AVG 9 Internet Security

Benutzerhandbuch

Dokumentversion 90.6 (14.9.2009)

Inhalt

1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG 9 Internet Security**.

Herzlichen Glückwunsch zum Kauf von AVG 9 Internet Security!

AVG 9 Internet Security zählt zu einer Reihe von preisgekrönten AVG-Produkten, die vollständige Sicherheit für Ihren PC bieten, damit Sie in Ruhe arbeiten können. Wie alle AVG-Produkte wurde **AVG 9 Internet Security** von Grund auf vollkommen neu gestaltet, um den anerkannten Schutz von AVG noch benutzerfreundlicher und effizienter bereitzustellen.

Ihr neues Produkt **AVG 9 Internet Security** verfügt über eine optimierte Oberfläche sowie aggressivere und schnellere Scans. Die Anzahl der automatisierten Sicherheitsfunktionen wurde zu Ihrer Unterstützung erhöht und neue ‚intelligente' Benutzeroptionen hinzugefügt, damit Sie unsere Sicherheitsfunktionen besser an Ihre Bedürfnisse anpassen können. Einfache Verwendung und hohe Sicherheit schließen einander nicht aus!

AVG wurde entwickelt, um Ihre Computer- und Netzwerkaktivitäten zu schützen. Genießen Sie den vollständigen Rundumschutz von AVG.

2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG 9 Internet Security wurde für den Schutz von Workstations mit den folgenden Betriebssystemen entwickelt:

- Windows 2000 Professional SP4 + Updaterollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 und x64, alle Editionen)
- Windows 7 (x86 und x64, alle Editionen)

(sowie ggf. höhere Service Packs für bestimmte Betriebssysteme)

***Hinweis**: Die Komponente Identitätsschutz wird von Windows 2000 und XP x64 nicht unterstützt. Bei diesen Betriebssystemen können Sie AVG 9 Internet Security installieren, jedoch ohne die Komponente Identitätsschutz.*

2.2. Minimale Hardware-Anforderungen

Hardware-Mindestanforderungen für **AVG 9 Internet Security**:

- Intel Pentium CPU 1,2 GHz
- 250 MB freier Festplattenspeicher (für die Installation)
- 256 MB RAM-Speicher

3. Optionen für die Installation von AVG

AVG kann entweder mithilfe der Installationsdatei installiert werden, die sich auf Ihrer Installations-CD befindet, oder Sie können die neueste Installationsdatei von der Website von AVG (http://www.avg.com/) herunterladen.

Vor der Installation von AVG sollten Sie auf jeden Fall prüfen, ob auf der Website von AVG (http://www.avg.com/) eine neue Installationsdatei verfügbar ist. Auf diese Weise können Sie sicher sein, dass Sie die neueste verfügbare Version von AVG 9 Internet Security installieren.

Wir empfehlen, unser neues Tool AVG Download-Manager auszuprobieren, der die Auswahl der korrekten Installationsdatei einfacher macht!

Während des Installationsvorgangs werden Sie nach Ihrer Lizenz-/Vertriebsnummer gefragt. Halten Sie diese bereit, bevor Sie mit der Installation beginnen. Die Vertriebsnummer befindet sich auf der Verpackung der CD. Wenn Sie AVG online erworben haben, wurde Ihnen die Lizenznummer per eMail zugeschickt.

4. AVG Download-Manager

AVG Download-Manager ist ein einfaches Tool, mit dem Sie die geeignete Installationsdatei für Ihr AVG-Produkt auswählen können. Auf der Grundlage der eingegebenen Daten wählt der Manager das betreffende Produkt, den Lizenztyp, die gewünschten Komponenten und die Sprache aus. Abschließend fährt **AVG Download-Manager** mit dem Herunterladen fort und startet den entsprechenden Installationsvorgang.

Warnung: *Bitte beachten Sie, dass der AVG Download-Manager nicht für die Editionen Netzwerk und SBS heruntergeladen werden kann, da nur die folgenden Betriebssysteme unterstützt werden: Windows 2000 (SP4 + SRP Rollup), Windows XP (SP2 und höher), Windows Vista (alle Editionen).*

AVG Download-Manager kann von der Website von AVG (http://www.avg.com/) heruntergeladen werden. Nachfolgend finden Sie eine kurze Beschreibung der einzelnen Schritte, die Sie im **AVG Download-Manager** ausführen müssen:

4.1. Sprachauswahl

Wählen Sie im ersten Schritt von **AVG Download-Manager** die Installationssprache aus dem Dropdown-Menü aus. Beachten Sie, dass die Sprachauswahl nur für den Installationsvorgang gilt. Nach der Installation können Sie die Sprache direkt in den Programmeinstellungen ändern. Klicken Sie anschließend zum Fortfahren auf ***Weiter***.

4.2. Verbindung prüfen

Im folgenden Schritt versucht der **AVG Download-Manager**, eine Verbindung mit dem Internet aufzubauen, so dass nach neuen Updates gesucht werden kann. Der Download kann erst fortgesetzt werden, wenn der **AVG Download-Manager** die Überprüfung der Verbindung abgeschlossen hat.

- Wenn der Test zu dem Ergebnis kommt, dass keine Verbindung hergestellt werden kann, überprüfen Sie, ob Sie tatsächlich mit dem Internet verbunden sind. Klicken Sie anschließend auf ***Wiederholen***

- Wenn Sie sich über eine Proxy-Verbindung mit dem Internet verbinden, klicken Sie auf die Schaltfläche ***Proxy-Einstellungen***, um Ihre Proxy-Einstellungen festzulegen:

- Wenn die Überprüfung erfolgreich war, klicken Sie auf ***Weiter***, um fortzufahren.

4.3. Proxy-Einstellungen

Wenn **AVG Download-Manager** Ihre Proxy-Einstellungen nicht erkennen kann, müssen Sie sie manuelle angeben. Geben Sie bitte folgende Daten ein:

- ***Server*** – Geben Sie den gültigen Namen deines Proxy-Servers oder die IP-Adresse ein
- ***Port*** – Geben Sie die entsprechende Portnummer an
- ***Proxy-Authentifizierung verwenden*** – Wenn ihr Proxy-Server eine Authentifizierung benötigt, aktivieren Sie dieses Kontrollkästchen.
- ***Authentifizierung wählen*** – Wählen Sie aus dem Dropdown-Menü den Authentifizierungstyp aus. Wir empfehlen dringend, den Standardwert beizubehalten (*die Anforderungen des Proxy-Servers werden dann automatisch übernommen*). Sie können jedoch auch, insbesondere wenn Sie ein fortgeschrittener Benutzer sind, die Option Standard (*wird von einigen Servern benötigt*) oder NTLM (*wird von allen ISA-Servern benötigt*) verwenden. Geben Sie anschließend einen gültigen ***Benutzernamen*** und ein gültiges ***Kennwort*** (optional) ein.

Bestätigen Sie Ihre Einstellungen durch Klicken auf die Schaltfläche ***Übernehmen***, und fahren Sie mit dem nächsten Schritt von **AVG Download-Manager** fort.

4.4. Wählen Sie einen Lizenztyp.

In diesem Schritt werden Sie aufgefordert, den Lizenztyp des Produkts auszuwählen, das Sie herunterladen möchten. Mit Hilfe der angegebenen Beschreibung können Sie dasjenige Produkt auswählen, das Ihren Anforderungen an besten entspricht:

- ***Vollversion*** – d. h. ***AVG Anti-Virus***, ***AVG Anti-Virus plus Firewall*** oder ***AVG Internet Security***
- ***Testversion*** – Bietet Ihnen die Möglichkeit, 30 Tage lang alle Features der Vollversion des Produkts von AVG zu verwenden
- ***Kostenlose Version*** – Bietet kostenlosen Schutz für Heimanwender. Die Funktionen der Anwendung sind jedoch beschränkt! Die kostenlose Version enthält außerdem nur einige der Features, die in der Vollversion des Produkts zur Verfügung stehen.

4.5. Dateien für die Installation herunterladen

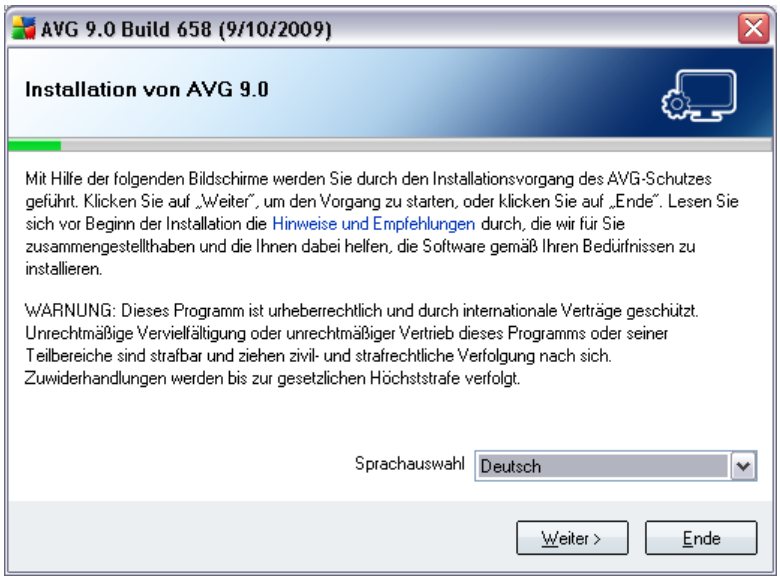
Sie haben jetzt alle Informationen angegeben, die der **AVG Download-Manager** benötigt, um das Installationspaket herunterzuladen und mit dem Installationsvorgang zu beginnen. Gehen Sie weiter zum AVG Installationsvorgang.

5. Installationsvorgang bei AVG

Für die Installation von auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. **AVG 9 Internet Security** Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei online herunterzuladen. Sie können die Datei von der Website von AVG (http://www.avg.com/) im Bereich ***Downloads*** herunterladen. Oder Sie können unser neues Tool ***AVG Download-Manager*** **verwenden**, das Ihnen dabei hilft, das von Ihnen benötigte Installationspaket zu erstellen und herunterzuladen und den Installationsvorgang zu starten.

Der Installationsvorgang besteht aus einer Abfolge von Dialogen, die jeweils eine kurze Beschreibung der erforderlichen Schritte enthalten. Im Folgenden werden die einzelnen Dialoge erläutert:

5.1. Beginn der Installation

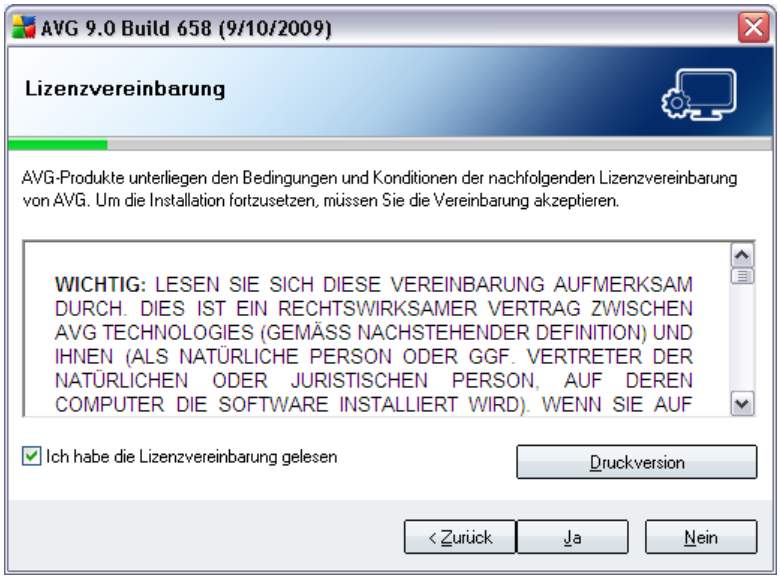


Zu Beginn des Installationsvorgangs wird das Fenster ***Installation von AVG 8.0*** angezeigt. Hier können Sie die Sprache für den Installationsvorgang auswählen. Im unteren Teil des Dialogs befindet sich die Option ***Sprache für die Installation auswählen***, wo Sie die gewünschte Sprache im Dropdown-Menü auswählen können. Klicken Sie anschließend auf ***Weiter***, um mit dem nächsten Dialog fortzufahren.

Achtung: *Hier wählen Sie nur die Sprache für den Installationsvorgang aus. Sie wählen nicht die Sprache für die AVG-Anwendung aus – diese können Sie später*

während des Installationsvorgangs festlegen!

5.2. Lizenzvereinbarung



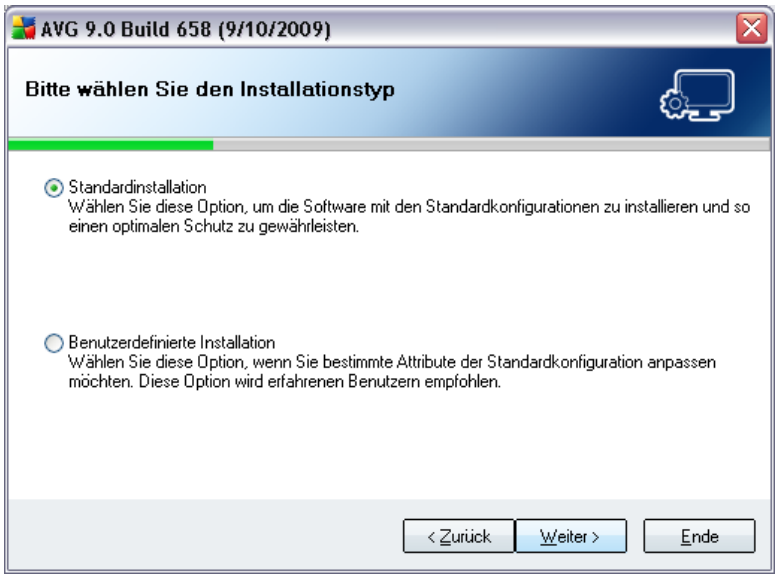
Der Dialog ***Lizenzvereinbarung*** enthält den vollständigen Text der Lizenzvereinbarung mit AVG. Bitte lesen Sie sich den Text sorgfältig durch, und bestätigen Sie, dass Sie die Vereinbarung gelesen, verstanden und akzeptiert haben, indem Sie das Kontrollkästchen ***Ich habe die Lizenzvereinbarung gelesen*** aktivieren und auf die Schaltfläche ***Akzeptieren*** klicken.

Falls Sie der Lizenzvereinbarung nicht zustimmen, klicken Sie auf ***Nicht akzeptieren*** , um den Installationsvorgang abzubrechen.

5.3. Systemstatus wird geprüft

Nachdem Sie die Lizenzvereinbarung akzeptiert haben, wird der Dialog ***Systemstatus wird geprüft...*** angezeigt. In diesem Dialog ist keine Aktion erforderlich. Das System wird geprüft, bevor die Installation von AVG gestartet werden kann. Bitte warten Sie, bis der Prozess abgeschlossen ist und der folgende Dialog angezeigt wird.

5.4. Bitte wählen Sie den Installationstyp



Im Dialog ***Installationstyp wählen*** können Sie zwischen zwei Installationsoptionen wählen: ***Standardinstallation*** und ***benutzerdefinierte Installation***.

Den meisten Benutzern wird empfohlen, die ***Standardinstallation*** beizubehalten, mit der AVG vollständig automatisch mit den vom Programmhersteller vordefinierten Einstellungen installiert wird. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration zukünftig geändert werden muss, können Sie diese Änderungen immer direkt in der Anwendung AVG vornehmen.

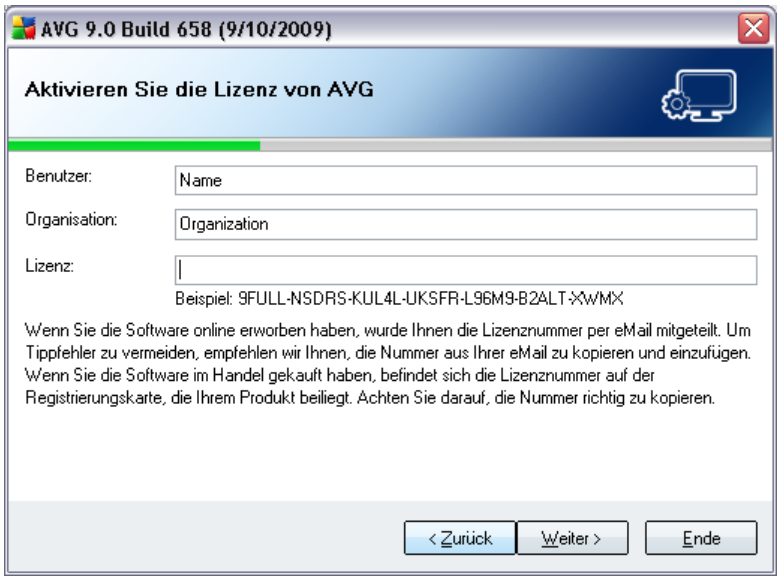
Die benutzerdefinierte Installation sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, AVG nicht mit den Standardeinstellungen zu installieren. Dies könnte beispielsweise der Fall sein, wenn bestimmte Systemanforderungen eingehalten werden müssen.

5.5. AVG Lizenz aktivieren

Im Dialog ***AVG-Lizenz aktivieren*** müssen Sie Ihre Registrierungsdaten eingeben. Geben Sie Ihren Namen (Feld ***Benutzer***) und den Namen Ihrer Organisation (Feld ***Organisation***) ein.

Geben Sie anschließend Ihre Lizenz-/Vertriebsnummer in das Textfeld ***Lizenznummer*** ein. Die Vertriebsnummer finden Sie auf der CD-Verpackung Ihres

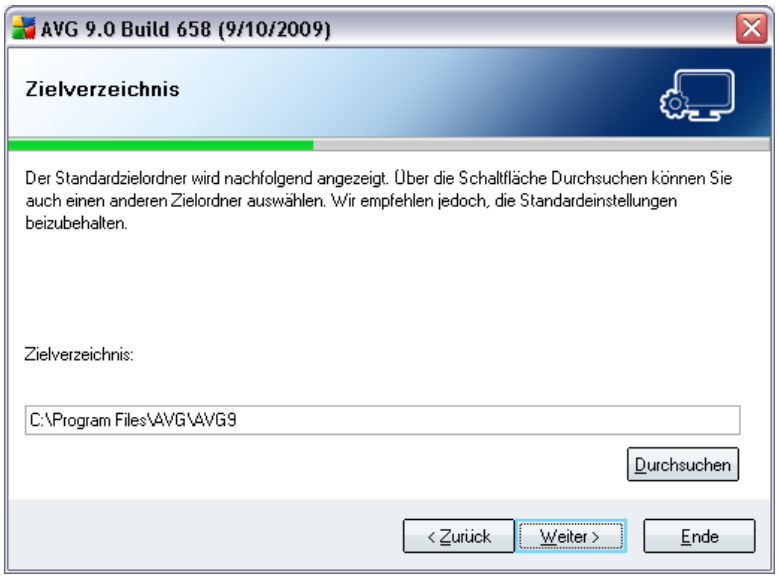
AVG 9 Internet Security -Pakets. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von **AVG 9 Internet Security** erhalten haben. Sie müssen die Nummer exakt wie dargestellt eingeben. Wenn die Lizenznummer in digitaler Form verfügbar ist (*in der eMail*), empfehlen wir Ihnen, diese zu kopieren und einzufügen.



Klicken Sie auf ***Weiter***, um mit der Installation fortzufahren.

Wenn Sie im vorherigen Schritt die Standardinstallation ausgewählt haben, werden Sie zum Dialog ***AVG Security Toolbar*** ***weitergeleitet.*** Wenn Sie die benutzerdefinierte Installation ausgewählt haben, wird der Dialog ***Zielverzeichnis*** angezeigt.

5.6. Benutzerdefinierte Installation – Zielverzeichnis

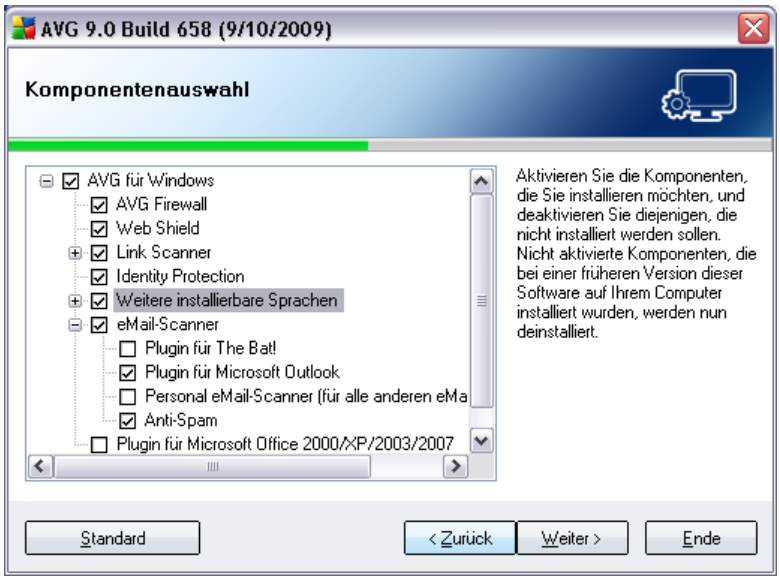


Im Dialog ***Zielverzeichnis*** können Sie den Speicherort für die Installation von **AVG 9 Internet Security** angeben. Standardmäßig wird AVG im Ordner C:/Programme installiert. Wenn der Ordner noch nicht existiert, werden Sie in einem Dialog dazu aufgefordert, der Erstellung dieses Ordners durch AVG zuzustimmen.

Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf ***Durchsuchen*** , um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus.

Klicken Sie zum Bestätigen auf ***Weiter***.

5.7. Benutzerdefinierte Installation – Komponentenauswahl



Im Dialog ***Komponentenauswahl*** wird eine Übersicht aller Komponenten von angezeigt, die installiert werden können. **AVG 9 Internet Security** Wenn die Standardeinstellungen nicht Ihren Anforderungen entsprechen, können Sie einzelne Komponenten entfernen oder hinzufügen.

Sie können jedoch nur Komponenten auswählen, die in Ihrer AVG Edition enthalten sind. Nur diese Komponenten werden im Dialogfeld „Komponentenauswahl" zur Installation angeboten!

- ***Sprachauswahl***

  Innerhalb der Liste zu installierender Komponenten können Sie die Sprache(n) auswählen, in der AVG installiert werden soll. Aktivieren Sie die Option ***Weitere installierte Sprachen***, und wählen Sie anschließend die gewünschte Sprachen aus dem Menü.

- ***Plugins für eMail-Scanner***

  Klicken Sie auf den Eintrag ***eMail-Scanner***, um diesen zu öffnen, und entscheiden Sie, welches Plugin installiert werden soll, um die Sicherheit Ihrer eMails zu gewährleisten. Standardmäßig wird das ***Plugin für Microsoft Outlook*** installiert. Wenn Ihre gekaufte Lizenz ***Anti-Spam*** umfasst, wird diese Komponente automatisch mit installiert. Eine andere Option ist das ***Plugin für The Bat!*** Wenn Sie einen anderen eMail-Client verwenden (*MS Exchange,*

Qualcomm, Eudora,...),wählen Sie die Option ***Personal eMail-Scanner*** aus, um Ihre eMail-Kommunikation automatisch zu sichern, unabhängig davon, welches eMail-Programm ausgeführt wird.

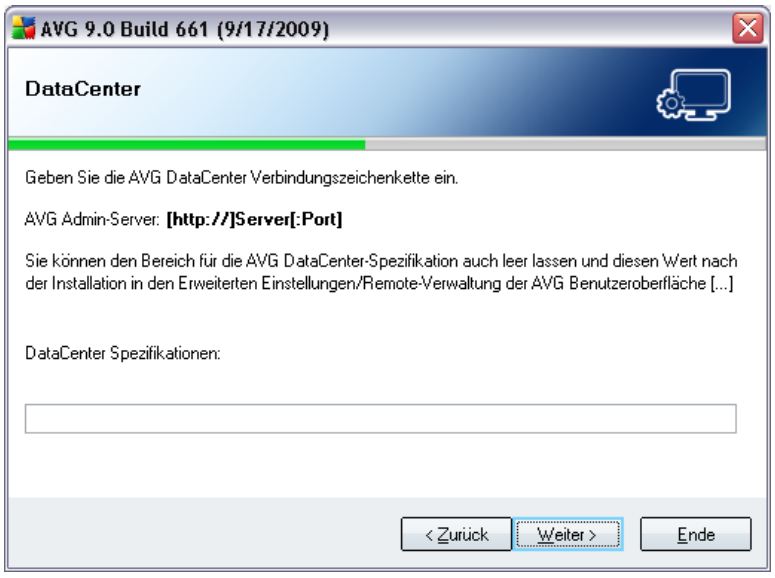
- ***Remote-Verwaltung***

  Wenn Sie vorhaben, Ihren Computer später mit der AVG Remote-Verwaltung zu verbinden, wählen Sie bitte auch den entsprechenden Eintrag zur Installation aus.

Klicken Sie zum Fortfahren auf die Schaltfläche ***Weiter*** .

5.8. AVG DataCenter

Wenn Sie im vorigen Dialog ***Benutzerdefinierte Installation – Komponentenauswahl*** den Eintrag ***Remote-Verwaltung*** zur Installation ausgewählt haben, müssen Sie die Parameter für das ***AVG DataCenter*** festlegen:



Geben Sie im Textfeld ***Spezifikation des AVG DataCenter*** bitte die Verbindungszeichenfolge für das ***AVG DataCenter*** ein – und zwar im Format *server:port*. Wenn diese Informationen momentan nicht verfügbar sind, lassen Sie das Feld leer, und nehmen Sie die Konfiguration später im Dialog ***Erweiterte Einstellungen/ Remote-Verwaltung*** vor.

Hinweis: *Genaue Informationen zur Remote-Verwaltung von AVG erhalten Sie im Benutzerhandbuch der AVG Netzwerk Edition, das Sie auf der Website von AVG (*

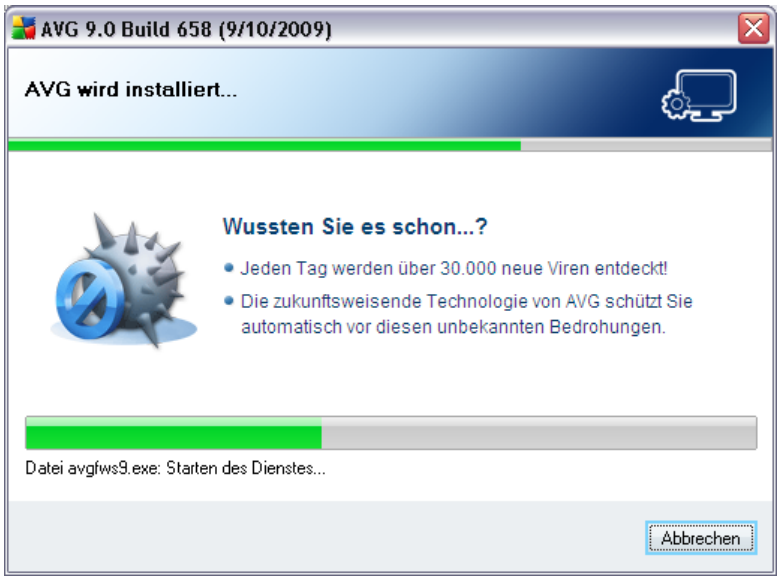
http://www.avg.com/) herunterladen können.

5.9. AVG Security Toolbar

Legen Sie im Dialog ***AVG Security Toolbar*** fest, ob Sie die ***AVG Security Toolbar*** installieren möchten (*Überprüfung von Suchergebnissen der unterstützten Suchmaschinen im Internet*). Wenn Sie die Standardeinstellungen nicht ändern, wird die Komponente automatisch in Ihrem Internetbrowser installiert, so dass Sie beim Surfen im Internet umfassend geschützt sind.

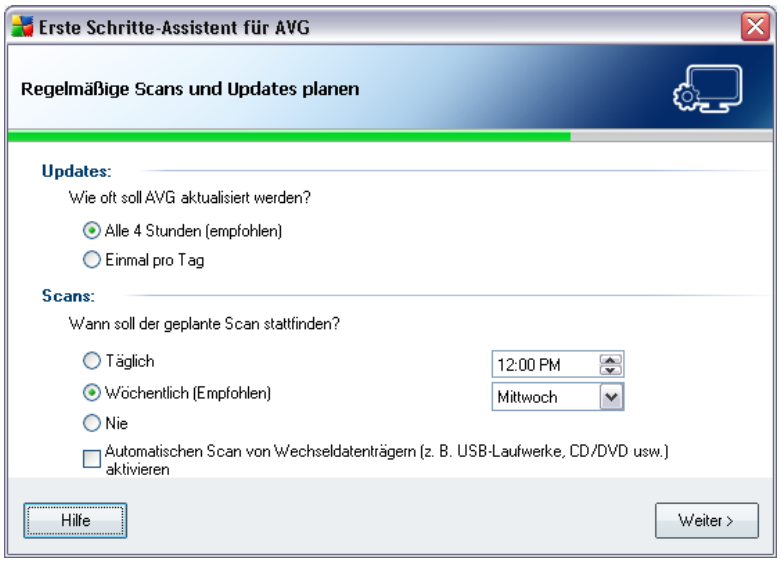
5.10. AVG installieren

Im Dialog ***AVG installieren***wird der Fortschritt des Installationsvorgangs angezeigt, eine Aktion ist hier nicht erforderlich:



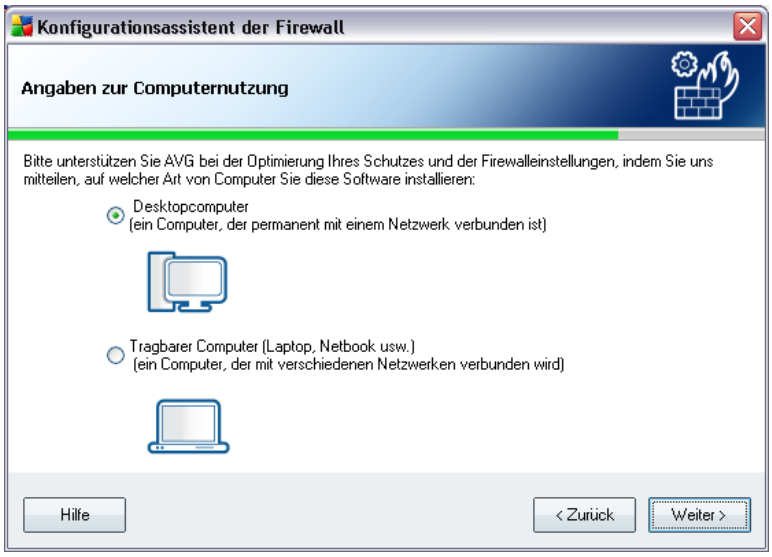
Nach Abschluss des Installationsvorgangs werden Sie automatisch zum nächsten Dialog weitergeleitet.

5.11. Regelmäßige Scans und Updates planen



Legen Sie im Dialog ***Regelmäßige Scans und Updates planen*** das Intervall für die Überprüfung auf neu verfügbare Aktualisierungsdateien fest, und geben Sie an, wann der geplante Scan ausgeführt werden soll. Es wird empfohlen, die Standardwerte beizubehalten. Klicken Sie zum Fortfahren auf ***Weiter***.

5.12. Angaben zur Computernutzung



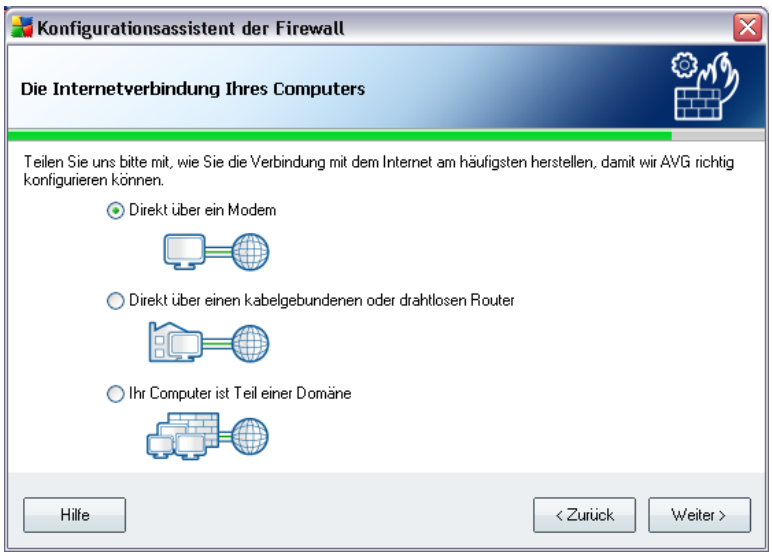
In diesem Dialog fragt Sie der ***Konfigurationsassistent der Firewall***, welche Art von Computer Sie nutzen. Ein Notebook beispielsweise, das von vielen verschiedenen Orten aus mit dem Internet verbunden wird (*Flughäfen, Hotelzimmer usw.*) benötigt strengere Sicherheitsregeln als ein Computer in einer Domäne (*Firmennetzwerk usw.*). Abhängig vom ausgewählten Computertypen werden die Standardregeln der ***Firewall*** mit unterschiedlichen Sicherheitsstufen festgelegt.

Es stehen zwei alternative Optionen zur Auswahl:

- ***Als Desktop-Computer***
- ***Ein tragbarer Computer***

Bestätigen Sie Ihre Auswahl durch Klicken auf die Schaltfläche ***Weiter***, und fahren Sie mit dem nächsten Dialog fort.

5.13. Das Netzwerkdesign Ihres Computers



In diesem Dialog werden Sie vom ***Konfigurationsassistenten der Firewall*** gefragt, wie Ihr Computer mit dem Internet verbunden ist. Abhängig vom ausgewählten Verbindungstyp werden die Standardregeln der ***Firewall*** mit einer geeigneten Sicherheitsstufe definiert.

Sie können zwischen drei alternativen Optionen wählen:

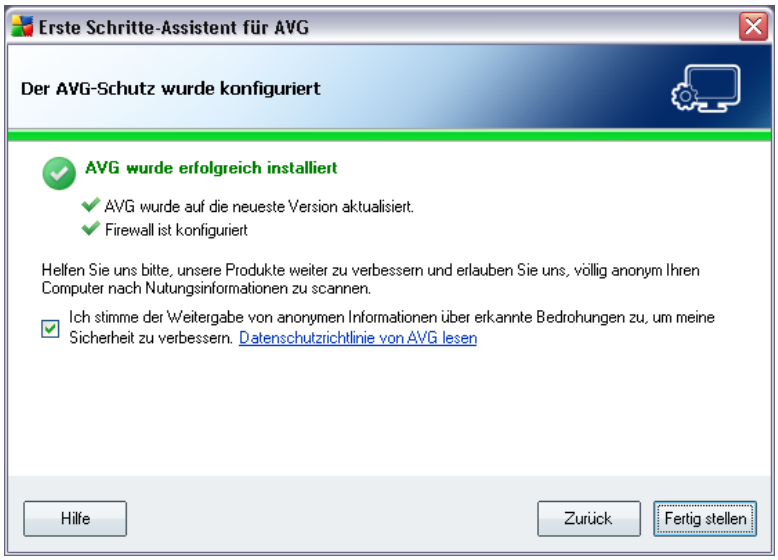
- ***Direkt mit dem Internet***

- ***Kleines Heimnetzwerk***
- ***Ihr Computer befindet sich in der Domain***

Wählen Sie den Verbindungstyp, der der Internetverbindung Ihres Computers am ehesten entspricht.

Bestätigen Sie Ihre Auswahl durch Klicken auf die Schaltfläche ***Weiter***, und fahren Sie mit dem nächsten Dialog fort.

5.14. Die Konfiguration des Schutzes von AVG ist abgeschlossen



Die Konfiguration von **AVG 9 Internet Security** wurde abgeschlossen.

In diesem Dialog können Sie festlegen, ob Sie die Option für das Versenden anonymer Berichte über Exploits und gefährliche Websites an das Virenlabor von AVG aktivieren möchten. Wenn ja, markieren Sie bitte die Option ***Ich stimme der Weitergabe von ANONYMEN Informationen über erkannte Bedrohungen zu, um meine Sicherheit zu verbessern***.

Klicken Sie am Ende auf die Schaltfläche ***Fertig stellen***. Möglicherweise müssen Sie Ihren Computer neu starten, um mit AVG arbeiten zu können.

6. Nach der Installation

6.1. Produktregistrierung

Nach Abschluss der **AVG 9 Internet Security** Installation registrieren Sie Ihr Produkt bitte, indem Sie auf der Website von AVG (http://www.avg.com/) die Seite ***Registrierung*** aufrufen (*folgen Sie den Anweisungen auf dieser Seite*). Nach der Registrierung erhalten Sie vollen Zugriff auf Ihr AVG-Benutzerkonto, den AVG Update-Newsletter und andere exklusive Dienste für registrierte Benutzer.

6.2. Zugriff auf die Benutzeroberfläche

Die***Benutzeroberfläche von AVG*** kann auf mehrere Arten geöffnet werden:

- durch Doppelklicken auf das AVG-Symbol in der Taskleiste
- durch Doppelklicken auf das AVG-Symbol auf dem Desktop
- über das Menü ***Start/Alle Programme/AVG 9.0/Benutzeroberfläche von AVG***

6.3. Gesamten Computer scannen

Es besteht das potentielle Risiko, dass vor der Installation von **AVG 9 Internet Security** bereits ein Virus auf Ihren Computer übertragen wurde. Aus diesem Grund sollten Sie die Option ***Gesamten Computer scannen*** ausführen, um sicherzustellen, dass Ihr Computer nicht infiziert ist.

Eine Anleitung, wie Sie die Option ***Gesamten Computer scannen*** ausführen, finden Sie im Kapitel ***AVG-Scans***.

6.4. Eicar-Test

Zur Überprüfung, ob **AVG 9 Internet Security** korrekt installiert wurde, können Sie den EICAR-Test durchführen.

Der EICAR-Test ist eine standardmäßige und absolut sichere Methode, um die Funktion von Virenschutzsystemen zu überprüfen. Es kann ohne Sicherheitsrisiko weitergegeben werden, da es sich dabei nicht um ein wirkliches Virus handelt und es auch keine Fragmente viralen Codes enthält. Die meisten Produkte reagieren jedoch, als würde es sich tatsächlich um ein Virus handeln (*es wird in der Regel mit einem*

offensichtlichen Namen wie „EICAR-AV-Test" gemeldet). Sie können das EICAR-Virus von der EICAR-Website unter www.eicar.com herunterladen und finden dort auch alle wichtigen Informationen zum EICAR-Test.

Laden Sie die Datei ***eicar.com*** herunter und speichern Sie sie auf Ihrer lokalen Festplatte. Unmittelbar nach der Bestätigung zum Herunterladen der Testdatei reagiert ***Web Shield*** mit einer Warnung. Diese Meldung von ***Web Shield*** zeigt, dass AVG korrekt auf dem Computer installiert ist.

Wenn AVG die EICAR-Testdatei nicht als Virus erkennt, sollten Sie die Programmkonfiguration überprüfen!

6.5. Standardkonfiguration von AVG

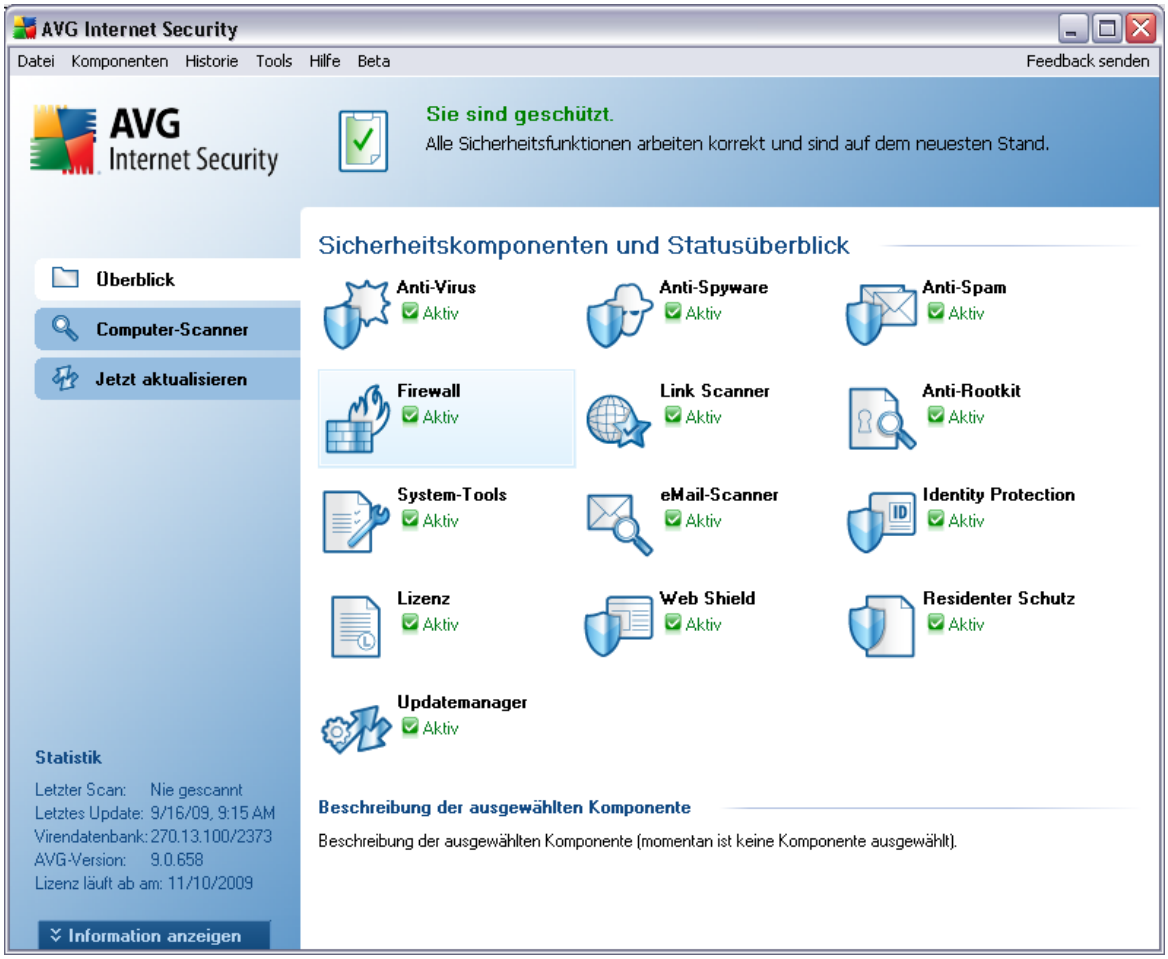
Die Standardkonfiguration (*Konfiguration der Anwendung unmittelbar nach der Installation*) von **AVG 9 Internet Security** ist vom Händler so eingestellt, dass alle Komponenten und Funktionen eine optimale Leistung erzielen.

Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben! Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

Geringfügige Änderungen an den Einstellungen der Komponenten von AVG können direkt über die Benutzeroberfläche der jeweiligen Komponente festgelegt werden. Wenn Sie die Konfiguration von AVG ändern und besser an Ihre Bedürfnisse anpassen möchten, wechseln Sie zu ***Erweiterte AVG-Einstellungen***, und wählen Sie im Systemmenü ***Tools/Erweiterte Einstellungen*** aus. Daraufhin wird der Dialog ***Erweiterte AVG-Einstellungen*** angezeigt, in dem Sie die Konfiguration von AVG ändern können.

7. Benutzeroberfläche von AVG

AVG 9 Internet Security (Hauptfenster):



Das Hauptfenster ist in mehrere Bereiche gegliedert:

- ***Systemmenü*** *(Leiste an der Oberseite des Fensters)* dient zur Standardnavigation für den Zugriff auf alle Komponenten, Dienste und Funktionen von AVG - Details >>

- ***Informationen zum Sicherheitsstatus*** *(oberer Bereich des Fensters)* enthält Informationen zum aktuellen Status Ihres AVG-Programms - Details >>

- ***Quick Links*** *(linker Bereich des Fensters)* ermöglichen das schnelle Aufrufen der wichtigsten und am häufigsten verwendeten AVG-Aufgaben - Details >>

- ***Komponentenübersicht*** *(zentraler Bereich des Fensters)* zeigt eine Übersicht über alle installierten Komponenten von AVG - Details >>

- ***Statistik*** *(linker unterer Bereich des Fensters)* enthält alle statistischen Daten zur Programmnutzung - Details >>

- ***Infobereich-Symbol*** *(untere rechte Ecke des Bildschirms, im Infobereich)* zeigt den aktuellen Status von AVG - Details >>

7.1. Systemmenü

Das ***Systemmenü*** ist die Standardnavigation, die in allen Anwendungen von Windows verwendet wird. Es befindet sich als horizontales Menü ganz oben im **AVG 9 Internet Security**Hauptfenster. Mit Hilfe des Systemmenüs können Sie auf bestimmte Komponenten, Funktionen und Dienste von AVG zugreifen.

Das Systemmenü ist in fünf Hauptbereiche eingeteilt:

7.1.1. Datei

- ***Beenden*** – schließt die Benutzeroberfläche von **AVG 9 Internet Security** . Die AVG-Anwendung wird jedoch weiterhin im Hintergrund ausgeführt, damit Ihr Computer geschützt ist!

