verschlüsseln, damit diese privat bleiben.
Firefox Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.
Internet Explorer Antiphishing-Schutz ist aktiviert	BitDefender schützt Sie während des Surfens vor Phishingversuchen.

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

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

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

12.3. Schwachstellen-Scan

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

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



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

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

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

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



13. Registrierung

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

13.1. Schritt 1/1 - BitDefender Antivirus 2009 registrieren

BitDefender Antivirus 2009

Registrierungsassistent

Schritt 1

Willkommen zum BitDefender Registrierungsassistent!

Dieser Assistent unterstützt Sie dabei Ihr Produkt zu registrieren und Ihr BitDefender-Konto zu aktivieren oder zu aktualisieren.

Ihr aktuelle Lizenzstatus bei BitDefender lautet: **Testversion**

Der aktuelle BitDefender Lizenzschlüssel ist: **704BE277EF7785580DF8**

Dieser Lizenzschlüssel wird ablaufen in: **30 Tag(e)**

Lizenzoptionen

If you want to keep the current key, please select the first option. If you want to add a new key, please select the second option and fill the key in the box below.

Weiterhin diesen Lizenzschlüssel verwenden

Ich möchte das Produkt mit einem neuen Lizenzschlüssel registrieren

Neuen Lizenzschlüssel eingeben:

Lizenzschlüssel kaufen

Um eine BitDefender-Lizenz zu erwerben besuchen Sie bitte unseren Onlineshop unter:
Erneuern Sie Ihren BitDefender Lizenzschlüssel

Hier finden Sie Ihre Lizenzschlüssel:

- 1) CD-Rom Kennzeichnung
- 2) Produkt-Registrierungskarte
- 3) E-Mail für den Online-Kauf

bitdefender Fertigstellen Abbrechen

Registrierung

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

BitDefender Antivirus 2009 registrieren:



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



Anmerkung

Sie finden den Lizenzschlüssel:

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

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

Klicken Sie auf **Fertigstellen**.



14. Ereignis

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

The screenshot shows the 'Historie & Ereignis Modul' window in BitDefender. It is divided into two main sections: 'Antivirus' and 'On-Demand Aufgaben'. The 'Antivirus' section contains a table with columns for 'Name der Aktion', 'Durchgeführte Aktion', and 'Datum und Zeit'. The 'On-Demand Aufgaben' section contains a table with columns for 'Name der Aktion', 'Aufgabenname', and 'Datum und Zeit'. Below the tables, there is a help text and a footer with the BitDefender logo and buttons for 'Liste löschen', 'Aktualisieren', and 'OK'.

Antivirus	
Name der Aktion	Durchgeführte Aktion
! Antivirus	Aktiviert
! Antivirus	Deaktiviert
! Antivirus	Aktiviert
! Antivirus	Deaktiviert
! Antivirus	Aktiviert
! Antivirus	Deaktiviert
! Antivirus	Aktiviert
! Antivirus	Deaktiviert
! Antivirus	Aktiviert

On-Demand Aufgaben		
Name der Aktion	Aufgabenname	Datum und Zeit
! Prüfvorgang abgeschlossen...	1159	8/19/2008 10:13:58 AM
! Prüfvorgang abgeschlossen...	1159	8/19/2008 10:13:28 AM
! Prüfvorgang abgeschlossen...	1159	8/19/2008 10:13:01 AM
! Prüfvorgang abgeschlossen...	1159	8/19/2008 10:12:27 AM
! Prüfvorgang abgebrochen.	Manuelle Prüfung	8/19/2008 10:10:05 AM
! Prüfvorgang abgebrochen.	Prüfvorgang des Aus...	8/19/2008 10:07:48 AM
! Prüfvorgang abgebrochen.	Prüfvorgang des Aus...	8/19/2008 10:03:09 AM
! Prüfvorgang abgebrochen.	Meine Dokumente	8/19/2008 10:00:59 AM
! Prüfvorgang abgebrochen.	Schnelle Systemprüf...	8/19/2008 10:00:51 AM

Ereignisanzeige

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

- Antivirus
- Privatsphäre
- Update
- Netzwerk



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

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



Erweiterte Administration



15. Allgemein

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

15.1. Dashboard

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

BitDefender Antivirus 2009 - Testversion [ZUR BASISANSICHT WECHSELN]

STATUS: Es existieren 2 Warnungen [ALLE BEHEBEN]

Dashboard | Einstellungen | SysInfo

Allgemein

- Antivirus
- Privatsphäre
- Prüfung auf Schwachstellen
- Verschlüsselung
- Spiele-/Laptop-Modus
- Netzwerk
- Update
- Registrierung

Statistiken

Geprüfte Dateien:	586
Desinfizierte Dateien:	0
Entdeckte Viren:	0
Letzte Prüfung:	Nie
Nächste Prüfung:	Nie

Übersicht

Zuletzt am:	8/18/2008 8:31 PM
Mein Konto:	testare_automata@live.com
Registrierung:	Testversion
Läuft ab in:	<div style="width: 100%; height: 10px; background-color: green;"></div> 30 Tage

Dateiaktivität

Das Netzwerk-Modul zeigt die BitDefender Home-Netzwerkstruktur an (grau hinterlegt, falls das Home-Netzwerk nicht konfiguriert sein sollte). Klicken Sie auf 'Netzwerk' um mit der Erstellung Ihres Home-Netzwerks zu beginnen.

bitdefender [Kaufen](#) - [Benutzerkonto](#) - [Registrieren](#) - [Hilfe](#) - [Support](#) - [Ereignis](#)

Dashboard

Das Dashboard besteht aus mehreren Bereichen:

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



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

15.1.1. Statistik

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

Objekt	Beschreibung
Überprüfte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung auf Malware überprüft wurden.
Desinfizierte Dateien	Zeigt die Anzahl der Dateien an, die während der letzten Prüfung desinfiziert wurden.
Entdeckte Viren	Zeigt die Anzahl der Viren an, die während der letzten Prüfung auf Ihrem System gefunden wurden.

15.1.2. Übersicht

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

Objekt	Beschreibung
Letztes Update	Zeigt das Datum an, zu dem Ihr BitDefender Produkt zuletzt aktualisiert wurde. Bitte führen Sie regelmäßig Updates durch, damit Ihr System vollständig geschützt ist.
Mein Benutzerkonto	Zeigt die E-Mail-Adresse an, die Sie benutzen können, um auf Ihr Online-Benutzerkonto zugreifen zu können, um Ihren Lizenzschlüssel zu erhalten und vom BitDefender Support und anderen Services profitieren zu können.
Registrierung	Zeigt Ihren Lizenzschlüssel und dessen Status an. Damit Ihr System sicher ist, müssen Sie BitDefender erneuern



Objekt	Beschreibung
	oder aktualisieren, wenn der Lizenzschlüssel abgelaufen ist.
Läuft ab in	Die Anzahl der Tage bis zum Ende des Lizenzschlüssels.

15.2. Einstellungen

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

Allgemeine Einstellungen

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



15.2.1. Allgemeine Einstellungen

- **Passwortschutz für Programm-Einstellung aktivieren** - die Passwort-Einstellung aktivieren, um Ihre BitDefender-Einstellungen zu schützen.



Anmerkung

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

Wenn Sie diese Option wählen erscheint das folgende Fenster:

Passwort eingeben

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

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



Wichtig

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

- **BitDefender-News anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Pop-Ups und Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren. Sie können BitDefender konfigurieren, damit die Pop-ups und Hinweise in der Basisansicht oder (bzw und) Profiansicht angezeigt werden.
- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart. Dies wird dringend empfohlen.
- **Aktivitätsanzeige aktivieren (grafische Bildschirmanzeige der Produktaktivität)** - zeigt die Leiste der **Scanaktivität** an wenn Windows läuft. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass die Scanaktivitätsleiste angezeigt wird.



Anmerkung

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

15.2.2. Virenbericht Einstellungen

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

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

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

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

15.3. System-Info

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

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



BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

Dashboard Einstellungen **SysInfo**

Allgemein

- Antivirus
- Privatsphäre
- Prüfung auf Schwachstellen
- Verschlüsselung
- Spiele-/Laptop-Modus
- Netzwerk
- Update
- Registrierung

Aktuelle Systemeinstellungen

Alle Benutzer (0)

- Load-Einträge (5)
 - Userinit (1)
 - Current User Shell (Objekt nicht gefunden)
 - Local Machine Shell (1)
 - Application Init DLLs (0)
 - Winlogon Notify (13)
- INI-Einträge (2)
 - win.ini Einträge (0)
 - system.ini Einträge (1)
- Bekannte DLLs (21)
- Shell-Handler (6)**
- Scripte (2)

Beschreibung des ausgewählten Objektes

Ausführbare Shells Diese Einstellungen befinden sich in der Registry.

Aktualisieren

Hier werden grundlegende Komponenten und Einstellungen Ihres Systems angezeigt. Wählen Sie ein Objekt um eine detaillierte Beschreibung zu sehen.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignisse

System-Info

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

Drei Schaltflächen sind verfügbar:

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



Anmerkung

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

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



16. Antivirus

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

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



Anmerkung

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

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

16.1. Echtzeitschutz

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

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



Echtzeitschutz

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



Wichtig

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

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

16.1.1. Sicherheitsstufe einstellen

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

Es gibt 3 mögliche Einstellungen:



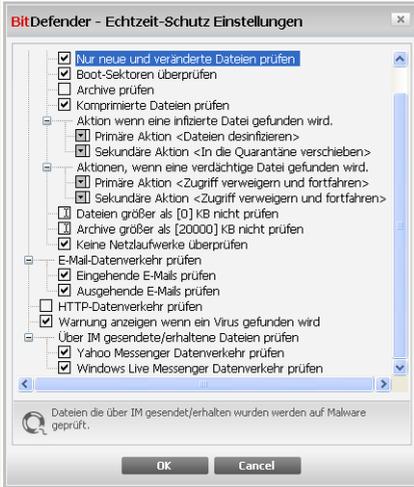
Sicherheitseinstellung	Beschreibung
Tolerant	<p>Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen.</p> <p>Programme und eingehende Nachrichten werden nur auf Viren hin geprüft. Neben den klassischen Signatur basierten Scans werden außerdem Heuristische Scans eingesetzt. Bei infizierten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

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

16.1.2. Sicherheitsstufe anpassen

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

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



Einstellungen des Virus Schild

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



Anmerkung

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

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

Table with 2 columns: Optionen, Beschreibung. Row 1: Dateien prüfen, Alle Dateien prüfen, Prüft alle vorhanden Dateien. Row 2: Programmdateien, Prüft ausschließlich Dateien mit den Dateierendungen: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe;



Optionen	Beschreibung
	<p>.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.</p> <p>Nur Dateien mit folgenden Erweiterungen Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.</p> <p>Auf Spyware prüfen Risikosoftware erkennen. Erkannte Dateien werden als infiziert behandelt. Software welche diese Dateien verwendet könnte Ihre Arbeit einstellen falls diese Option aktiviert ist.</p> <p>Wählen Sie Dialer und Anwendungen vom Scan ausschließen, wenn Sie diese Dateien vom Scan ausschließen wollen.</p>
Bootsektor prüfen	Prüft die Bootsektoren des Systems.
Archive prüfen	Auch der Inhalt von Archiven wird geprüft. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Komprimierte Dateien prüfen	Alle komprimierten Dateien werden überprüft.
Direktverbindung	<p>Nun können Sie eine der folgenden Möglichkeiten auswählen:</p> <p>Zugriff verweigern und fortfahren Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.</p> <p>Datei säubern Desinfiziert die infizierten Dateien.</p> <p>Datei löschen Infizierte Dateien werden ohne Warnung sofort gelöscht.</p> <p>In Quarantäne verschieben Verschiebt die infizierte Datei in die Quarantäne.</p>
Aktionsoptionen	Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die erste Aktion fehlschlägt.



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

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

Die folgenden Optionen sind verfügbar:

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

- **HTTP-Datenverkehr prüfen** - prüft HTTP Datenverkehr.



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

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

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

- **Dateien, die über IM erhalten/gesendet wurden prüfen.** Um Dateien zu prüfen, die Sie über Yahoo Messenger oder Windows Live Messenger erhalten oder senden, markieren Sie die entsprechenden Kontrollkästchen.

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

16.1.3. Konfigurieren Sie die Verhaltensprüfung.

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

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



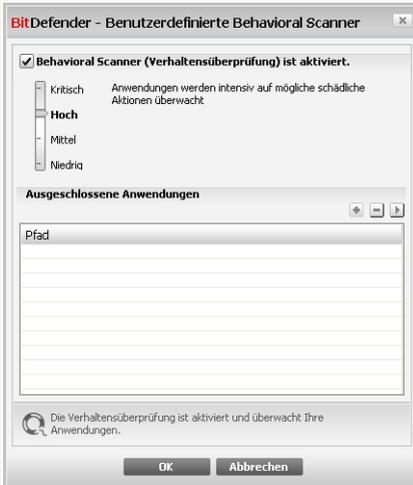
Benachrichtigung der Verhaltensprüfung

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

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



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



Benutzerdefinierte Behavioral Scanner

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



Wichtig

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

Sicherheitsgrad einstellen

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



Anmerkung

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

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



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

Ausgeschlossene Anwendungen verwalten

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

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

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

16.1.4. Echtzeitschutz deaktivieren

Wenn Sie den Echtzeitschutz deaktivieren möchten erscheint ein Warnfenster.