7.1.2. Komponenten

Der Menüpunkt ***Komponenten*** des Systemmenüs enthält Links zu allen installierten Komponenten von AVG, wobei jeweils der Standarddialog in der Benutzeroberfläche geöffnet wird:

- ***Systemüberblick*** – öffnet den Standarddialog der Benutzeroberfläche mit einer Übersicht über alle installierten Komponenten und deren Status

- ***Anti-Virus*** – öffnet die Standardseite der Komponente ***Anti-Virus***

- ***Anti-Rootkit*** – öffnet die Standardseite der Komponente ***Anti-Rootkit***

- ***Anti-Spyware*** – öffnet die Standardseite der Komponente ***Anti-Spyware***

- ***Firewall*** – öffnet die Standardseite der Komponente ***Firewall***

- ***Link Scanner*** – öffnet die Standardseite der Komponente ***Link Scanner***
- ***System Tools*** – öffnet die Standardseite der ***System Tools***
- ***Anti-Spam*** – öffnet die Standardseite der Komponente ***Anti-Spam***
- ***eMail-Scanner*** – öffnet die Standardseite der Komponente ***eMail-Scanner***
- ***Identitätsschutz*** – Öffnet die Standardseite der Komponente ***Identitätsschutz***
- ***Lizenz*** – öffnet die Standardseite der Komponente ***Lizenz***
- ***Web Shield*** – öffnet die Standardseite der Komponente ***Web Shield***
- ***Residenter Schutz*** – öffnet die Standardseite der Komponente ***Residenter Schutz***
- ***Updatemanager*** – öffnet die Standardseite der Komponente ***Updatemanager***

7.1.3. Verlauf

- ***Scan-Ergebnisse*** - Wechsel zur Testoberfläche von AVG, und zwar zum Dialog ***Übersicht über Scan-Ergebnisse***
- ***Residenter Schutz*** - Anzeigen einen Dialogs mit einer Übersicht über Bedrohungen, erkannt durch den ***Residenten Schutz***
- ***eMail-Scanner*** - Anzeige eines Dialogs mit einer Übersicht über eMail-Anhänge, die von der Komponente ***eMail-Scanner*** als gefährlich erkannt wurden
- ***Funde des Web Shield*** – Öffnet einen Dialog mit einer Übersicht über Bedrohungen, die von ***Web Shield erkannt wurden***
- ***Virenquarantäne*** - Anzeige der Oberfläche der Virenquarantäne (***Virenquarantäne***), in die AVG alle erkannten Infektionen verschiebt, die nicht automatisch geheilt werden können. Innerhalb dieser Quarantäne werden die infizierten Dateien isoliert, so das die Sicherheit Ihres Computers gewährleistet ist. Gleichzeitig werden die infizierten Dateien für eine mögliche Reparatur gespeichert.
- ***Ereignisprotokoll*** - Anzeige der Ereignisprotokoll Oberfläche mit einer Übersicht über alle protokollierten Aktionen **AVG 9 Internet Security** .

- ***Firewall*** – Öffnet die Benutzeroberfläche der Firewall-Einstellungen auf dem Reiter ***Protokolle*** mit einer detaillierten Übersicht über alle Firewall-Aktionen

7.1.4. Tools

- ***Computer scannen*** – wechselt zur Scan-Oberfläche von AVG und startet einen Scan des gesamten Computers

- ***Ausgewählten Ordner scannen*** – wechselt zur Scan-Oberfläche von AVG , wo Sie in der Baumstruktur Ihres Computers entscheiden können, welche Dateien und Ordner gescannt werden sollen

- ***Datei scannen*** – Dabei können Sie in der Baumstruktur Ihres Laufwerks eine einzelne Datei auswählen und einen On-Demand-Scan durchführen

- ***Aktualisieren*** – startet automatisch den Aktualisierungsvorgang von **AVG 9 Internet Security**

- ***Aus Verzeichnis aktualisieren*** – führt den Aktualisierungsvorgang von den Aktualisierungsdateien aus, die sich in einem dafür vorgesehenen Ordner auf Ihrem lokalen Laufwerk befinden. Die Verwendung dieser Option empfehlen wir Ihnen jedoch nur in Notfällen, z. B. wenn keine Verbindung zum Internet vorhanden ist (*beispielsweise wenn Ihr Computer infiziert ist und die Verbindung zum Internet verloren hat oder Ihr Computer mit einem Netzwerk verbunden ist, das keinen Zugang zum Internet hat*). Wählen Sie im neu geöffneten Fenster den Ordner, in dem Sie die Aktualisierungsdatei zuvor gespeichert haben, und starten Sie den Aktualisierungsvorgang.

- ***Erweiterte Einstellungen*** – Öffnet den Dialog ***Erweiterte AVG-Einstellungen*** , in dem Sie die Konfiguration von **AVG 9 Internet Security** bearbeiten können. Im Allgemeinen empfehlen wir Ihnen, die Standardeinstellungen der Software beizubehalten, die vom Software-Hersteller festgelegt wurden.

- ***Firewall-Einstellungen*** – öffnet einen eigenen Dialog für die erweiterte Konfiguration der ***Firewall***

7.1.5. Hilfe

- ***Inhalt*** – öffnet die Hilfedateien von AVG

- ***Onlinehilfe*** – Öffnet die Website von AVG (http://www.avg.com/) auf der Hauptseite des Kundendienstes

- ***Ihr AVG-Web*** – Öffnet die Startseite der Website von AVG (http://www.avg.

com/)

- ***Virenenzyklopädie*** – öffnet die Online-***Virenenzyklopädie*** , aus der Sie genaue Informationen über das ermittelte Virus abrufen können

- ***Erneut aktivieren*** – Öffnet den Dialog ***AVG aktivieren*** mit den Daten, die Sie im Dialog ***AVG personalisieren*** des Installationsvorgangs eingegeben haben. In diesem Dialog können Sie Ihre Lizenznummer eingeben, um entweder die Vertriebsnummer (*die Nummer, mit der Sie AVG installiert haben*) oder die alte Lizenznummer (*zum Beispiel beim Upgrade auf ein neues AVG-Produkt*) zu ersetzen.

- ***Jetzt registrieren*** – Stellt eine Verbindung zur Registrierungsseite der Website von AVG (http://www.avg.com/) her. Bitte geben Sie Ihre Registrierungsdaten ein – Nur Kunden, die ihr AVG-Produkt registrieren, erhalten auch kostenlosen technischen Support.

- ***Info zu AVG*** – Öffnet den Dialog ***Information*** mit fünf Reitern, die Informationen über den Namen des Programms, das Programm selbst und die Version der Virendatenbank sowie Systeminformationen, die Lizenzvereinbarung und Kontaktdaten von ***AVG Technologies CZ***enthalten.

7.2. Informationen zum Sicherheitsstatus

Der Bereich ***Informationen zum Sicherheitsstatus*** befindet sich im oberen Teil des Hauptfensters von AVG. In diesem Bereich finden Sie stets Informationen zum aktuellen Sicherheitsstatus Ihrer **AVG 9 Internet Security**. Bitte verschaffen Sie sich eine Übersicht über Symbole, die in diesem Bereich möglicherweise angezeigt werden und über ihre Bedeutung:


Das grüne Symbol zeigt an, dass Ihr AVG vollständig funktioniert. Ihr Computer ist vollständig geschützt und befindet sich auf dem aktuellsten Stand. Alle installierten Komponenten werden ordnungsgemäß ausgeführt.


Das orangefarbene Symbol warnt Sie, wenn eine oder mehrere Komponenten falsch konfiguriert sind. Überprüfen Sie deren Eigenschaften/ Einstellungen. Es besteht kein grundlegendes Problem in AVG, und Sie haben sich wahrscheinlich entschieden, einige Komponenten aus bestimmten Gründen zu deaktivieren. Sie sind immer noch durch AVG geschützt. Sie sollten jedoch die Einstellungen der problematischen Komponente überprüfen! Den Namen der

Komponente finden Sie im Bereich ***Informationen zum Sicherheitsstatus*** .

Dieses Symbol wird auch dann angezeigt, wenn Sie sich aus einem bestimmten Grund dazu entschieden haben, den Fehlerstatus einer Komponente zu ignorieren (*die Option „Komponentenstatus ignorieren" ist im Kontextmenü verfügbar, das sich durch einen Klick mit der rechten Maustaste auf das Komponentensymbol in der Komponentenübersicht des Hauptfensters von AVG öffnen lässt*). Es kann vorkommen, dass Sie diese Option in bestimmten Situationen verwenden müssen, aber es wird dringend empfohlen, die Option „***Komponentenstatus ignorieren***" so bald wie möglich zu deaktivieren.

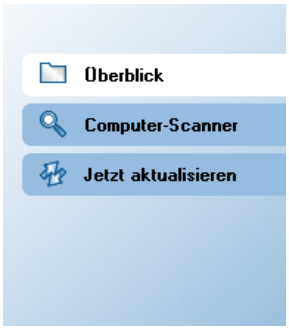
 Das rote Symbol zeigt an, dass sich AVG in einem kritischen Status befindet! Eine oder mehrere Komponenten werden nicht korrekt ausgeführt, und AVG kann Ihren Computer nicht schützen. Bitte beheben Sie unverzüglich das berichtete Problem. Wenn Sie den Fehler nicht selbst beheben können, wenden Sie sich an den Technischen Support von AVG.

Es ist äußerst empfehlenswert, auf die ***Informationen zum Sicherheitsstatus*** zu achten und ein angezeigtes Problem unverzüglich zu lösen. Anderenfalls ist Ihr Computer gefährdet!

Hinweis: *Statusinformationen von AVG erhalten Sie auch jederzeit über das Symbol im Infobereich.*

7.3. Quick Links

Mit Hilfe der Quick Links *(im linken Bereich der Benutzeroberfläche von AVG)* können Sie sofort auf die wichtigsten und am häufigsten verwendeten Features von AVG zugreifen:



- ***Überblick*** – Mit diesem Link können Sie von jeder aktuell geöffneten

Oberfläche von AVG zur Standardoberfläche wechseln, auf der Sie eine Übersicht über alle installierten Komponenten erhalten. Siehe Kapitel ***Komponentenübersicht*** >>

- ***Computer-Scanner*** – Mit diesem Link öffnen Sie die Scan-Oberfläche von AVG, auf der Sie Scans direkt ausführen, Scans planen oder ihre Parameter bearbeiten können. Siehe Kapitel ***AVG-Tests*** >>

- ***Jetzt aktualisieren*** – Mit diesem Link wird die Aktualisierungsoberfläche geöffnet und der Aktualisierungsprozess von AVG unmittelbar gestartet. Siehe Kapitel ***AVG Updates*** >>

Auf diese Links können Sie jederzeit über die Benutzeroberfläche zugreifen. Wenn Sie einen Prozess über einen Quick Link ausführen, wechselt die GUI zu einem neuen Dialog, die Quick Links bleiben aber weiter verfügbar. Außerdem wird der ausgeführte Prozess grafisch angezeigt (*Abbildung 2)*.

7.4. Komponentenübersicht

Der Bereich ***Sicherheitskomponenten und Statusüberblick*** befindet sich in der Mitte der Benutzeroberfläche von AVG. Er ist in zwei Teile gegliedert:

- Übersicht über alle installierten Komponenten in Symbolform mit Angabe des jeweiligen Status (Aktiv oder Nicht aktiv)

- Beschreibung einer ausgewählten Komponente

In **AVG 9 Internet Security** enthält der Bereich ***Sicherheitskomponenten und Statusüberblick*** Informationen zu folgenden Komponenten:

- ***Anti-Virus*** stellt sicher, dass Ihr Computer vor Viren geschützt wird – Details >>

- ***Anti-Spyware*** scannt Ihre Anwendungen im Hintergrund, während Sie damit arbeiten – Details >>

- ***Anti-Spam*** überprüft alle eingehenden eMail-Nachrichten und markiert unerwünschte Nachrichten als SPAM – Details >>

- ***Firewall*** steuert, wie Ihr Computer Daten mit anderen Computern im Internet oder im lokalen Netzwerk austauscht – Details >>

- ***Link Scanner*** überprüft die Suchergebnisse, die in Ihrem Internetbrowser angezeigt werden – Details >>

- ***Anti-Rootkit*** erkennt Programme und Technologien, die darauf abzielen, Malware zu verbergen – Details >>
- ***System-Tools*** bietet einen detaillierten Überblick über die Umgebung von AVG – Details >>
- ***eMail-Scanner*** überprüft alle eingehenden und ausgehenden eMails auf Viren – Details >>
- ***Identitätsschutz*** – Eine Komponente für Anti-Malware, mit der Ihre persönlichen digitalen Daten vor Identitätsdiebstahl geschützt werden – Details >>
- ***Lizenz*** zeigt den vollständigen Wortlaut der AVG-Lizenzvereinbarung an – Details >>
- ***Web Shield*** scannt alle Daten, die mit einem Webbrowser heruntergeladen werden – Details >>
- ***Residenter Schutz*** wird im Hintergrund ausgeführt und scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden – Details >>
- ***Updatemanager*** kontrolliert alle Aktualisierungen von AVG – Details >>

Klicken Sie auf eines der Komponentensymbole, um die Komponente in der Übersicht zu markieren. Im unteren Teil der Benutzeroberfläche wird eine kurze Funktionsbeschreibung der ausgewählten Komponente angezeigt. Doppelklicken Sie auf ein Symbol, um die Benutzeroberfläche der jeweiligen Komponente mit einer Auflistung von statistischen Basisdaten anzuzeigen.

Klicken Sie mit der rechten Maustaste auf das Komponentensymbol, um das Kontextmenü einzublenden: Darüber können Sie nicht nur die grafische Benutzeroberfläche der Komponente öffnen, sondern auch die Option ***Komponentenstatus ignorieren*** auswählen. Wählen Sie diese Option, wenn Ihnen bekannt ist, dass die Komponente einen Fehlerstatus aufweist, AVG aber aus einem bestimmten Grund aktiviert bleiben soll und Sie nicht durch die graue Farbe des Symbols im Infobereich gewarnt werden möchten.

7.5. Statistik

Der Bereich***Statistik*** befindet sich im linken, unteren Bereich der Benutzeroberfläche von AVG. Dort finden Sie eine Liste von Informationen hinsichtlich der Programmvorgänge:

- ***Letzter Scan*** – Hier ist das Datum des letzten durchgeführten Scans angegeben
- ***Letztes Update*** – Hier ist das Datum der letzten Aktualisierung angegeben
- ***Virendatenbank*** – Hier wird die aktuell installierte Version der Virendatenbank angegeben
- ***AVG-Version*** – Hier erhalten Sie Informationen zur installierten AVG-Version *(die Versionsnummer wird im Format 8.0.xx angegeben, wobei 8.0 die Version der Produktlinie ist, und xx für die Build-Nummer steht)*
- ***Lizenz läuft ab am:*** – Hier wird das Ablaufdatum Ihrer Lizenz von AVG angegeben

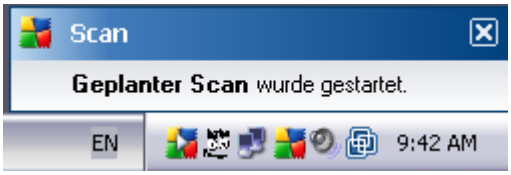
7.6. Infobereich-Symbol

Das Infobereich-Symbol (*auf Ihrer Taskleiste von Windows*) zeigt den aktuellen Status Ihrer **AVG 9 Internet Security** an. Es wird immer in Ihrem Infobereich angezeigt, unabhängig davon, ob Ihr Hauptfenster von AVG geöffnet oder geschlossen ist.

Durch die Vollfarbe des ***Infobereichsymbols*** wird angezeigt, dass alle Komponenten von AVG aktiv und voll funktionsfähig sind. Das AVG-Symbol im Infobereich wird auch dann in Vollfarbe angezeigt, wenn AVG einen Fehlerstatus aufweist und Sie sich absichtlich dafür entschieden haben, den ***Komponentenstatus zu ignorieren***.

Ein graues Symbol, das farbig wird, mit einem Ausrufezeichen zeigt ein Problem an (*inaktive Komponente, Fehlerstatus usw.*). Doppelklicken Sie auf das ***Infobereich-Symbol***, um das Hauptfenster zu öffnen und eine Komponente zu bearbeiten.

Über das Symbol im Infobereich werden Sie außerdem über laufende Aktivitäten von AVG und eventuelle Statusänderungen des Programms informiert (*z. B. automatischer Start eines geplanten Scans oder Updates, Firewall-Profilwechsel, Statusänderung einer Komponente, Auftreten eines Fehlerstatus usw.*). Dabei wird über das AVG-Symbol im Infobereich ein Popup-Fenster geöffnet:



Das ***Infobereich-Symbol*** kann auch als Quick Link verwendet werden, um auf das Hauptfenster von AVG zuzugreifen. Doppelklicken Sie dazu auf das Symbol. Wenn Sie mit der rechten Maustaste auf das ***Infobereich-Symbol*** klicken, wird ein kurzes Kontextmenü mit den folgenden Optionen geöffnet:

- ***Benutzeroberfläche von AVG öffnen*** – Klicken Sie hierauf, um die Benutzeroberfläche von AVG zu öffnen
- ***Jetzt aktualisieren*** – startet den Aktualisierungsvorgang sofort

8. Komponenten von AVG

8.1. Anti-Virus

8.1.1. Anti-Virus Grundlagen

Die Scan-Engine der Antivirensoftware überprüft alle Dateien und Dateiaktivitäten (Öffnen/Schließen von Dateien usw.) auf bekannte Viren. Alle erkannten Viren werden blockiert, so dass sie keine Aktionen ausführen können, und anschließend bereinigt oder in die Quarantäne verschoben. Die meisten Antivirenprodukte verwenden auch einen heuristischen Scan, mit dem Dateien auf typische Virenmerkmale (sogenannte Virensignaturen) überprüft werden. Auf diese Weise kann der Antivirenscanner neue, unbekannte Viren erkennen, wenn diese typische Merkmale eines vorhandenen Virus aufweisen.

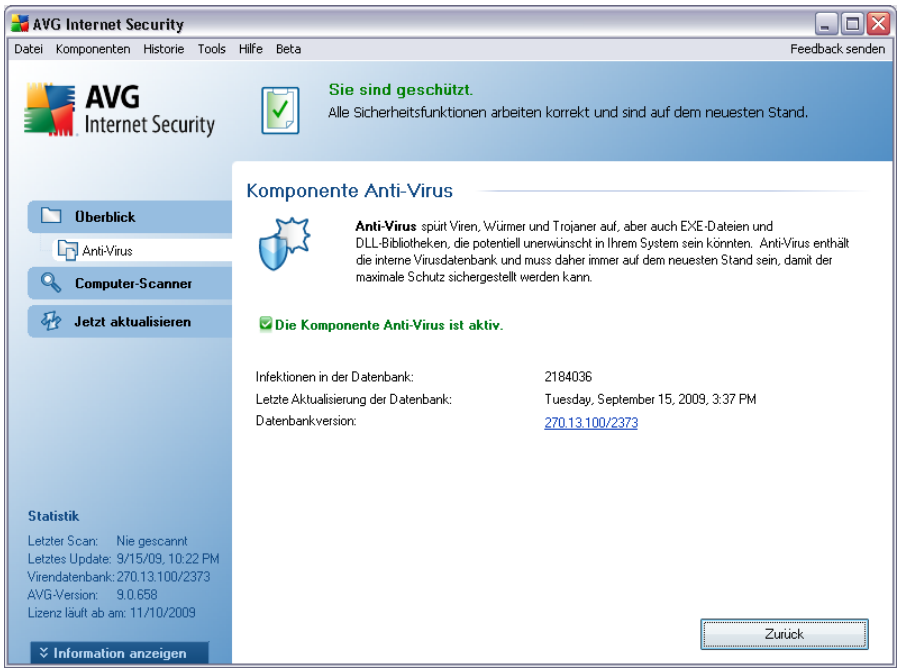
Die wichtigste Funktion des Virenschutzes ist, sicherzustellen, dass keine bekannten Viren auf dem Computer ausgeführt werden können!

Während eine einzige Technologie häufig nicht in der Lage ist, alle Viren zu erkennen oder zu identifizieren, gewährleistet ***Anti-Virus*** durch Kombination mehrerer Technologien einen umfassenden Schutz des Computers:

- Scannen – Die Suche nach Zeichenfolgen, die charakteristisch für ein bestimmtes Virus sind
- Heuristische Analyse – Dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung
- Generische Erkennung – Erkennung von Anweisungen, die typisch für ein bestimmtes Virus oder eine Gruppe von Viren sind

AVG kann zudem im System unerwünschte ausführbare Anwendungen oder DLL-Bibliotheken analysieren und erkennen. Diese Bedrohungen bezeichnen wir als potentiell unerwünschte Programme (verschiedene Arten von Spyware, Adware usw.). Außerdem durchsucht AVG Ihre System-Registry nach verdächtigen Einträgen, temporären Internetdateien und Tracking Cookies und ermöglicht Ihnen, alle potentiell schädlichen Elemente wie jegliche andere Infektion zu behandeln.

8.1.2. Benutzeroberfläche des Anti-Virus



Die Benutzeroberfläche von ***Anti-Virus*** enthält grundlegende Informationen zur Funktionalität der Komponente und zum aktuellen Status (*Die Komponente Anti-Virus ist aktiv*) sowie eine Übersicht über statistische Daten zu ***Anti-Virus***:

- ***Infektionen in der Datenbank*** – Anzahl der in der aktuellen Version der Virendatenbank definierten Viren
- ***Letzte Aktualisierung der Datenbank*** – Datum und Uhrzeit der letzten Aktualisierung der Virendatenbank
- ***Datenbankversion*** – Versionsnummer der aktuellsten Virendatenbank; wird bei jeder Aktualisierung der Virendatenbank erhöht

Der Dialog enthält nur eine Schaltfläche (***Zurück***), mit der Sie zum Hauptfenster der Benutzeroberfläche von AVG (Sicherheitskomponenten und Statusüberblick) zurückkehren können.

Hinweis: *Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der*

Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

8.2. Anti-Spyware

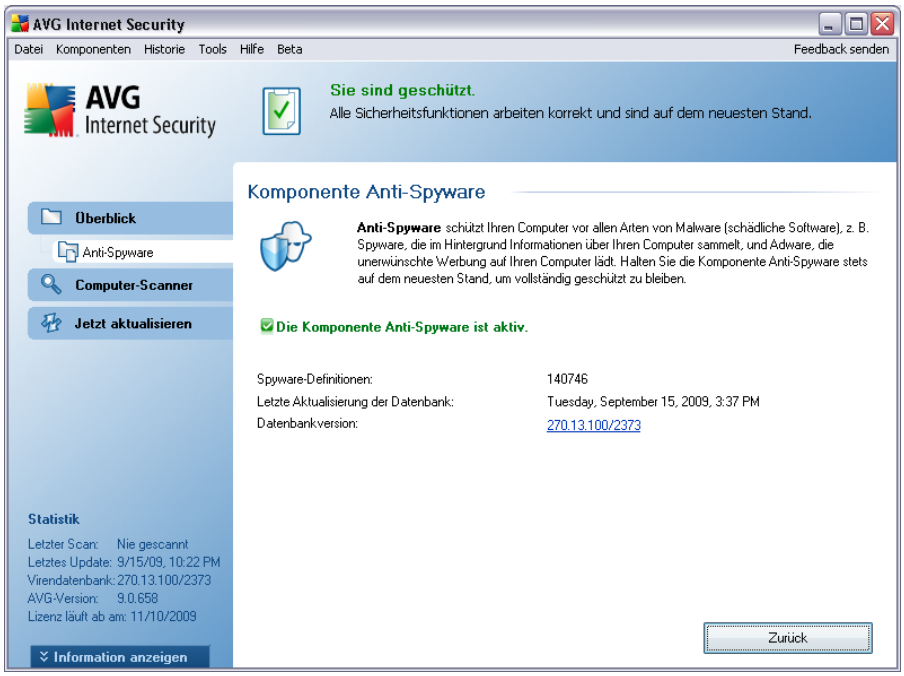
8.2.1. Anti-Spyware Grundlagen

Spyware wird normalerweise als eine Art Malware definiert, d. h. Software, die ohne Wissen und Zustimmung des Benutzers Informationen auf dem Computer sammelt. Einige Spyware-Programme können bewusst installiert werden und enthalten häufig Werbung, Popup-Fenster oder ähnlich unerfreuliche Software.

Derzeit geht die größte Infektionsgefahr von Websites mit potentiell gefährlichen Inhalten aus. Jedoch ist auch eine Übertragung per eMail oder durch Würmer und Viren eine durchaus gängige Infektionsmöglichkeit. Der wichtigste Schutz ist ein Scanner, der ständig im Hintergrund ausgeführt wird, wie z. B. die Komponente ***Anti-Spyware***, die wie ein residenter Schutz funktioniert und Ihre Anwendungen während der Arbeit im Hintergrund überprüft.

Es ist allerdings möglich, dass Malware bereits vor der Installation von AVG auf den Computer übertragen wurde oder dass Sie **AVG 9 Internet Security** nicht mit den neuesten Datenbank- und Programmaktualisierungen ausgestattet haben. Daher können Sie mit AVG Ihren Computer mithilfe der Scan-Funktion vollständig auf Malware bzw. Spyware überprüfen. Außerdem erkennt die Komponente ruhende und nicht aktive Malware, d. h. Malware, die heruntergeladen, aber noch nicht aktiviert wurde.

8.2.2. Benutzeroberfläche der Anti-Spyware



Die Benutzeroberfläche von ***Anti-Spyware*** enthält eine Übersicht über die Funktionsweise der Komponente, Informationen zum aktuellen Status (*Die Komponente Anti-Spyware ist aktiv*) sowie statistische Daten zu ***Anti-Spyware***:

- ***Spyware-Definitionen*** – Anzahl der in der neuesten Spyware-Datenbankversion definierten Spyware-Muster
- ***Letzte Aktualisierung der Datenbank*** – Datum und Uhrzeit der letzten Aktualisierung der Spyware-Datenbank
- ***Datenbankversion*** – Versionsnummer der aktuellsten Spyware-Datenbank; wird bei jeder Aktualisierung der Virendatenbank erhöht

Der Dialog enthält nur eine Schaltfläche (***Zurück***), mit der Sie zum Hauptfenster der Benutzeroberfläche von AVG (Sicherheitskomponenten und Statusüberblick) zurückkehren können.

Hinweis: Alle *Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der*

Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

8.3. Anti-Spam

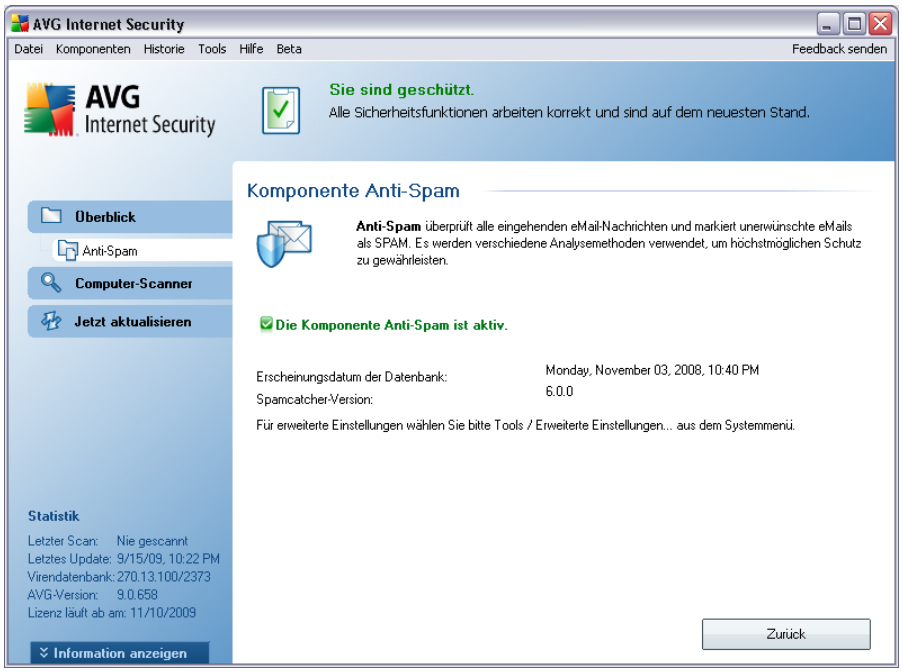
Unter Spam versteht man unerwünschte eMails, die meist für ein Produkt oder eine Dienstleistung werben. Sie werden mittels Massenversand an eine riesige Anzahl von eMail-Adressen verschickt und füllen so die Mailboxen der Empfänger. Spam bezieht sich nicht auf legitime Werbemails, für die der Verbraucher sein Einverständnis gegeben hat. Spam ist nicht nur störend, sondern auch oft eine Quelle für Betrugsversuche, Viren und beleidigende Inhalte.

8.3.1. Grundlagen zu Anti-Spam

AVG Anti-Spam überprüft alle eingehenden eMails und markiert unerwünschte Nachrichten als Spam. ***AVG Anti-Spam*** kann den Betreff einer eMail (*die als Spam eingestuft worden ist*) durch das Hinzufügen einer speziellen Zeichenfolge ändern. So können Sie Ihre eMails in Ihrem eMail-Client bequem filtern.

AVG Anti-Spam verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit optimalen Schutz vor unerwünschten eMail-Nachrichten. ***AVG Anti-Spam*** nutzt zur Erkennung von Spam eine Datenbank, die in regelmäßigen Abständen aktualisiert wird. Sie können auch RBL-Server verwenden (*öffentliche Datenbanken, in denen „bekannte Spam-Absender" erfasst sind*) und eMail-Adressen manuell zu Ihrer Whitelist (*eMails von diesen Absendern nie als Spam kennzeichnen*) oder zu Ihrer Blacklist (*immer als Spam kennzeichnen*) hinzufügen.

8.3.2. Benutzeroberfläche des Anti-Spam



Der Dialog der Komponente ***Anti-Spam*** enthält eine kurze Beschreibung der Funktionsweise der Komponente, Informationen zum aktuellen Status (*die Komponente Anti-Spam ist aktiv*) sowie die folgenden statistischen Daten:

- ***Erscheinungsdatum der Datenbank*** – Datum und Uhrzeit der letzten Aktualisierung und Veröffentlichung der Spam-Datenbank
- ***Spamcatcher-Version*** – Versionsnummer der neuesten Anti-Spam-Engine

Auf dieser Oberfläche der Komponente steht nur eine Schaltfläche zur Verfügung (***Zurück***) – Klicken Sie auf diese Schaltfläche, um zur standardmäßigen Benutzeroberfläche von AVG zurückzukehren (*Komponentenübersicht*).

Hinweis: *Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option* ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

8.4. Anti-Rootkit

Ein Rootkit ist ein Programm, das ohne Genehmigung der Systembesitzer oder berechtigten Benutzer die Kontrolle über ein Computersystem übernimmt. Ein Zugriff auf die Hardware ist meist nicht erforderlich, da ein Rootkit darauf abzielt, die Kontrolle über das Betriebssystem, das auf der Hardware ausgeführt wird, zu übernehmen. Rootkits verbergen ihre Existenz auf dem System üblicherweise, indem sie die standardmäßigen Sicherheitsmechanismen des Betriebssystems außer Kraft setzen oder umgehen. Oft handelt es sich bei diesen Programmen gleichzeitig um Trojaner, die bei Benutzern den Eindruck erwecken, sie könnten ohne Risiko auf ihren Systemen ausgeführt werden. Dies wird mit Techniken wie dem Verbergen von ausgeführten Prozessen vor Überwachungsprogrammen oder dem Verbergen von Dateien oder Systemdaten vor dem Betriebssystem erzielt.

8.4.1. Grundlagen zu Anti-Rootkit

AVG Anti-Rootkit ist ein spezielles Tool für die Erkennung und wirksame Entfernung gefährlicher Rootkits, also von Programmen und Technologien, die die Anwesenheit schädlicher Software auf Ihrem Computer verbergen können. ***AVG Anti-Rootkit*** erkennt Rootkits auf Basis eines vordefinierten Regelsatzes. Bitte beachten Sie, dass alle Rootkits erkannt werden (*nicht nur die infizierten*). Wenn ***AVG Anti-Rootkit*** ein Rootkit entdeckt, heißt das nicht unbedingt, dass das Rootkit auch infiziert ist. Manchmal werden Rootkits als Treiber eingesetzt oder sie gehören zu ordnungsgemäßen Anwendungen.

8.4.2. Benutzeroberfläche von Anti-Rootkit

Die Benutzeroberfläche von ***Anti-Rootkit*** enthält eine kurze Beschreibung der Funktionsweise der Komponentesowie Informationen über den aktuellen Status der Komponente (*Die Komponente Anti-Rootkit ist aktiv*) und über den Zeitpunkt des letzten mit ***Anti-Rootkit*** durchgeführten Tests.

Im unteren Teil des Dialogs finden Sie den Bereich ***Einstellungen für Anti-Rootkit***, in dem Sie einige grundlegende Funktionen für das Scannen nach vorhandenen Rootkits einstellen können. Markieren Sie zunächst die entsprechenden Kontrollkästchen, um festzulegen, welche Objekte gescannt werden sollen:

- ***Anwendungen scannen***
- ***DLL-Bibliotheken scannen***
- ***Treiber scannen***

Wählen Sie anschließend den Rootkit-Scanmodus aus:

- ***Schneller Rootkit-Scan*** – Nur der Systemordner wird gescannt (*normalerweise C:\Windows*)

- ***Vollständiger Rootkit-Scan*** – Alle verfügbaren Datenträger, mit Ausnahme von A: und B:, werden gescannt

Verfügbare Schaltflächen:

- ***Nach Rootkits suchen*** – Da der Rootkit-Scan kein integrierter Bestandteil des ***Scans für den gesamten Computer*** ist, können Sie den Rootkit-Scan mit dieser Schaltfläche direkt über die Benutzeroberfläche von ***Anti-Rootkit*** ausführen

- ***Änderungen speichern*** – Mit dieser Schaltfläche können Sie alle auf dieser Benutzeroberfläche vorgenommenen Änderungen speichern und zur ***Benutzeroberfläche von AVG*** (Komponentenüberblick) zurückkehren

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (Komponentenüberblick) zurückkehren, ohne Änderungen zu speichern

8.5. System-Tools

System-Tools sind Tools, die eine detaillierte Zusammenfassung der Umgebung von **AVG 9 Internet Security** zur Verfügung stellen. Die Komponente zeigt eine Übersicht über:

- Prozesse – Eine Liste der Prozesse (d. h. ausgeführte Anwendungen), die auf Ihrem Computer gerade aktiv sind

- Netzwerkverbindungen – Eine Liste der momentan aktiven Verbindungen

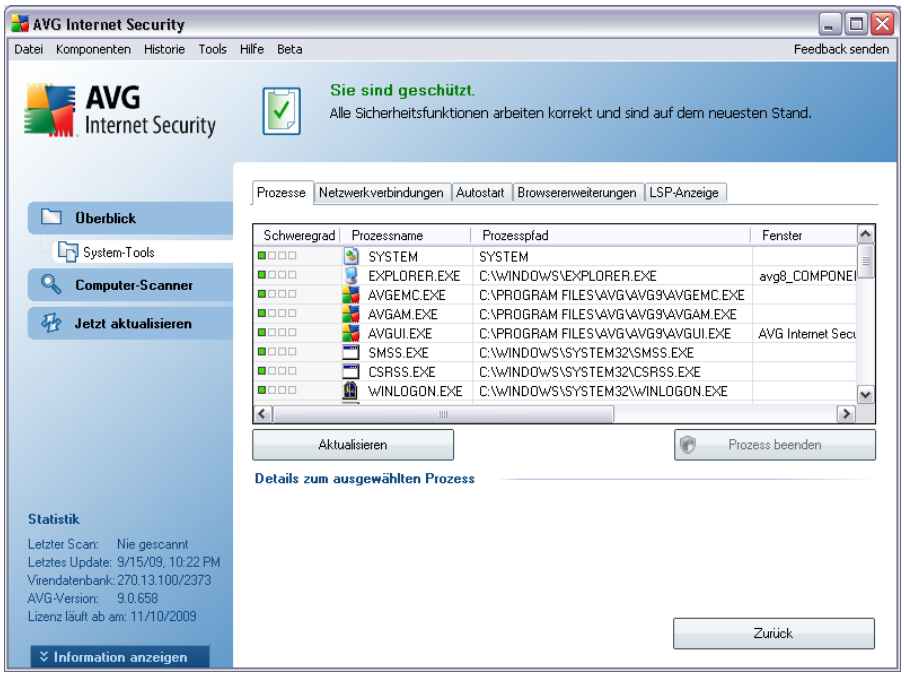
- Autostart – Eine Liste aller Anwendungen, die während des Starts von Windows ausgeführt werden

- Browsererweiterungen – Eine Liste der Plugins (z. B. Anwendungen), die in Ihrem Internetbrowser installiert sind

- LSP-Anzeige – Eine Liste des Layered Service Providers (LSP)

Die einzelnen Übersichten können auch bearbeitet werden, dies wird jedoch nur für sehr erfahrene Benutzer empfohlen!

8.5.1. Prozesse



Der Dialog ***Prozesse*** enthält eine Liste der Prozesse (*z. B. ausgeführte Anwendungen*), die derzeit auf dem Computer aktiv sind. Die Liste besteht aus mehreren Spalten:

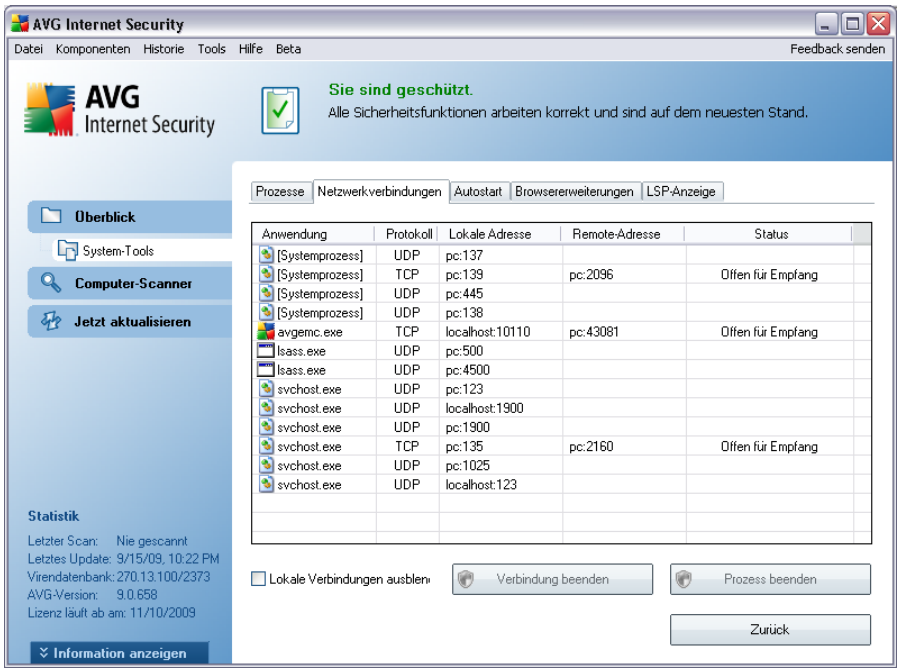
- ***Schweregrad*** – Eine grafische Darstellung des Schweregrads des jeweiligen Prozesses auf einer vierstufigen Skala von weniger schwer (■□□□) bis kritisch (■■■■)
- ***Prozessname*** – Name des ausgeführten Prozesses
- ***Prozesspfad*** – Physischer Pfad zum ausgeführten Prozess
- ***Fenster*** – Zeigt den Namen des Anwendungsfensters an, falls verfügbar
- ***Internet*** – Zeigt an, ob der ausgeführte Prozess mit dem Internet verbunden ist (*Ja/Nein*)
- ***Dienst*** – Zeigt an, ob der ausgeführte Prozess ein Dienst ist (*Ja/Nein*)
- ***PID*** – Die Prozesskennung ist eine eindeutige Windows-interne Prozesskennung

Schaltflächen

Auf der Oberfläche von ***System-Tools*** stehen folgende Schaltflächen zur Verfügung:

- ***Aktualisieren*** – Hiermit lässt sich die Liste der Prozesse mit ihrem aktuellen Status aktualisieren
- ***Prozess beenden*** – Sie können eine oder mehrere Anwendungen auswählen und durch Klicken auf diese Schaltfläche beenden. ***Es wird dringend davon abgeraten, Anwendungen zu beenden, es sei denn, Sie sind sich sicher, dass diese Anwendungen eine tatsächliche Bedrohung darstellen!***
- ***Zurück*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren.

8.5.2. Netzwerkverbindungen



Der Dialog ***Netzwerkverbindungen*** enthält eine Liste der gegenwärtig aktiven Verbindungen. Die Liste umfasst die folgenden Spalten:

- ***Anwendung*** – Der Name der Anwendung, die mit der Verbindung verknüpft

ist. Diese Information steht ausschließlich in Windows XP zur Verfügung.

- ***Protokoll*** – das für die Verbindung verwendete Übertragungsprotokoll:
  - TCP – ein zusammen mit dem Internet Protocol (IP) verwendetes Protokoll zur Datenübertragung im Internet
  - UDP – eine Alternative zum TCP-Protokoll
- ***Lokale Adresse*** – die IP-Adresse des lokalen Computers sowie die verwendete Portnummer
- ***Remote-Adresse*** – die IP-Adresse des Remote-Computers und die entsprechende Portnummer. Gegebenenfalls wird auch der Hostname des Remote-Computers ermittelt.
- ***Status*** – zeigt den wahrscheinlichsten aktuellen Status an (*Verbunden, Server sollte schließen, Abrufen, Aktives Schließen beendet, Passives Schließen, Aktives Schließen*)

Um ausschließlich externe Verbindungen anzuzeigen, aktivieren Sie im unteren Bereich des Dialogs unterhalb der Liste das Kontrollkästchen ***Lokale Verbindungen ausblenden***.

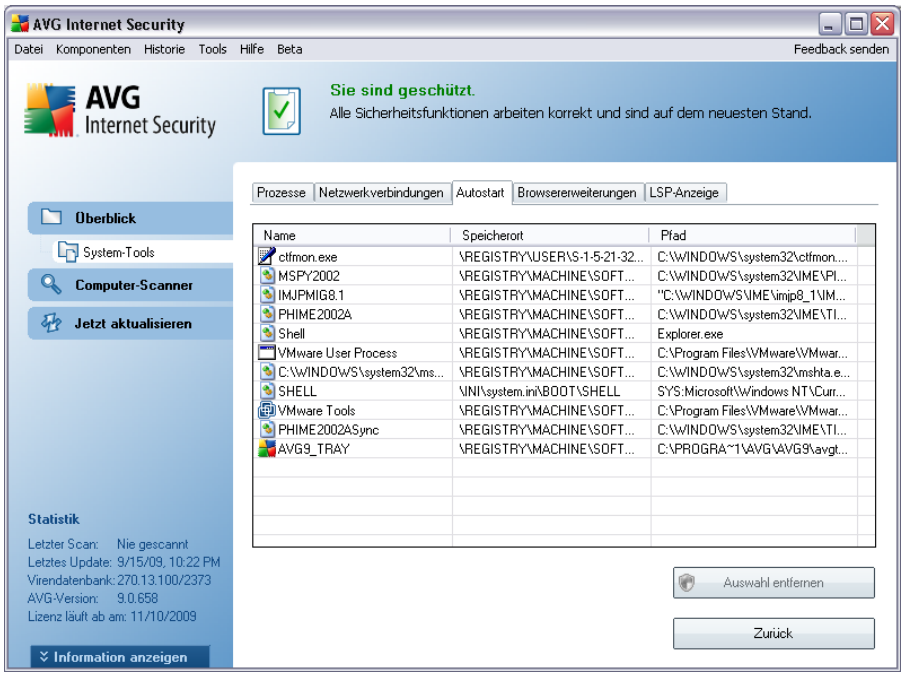
Schaltflächen

Folgende Schaltflächen sind verfügbar:

- ***Verbindung beenden*** – schließt eine oder mehrere in der Liste ausgewählte Verbindungen
- ***Prozess beenden*** – schließt eine oder mehrere Anwendungen, die mit den in der Liste ausgewählten Verbindungen verknüpft sind (*diese Schaltfläche steht nur unter Windows XP zur Verfügung*)
- ***Zurück*** – Hiermit kehren Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurück.

Manchmal können nur Anwendungen mit dem Status "Verbunden" beendet werden. Es wird dringend davon abgeraten, Verbindungen zu beenden, es sei denn, Sie sind sich sicher, dass sie eine tatsächliche Bedrohung darstellen!

8.5.3. Autostart

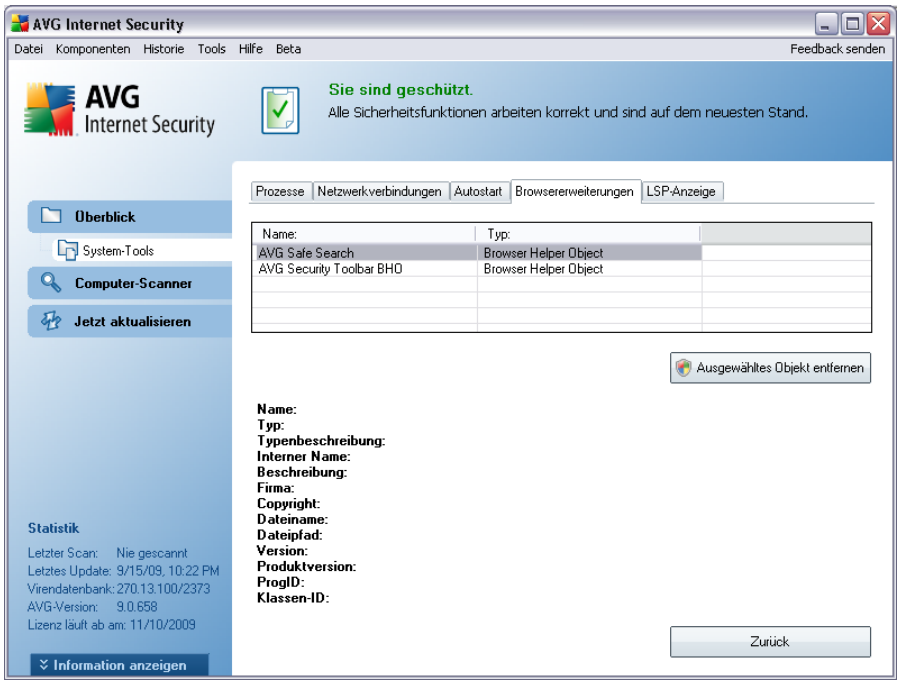


Im Dialog ***Autostart*** sind alle Anwendungen aufgelistet, die während des Starts von Windows ausgeführt werden. Sehr häufig erstellen Malware-Anwendungen automatisch selbst einen Registry-Eintrag für den Systemstart.