Echtzeitschutz deaktivieren

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



Warnung

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

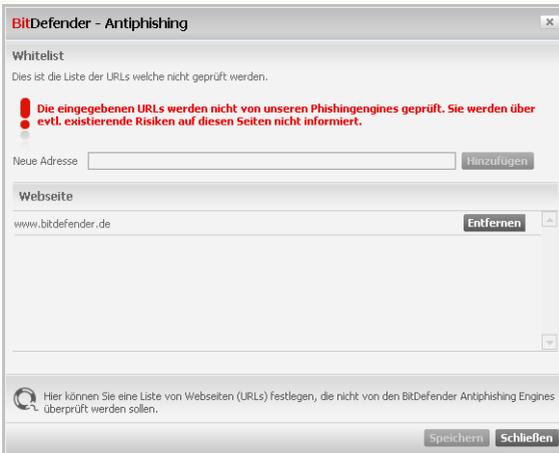
16.1.5. Antiphishingschutz konfigurieren

BitDefender bietet Antiphishingschutz in Echtzeit für:

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

Sie können den Antiphishingschutz für bestimmte Anwendungen oder komplett deaktivieren.

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



Antiphishing Whitelist

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



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



Anmerkung

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

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

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

16.2. Prüfvorgang

Die Aufgabe der BitDefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird in erster Linie erreicht, indem Ihre E-Mail-Anhänge und Downloads überprüft und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

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

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



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

16.2.1. Prüfaufgaben

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

Jede Aufgabe hat ein **Einstellungen** Fenster welches Ihnen erlaubt die Einstellungen einzustellen und die Prüfberichte zu betrachten. Weitere Informationen finden Sie unter „*Konfiguration einer Prüfaufgabe*“ (S. 106).

Es gibt drei verschiedene Einstellungen der Prüfoptionen:



- **Systemaufgaben** - Enthält eine Liste von standard Systemeinstellungen. Die folgenden 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 <code>Windows</code> , <code>Programme</code> und <code>All Users</code> . In der Voreinstellung wird nach allen Arten von Schädlingen geprüft, ausgenommen Rootkits. Ausserdem wird der Arbeitsspeicher, die Registry 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 Priorität 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 schädlingfrei sind.



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

Drei Schaltflächen sind verfügbar:

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



Anmerkung

Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

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

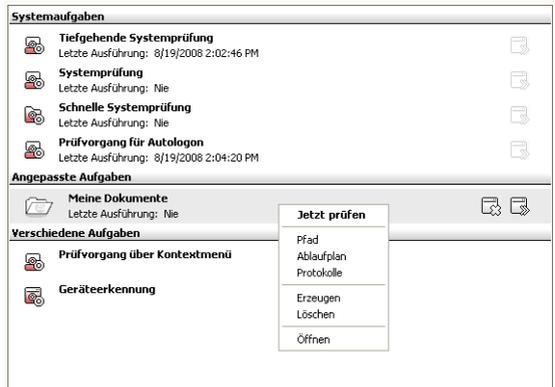
Jede Prüfung hat ihre eigenen **Eigenschaften** Fenster, in welchem Sie die Prüfoptionen konfigurieren, das Ziel der Prüfung festlegen, die Tasks planen oder die Berichte ansehen können.

16.2.2. Verwenden des Kontextmenüs

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

Folgende Aktionen stehen zur Verfügung:

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



Shortcut Menü



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



Anmerkung

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

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



Anmerkung

Für Systemaufgaben nicht verfügbar. Sie können Systemaufgaben nicht löschen.

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



Anmerkung

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

16.2.3. Erstellen von Zeitgesteuerten Aufgaben

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

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



16.2.4. Konfiguration einer Prüfaufgabe

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

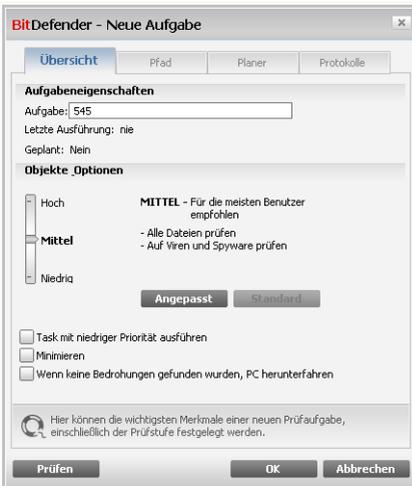


Anmerkung

Weitere Inhalte und Einzelheiten zum Reiter **Prüfberichte** finden Sie in der Produktbeschreibung auf Seite „**Prüfberichte anzeigen**“ (S. 124).

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:

<i>Sicherheits</i> einstellung	<i>Beschreibung</i>
Niedrig	Bietet ausreichende Entdeckung. Belastung der Ressourcen ist niedrig. Die Programme werden nur auf Viren hin geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
Mittel	Bietet eine gute Entdeckung. Belastung der Ressourcen ist mittel. Alle Dateien werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.
Hoch	Bietet eine hohe Entdeckung. Belastung der Ressourcen ist hoch. Alle Dateien und Archive werden auf Viren und Spyware geprüft. Neben der Signatur-basierten Prüfung wird ebenfalls die Heuristik eingesetzt.

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

- **Aufgaben mit niedriger Priorität ausführen.** Herabstufung der Priorität des Prüfungsvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfungsvorgang dauert damit aber entsprechend länger.
- **Minimieren des Prüffensers beim Scan-Start.** Es verkleinert das Prüffenster beim Prüfungsvorgang in die untere **Symbolleiste**. Es kann durch einen Doppelklick auf das BitDefender - Logo in der Symbolleiste wieder geöffnet werden.
- **Herunterfahren des Computers nach erfolgreichem Prüfungsvorgang 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-Exploremenü aufgebaut. Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Die Prüfoptionen sind in 3 Kategorien unterteilt:

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

Optionen	Beschreibung
Dateien prüfen	Sucht nach bekannten Viren.



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

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

Optionen	Beschreibung	
Dateien	Alle Dateien prüfen	Prüft alle vorhanden Dateien.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateierendungen: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php;



Optionen	Beschreibung
	asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml und nws.
Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Komprimierte Dateien	Alle komprimierten Dateien werden überprüft.
Archive	Prüft den Inhalt von eingepackten Archiven. Die Prüfung archivierter Dateien verlängert die benötigte Zeit für die Prüfung und erfordert mehr Systemressourcen. Sie können auf Begrenzung der Archivgröße klicken und die maximale Größe der zu prüfenden Archive in Kilobytes (KB) eingeben.
Postfächer	Prüft den Inhalt von E-Mails und deren Attachments.
Boot-Sektoren	Prüft die Bootsektoren des Systems.
Speicher prüfen	Prüft den Speicher auf Viren und andere Malware.
Registry prüfen	Prüft Einträge in der Systemregistrierung.
Cookies prüfen	Prüft gespeicherte Cookies von Webseiten.

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



Anmerkung

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

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



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

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

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



Anmerkung

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

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



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

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

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



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

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

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

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

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



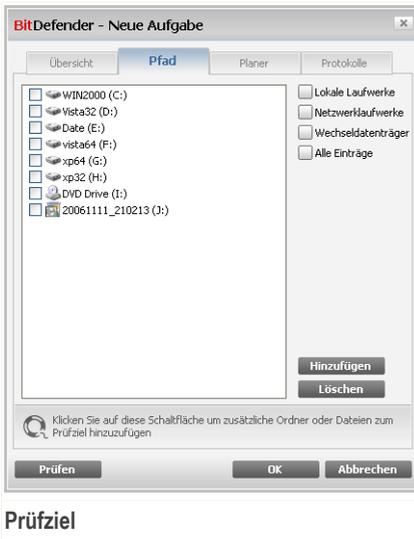
Anmerkung

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

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

Festlegen der Zielobjekte

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



Prüfziel

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

Dieser Bereich enthält folgende Schaltflächen:

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



Anmerkung

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

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



Anmerkung

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

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

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



Anmerkung

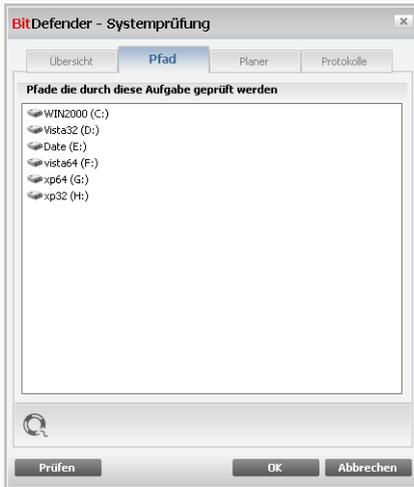
Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

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

Prüfziel der Systemaufgaben anzeigen

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

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



Prüfziel der vollständigen Systemprüfung

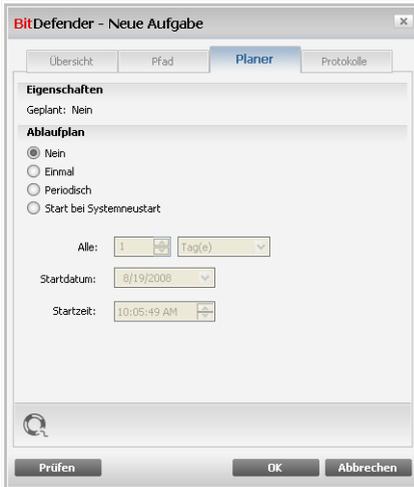
Vollständige Systemprüfung und **Tiefe Systemprüfung** werden alle lokalen Laufwerke prüfen, während **Schnelle Systemprüfung** nur die Ordner `Windows` und `Programme/Dateien` prüfen wird.

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

Zeitgesteuerte Aufgaben festlegen

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

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



Planer

Hier können Sie die Einstellungen zum geplanten Prüfungsvorgang einsehen.

Wenn Sie Prüfungsvorgänge 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 Prüfungsvorgang in festgelegten Zeitabständen (Stunden, Tage, Wochen, Monate, Jahre) beginnend mit einem fest definierten Zeitpunkt (Datum und Uhrzeit).

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

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



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

16.2.5. Prüfoptionen

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



Anmerkung

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

Prüfoptionen

BitDefender bietet vier Arten einen Prüfvorgang durchzuführen:

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

Sofortiges Prüfen

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

Folgende Optionen sind wählbar:

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

Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 120) in diesem Handbuch.



Scannen mit dem Kontextmenü

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



Prüfvorgang über Kontextmenü

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

Der BitDefender Scanner wird geöffnet und der Prüfvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 120) in diesem Handbuch.

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

Prüfen per Drag & Drop

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



Herüberziehen der Datei



Ablegen der Datei



Der BitDefender Scanner wird geöffnet und der Prüfungsvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 120) in diesem Handbuch.

Manuelle Prüfung

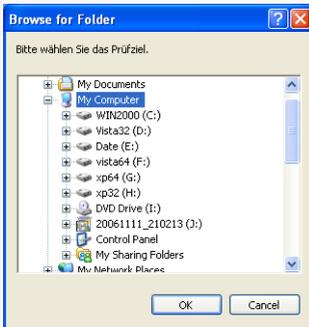
Die Manuelle Prüfung besteht daraus das zu prüfende Objekt direkt über die BitDefender Manuelle Prüfungsoption über den BitDefender Startmenüeintrag zu wählen.



Anmerkung

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

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



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

Der BitDefender Scanner wird geöffnet und der Prüfungsvorgang gestartet. Weitere Informationen finden Sie unter dem Kapitel „*BitDefender Scanner*“ (S. 120) in diesem Handbuch.

Manuelle Prüfung

BitDefender Scanner

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

Schritt 1/3 - Prüfungsvorgang

BitDefender prüft die gewählten Dateien und Ordner.



BitDefender 2009 - Tiefgehende Systemprüfung

Prüfvorgang - Schritt 1/3

1. Schritt | 2. Schritt | 3. Schritt

Prüfstatus

Kürzlich geprüftes Objekt =>HKEY_LOCAL_MACHINE\SYSTEM\CURRE...Path=>H:\WINDOWS\SYSTEM32\DRIVERS\DMIO.SYS

Vergangene Zeit: 00:00:02

Dateien/Sek: 24

Prüfstatistiken

Geprüfte Objekte:	48
Nicht geprüfte Objekte:	0
Infiizierte Objekte:	0
Verdächtige Objekte:	0
Versteckte Objekte:	0
Versteckte Prozesse:	0

Antivirus Prüffortschritt. Der obere Bereich zeigt den Fortschritt des Prozesses an und der untere Bereich die dazugehörigen Statistiken. BitDefender wird standardmäßig probieren die als infiziert entdeckten Objekte zu desinfizieren.

Pause **Beenden** **Abbrechen**

Prüfvorgänge durchführen

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



Anmerkung

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

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

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

Bitte warten Sie bis BitDefender den Prüfvorgang beendet hat.

Schritt 2/3 - Aktionsauswahl

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



The screenshot shows the BitDefender 2009 interface during a scan. The window title is "BitDefender 2009 - 1159". The main area is titled "Prüfung - Schritt 2/3" and "Ergebnis Übersicht". It displays a scan result for a threat named "Win32.Parkit.C" found in the file "H:\Documents and Settings\...\rea\Desktop\av_testbed\3.vir". The risk level is "1 Risiko verbleibt (Desinfizieren fehlgeschlagen)". Below this, a table lists the detected threat with columns for "Dateipfad", "Bedrohungsname", and "Aktionsergebnis". The table shows one entry: "H:\Documents and Settings\...\rea\Desktop\av_testbed\3.vir" with threat name "Win32.Parkit.C" and result "Desinfiziert". At the bottom, there is a "Fortfahren" button and a note: "Diese Aktion wurde von BitDefender gegen die gefundene Bedrohung durchgeführt".