Sie können einen oder mehrere Einträge löschen, indem Sie diese markieren und auf die Schaltfläche ***Auswahl entfernen*** klicken. Mit der Schaltfläche ***Zurück*** können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren.

Es wird dringend davon abgeraten, Anwendungen zu löschen, es sei denn, Sie sind sich sicher, dass diese Anwendungen eine tatsächliche Bedrohung darstellen!

8.5.4. Browsererweiterungen



Der Dialog ***Browsererweiterungen*** enthält eine Liste der Plugins (*z. B. Anwendungen*) die in Ihrem Internetbrowser integriert sind. Diese Liste kann sowohl zulässige Anwendungs-Plugins als auch potentielle Malware-Programme enthalten. Klicken Sie in der Liste auf ein Objekt, um im unteren Bereich des Dialogs detaillierte Informationen über das ausgewählte Plugin anzuzeigen.

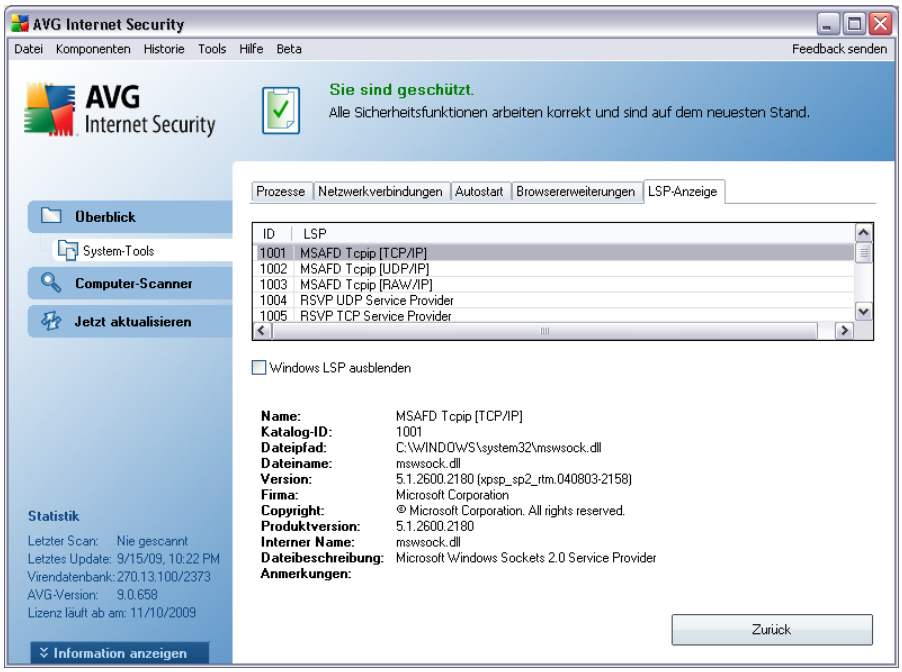
Schaltflächen

Auf dem Reiter ***Browsererweiterung*** stehen die folgenden Schaltflächen zur Verfügung:

- ***Ausgewähltes Objekt entfernen*** – Entfernt das in der Liste momentan markierte Plugin. ***Es wird dringend davon abgeraten, Plugins zu löschen, es sei denn, Sie sind sich sicher, dass diese Plugins eine tatsächliche Bedrohung darstellen!***

- ***Zurück*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren.

8.5.5. LSP-Anzeige



Der Dialog ***LSP-Anzeige*** enthält eine Liste der Layered Service Provider (LSP).

Ein ***Layered Service Provider*** (LSP) ist ein Systemtreiber, der mit den Netzwerkdiensten des Windows-Betriebssystems verknüpft ist. Er verfügt über Zugriffsmöglichkeiten auf alle Daten, die über den Computer empfangen und versendet werden, und er ist in der Lage, diese Daten zu ändern. Einige LSPs sind erforderlich, damit Windows eine Verbindung mit anderen Computern oder dem Internet herstellen kann. Bestimmte Malware-Anwendungen installieren sich jedoch selbst als LSP und haben damit Zugriff auf alle über den Computer übertragenen Daten. Daher kann Sie dieser Überblick dabei unterstützen, alle von LSPs ausgehenden potentiellen Bedrohungen zu überprüfen.

Unter bestimmten Umständen ist es auch möglich, beschädigte LSPs zu reparieren (*beispielsweise wenn die Datei entfernt wurde, die Registrierungseinträge jedoch unverändert geblieben sind*). Sobald ein reparabler LSP erkannt wurde, wird eine neue Schaltfläche zum Beheben des Problems angezeigt.

Entfernen Sie die Markierung im Kontrollkästchen Windows-LSP ausblenden***, um den Windows LSP in die Liste aufzunehmen.*** Mit der Schaltfläche ***Zurück*** können Sie zur Hauptseite der ***Benutzeroberfläche von AVG*** zurückkehren (*Komponentenübersicht*).

8.6. Firewall

Die Firewall ist ein System, das Richtlinien für die Zugangskontrolle zwischen mehreren Netzwerken durch das Blockieren und Zulassen von Datenverkehr durchsetzt. Jede Firewall verfügt über Regeln, die das interne Netzwerk vor Angriffen von außen (normalerweise aus dem Internet) schützen und die Kommunikation an jedem einzelnen Netzwerk-Port kontrollieren. Die Kommunikation wird gemäß der festgelegten Richtlinien bewertet und dann entweder zugelassen oder abgelehnt. Wenn die Firewall einen Angriffsversuch erkennt, „blockiert" sie diesen und verweigert dem Angreifer den Zugriff auf den Computer.

Die Konfiguration der Firewall lässt interne/externe Kommunikation (in beide Richtungen, eingehend oder ausgehend) über definierte Ports und für definierte Software-Anwendungen zu oder verweigert diese. Beispielsweise kann die Firewall so konfiguriert werden, dass nur eine Datenübertragung per Microsoft Explorer zugelassen wird. Jeder Versuch, Daten mit einem anderen Browser zu übertragen, würde blockiert.

Die Firewall verhindert, dass Ihre persönlichen Informationen ohne Ihre Erlaubnis von Ihrem Computer versandt werden. Sie steuert, wie Ihr Computer Daten mit anderen Computern im Internet oder im lokalen Netzwerk austauscht. Innerhalb einer Organisation schützt die Firewall Einzelrechner außerdem gegen Angriffe, die von internen Benutzern anderer Computer im Netzwerk ausgehen.

Empfehlung: *Es ist grundsätzlich nicht empfehlenswert, auf einem Computer mehr als eine Firewall zu verwenden. Die Sicherheit des Computers wird durch die Installation von mehreren Firewalls nicht erhöht. Es ist eher wahrscheinlich, dass Konflikte zwischen diesen Anwendungen auftreten. Daher wird empfohlen, nur eine Firewall auf einem Computer zu verwenden und alle anderen Firewalls zu deaktivieren. So wird das Risiko möglicher Konflikte und diesbezüglicher Probleme ausgeschlossen.*

8.6.1. Firewall-Richtlinien

Die Komponente ***Firewall*** in AVG kontrolliert den Verkehr an jedem einzelnen Netzwerk-Port Ihres Computers. Abhängig von den definierten Regeln wertet die ***Firewall***Anwendungen aus, die entweder auf Ihrem Computer laufen (und sich mit dem Internet/lokalen Netzwerk verbinden wollen) oder die von außen eine Verbindung zu Ihrem Computer herstellen möchten. Für jede dieser Anwendungen wird dann von der ***Firewall*** darüber entschieden, ob die Kommunikation über die Netzwerkports zugelassen oder verweigert wird. Bei einer unbekannten Anwendung (ohne festgelegte ***Firewall***-Regeln) werden Sie von der***Firewall*** standardmäßig dazu aufgefordert, anzugeben, ob Sie die Kommunikation zulassen oder blockieren möchten.

Hinweis: *Die AVG Firewall ist nicht für Serverplattformen vorgesehen!*

Funktionen der AVG Firewall:

- Automatisches Zulassen oder Blockieren von Kommunikationsversuchen bekannter Anwendungen oder Aufforderung zur Bestätigung
- Verwendung umfassender Profile mit vordefinierten Regeln anhand individueller Anforderungen
- Archivierung aller festgelegten Profile und Einstellungen
- Automatischer Profilwechsel beim Herstellen einer Verbindung zu wechselnden Netzwerken oder bei Verwendung verschiedener Netzwerkadapter

8.6.2. Firewall-Profile

Die ***Firewall*** ermöglicht das Festlegen spezifischer Sicherheitsregeln, je nachdem, ob es sich um einen Computer in einer Domäne, einen Einzelplatzrechner oder um ein Notebook handelt. Für jede dieser Optionen ist eine andere Sicherheitsstufe erforderlich, die von den entsprechenden Profilen abgedeckt wird. Ein***Firewall***-Profil ist also kurz gesagt eine spezifische Konfiguration der Komponente ***Firewall*** und Sie können verschiedene vordefinierte Konfigurationen verwenden.

Verfügbare Profile

- ***Alle zulassen*** – ist ein ***Firewall***-Systemprofil, das vom Hersteller voreingestellt wurde und immer vorhanden ist. Wenn dieses Profil aktiviert ist, bestehen weder Einschränkungen hinsichtlich der Netzwerkkommunikation noch werden Sicherheitsrichtlinien angewendet – genau wie bei einer deaktivierten ***Firewall*** *(d. h. alle Anwendungen werden zugelassen, Pakete werden jedoch weiterhin überprüft – um jede Filterung zu deaktivieren, müssen Sie die Firewall deaktivieren)*. Dieses Systemprofil kann weder kopiert noch gelöscht werden, und die Einstellungen können nicht geändert werden.
- ***Alle blockieren*** – ist ein ***Firewall***-Systemprofil, das vom Hersteller voreingestellt wurde und immer vorhanden ist. Wenn dieses Profil aktiviert ist, wird die gesamte Netzwerkkommunikation blockiert und der Computer ist weder über externe Netzwerke erreichbar, noch kann er mit diesen kommunizieren. Dieses Systemprofil kann weder kopiert noch gelöscht werden, und die Einstellungen können nicht geändert werden.

- ***Benutzerdefinierte Profile***:

  - ***Computer unterwegs*** – Geeignet für alle gängigen Desktop-PCs, die direkt mit dem Internet verbunden sind, sowie für Notebooks, die außerhalb des sicheren Unternehmensnetzwerks mit dem Internet verbunden werden. Wählen Sie diese Option aus, wenn Sie die Verbindung von zu Hause herstellen oder Ihr Computer Bestandteil eines kleinen Unternehmensnetzwerks ohne zentrale Steuerung ist. Wählen Sie diese Option außerdem, wenn Sie auf Reisen sind und Verbindungen von verschiedenen unbekannten und möglicherweise gefährlichen Orten herstellen möchten (*in Internetcafés, Hotelzimmern usw.*). Es werden strengere Regeln erstellt, da angenommen wird, dass solche Computer über keinen zusätzlichen Schutz verfügen und deshalb die höchstmögliche Schutzstufe erfordern.

  - ***Computer in Domäne*** – Geeignet für Computer in einem lokalen Netzwerk, beispielsweise in einer Schule oder einem Unternehmensnetzwerk. Es wird davon ausgegangen, dass das Netzwerk durch weitere Schutzmaßnahmen geschützt ist, so dass eine niedrigere Sicherheitsstufe als bei Einzelplatzrechnern verwendet werden kann.

  - ***Heim- oder Büronetzwerk*** – Geeignet für Computer in einem kleinen Netzwerk, beispielsweise zu Hause oder in einem kleinen Unternehmen, in dem in aller Regel mehrere Computer ohne „zentralen" Administrator verbunden sind.

Profilwechsel

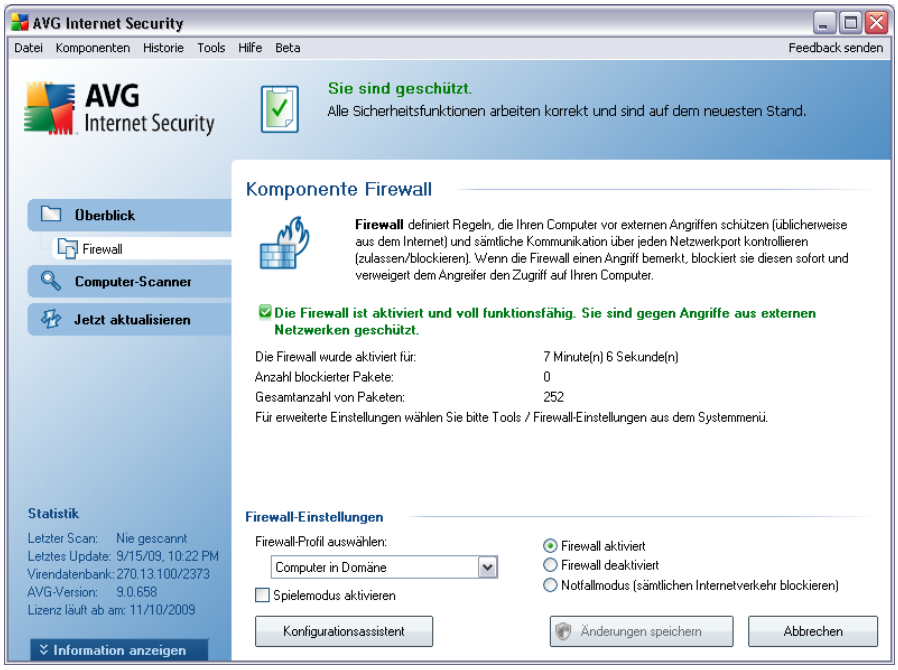
Diese Funktion bewirkt, dass die ***Firewall*** bei Verwendung eines bestimmten Netzwerkadapters oder bei Verbindung mit einem bestimmten Netzwerktyp automatisch in das festgelegte Profil wechselt. Wenn für einen Netzwerkbereich noch kein Profil festgelegt wurde, zeigt die ***Firewall*** beim nächsten Herstellen einer Verbindung mit diesem Bereich einen Dialog an, in dem Sie aufgefordert werden, ein Profil zuzuweisen.

Sie können allen lokalen Netzwerkschnittstellen oder -bereichen ein Profil zuweisen und im Dialog ***Profilauswahl***weitere Einstellungen definieren; in diesem Dialog können Sie die Funktion auch deaktivieren, wenn Sie sie nicht verwenden möchten. (*In diesem Fall wird für alle Verbindungen das Standardprofil verwendet*.)

Die Funktion wird vor allem von Notebookbenutzern als hilfreich erachtet, die verschiedene Verbindungstypen verwenden. Wenn Sie einen Desktop-Computer besitzen und nur einen Verbindungstyp verwenden (*beispielsweise eine*

kabelgebundene Internetverbindung), brauchen Sie sich über Profilwechsel keine Gedanken zu machen, da Sie diese Funktion höchstwahrscheinlich nicht benötigen.

8.6.3. Benutzeroberfläche der Firewall



Die Benutzeroberfläche der ***Firewall*** umfasst grundlegende Informationen über die Funktionen der Komponente sowie eine kurze Übersicht mit statistischen Zahlen der ***Firewall***:

- ***Die Firewall wurde aktiviert für*** – Zeit, die seit dem letzten Start der Firewall abgelaufen ist
- ***Anzahl blockierter Pakete*** - Anzahl der blockierten Pakete aus der Gesamtanzahl der überprüften Pakete
- ***Gesamtanzahl von Paketen*** - Anzahl der Pakete, die überprüft wurden, während die Firewall ausgeführt wurde

Basiskonfiguration der Komponente

- ***Firewall-Profil auswählen*** – Wählen Sie im Dropdown-Menü eines der definierten Profile aus ; zwei Profile sind jederzeit verfügbar (die

Standardprofile ***Alle zulassen*** *und* ***Alle blockieren***), weitere Profile wurden manuell durch eine Bearbeitung der Profile im Dialog ***Profile*** der ***Firewall-Einstellungen*** hinzugefügt.

- ***Spielemodus aktivieren*** – Aktivieren Sie dieses Kontrollkästchen, um sicherzustellen, dass während der Ausführung von Anwendungen im Vollbildmodus (Spiele, PowerPoint-Präsentationen usw.) keine Dialoge von der ***Firewall*** angezeigt werden, in denen Sie aufgefordert werden, die Kommunikation für unbekannte Anwendungen zuzulassen oder zu blockieren. Wenn eine unbekannte Anwendung versucht, zu diesem Zeitpunkt über das Netzwerk zu kommunizieren, wird die ***Firewall*** , abhängig von den Einstellungen im aktuellen Profil, diesen Versuch zulassen oder blockieren.

- ***Firewall-Status***:

  - ***Firewall aktiviert*** - Wählen Sie diese Option aus, um die Kommunikation der Anwendungen zu erlauben, die in den Regeln des ausgewählten ***Firewall***-Profils als „zulässig" gekennzeichnet sind

  - ***Firewall deaktiviert*** - Mit dieser Option wird die ***Firewall*** vollständig ausgeschaltet und der gesamte Netzwerkverkehr wird ohne Überprüfung zugelassen!

  - ***Notfallmodus (sämtlichen Internetverkehr blockieren)*** - Wählen Sie diese Option, um den gesamten Datenverkehr an jedem einzelnen Netzwerkport zu blockieren; die ***Firewall*** wird weiterhin ausgeführt, aber der gesamte Netzwerkverkehr ist gestoppt

Hinweis: *Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Falls Sie Änderungen an der Konfiguration der Firewall vornehmen müssen, wählen Sie im Systemmenü die Option* ***Tools/ Firewall-Einstellungen*** *aus, und bearbeiten Sie die Konfiguration der Firewall im daraufhin angezeigten Dialog* ***Firewall-Einstellungen*** *.*

Schaltflächen

- ***Konfigurationsassistent*** – Klicken Sie auf diese Schaltfläche, um den entsprechenden Dialog (*beim Installationsvorgang verwendet*) namens ***Angaben zur Computernutzung*** aufzurufen, wo Sie die Konfiguration der ***Firewall*** vornehmen können

- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückkehren

8.7. eMail-Scanner

eMails sind eine der häufigsten Quellen von Viren und Trojanern. eMail-Nachrichten können jedoch in Form von Phishing und Spam auch noch andere Risiken in sich bergen. Kostenlose eMail-Konten sind häufiger solchen schädlichen eMails ausgesetzt (*da nur selten Technologie für Anti-Spam eingesetzt wird*); solche Konten werden vor allem von privaten Benutzern verwendet. Durch das Aufsuchen unbekannter Websites sowie das Ausfüllen von Online-Formularen mit persönlichen Daten (*inklusive eMail-Adresse*) erhöht sich für private Benutzer das Risiko, Opfer eines Angriffs via eMail zu werden. Unternehmen nutzen in der Regel eigene eMail-Konten und verwenden Anti-Spam-Filter, um die beschriebenen Risiken zu minimieren.

8.7.1. Grundlagen zum eMail-Scanner

Die Komponente ***eMail-Scanner*** prüft eingehende und ausgehende eMails automatisch. Sie können diese Komponente für eMail-Clients verwenden, die über kein Plugin von AVG verfügen (*Outlook Express, Mozilla, Incredimail usw.*).

Während der Installation von AVG werden für die Prüfung der eMails automatische Server eingerichtet: einer für die Prüfung eingehender eMails und einer für die Prüfung ausgehender eMails. Mithilfe dieser beiden Server werden eMails an den Ports 110 und 25 (*den Standardports für das Senden/Empfangen von eMails*) automatisch überprüft.

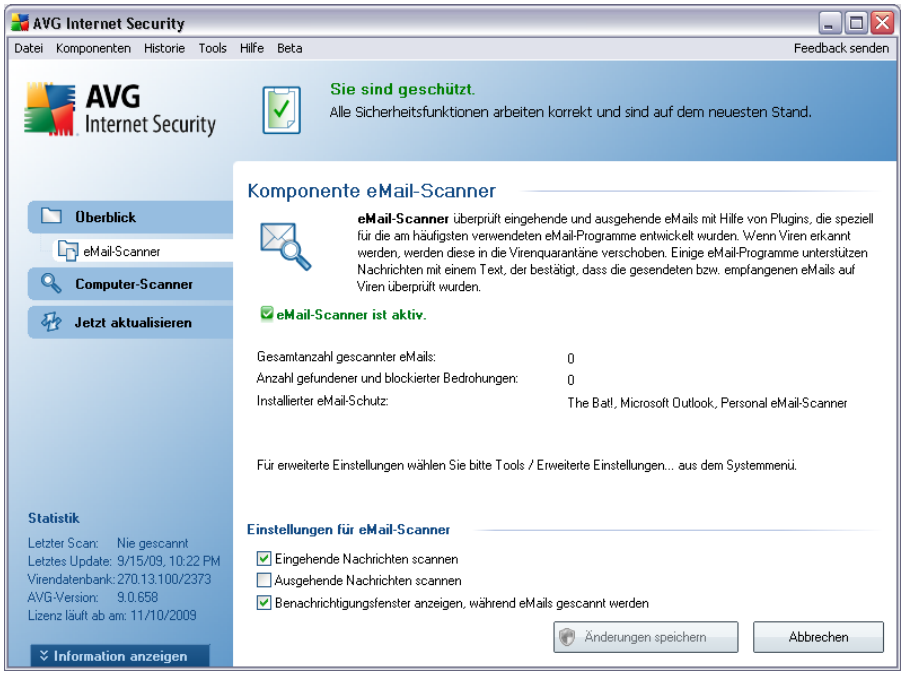
eMail-Scanner fungiert als Schnittstelle zwischen dem jeweiligen eMail-Client und eMail-Servern im Internet.

- ***Eingehende eMail:*** Beim Empfang einer eMail vom Server prüft die Komponente ***eMail-Scanner*** die Nachricht auf Viren, entfernt infizierte Anhänge und fügt eine Zertifizierung hinzu. Sobald ein Virus erkannt wird, wird es umgehend in die ***Virenquarantäne*** verschoben. Dann wird die Nachricht an den eMail-Client übergeben.

- ***Ausgehende eMail:*** Die Nachricht wird vom eMail-Client an eMail-Scanner gesendet; dieser prüft die Nachricht mitsamt Anhängen auf Viren und leitet die eMail an den SMTP-Server weiter (*die Prüfung ausgehender eMails ist standardmäßig deaktiviert, kann jedoch manuell aktiviert werden*).

Hinweis: *AVG eMail-Scanner ist nicht für Serverplattformen vorgesehen!*

8.7.2. Benutzeroberfläche des eMail-Scanners



Der Dialog der Komponente ***eMail-Scanner*** enthält eine kurze Funktionsbeschreibung der Komponente, Informationen über den aktuellen Status (*eMail-Scanner ist aktiv.*) sowie die folgenden statistischen Daten:

- ***Gesamtanzahl gescannter eMails*** – Anzahl der eMails, die seit dem letzten Start des ***eMail-Scanners*** gescannt wurden (*bei Bedarf kann dieser Wert zurückgesetzt werden, z. B. zu Statistikzwecken – Wert zurücksetzen*)
- ***Anzahl gefundener und blockierter Bedrohungen*** – Anzahl der Infektionen, die seit dem letzten Start des ***eMail-Scanners*** in eMail-Nachrichten gefunden wurden
- ***Installierter eMail-Schutz*** – Informationen zu einem bestimmten eMail-Schutz-Plugin bezüglich Ihres installierten Standard-eMail-Clients

Basiskonfiguration der Komponente

Im unteren Teil des Dialogs befindet sich der Bereich ***Einstellungen für eMail-***

Scanner, in dem Sie einige Grundfunktionen der Komponente bearbeiten können:

- ***Eingehende Nachrichten scannen*** – Aktivieren Sie diesen Eintrag, damit alle in Ihrem Konto eingehenden eMails auf Viren überprüft werden. Dieser Eintrag ist standardmäßig aktiviert, und wir empfehlen Ihnen ausdrücklich, diese Einstellung nicht zu ändern!

- ***Ausgehende Nachrichten scannen*** – Markieren Sie diesen Eintrag, damit alle eMails, die von Ihrem Konto gesendet werden, auf Viren geprüft werden. Standardmäßig ist dieser Eintrag deaktiviert.

- *Benachrichtigungssymbol anzeigen, während eMails gescannt werden* – Während des Scanvorgangs zeigt der ***eMail-Scanner*** einen Benachrichtigungsdialog mit Informationen über die von der Komponente gerade ausgeführte Aufgabe an (*Herstellen einer Verbindung zum Server, Herunterladen einer Nachricht, Scannen der Nachricht usw.*). Diese Option ist aktiviert und kann nicht bearbeitet werden.

Eine erweiterte Konfiguration der Komponente ***eMail-Scanner*** kann über das Systemmenü mit den Optionen ***Tools / Erweiterte Einstellungen*** durchgeführt werden. Die erweiterte Konfiguration sollte jedoch nur von erfahrenen Benutzern verwendet werden!

Hinweis: *Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option* ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

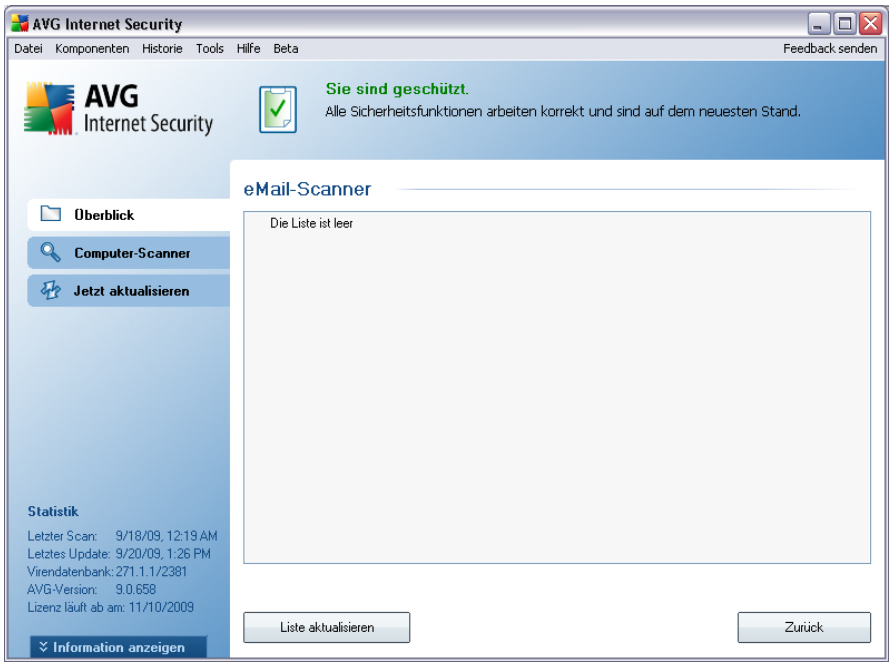
Schaltflächen

Auf der Benutzeroberfläche des ***eMail-Scanners*** sind folgende Schaltflächen verfügbar:

- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie in diesem Dialog durchgeführt haben, zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der Benutzeroberfläche von AVG (Komponentenübersicht) zurückkehren

8.7.3. eMail-Scanner-Erkennung



Im Dialog ***eMail-Scanner-Erkennung*** (*erreichbar im Systemmenü über die Option Historie/eMail-Scanner*) wird eine Liste aller Funde angezeigt, die von der Komponente ***eMail-Scanner*** **.**erkannt wurden. Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Infektion*** - Beschreibung (nach Möglichkeit auch Name) des erkannten Objekts
- ***Objekt*** - Speicherort des Objekts
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Der Zeitpunkt (Datum und Uhrzeit), zu dem das verdächtige Objekt entdeckt wurde
- ***Objekttyp*** - Typ des erkannten Objekts

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei exportieren***) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***).

Schaltflächen

Auf der Benutzeroberfläche der ***eMail-Scanner-Erkennung*** stehen die folgenden Schaltflächen zur Verfügung:

- ***Liste aktualisieren*** – Aktualisiert die Liste der erkannten Bedrohungen
- ***Zurück*** – Mit dieser Schaltfläche können Sie zur ***Standardbenutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren

8.8. Identitätsschutz

AVG Identitätsschutz ist ein Anti-Malware-Produkt, das Identitätsdiebe daran hindert, Ihre Kennwörter, Bankkontodetails, Kreditkartennummern und andere persönliche Daten zu stehlen, wozu sie verschiedene Arten bösartiger Software (*Malware*) verwenden, die es auf Ihren Computer absehen. Es sorgt sicher, dass alle auf Ihrem Computer ausgeführten Programme ordnungsgemäß funktionieren. ***AVG Identitätsschutz*** erkennt und blockiert kontinuierlich verdächtiges Verhalten und schützt Ihren Computer vor neuer Malware.

8.8.1. Grundlagen des Identitätsschutzes

AVG Identitätsschutz ist eine Anti-Malware-Komponente, die Sie mithilfe von Verhaltenstechnologien vor allen Arten von Malware schützt(*Spyware, Bots, Identitätsdiebstahl usw.*) und mit dem Zero-Day-Schutz vor neuen Viren bewahrt. Während Malware immer komplexer wird und in Form normaler Programme auftreten kann, mit denen Identitätsräuber in Ihren Computer eindringen, schützt Sie ***AVG Identitätsschutz*** vor dieser Art ausführungsbasierter Malware. Es handelt sich um einen Zusatzschutz für ***AVG Anti-Virus*** , der Sie auf Grundlage von Signatur- und Scanverfahren vor dateibasierten und bekannten Viren schützt.

Wir empfehlen Ihnen dringend, sowohl AVG Anti-Virus als auch AVG Identitätsschutz zu installieren, um einen vollständigen Schutz Ihres PCs zu gewährleisten.

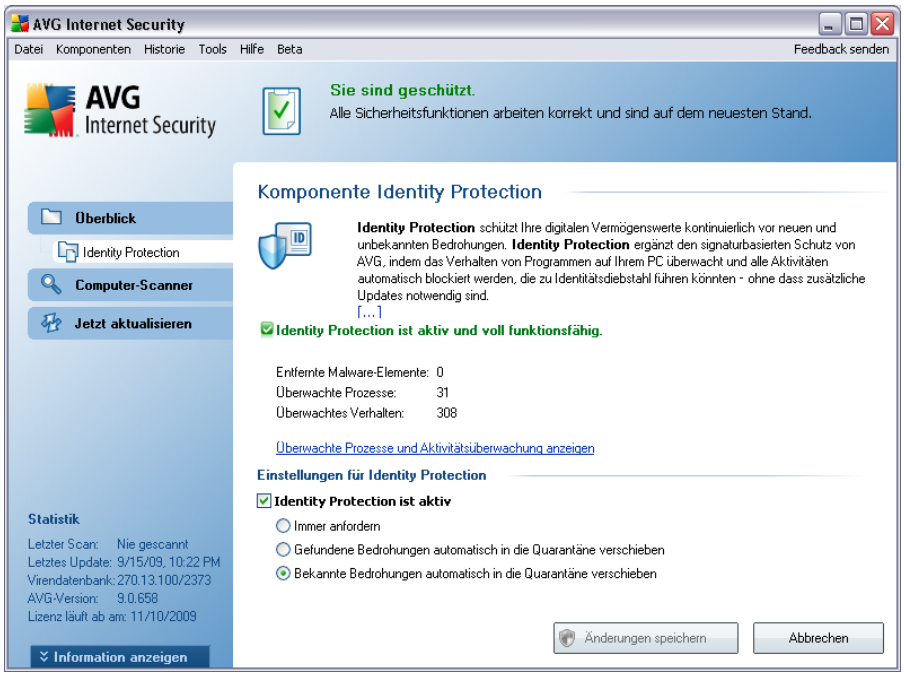
8.8.2. Benutzeroberfläche des Identitätsschutzes

Die Benutzeroberfläche der Komponente ***Identitätsschutz*** umfasst eine kurze Beschreibung der Grundfunktionen der Komponente, ihren Status (*AVG Identitätsschutz ist aktiviert und voll funktionsfähig.*) und verschiedene statistische Daten:

- ***Entfernte Malware-Elemente*** – Gibt die Zahl der als Malware ermittelten und entfernten Anwendungen an

- ***Überwachte Prozesse*** – Die Zahl der momentan ausgeführten Anwendungen, die mit dem Identitätsschutz überwacht werden

- ***Überwachtes Verhalten*** – Die Zahl der spezifischen Aktionen, die in den überwachten Anwendungen ausgeführt werden



Basiskonfiguration der Komponente

Im unteren Bereich des Dialogs finden Sie die ***Einstellungen für Identitätsschutz***, wo Sie bestimmte Grundfunktionen der Komponente bearbeiten können:

- ***Identitätsschutz ist aktiv*** – (*standardmäßig aktiviert*): Markieren Sie diese Option, um den Identitätsschutz zu aktivieren und weitere Bearbeitungsoptionen zu öffnen.

In manchen Fällen meldet ***Identitätsschutz***, dass eine seriöse Datei verdächtig oder gefährlich ist. Da ***Identitätsschutz*** Bedrohungen auf Grundlage ihres Verhaltens erkennt, tritt dies normalerweise dann auf, wenn ein Programm versucht, gedrückte Tasten zu überwachen, andere Programme oder einen neuen Treiber auf dem Computer zu installieren.

Wählen Sie daher bitte eine der folgenden Optionen, um das Verhalten von ***Identitätsschutz*** bei Erkennung einer verdächtigen Aktivität festzulegen:

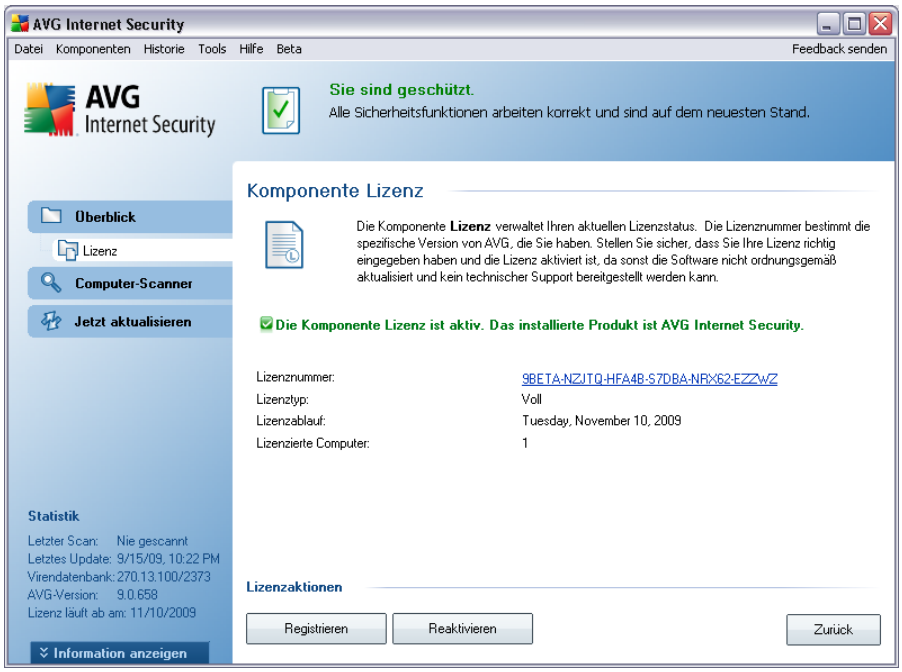
- ***Immer anfordern*** – Wenn eine Anwendung als Malware erkannt wird, werden Sie gefragt, ob diese blockiert werden soll
- ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** – Alle als Malware erkannten Anwendungen werden automatisch blockiert
- ***Bekannte Bedrohungen automatisch in die Quarantäne verschieben*** – Nur Anwendungen, bei denen es sich mit absoluter Sicherheit um Malware handelt, werden blockiert (*diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Einstellung nur dann zu ändern, wenn Sie einen guten Grund dafür haben*)

Schaltflächen

Auf der Benutzeroberfläche des ***eMail-Scanners*** sind folgende Schaltflächen verfügbar:

- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie in diesem Dialog durchgeführt haben, zu speichern und zu übernehmen
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der Benutzeroberfläche von AVG (Komponentenübersicht) zurückkehren

8.9. Lizenz



Die Komponente ***Lizenz*** enthält eine kurze Beschreibung der Funktionsweise der Komponente, Informationen zum aktuellen Status (*die Komponente Lizenz ist aktiv.*) sowie die folgenden Informationen:

- ***Lizenznummer*** – Hier ist die Lizenznummer vollständig dargestellt. Wenn Sie die Lizenznummer eingeben, müssen Sie diese absolut präzise und exakt wie angezeigt eingeben. Aus diesem Grund empfehlen wir ausdrücklich, zur Verwendung der Lizenznummer die Methode „Kopieren und Einfügen" zu nutzen.

- ***Lizenztyp*** – Gibt den installierten Produkttyp an.

- ***Lizenzablauf*** – Dieses Datum zeigt, wie lange Ihre Lizenz gültig ist. Wenn Sie **AVG 9 Internet Security** über dieses Datum hinaus weiter verwenden möchten, müssen Sie Ihre Lizenz verlängern. Die Verlängerung der Lizenz kann online auf der Website von AVG (http://www.avg.com/) durchgeführt werden.

- ***Lizenzierte Computer*** – Gibt an, auf wie vielen Workstations **AVG 9 Internet Security** installiert werden darf.

Schaltflächen

- ***Registrieren*** – Stellt eine Verbindung zur Registrierungsseite der Website von AVG (http://www.avg.com/) her. Bitte geben Sie Ihre Registrierungsdaten ein; nur Kunden, die ihr AVG-Produkt registrieren, erhalten kostenlosen technischen Support.

- ***Reaktivieren***– Öffnet den Dialog ***AVG aktivieren***mit den Daten, die Sie im Dialog ***AVG personalisieren***des Installationsvorgangs eingegeben haben. In diesem Dialog können Sie Ihre Lizenznummer eingeben, um entweder die Vertriebsnummer (*die Nummer, mit der Sie AVG installiert haben*) oder die alte Lizenznummer (*zum Beispiel beim Upgrade auf ein neues AVG-Produkt*) zu ersetzen.

- ***Zurück*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der Benutzeroberfläche von AVG (Komponentenübersicht) zurückkehren.

8.10. Link Scanner

8.10.1. Grundlagen zum Link Scanner

Die Komponente ***Link Scanner*** bietet Schutz vor Websites, mit denen über den Webbrowser oder seine Plugins Malware auf Ihrem Computer installiert wird. Die Technologie von ***Link Scanner*** umfasst zwei Hauptbestandteile: ***AVG Search-Shield*** und ***AVG Active Surf-Shield***:

- ***AVG Search-Shield*** enthält eine Liste von Websites (*URL-Adressen*), deren Gefährlichkeit bekannt ist. Wenn Sie die Suchmaschinen Google, Yahoo!, MSN oder Baidu verwenden, werden alle Suchergebnisse gemäß dieser Liste überprüft. Jedes Ergebnis erhält anschließend ein Zertifikatssymbol (*bei Suchergebnissen von Yahoo! werden nur die Zertifikatssymbole für „Website-Exploits" angezeigt*). Websites, deren Adresse Sie direkt in den Browser eingeben oder auf die Sie über einen Link auf einer anderen Website oder in einer eMail gelangen, werden automatisch überprüft und gegebenenfalls blockiert.

- ***AVG Active Surf-Shield*** scannt die Inhalte der von Ihnen besuchten Websites unabhängig von deren Adresse. Selbst wenn eine Website nicht von ***AVG Search-Shield*** erkannt wird (*z. B. wenn eine neue verseuchte Website erstellt wird oder wenn eine bislang saubere Website nun Malware enthält*), wird diese von ***AVG Active Surf-Shield*** erkannt und blockiert, sobald Sie

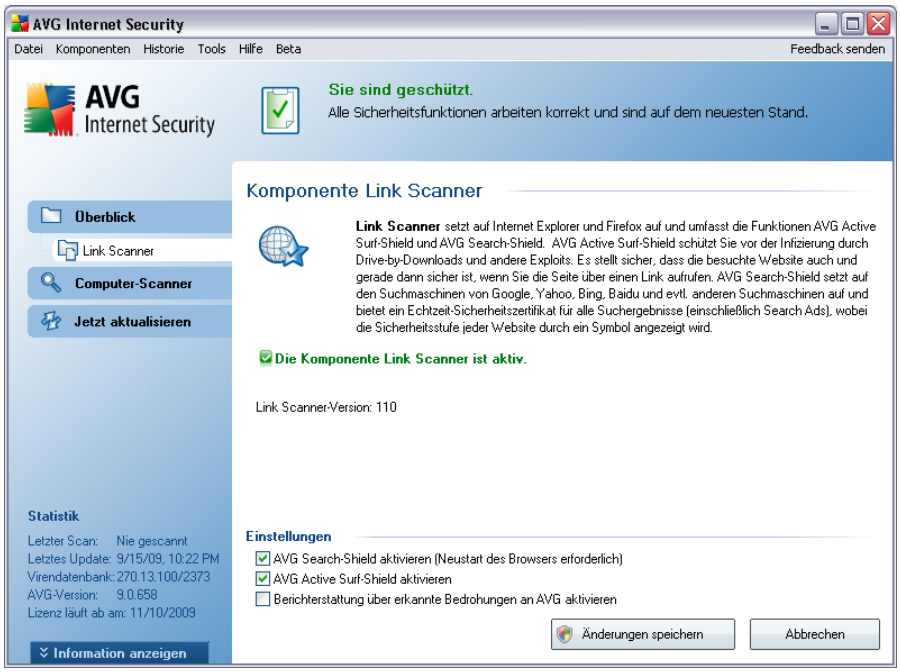
versuchen, die Website aufzurufen.

Hinweis: *Der AVG Link Scanner ist nicht für Serverplattformen vorgesehen!*

8.10.2. Benutzeroberfläche des Link Scanners

Die Komponente ***Link Scanner*** besteht aus zwei Teilen, die Sie in der Oberfläche der ***Komponente Link Scanner*** aktivieren oder deaktivieren können:

Die Benutzeroberfläche von ***Link Scanner*** umfasst eine kurze Beschreibung der Funktionen der Komponente sowie Informationen über deren aktuellen Status (*Die Komponente Link Scanner ist aktiv.*). Darüber hinaus können Sie die neueste Versionsnummer der ***Link Scanner***-Datenbank (|*Link Scanner-Version*) abrufen.



Im unteren Bereich des Dialogs können Sie verschiedene Optionen bearbeiten:

- ***AVG Search-Shield*** aktivieren – (*standardmäßig aktiviert*): Benachrichtigungssymbole zu Suchabfragen in Google, Yahoo! oder MSN, die darauf hinweisen, dass der Inhalt der als Suchergebnis angezeigten Websites überprüft wurde.

- ***AVG Active Surf-Shield*** aktivieren – *(standardmäßig aktiviert*): Aktiver (*Echtzeit*-) Schutz vor unbeabsichtigtem Zugriff auf Exploit-Sites. Die

Verbindungsherstellung zu bekannten bösartigen Sites und deren schädlichem Inhalt wird blockiert, wenn der Benutzer diese Sites über einen Webbrowser (*oder eine andere Anwendung, die HTTP verwendet*), aufruft.

- ***Berichterstattung über erkannte Bedrohungen an AVG aktivieren*** – Aktivieren Sie diese Option, um die Rückmeldung über Exploits und bösartige Sites, die von Benutzern über ***Safe Surf*** oder ***Safe Search*** gefunden wurden, zu ermöglichen und so die Datenbank mit Informationen über schädliche Aktivitäten im Web zu vervollständigen.

8.10.3. AVG Search-Shield

Wenn das Internet mit aktiviertem***AVG Search-Shield*** durchsucht wird, werden alle angezeigten Suchergebnisse der bekanntesten Suchmaschinen wie Yahoo!, Google, MSN usw. auf gefährliche oder verdächtige Links hin untersucht. Da die ***AVG Security Toolbar*** diese Links überprüft und gefährliche Links entsprechend markiert, werden Sie gewarnt, bevor Sie auf solche Links klicken. So können Sie sicherstellen, dass Sie ausschließlich sichere Websites aufrufen.

Während ein Link auf der Seite mit den Suchergebnissen überprüft wird, weist ein Symbol neben dem Link auf diese laufende Überprüfung hin. Sobald die Bewertung abgeschlossen ist, wird das entsprechende Informationssymbol angezeigt:

 Die verlinkte Seite stellt kein Sicherheitsrisiko dar. (*Bei der Suche mit Yahoo! wird innerhalb der AVG Security Toolbar das rotierende AVG-Symbol nicht angezeigt!*)

 Die verlinkte Seite enthält keine Bedrohungen, wird aber als verdächtig eingestuft (*die Herkunft/der Zweck der Seite ist fragwürdig, weshalb von Online-Einkäufen usw. abgeraten wird*).