Dateipfad	Bedrohungsname	Aktionsergebnis
H:\Documents and Settings\...\rea\Desktop\av_testbed\3.vir	Win32.Parkit.C	Desinfiziert

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

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

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

Folgende Aktionen stehen zur Verfügung:

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



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

Schritt 3/3 - Zusammenfassung

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

www.bitdefender.de'. At the bottom, there is a search bar with the text 'Die Anzahl der Objekte, deren Prüfung nicht abgeschlossen werden konnte', the BitDefender logo, and two buttons: 'Protokolldatei anzeigen' and 'Schließen'."/>

BitDefender 2009 - 1159

Prüfung - Schritt 3/3

	1. Schritt	2. Schritt	3. Schritt
Ergebnis Übersicht			
Geklärte Objekte:	1		
Ungeklärte Objekte:	1		
Geschützte Objekte:	0		
Ignorierte Objekte:	0		
Fehlgeschlagene Objekte:	1		

1 Datei konnte nicht gereinigt werden, ihr System ist also nicht virenfrei. Weitere Details: www.bitdefender.de

Die Anzahl der Objekte, deren Prüfung nicht abgeschlossen werden konnte

Protokolldatei anzeigen Schließen

Übersicht

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



Wichtig

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

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



BitDefender konnte einige Probleme nicht lösen

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

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

Von BitDefender entdeckte verdächtige Dateien

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

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

16.2.6. Prüfberichte anzeigen

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



Prüfberichte



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

Zwei Schaltflächen sind verfügbar:

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



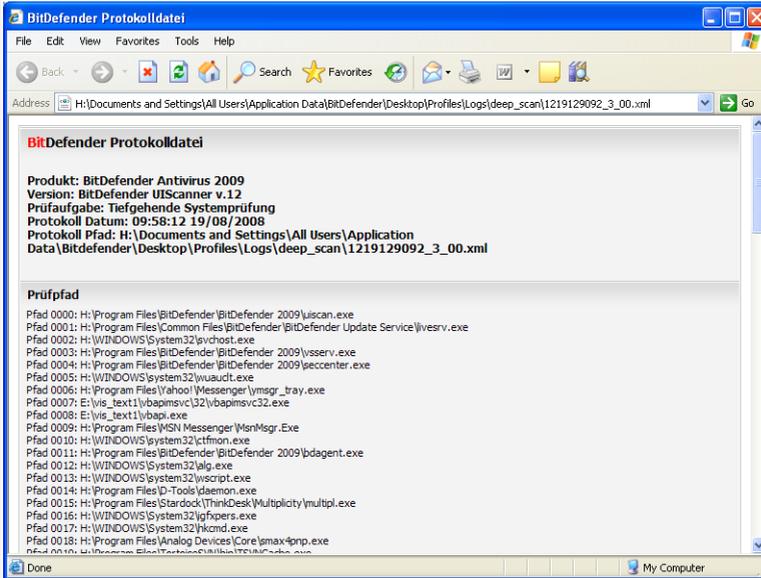
Anmerkung

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

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

Beispiel Prüfbericht

Das folgende Bild zeigt ein Beispiel eines Prüfberichts:



Beispiel Prüfbericht

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

16.3. Vom Prüfvorgang ausgeschlossene Objekte

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

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

Zwei Arten von Objekten können vom Prüfen ausgenommen werden:

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



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



Anmerkung

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

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

BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es besteht noch 1 Problem DIESES PROBLEM

Schild Virenscan **Ausnahmen** Quarantäne

Allgemein
Antivirus
Privatsphäre
Prüfung auf Schwachstellen
Verschlüsselung
Spiele-/Laptop-Modus
Netzwerk
Update
Registrierung

Ausnahmen aktiviert

Vom Prüfvorgang ausgeschlossene Objekte	On-Access	On-Demand
Dateien und Ordner		
c:\	Ja	Ja
Erweiterungen		
*.zip (Komprimiertes Dateiarchiv)	Ja	Ja

Übernehmen Verwerfen

Klicken Sie hier um die letzten Änderungen anzuwenden

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Ausnahmen

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



Anmerkung

Die vorgenommenen Ausnahmen werden bei der Kontextmenüprüfung NICHT berücksichtigt.



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

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



Anmerkung

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

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

16.3.1. Pfade vom Prüfen ausnehmen

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



Schritt 1/4 - Wählen Sie die Objektart

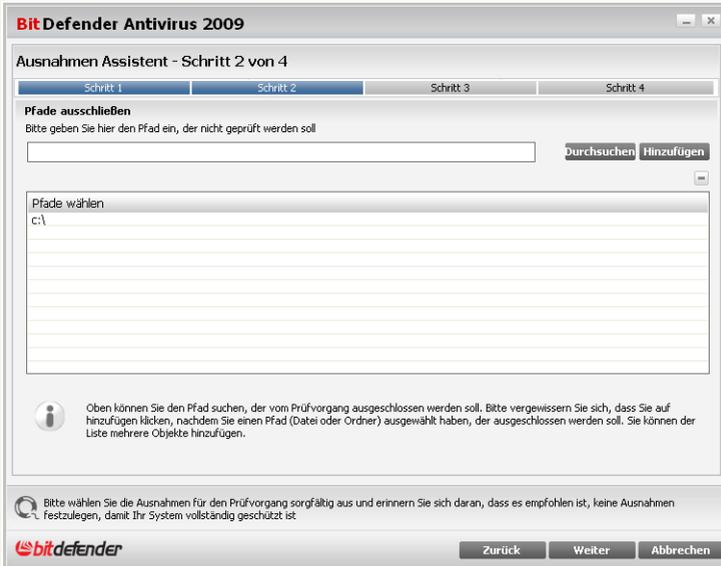


Objektart

Bitte wählen Sie welche Art von Ausnahme Sie erstellen möchten.
Klicken Sie auf **Weiter**.



Schritt 2/4 - Festlegen des Pfads



Ausgenommene Pfade

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

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



Anmerkung

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

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



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

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp

BitDefender Antivirus 2009

Ausnahmen Assistent - Schritt 3 von 4

Schritt 1 Schritt 2 Schritt 3 Schritt 4

Betrifft

Bitte wählen Sie die Art des Prüfvorgangs, der für die ausgewählten Ausnahmen durchgeführt werden soll: On-Demand, On-Access oder beides. Klicken Sie auf den Text in jeder Zelle in der rechten Spalte der untenstehenden Tabelle und wählen Sie die Option, die Ihren Bedürfnissen am Besten entspricht.

Ausgewählte Objekte	Betrifft
c:\	Beide

Bitte wählen Sie die Ausnahmen für den Prüfvorgang sorgfältig aus und erinnern Sie sich daran, dass es empfohlen ist, keine Ausnahmen festzulegen, damit Ihr System vollständig geschützt ist.

bitdefender Zurück Weiter Abbrechen

Prüftyp

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

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

Klicken Sie auf **Weiter**.



Schritt 4/4 - Ausgeschlossene Dateien prüfen

The screenshot shows a window titled "BitDefender Antivirus 2009" with a sub-title "Ausnahmen Assistent - Schritt 4 von 4". At the top, there are four tabs labeled "Schritt 1", "Schritt 2", "Schritt 3", and "Schritt 4", with "Schritt 4" being the active tab. The main content area is titled "Fertigstellen" and contains an information icon followed by the text: "Wir empfehlen Ihnen eine On-Demand-Prüfung des ausgeschlossenen Ziels durchzuführen, um abzusichern, dass Ihr Computer frei von Viren ist. Bitte beachten Sie, dass, wenn Sie den Prüfvorgang fortsetzen, ein Assistent für den On-Demand-Prüfung angezeigt wird. Am Ende dieses Assistenten werden Sie dazu aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen, falls Viren entdeckt wurden." Below this text is a checkbox with the label "Wählen Sie, ob der Prüfvorgang gestartet werden soll, wenn Sie auf beenden klicken". At the bottom of the dialog, there is a small warning icon and the text: "Bitte wählen Sie die Ausnahmen für den Prüfvorgang sorgfältig aus und erinnern Sie sich daran, dass es empfohlen ist, keine Ausnahmen festzulegen, damit Ihr System vollständig geschützt ist". The BitDefender logo is in the bottom left corner, and three buttons labeled "Zurück", "Fertigstellen", and "Abbrechen" are in the bottom right corner.

Ausgeschlossene Dateien prüfen

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

Klicken Sie auf **Fertigstellen**.

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

16.3.2. Dateierweiterungen vom Prüfen ausnehmen

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



Schritt 1/4 - Wählen Sie die Objektart

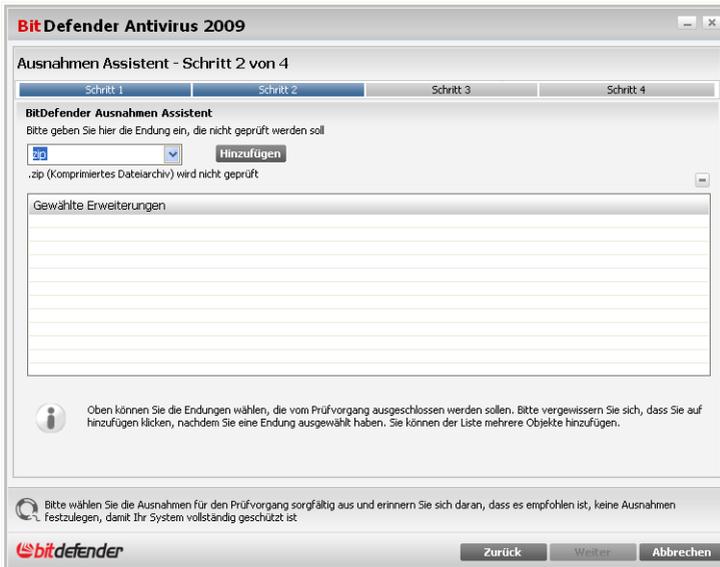


Objektart

Wählen Sie die Option um eine Dateierweiterung vom Prüfen auszunehmen.
Klicken Sie auf **Weiter**.



Schritt 2/4 - Erweiterungen festlegen



Ausgenommene Erweiterungen

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

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



Anmerkung

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

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

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



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

Klicken Sie auf **Weiter**.

Schritt 3/4 - Wählen Sie den Prüftyp

BitDefender Antivirus 2009

Ausnahmen Assistent - Schritt 3 von 4

Schritt 1 Schritt 2 Schritt 3 Schritt 4

Betrifft

Bitte wählen Sie die Art des Prüfvorgangs, der für die ausgewählten Ausnahmen durchgeführt werden soll: On-Demand, On-Access oder beides. Klicken Sie auf den Text in jeder Zelle in der rechten Spalte der untenstehenden Tabelle und wählen Sie die Option, die Ihren Bedürfnissen am Besten entspricht.

Ausgewählte Objekte	Betrifft
*.zip (Komprimiertes Dateiarchiv)	Beide

Bitte wählen Sie die Ausnahmen für den Prüfvorgang sorgfältig aus und erinnern Sie sich daran, dass es empfohlen ist, keine Ausnahmen festzulegen, damit Ihr System vollständig geschützt ist.

bitdefender Zurück Weiter Abbrechen

Prüftyp

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

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

Klicken Sie auf **Weiter**.



Schritt 4/4 - Wählen Sie den Prüftyp



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

Klicken Sie auf **Fertigstellen**.

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

16.4. Quarantäne

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



16.4.1. Quarantäne-Dateien verwalten

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

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

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

16.4.2. Quarantäne-Einstellungen konfigurieren

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



Quarantäne Einstellungen

Über die Quarantäne-Einstellungen können Sie folgende Aktionen festlegen:



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



Anmerkung

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

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



Anmerkung

Standardmässig prüft BitDefender die Dateien in Quarantäne einmal täglich auf Duplikate.

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



Anmerkung

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

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

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



17. Privatsphärekontrolle

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

17.1. Status der Privatsphärekontrolle:

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



BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

Status Identität Registry Cookie Script

Allgemein
Antivirus
Privatsphäre
Prüfung auf Schwachstellen
Verschlüsselung
Spiele-/Laptop-Modus
Netzwerk
Update
Registrierung

Privatsphäre ist aktiviert
Identitätskontrolle ist deaktiviert

Sicherheitsstufe

Agressiv
Standard
Tolerant

Tolerant
- Identität Kontrolle ist deaktiviert
- Registry Kontrolle ist deaktiviert
- Cookie Kontrolle ist deaktiviert
- Script Kontrolle ist deaktiviert

Anpassen Standard

Privatsphäre Kontrollstatistik

Informationen zur Identität blockiert: 0
Registry blockiert: 0
Cookies blockiert: 0
Scripte blockiert: 0

Das Modul für den Privatsphäreschutz ist nun deaktiviert. Für die Sicherheit Ihrer Daten empfehlen wir Ihnen, den Privatsphäreschutz jederzeit aktiviert zu halten.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Status der Privatsphärekontrolle:

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



Wichtig

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

Die Privatsphäre schützt Ihren Computer mit diesen wichtigen Kontrollmechanismen:

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



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

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

17.1.1. Sicherheitsstufe einstellen

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

Es gibt 3 mögliche Einstellungen:

Sicherheitseinstellung	Beschreibung
Tolerant	Registrierung aktiviert.
Standard	Registry Kontrolle und Identität sind aktiviert.
Aggressiv	Registry Kontrolle , Identität und Script Kontrolle sind aktiviert.

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

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

17.2. Antispyware/Identitätskontrolle

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

Ob es sich um Ihre E-Mail Adresse handelt oder um Ihre Kreditkartennummer, wenn sie in die falschen Hände geraten können diese Informationen großen Schaden anrichten: Sie werden möglicherweise in Spam Mails ertrinken oder sich über ein geleertes Konto wundern.

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



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

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

Warum sollten Sie die Identitätskontrolle verwenden?

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

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

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

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

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

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



Schritt 1/4 - Willkommensfenster



Begrüßungsfenster

Klicken Sie auf **Weiter**.