 Die verlinkte Seite ist entweder selbst sicher, enthält aber weitere Links zu tatsächlich gefährlichen Seiten oder weist verdächtigen Code auf, auch wenn dieser momentan keine direkte Bedrohung darstellt.

 Die verlinkte Seite enthält aktive Bedrohungen! Aus Sicherheitsgründen können Sie nicht auf diese Seite zugreifen.

 Auf die verlinkte Seite kann nicht zugegriffen werden. Darum konnte sie auch nicht gescannt werden.

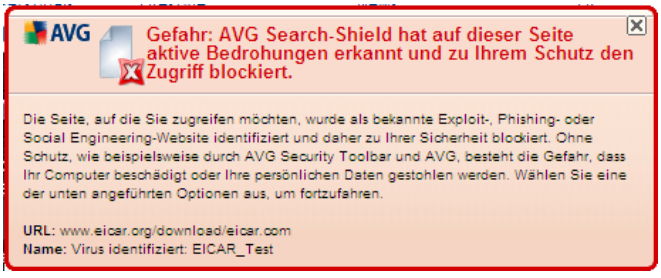
Wenn Sie mit der Maus über ein bestimmtes Bewertungssymbol fahren, werden Details zu dem entsprechenden Link angezeigt. Zu den Informationen gehören Details

über die Art der Gefahr (sofern vorhanden), die IP-Adresse des Links sowie den Zeitpunkt der Überprüfung durch AVG:

8.10.4. AVG Active Surf-Shield

Diese leistungsfähige Schutzfunktion sorgt dafür, dass bösartige Inhalte von jeder Webseite, die Sie öffnen möchten, blockiert und nicht auf Ihren Computer heruntergeladen werden können. Wenn diese Funktion aktiviert ist und Sie auf einen gefährlichen Link klicken oder die Internetadresse einer gefährlichen Site eingeben, wird die entsprechende Webseite automatisch blockiert, damit sich Ihr Computer nicht infiziert. Denken Sie daran, dass Website-Exploits Ihren Computer bereits infizieren können, wenn Sie einfach nur die entsprechende Site besuchen. Wenn Sie versuchen, auf eine gefährliche Webseite mit Exploits oder anderen ernsthaften Bedrohungen zuzugreifen, hält die ***AVG Security Toolbar*** Ihren Browser davon ab, die Seite zu öffnen.

Wenn Sie in Ihrem Webbrowser auf eine gefährliche Website stoßen, werden Sie von der ***AVG Security Toolbar*** mit einem Fenster gewarnt, das in etwa wie folgt aussieht:



Der Aufruf einer solchen Website ist äußerst gefährlich und wird nicht empfohlen!

8.11. Web Shield

8.11.1. Grundlagen zu Web Shield

Web Shield ist eine Art von Echtzeitschutz. Der Inhalt besuchter Webseiten (und möglicher enthaltener Dateien) wird gescannt, noch bevor sie in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen werden.

Web Shield erkennt, ob eine Seite, die Sie gerade besuchen, gefährliches Javascript enthält, und verhindert die Anzeige der Seite. Die Komponente erkennt auch die auf einer Seite enthaltene Malware, stoppt automatisch das Herunterladen und sorgt so dafür, dass sie niemals auf Ihren Computer gelangt.

Hinweis: *AVG Web Shield ist nicht für Serverplattformen vorgesehen!*

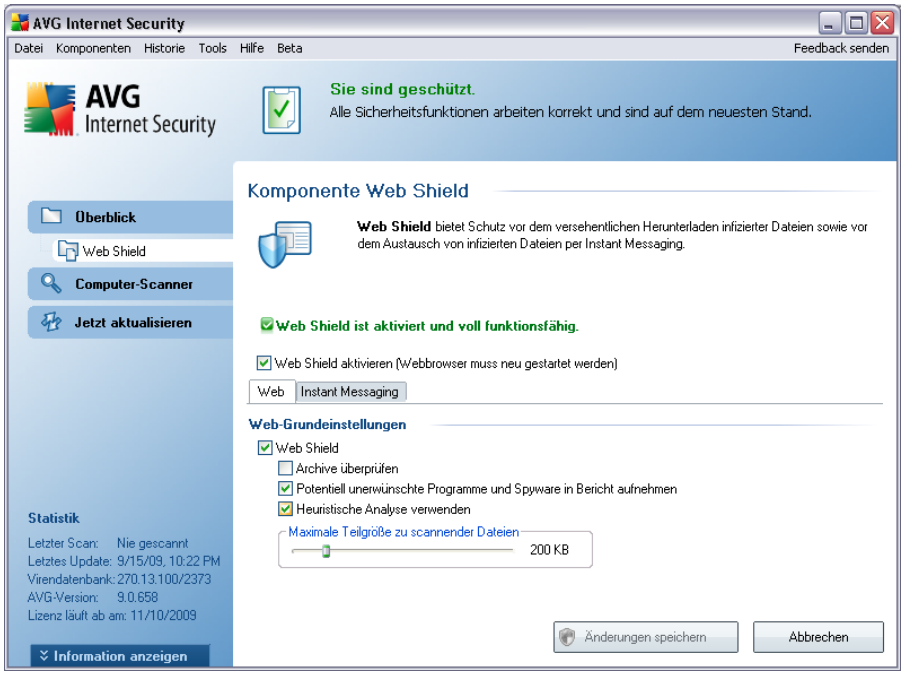
8.11.2. Benutzeroberfläche des Web Shield

Auf der Oberfläche der Komponente ***Web Shield*** wird das Verhalten dieses Schutzmechanismus beschrieben. Zudem enthält sie Informationen zum aktuellen Status der Komponente (*Web Shield ist aktiviert und voll funktionsfähig.*). Im unteren Bereich des Dialogs werden grundlegende Optionen zur Bearbeitung der Funktionsweise der Komponente angezeigt.

Basiskonfiguration der Komponente

Zunächst haben Sie die Möglichkeit, ***Web Shield*** jederzeit ein- und auszuschalten, indem Sie die Option ***Web Shield aktivieren*** markieren. Standardmäßig ist die Option aktiviert, und die Komponente ***Web Shield*** ist aktiv. Es wird empfohlen, diese Einstellung beizubehalten, sofern Sie keinen wichtigen Grund haben, die Komponente zu deaktivieren. Wenn die Option aktiviert ist und ***Web Shield*** ausgeführt wird, stehen auf zwei Reitern weitere Konfigurationsoptionen zur Verfügung:

- ***Web*** – Sie können die Konfiguration der Komponente hinsichtlich der Prüfung von Website-Inhalten bearbeiten. Auf der Bearbeitungsoberfläche können Sie die folgenden grundlegenden Optionen konfigurieren:

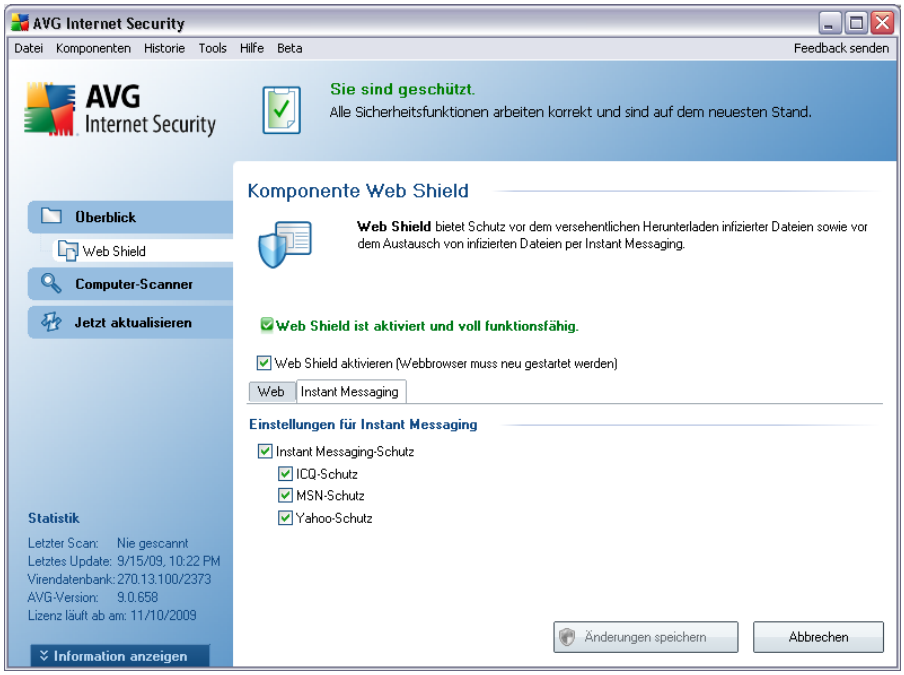


o ***Web-Schutz*** – Diese Option bestätigt, dass ***Web-Schutz*** Inhalte von Internetseiten scannen soll. Wenn diese Option aktiviert ist (*standardmäßig aktiviert*), können Sie darüber hinaus folgende Elemente aktivieren/deaktivieren:

- ***Archive überprüfen*** – Archivinhalte, die möglicherweise auf einer angezeigten Webseite enthalten sind, werden ebenfalls gescannt
- ***„Potentiell unerwünschte Programme" in Bericht aufnehmen*** – Scannen Sie potentiell unerwünschte Programme (*ausführbare Programme, die möglicherweise Spyware oder Adware sind*), die in Internetseiten integriert sind
- ***Heuristische Analyse verwenden***– Der Inhalt der angezeigten Webseite wird mit Hilfe der Methode heuristische Analyse gescannt *(dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung – siehe Kapitel Grundlagen zu Anti-Virus*)
- ***Maximale Größe zu scannender Dateien*** – Wenn die angezeigte Webseite Dateien enthält, können Sie deren Inhalte scannen, noch bevor diese auf Ihren Computer heruntergeladen werden. Das Scannen großer Dateien kann jedoch einige Zeit in Anspruch nehmen

und das Herunterladen der Webseite ist signifikant langsamer. Mit Hilfe des Schiebereglers können Sie die maximale Größe einer Datei festlegen, die noch mit ***Web Shield*** gescannt werden soll. Selbst wenn die heruntergeladene Datei größer als festgelegt ist und daher nicht mit ***Web Shield*** gescannt wird, sind Sie weiterhin geschützt: Sollte die Datei infiziert sein, wird dies vom ***Residenten Schutz*** sofort erkannt.

- ***Instant Messaging*** – Hier können Sie die Einstellungen der Komponente hinsichtlich des Scans von Instant Messaging (*z. B. ICQ, MSN Messenger, Yahoo ...*) bearbeiten.



  - Instant Messaging-Schutz – Aktivieren Sie diese Option, wenn Web Shield die Online-Kommunikation auf Viren prüfen soll. Wenn diese Option aktiviert ist, können Sie zusätzlich angeben, welche Instant Messaging-Anwendung kontrolliert werden soll – derzeit unterstützt **AVG 9 Internet Security** die Anwendungen ICQ, MSN und Yahoo.

Hinweis: Alle *Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü*

die Option ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

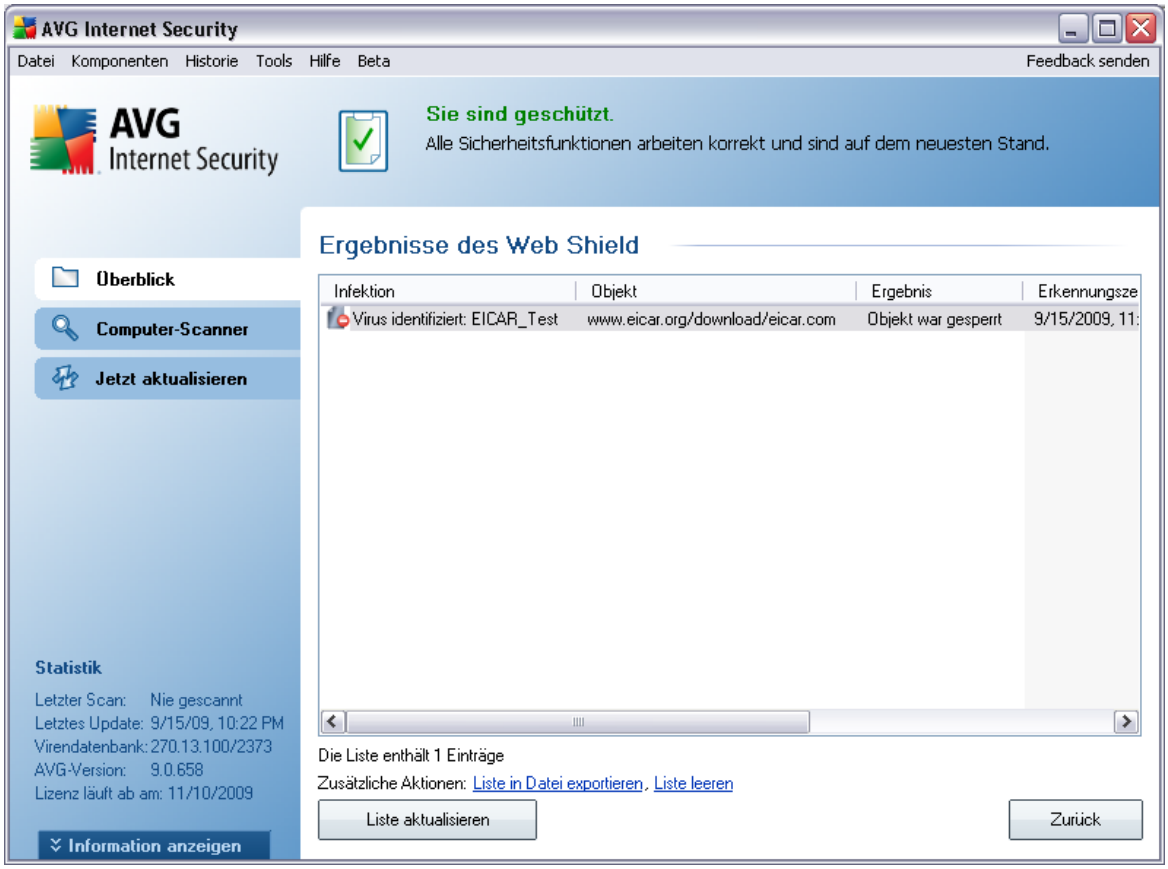
Auf der Oberfläche von ***Web Shield*** stehen folgende Schaltflächen zur Verfügung:

- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückkehren

8.11.3. Erkennung durch Web Shield

Web Shield scannt den Inhalt besuchter Webseiten und möglicher enthaltener Dateien, noch bevor dieser in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen wird. Wenn eine Bedrohung erkannt wird, werden Sie unmittelbar mit folgendem Dialog gewarnt:

Die verdächtige Webseite wird nicht geöffnet, und die erkannte Bedrohung wird in die Liste der ***Funde von Web Shield*** eingetragen – Diese Übersicht der entdeckten Bedrohungen können Sie im Systemmenü unter ***Verlauf/Funde von Web Shield*** aufrufen.



Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Infektion*** – Beschreibung (*nach Möglichkeit auch Name*) des erkannten Objekts
- ***Objekt*** – Quelle des Objekts (*Webseite*)
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Zeitpunkt (Datum und Uhrzeit), zu dem die Bedrohung entdeckt und blockiert wurde
- ***Objekttyp*** - Typ des erkannten Objekts
- ***Vorgang*** - Ausgeführte Aktion, mit der das potentiell gefährliche Objekt aufgerufen wurde, so dass es erkannt werden konnte

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei exportieren***) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***). Die Schaltfläche ***Liste aktualisieren*** aktualisiert die Liste der von ***Web Shield*** erkannten Funde. Mit der Schaltfläche ***Zurück*** können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren.

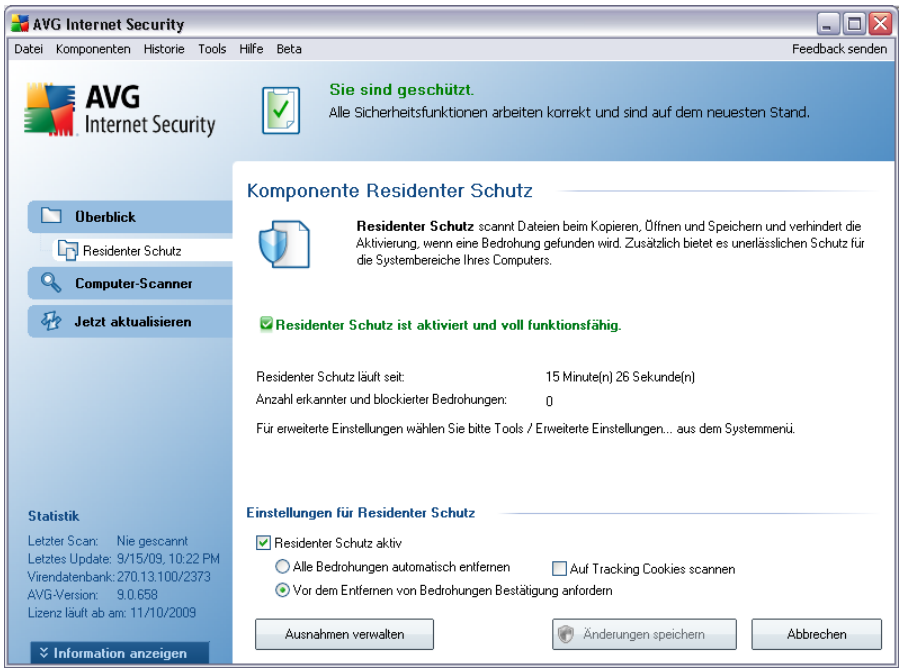
8.12. Residenter Schutz

8.12.1. Residenter Schutz Grundlagen

Die Komponente ***Residenter Schutz*** gewährt Ihrem Computer dauerhaften Schutz. Sie scannt jede einzelne Datei, die geöffnet, gespeichert oder kopiert wird und überwacht die Systembereiche Ihres Computers. Wenn der ***Residente Schutz*** in einer Datei, auf die zugegriffen wird, ein Virus entdeckt, stoppt die Komponente den aktuell ausgeführten Vorgang und gestattet es dem Virus nicht, sich zu aktivieren. Normalerweise nehmen Sie diesen Vorgang nicht wahr, da er „im Hintergrund" abläuft und Sie nur informiert werden, wenn Bedrohungen gefunden werden; gleichzeitig blockiert der ***Residente Schutz*** die Aktivierung der Bedrohung und entfernt sie. Der ***Residente Schutz*** wird beim Systemstart in den Speicher Ihres Computers geladen.

Warnung: Der Residente Schutz wird beim Systemstart in den Speicher Ihres Computers geladen. Sie sollten den Schutz in keinem Fall deaktivieren!

8.12.2. Benutzeroberfläche des Residenten Schutzes



Neben einer Übersicht über die wichtigsten statistischen Daten und Informationen über den aktuellen Status der Komponente (*Residenter Schutz ist aktiviert und voll funktionsfähig*) enthält die Oberfläche des ***Residenten Schutzes*** einige grundlegende Komponenteneinstellungen. Folgende statistische Daten werden angezeigt:

- ***Residenter Schutz läuft seit*** - Abgelaufene Zeit seit dem letzten Start der Komponenten
- ***Anzahl erkannter und blockierter Bedrohungen*** - Anzahl der erkannten Infektionen, deren Ausführung verhindert wurde (*bei Bedarf kann dieser Wert zurückgesetzt werden, z. B. zu Statistikzwecken – Wert zurücksetzen*)

Basiskonfiguration der Komponente

Im unteren Teil des Dialogs befindet sich der Bereich ***Einstellungen für Residenter Schutz*** , in dem Sie einige Basiseinstellungen für die Funktionsweise der Komponente bearbeiten können (*eine detaillierte Konfiguration ist, wie bei allen anderen Komponenten, über die Option „Tools"/„Erweiterte Einstellungen" des Systemmenüs möglich*).

Über die Option ***Residenter Schutz aktiv*** können Sie den Residenten Schutz einfach ein- und ausschalten. Standardmäßig ist die Funktion aktiviert. Mit dem Residenten Schutz können Sie zudem festlegen, wie erkannte Infektionen behandelt (entfernt) werden sollen:

- entweder automatisch (***Alle Bedrohungen automatisch entfernen***)
- oder erst nach Bestätigung durch den Benutzer (***Vor dem Entfernen von Bedrohungen Bestätigung anfordern***)

Diese Auswahl hat keinen Einfluss auf die Sicherheitsstufe und kann beliebig festgelegt werden.

In beiden Fällen haben Sie die Wahl, ***Cookies automatisch zu entfernen.*** In bestimmten Fällen kann es sinnvoll sein, diese Option zu aktivieren, um maximale Sicherheit zu erzielen, sie ist jedoch standardmäßig deaktiviert. (*Cookies = Textpakete, die von einem Server an einen Webbrowser gesendet und dann bei jedem Zugriff des Browsers auf diesen Server unverändert vom Browser zurückgesendet werden. HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

Hinweis: Alle *Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option* ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

Auf der Oberfläche des ***Residenten Schutzes*** stehen folgende Schaltflächen zur Verfügung:

- ***Ausnahmen verwalten*** - öffnet den Dialog ***Residenter Schutz – Verzeichnis-Ausnahmen***, wo Sie Ordner festlegen können, die vom ***Residenten Schutz*** nicht durchsucht werden sollen.
- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie in diesem Dialog durchgeführt haben, zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren

8.12.3. Erkennungen durch den Residenten Schutz

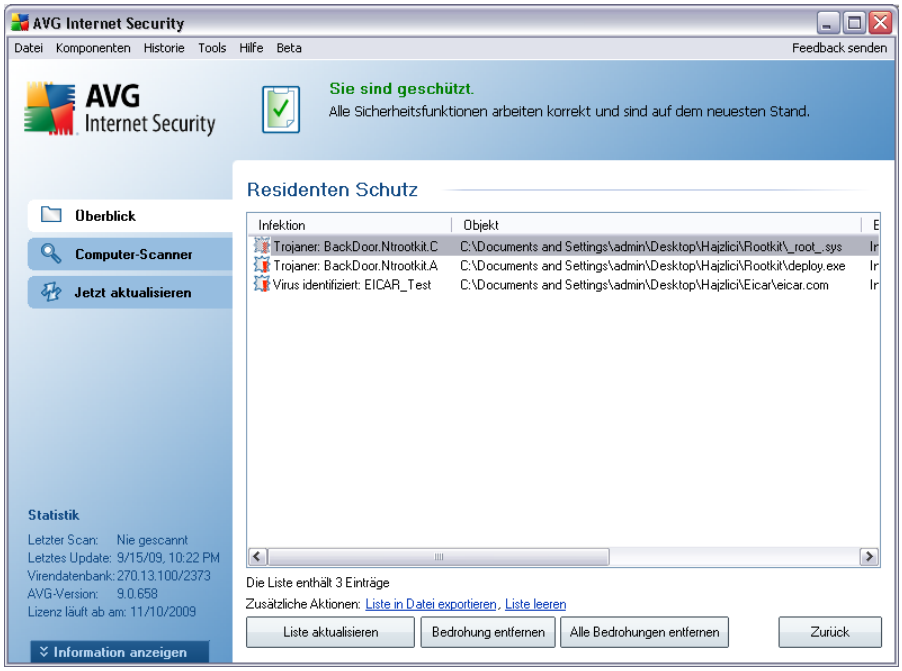
Residenter Schutz scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden. Wenn ein Virus oder eine andere Bedrohung erkannt wird, werden Sie unmittelbar mit folgendem Dialog gewarnt:

Der Dialog enthält Informationen über die erkannte Bedrohung und fordert Sie auf, zu entscheiden, welche Aktion jetzt durchgeführt werden soll:

- ***Heilen*** – Wenn eine Gegenmaßnahme verfügbar ist, heilt AVG die infizierte Datei automatisch. Diese Option ist die empfohlene Aktion
- ***In Quarantäne verschieben*** – Der Virus wird in die AVG-***Virenquarantäne verschoben***

- ***Gehe zu Datei*** – Mit dieser Option werden Sie zum genauen Speicherort des verdächtigen Objekts weitergeleitet (*öffnet ein neues Fenster von Windows Explorer*)
- ***Ignorieren*** – Es wird dringend empfohlen, diese Option NICHT zu verwenden, wenn Sie keinen wirklich guten Grund dazu haben!

Die Gesamtübersicht aller vom ***Residenten Schutz*** gefundenen Bedrohungen kann im Dialog ***Erkennung durch den Residenten Schutz*** aufgerufen werden, und zwar im Systemmenü unter der Option ***Verlauf/Ergebnisse des Residenten Schutzes*** :



Der Bereich ***Residenten Schutz*** enthält eine Übersicht über Objekte, die durch den ***Residenten Schutz*** erkannt, als gefährlich bewertet und entweder geheilt oder in die ***Virenquarantäne*** verschoben wurden. Zu jedem erkannten Objekt werden die folgenden Informationen angegeben:

- ***Infektion*** - Beschreibung (nach Möglichkeit auch Name) des erkannten Objekts
- ***Objekt*** - Speicherort des Objekts
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Der Zeitpunkt (Datum und Uhrzeit), zu dem das verdächtige Objekt entdeckt wurde
- ***Objekttyp*** - Typ des erkannten Objekts
- ***Vorgang*** - Ausgeführte Aktion, mit der das potentiell gefährliche Objekt aufgerufen wurde, so dass es erkannt werden konnte

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei***

exportieren) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***). Die Schaltfläche ***Liste aktualisieren*** aktualisiert die Liste der vom ***Residenten Schutz*** erkannten Funde. Mit der Schaltfläche ***Zurück*** können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren.

8.13. Updatemanager

Keine Sicherheits-Software kann einen wirksamen Schutz gegen verschiedene Bedrohungen bieten, wenn sie nicht regelmäßig aktualisiert wird! Verfasser von Viren suchen stets nach neuen Lücken in Software und Betriebssystemen, die sie ausnutzen können. Jeden Tage gibt es neue Viren, neue Malware und neue Hacker-Angriffe. Software-Hersteller geben daher ständig neue Updates und Sicherheits-Patches heraus, mit denen entdeckte Sicherheitslücken geschlossen werden sollen.

Es ist entscheidend, dass Sie AVG regelmäßig aktualisieren!

Der ***Updatemanager*** hilft Ihnen dabei, regelmäßige Aktualisierungen zu steuern. In dieser Komponente können Sie das automatische Herunterladen von Aktualisierungsdateien aus dem Internet oder Ihrem lokalen Netzwerk planen. Wenn möglich, sollten Virendefinitionen täglich aktualisiert werden. Weniger dringende Programmupdates können wöchentlich gestartet werden.

Hinweis: *Im Kapitel AVG Updates finden Sie weitere Informationen zu Aktualisierungsstufen und -arten!*

AVG Download-Manager ist ein einfaches Tool, mit dem Sie AVG Home Security-Produkte bequem herunterladen können. Basierend auf Ihrer Auswahl definiert der Download-Manager die Konfiguration entsprechend dem Produkt, dem Lizenztyp und der Sprache. Der Vorteil dieses Tools besteht darin, dass Sie damit Produkte von AVG Ihren Bedingungen entsprechend herunterladen können. Außerdem wird immer die neueste Installationsdatei heruntergeladen, so dass das AVG-Programm nach der Installation auf dem neuesten Stand ist.

AVG Download-Manager

- Laden Sie stets die neueste Installationsdatei herunter;
- Reduziert die Größe der heruntergeladenen Datei;
- Unterstützt die Wiederaufnahme eines Downloads, wenn der Download aus irgendeinem Grund fehlgeschlagen ist;
- Funktioniert bei allen AVG Home-Editionen

Hinweis: *Bitte beachten Sie, dass AVG Download-Manager nicht für die Editionen Netzwerk und SBS heruntergeladen werden kann, da nur die folgenden Betriebssysteme unterstützt werden: Windows 2000 (SP4 + SRP Rollup), Windows XP (SP2 und höher), Windows Vista (alle Editionen).*

8.13.1. Grundlagen zum Updatemanager

AVG Download-Manager funktioniert wie folgt:

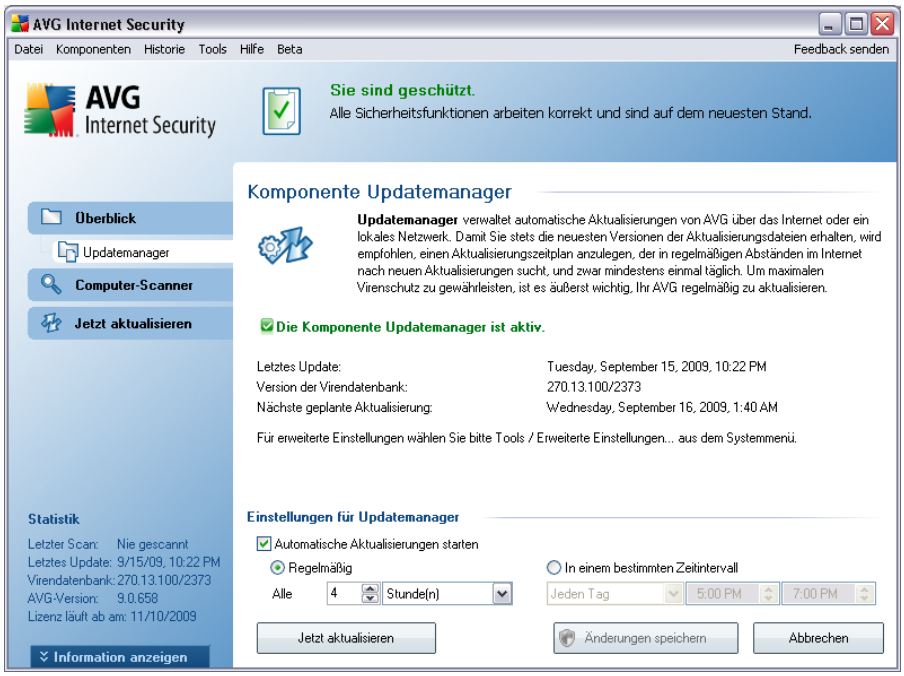
- Im ersten Schritt müssen Sie die Anwendung ***AVG Download-Manager*** herunterladen. Nach dem Start fragt Sie ***AVG Download-Manager*** , in welcher Sprache die Installation durchgeführt werden soll.

- Danach versucht ***AVG Download-Manager***, eine Verbindung mit dem Internet aufzubauen und einen Konnektivitätstest durchzuführen. Wenn die Verbindung erfolgreich war, können Sie auswählen, welche Programmversion von AVG Sie installieren möchten (*Vollversion, Testversion oder Free Edition*).

- Sobald Sie die Programmversion von AVG ausgewählt haben, werden Sie aufgefordert, ein Produkt auszuwählen, das Sie installieren möchten.

- Abschließend werden alle erforderlichen Installationsdateien heruntergeladen. ***AVG Download-Manager*** wird geschlossen, und die Installation von AVG wird gestartet.

8.13.2. Benutzeroberfläche des Updatemanagers



Auf der Oberfläche des ***Updatemanager*** werden Informationen zur Funktion der Komponente und zu ihrem aktuellen Status (*Updatemanager ist aktiv.*) sowie wichtige statistische Daten angezeigt:

- ***Letztes Update*** – Hier werden Datum und Uhrzeit der Datenbankaktualisierung angegeben
- ***Version der Virendatenbank*** – Hier wird die Versionsnummer der aktuellsten Virendatenbank angegeben; diese Nummer wird bei jeder Aktualisierung der Virendatenbank erhöht
- ***Nächstes geplantes Update*** – Gibt an, wann die Datenbank laut Zeitplan erneut aktualisiert werden soll

Basiskonfiguration der Komponente

Im unteren Teil des Dialogs finden Sie den Bereich ***Einstellungen für Updatemanager***, in dem Sie einige Regeln des Aktualisierungsstarts ändern können. Sie können festlegen, ob die Aktualisierungsdateien automatisch (***Automatische Aktualisierungen starten***) oder On-Demand heruntergeladen werden sollen.

Standardmäßig ist die Option ***Automatische Aktualisierungen starten*** aktiviert, und wir empfehlen, dies auch so zu belassen! Das regelmäßige Herunterladen der aktuellsten Updatedateien ist entscheidend für das Funktionieren jeder Sicherheits-Software!

Sie können weiter festlegen, wann das Update gestartet werden soll:

- ***Regelmäßig*** – Hier können Sie das Zeitintervall festlegen
- ***In einem bestimmten Zeitintervall*** – Hier werden das exakte Datum und die exakte Uhrzeit festgelegt

Standardmäßig ist das Update auf alle 4 Stunden eingestellt. Wenn Sie keinen wichtigen Grund haben, dies zu ändern, sollten Sie diese Einstellung beibehalten!

Hinweis: Alle *Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü die Option* ***Tools / Erweiterte Einstellungen****, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

Auf der Oberfläche des ***Updatemanager*** stehen folgende Schaltflächen zur Verfügung:

- ***Jetzt aktualisieren*** – Hiermit wird das Update unmittelbar, On-Demand gestartet
- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (Komponentenübersicht) zurückkehren

8.14. AVG Security Toolbar

Die AVG Security Toolbar ist ein neues Tool, das mit dem ***Link Scanner*** zusammenarbeitet und Suchergebnisse der unterstützten Suchmaschinen im Internet (*Yahoo!, Google, MSN, Baidu*) überprüft.

Wenn Sie sich bei der Installation von **AVG 9 Internet Security** für eine Installation der Toolbar entscheiden, wird sie automatisch in Ihren Webbrowser integriert.

Die AVG Security Toolbarkönnen Sie zur Verwaltung von Funktionen im ***Link Scanner*** und zur Anpassung seines Verhaltens sowie zur Aktualisierung von **AVG 9 Internet Security** verwenden, wenn neue Updates zur Verfügung stehen.

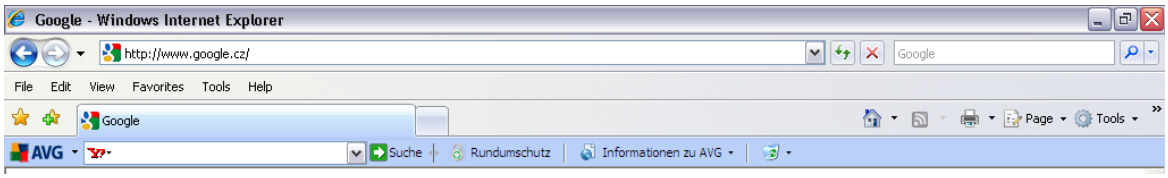
Hinweis: *Wenn Sie einen alternativen Browser verwenden (zum Beispiel Avant), kann unerwartetes Verhalten auftreten.*

8.14.1. AVG Security Toolbar Schnittstelle

Die ***AVG Security Toolbar*** ist für die Arbeit mit ***MS Internet Explorer*** (*Version 6.0 oder höher*) und ***Mozilla Firefox*** (*Version 1.5 oder höher*) ausgelegt.

Hinweis: *Die AVG Security Toolbar ist nicht für Serverplattformen vorgesehen!*

Nachdem Sie sich entschieden haben, die ***AVG Security Toolbar*** zu installieren (*während der Installation von AVG wurden Sie gefragt, ob Sie die Komponente installieren möchten oder nicht*), wird die Komponente in Ihrem Webbrowser unterhalb der Adresszeile angezeigt:



Die ***AVG Security Toolbar*** enthält die folgenden Elemente:

- ***Die Schaltfläche mit dem AVG-Logo*** – bietet Zugang zu allgemeinen Funktionen der Toolbar. Wenn Sie auf die Schaltfläche mit dem Logo klicken, werden Sie auf die Website von AVG (http://www.avg.com/) weitergeleitet. Wenn Sie neben das AVG-Symbol klicken, wird eines der folgenden Elemente geöffnet:
    - ***Toolbar Info*** – Link zur Homepage der ***AVG Security Toolbar*** mit ausführlichen Informationen, wie die Toolbar zu Ihrem Schutz beiträgt.
    - ***AVG 9.0 starten*** – Öffnet die Benutzeroberfläche von AVG
    - ***Optionen*** – Öffnet einen Konfigurationsdialog, in dem Sie die Einstellungen der ***AVG Security Toolbar*** an Ihre Anforderungen anpassen können – siehe folgendes Kapitel ***Optionen der AVG***

Security Toolbar

- ***Verlauf löschen*** – Mit dieser Option können Sie in der AVG Security Toolbar den *Gesamten Verlauf löschen* oder den *Suchverlauf löschen, Browserverlauf löschen, Download-Verlauf löschen* und *Cookies löschen*.

- ***Aktualisieren*** – überprüft, ob neue Updates für Ihre ***AVG Security Toolbar vorhanden sind***

- ***Hilfe*** – bietet Optionen zum Öffnen der Hilfedatei, zum Kontaktieren des ***technischen Supports von AVG*** oder zum Anzeigen der aktuellen Version Ihres Toolbar-

- ***Yahoo! Suchfeldes*** – ein bequemer und sicherer Weg, um das Internet mit Yahoo! zu durchsuchen. Geben Sie in das Suchfeld ein Wort oder eine Wortgruppe ein, und klicken Sie auf ***Suchen***, um die Suche direkt auf dem Yahoo!- Server zu starten, unabhängig davon, welche Seite gerade angezeigt wird. Im Suchfeld wird auch Ihr Suchverlauf angezeigt. Suchen, die Sie über das Suchfeld durchführen, werden mit AVG Search-Shield ***geprüft.***

- ***Schaltfläche „AVG Active Surf-Shield"*** – Mit dieser Ein-/Aus-Schaltfläche können Sie den Schutzstatus von ***AVG Active Surf-Shield*** überprüfen.

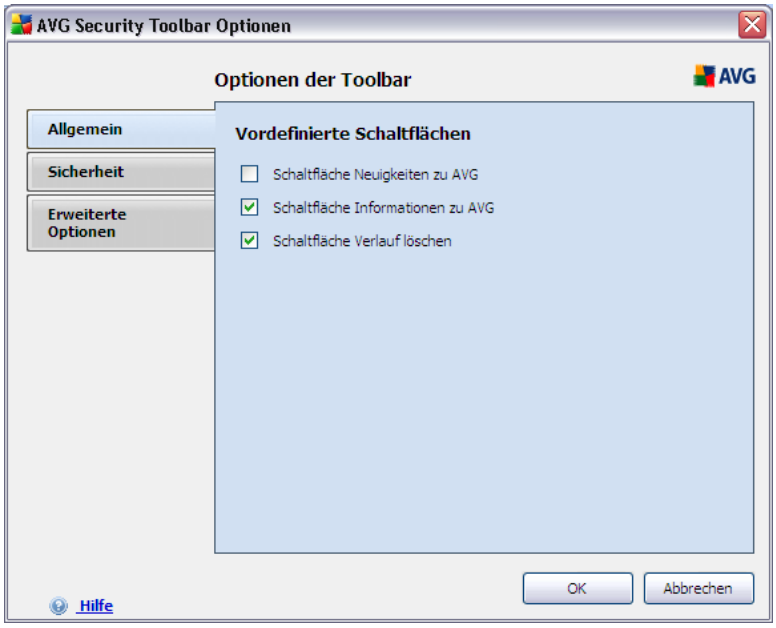
- ***Schaltfläche „AVG Search-Shield"*** – Mit dieser Ein-/Aus-Schaltfläche können Sie den Schutzstatus von ***AVG Search-Shield*** überprüfen.

- ***Schaltfläche „AVG Info"*** – Umfasst Links zu wichtigen Sicherheitsinformationen auf der Website von AVG (http://www.avg.com/).

8.14.2. Optionen der AVG Security Toolbar

Alle Parameter der ***AVG Security Toolbar*** können Sie direkt im Bereich ***AVG Security Toolbar*** konfigurieren. Mit dem Menüeintrag *AVG/Optionen* der Toolbar wird die Bearbeitungsoberfläche in einem Dialog namens ***Optionen der Toolbar*** geöffnet, der aus drei Bereichen besteht:

- ***Allgemein***



Auf diesem Reiter können Sie die Schaltfläche festlegen, die im Bereich ***AVG Security Toolbar*** angezeigt bzw. ausgeblendet werden soll:

- ***Schaltfläche „AVG Neuigkeiten"*** – Mit dieser Option wird die Schaltfläche ***AVG Neuigkeiten*** angezeigt. Wenn Sie auf die Schaltfläche im Bereich ***AVG Security Toolbar*** klicken, wird ein Dropdown-Menü geöffnet, das Links zu aktuellen Pressemitteilungen über AVG enthält.

- ***Schaltfläche „AVG Info"*** – Mit der Schaltfläche ***AVG Info*** lässt sich ein Menü mit den folgenden Optionen öffnen:

  - *Toolbar-Info* – Öffnet die Produktseite der ***AVG Security Toolbar*** mit detaillierten Informationen über die Komponente

  - *Infos zu Bedrohungen* – Öffnet die Website des Virenlabors von AVG mit Informationen über aktuelle Bedrohungen, Empfehlungen zur Entfernung von Viren, einer FAQ-Liste usw.

  - *AVG Neuigkeiten* – Öffnet die Webseite mit den neuesten Pressemitteilungen über AVG

  - *Aktuelle Bedrohungsstufe* – Öffnet die Webseite des Virenlabors mit einer grafischen Darstellung der aktuellen Bedrohungslage im Internet

- *Virenenzyklopädie* – Öffnet die Seite mit der Virenenzyklopädie, auf der Sie einzelne Viren per Namen suchen und detaillierte Informationen abrufen können

o ***Schaltfläche „Verlauf löschen"*** – Mit dieser Schaltfläche können Sie den *Gesamten Verlauf löschen*oder den *Suchverlauf löschen, Browserverlauf löschen, Download-Verlauf löschen* oder *Cookies löschen* – und zwar direkt über den Bereich ***AVG Security Toolbar***.

- ***Sicherheit***

Der Reiter ***Sicherheit*** besteht aus zwei Bereichen, ***AVG Browser Security*** und ***Bewertungen***, in denen Sie einzelne Kontrollkästchen aktivieren können, um Funktionen der ***AVG Security Toolbar*** zuzuweisen, die Sie verwenden möchten:

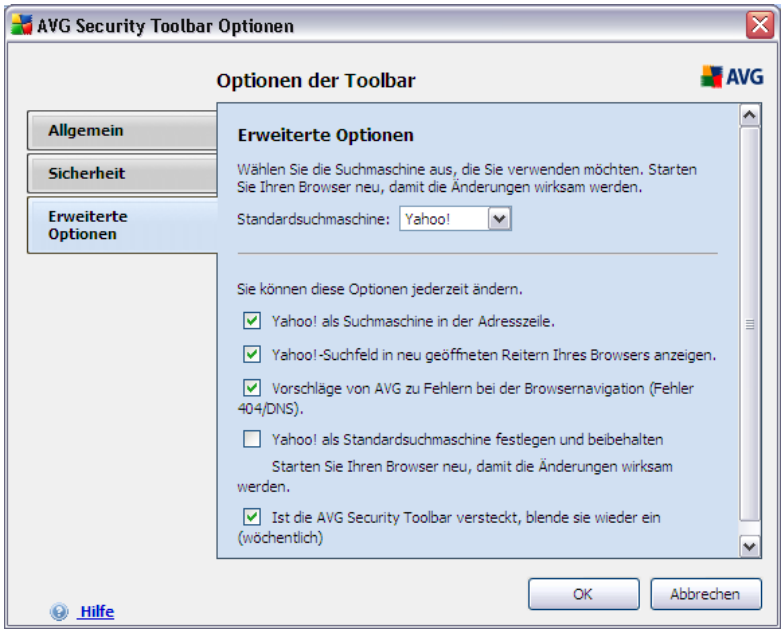
o ***AVG Browser Security*** – Aktivieren Sie diesen Eintrag, um das ***AVG Search-Shield*** und/oder ***AVG Active Surf-Shield*** zu aktivieren oder zu deaktivieren

o ***Bewertungen*** – Wählen Sie die gewünschten grafischen Symbole aus, die von der Komponente ***AVG Search-Shield*** zur Bewertung von Suchergebnissen verwendet werden sollen:

- Die Seite ist sicher
- Die Seite ist leicht verdächtig
- Die Seite umfasst Links zu wirklich gefährlichen Seiten
- Die Seite enthält aktive Bedrohungen
- Auf die Seite kann nicht zugegriffen werden. Darum konnte sie nicht gescannt werden

Markieren Sie die gewünschte Option, um zu bestätigen, dass Sie über diese Bedrohungsstufe informiert werden möchten. Die Anzeige der roten Markierung, die für Seiten mit aktiven und gefährlichen Bedrohungen steht, lässt sich nicht deaktivieren. ***Auch hier empfehlen wir, die Standardkonfiguration des Programmherstellers beizubehalten, solange Sie nicht einen guten Grund für eine Änderung haben.***

- ***Erweiterte Optionen***



Auf dem Reiter ***Erweiterte Optionen*** können Sie weitere spezifische Einstellungen der ***AVG Security Toolbar*** aktivieren oder deaktivieren:

- ***Yahoo! als Suchanbieter für die Adressleiste*** – (*standardmäßig aktiviert*) – Wenn diese Option aktiviert ist, können Sie Suchbegriffe direkt in die Adresszeile Ihres Browsers eingeben und Yahoo! sucht automatisch nach relevanten Websites.

- ***Yahoo!-Suchfeld Suchfeld in neuen Reitern des Browsers*** – (*standardmäßig aktiviert*) – Wenn diese Option aktiviert ist, wird das Suchfeld von Yahoo! in jedem neu geöffneten Reiter des Internetbrowsers angezeigt.