Schritt 2/4 - Typ und Daten der Regel auswählen

BitDefender 2009 - Identitätsregeln-Assistent

Name der Regel

Art der Regel

Daten der Regel

Persönliche Informationen sind verschlüsselt und kann nur von Ihnen eingesehen werden. Zur zusätzlichen Sicherung geben Sie bitte nur einen Teil der zu sichernden Informationen ein (Falls Sie den E-Mail Verkehr von E-Mail Adressen filtern möchten gehen Sie wie folgt vor: john.doe@example.com benötigt nur die Zeichenfolge "John")

Regelnamen hier eingeben

Zurück Weiter Abbrechen

Typ und Richtung auswählen

Hier können Sie die Parameter auswählen:

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



Anmerkung

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

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

Klicken Sie auf **Weiter**.



Schritt 3/4 - Datenverkehr auswählen

BitDefender 2009 - Identitätsregeln-Assistent

HTTP überprüfen
 SMTP-Daten überprüfen
 Instant Messaging prüfen
 Vergleiche ganze Wörter
 Zeichensatz

HTTP (Web) Datenverkehr und IM (Messenger) Datenverkehr HTTP-Datenverkehr (Web), der Ihre persönlichen Daten enthält, wird blockiert.

Markieren zur Aktivierung der Prüfung des HTTP-Datenverkehrs

Zurück Weiter Abbrechen

Datenverkehr auswählen

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

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

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

Klicken Sie auf **Weiter**.



Schritt 4/4 - Regel beschreiben

BitDefender 2009 - Identitätsregeln-Assistent

Beschreibung der Regel

Geben Sie eine Beschreibung für diese Regel an. Die so erstellte Beschreibung hilft Ihnen zu erkennen welche Informationen gesperrt werden sollen.

Beschreibung für diese Regel eingeben

Zurück Fertigstellen Abbrechen

Beschreibung der Regel

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

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

17.2.2. Definition von Ausnahmen

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

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



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

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

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

Regel editieren

17.3. Registrierung prüfen

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

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

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



Registrierungsalarm

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

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

Je nach Ihrer Auswahl wird eine Regel erstellt und in der Regeltabelle aufgelistet. Dieselbe Aktion wird immer ausgeführt wenn diese Anwendung versucht einen Registryeintrag zu ändern.



Anmerkung

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

Um die Registry-Kontrolle zu konfigurieren klicken auf **Privatsphäre>Registry** in der erweiterten Ansicht.



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

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



Cookie-Alarm

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

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

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



Anmerkung

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

Um die Cookie-Kontrolle zu konfigurieren klicken Sie auf **Privatsphäre>Cookie** in der erweiterten Ansicht.



17.4.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



Adresse, Aktion und Richtung auswählen

Hier können Sie die Parameter auswählen:

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

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

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

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



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



Anmerkung

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

Klicken Sie auf **Fertigstellen**.

17.5. Skript-Kontrolle

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

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

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

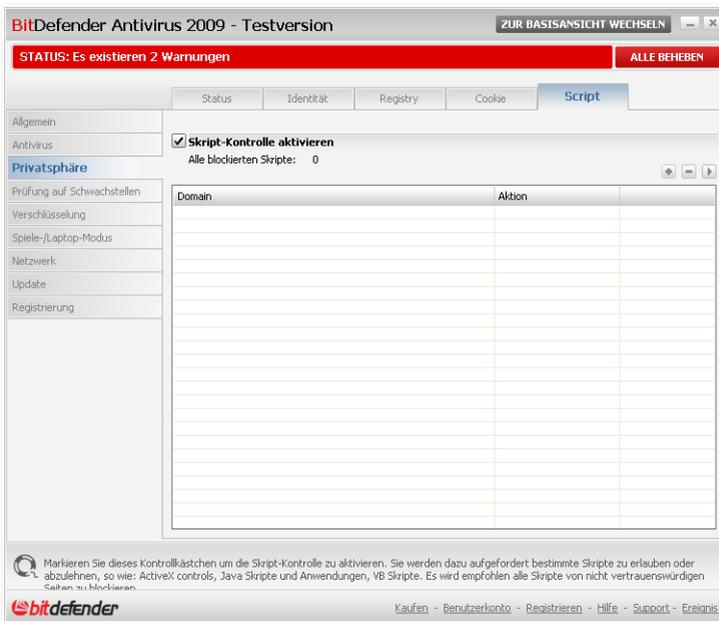


Skript-Alarm

Der Namen der Quelle wird Ihnen angezeigt.

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

Um die Skript-Kontrolle zu konfigurieren klicken Sie auf **Privatsphäre>Skript** in der erweiterten Ansicht.



Skript-Kontrolle



Sie können eine Liste der Regeln in der Aufstellung ansehen.



Wichtig

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

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

Um eine Regel manuell zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen** und führen Sie die gewünschten Änderungen im Konfigurationsfenster durch.

17.5.1. Konfigurationsfenster

Wenn Sie eine Regel manuell verändern oder hinzufügen, wird ein Konfigurationsfenster erscheinen.



Adresse und Aktion auswählen

Hier können Sie die Parameter auswählen:

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



<i>Aktion</i>	<i>Beschreibung</i>
Zulassen	Die Scripts auf dieser Domäne werden ausgeführt.
Verweigern	Die Scripts auf dieser Domäne werden nicht ausgeführt.

Klicken Sie auf **Fertigstellen**.



18. Instant Messaging (IM) Verschlüsselung

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

- Ihr Chatpartner hat eine BitDefender Version installiert, die die IM-Verschlüsselung unterstützt und die IM-Verschlüsselung ist für die Instant Messaging Anwendung aktiviert, die verwendet wird.
- Sie und Ihr Chatpartner verwenden entweder Yahoo Messenger oder Windows Live (MSN) Messenger.



Wichtig

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

Um die IM-Verschlüsselung zu konfigurieren klicken Sie auf **Verschlüsselung>IM-Verschlüsselung** in der erweiterten Ansicht.



Anmerkung

Sie können die IM-Verschlüsselung einfach mit der BitDefender Toolbar von dem Chat-Fenster aus konfigurieren. Für weitere Informationen lesen Sie bitte „*Integration in Messenger*“ (S. 37).



The screenshot shows the BitDefender Antivirus 2009 - Testversion interface. At the top, there is a red status bar with the text "STATUS: Es existieren 2 Warnungen" and a button "ALLE BEHEBEN". Below this, the "Verschlüsselung" (Encryption) settings are displayed. The "Allgemein" (General) section shows that "IM-Verschlüsselung ist deaktiviert" (IM encryption is deactivated). Underneath, there are two checkboxes: "Yahoo Messenger Verschlüsselung ist deaktiviert" and "Windows Live (MSN) Messenger Verschlüsselung ist deaktiviert". Below these are two tables:

Verschlüsselungsausnahmen

Benutzer ID	IM-Programm
-------------	-------------

Aktuelle Verbindungen

Benutzer ID	IM-Programm	Verschlüsselungsstatus
-------------	-------------	------------------------

At the bottom of the interface, there is a note: "Hier können Sie die Komponente IM-Verschlüsselung genau konfigurieren." and the BitDefender logo. In the bottom right corner, there are links: "Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis".

Instant Messenger Verschlüsselung

Die IM-Verschlüsselung ist standardmäßig für Yahoo Messenger und Windows Live (MSN) Messenger aktiviert. Sie können die IM-Verschlüsselung für eine bestimmte Anwendung oder komplett deaktivieren.

Zwei Tabellen werden angezeigt:

- **Verschlüsselungsausnahmen** - listet die Benutzer-IDs und das entsprechende IM-Programm auf, für den die Verschlüsselung deaktiviert ist. Um einen Kontakt aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf die Schaltfläche **Entfernen**.
- **Aktuelle Verbindungen** - listet die aktuellen Instant Messaging Verbindungen auf (Benutzer ID und entsprechendes IM-Programm) und zeigt an, ob diese verschlüsselt sind oder nicht. Eine Verbindung kann aus folgenden Gründen nicht verschlüsselt sein:
 - Sie haben die Verschlüsselung für den entsprechenden Kontakt deaktiviert.



- Ihr Kontakt hat keine BitDefender Version installiert, die eine IM-Verschlüsselung unterstützt.

18.1. Verschlüsselung für bestimmte Benutzer deaktivieren

Um die Verschlüsselung für einen bestimmten Benutzer zu deaktivieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie auf die Schaltfläche **Hinzufügen** um das Konfigurationsfenster zu öffnen.



Kontakte hinzufügen

2. Geben Sie die Benutzer-ID Ihres Kontaktes in das Editierfeld ein.
3. Wählen Sie die Chat-Anwendung des Kontaktes.
4. Klicken Sie auf **OK**.



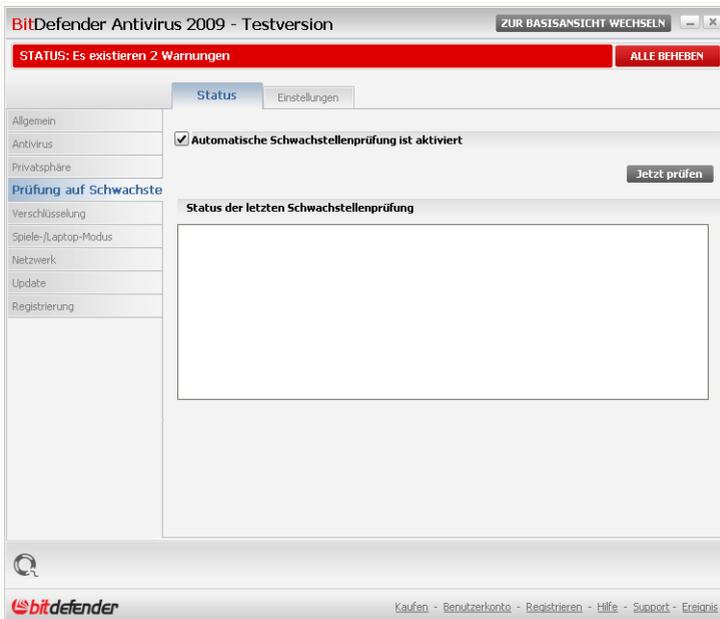
19. Prüfung auf Schwachstellen

Ein wichtiger Schritt für den Schutz Ihres Computers gegen Hacker und schädliche Anwendungen besteht darin, das Betriebssystem und die Programme, die Sie oft verwenden, stets auf dem neusten Stand zu halten. Und um einen ungewünschten Zugriff auf Ihren Computer zu vermeiden sind sichere Passwörter (Passwörter die nicht einfach umgangen werden können) für jedes Windows-Benutzerkonto notwendig.

BitDefender überprüft Ihr System regelmäßig auf Schwachstellen und benachrichtigt Sie über bestehende Probleme oder Risiken.

19.1. Status

Um die automatische Prüfung auf Schwachstellen zu konfigurieren oder eine Prüfung auf Schwachstellen auszuführen, klicken Sie auf **Schwachstellen>Status** in der erweiterten Ansicht.



Status der Schwachstellen Prüfung



Jede Tabelle zeigt die gelöste Objekte aus der letzten Schwachstellen Prüfung und deren aktuellen Status an. Hier können Sie sehen, welche Aktion Sie durchführen sollen, um jede Schwachstelle zu beheben, falls welche vorhanden. Wenn die Aktion **Keine** ist, dann wird diese Angelegenheit keine Schwachstelle darstellen.



Wichtig

Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die **Automatische Prüfung auf Schwachstellen** aktiviert.

19.1.1. Schwachstellen beheben

Um eine bestimmte Schwachstelle zu beheben, klicken Sie doppelt darauf und von der Situation abhängig, fahren Sie folgenderweise fort:

- Klicken Sie auf **Alle System-Updates installieren**, um die verfügbaren Windows Updates zu installieren.
- Wenn eine Anwendung nicht auf dem neusten Stand ist, Nutzen Sie den auf der Webseite **verfügbaren**) Link um die aktuellste Version herunterzuladen und zu installieren.
- Falls ein Windowskonto ein schwaches Passwort hat, fordern Sie den Benutzer beim nächsten Windows-Login auf das Passwort zu ändern oder ändern Sie es selbst.

Um Ihren Computer auf Schwachstellen zu prüfen, klicken Sie auf **Jetzt prüfen** und folgen Sie den Schritten des Assistenten um die Schwachstellen zu beheben.



Schritt 1/6 - Auswahl der zu prüfenden Schwachstellen

BitDefender Total Security 2009

BitDefender Assistent für Schwachstellen-Prüfung

1. Schritt 2. Schritt 3. Schritt 4. Schritt Schritt 5 Schritt 6

Aufgaben auswählen

Dieser Assistent wird Sie durch die erforderlichen Aktionen führen um Anwendungen zu erkennen die nicht mehr auf dem neusten Stand sind und Windows-Benutzerkonten mit einem schwachen Passwort. Bitte wählen Sie aus der unteren Liste, welche Objekte auf Schwachstellen geprüft werden sollen.

- Passwörter für Windows-Benutzerkonten jetzt prüfen
- Auf Anwendungs-Updates prüfen
- Auf wichtige Windows-Updates prüfen
- Auf optionale Windows-Updates prüfen

 Markieren Sie dieses Kontrollkästchen, damit BitDefender die Passwörter der Windows Benutzerkonten auf Ihrem Computer überprüft: Diese Passwörter sollten Buchstaben, Zahlen und Zeichen enthalten, um einen ausreichenden Schutz zu bieten.

 Weiter Abbrechen

Schwachstellen

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



Schritt 2/6 - Nach Schwachstellen suchen



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



Schritt 3/6 - Unsicheres Passwort ändern

BitDefender Total Security 2009

BitDefender Assistent für Schwachstellen-Prüfung

1. Schritt | 2. Schritt | 3. Schritt | 4. Schritt | Schritt 5 | Schritt 6

Passwörter für Windows-Benutzerkonten jetzt prüfen

Benutzername	Festigkeit	Status
Administrator	Strong	Ok
amirea	Strong	Ok

Dies ist eine Liste der eingestellten Passwörter der Windows Benutzerkonten auf Ihrem Computer und die Sicherheitsstufe, die sie darstellen. Klicken Sie auf die Schaltfläche "Feststellen" um unsichere Passwörter zu ändern.

bitdefender

Weiter Abbrechen

Passwörter von Benutzern

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

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

BitDefender

Choose method to fix:

Force user to change password at next login

Change user password

Type password:

Confirm password:

OK Close

Passwort ändern



Wählen Sie die Methode um ein Problem zu beheben:

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



Anmerkung

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

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

Klicken Sie auf **Weiter**.



Schritt 4/6 - Anwendungen aktualisieren

The screenshot shows the BitDefender Total Security 2009 interface during a vulnerability check. The window title is "BitDefender Total Security 2009" and the subtitle is "BitDefender Assistent für Schwachstellen-Prüfung". The progress bar indicates "4. Schritt" (Step 4) is active. The main heading is "Auf Anwendungs-Updates prüfen". Below this is a table with the following data:

Anwendung	Installierte Version	Aktuellste Version	Status
Adobe Reader	8.1.2	8.1.2	Auf dem neusten Stand
Yahoo! Messenger	8.1.0.421	8.1.0.241	Auf dem neusten Stand
Firefox	3.0 (en-US)	3.0 (en-US)	Auf dem neusten Stand

Below the table, there is a search icon and the text: "Dies ist eine Liste der Anwendungen, die von BitDefender unterstützt werden und der verfügbaren Updates (falls vorhanden).". At the bottom of the window, there is the BitDefender logo and two buttons: "Weiter" and "Abbrechen".

Anwendungen

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

Klicken Sie auf **Weiter**.



Schritt 5/6 - Windows aktualisieren

The screenshot shows the BitDefender Total Security 2009 interface during a vulnerability check. The window title is "BitDefender Total Security 2009" and the subtitle is "BitDefender Assistent für Schwachstellen-Prüfung". The progress bar indicates "Schritt 5" of 6 steps. The main section is titled "Windows Updates" and contains a list of updates under the heading "Auf wichtige Windows-Updates prüfen". The list includes updates such as "Security Update for Windows XP (KB901190)", "Security Update for Microsoft XML Core Services 6.0 and Microsoft XML Core Services 6.0 Service Pack 1 (KB933579)", "Microsoft .NET Framework 2.0 Service Pack 1 (KB110906)", "Microsoft .NET Framework 1.1 Service Pack 1", "Security Update for Windows XP (KB950749)", "Update for Windows XP (KB932823)", "Security Update for Windows XP (KB950762)", "Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB936181)", "Security Update for Windows XP (KB951376)", "Security Update for Windows XP (KB951698)", "Windows XP Service Pack 3 (KB936929)", "Security Update for Windows XP (KB951748)", "Cumulative Security Update for ActiveX Killbits for Windows XP (KB953839)", "Windows Malicious Software Removal Tool - August 2008 (KB990830)", and "Security Update for Outlook Express for Windows XP (KB951066)". Below the list is a button labeled "Alle System-Updates installieren". A note below the button says "Dies ist eine Liste der wichtigen und weniger wichtigen Updates für Windows-Anwendungen". At the bottom of the window are the BitDefender logo and two buttons: "Weiter" and "Abbrechen".

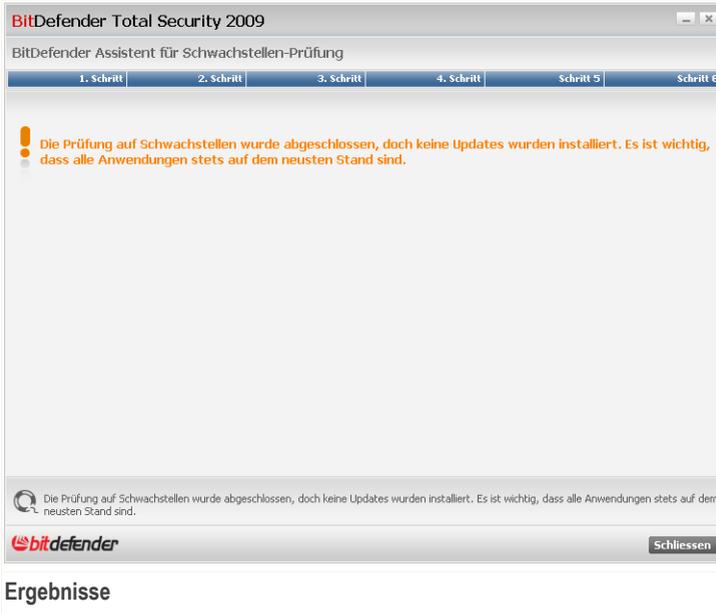
Windows Updates

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

Klicken Sie auf **Weiter**.



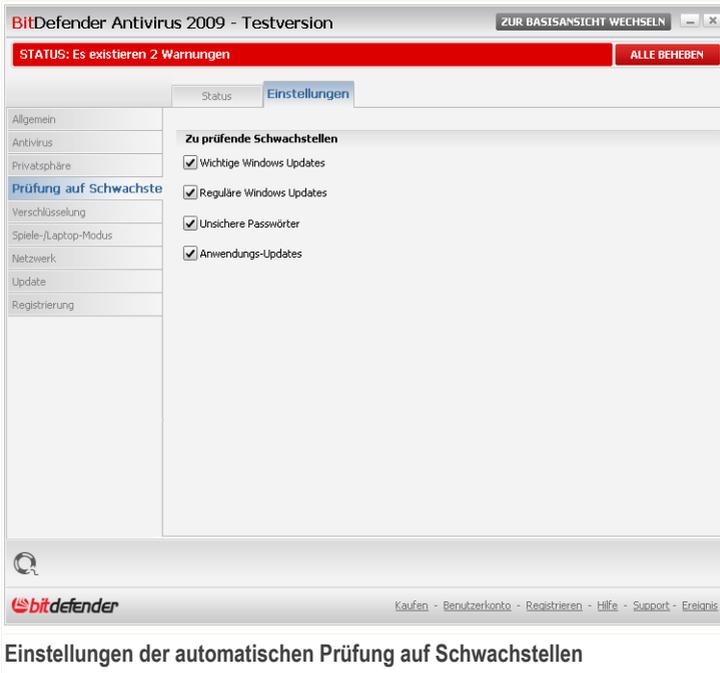
Schritt 6/6 - Ergebnisse betrachten



Klicken Sie auf **Schließen**.

19.2. Einstellungen

Um die Einstellungen für die automatische Prüfung auf Schwachstellen zu verwalten, klicken Sie auf **Schwachstellen>Einstellungen** in der erweiterten Ansicht.



Einstellungen der automatischen Prüfung auf Schwachstellen

Markieren Sie die Kontrollkästchen der entsprechenden Systemschwachstellen die regelmäßig überprüft werden sollen.

- **Wichtige Windows Updates**
- **Normale Windows Updates**
- **Unsichere Passwörter**
- **Anwendungs-Updates**



Anmerkung

Wenn Sie das Kontrollkästchen für eine bestimmte Schwachstelle freilassen, wird BitDefender Sie nicht über die entsprechenden Probleme und Risiken informieren.



20. Spiele-/Laptop-Modus

Das Modul Spiele-/Laptop-Modus gibt Ihnen die Möglichkeit spezielle Betriebsmodi von BitDefender zu konfigurieren.

- Der **Spiele-Modus** verändert die Schutzeinstellungen zeitweise derart, dass ihr Einfluss auf die Leistungsfähigkeit des Systems während Sie spielen so gering wie möglich ist.
- Der **Laptop-Modus** stoppt voreingestellte Aufgaben wenn der Laptop über einen Akku betrieben wird, um dessen Laufzeit zu verlängern.

20.1. Spiele-Modus

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

- Alle BitDefender Alarme und Pop-ups werden deaktiviert.
- Der Echtzeit-Schutz wird auf **Tolerant** gestellt.
- Updates werden nicht standardmäßig durchgeführt.



Anmerkung

Um diese Einstellung zu ändern, gehen Sie zu **Update>Einstellungen** und lassen Sie das Kontrollkästchen **Kein Update im Spiele-Modus** frei.

- Voreingestellte Prüfaufgaben sind standardmäßig deaktiviert.

BitDefender startet den Spiele-Modus standardmäßig wenn Sie ein Spiel starten, das sich auf der Liste der bekannten Spiele von BitDefender befindet, oder wenn eine Anwendung auf dem ganzen Bildschirm ausgeführt wird. Mit dem Tastenkürzel **Strg+Alt+Shift+G** können Sie den Spiele-Modus manuell starten. Es wird dringend empfohlen dass Sie den Spiele-Modus verlassen, wenn Sie mit dem Spielen fertig sind (Sie können dafür das selbe Tastenkürzel verwenden **Ctrl+Alt+Shift+G**).



Anmerkung

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



Um den Spiele-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Spiele-Modus** in der Profiansicht.

BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es existieren 2 Warnungen ALLE BEHEBEN

Spiele-Modus Laptop-Modus

Allgemein
Antivirus
Privatsphäre
Prüfung auf Schwachstellen
Verschlüsselung
Spiele-/Laptop-Modus
Netzwerk
Update
Registrierung

Aktueller Status
Spiele-Modus ist deaktiviert Spiele-Modus starten

Automatischer Spiele-Modus ist aktiviert

Liste mit von BitDefender vorgegebenen Spielen verwenden Spiele verwalten
 Den Spiele-Modus bei Vollbild aktivieren
 Fragen ob die Anwendung zur Whitelist hinzugefügt werden soll

Einstellungen Weitere Einstellungen

Prüfaufgabe
 Aufgabe überspringen
 Aufgabe verschieben

Markieren Sie dieses Kontrollkästchen, damit der Spiele-Modus für eine von BitDefender festgelegte Spieliste angewendet wird. Diese beinhaltet die bekanntesten Spiele auf dem Markt und kann mit anderen Spielen ergänzt werden.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Spiele-Modus

Im oberen Bereich des Abschnitts können Sie den Status des Spiele-Modus sehen. Sie können auf **Spiele-Modus starten** oder **Spiele-Modus beenden** klicken um den aktuellen Status zu verändern.

20.1.1. Automatischer Spiele-Modus konfigurieren

Mit dem automatischen Spiele-Modus kann BitDefender automatisch den Spiele-Modus starten, wenn ein Spiel entdeckt wird. Folgende Optionen können konfiguriert werden:

- **Von BitDefender zur Verfügung gestellte Spieliste verwenden** - wenn Sie ein Spiel der Liste der bekannten Spiele starten, startet BitDefender automatisch den Spiele-Modus. Um diese Liste zu sehen, klicken Sie auf **Spiele verwalten** und dann **Erlaubte Spiele ansehen**.



- **Spiele-Modus bei Vollbild starten** -wenn eine Anwendung auf dem gesamten Bildschirm ausgeführt wird startet der Spiele-Modus automatisch.
- **Anwendung zur Spielereiste hinzufügen?** - um aufgefordert zu werden, eine neue Anwendung zur Spielereiste hinzuzufügen wenn Sie das Vollbild verlassen. Indem Sie eine neue Anwendung zur Spielereiste hinzufügen, wird BitDefender den Spiele-Modus automatisch starten, wenn Sie diese Anwendung das nächste Mal starten.

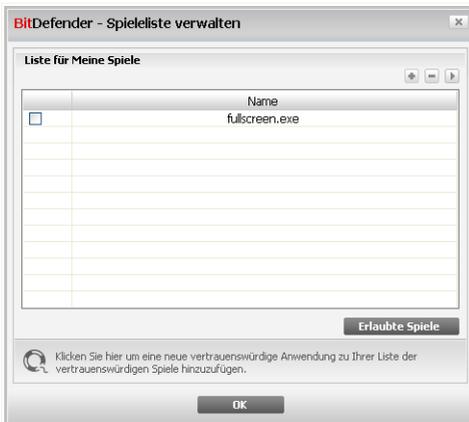


Anmerkung

Wenn Sie nicht möchten, dass BitDefender den Spielmodus automatisch startet, lassen Sie das Kontrollkästchen **Automatischer Spiele-Modus** frei.

20.1.2. Spielereiste verwalten

BitDefender startet den Spiele-Modus automatisch, wenn eine Anwendung gestartet wird die sich auf der Spielereiste befindet. Um die Spielereiste zu sehen und zu verwalten, klicken Sie auf **Spiele verwalten**. Ein neues Fenster wird sich öffnen.



Spieleliste

Neue Anwendungen werden automatisch zur Liste hinzugefügt, wenn:

- Sie ein Spiel starten das Bitdefender bekannt ist. Um diese Liste zu sehen, klicken Sie auf **Erlaubte Spiele betrachten**.



- Nachdem Sie das Vollbild beendet haben, können Sie das Spiel über das Aufforderungsfenster zur Spieliste hinzufügen.

Wenn Sie den automatischen Spiele-Modus für eine bestimmte Anwendung von der Liste deaktivieren möchten, lassen Sie das entsprechende Kontrollkästchen frei. Sie sollten den automatischen Spiele-Modus für reguläre Anwendungen die den gesamten Bildschirm verwenden deaktiviert lassen, so wie Web-Browser und Mediaplayer.

Um die Spiele-Liste zu verwalten, können Sie die Schaltflächen verwenden, die sich im oberen Bereich der Tabelle befinden:

- Klicken Sie auf **Hinzufügen** um eine neue Anwendung zu der Spieliste hinzufügen.
- **Entfernen** - dient zum Entfernen einer Anwendung von der Spieliste.
- Klicken Sie auf **OK** um den Eintrag aus der Spieliste zu editieren.