- ***Vorschläge von AVG zu Fehlern bei der Browsernavigation (Fehler 404/DNS)*** – (*standardmäßig aktiviert*) – Wenn Sie bei der Suche im Internet auf eine nicht vorhandene Seite bzw. eine Seite stoßen, die nicht angezeigt werden kann (*Fehler 404*), zeigt die ***AVG Security Toolbar*** automatisch eine Übersicht mit ähnlichen Seiten zum gesuchten Thema an.

- ***Yahoo! als Suchmaschine Ihres Browsers festlegen und beibehalten*** – (*standardmäßig deaktiviert*) – Yahoo! ist die Standardsuchmaschine für die Suche im Internet mit der ***AVG Security Toolbar***; durch die Aktivierung dieser Option wird diese Suchmaschine auch als Standardsuchmaschine Ihres Webbrowsers verwendet.

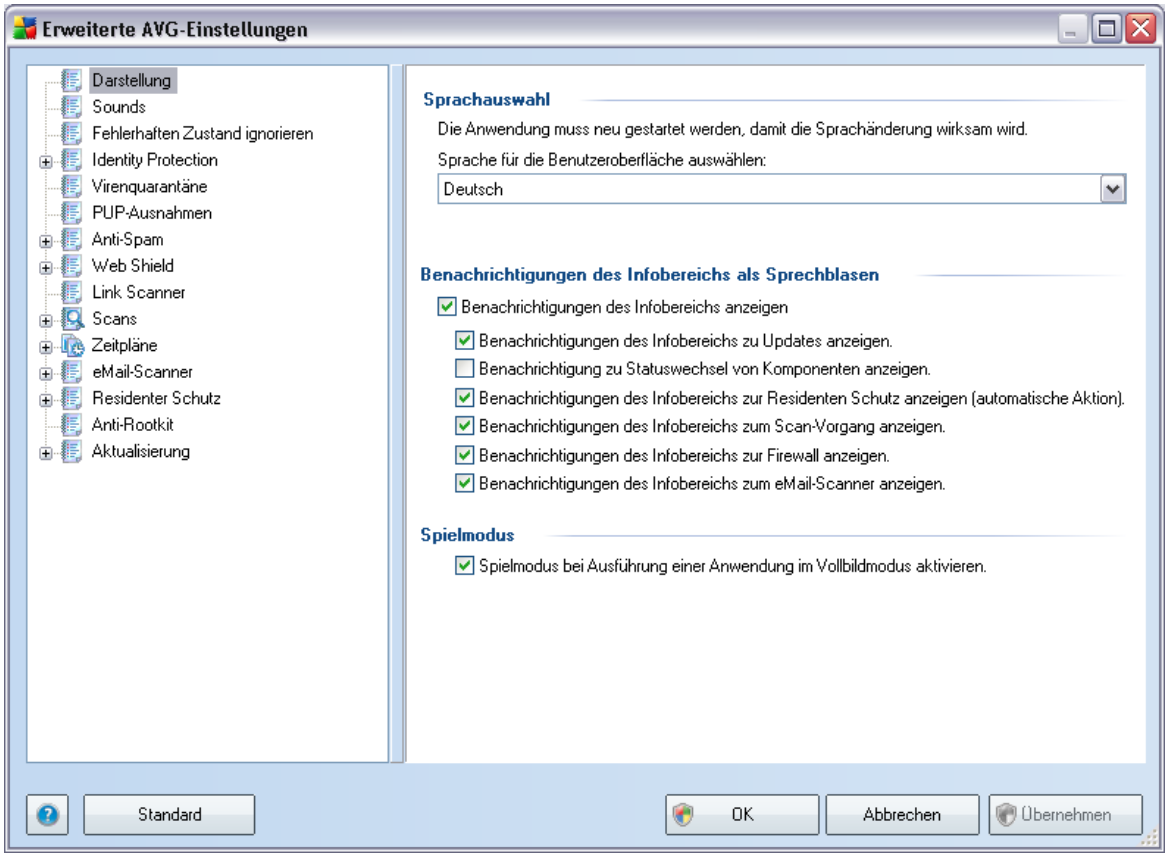
- ***AVG Security Toolbar wieder einblenden, wenn sie ausgeblendet ist (wöchentlich)*** – (*standardmäßig aktiviert*) – Diese Option ist standardmäßig aktiviert; wenn Sie Ihre ***AVG Security Toolbar*** aus Versehen ausblenden, wird sie nach einer Woche wieder eingeblendet.

9. Erweiterte Einstellungen von AVG

Der Dialog für die erweiterte Konfiguration von **AVG 9 Internet Security** wird in einem neuen Fenster mit der Bezeichnung ***Erweiterte AVG-Einstellungen*** geöffnet. Das Fenster ist in zwei Bereiche unterteilt: Der linke Bereich enthält eine Baumstruktur zur Navigation durch die Konfigurationsoptionen. Wählen Sie die Komponente (*oder den Teil einer Komponente*) aus, deren Konfiguration Sie ändern möchten, um den entsprechenden Bearbeitungsdialog im rechten Bereich des Fensters zu öffnen.

9.1. Darstellung

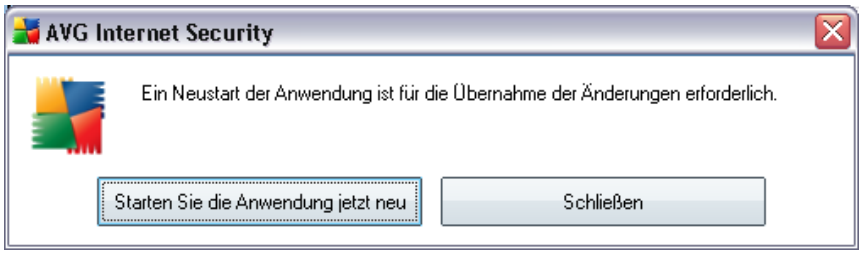
Der erste Eintrag der Baumstruktur, ***Darstellung***, bezieht sich auf die allgemeinen Einstellungen der Benutzeroberfläche von AVG und auf einige grundlegende Optionen für das Verhalten der Anwendung:



Sprachauswahl

Im Bereich ***Sprachauswahl*** kann aus dem Dropdown-Menü die gewünschte Sprache ausgewählt werden. Diese Sprache wird dann für die gesamte Benutzeroberfläche von AVG verwendet. Das Dropdown-Menü enthält nur die Sprachen, die Sie zuvor während des Installationsvorgangs zur Installation ausgewählt haben (siehe Kapitel Benutzerdefinierte Installation – Komponentenauswahl). Um den Wechsel zur ausgewählten Sprache abzuschließen, müssen Sie die Benutzeroberfläche wie folgt neu starten:

- Wählen Sie die gewünschte Sprache aus, und bestätigen Sie Ihre Auswahl mit der Schaltfläche ***Übernehmen*** (rechte untere Ecke)
- Klicken Sie zum Bestätigen auf die Schaltfläche ***OK***
- Es wird ein Dialog angezeigt, in dem Sie darüber informiert werden, dass nach einer Sprachänderung der Benutzeroberfläche von AVG ein Neustart der Anwendung erforderlich ist:



Benachrichtigungen des Infobereichs als Sprechblasen

In diesem Bereich können Sie die Anzeige von Benachrichtigungen des Infobereichs als Sprechblasen über den Status der Anwendung deaktivieren. Standardmäßig wird die Anzeige dieser Sprechblasen zugelassen, und es wird empfohlen, diese Konfiguration beizubehalten! Die Benachrichtigungen in den Sprechblasen enthalten meist Informationen über Statusänderungen der einzelnen Komponenten von AVG und sollten daher beachtet werden!

Wenn Sie dennoch möchten, dass diese Benachrichtigungen nicht angezeigt werden oder dass nur bestimmte Benachrichtigungen (zu einer bestimmten Komponente von AVG) angezeigt werden, können Sie dies durch Aktivierung/Deaktivierung der folgenden Optionen festlegen:

- ***Benachrichtigungen des Infobereichs anzeigen*** – Diese Option ist standardmäßig (*aktiviert*), so dass die Benachrichtigungen angezeigt werden. Wenn Sie die Markierung dieser Option aufheben, wird die Anzeige von Benachrichtigungen in Sprechblasen vollständig deaktiviert. Wenn diese Funktion aktiviert ist, können Sie auswählen, welche Benachrichtigungen angezeigt werden sollen:

    - ***Benachrichtigungen des Infobereichs zu Updates*** anzeigen – Legen Sie fest, ob Informationen zum Start, Fortschritt und Abschluss des Aktualisierungsvorgangs von AVG angezeigt werden sollen;

    - ***Benachrichtigungen zum Statuswechsel von Komponenten anzeigen*** – Legen Sie fest, ob Informationen zur Aktivität/Inaktivität der Komponenten angezeigt werden sollen und ob Sie über auftretende Probleme informiert werden möchten. Die Option zur Benachrichtigung über den fehlerhaften Status einer Komponente entspricht der Informationsfunktion des Infobereichsymbols, das (durch einen Farbwechsel) auf Probleme aufmerksam macht, die im Zusammenhang mit AVG-Komponenten auftreten;

    - ***Benachrichtigungen des Infobereichs zum Residenten Schutz anzeigen*** – Legen Sie fest, ob Informationen zum Speichern, Kopieren und Öffnen von Dateien angezeigt werden sollen;

    - ***Benachrichtigungen des Infobereichs zum Scan-Vorgang*** anzeigen – Legen Sie fest, ob Informationen zum automatischen Start, Fortschritt und Abschluss des geplanten Scan-Vorgangs angezeigt werden sollen;

    - ***Benachrichtigungen des Infobereichs zur Firewallanzeigen –*** Legen Sie fest, ob Informationen zum Status und zu Prozessen der Firewall (z. B. Warnmeldungen bezüglich der Aktivierung/Deaktivierung der Komponente, eine mögliche Blockierung des Datenverkehrs usw.) angezeigt werden sollen;

    - ***Benachrichtigungen des Infobereichs zum eMail-Scanner anzeigen*** – Legen Sie fest, ob Informationen zur Überprüfung aller eingehenden und ausgehenden eMails angezeigt werden sollen.

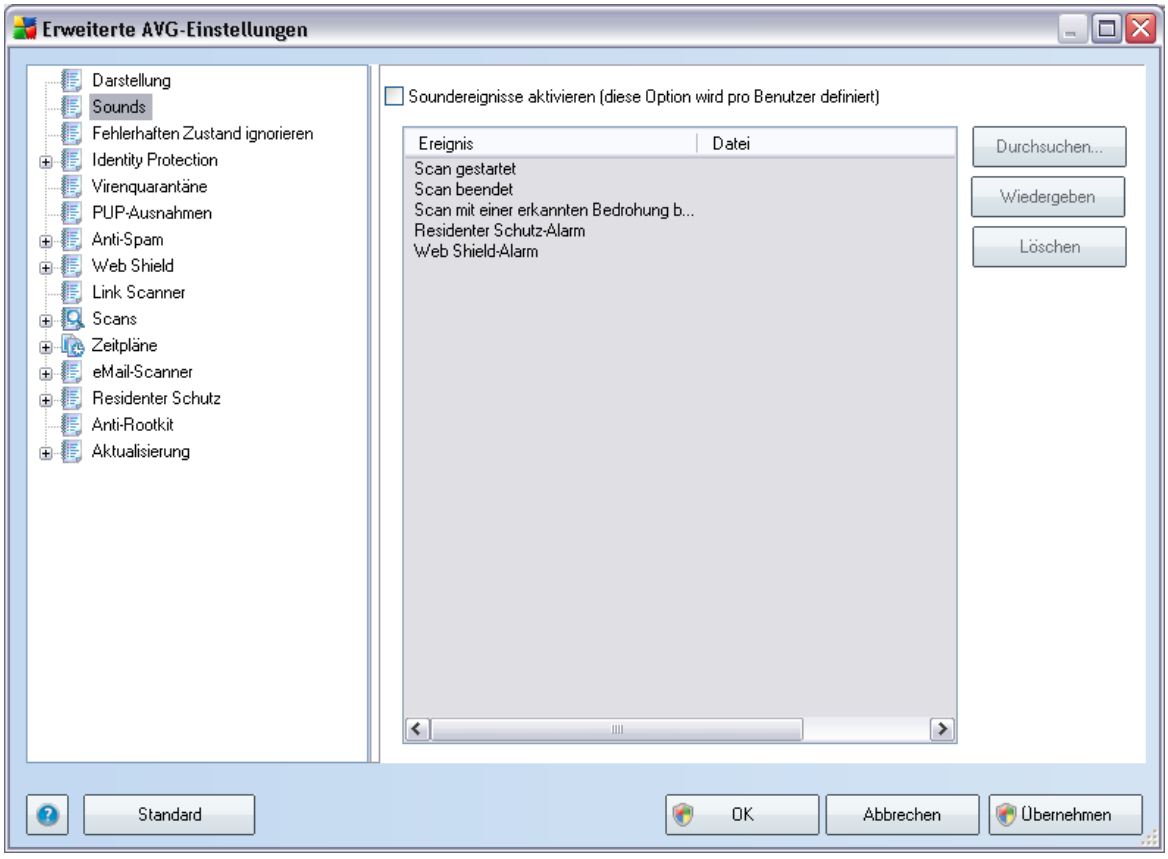
Spielmodus

Diese Funktion von AVG wurde für Anwendungen mit Vollbildmodus entwickelt, die über das Internet kommunizieren, wobei mögliche Dialoge von AVG die

Funktionsfähigkeit der Anwendung beeinträchtigen würden (*durch eine Minimierung oder Beeinträchtigung der Grafik*). Um dies zu vermeiden, sollten Sie das Kontrollkästchen ***Spielmodus bei Ausführung einer Anwendung im Vollbildmodus aktivieren*** aktiviert lassen (*Standardeinstellung*).

9.2. Sounds

Im Dialog ***Sounds*** können Sie festlegen, ob Sie bei bestimmten Aktionen von AVG per Soundbenachrichtigung informiert werden möchten. Wenn ja, aktivieren Sie die Option ***Soundereignisse aktivieren*** (*standardmäßig deaktiviert*), um die Liste der Aktionen von AVG zu aktivieren:

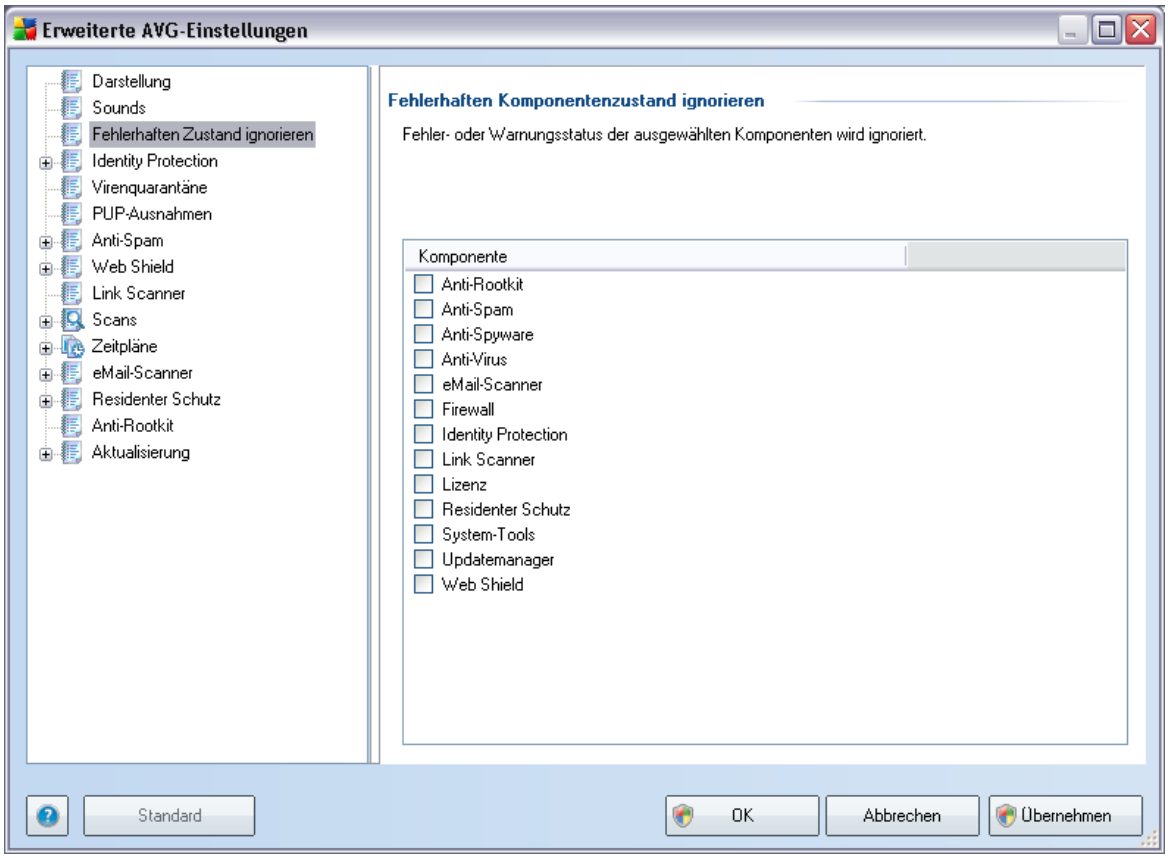


Wählen Sie nun aus der Liste das gewünschte Ereignis aus, und suchen Sie auf Ihrem Datenträger nach einem Sound (***Durchsuchen***), den Sie diesem Ereignis zuweisen möchten. Um den ausgewählten Sound anzuhören, markieren Sie das Ereignis in der Liste, und klicken Sie auf die Schaltfläche ***Wiedergeben*** . Verwenden Sie die Schaltfläche ***Löschen***, um den einem Ereignis zugewiesenen Sound zu entfernen.

Hinweis: *Es werden ausschließlich Sounds vom Typ *.wav unterstützt!*

9.3. Fehlerhaften Zustand ignorieren

Im Dialog ***Fehlerhaften Komponentenzustand ignorieren*** können Sie die Komponenten markieren, über die Sie nicht informiert werden möchten:



Standardmäßig sind alle Komponenten in dieser Liste deaktiviert. Das bedeutet: Wenn eine Komponente einen Fehlerstatus aufweist, erhalten Sie sofort eine Nachricht über das

- ***Symbol im Infobereich*** – Wenn alle Teile von AVG ordnungsgemäß funktionieren, wird das Symbol in vier Farben dargestellt. Tritt ein Fehler auf, wird das Symbol mit einem gelben Ausrufezeichen angezeigt
- und eine Beschreibung zum bestehenden Problem wird im Bereich ***Informationen zum Sicherheitsstatus*** im Hauptfenster von AVG angezeigt.

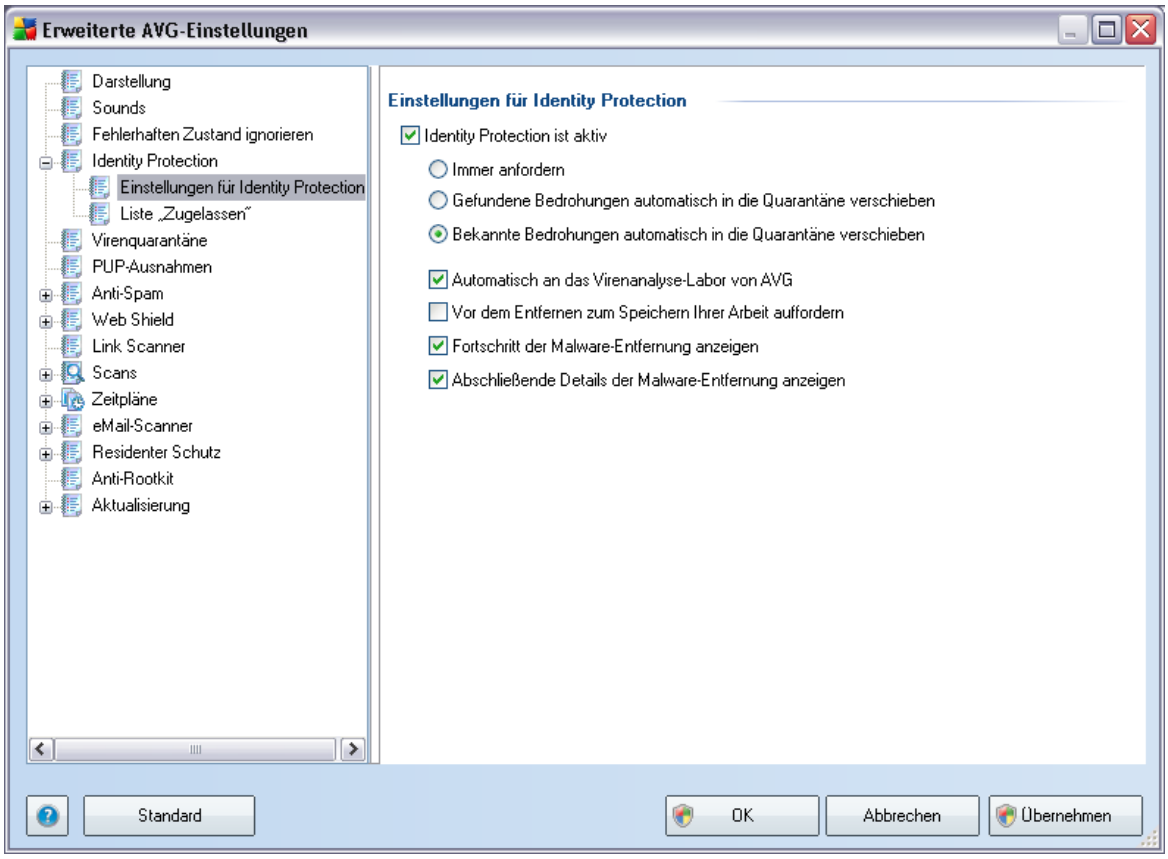
Es kann vorkommen, dass Sie aus bestimmten Gründen eine Komponente vorübergehend deaktivieren möchten. (*Die Deaktivierung einer Komponente wird nicht empfohlen. Achten Sie darauf, dass alle Komponenten aktiviert und die jeweiligen Standardeinstellungen vorgenommen sind*). In diesem Fall zeigt das Symbol im Infobereich automatisch eine Nachricht zum Fehlerstatus der Komponente an. Dieser spezielle Fall stellt natürlich keinen Fehler im eigentlichen Sinne dar, da er von Ihnen absichtlich herbeigeführt wurde und Sie sich über das potentielle Risiko bewusst sind. Sobald das Symbol grau angezeigt wird, kann es keine weiteren Fehler melden.

Für diesen Fall können Sie im oben angezeigten Dialog Komponenten auswählen, die eventuell einen fehlerhaften Status aufweisen (*oder deaktiviert sind*) oder über die Sie keine Informationen erhalten möchten. Alternativ steht für einige Komponenten die Option ***Komponentenstatus ignorieren*** zur Verfügung, die über die Komponentenübersicht im Hauptfenster von AVG festgelegt werden kann.

9.4. Identitätsschutz

9.4.1. Einstellungen des Identitätsschutzes

Im Dialog ***Einstellungen für Identitätsschutz*** können Sie die Grundfunktionen von ***Identitätsschutz*** aktivieren und deaktivieren:

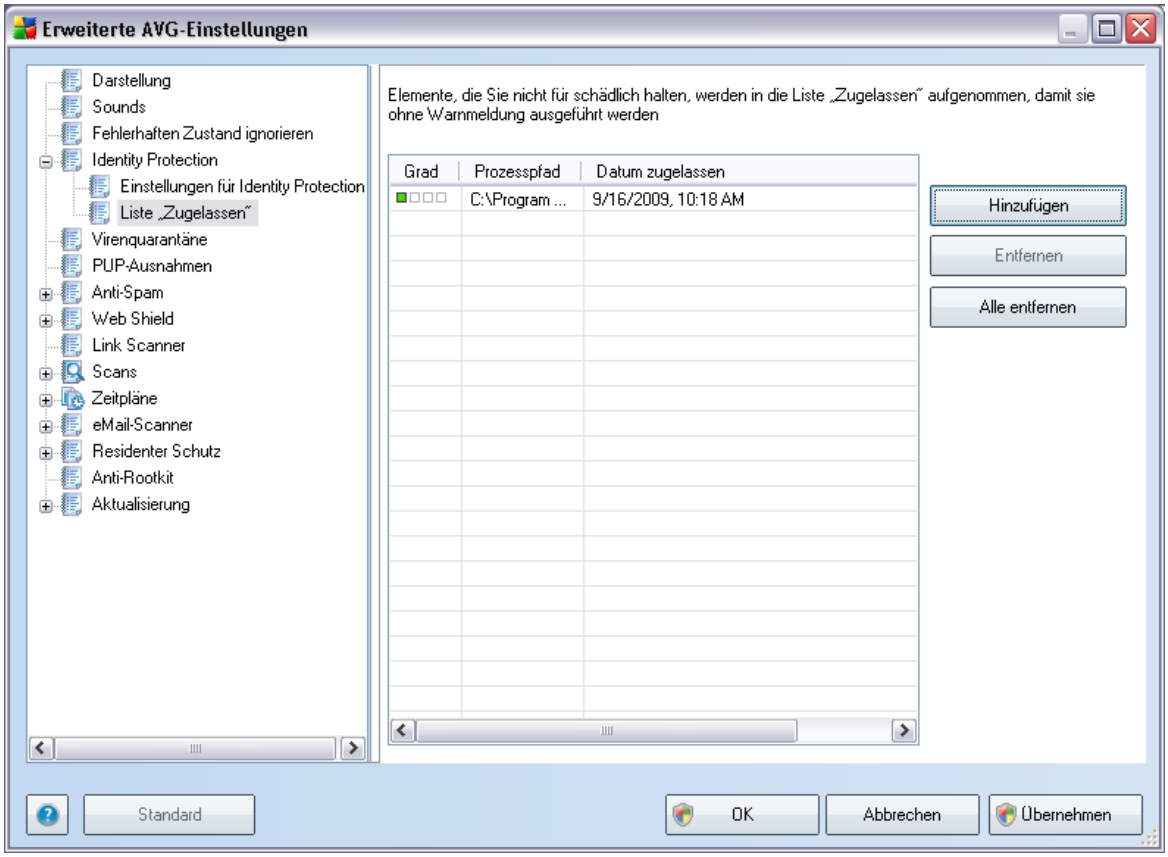


- ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** – (*standardmäßig deaktiviert*): Wenn Sie dieses Kontrollkästchen aktivieren, werden alle potentiell gefährlichen Bedrohungen umgehend in die sichere AVG Virenquarantäne verschoben. Wenn Sie die Standardeinstellungen beibehalten, werden Sie bei der Erkennung einer Bedrohung gefragt, ob diese in die Virenquarantäne verschoben werden soll. Damit wird sichergestellt, dass keine Anwendungen entfernt werden, die Sie ausführen möchten.

- ***Automatisch an das Virenlabor von AVG senden*** – (*standardmäßig aktiviert*): Bitte lassen Sie dieses Kontrollkästchen aktiviert, um die Datenbank mit Informationen über schädliche Aktivitäten im Web zu vervollständigen und uns dabei zu helfen, neue Bedrohungen zu identifizieren.

9.4.2. Liste „Zugelassen"

Wenn Sie im Dialog ***Einstellungen für Identitätsschutz*** entschieden haben, den Eintrag ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** deaktiviert zu lassen, werden Sie bei jeder Erkennung von potentieller Malware gefragt, ob diese entfernt werden soll. Wenn Sie dann die (*aufgrund ihres Verhaltens*) als verdächtig eingestufte Anwendung als sicher kennzeichnen, bestätigen Sie, dass diese auf Ihrem Computer belassen werden soll. Die Anwendung wird der sogenannten ***Liste „Zugelassen"*** hinzugefügt und nicht mehr als potentiell gefährlich gekennzeichnet:



Die ***Liste „Zugelassen"*** enthält für jede Anwendung die folgenden Informationen:

- ***Grad*** – Eine grafische Darstellung des Schweregrads des Prozesses auf einer vierstufigen Skala von weniger schwer (■□□□) bis kritisch(■■■■)
- ***Prozesspfad*** – Der Pfad zum Speicherort der ausführbaren Datei (des

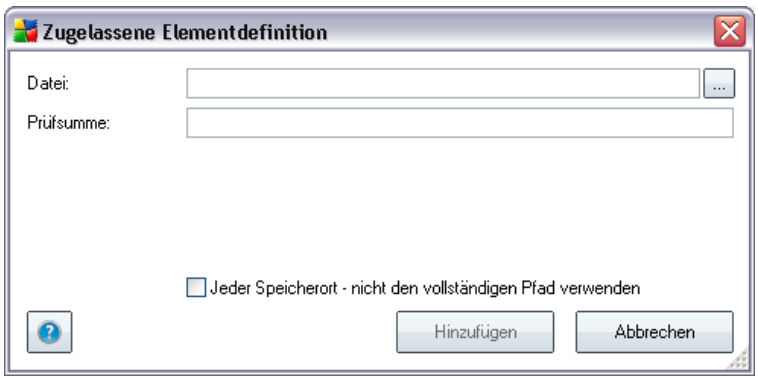
Prozesses)

- ***Datum zugelassen*** – Das Datum, an dem Sie die Anwendung manuell als sicher eingestuft haben

Schaltflächen

Im Dialog ***Liste „Zugelassen"*** stehen die folgenden Schaltflächen zur Verfügung:

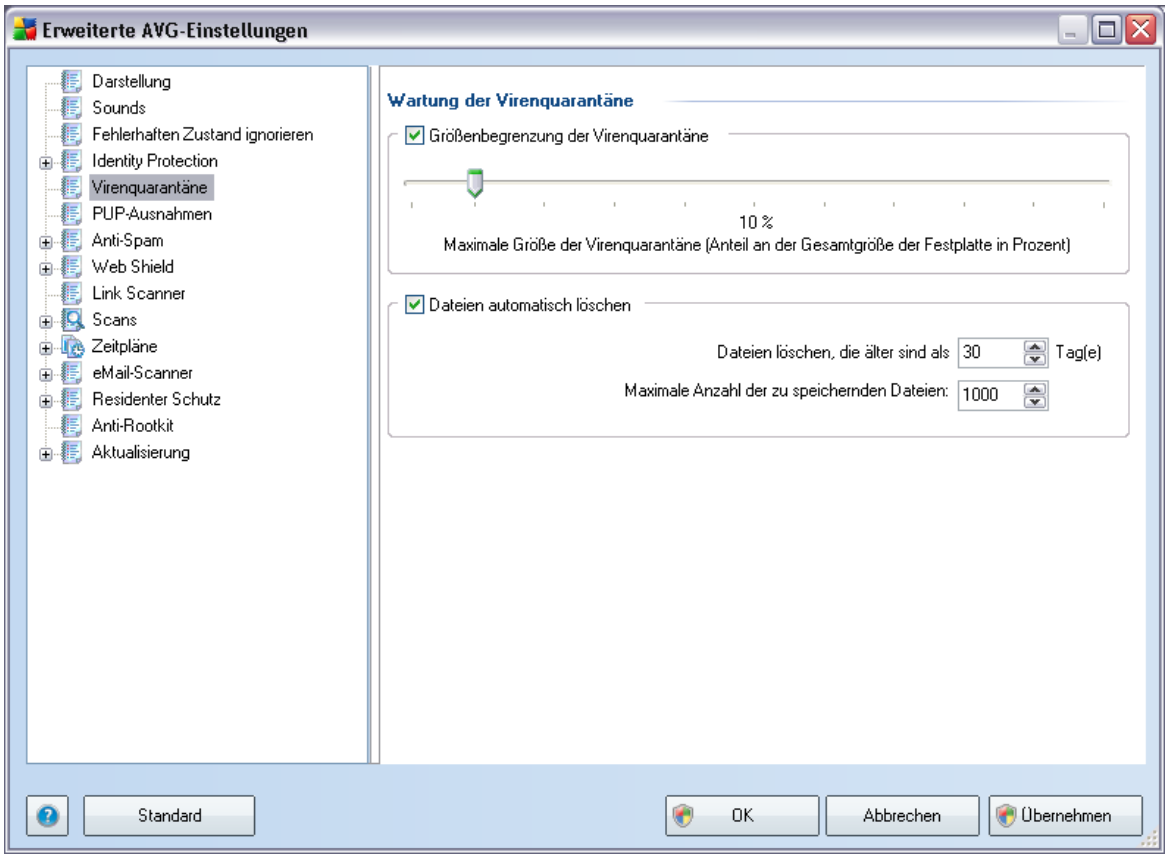
- ***Hinzufügen*** – Klicken Sie auf diese Schaltfläche, um der Liste „Zugelassen" eine neue Anwendung hinzuzufügen. Es wird der folgende Dialog angezeigt:



  - ***Datei*** – Geben Sie den vollständigen Pfad zur Datei (*Anwendung*) ein, die als Ausnahme eingestuft werden soll
  - ***Prüfsumme*** – Zeigt die eindeutige Signatur der ausgewählten Datei an. Bei der Prüfsumme handelt es sich um eine automatisch erzeugte Zeichenfolge, mit der AVG die ausgewählte Datei eindeutig von anderen Dateien unterscheiden kann. Die Prüfsumme wird erzeugt und angezeigt, nachdem die Datei erfolgreich hinzugefügt wurde.
  - ***Jeder Speicherort*** – Verwenden Sie nicht den vollständigen Pfad – Wenn Sie diese Datei nur bei diesem bestimmten Speicherort als Ausnahme festlegen möchten, lassen Sie das Kontrollkästchen deaktiviert

- ***Entfernen*** – Klicken Sie auf diese Schaltfläche, um die ausgewählte Anwendung aus der Liste zu entfernen
- ***Alle entfernen*** – Klicken Sie auf diese Schaltfläche, um alle aufgelisteten Anwendungen zu entfernen

9.5. Virenquarantäne



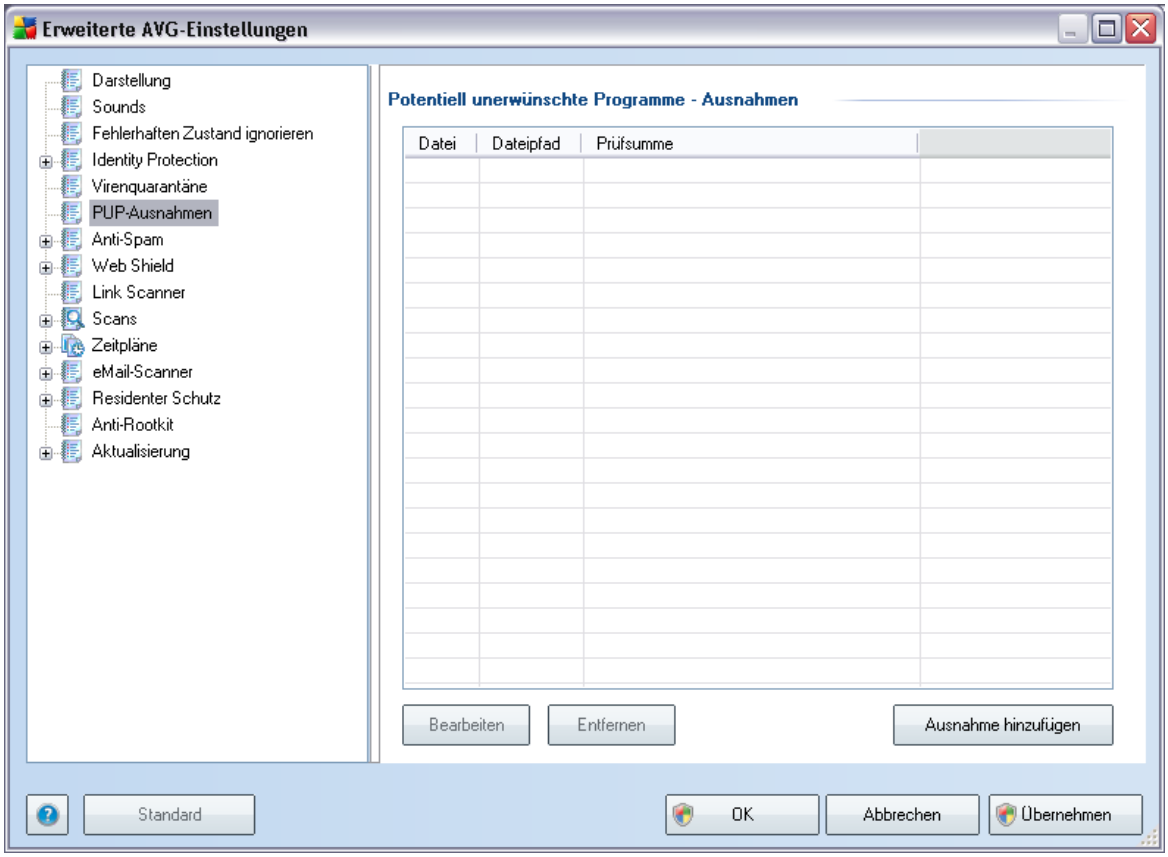
Im Dialog ***Wartung der Virenquarantäne*** können Sie mehrere Parameter hinsichtlich der Verwaltung der in der ***Virenquarantäne*** gespeicherten Objekte festlegen:

- ***Größenbegrenzung der Virenquarantäne*** – Mithilfe des Schiebereglers können Sie die maximale Größe der ***Virenquarantäne*** festlegen. Die Größe wird proportional zur Größe Ihrer lokalen Festplatte angegeben.

- ***Dateien automatisch löschen*** – In diesem Bereich wird die maximale Dauer festgelegt, die Objekte in der ***Virenquarantäne*** gespeichert werden (***Dateien löschen, die älter sind als ... Tage***), und die maximale Anzahl der in der ***Virenquarantäne*** gespeicherten Dateien (***Maximale Anzahl der zu speichernden Dateien***) bestimmt

9.6. PUP-Ausnahmen

AVG 9 Internet Security ist in der Lage, ausführbare Anwendungen oder DLL-Bibliotheken, die im System potentiell unerwünscht sind, zu erkennen und zu analysieren. In bestimmten Fällen kann sich der Benutzer dazu entscheiden, unerwünschte Programme auf dem Computer zu belassen (*Programme, die absichtlich installiert worden sind*). Einige Programme (besonders kostenlose) enthalten Adware. Adware kann von AVG als ***potentiell unerwünschtes Programm*** erkannt und gemeldet werden. Wenn Sie ein derartiges Programm auf Ihrem Computer behalten möchten, können Sie es als Ausnahme eines potentiell unerwünschten Programms definieren:

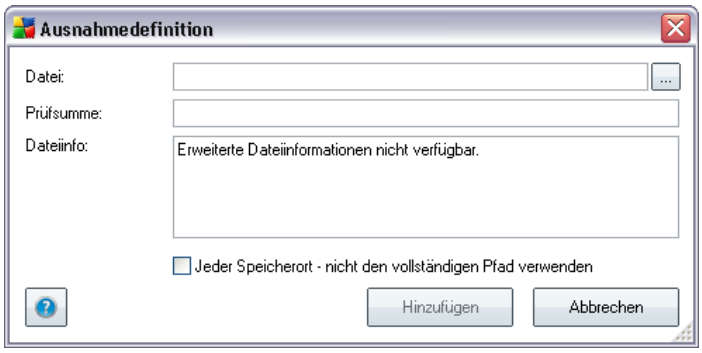


Im Dialog ***Potentiell unerwünschten Programmen - Ausnahmen*** wird eine Liste der bereits definierten und aktuell gültigen Ausnahmen an potentiell unerwünschten Programmen angezeigt. Sie können die Liste bearbeiten, vorhandene Einträge löschen oder neue Ausnahmen hinzufügen. Für jede einzelne Ausnahme finden sich in der Liste die folgenden Angaben:

- ***Datei*** – Gibt den Namen der jeweiligen Anwendung an
- ***Dateipfad*** – Zeigt den Pfad zum Speicherort der Anwendung an
- ***Prüfsumme*** – Zeigt die eindeutige Signatur der ausgewählten Datei an. Bei der Prüfsumme handelt es sich um eine automatisch erzeugte Zeichenfolge, mit der AVG die ausgewählte Datei eindeutig von anderen Dateien unterscheiden kann. Die Prüfsumme wird erzeugt und angezeigt, nachdem die Datei erfolgreich hinzugefügt wurde.

Schaltflächen

- ***Bearbeiten*** – Öffnet einen Bearbeitungsdialog (*der identisch ist mit dem Dialog für die Definition einer neuen Ausnahme; siehe unten*) einer bereits definierten Ausnahme, in dem Sie die Parameter der Ausnahme ändern können
- ***Entfernen***– Löscht das ausgewählte Element aus der Liste der Ausnahmen
- ***Ausnahme hinzufügen*** – Öffnet einen Bearbeitungsdialog, in dem Sie die Parameter der zu erstellenden neuen Ausnahme definieren können:



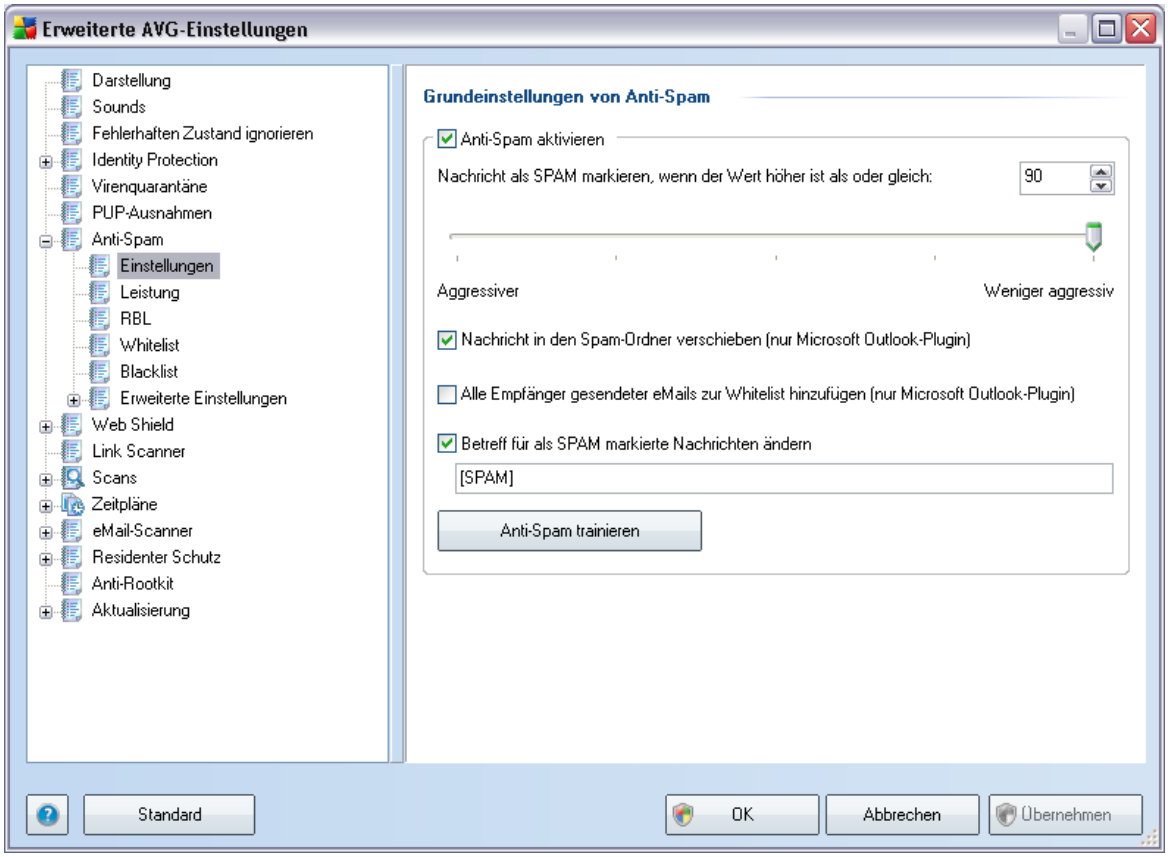
  - ***Datei*** – Geben Sie den vollständigen Pfad zu der Datei ein, die Sie als Ausnahme definieren möchten
  - ***Prüfsumme*** – Zeigt die eindeutige Signatur der ausgewählten Datei an. Bei der Prüfsumme handelt es sich um eine automatisch erzeugte Zeichenfolge, mit der AVG die ausgewählte Datei eindeutig von anderen Dateien unterscheiden kann. Die Prüfsumme wird erzeugt und angezeigt, nachdem die Datei erfolgreich hinzugefügt wurde.

- **Dateiinfo** – Zeigt alle zusätzlichen Informationen über die Datei an (*Lizenz-/Versionsdaten usw.*)

- **Jeder Speicherort – nicht den vollständigen Pfad verwenden** – Wenn Sie diese Datei nur für diesen bestimmten Speicherort als Ausnahme festlegen möchten, lassen Sie das Kontrollkästchen deaktiviert

9.7. Anti-Spam

9.7.1. Einstellungen



Im Dialog ***Grundeinstellungen von Anti-Spam*** können Sie das Kontrollkästchen ***Anti-Spam aktivieren*** aktivieren bzw. deaktivieren, um festzulegen, ob eMails auf Spam geprüft werden sollen. Diese Option ist standardmäßig aktiviert; auch hier

empfehlen wir Ihnen, diese Konfiguration beizubehalten, solange Sie nicht einen guten Grund für eine Änderung haben.

Des Weiteren können Sie mehr oder weniger aggressive Maßnahmen für Bewertungen auswählen. Der ***Anti-Spam***-Filter weist jeder Nachricht eine Bewertung zu (*z. B. wie sehr der Nachrichteninhalt SPAM ähnelt*), die auf verschiedenen dynamischen Prüftechniken basiert. Sie können die Einstellung ***Nachricht als Spam markieren, wenn der Wert höher ist als*** anpassen, indem Sie entweder einen Wert aus (*0 bis 100*) eingeben oder den Schieberegler nach links oder rechts verschieben (*mit dem Schieberegler können nur Werte zwischen 50 und 90 eingestellt werden*).