Spiele hinzufügen oder bearbeiten

Wenn Sie einen Eintrag der Spiele-Liste hinzufügen oder bearbeiten, wird folgendes Fenster erscheinen:



Spiel hinzufügen

Klicken Sie auf **Durchsuchen** um die Anwendung auszuwählen oder geben Sie den vollständigen Pfad der Anwendung in das Editierfeld ein.

Wenn Sie nicht möchten, dass der Spiele-Modus automatisch gestartet wird, wenn die ausgewählte Anwendung gestartet wurde, wählen Sie **Deaktivieren**.

Klicken Sie auf **OK** um den Eintrag zu der Spieliste hinzuzufügen.



20.1.3. Einstellungen des Spiele-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Prüfungsaufgabe** - um zu verhindern, dass voreingestellte Prüfungsaufgaben im Spielemodus ausgeführt werden. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.
Aufgabe verschieben	Die voreingestellte Aufgabe wird sofort ausgeführt, sobald der Spiele-Modus beendet wird.

20.1.4. Tastenkombination für Spielmodus ändern

Mit dem Tastenkürzel `Strg+Alt+Shift+G` können Sie den Spiele-Modus manuell starten. Wenn Sie die Tastenkombination ändern möchten, befolgen Sie folgende Schritte:

1. Klicken Sie auf **Weitere Einstellungen**. Ein neues Fenster wird sich öffnen.



Mehr Einstellungen

2. Wählen Sie die gewünschte Tastenkombination unter der Option **Tastenkombination aktivieren** :



- Wählen Sie die Tastenkombination die Sie verwenden möchten indem Sie folgende Tasten markieren : Steuerung (**Strg**), Shift (**Shift**) oder Alt-Taste (**Alt**).
- Geben Sie im Editierfeld die Taste ein, die Sie benutzen möchten.

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

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



Anmerkung

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

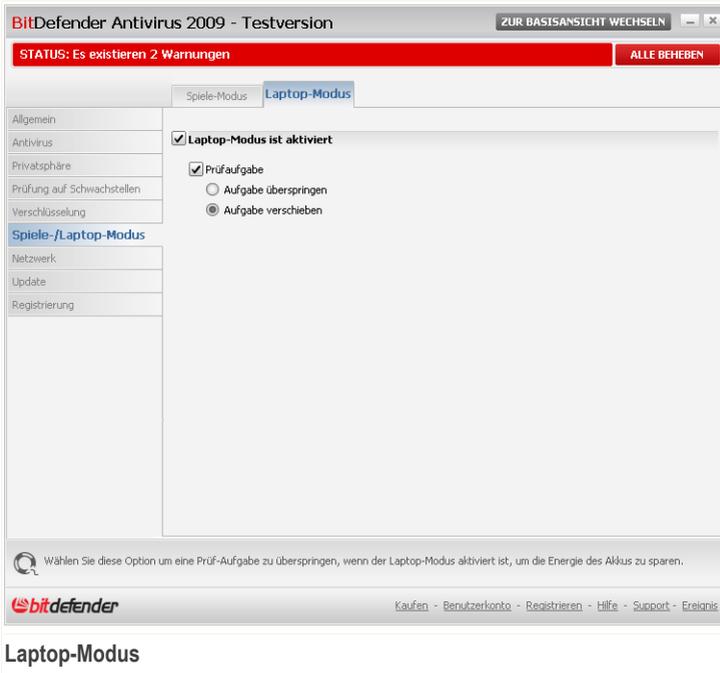
20.2. Laptop-Modus

Der Laptop-Modus wurde für Nutzer von Laptops und Notebooks konzipiert. Er soll den Energieverbrauch von BitDefender so gering wie möglich halten um den Einfluss auf die Akkulaufzeit zu minimieren.

Während der Laptop-Modus ausgeführt wird, werden voreingestellte Aufgaben standardmäßig nicht durchgeführt.

BitDefender erkennt wenn Ihr Laptop über ein Akku läuft und startet den Laptop-Modus automatisch. Ebenso beendet BitDefender automatisch den Laptop-Modus, wenn erkannt wird dass der Laptop nicht mehr über einen Akku betrieben wird.

Um den Laptop-Modus zu konfigurieren klicken Sie auf **Spiele / Laptop Modus>Laptop-Modus** in der Profiansicht.



Sie können sehen ob der Laptop-Modus aktiviert ist oder nicht. Wenn der Laptop-Modus aktiviert ist, wird BitDefender die konfigurierten Einstellungen anwenden, wenn der Laptop über einen Akku betrieben wird.

20.2.1. Einstellungen des Laptop-Modus konfigurieren

Um das Verhalten voreingestellter Aufgaben zu konfigurieren, verwenden Sie diese Optionen:

- **Prüfaufgabe** - um zu verhindern, dass Prüfaufgaben durchgeführt werden, wenn der Laptop-Modus ausgeführt wird. Folgende Optionen sind wählbar:

Optionen	Beschreibung
Aufgabe überspringen	Die voreingestellte Aufgabe wird überhaupt nicht ausgeführt.



<i>Optionen</i>	<i>Beschreibung</i>
Aufgabe verschieben	Die Aufgabe wird sofort durchgeführt, sobald der Laptop-Modus beendet wird.



21. Netzwerk

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

BitDefender Antivirus 2009 - Testversion

ZUR BASISANSICHT WECHSELN

STATUS: Es besteht noch 1 Problem ALLE BEHEBEN

Netzwerk

INTERNET 10.10.0.1

Kein PC (klicken Sie hier um hinzuzufügen)

Netzwerk beitreten/erstellen

bitdefender

Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

Netzwerkübersicht

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

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



3. Fügen Sie die Computer die Sie verwalten möchten ebenfalls auf Ihrem Computer hinzu.

21.1. Dem BitDefender-Netzwerk beitreten

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

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

The screenshot shows a dialog box titled "BitDefender" with a close button (X) in the top right corner. The main title of the dialog is "Passwort eingeben". Below the title, there is a short paragraph of text: "Aus Sicherheitsgründen ist ein Passwort erforderlich um einem Netzwerk beizutreten oder ein Neues zu erstellen. (Es schützt den Zugriff auf Ihren Computer über das Netzwerk)". Underneath this text are two input fields. The first is labeled "Passwort eingeben:" and the second is labeled "Passwort wiederholen:". At the bottom of the dialog, there are two buttons: "OK" and "Abbrechen".

Passwort konfigurieren

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

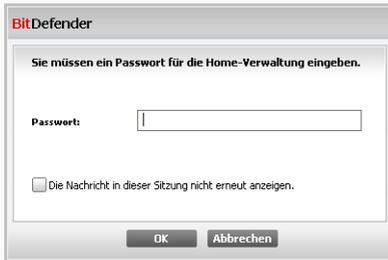
Sie sehen den Namen des Computers in der Netzwerkübersicht.

21.2. Computer zum BitDefender-Netzwerk hinzufügen

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

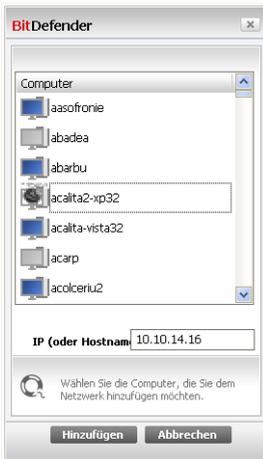
Um einen Computer zum BitDefender Home-Netzwerk hinzuzufügen, befolgen Sie die folgenden Schritte:

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



Passwort eingeben

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



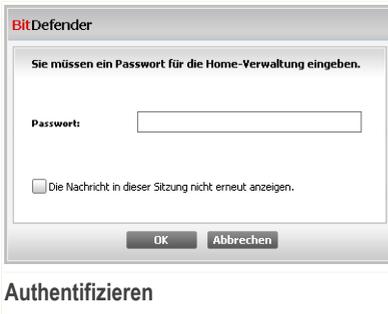
Computer hinzufügen

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

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



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



The screenshot shows a dialog box titled "BitDefender". The main text reads: "Sie müssen ein Passwort für die Home-Verwaltung eingeben." Below this is a label "Passwort:" followed by a text input field. At the bottom left, there is a checkbox with the text "Die Nachricht in dieser Sitzung nicht erneut anzeigen." At the bottom right, there are two buttons: "OK" and "Abbrechen". Below the dialog box, the word "Authentifizieren" is written in a larger font.

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



Anmerkung

Sie können bis zu fünf Computern zu der Netzwerkübersicht hinzufügen.

21.3. Das BitDefender-Netzwerk verwalten

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



BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es besteht noch 1 Problem ALLE BEHEBEN

Netzwerk

INTERNET

mscrlat
10.10.17.37
1 Risiken
Testversion

mscrlat
Dieser Comp

Kein PC (klick
hinzufügen)

Kein PC (klick
hinzufügen)

Kein PC (klicken Sie hier um

Diesen Computer registrieren (mit Lizenzschlüssel)
Passwort für Einstellungen festlegen
Prüfung ausführen
Probleme auf diesem Computer feststellen
Historie dieses Computers anzeigen
Ein Update auf diesem Computer ausführen
Profil anwenden
Eine Tuning-Aufgabe auf diesem Computer ausführen
Diesen Computer als Update-Server für das Netzwerk einrichten

Computer hinzufügen Netzwerk verlassen Aktualisieren

This item represents a computer in your home network. To add a PC you have to join or create a network by clicking on "Join/Create Network".

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignisse

Netzwerkübersicht

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

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

- **Diesen Computer registrieren**
- **Passwort für Einstellungen einstellen**
- **Prüf-Aufgabe ausführen**
- **Risiken auf diesem Computer feststellen**
- **Historie dieses Computers anzeigen**
- **Jetzt ein Update auf diesem Computer durchführen**



- Profil anwenden
- Tuning-Aufgabe auf diesem Computer durchführen
- Diesen Computer als Update-Server für dieses Netzwerk festlegen

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

Passwort eingeben

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



Anmerkung

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



22. Update (Aktualisierung)

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

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

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

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

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates für die AntiViren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virendefinitions-Update**.
- **Updates für die AntiSpyware Prüfung** - Neue Spyware Signaturen werden kontinuierlich zur BitDefender Datenbank hinzugefügt. Diesen Vorgang nennt man **AntiSpyware-Update**.
- **Produkt-Update** - Wenn eine neue Version von BitDefender erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Produkt-Update**.

22.1. Automatisches Update

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



BitDefender Antivirus 2009 - Testversion ZUR BASISANSICHT WECHSELN

STATUS: Es besteht noch 1 Problem DIESES PROBLEM

Update Einstellungen

Allgemein
Antivirus
Privatsphäre
Prüfung auf Schwachstellen
Verschlüsselung
Spiele-/Laptop-Modus
Netzwerk
Update
Registrierung

Automatisches Update ist aktiviert

Letzte Prüfung: 8/18/2008 8:31:05 PM
Letztes Update: 8/18/2008 8:31:36 PM **Jetzt aktualisieren**

Virensignatur-Eigenschaften

Virensignaturen: 1564751
Engine-Version: 7.20573 **Virenlste anzeigen**

Download-Status

Datei: 0 % 0 kb
Gesamtes Update 0 % 0 kb

Das Netzwerk-Modul zeigt die BitDefender Home-Netzwerkstruktur an (grau hinterlegt, falls das Home-Netzwerk nicht konfiguriert sein sollte).
Klicken Sie auf 'Netzwerk' um mit der Erstellung Ihres Home-Netzwerks zu beginnen.

bitdefender Kaufen - Benutzerkonto - Registrieren - Hilfe - Support - Ereignis

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 **Virenlste 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 Virenlste** klicken, um auf die Online-Signaturdatenbank von BitDefender zuzugreifen.



22.1.1. 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.

22.1.2. Automatisches Update deaktivieren

Wenn Sie das Automatische Update deaktivieren erscheint ein Warnfenster.



Automatisches Update deaktivieren

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



Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen die Deaktivierungszeit so gering wie möglich zu halten da BitDefender Sie nur gegen die neusten Bedrohungen schützen kann wenn dieser aktuell ist.



22.2. 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 separat beschrieben.



22.2.1. Update-Adresse

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



Anmerkung

Ändern Sie diese Einstellungen 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. 192)

22.2.2. 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 **Zeitintervall** 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 fragt den Benutzer bevor ein Update installiert wird.



22.2.3. 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.

22.2.4. Weitere Einstellungen konfigurieren

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

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



Anmerkung

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

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

22.2.5. 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.

Proxyeinstellungen

Administrator Proxyeinstellungen (Zum Installationszeitpunkt erkannt)

Adresse: Port: Benutzername:
Passwort:

Momentaner Benutzer Proxyeinstellungen (Aus Standard-Browser)

Adresse: Port: Benutzername:
Passwort:

Definieren Sie Ihre eigenen Proxyeinstellungen

Adresse: Port: Benutzername:
Passwort:

Hier können Sie die Administrator Proxyeinstellungen ändern.

OK Abbrechen

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 eingeloggtten Benutzers verwendeten Browser werden übernommen. Sollte ein Benutzername und Passwort nötig sein so geben Sie diesen in die dafür vorgesehenen Felder ein.



Anmerkung

Die unterstützten 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 Administrator 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 verwendet. Wenn auch dies nicht zum Erfolg 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.



23. Registrierung

Um komplette Informationen über Ihr BitDefender-Produkt und den Registrierungsstatus zu erhalten, klicken Sie auf **Registrierung** in der erweiterten Ansicht.

Registrierung

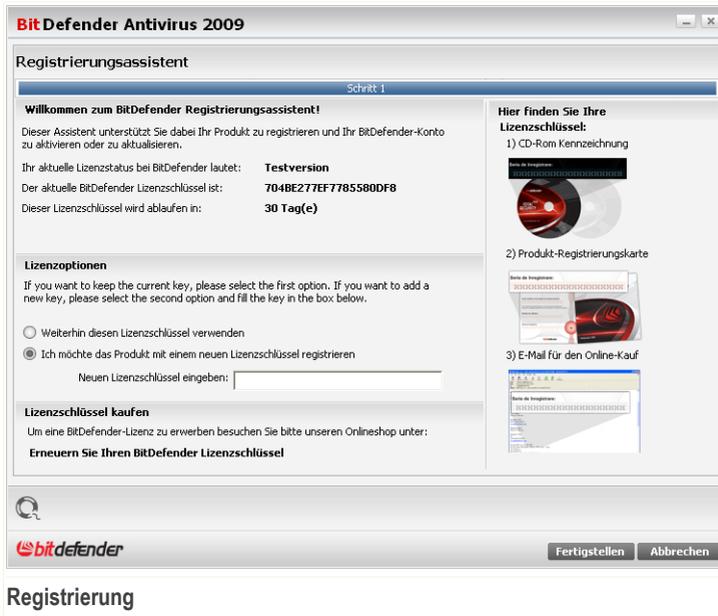
In diesem Abschnitt werden folgende Bereiche angezeigt:

- **Produktinformation:** Das BitDefender-Produkt und die Version.
- **Registrierungsinformationen:** Die E-Mail-Adresse die verwendet wurde um Ihr BitDefender Benutzerkonto (falls konfiguriert) zu erstellen, der aktuelle Lizenzschlüssel und wie viele Tage verbleiben bis die Lizenz abläuft.



23.1. BitDefender Antivirus 2009 registrieren

Klicken Sie auf **Jetzt registrieren** um das Fenster für die Produktregistrierung zu öffnen.



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

BitDefender Antivirus 2009 registrieren:

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



Anmerkung

- Sie finden den Lizenzschlüssel:
- Auf dem CD-Aufdruck.
 - Auf der Registrierungskarte des Produktes.



- In der E-Mail-Bestätigung des Online-Kaufs.

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

Klicken Sie auf **Fertigstellen**.

23.2. Ein BitDefender Benutzerkonto erstellen

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



Wichtig

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

Wenn Sie noch kein BitDefender-Benutzerkonto erstellt haben, klicken Sie auf **Ein Benutzerkonto erstellen** um das Fenster für die Benutzerkontoregistrierung zu öffnen.



BitDefender Antivirus 2009

Benutzerkonto erstellen

Schritt 1

Registrierung meines Kontos

Informationen über ein existierendes BitDefender Benutzerkonto wurden auf Ihrem PC gefunden. Das BitDefender Benutzerkonto gewährt Ihnen Zugriff zum technischen Support, zu Spezialangeboten und Sonderaktionen. Wenn Sie Ihren Lizenzschlüssel für BitDefender verlieren, können Sie ihn wiederherhalten, indem Sie sich unter <http://myaccount.bitdefender.com> einloggen. Sie können sich in ein existierendes BitDefender Benutzerkonto einloggen oder ein Neues erstellen.

<input checked="" type="radio"/> In ein existierendes Benutzerkonto einloggen	<input type="radio"/> Ein neues BitDefender Benutzerkonto erstellen
E-Mail-Adresse: <input type="text"/>	E-Mail-Adresse: <input type="text"/>
Passwort: <input type="text"/>	Passwort: <input type="text"/>
Passwort vergessen?	Passwort erneut eingeben: <input type="text"/>
	Vorname: <input type="text"/>
	Nachname: <input type="text"/>
	Land: <input type="text"/>
<input type="radio"/> Registrierung überspringen	

Send me all messages from BitDefender
 Send me only the most important messages
 Don't send me any messages

Fertigstellen **Abbrechen**

Kontoerstellung

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

- „Ich habe noch kein BitDefender-Benutzerkonto“ (S. 198)
- „Ich habe bereits ein BitDefender Nutzerkonto.“ (S. 199)

Ich habe noch kein BitDefender-Benutzerkonto

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

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.
- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort sollte mindestens 6 Zeichen haben.



- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.
- **Land** - wählen Sie das Land Ihres Wohnsitzes aus.



Anmerkung

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

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

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

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

Klicken Sie auf **Fertigstellen**.

Ich habe bereits ein BitDefender Nutzerkonto.

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

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

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

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

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



- **Senden Sie mir keine Nachrichten**

Klicken Sie auf **Fertigstellen**.



Hilfe erhalten



24. Support

Als eines der führenden Dienstleistungsunternehmen für IT Sicherheitslösungen möchten wir Ihnen eine möglichst schnelle, kompetente und unkomplizierte technische Unterstützung bei auftretenden Fragen anbieten. Unser technischer Support ist zu diesem Zweck stets mit den aktuellsten Virensignaturen, neuesten Informationen und präzisen Antworten auf wiederkehrende Fragen ausgestattet.

Insbesondere zeichnet sich BITDEFENDER durch ein hohes Maß an Innovation, ein hervorragendes Preis-Leistungsverhältnis und eine kurze Reaktionszeit in allen Belangen aus. Kundenzufriedenheit ist für uns nicht nur eine Floskel, sondern Firmenphilosophie.

Wir freuen uns auf die Kontaktaufnahme zu unseren technischen Support und stehen Ihnen mit Rat und Tat zur Seite. Nutzen Sie hierfür einfach unseren E-Mail Kontakt support@bitdefender.de oder rufen Sie uns Werktags unter +49 2301 91 84 555 an. Falls Sie den Weg über E-Mail bevorzugen, teilen Sie uns bitte mit, welches Produkt und Betriebssystem Sie verwenden und beschreiben Sie das aufgetretene Problem so detailliert als möglich.

24.1. BitDefender Knowledge Base

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

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

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



24.2. Nach Hilfe fragen

24.2.1. Zur Web-Selbstbedienung gehen

Fragen zur Installation? Montags bis Freitags von 08.00 Uhr bis 20.00 Uhr stehen Ihnen unsere deutschsprachigen Techniker kostenfrei gerne zur Verfügung.

Bitte folgen Sie den Links:

Deutsch

<http://www.bitdefender.com/de/KnowledgeBase/>

Englisch

<http://www.bitdefender.com/site/KnowledgeBase/>

Französisch

<http://www.bitdefender.com/fr/KnowledgeBase/>

Romanian

<http://www.bitdefender.com/ro/KnowledgeBase/>

Spanish

<http://www.bitdefender.com/es/KnowledgeBase/>

24.2.2. Ein Supportticket öffnen

Wenn Sie ein Supportticket und Hilfe per EMail erhalten möchten, folgen Sie einem der folgenden Links:

Deutsch: <http://www.bitdefender.de/site/Main/contact/1/>

English: <http://www.bitdefender.com/site/Main/contact/1/>

French: <http://www.bitdefender.fr/site/Main/contact/1/>

Romanian: <http://www.bitdefender.ro/site/Main/contact/1/>

Spanish: <http://www.bitdefender.es/site/Main/contact/1/>



24.3. Kontaktinformation

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

24.3.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de

Technische Unterstützung: support@bitdefender.de

Dokumentation documentation@bitdefender.com

Partner Programm: vertrieb@bitdefender.de

Marketing: marketing@bitdefender.de

Media Relations presse@bitdefender.de

Jobs: jobs@bitdefender.de

Virus Einsendungen: virus_submission@bitdefender.com

Spam Einsendungen: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Produkt Webseite: <http://www.bitdefender.de>

Produkt ftp Archive: <http://www.bitdefender.de>

Local distributors: http://www.bitdefender.com/partner_list

BitDefender Knowledge Base: <http://kb.bitdefender.de>

24.3.2. Niederlassungen

Die BitDefender Niederlassungen stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

Deutschland

BitDefender GmbH

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Hotline: +49 2301 91 84 555



Technische Beratung: support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: <http://www.bitdefender.de>

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Telefon: 1-954-776-6262
Web: <http://www.bitdefender.com>

Technischer Support (Nur registrierte Benutzer):

- E-mail: support@bitdefender.de
- Telefon (gebührenfrei):
 - USA: 1-888-868-1873
 - Kanada: 1-866-947-1873

Kundenservice (Nur registrierte Benutzer):

- E-mail: customerservice@bitdefender.com
- Telefon (gebührenfrei):
 - USA: 1-888-868-1873
 - Kanada: 1-866-947-1873

Großbritannien und Irland

Business Center 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Tel: +40 21 - 233 07 80
Email support@bitdefender.de
Vertrieb: vertrieb@bitdefender.de
Web: <http://www.bitdefender.co.uk>
Technische Unterstützung: support@bitdefender.de

Spain

Constelación Negocial, S.L

C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com



Ventas: comercial@bitdefender-es.com
Tel: +34 932189615
Fax: +34 932179128
Sitio web del producto: <http://www.bitdefender-es.com>

Romania

BITDEFENDER

West Gate Park, Building H2, 24 Preciziei Street
Tettngang

Technische Unterstützung: support@bitdefender.de

Vertrieb: vertrieb@bitdefender.de

Tel.: +40 21 3001226; +40 21 3001227; +40 21 3001228; +40 21 3001229

Fax: +40 21 2641799

Produkt Webseite: <http://www.bitdefender.de>



BitDefender Antivirus 2009

BitDefender Notfall CD



25. Übersicht

BitDefender Antivirus 2009 verfügt über eine bootfähige CD-ROM (BitDefender Notfall CD) die fähig ist, alle Festplatten zu prüfen und zu desinfizieren, bevor Ihr Betriebssystem startet.

Sie sollten die BitDefender Notfall CD immer dann verwenden, wenn Ihr System aufgrund von Virusinfektionen nicht mehr richtig funktioniert. Dies passiert für gewöhnlich, wenn Sie kein AntiVirus-Programm benutzen.

Das Update der Virensignaturen wird automatisch ohne Benutzereingriff jedes Mal vollzogen, wenn Sie die BitDefender Notfall CD starten.

Die BitDefender Notfall CD ist eine mit BitDefender erweiterte Knoppix-Distribution, welche die neueste Version von BitDefender für Linux in das GNU/Linux integriert. Es beinhaltet einen SMTP Antivirus/Antispam-Schutz und einen On Demand Scanner, der in der Lage ist, Festplatten (inkl. Windows NTFS-Partition), Samba-Freigaben und NFS Mount Points zu überprüfen und zu desinfizieren. Ausserdem kann er verwendet werden um Daten wiederherzustellen wenn Windows nicht mehr startet.



Anmerkung

Die BitDefender Rescue CD kann unter folgendem Link heruntergeladen werden:
http://download.bitdefender.com/rescue_cd/

25.1. Systemanforderungen

Bevor Sie die BitDefender Notfall CD booten, stellen Sie bitte sicher dass Ihr System die folgenden Voraussetzungen erfüllt:

Prozessortyp

X86 kompatibel mit einem Minimum von 166 MHz, aber bitte erwarten Sie in diesem Falle keine zufrieden stellende Systemleistung. Eine i686 Prozessorgeneration mit 800 MHz wäre die bessere Wahl.

Speicher

512 MB Arbeitsspeicher (1 GB empfohlen)

CD-ROM

CD-Rom-Laufwerk und die BIOS-Einstellungen, um von CD zu booten.

Internetverbindung

Obwohl die BitDefender Notfall CD auch ohne Internetverbindung lauffähig ist, benötigen die Update-Vorgänge eine aktive HTTP-Verbindung oder durch einen



Proxy Server. Daher ist für einen aktuellen Schutz eine Internetverbindung ein MUSS.

Grafische Auflösung

Standard SVGA-kompatible Grafikkarte.

25.2. Integrierte Software

Die BitDefender Notfall CD enthält die folgenden Software-Pakete.

Xedit

Dies ist ein Texteditor.

Vim

Hierbei handelt es sich um einen mächtigen Texteditor mit Syntax hervorhebung, GUI und vielem mehr. Für mehr Informationen besuchen Sie die [Vim Webseite](#).

Xcalc

Ist ein Taschenrechner.

RoxFiler

RoxFiler ist ein schneller grafischer Dateimanager.

Für weitere Informationen besuchen Sie die [RoxFiler Webseite](#).

MidnightCommander

GNU Midnight Commander (mc) ist ein textbasierender Dateimanager.

Für mehr Informationen besuchen Sie die [MC Webseite](#).

Pstree

Pstree zeigt die laufenden Prozesse an.

Top

Top zeigt die Linux Tasks an.

Xkill

Xkill beendet einen Client nach seinen X-Quellen.

Partition Image

Partition Image hilft Ihnen dabei EXT2, Reiserfs, NTFS, HPFS, FAT16, und FAT32 Dateisysteme in Imagedateien zu sichern. Dieses Programm kann für Backupzwecke sinnvoll sein.

Für weitere Informationen besuchen Sie die [Partimage Webseite](#).



GtkRecover

GtkRecover ist eine grafische Version des Konsolenprogramms Recover. Es hilft Ihnen beim Sichern von Dateien.

Für mehr Informationen besuchen Sie die [GtkRecover Webseite](#).

ChkRootKit

ChkRootKit ist ein Programm welches Ihnen bei der Suche nach Rootkits hilft.

Für mehr Informationen besuchen Sie die [ChkRootKit Webseite](#).

Nessus Network Scanner

Nessus ist ein Remote-Sicherheitsscanner für Linux, Solaris, FreeBSD, und Mac OS X.

Für weitere Informationen besuchen Sie die [Nessus Webseite](#).

lpraf

lpraf ist eine IP Netzwerk-Monitoring Software.

Für weitere Informationen besuchen Sie die [lpraf Webseite](#).

lftop

lftop zeigt die verwendete Bandbreite für eine Schnittstelle an.

Für mehr Informationen besuchen Sie die [lftop Webseite](#).

MTR

MTR ist ein Netzwerkd Diagnose-Tool.

Für weitere Informationen besuchen Sie die [MTR Webseite](#).

PPPStatus

PPPStatus zeigt Statistiken zum ein- und ausgehenden TCP/IP Verkehr.