Wir empfehlen, den Schwellenwert zwischen 50 und 90 oder, wenn Sie wirklich unsicher sind, auf 90 einzustellen. Im Folgenden finden Sie eine kurze Erläuterung der Schwellenwerte:

- ***Wert 90–99*** – Die meisten eingehenden eMails werden normal in den Posteingang geleitet (ohne als Spam gekennzeichnet zu werden). Die am leichtesten als Spam identifizierbaren eMails werden ausgefiltert, aber es kann immer noch ein großer Anteil an Spam auf Ihren Computer gelangen.

- ***Wert 80–89*** – eMail-Nachrichten, die Spam sein könnten, werden ausgefiltert. Auch einige nicht als Spam zu klassifizierende Nachrichten werden eventuell fälschlicherweise ausgefiltert.

- ***Wert 60–79*** – Als relativ aggressive Konfiguration einzuordnen. Alle eMails, die möglicherweise als Spam einzustufen sind, werden ausgefiltert. Es ist wahrscheinlich, dass auch nicht als Spam zu klassifizierende Nachrichten ausgefiltert werden.

- ***Wert 1–59*** – Sehr aggressive Konfiguration. Es ist sehr wahrscheinlich, dass auch Nachrichten abgefangen werden, die nicht wirklich Spam sind. Dieser Wertebereich wird für den normalen Gebrauch nicht empfohlen.

- ***Wert 0*** – In diesem Modus erhalten Sie nur eMails von Absendern, die in Ihre ***Whitelist*** eingetragen sind. Alle anderen eMails werden als Spam betrachtet. ***Dieser Wertebereich wird für den normalen Gebrauch nicht empfohlen.***

Im Dialog ***Grundeinstellungen von Anti-Spam*** können Sie zudem festlegen, wie die erkannten Spam-Nachrichten behandelt werden sollen:

- ***Nachricht in den Spam-Ordner verschieben*** – Aktivieren Sie diese Option, wenn alle erkannten Spam-Nachrichten automatisch in den Junk-Ordner Ihres eMail-Clients verschoben werden sollen;

- ***Alle Empfänger gesendeter eMails zur Whitelist hinzufügen*** – Aktivieren

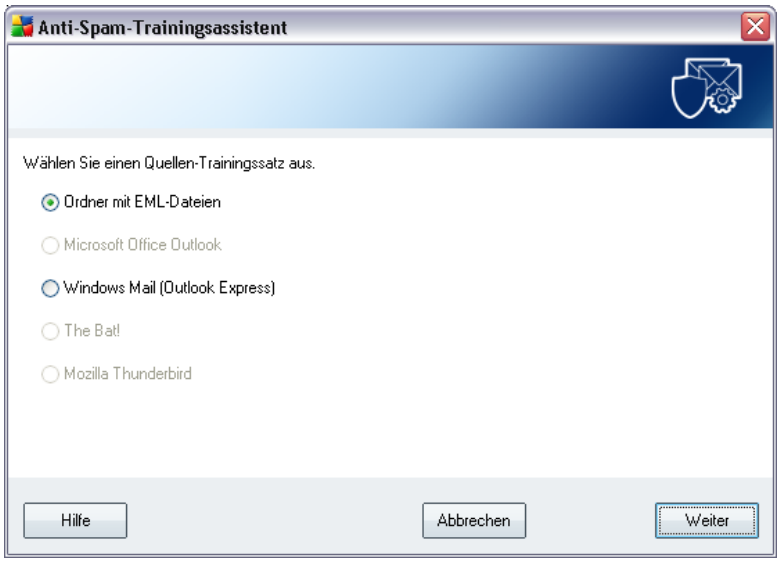
Sie dieses Kontrollkästchen, um zu bestätigen, dass allen Empfängern gesendeter eMails vertraut werden kann, und alle eMails, die von diesen eMail-Kontos kommen, zugestellt werden können;

- ***Betreff für als SPAM markierte Nachrichten ändern*** – Aktivieren Sie dieses Kontrollkästchen, wenn alle als Spam erkannten Nachrichten mit einem bestimmten Wort oder Zeichen im Betrefffeld markiert werden sollen; den gewünschten Text können Sie in das aktivierte Textfeld eingeben.

Schaltflächen

Anti-Spam trainieren dient zum Öffnen des ***Anti-Spam-Trainingsassistenten***, der im nächsten Kapitel genauer beschrieben wird.

Im ersten Dialog des ***Anti-Spam-Trainingsassistenten*** werden Sie dazu aufgefordert, die Quelle der eMail-Nachrichten auszuwählen, die Sie für das Training verwenden möchten. In der Regel wählen Sie eMails aus, die nicht als Spam erkannt oder fälschlicherweise als Spam eingestuft worden sind.



Dabei stehen Ihnen die folgenden Optionen zur Verfügung:

- ***Ein bestimmter eMail-Client*** – Wenn Sie einen der aufgelisteten eMail-Clients verwenden (*MS Outlook, Outlook Express, The Bat! oder Mozilla Thunderbird*), wählen Sie einfach die entsprechende Option aus

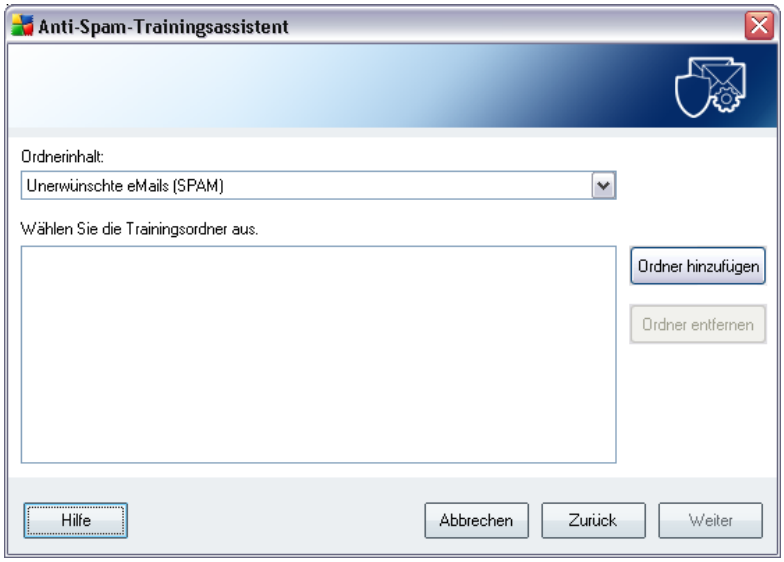
- ***Ordner mit EML-Dateien*** – Wenn Sie ein anderes eMail-Programm verwenden, sollten Sie die Nachrichten zunächst in einem bestimmten Ordner speichern (*im .eml-Format*) oder sicherstellen, dass Sie den Speicherort der Nachrichtenordner Ihres eMail-Clients kennen. Wählen Sie anschließend ***Ordner mit EML-Dateien***, damit Sie den gewünschten Ordner im nächsten Schritt auffinden können

Um das Trainingsverfahren zu beschleunigen, ist es empfehlenswert, die eMails in den Ordnern zunächst zu sortieren, damit der Ordner, den Sie für Trainingszwecke verwenden, ausschließlich Übungsnachrichten enthält (entweder gewünschte oder unerwünschte). Dieser Schritt ist jedoch nicht zwingend erforderlich, da Sie die eMails auch später filtern können.

Wählen Sie die entsprechende Option, und klicken Sie auf ***Weiter***, um mit dem Assistenten fortzufahren.

Der in diesem Schritt angezeigte Dialog hängt von Ihrer vorherigen Auswahl ab.

Ordner mit EML-Dateien



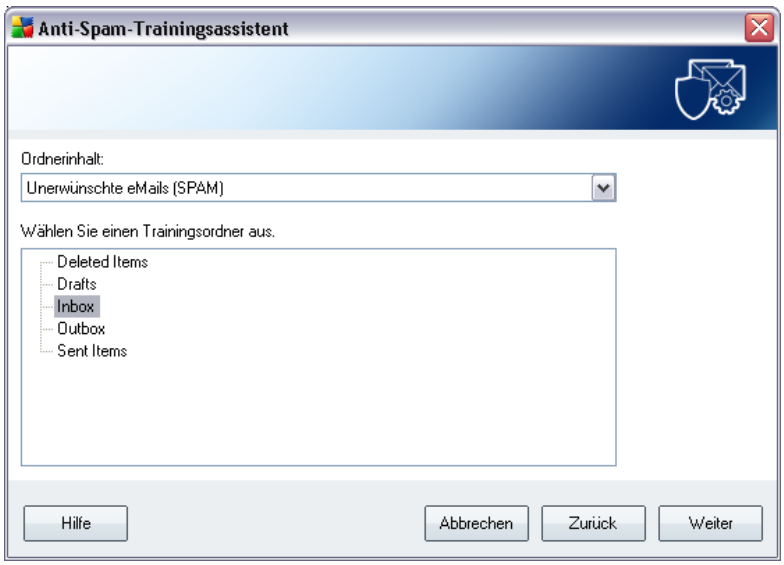
Wählen Sie in diesem Dialog bitte den Ordner mit den Nachrichten aus, den Sie für Trainingszwecke verwenden möchten. Klicken Sie auf die Schaltfläche ***Ordner hinzufügen***, um den Ordner mit den EML-Dateien zu suchen (*gespeicherte eMail-Nachrichten*). Der ausgewählte Ordner wird anschließend im Dialog angezeigt.

Wählen Sie im Dropdown-Menü ***Ordnerinhalt*** eine der zwei Optionen – ob der ausgewählte Ordner gewünschte (*HAM*-) oder unerwünschte (*SPAM*-) Nachrichten enthält. Bitte beachten Sie, dass Sie die Nachrichten im nächsten Schritt filtern können; der Ordner muss also nicht nur Trainings-eMails umfassen. Sie können nicht gewollte ausgewählte Ordner auch aus der Liste entfernen, indem Sie auf die Schaltfläche ***Ordner entfernen*** klicken.

Klicken Sie im Anschluss daran auf ***Weiter***, um zum Dialog zu den ***Filteroptionen für Nachrichten*** zu gelangen.

Ein bestimmter eMail-Client

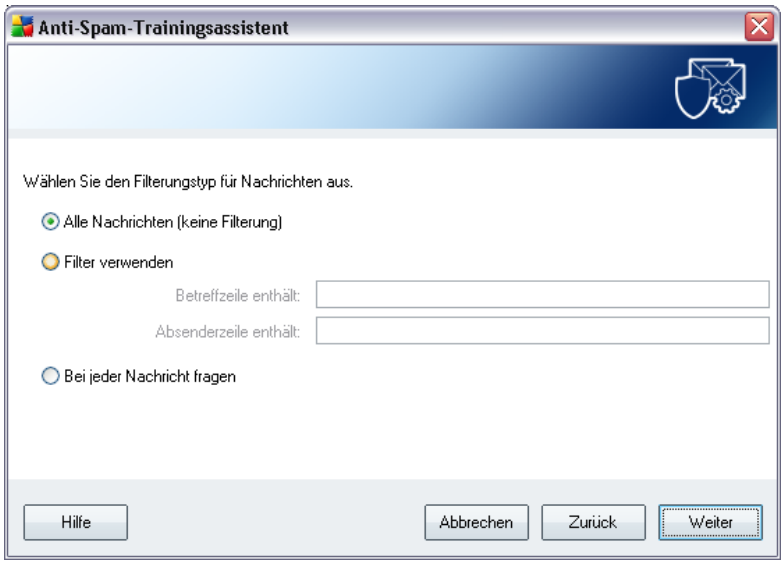
Sobald Sie eine der Optionen bestätigen, wird ein neuer Dialog angezeigt.



Hinweis: *Wenn Sie Microsoft Office Outlook verwenden, werden Sie zunächst dazu aufgefordert, ein Profil in „MS Office Outlook" auszuwählen.*

Wählen Sie im Dropdown-Menü ***Ordnerinhalt***eine der folgenden zwei Optionen – ob der ausgewählte Ordner erwünschte (*HAM*-) oder unerwünschte (*SPAM*-) Nachrichten enthält. Bitte beachten Sie, dass Sie die Nachrichten im nächsten Schritt filtern können; der Ordner muss also nicht nur Trainings-eMails umfassen. Im Hauptabschnitt des Dialogs wird eine Baumstruktur des ausgewählten eMail-Clients angezeigt. Bitte suchen Sie nach dem gewünschten Ordner, und wählen Sie ihn mit der Maus aus.

Klicken Sie im Anschluss daran auf ***Weiter***, und fahren Sie fort mit den ***Filteroptionen für Nachrichten***.



In diesem Dialog können Sie die Filtereinstellungen für Ihre eMail-Nachrichten vornehmen.

Wenn Sie sicher sind, dass der ausgewählte Ordner ausschließlich Nachrichten für Übungszwecke enthält, wählen Sie die Option***Alle Nachrichten (kein Filtern)***.

Wenn Sie sich angesichts der im Ordner enthaltenen Nachrichten nicht sicher sind, kann Sie der Assistent nach jeder einzelnen Nachricht fragen (so können Sie entscheiden, welche Nachrichten zu Übungszwecken verwendet werden sollen und welche nicht) - wählen Sie hierzu die Option ***Bei jeder Nachricht fragen***.

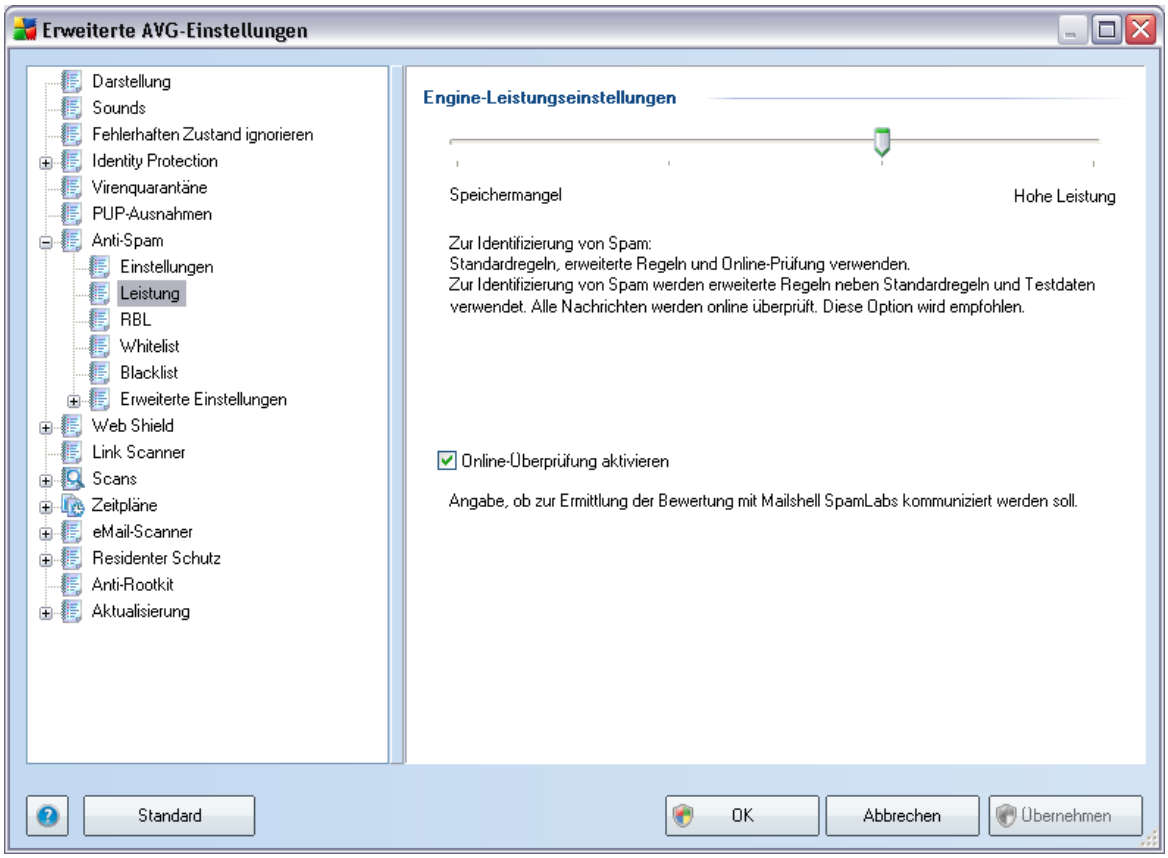
Genauere Filtereinstellungen können Sie vornehmen, wenn Sie die Option ***Filter verwenden*** auswählen. Sie können ein Wort (*Name*), ein Teil eines Wortes oder eine Phrase eingeben, um im Betreff bzw. im Absenderfeld der eMail danach zu suchen. Alle Nachrichten, die den eingegebenen Kriterien genau entsprechen, werden ohne weitere Nachfrage für das Training verwendet.

Achtung!:*Wenn Sie beide Textfelder ausfüllen, werden auch Adressen verwendet, die lediglich eines der Kriterien erfüllen!*

Nachdem Sie die gewünschte Option gewählt haben, klicken Sie auf ***Weiter***. Im folgenden Dialog wird Ihnen lediglich mitgeteilt, dass der Assistent zur Bearbeitung

der Nachrichten bereit ist. Um das Training zu starten, klicken Sie erneut auf die Schaltfläche ***Weiter***. Das Training wird nun den zuvor ausgewählten Bedingungen entsprechend gestartet.

9.7.2. Leistung



Der Dialog ***Engine-Leistungseinstellungen*** (*zu öffnen über das Element* ***Leistung*** *im linken Navigationsbereich*) enthält Leistungseinstellungen für die Komponente ***Anti-Spam***. Bewegen Sie den Schieberegler nach links oder rechts, um die Scan-Leistung zwischen den Modi ***Speichermangel*** / ***Hohe Leistung*** einzustellen.

- ***Speichermangel*** – Beim Scanvorgang werden zur Identifizierung von Spam keine Regeln verwendet. Zur Identifizierung werden nur Testdaten verwendet. Dieser Modus ist nicht für den allgemeinen Gebrauch empfohlen, es sei denn, die Computer-Hardware ist wirklich sehr langsam.

- ***Hohe Leistung*** – Für diesen Modus ist sehr viel Speicher erforderlich.

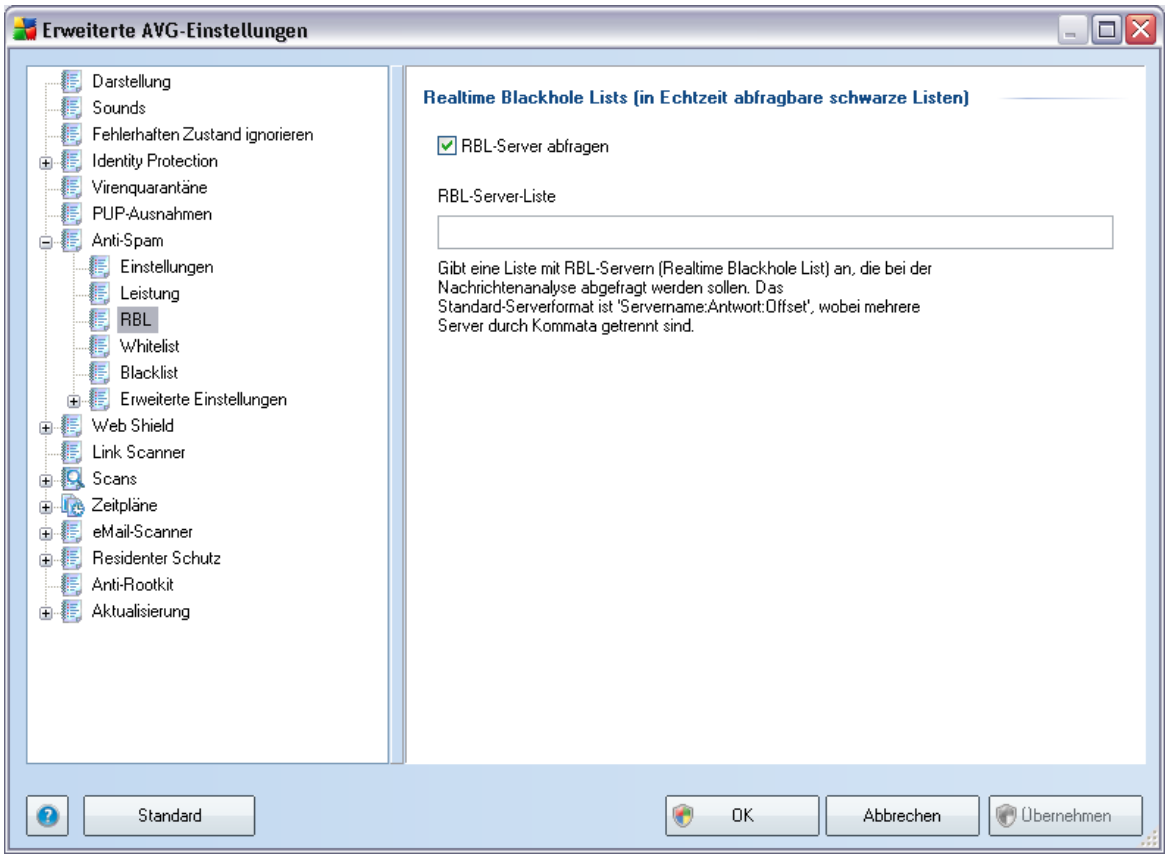
Während des Scanvorgangs werden zur Identifizierung von Spam folgende Funktionen verwendet: Regeln und Spam-Datenbank-Cache, einfache und erweiterte Regeln, IP-Adressen von Spammern und Spammer-Datenbanken.

Die Option ***Online-Überprüfung aktivieren*** ist standardmäßig aktiviert. Auf diese Weise wird eine genauere Erkennung von Spam durch Kommunikation mit den Mailshell-Servern ermöglicht (z. B. werden die gescannten Daten online mit den Mailshell-Datenbanken verglichen).

Grundsätzlich wird empfohlen, die Standardeinstellungen beizubehalten und nur dann zu ändern, wenn ein triftiger Grund vorliegt. Änderungen an dieser Konfiguration sollten nur von erfahrenen Benutzern durchgeführt werden!

9.7.3. RBL

Der Eintrag ***RBL*** öffnet den Bearbeitungsdialog ***Realtime Blackhole List (in Echtzeit abfragbare schwarze Listen)***:



In diesem Dialog können Sie die Funktion ***RBL-Server abfragen*** aktivieren und deaktivieren.

Der RBL-Server (*Realtime Blackhole Lists (in Echtzeit abfragbare schwarze Listen)*) ist ein DNS-Server mit einer umfangreichen Datenbank bekannter Spam-Sender. Bei Aktivierung dieser Funktion werden alle eMails mit den Adressen der RBL-Serverdatenbank verglichen und als Spam markiert, wenn Sie einem Datenbankeintrag entsprechen. Die RBL-Serverdatenbanken enthalten die allerneuesten Spam-Fingerabdrücke und ermöglichen so die beste und exakteste Spam-Erkennung. Diese Funktion ist besonders nützlich für Benutzer, die sehr viel Spam empfangen, der normalerweise nicht von der Anti-Spam-Engine erkannt wird.

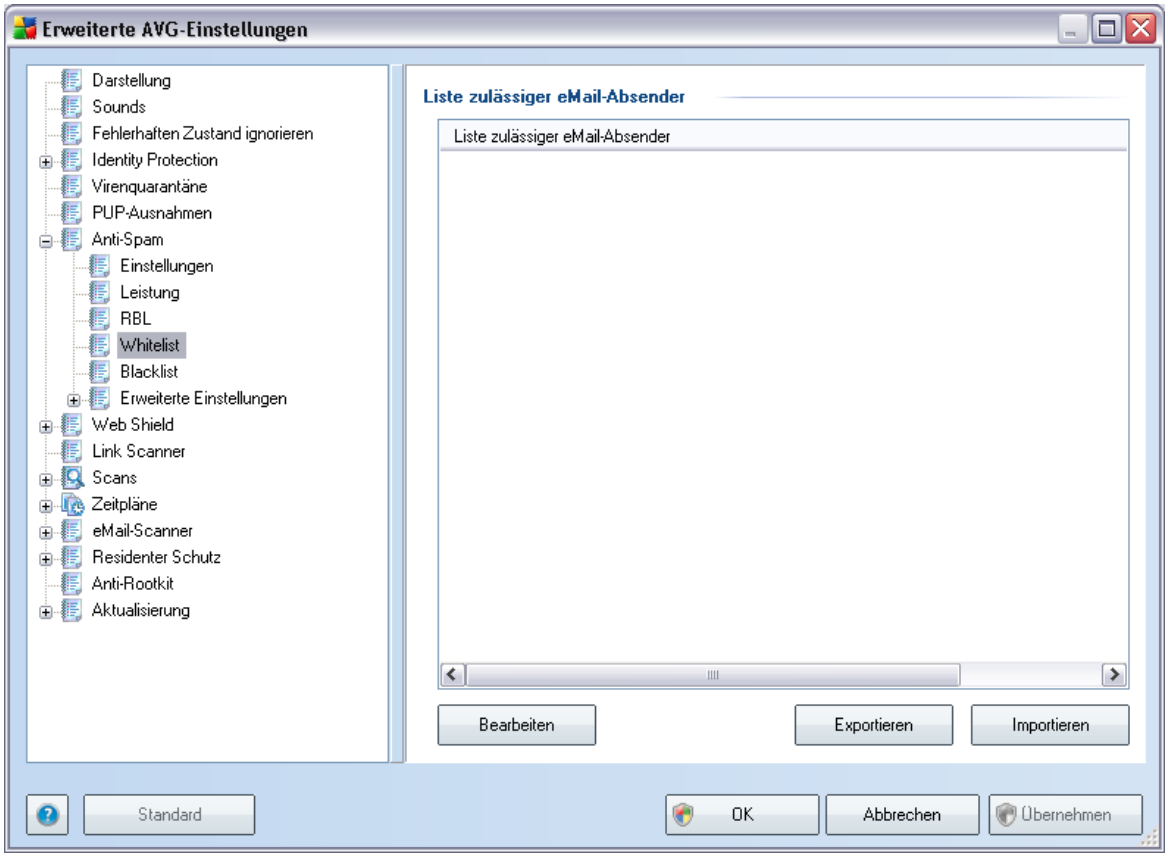
Über die ***RBL-Server-Liste*** können Sie spezielle RBL-Serverstandorte festlegen.

Hinweis: *Wenn Sie diese Funktion aktivieren, kann das den Empfang von eMails auf einigen Systemen und unter einigen Konfigurationen verlangsamen, da jede einzelne Nachricht mit der RBL-Serverdatenbank abgeglichen werden muss.*

Es werden keine persönlichen Daten an den Server gesendet!

9.7.4. Whitelist

Über den Eintrag ***Whitelist*** wird ein Dialog namens ***Liste zulässiger eMail-Absender*** mit einer allgemeinen Liste zulässiger Adressen von eMail-Absendern und Domainnamen geöffnet, deren Nachrichten niemals als Spam eingestuft werden.



In der Bearbeitungsoberfläche können Sie eine Liste mit Absendern erstellen, bei denen Sie sicher sind, dass sie Ihnen nie unerwünschte Nachrichten (Spam) senden werden. Sie können auch eine Liste mit vollständigen Domainnamen erstellen (*z. B. avg.com*), von denen Sie wissen, dass sie keine Spam-Nachrichten erzeugen.

Sobald Sie eine solche Liste von Absendern und/oder Domainnamen vorbereitet haben, können Sie die Adressen entweder direkt einzeln in die Liste eingeben oder die gesamte Liste in einem Schritt importieren. Folgende Schaltflächen sind verfügbar:

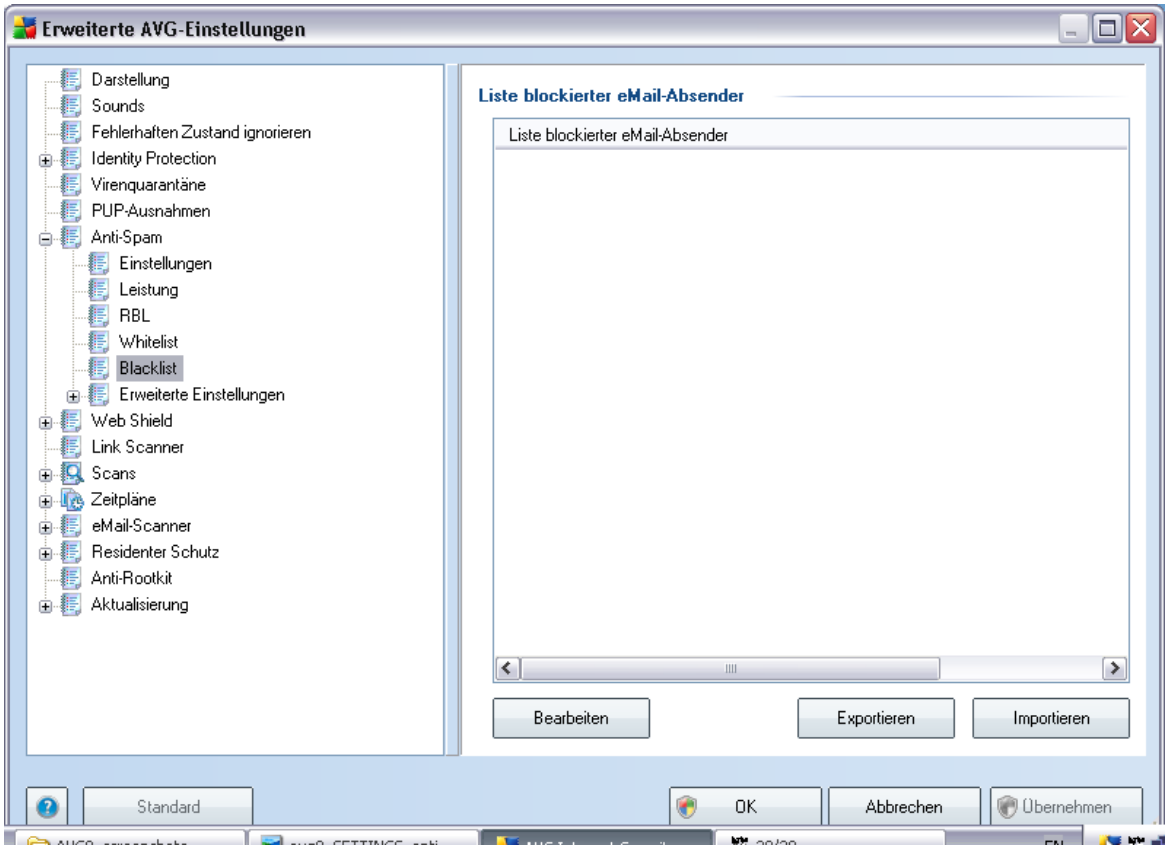
- ***Bearbeiten*** – Klicken Sie auf diese Schaltfläche, um einen Dialog zu öffnen, in dem Sie manuell eine Liste von Adressen eingeben können (*Sie können die Adressen auch mittels Kopieren und Einfügen eingeben*). Tragen Sie jeweils ein Element (*Absender, Domainname*) pro Zeile ein.

- ***Exportieren*** – Wenn Sie die Datensätze exportieren möchten, klicken Sie auf diese Schaltfläche. Alle Datensätze werden in einer reinen Textdatei gespeichert.

- ***Importieren*** – Wenn Sie bereits eine Textdatei mit eMail-Adressen/ Domainnamen vorbereitet haben, können Sie sie einfach über diese Schaltfläche importieren. Die Eingabedatei muss im reinen Textformat vorliegen, und der Inhalt darf jeweils nur ein Element (*Absender, Domainname*) pro Zeile enthalten.

9.7.5. Blacklist

Wenn Sie den Eintrag ***Blacklist*** auswählen, wird ein Dialog mit einer allgemeinen Liste blockierter eMail-Absenderadressen und Domainnamen angezeigt, deren Nachrichten immer als Spam markiert werden.



In der Bearbeitungsoberfläche können Sie eine Liste mit Absendern erstellen, von denen Sie unerwünschte Nachrichten (Spam) erwarten. Sie können auch eine Liste mit vollständigen Domainnamen (*z. B. spammingcompany.com*) erstellen, von denen Sie Spam-Nachrichten erwarten oder erhalten. Sämtliche eMail-Nachrichten der aufgelisteten Adressen und Domains werden als Spam identifiziert.

Sobald Sie eine solche Liste von Absendern und/oder Domainnamen vorbereitet haben, können Sie die Adressen entweder direkt einzeln in die Liste eingeben oder die gesamte Liste in einem Schritt importieren. Folgende Schaltflächen sind verfügbar:

- ***Bearbeiten*** – Klicken Sie auf diese Schaltfläche, um einen Dialog zu öffnen, in dem Sie manuell eine Liste von Adressen eingeben können (*(Sie können die Adressen auch mittels Kopieren und Einfügen eingeben*). Tragen Sie jeweils ein Element (*Absender, Domainname*) pro Zeile ein.

- ***Exportieren*** – Wenn Sie die Datensätze exportieren möchten, klicken Sie auf diese Schaltfläche. Alle Datensätze werden in einer reinen Textdatei gespeichert.

- ***Importieren*** – Wenn Sie bereits eine Textdatei mit eMail-Adressen/ Domainnamen vorbereitet haben, können Sie sie einfach über diese Schaltfläche importieren. Die Eingabedatei muss im reinen Textformat vorliegen, und der Inhalt darf jeweils nur ein Element (*Absender, Domainname*) pro Zeile enthalten.

9.7.6. Erweiterte Einstellungen

Grundsätzlich wird empfohlen, die Standardeinstellungen beizubehalten und nur dann zu ändern, wenn ein triftiger Grund vorliegt. Konfigurationsänderungen sollten nur von erfahrenen Benutzern durchgeführt werden!

Wenn Sie dennoch der Meinung sind, dass Sie die Konfiguration von ***Anti-Spam*** im Detail ändern müssen, folgen Sie den Anweisungen direkt auf der Benutzeroberfläche. Im Allgemeinen finden Sie in jedem Dialog eine bestimmte Funktion, die Sie bearbeiten können, sowie die zugehörige Beschreibung:

- ***Cache*** – Fingerabdruck, Domainprüfung, LegitRepute

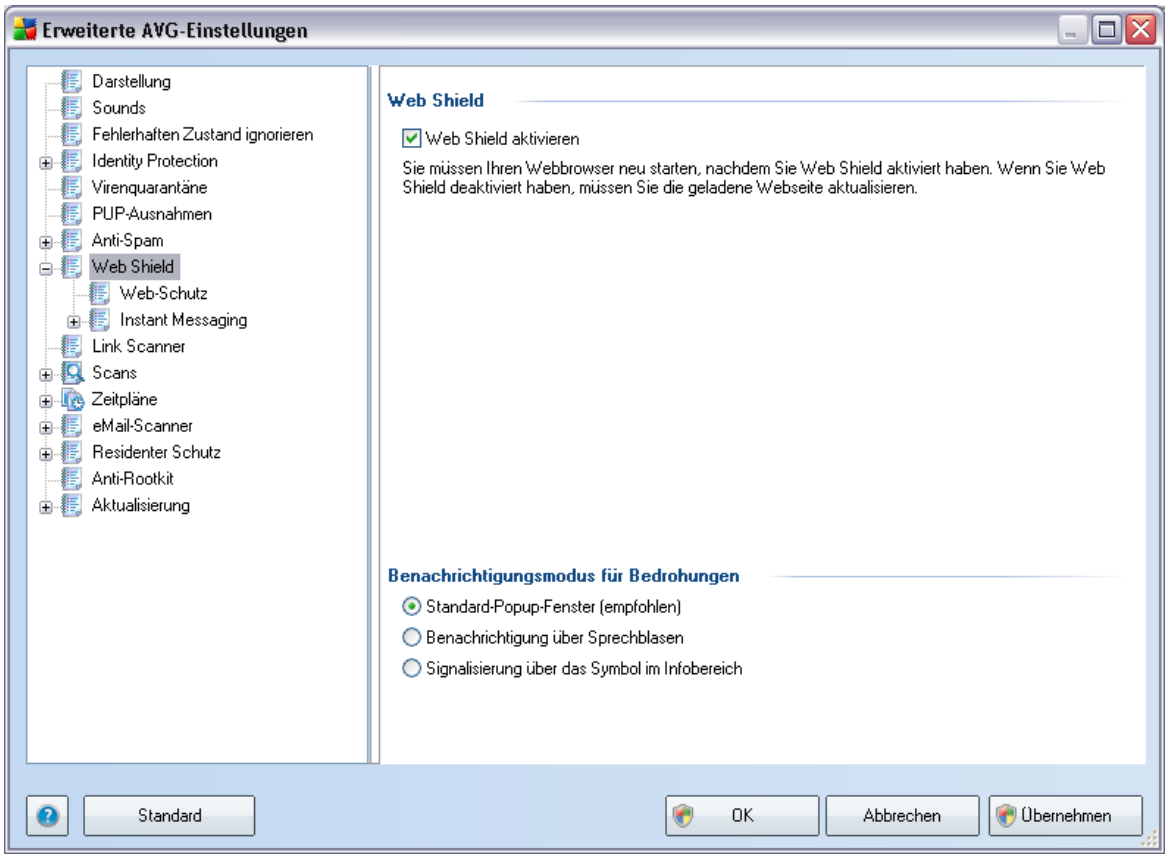
- ***Training*** – Worttraining, Bewertungshistorie, Bewertungs-Offset, maximale Worteinträge, Schwellenwert für Autotraining, Gewicht, Schreibpuffer

- ***Filtern*** – Sprachenliste, Länderliste, genehmigte IPs, blockierte IPs, blockierte Länder, blockierte Zeichensätze, gefälschte Absender

- ***RBL*** – RBL-Server, Mehrfachtreffer, Schwellenwert, Timeout, maximale IPs

- ***Internetverbindung*** – Timeout

9.8. Web Shield



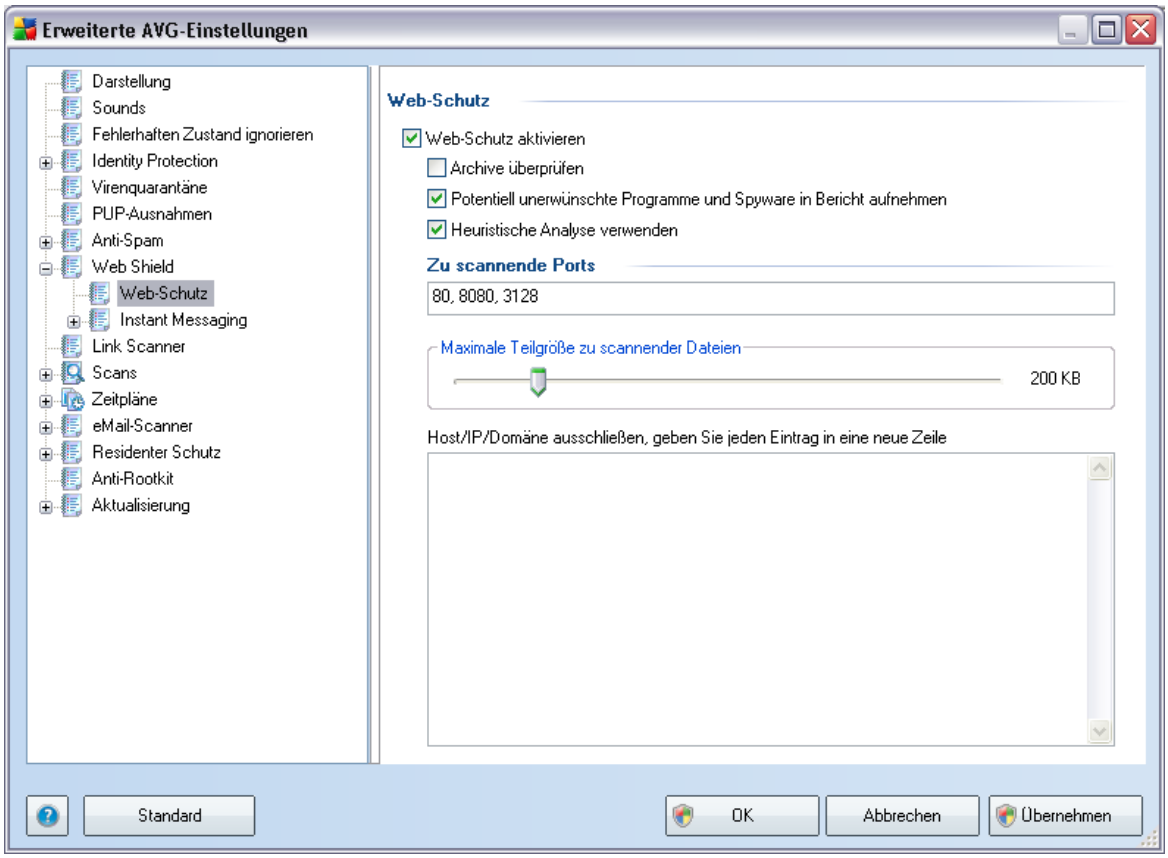
Im Dialog ***Web-Schutz*** können Sie die gesamte Komponente ***Web Shield*** mit der Option ***Web Shield aktivieren*** aktivieren bzw. deaktivieren (*standardmäßig aktiviert*). Erweiterte Einstellungen dieser Komponente finden Sie in den nachfolgenden Dialogen, die im Navigationsbaum aufgeführt werden:

- ***Web-Schutz***
- ***Instant Messaging***

Benachrichtigungsmodus für Bedrohungen

Im unteren Bereich des Dialogs können Sie auswählen, wie Sie über mögliche Bedrohungen informiert werden möchten: mit einem Standard-Popup-Fenster, mit einer Benachrichtigung über Sprechblasen oder durch ein Symbol im Infobereich.

9.8.1. Web-Schutz



Im Dialog ***Web-Schutz*** können Sie die Konfiguration der Komponente hinsichtlich des Scans von Website-Inhalten bearbeiten. Auf der Bearbeitungsoberfläche können Sie die folgenden grundlegenden Optionen konfigurieren:

- ***Web-Schutz aktivieren*** – Mit dieser Option wird bestätigt, dass ***Web Shield*** die Inhalte von Seiten im Internet scannen soll. Wenn diese Option aktiviert ist (*standardmäßig aktiviert*), können Sie darüber hinaus folgende Elemente aktivieren/deaktivieren:
    - ***Archive überprüfen*** – Archivinhalte, die möglicherweise auf einer angezeigten Webseite enthalten sind, werden ebenfalls gescannt .
    - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – Die aufgerufene Webseite wird auf potentiell unerwünschte Programme (*ausführbare Programme, die möglicherweise*

Spyware oder Adware sind) und Spyware gescannt.

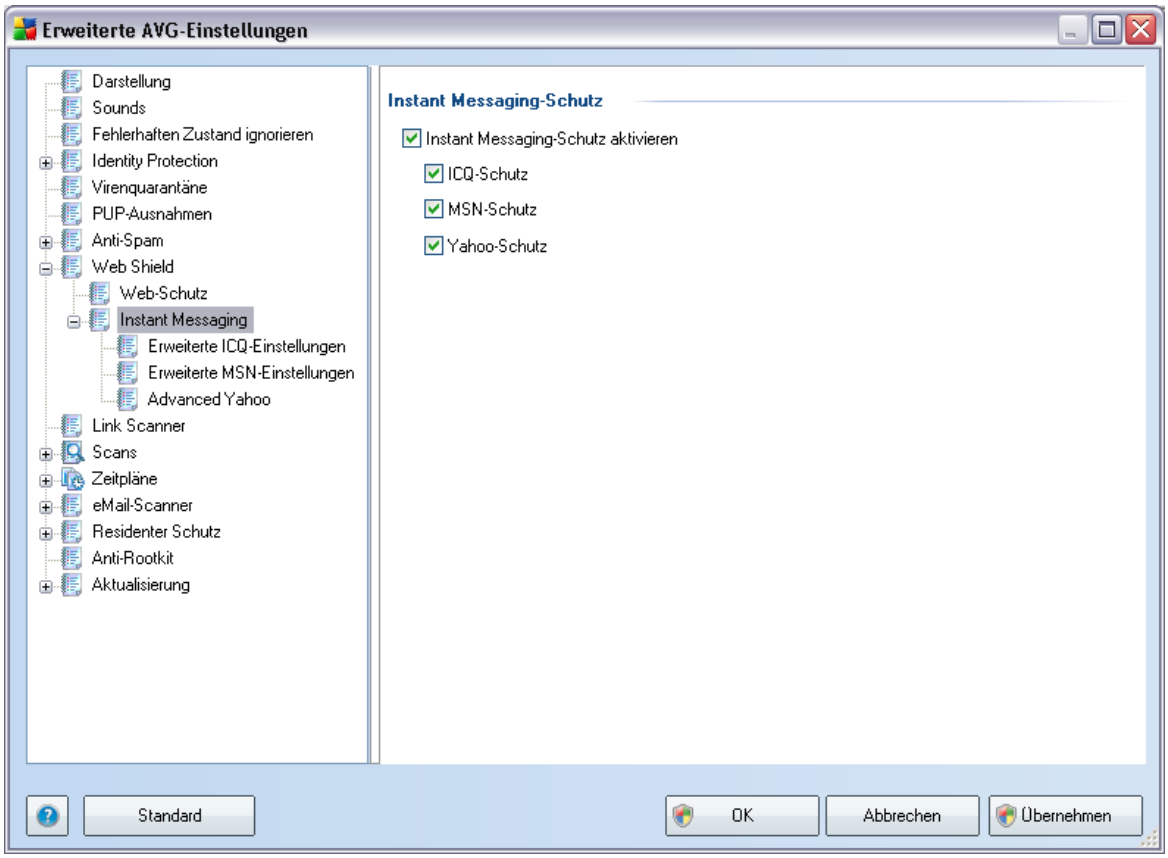
- ***Heuristische Analyse verwenden*** – Der Inhalt der angezeigten Webseite wird mit Hilfe der Methode heuristische Analyse gescannt (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*).

- ***Zu scannende Ports*** – In diesem Feld werden die standardmäßigen Portnummern für die HTTP-Kommunikation aufgelistet. Wenn Ihr Computer anders konfiguriert ist, können Sie die Portnummern je nach Bedarf ändern.

- ***Maximale Teilgröße zu scannender Dateien*** – Wenn die angezeigte Webseite Dateien enthält, können Sie deren Inhalte scannen, noch bevor diese auf Ihren Computer heruntergeladen werden. Das Scannen großer Dateien kann jedoch einige Zeit in Anspruch nehmen und das Herunterladen der Webseite ist signifikant langsamer. Mit Hilfe des Schiebereglers können Sie die maximale Größe einer Datei festlegen, die noch mit ***Web Shield*** gescannt werden soll. Selbst wenn die heruntergeladene Datei größer als festgelegt ist und daher nicht mit Web Shield gescannt wird, sind Sie weiterhin geschützt: Sollte die Datei infiziert sein, wird dies von ***Residenter Schutz*** sofort erkannt.

- ***Host/IP/Domäne ausschließen*** – In dieses Textfeld können Sie den genauen Namen eines Servers (*Host oder IP-Adresse, IP-Adresse mit Maske oder URL*) oder einer Domäne eingeben, die nicht von***Web Shield*** *gescannt werden sollen.* Schließen Sie daher nur Hosts aus, die mit Sicherheit keine gefährlichen Webinhalte bereitstellen.

9.8.2. Instant Messaging

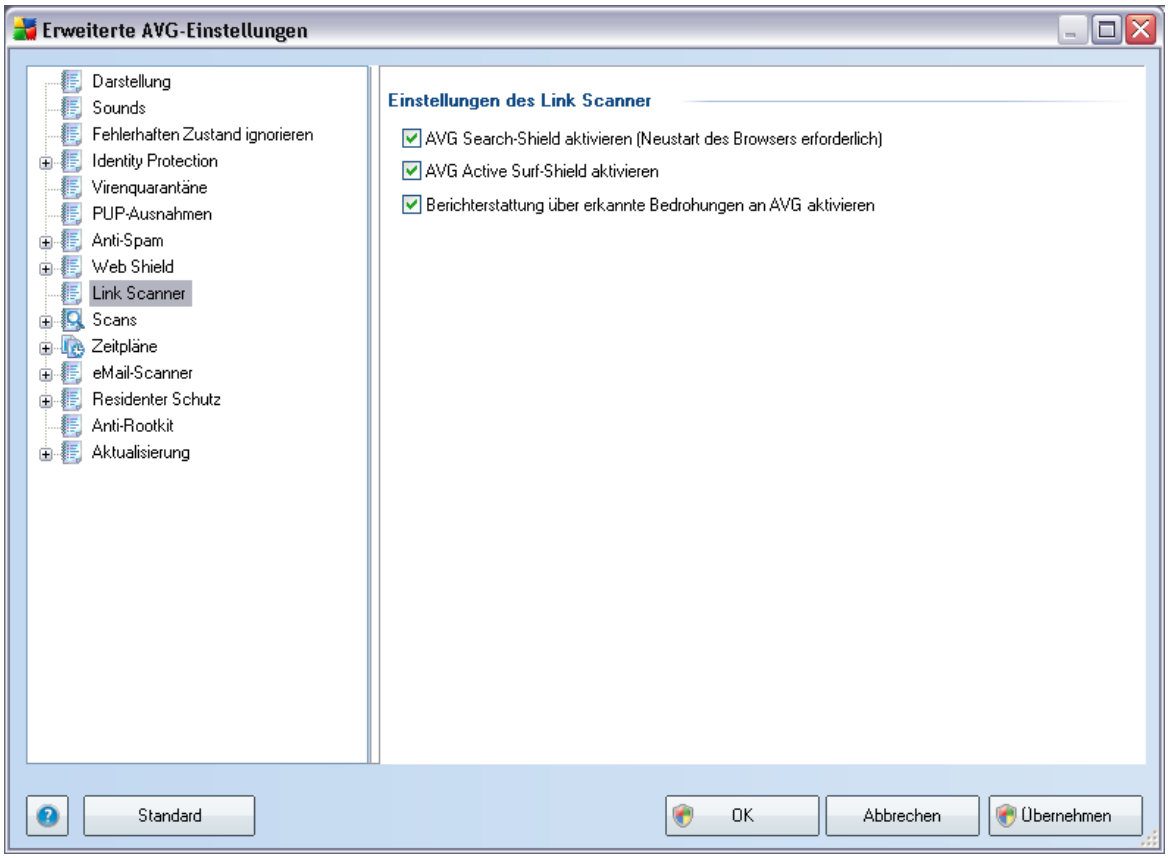


Im Dialog ***Instant Messaging-Schutz*** können Sie die Einstellungen der Komponente ***Web Shield*** im Zusammenhang mit dem Scannen von Instant Messaging bearbeiten. Momentan werden die folgenden drei Instant Messaging-Programme unterstützt: ***ICQ***, ***MSN*** und ***Yahoo*** – Aktivieren Sie die jeweiligen Einträge, wenn Sie möchten, dass ***Web Shield*** die Online-Kommunikation auf Viren überprüft.

Genaue Angaben zu zugelassenen/blockierten Benutzern können Sie im entsprechenden Dialog (***Erweiterte ICQ-Einstellungen***, ***Erweiterte MSN-Einstellungen und erweiterte Yahoo-Einstellungen***) überprüfen und bearbeiten. Sie können auch eine ***Whitelist*** (*Liste der Benutzer, die mit Ihnen kommunizieren dürfen*) sowie eine ***Blacklist*** (*Benutzer, die gesperrt werden sollen*) festlegen.

9.9. Link Scanner

Im Dialog ***Einstellungen des Link Scanner*** können Sie die Grundfunktionen von ***Link Scanner*** aktivieren oder deaktivieren:



- ***AVG Search-Shield aktivieren*** – (*standardmäßig aktiviert*): Benachrichtigungssymbole zu Suchabfragen in Google, Yahoo!, MSN oder Baidu, die darauf hinweisen, dass der Inhalt der als Suchergebnis angezeigten Websites überprüft wurde.

- ***AVG Active Surf-Shield*** aktivieren – *(standardmäßig aktiviert*): Aktiver (*Echtzeit*-) Schutz vor unbeabsichtigtem Zugriff auf Exploit-Sites. Die Verbindungsherstellung zu bekannten bösartigen Sites und deren schädlichem Inhalt wird blockiert, wenn der Benutzer diese Sites über einen Webbrowser (*oder eine andere HTTP-basierte Anwendung*) aufruft.

- ***Berichterstattung über erkannte Bedrohungen an AVG aktivieren*** – (

standardmäßig aktiviert): Aktivieren Sie diesen Eintrag, um die Rückmeldung über Exploits und bösartige Sites, die von Benutzern über ***AVG Active Surf-Shield*** oder ***AVG Search-Shield*** gefunden wurden, zu ermöglichen und so die Datenbank mit Informationen über schädliche Aktivitäten im Web zu vervollständigen.

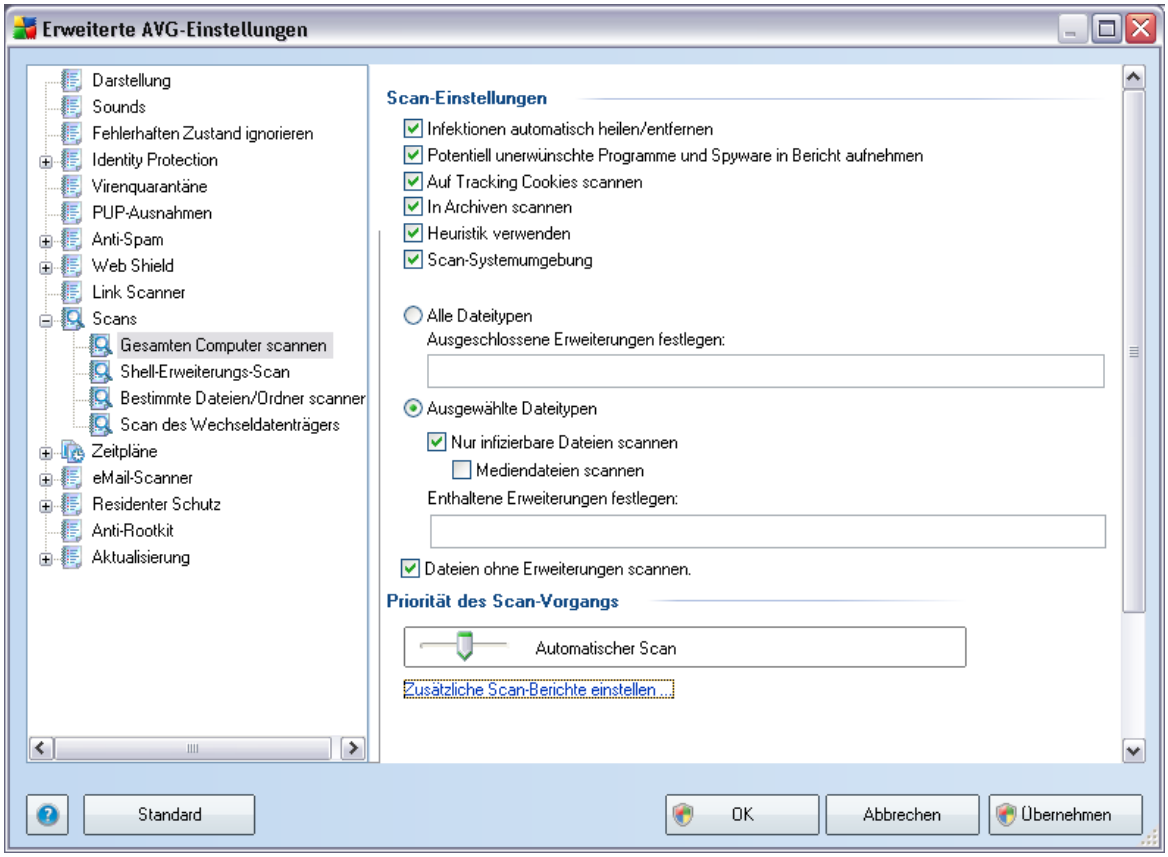
9.10. Scans

Die erweiterten Scan-Einstellungen sind in drei Kategorien eingeteilt, entsprechend den vom Software-Hersteller festgelegten Scan-Arten:

- ***Gesamten Computer scannen*** – Vordefinierter Standard-Scan des gesamten Computers
- ***Shell-Erweiterungs-Scan*** – Bestimmter Scan eines ausgewählten Objekts direkt von der Umgebung des Windows Explorer aus
- ***Bestimmte Dateien/Ordner scannen*** – Vordefinierter Standard-Scan ausgewählter Bereiche Ihres Computers
- ***Scan des Wechseldatenträgers*** – Bestimmter Scan der Wechseldatenträger, die an Ihren Computer angeschlossen sind

9.10.1. Gesamten Computer scannen

Mit der Option ***Gesamten Computer scannen*** können Sie die Parameter eines Scans bearbeiten, die vom Software-Hersteller vordefiniert wurden, ***Gesamten Computer scannen***:



Scan-Einstellungen

Im Bereich ***Scan-Einstellungen*** finden Sie eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können:

- ***Infektionen automatisch heilen/entfernen*** – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, wenn eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch geheilt werden kann oder wenn Sie diese Option deaktivieren, werden Sie über einen Virenfund unterrichtet, und Sie können entscheiden, was mit der erkannten Infektion geschehen soll. Es wird empfohlen, die infizierte Datei in die Virenquarantäne zu verschieben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – Dieser Parameter steuert die Funktion ***Anti-Virus***, mit der sich potentiell unerwünschte Programme (*ausführbare Programme, die*

Spyware oder Adware ausführen können) entdecken, blockieren oder entfernen lassen;

- ***Auf Tracking Cookies scannen*** – Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden; (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Voreinstellungen und Inhalte ihrer Warenkörbe*)

- ***In Archiven scannen*** – Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

- ***Heuristik verwenden*** – Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet;

- ***Scan-Systemumgebung*** – Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

Außerdem sollten Sie entscheiden, welche Elemente gescannt werden

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen; oder

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

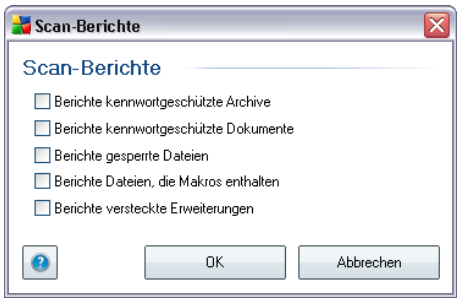
- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

Priorität des Scan-Vorgangs

Im Bereich ***Priorität des Scan-Vorgangs*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf eine mittlere Höhe der automatischen Ressourcennutzung eingestellt. Wenn der Scan schneller ausgeführt werden soll, nimmt der Scan weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan ist aber deutlich erhöht, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*Diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber niemand daran arbeitet*). Auf der anderen Seite können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

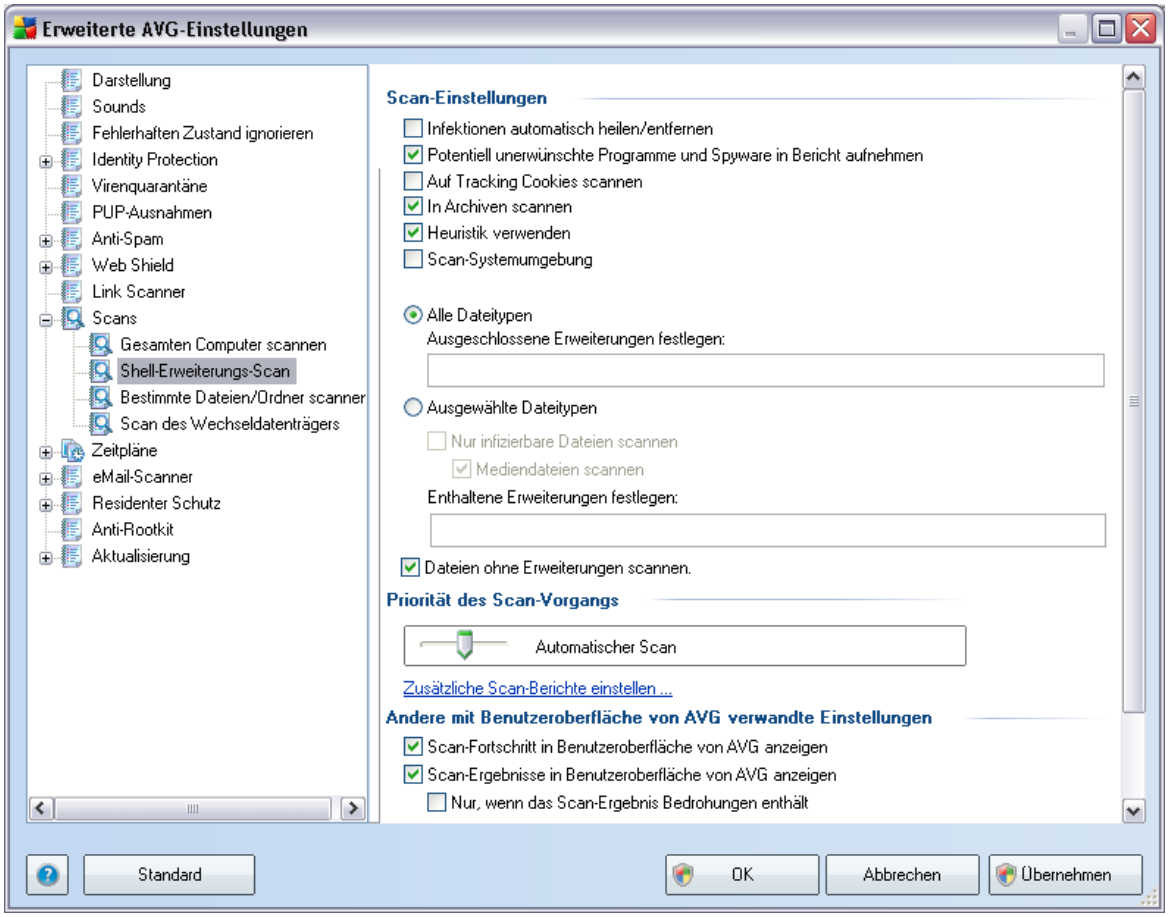
Zusätzliche Scan-Berichte einstellen ...

Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen ...***, um den separaten Dialog ***Scan-Berichte*** zu öffnen, wo Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



9.10.2. Shell-Erweiterungs-Scan

Ähnlich der vorhergehenden Option ***Gesamten Computer scannen*** enthält das Element ***Shell-Erweiterungs-Scan*** verschiedene Optionen zum Bearbeiten des vom Software-Hersteller vordefinierten Scans. Hier bezieht sich die Konfiguration auf das Scannen von bestimmten Objekten, das direkt von der Umgebung des Windows Explorer aus gestartet wird (*Shell-Erweiterung*). Siehe Kapitel ***Scans aus dem Windows Explorer***:

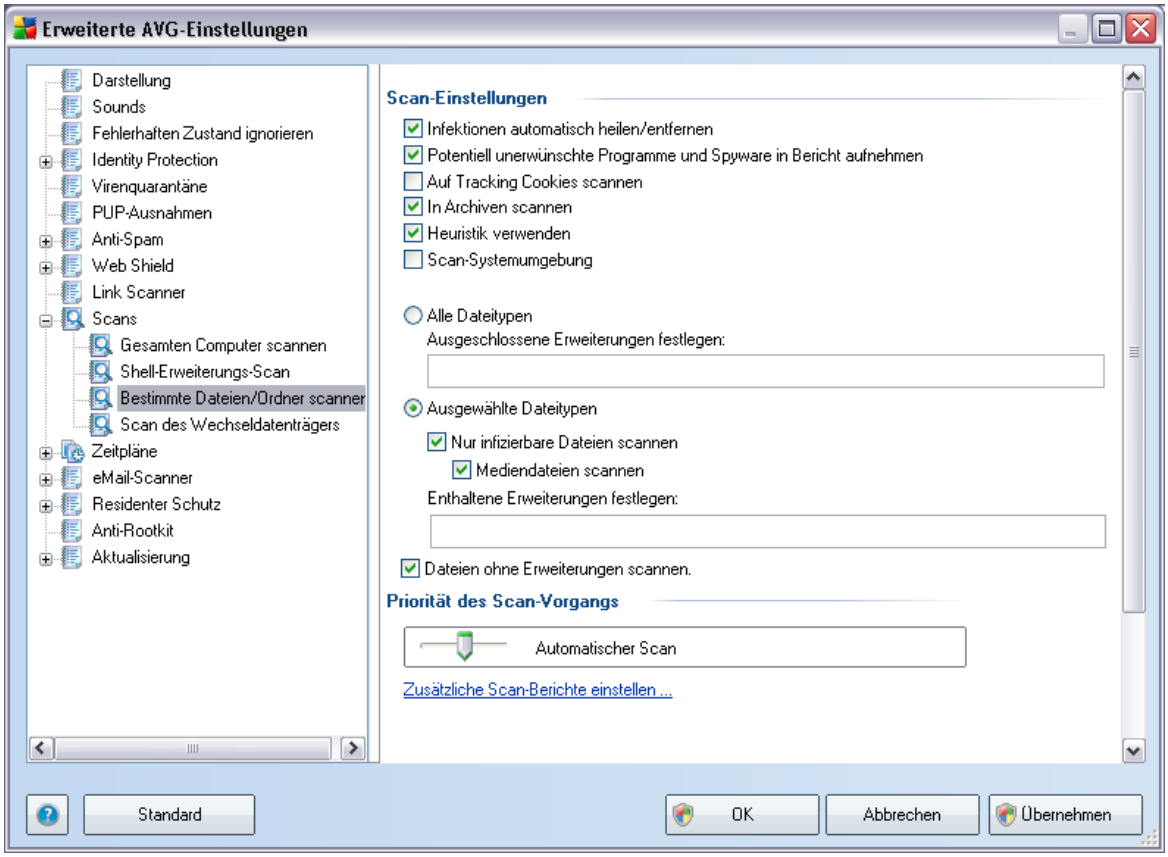


Die Parameterliste stimmt mit der Parameterliste der Option ***Gesamten Computer scannen*** überein. Die Standardeinstellungen unterscheiden sich jedoch: Während bei·***Gesamten Computer scannen*** die meisten Parameter ausgewählt sind, sind beim ***Shell-Erweiterungs-Scan*** (***Scans aus dem Windows Explorer***) nur die wichtigsten Parameter aktiviert.

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***AVG Erweiterte Einstellungen / Gesamten Computer scannen****.*

9.10.3. Bestimmte Dateien/Ordner scannen

Die Bearbeitungsoberfläche für die Option ***Bestimmte Dateien/Ordner scannen*** stimmt mit dem Bearbeitungsdialog der Option ***Gesamten Computer scannen*** überein. Alle Konfigurationsoptionen sind gleich; die Standardeinstellungen für die Option ***Gesamten Computer scannen*** sind jedoch strenger:

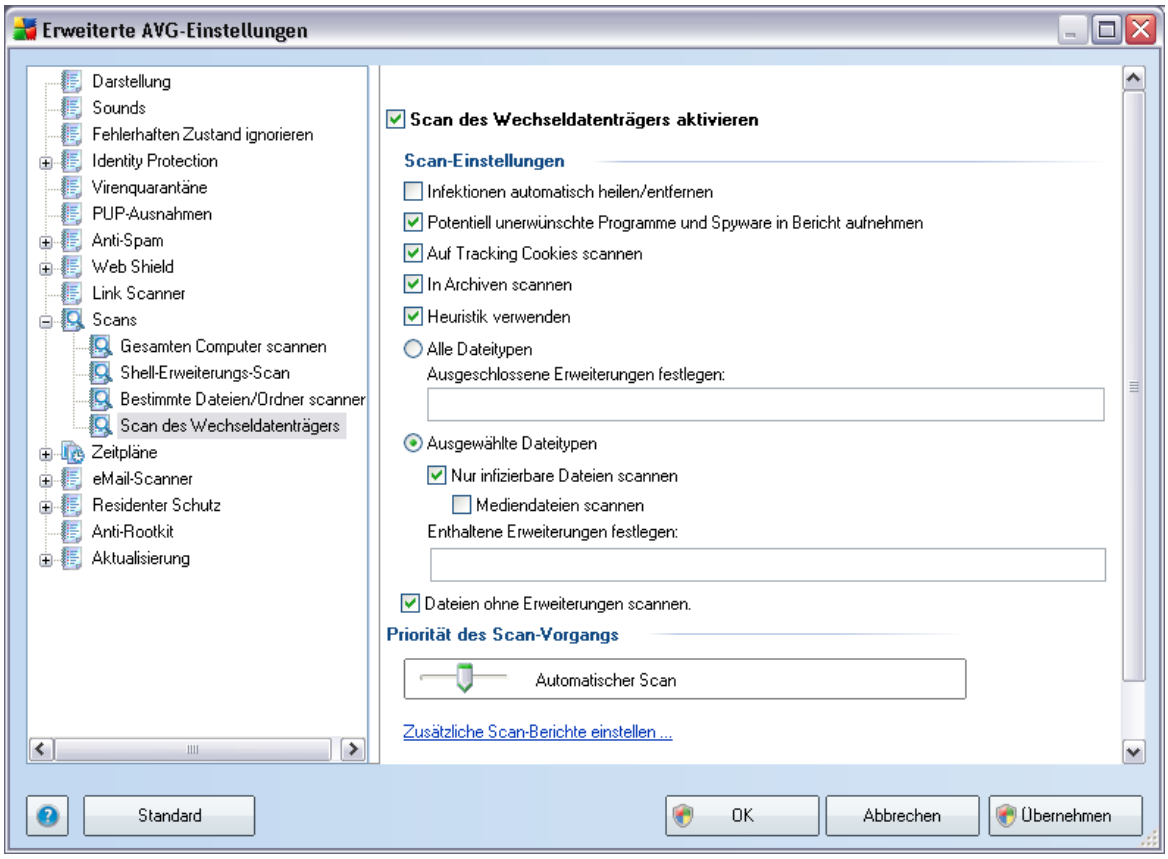


Alle Parameter, die in diesem Konfigurationsdialog festgelegt werden, gelten nur für die Scan-Bereiche, die unter der Option ***Bestimmte Dateien/Ordner scannen*** ausgewählt wurden! Wenn Sie die Option ***Auf Rootkits scannen*** in diesem Konfigurationsdialog aktivieren, wird lediglich ein schneller Rootkit-Test durchgeführt, d. h. nur ausgewählte Bereiche werden gescannt.

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***AVG Erweiterte Einstellungen / Gesamten Computer scannen***.

9.10.4. Scan des Wechseldatenträgers

Die Bearbeitungsoberfläche für die Option ***Scan des Wechseldatenträgers*** ist auch dem Bearbeitungsdialog der Option ***Gesamten Computer scannen*** sehr ähnlich:



Der ***Scan des Wechseldatenträgers*** wird automatisch gestartet, sobald Sie einen Wechseldatenträger an Ihren Computer anschließen. Standardmäßig ist der Scan deaktiviert. Es ist jedoch entscheidend, Wechseldatenträger auf potentielle Bedrohungen zu scannen, da diese die Hauptquelle von Infektionen sind. Aktivieren Sie das Kontrollkästchen ***Scan des Wechseldatenträgers aktivieren***, damit dieser Scan bereit ist und bei Bedarf automatisch gestartet werden kann.

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***AVG Erweiterte Einstellungen / Gesamten Computer scannen****.*

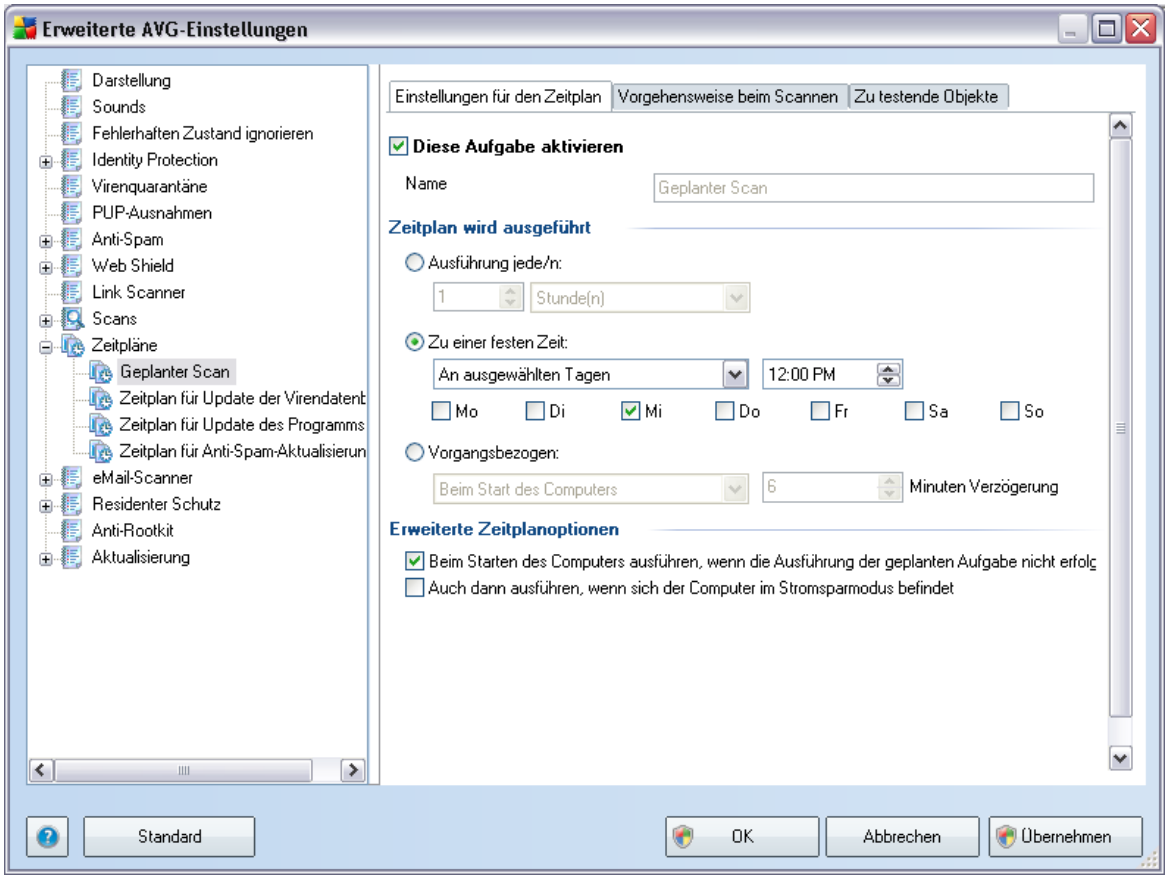
9.11. Zeitpläne

Im Bereich ***Zeitpläne*** können Sie die Standardeinstellungen für folgende Zeitpläne bearbeiten:

- Zeitplan für Scans des gesamten Computers
- Zeitplan für Update der Virendatenbank
- Zeitplan für Update des Programms
- Zeitplan für Anti-Spam-Aktualisierung

9.11.1. Geplanter Scan

Auf drei Reitern können die Parameter für den geplanten Scan bearbeitet (*oder ein neuer Zeitplan erstellt*) werden:



Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um den geplanten Scan vorübergehend zu deaktivieren. Anschließend können Sie den Zeitplan bei Bedarf wieder aktivieren.

Das Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) enthält den vom Programmhersteller zugewiesenen Namen für diesen Zeitplan. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag* ***Zeitplan für Update des Programms*** *klicken*) können Sie einen eigenen Namen angeben; in diesem Fall kann das Textfeld bearbeitet werden. Wählen Sie nach Möglichkeit kurze, beschreibende Namen für Ihre Scans, damit Sie die einzelnen Scans später leicht unterscheiden und wiederfinden können.

Beispiel: *Sie sollten einen Scan nicht „Neuer Scan" oder „Mein Scan" nennen, da*

diese Namen nichts darüber aussagen, was der Scan tatsächlich überprüft. Ein Beispiel für einen guten, beschreibenden Namen wäre andererseits „Scan von Systembereichen" usw. Es ist auch nicht erforderlich, im Namen des Scans anzugeben, ob es sich um einen Scan des gesamten Computers handelt oder lediglich um den Scan bestimmter Dateien oder Ordner. Ihre eigenen Scans sind immer bestimmte Versionen eines Scans bestimmter Dateien oder Ordner.

In diesem Dialog können Sie weiterhin folgende Parameter für den Scan festlegen:

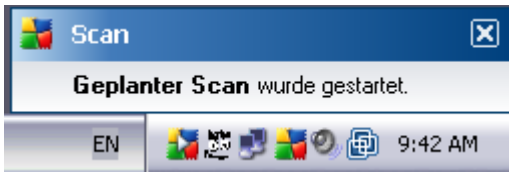
Zeitplan wird ausgeführt

Hier können Sie die Zeitintervalle für den Start des neu geplanten Scans festlegen. Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum (***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Scans auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

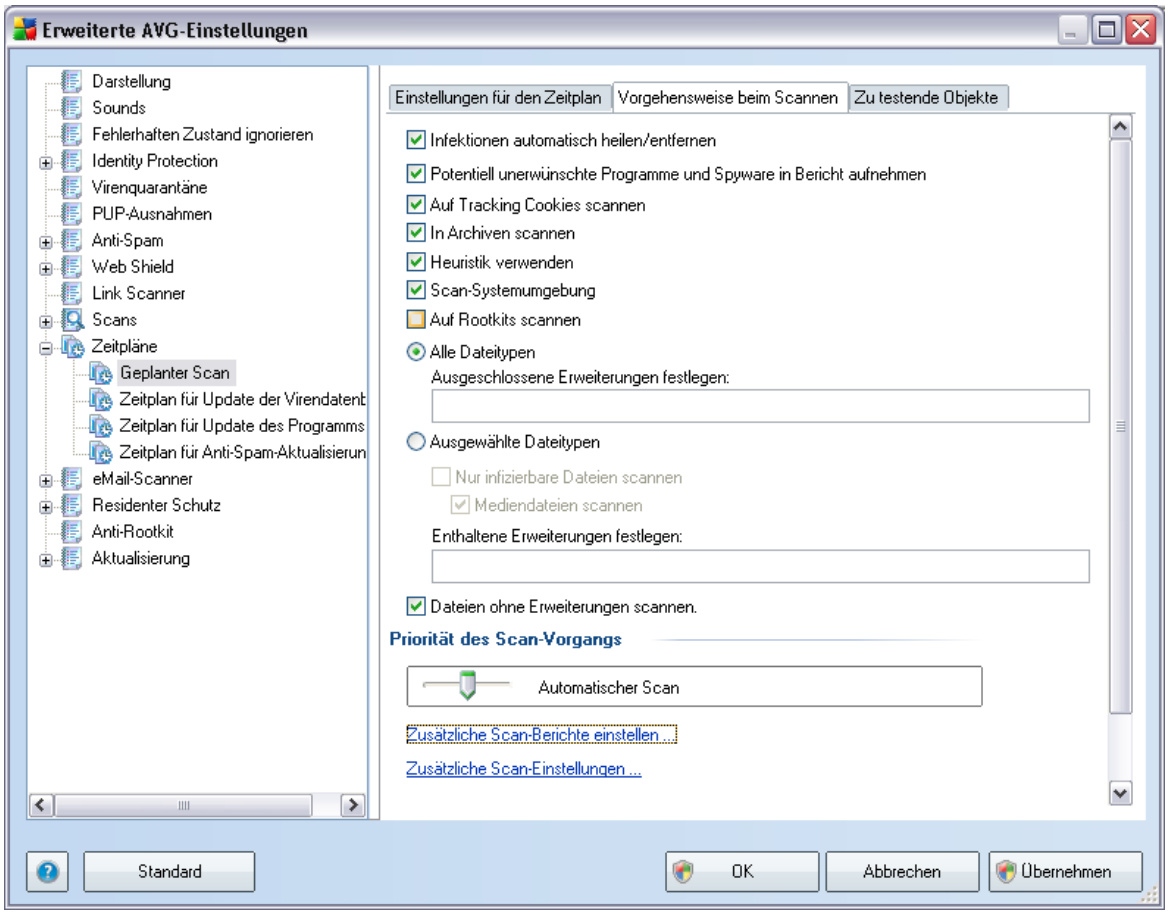
Erweiterte Zeitplanoptionen

In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist.

Sobald der geplante Scan zu der von Ihnen festgelegten Zeit startet, werden Sie über ein Popup-Fenster darüber informiert, das über dem AVG-Symbol im Infobereich geöffnet wird:



Daraufhin wird ein neues AVG-Symbol im Infobereich angezeigt (*in Vollfarbe und mit einem weißen Pfeil – siehe Abbildung oben*), das Sie darauf hinweist, dass gerade ein geplanter Scan durchgeführt wird. Klicken Sie während des Scanvorgangs mit der rechten Maustaste auf das AVG-Symbol. Daraufhin wird ein Kontextmenü geöffnet, über das Sie den laufenden Scan unterbrechen oder auch anhalten können:



Der Reiter ***Vorgehensweise beim Scannen*** enthält eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. Standardmäßig sind die meisten Parameter aktiviert und ihre Funktionen werden während des Scans angewandt. Wenn Sie keinen wichtigen Grund haben, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten:

- ***Infektionen automatisch heilen/entfernen*** – (*standardmäßig aktiviert*): Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch

geheilt, wenn eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch geheilt werden kann oder wenn Sie diese Option deaktivieren, werden Sie über einen Virenfund unterrichtet, und Sie können entscheiden, was mit der erkannten Infektion geschehen soll. Es wird empfohlen, die infizierte Datei in die Virenquarantäne zu verschieben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert*): Mit diesem Parameter können Sie die Funktion Anti-Virus verwalten, mit der sich potentiell unerwünschte Programme (*ausführbare Dateien, die Spyware oder Adware ausführen können*) erkennen, blockieren und entfernen lassen;

- ***Auf Tracking Cookies scannen*** – (*standardmäßig aktiviert*): Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen; (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und zum Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Voreinstellungen für Websites und Inhalte ihrer Warenkörbe*)

- ***In Archiven scannen*** – (*standardmäßig aktiviert*): Dieser Parameter legt fest, dass Scans alle Dateien überprüfen sollen, selbst wenn sie in Archiven wie ZIP, RAR usw. gespeichert sind.

- ***Heuristik verwenden*** – (*standardmäßig aktiviert*): Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet;

- ***Scan-Systemumgebung*** – (*standardmäßig aktiviert*): Beim Scan werden auch die Systembereiche Ihres Computers überprüft;

- ***Auf Rootkits scannen*** – Aktivieren Sie diese Option, wenn die Rootkit-Erkennung während des Scans des gesamten Computers durchgeführt werden soll. Die Rootkit-Erkennung kann über die Komponente ***Anti-Rootkit*** auch separat durchgeführt werden;

Außerdem sollten Sie entscheiden, welche Elemente gescannt werden

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen; oder

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien –*

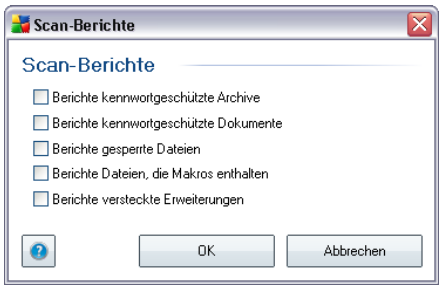
wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

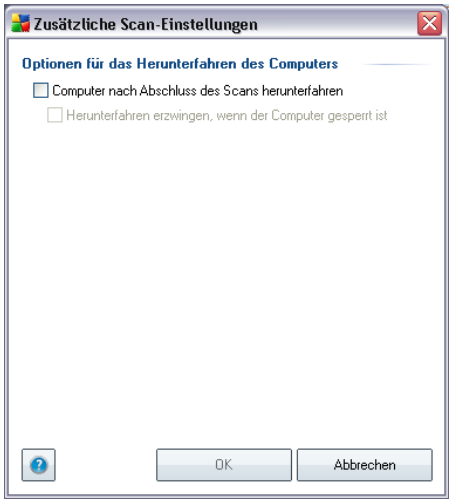
Priorität des Scan-Vorgangs

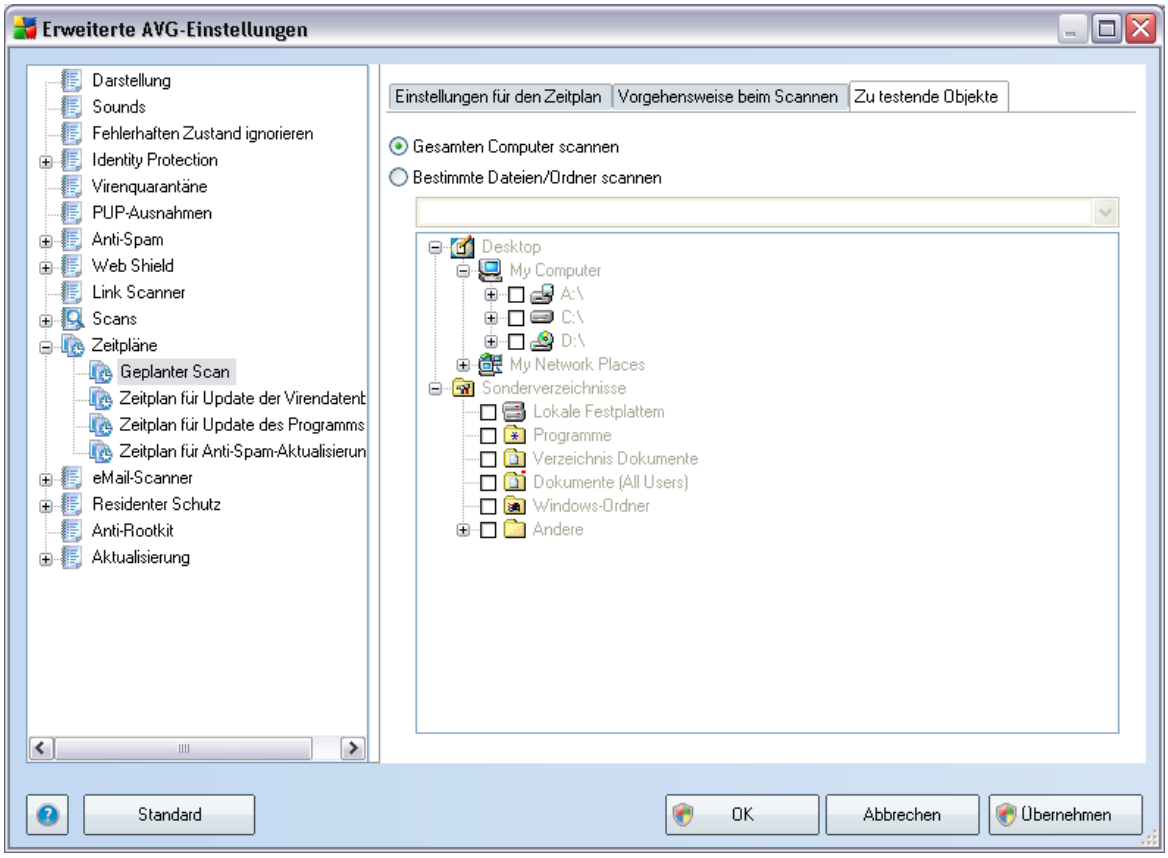
Im Bereich ***Priorität des Scan-Vorgangs*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist diese Option auf eine mittlere Höhe der automatischen Ressourcennutzung eingestellt. Wenn der Scan schneller ausgeführt werden soll, nimmt der Scan zwar weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan liegt aber deutlich höher, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*Diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber niemand daran arbeitet*). Auf der anderen Seite können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen ...***, um den separaten Dialog ***Scan-Berichte*** zu öffnen, wo Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



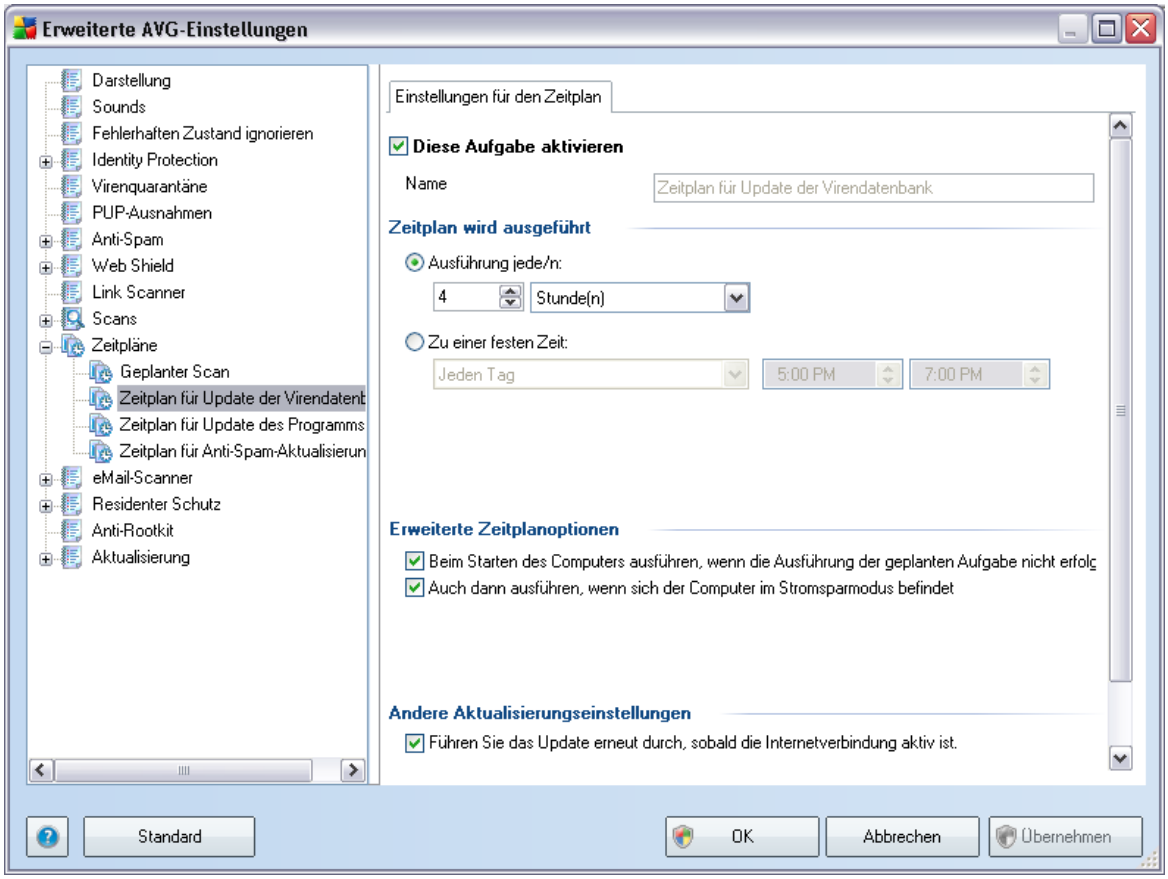
Klicken Sie auf ***Zusätzliche Scan-Einstellungen***, um einen neuen Dialog aufzurufen, in dem Sie Optionen für das Herunterfahren des Computers ***wählen können***. Legen Sie dort fest, ob der Computer nach dem Scan automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).