Für weitere Informationen besuchen Sie die [PPPStatus Webseite](#).

Wavemon

Wavemon ist eine Monitoring-Anwendung für Kabellose Netzwerke.

Für mehr Informationen besuchen Sie die [Wavemon Webseite](#).

USBView

USBView zeigt Informationen über angeschlossene USB Geräte.

Für mehr Informationen besuchen Sie die [USBView Webseite](#).

Pppconfig

Pppconfig hilft bei der automatischen Erstellung einer PPP-Wahlverbindung.



DSL/PPPoE

DSL/PPPoE konfiguriert eine PPPoE (ADSL) Verbindung.

i810rotate

i810rotate aktiviert den Video Output auf i810 Hardware unter Verwendung von i810switch(1).

Für weitere Informationen besuchen Sie die [i810rotate Webseite](#).

Mutt

Mutt ist ein mächtiger textbasierender MIME Mail Client.

Für weitere Informationen besuchen Sie die [Mutt Webseite](#).

Mozilla Firefox

Mozilla Firefox ist ein bekannter Internet Browser.

Für weitere Informationen besuchen Sie die [Mozilla Firefox Webseite](#).

Elinks

Elinks ist ein textbasierter Internet Browser.

Für weitere Informationen besuchen Sie die [Elinks Webseite](#).



26. BitDefender Notfall CD Anleitung

Dieses Kapitel enthält Informationen darüber wie Sie die BitDefender Notfall CD starten und stoppen, zum Prüfen auf Schädlinge sowie zum Sichern von Daten verwenden können. Mit den in der BitDefender Notfall CD enthaltenen Programmen erhalten Sie mächtige Werkzeuge auf welche wir leider nicht alle eingehen können.

26.1. BitDefender Notfall CD starten

Um von der CD-ROM starten zu können, müssen Sie zunächst das BIOS Ihres Computers so konfigurieren, dass die Bootreihenfolge folgendermaßen aussieht: CD-ROM Laufwerk, Floppy-Laufwerk, Festplatte.

Starten Sie nun Ihren Computer neu und warten Sie, bis der initiale Bootvorgang abgeschlossen wurde. Sie bekommen nun den BitDefender Notfall CD Startbildschirm angezeigt. Folgen Sie nun bitte den auf dem Bildschirm angegebenen Schritten.



Anmerkung

Wählen Sie aus der Liste die Sprache die Sie für die Notfall CD verwenden möchten



LinuxDefender Startbildschirm



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

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



Der LinuxDefender Desktop

26.2. BitDefender Notfall CD stoppen

Sie können den Computer sicher herunterfahren indem Sie den Menüpunkt **Exit** im Kontextmenü (Rechtsklick) wählen. Alternativ verwenden Sie das **halt** Kommando im Terminal.



Wählen Sie "EXIT"

Sobald die BitDefender Notfall CD alle Programme beendet hat, bekommen Sie das folgende Bild angezeigt. Sobald dieses angezeigt wird, können Sie die CD aus dem Laufwerk entfernen, den Einschub schließen und den Computer neu starten.



```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
(d) (khsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Warten auf diese Nachricht, wenn der Rechner heruntergefahren wird

26.3. Wie führe ich einen Prüfvorgang durch?

Nachdem der Rechner gestartet wurde wird ein Assistent geöffnet welcher Ihnen hilft einen vollständigen Prüfvorgang Ihres Rechners durchzuführen. Alles was Sie tun müssen ist auf die **Start** Schaltfläche zu klicken.



Anmerkung

Wenn Ihre Bildschirmauflösung nicht hoch genug ist werden Sie gefragt ob Sie im Textmodus starten möchten.

Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

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



Anmerkung

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

2. Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.
Die Risiken werden in Gruppen angezeigt. Klicken Sie auf "+", um eine Gruppe zu öffnen, und auf "-", um diese wieder zu schließen.



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

3. Ihnen wird eine Zusammenfassung angezeigt.

Wenn Sie ein bestimmtes Verzeichniss prüfen möchten dann befolgen Sie die folgenden Schritte:

Wählen Sie die gewünschten Ordner aus und klicken Sie per Rechtsklick auf diese. Wählen Sie nun aus dem Kontextmenü den Eintrag **Send to** und klicken Sie nun auf **BitDefender Scanner**.

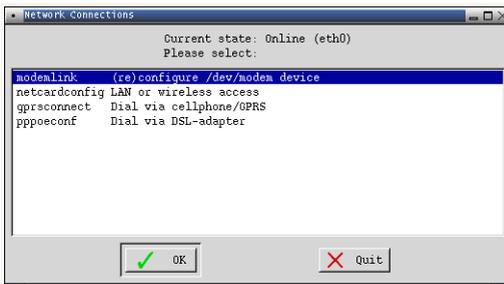
Oder Sie können den folgenden Befehl als Root von einem Terminal ausgeben. Der **BitDefender Antivirus-Scanner** beginnt mit der ausgewählten Datei oder Pfad als Default-Position zu scannen.

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

26.4. Wie kann ich die Internetverbindung konfigurieren?

Falls Sie über ein Netzwerk mit DHCP-Funktionalität verfügen und eine Netzwerkkarte in Ihrem Computer installiert ist, sollte LinuxDefender die notwendigen Einstellungen automatisch erkennen. Für eine manuelle Konfiguration folgen Sie bitte den folgenden Schritten.

1. Doppelklicken Sie auf die Verknüpfung für Netzwerkverbindungen auf Ihrem Arbeitsplatz. Das folgende Fenster erscheint.



Netzwerkverbindungen



2. Wählen Sie die Verbindung, die Sie verwenden und klicken Sie auf OK.

Verbindung	Beschreibung
modemlink	Wählen Sie diese Verbindung, wenn Sie ein Modem und eine Telefonleitung verwenden um eine Verbindung zum Internet herzustellen.
netcardconfig	Wählen Sie diese Verbindung, wenn Sie über ein LAN-Netzwerk die Verbindung zu dem Internet herstellen. Dies gilt auch für drahtlose Verbindungen.
gprsconnect	Wählen Sie diese Verbindung, wenn Sie über ein Handynetzwerk unter Verwendung eines GPRS (General Packet Radio Service) Protokolls eine Verbindung zu dem Internet herstellen. Sie können auch ein GPRS-Modem anstelle eines Handys verwenden.
pppoeconf	Wählen Sie diese Verbindung, wenn Sie über ein DSL-Modem eine Verbindung mit dem Internet herstellen.

3. Folgen Sie den Instruktionen auf dem Bildschirm. Wenn Sie nicht sicher sein sollten was Sie schreiben sollen, konsultieren Sie Ihren Netzwerkadministrator.



Wichtig

Bitte achten Sie darauf, dass Sie nur mit den oben genannten Optionen das Modem aktivieren. Um die Netzwerkverbindung zu konfigurieren, befolgen Sie diese Schritte.

1. Klicken Sie mit der rechten Maustaste auf den Desktop. Das Kontextmenu der BitDefender Rescue CD erscheint.
2. Wählen Sie **Terminal (als Root)**.
3. Geben Sie die folgenden Befehle ein:

```
# pppconfig
```

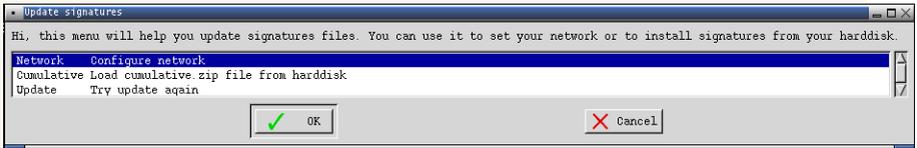
4. Folgen Sie den Instruktionen auf dem Bildschirm. Wenn Sie nicht sicher sein sollten was Sie schreiben sollen, konsultieren Sie Ihren Netzwerkadministrator.



26.5. Wie kann ich BitDefender aktualisieren?

Nach dem Starten wird automatisch ein Virensignaturupdate durchgeführt. Wenn Sie diesen Schritt jedoch übersprungen haben, können Sie hier erfahren wie BitDefender aktualisiert werden kann.

1. Doppelklicken sie auf die Verknüpfung für Signatur-Updates auf dem Arbeitsplatz. Das folgende Fenster erscheint.



Signatur-Updates

2. Sie können hierzu eine der folgenden Methoden wählen:
 - Klicken Sie auf **Gesammelt** um Signaturen zu installieren die sich bereits auf Ihrer Festplatte befinden, indem Sie Ihren Computer durchsuchen und die `Dateicumulative.zip` laden.
 - Wählen Sie **Update** um eine sofortige Verbindung mit dem Internet herzustellen und die aktuellsten Virensignaturen herunterzuladen.
3. Klicken Sie auf **OK**.

26.5.1. Wie kann ich BitDefender über einen Proxy-Server aktualisieren?

Wenn ein Proxy-Server zwischen Ihrem Computer und dem Internet besteht, müssen einige Einstellungen vorgenommen werden, um die Erkennung von Virenstrukturen zu aktualisieren.

Um BitDefender über einen Proxy-Server zu aktualisieren, befolgen Sie die folgenden Schritte:

1. Klicken Sie mit der rechten Maustaste auf den Desktop. Das Kontextmenu der BitDefender Rescue CD erscheint.
2. Wählen Sie **Terminal (als Root)**.
3. Geben Sie folgenden Befehl ein: `cd /ramdisk/BitDefender-scanner/etc`.
4. Geben Sie folgenden Befehl ein: `mcedit bdscan.conf` to edit this file by using GNU Midnight Commander (mc).



5. Kommentieren Sie die folgende Zeile aus: `#HttpProxy =` (löschen Sie nur das Zeichen #), und geben Sie die Domain, den Benutzernamen, das Passwort und den Server-Port des Proxy-Servers ein. Die entsprechende Zeile muss beispielsweise so aussehen:

```
HttpProxy = myuser:mypassword@proxy.company.com:8080
```

6. Drücken Sie **F2** um die aktuelle Datei zu speichern und drücken Sie dann **F10** um Sie zu schließen.
7. Geben Sie folgenden Befehl ein: **bdscan update**.

26.6. Wie sichere ich meine Daten?

Nehmen wir einmal an das Sie Ihre Betriebssystem aus unbekanntem Gründen nicht mehr starten können. Sie jedoch dringend wichtigen Daten von Ihrem Computer benötigen. Hier kann Ihnen die BitDefender Notfall CD behilflich sein.

Um Ihre Daten von Ihrem Computer auf einen Wechseldatenträger, wie z.B. einen USB Stick zu sichern befolgen Sie die folgenden Schritte:

1. Legen Sie die BitDefender Notfall CD in das CD-Laufwerk, stecken Sie den USB Stick ein und starten Sie dann Ihren Computer neu.



Anmerkung

Wenn Sie den USB Stick später verbinden müssen Sie das externe Gerät mit den folgenden Schritte mounten:

- a. Klicken Sie auf die Verknüpfung Terminal Emulator auf dem Arbeitsplatz.
- b. Geben Sie den folgenden Befehl ein:

```
# mount /media/sdb1
```

Bitte beachten Sie, dass dies je nach Ihrer Computerkonfiguration `sda1` anstelle von `sdb1` sein kann.

2. Warten Sie bis die BitDefender Notfall CD gestartet wurde. Das folgende Fenster erscheint.



Der Desktop

3. Doppelklicken Sie die Partition auf welcher die Daten gespeichert sind (z.B. [sda3]).



Anmerkung

Wenn Sie mit der BitDefender Notfall CD arbeiten werden Sie mit Linux-Partitionenamen in Kontakt kommen. So kann [sda1] zum Beispiel für Laufwerk (C:) Ihrer Windows Partition stehen, [sda3] für (F:), und [sdb1] für den USB Stick.



Wichtig

Wenn der Computer nicht ordnungsgemäß heruntergefahren wurde, kann es sein, dass bestimmte Partitionen nicht automatisch gemountet wurden. Um eine Partition zu mounten, befolgen Sie diese Schritte.

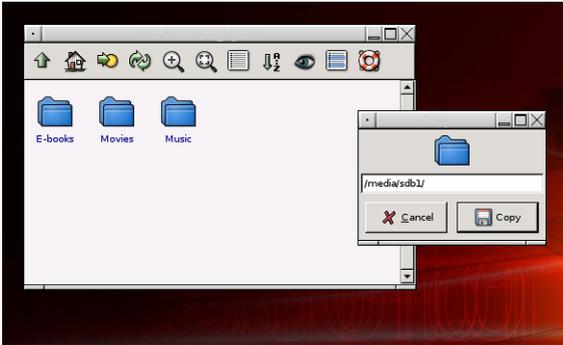
- a. Klicken Sie auf die Verknüpfung Terminal Emulator auf dem Arbeitsplatz.
- b. Geben Sie den folgenden Befehl ein:

```
# mount /media/partition_name
```

4. Durchsuchen Sie die Partitionen nach den gewünschten Dateien und Ordnern. Für Instanz, Meine Daten enthält Filme, Musik und E-books Sub-Datenverzeichnisse.



5. Rechtsklicken Sie den gewünschten Ordner und wählen Sie **Copy**. Das folgende Fenster erscheint.



Daten speichern

6. Tippen Sie `/media/sdb1/` in das vorgesehene Feld und klicken Sie dann auf **Copy**.

Bitte beachten Sie, dass dies je nach Ihrer Computerkonfiguration `sda1` anstelle von `sdb1` sein kann.



Glossar

AktiveX

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

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

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, andererseits 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 Netzwerkservers 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 Virens Scanner 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 einem normalen 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 stattgefundenen Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit den 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 abrufen. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet heruntergeladen 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 besteht Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

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

Symbolleiste

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

TCP/IP

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

Trojaner

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

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



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

Update (Aktualisierung)

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

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

Virus

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

Virusdefinition

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

Wurm

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