Zusätzliche Scan-Einstellungen
Optionen für das Herunterfahren des Computers
Computer nach Abschluss des Scans herunterfahren
Herunterfahren erzwingen, wenn der Computer gesperrt ist
OK
Abbrechen


Erweiterte AVG-Einstellungen
Darstellung
Sounds
Fehlerhaften Zustand ignorieren
Identity Protection
Virenquarantäne
PUP-Ausnahmen
Anti-Spam
Web Shield
Link Scanner
Scans
Zeitpläne
Geplanter Scan
Zeitplan für Update der Virendatenb
Zeitplan für Update des Programms
Zeitplan für Anti-Spam-Aktualisierun
eMail-Scanner
Residenter Schutz
Anti-Rootkit
Aktualisierung
Einstellungen für den Zeitplan
Vorgehensweise beim Scannen
Zu testende Objekte
Gesamten Computer scannen
Bestimmte Dateien/Ordner scannen
Desktop
My Computer
A:\
C:\
D:\
My Network Places
Sonderverzeichnisse
Lokale Festplattem
Programme
Verzeichnis Dokumente
Dokumente (All Users)
Windows-Ordner
Andere
Standard
OK
Abbrechen
Übernehmen

Auf dem Reiter ***Zu testende Objekte*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien/Ordner scannen planen möchten. Wenn Sie die Option „Bestimmte Dateien oder Ordner scannen" auswählen, wird im unteren Bereich dieses Dialogs die angezeigte Baumstruktur aktiviert, und Sie können die zu scannenden Ordner festlegen.

9.11.2. Zeitplan für Update der Virendatenbank



Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um das geplante Update der Virendatenbank vorübergehend zu deaktivieren. Anschließend können Sie den Zeitplan bei Bedarf hier wieder aktivieren.

Der grundlegende Aktualisierungszeitplan der Virendatenbank erfolgt über die Komponente ***Updatemanager***. In diesem Dialog können Sie verschiedene Parameter des Aktualisierungszeitplans der Virendatenbank im Detail festlegen:

Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag* ***Zeitplan für Update der Virendatenbank*** *klicken*) können Sie einen eigenen Namen festlegen, den Sie in das entsprechende Textfeld eingeben. Versuchen Sie, Ihren Zeitplänen kurze, beschreibende Namen zu geben, um sie später leicht wiedererkennen zu können.

Zeitplan wird ausgeführt

Legen Sie in diesem Bereich die Zeitintervalle fest, in denen das neu geplante Update der Virendatenbank durchgeführt werden soll. Sie können entweder wiederholte Starts des Updates nach einem bestimmten Zeitraum (***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Updates auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

Erweiterte Zeitplanoptionen

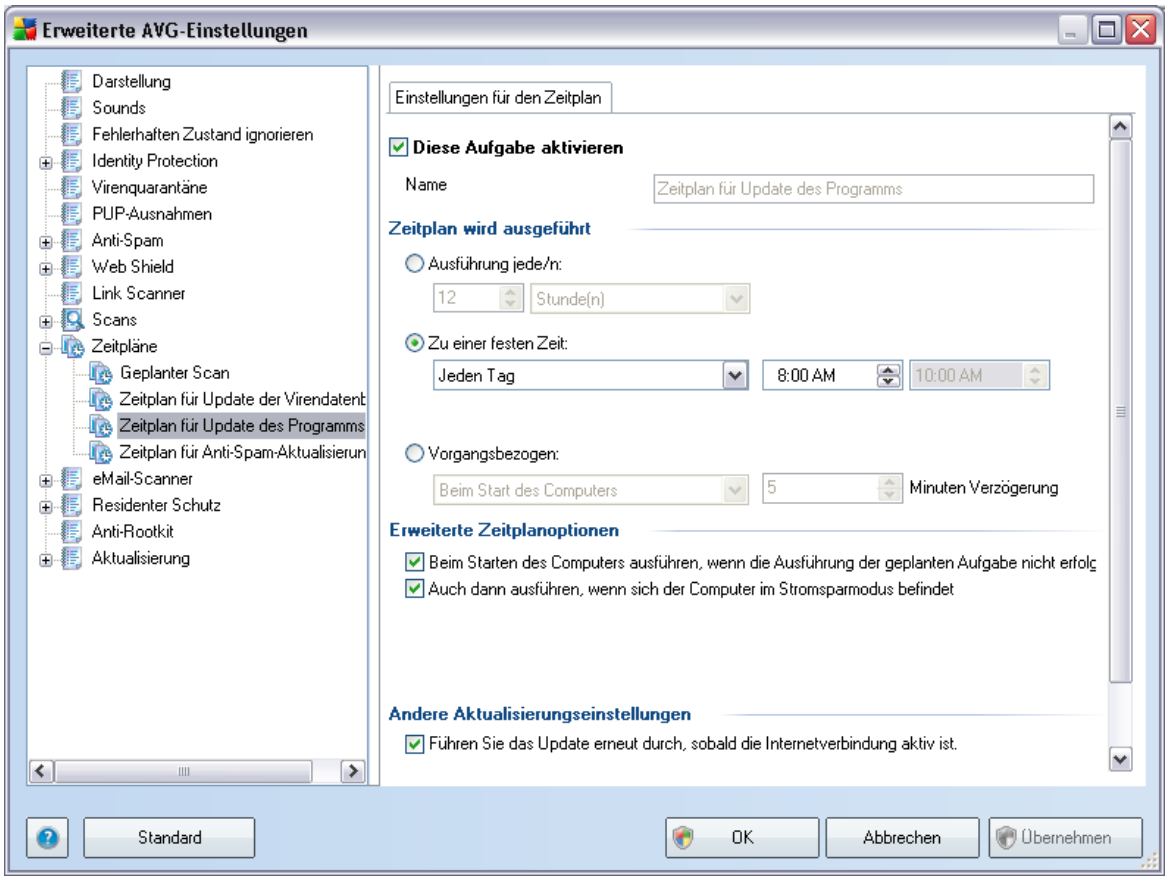
In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen die Virendatenbank aktualisiert werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder ganz ausgeschaltet ist).

Andere Aktualisierungseinstellungen

Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung neu gestartet wird.

Sobald das geplante Update zu der von Ihnen festgelegten Zeit startet, werden Sie in einem Popup-Fenster darüber informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog* ***Erweiterte Einstellungen/Darstellung*** *beibehalten)*.

9.11.3. Zeitplan für Update des Programms



Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um auf einfache Weise das geplante Programm-Update vorübergehend z.B. zu deaktivieren. Anschließend können Sie den Updatezeitplan bei Bedarf hier wieder aktivieren.

Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) befindet sich der Name, den der Zeitplan vom Programmhersteller erhalten hat. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag* ***Zeitplan für Update des Programms*** *klicken*) können Sie Ihren eigenen Namen angeben; in diesem Fall kann das Textfeld bearbeitet werden. Versuchen Sie, Ihren Zeitplänen kurze, beschreibende Namen zu geben, um sie später leicht wiedererkennen zu können.

Zeitplan wird ausgeführt

Legen Sie hier die Zeitintervalle für das Ausführen des neu geplanten Programmupdates fest. Sie können entweder wiederholte Starts des Updates nach einem bestimmten Zeitraum (***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Updates auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

Erweiterte Zeitplanoptionen

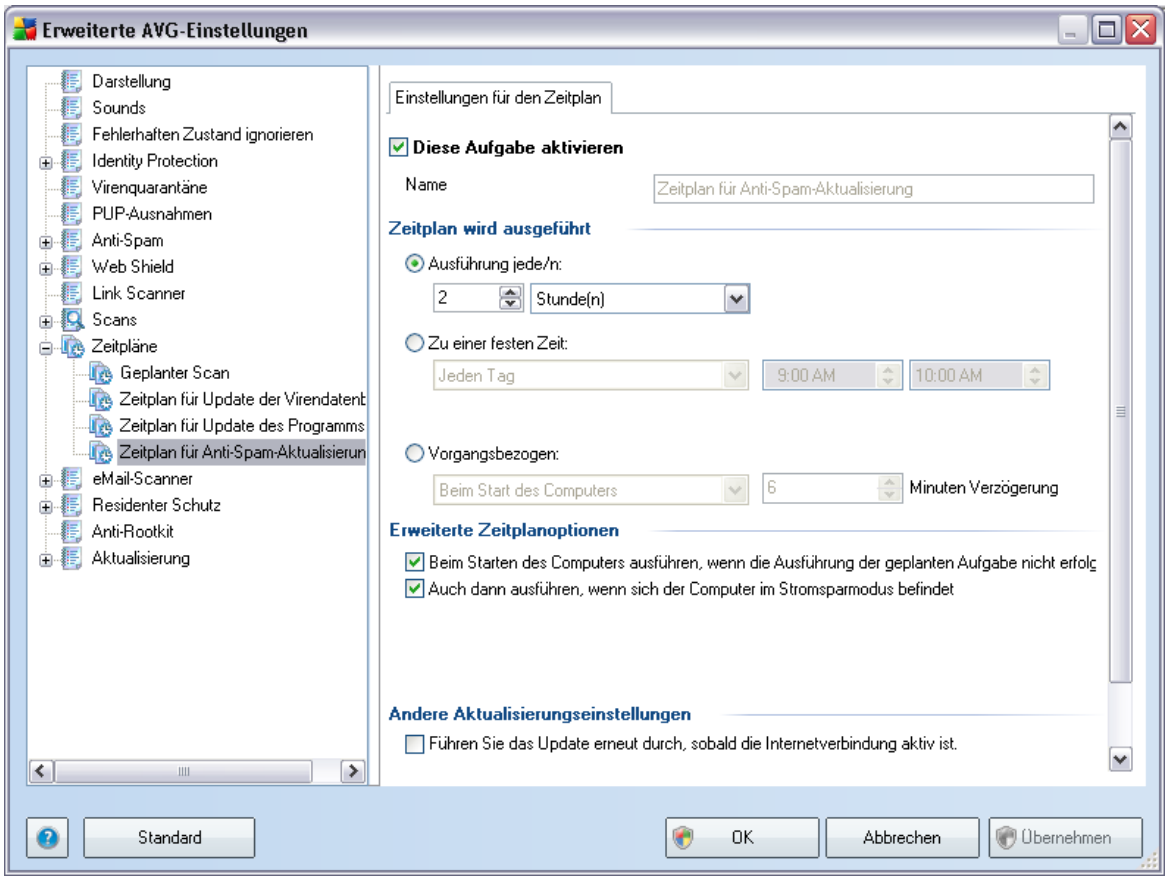
In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen das Programmupdate gestartet werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder komplett ausgeschaltet ist).

Andere Aktualisierungseinstellungen

Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung erneut gestartet wird.

Sobald das geplante Update zu der von Ihnen festgelegten Zeit startet, werden Sie in einem Popup-Fenster darüber informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog* ***Erweiterte Einstellungen/Darstellung*** *beibehalten)*.

9.11.4. Zeitplan für Anti-Spam-Aktualisierung



Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um das geplante Update von ***Anti-Spam*** ***vorübergehend zu deaktivieren. Anschließend können Sie den Updatezeitplan bei Bedarf hier wieder aktivieren.***

Die grundlegende Updateplanung für ***Anti-Spam*** erfolgt über die Komponente ***Updatemanager***. In diesem Dialog können Sie genauere Parameter für den Updatezeitplan festlegen:

Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) sehen Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag* ***Zeitplan für Anti-Spam-Update*** *klicken*) können Sie einen eigenen Namen festlegen und in das entsprechende Textfeld eingeben. Versuchen Sie, für Ihre Zeitpläne kurze,

beschreibende Namen zu verwenden, die sie später leicht wiedererkennen zu können.

Zeitplan wird ausgeführt

Geben Sie hier die Zeitabstände für den neu geplanten Start der Updates von ***Anti-Spam*** an. Sie können entweder wiederholte Updates von ***Anti-Spam*** nach einem bestimmten Zeitraum (***Ausführung jede/n ...***) oder ein bestimmtes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das ein Update auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

Erweiterte Zeitplanoptionen

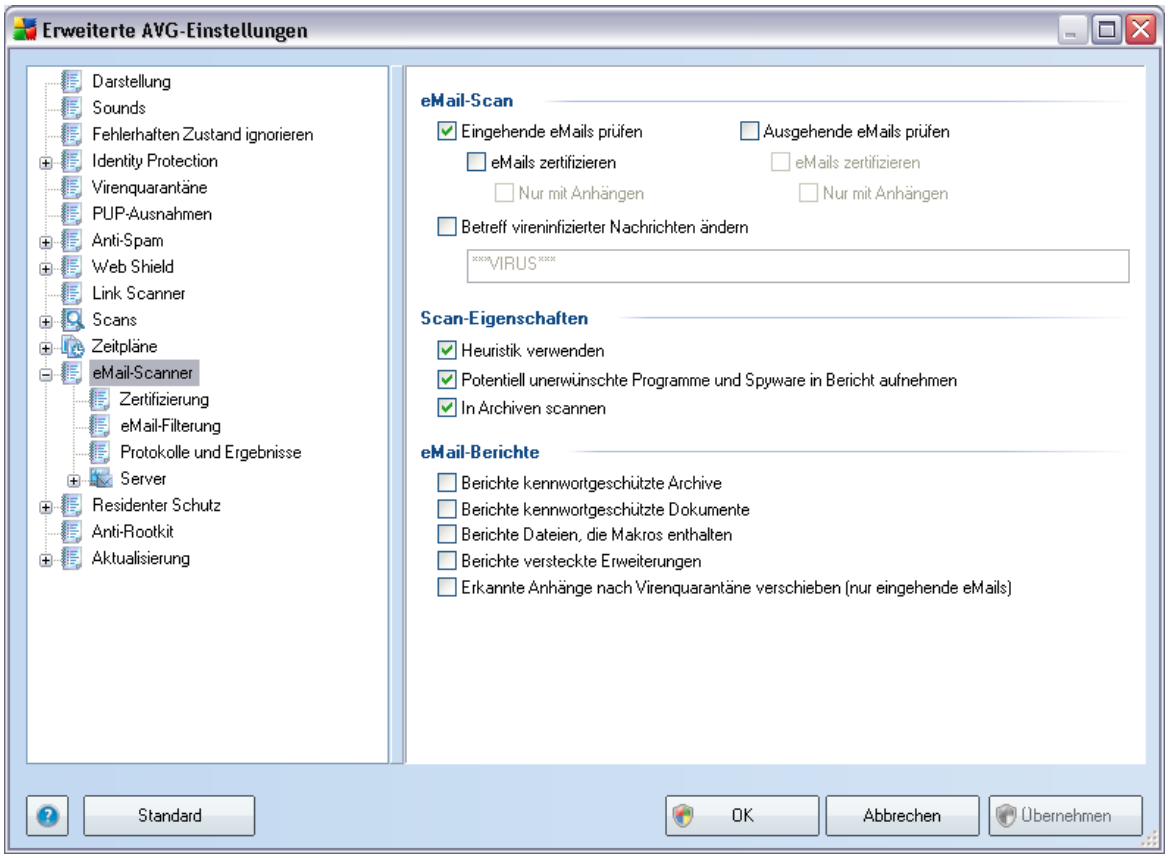
In diesem Bereich können Sie festlegen, unter welchen Bedingungen das Update von ***Anti-Spam*** gestartet oder nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder ganz ausgeschaltet ist.

Andere Aktualisierungseinstellungen

Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Updates von ***Anti-Spam*** das Update sofort nach der Wiederherstellung der Internetverbindung neu gestartet wird.

Sobald der geplante Scan zu der von Ihnen festgelegten Zeit startet, werden Sie über ein Popup-Fenster darüber informiert, das sich über dem AVG-Symbol im Infobereich öffnet (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog* ***Erweiterte Einstellungen/Darstellung*** *beibehalten)*.

9.12. eMail-Scanner



Der Dialog ***eMail-Scanner*** ist in drei Bereiche unterteilt:

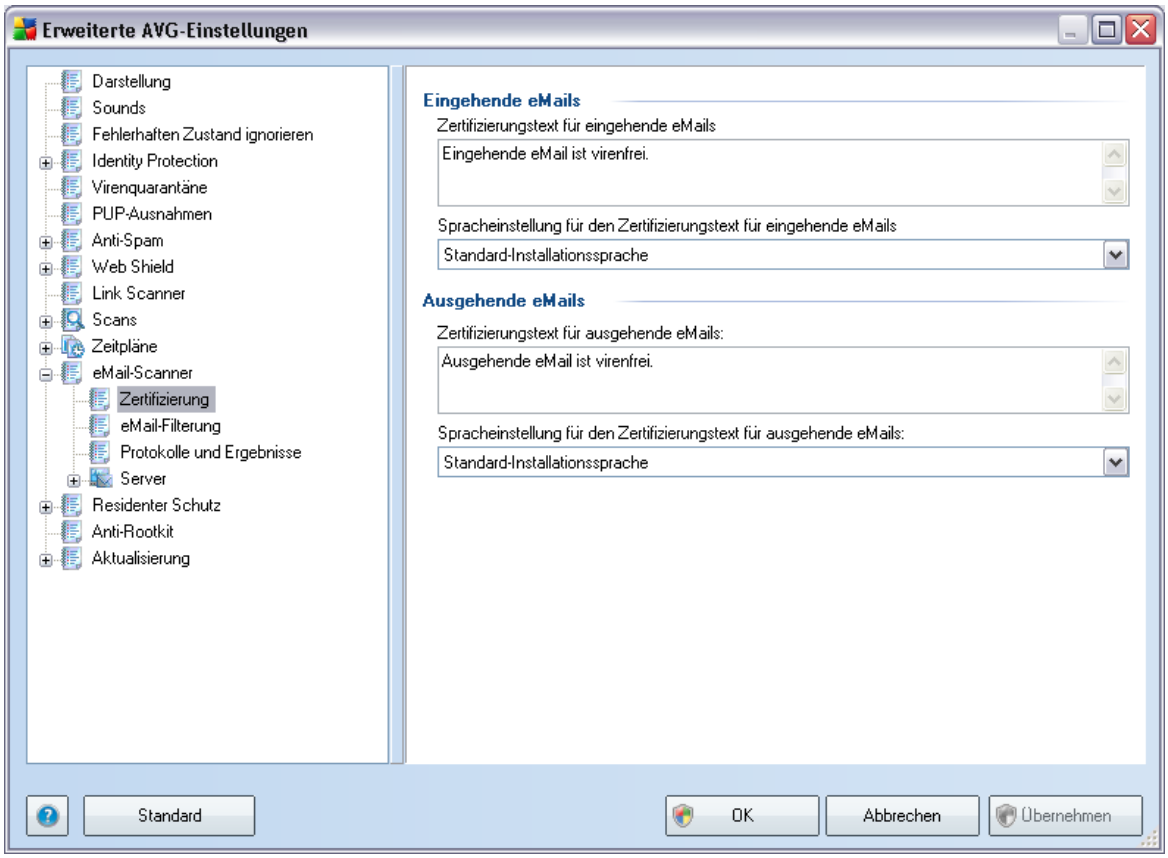
- ***eMail-Scan*** – In diesem Bereich können Sie auswählen, ob eingehende/ausgehende eMail-Nachrichten gescannt werden sollen und ob alle eMails oder nur eMails mit Anhang zertifiziert werden sollen (*die Zertifizierung von eMails als virenfrei wird im Format HTML/RTF nicht unterstützt*). Zusätzlich können Sie auswählen, ob AVG den Betreff für Nachrichten, die potentielle Viren enthalten, ändern soll. Markieren Sie das Kontrollkästchen ***Betreff vireninfizierter Nachrichten ändern*** und ändern Sie den Text nach Bedarf (*voreingestellt ist: ***VIRUS****).

- ***Scan-Eigenschaften*** – Legen Sie fest, ob beim Scannen eine heuristische Analyse zum Einsatz kommen soll (***Heuristische Methode verwenden***), nach potentiell unerwünschten Programmen gesucht werden soll (***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen***) und ob

Archive überprüft werden sollen (***In Archiven scannen***).

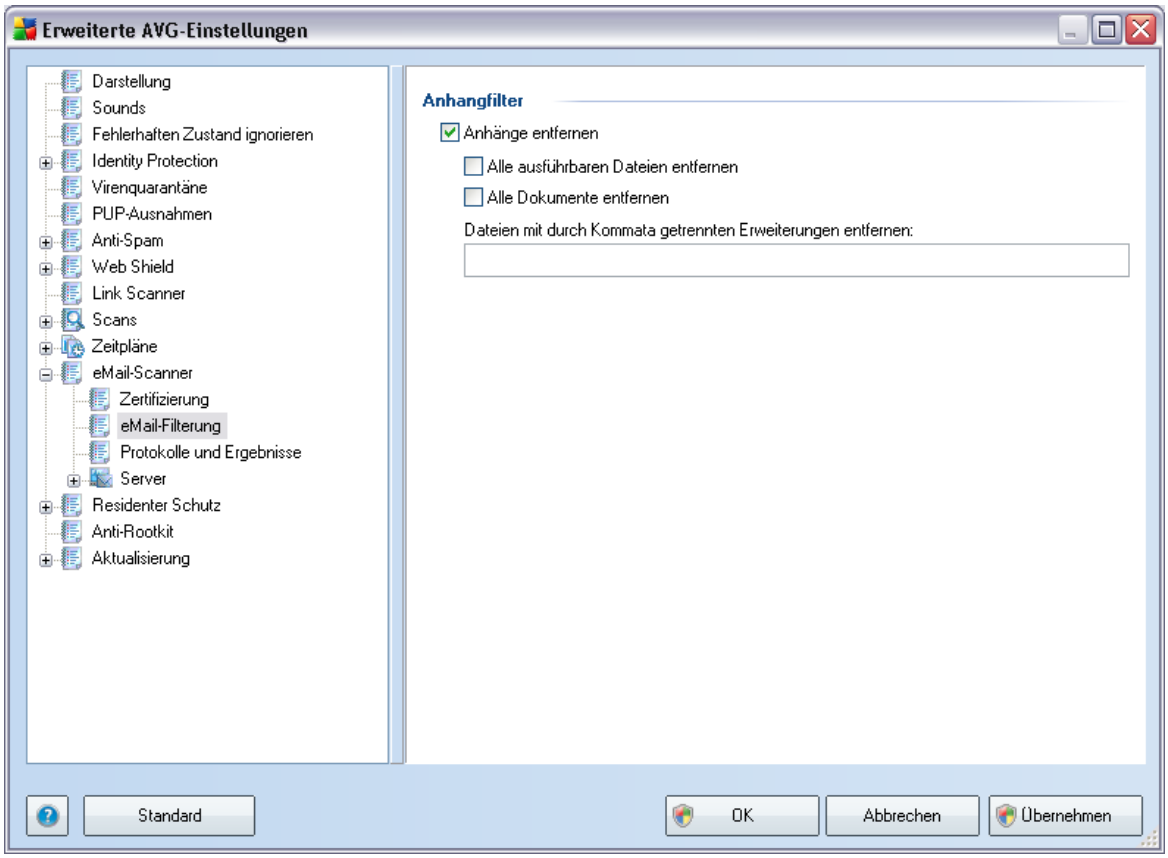
- ***eMail-Berichte*** – Geben Sie an, ob Sie per eMail über kennwortgeschützte Archive, kennwortgeschützte Dokumente, Dateien mit Makros und/oder Dateien mit versteckter Erweiterung benachrichtigt werden möchten, die als Anhang der gescannten eMail-Nachricht erkannt wurden. Wird eine solche Nachricht während des Scans identifiziert, geben Sie an, ob das erkannte infektiöse Objekt in die ***Virenquarantäne*** verschoben werden soll.

9.12.1. Zertifizierung



Im Dialog ***Zertifizierung*** können Sie genau angeben, welchen Text der Zertifizierungshinweis enthalten soll und in welcher Sprache er angezeigt werden soll. Definieren Sie einen separaten Text für ***eingehende eMails*** und ***ausgehende eMails***.

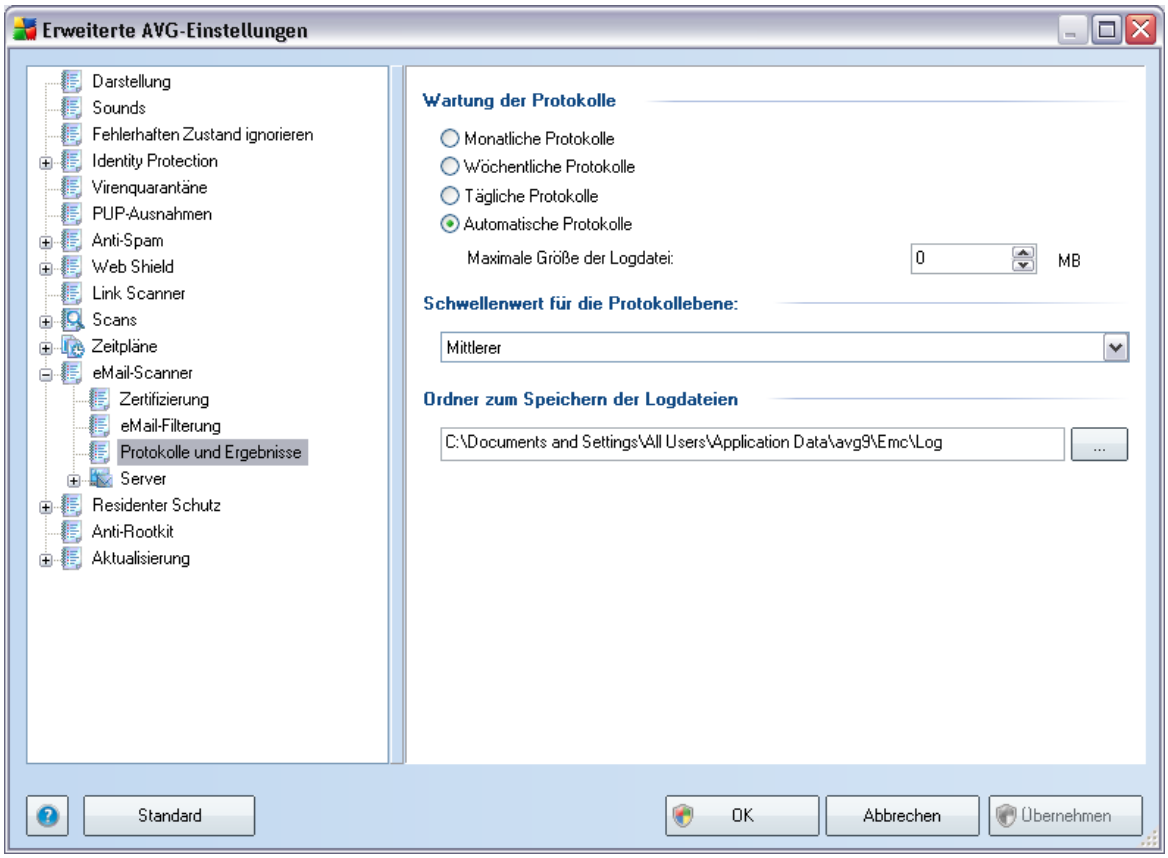
9.12.2. eMail-Filterung



Im Dialog ***Anhangfilter*** können Sie Parameter für das Scannen von eMail-Anhängen festlegen. Standardmäßig ist die Option ***Anhänge entfernen*** deaktiviert. Wenn Sie die Option aktivieren, werden alle eMail-Anhänge, die als infektiös oder potentiell gefährlich erkannt werden, automatisch entfernt. Wenn Sie möchten, dass nur bestimmte Arten von Anhängen entfernt werden, wählen Sie die entsprechende Option aus:

- ***Alle ausführbaren Dateien entfernen*** – Alle Dateien des Typs *.exe werden gelöscht
- ***Alle Dokumente entfernen*** – Alle Dateien des Typs *.doc werden gelöscht
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Alle Dateien mit den definierten Erweiterungen werden entfernt

9.12.3. Protokolle und Ergebnisse

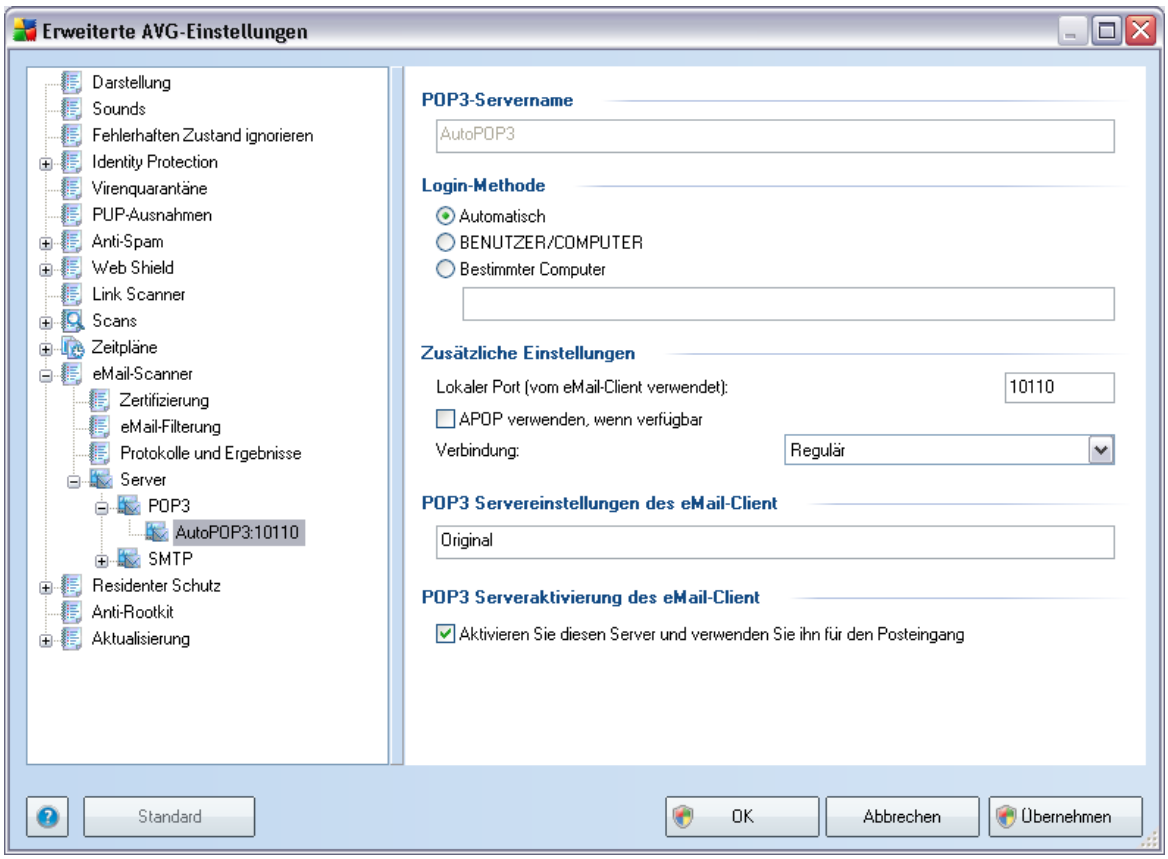


Im Dialog, der über das Navigationselement ***Protokolle und Ergebnisse*** geöffnet wird, können Sie Parameter für die Wartung von Ergebnissen des eMail-Scans festlegen. Der Dialog ist in mehrere Bereiche gegliedert.

- ***Wartung der Protokolle*** – Legen Sie fest, ob Informationen über eMail-Scans täglich, wöchentlich, monatlich ... protokolliert werden sollen und wie groß die Protokolldatei maximal sein darf (*in MB*)
- ***Schwellenwert für die Protokollebene*** – Standardmäßig ist die mittlere Ebene eingestellt – Sie können jedoch eine niedrigere Ebene (*Protokollierung von grundlegenden Verbindungsinformationen*) oder eine höhere Ebene (*Protokollierung des gesamten Datenverkehrs*) einstellen
- ***Ordner zum Speichern der Logdateien*** – Geben Sie an, wo die Logdatei gespeichert werden soll

9.12.4. Server

Im Bereich ***Server*** können Sie die Parameter der Server der Komponente ***eMail-Scanner*** bearbeiten oder mit Hilfe der Schaltfläche ***Neuen Server hinzufügen*** einen neuen Server einrichten.



In diesem Dialog (zu öffnen über ***Server / POP3***) können Sie einen neuen ***eMail-Scanner***-Server einrichten, der das POP3-Protokoll für eingehende eMails verwenden soll:

- ***POP3-Servername*** – Geben Sie den Namen des Servers ein, oder behalten Sie den Standardnamen AutoPOP3 bei
- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für eingehende eMails bestimmt werden soll:

- ***Automatisch*** – Die Anmeldung erfolgt den Einstellungen Ihres eMail-Programms entsprechend automatisch.

- ***BENUTZER/COMPUTER*** – Die einfachste und am häufigsten verwendete Methode zur Bestimmung des Ziel-Mailservers ist die Proxy-Methode. Um diese Methode zu verwenden, geben Sie Name oder Adresse (oder auch den Port) als Teil des Anmelde-Benutzernamens für den betreffenden Mailserver an, wobei die beiden Parameter durch das Zeichen / voneinander abgetrennt sind. Für das Konto Benutzer1 auf dem Server pop.acme.com und den Port 8200 beispielsweise würden Sie Benutzer1/pop.acme.com:8200 als Anmeldename verwenden.

- ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres Mailservers an. Der Anmeldename bleibt unverändert. Als Namen können Sie einen Domainnamen (z. B. pop.acme.com) oder eine IP-Adresse (z. B. 123.45.67.89) verwenden. Wenn der Mailserver keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen verwendet wird (z. B. pop.acme.com:8200). Der Standardport für die POP3-Kommunikation ist 110.

- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:

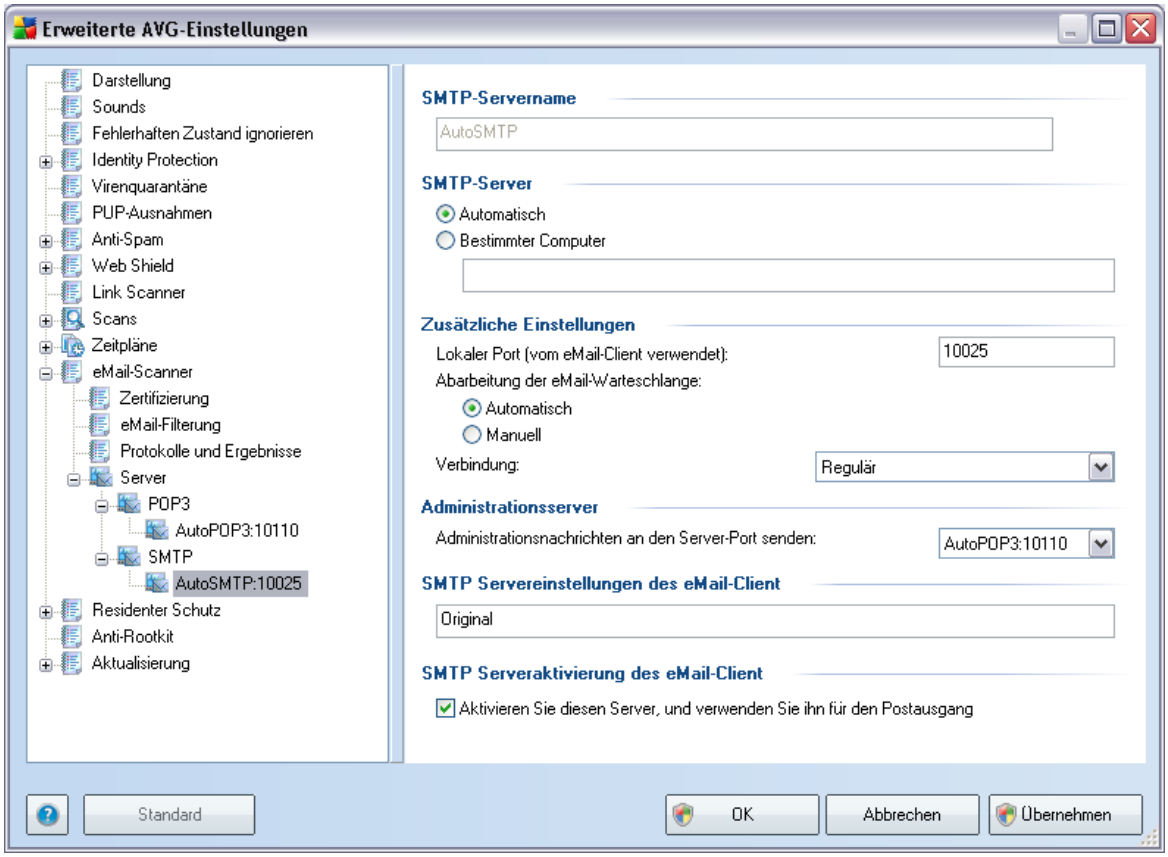
  - ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung ankommen soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die POP3-Kommunikation angeben.

  - ***APOP verwenden, wenn verfügbar*** – Diese Option sorgt bei der Mailserver-Anmeldung für mehr Sicherheit. Damit wird sichergestellt, dass der ***eMail-Scanner*** eine alternative Methode für die Weitergabe des Kennworts für das Benutzerkonto zur Anmeldung verwendet und das Kennwort nicht in einem offenen, sondern in einem verschlüsselten Format an den Server sendet, wofür eine vom Server erhaltene Variablenkette verwendet wird. Natürlich steht diese Funktion nur dann zur Verfügung, wenn der Ziel-Mailserver sie unterstützt.

  - ***Verbindung*** – In diesem Dropdown-Menü können Sie angeben, welche Verbindungsart verwendet werden soll (regulär/SSL/SSL-Standardwert). Wenn Sie die SSL-Verbindung wählen, werden die Daten verschlüsselt versendet, und es besteht kein Risiko, dass sie von Dritten verfolgt oder überwacht werden. Diese Funktion steht ebenfalls nur dann zur Verfügung, wenn der Ziel-Mailserver sie unterstützt.

- ***POP3-Serveraktivierung des eMail-Client*** – Dieser Bereich enthält einen Überblick über die Konfigurationseinstellungen für die korrekte Konfiguration Ihres eMail-Clients (so dass der ***eMail-Scanner*** alle eingehenden eMails prüft). Dabei handelt es sich um eine Zusammenfassung, die auf den in diesem Dialog sowie in anderen, verwandten Dialogen angegebenen entsprechenden Parametern basiert.

- ***Serveraktivierung für eMail-Client POP3*** – Markieren Sie diese Option, um den angegebenen POP3-Server zu aktivieren oder zu deaktivieren



In diesem Dialog (geöffnet über ***Server / SMTP***) können Sie einen neuen ***eMail-Scanner-***Server einrichten, der das SMTP-Protokoll für ausgehende eMails verwendet:

- ***SMTP-Servername*** – Geben Sie den Namen des Servers ein oder behalten Sie den Standardnamen von AutoSMTP bei

- ***SMTP-Server*** – Hiermit wird die Methode für die Bestimmung des eMail-Servers festgelegt, der für ausgehende eMails verwendet wird:

    - ***Automatisch*** – Die Anmeldung erfolgt automatisch, den Einstellungen Ihres eMail-Programms entsprechend

    - ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres eMail-Servers an. Als Namen können Sie einen Domainnamen (z. B. smtp.acme.com) oder eine IP-Adresse (z. B. 123.45.67.89) verwenden. Wenn der eMail-Server keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen verwendet wird (z. B. smtp. acme.com:8200). Der Standardport für die SMTP-Kommunikation ist 25.

- ***Zusätzliche Einstellungen*** – Hier werden detailliertere Parameter festgelegt:

    - ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung erwartet werden soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die SMTP-Kommunikation angeben.

    - ***Abarbeitung der eMail-Warteschlange*** – Hier wird das Verhalten des ***eMail-Scanners*** bei der Verarbeitung der Anforderungen für das Senden von eMails festgelegt:

        - Automatisch – Die ausgehende eMail wird sofort an den Ziel-eMail-Server gesendet

        - Manuell – Die Nachricht wird in die Warteschlange der ausgehenden Nachrichten eingereiht und später gesendet

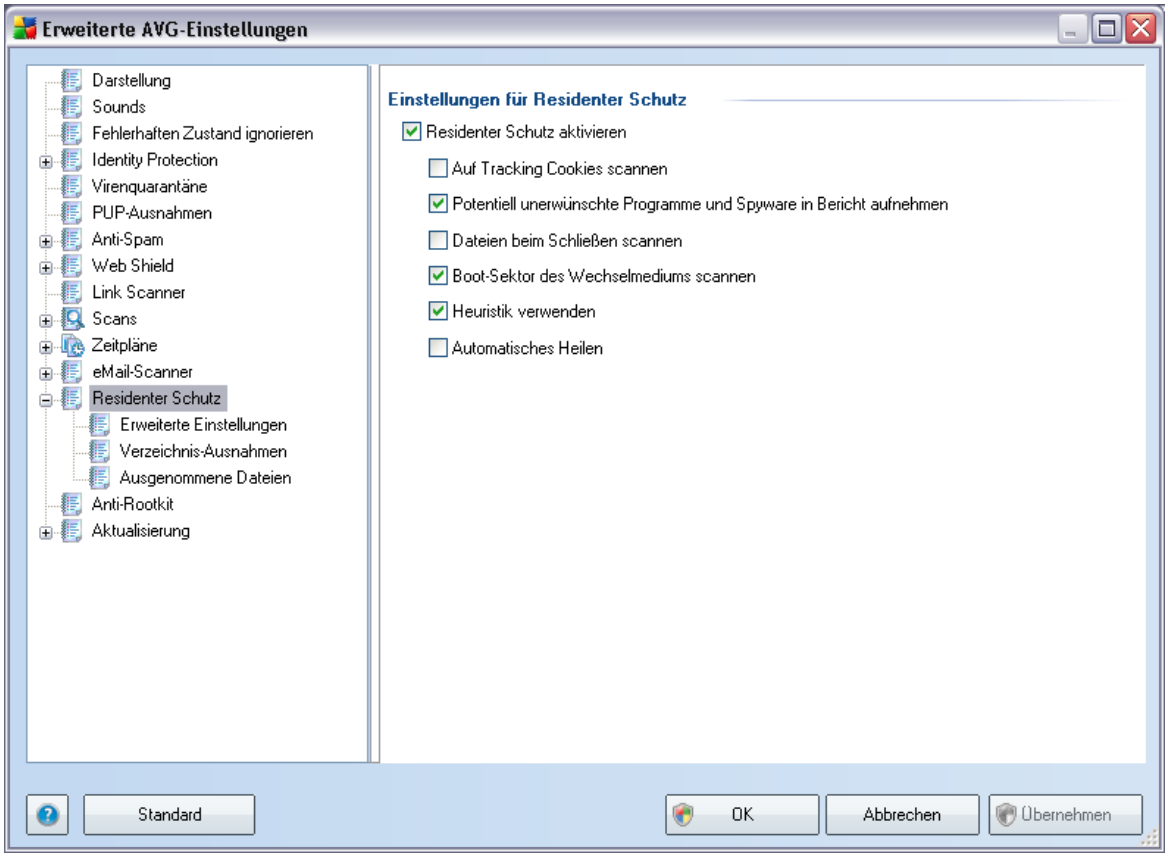
    - ***Verbindung*** – In diesem Dropdown-Menü können Sie angeben, welche Verbindungsart verwendet werden soll (regulär/SSL/SSL-Standardwert). Wenn Sie die SSL-Verbindung wählen, werden die Daten verschlüsselt versendet, und es besteht kein Risiko, dass sie von Dritten verfolgt oder überwacht werden. Diese Funktion steht nur dann zur Verfügung, wenn der Ziel-eMail-Server sie unterstützt.

- ***Administrationsserver*** – Dies zeigt die Portnummer des Servers an, der für die Rückübermittlung von Administrationsberichten verwendet wird. Diese Nachrichten werden beispielsweise generiert, wenn der Ziel-eMail-Server die ausgehende Nachricht zurückweist oder wenn dieser eMail-Server nicht zur Verfügung steht.

- ***Servereinstellungen für den eMail-Client SMTP*** – Diese Option bietet Informationen darüber, wie das eMail-Programm konfiguriert werden muss, so dass ausgehende eMails unter Verwendung des gerade geänderten Servers für die Überprüfung ausgehender Nachrichten geprüft werden. Dies ist eine Zusammenfassung, die auf den in diesem Dialog sowie in anderen, verwandten Dialogen angegebenen entsprechenden Parametern basiert.

9.13. Residenter Schutz

Die Komponente ***Residenter Schutz*** bietet Echtzeitschutz von Dateien und Ordnern gegen Viren, Spyware und andere Malware.



Im Dialog ***Einstellungen für Residenter Schutz*** können Sie den Schutz durch ***Residenter Schutz*** vollständig aktivieren oder deaktivieren, indem Sie die Option ***Residenter Schutz aktivieren*** aktivieren oder deaktivieren (*Standardmäßig ist diese Option aktiviert*). Darüber hinaus können Sie auswählen, welche Features von ***Residenter Schutz*** aktiviert werden sollen:

- ***Auf Tracking Cookies scannen*** – Mit diesem Parameter wird festgelegt, dass während des Scanvorgangs Cookies erkannt werden sollen. (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*)

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert*) – Es wird nach potentiell unerwünschten Programmen (*ausführbare Anwendungen, die verschiedene Arten von Spyware oder Adware darstellen können*) gesucht

- ***Dateien beim Schließen scannen*** – Diese Option sorgt dafür, dass AVG aktive Objekte (z. B. Anwendungen oder Dokumente) sowohl beim Öffnen als auch beim Beenden scannt. Durch dieses Feature ist Ihr Computer auch gegen einige fortschrittliche Virenarten geschützt

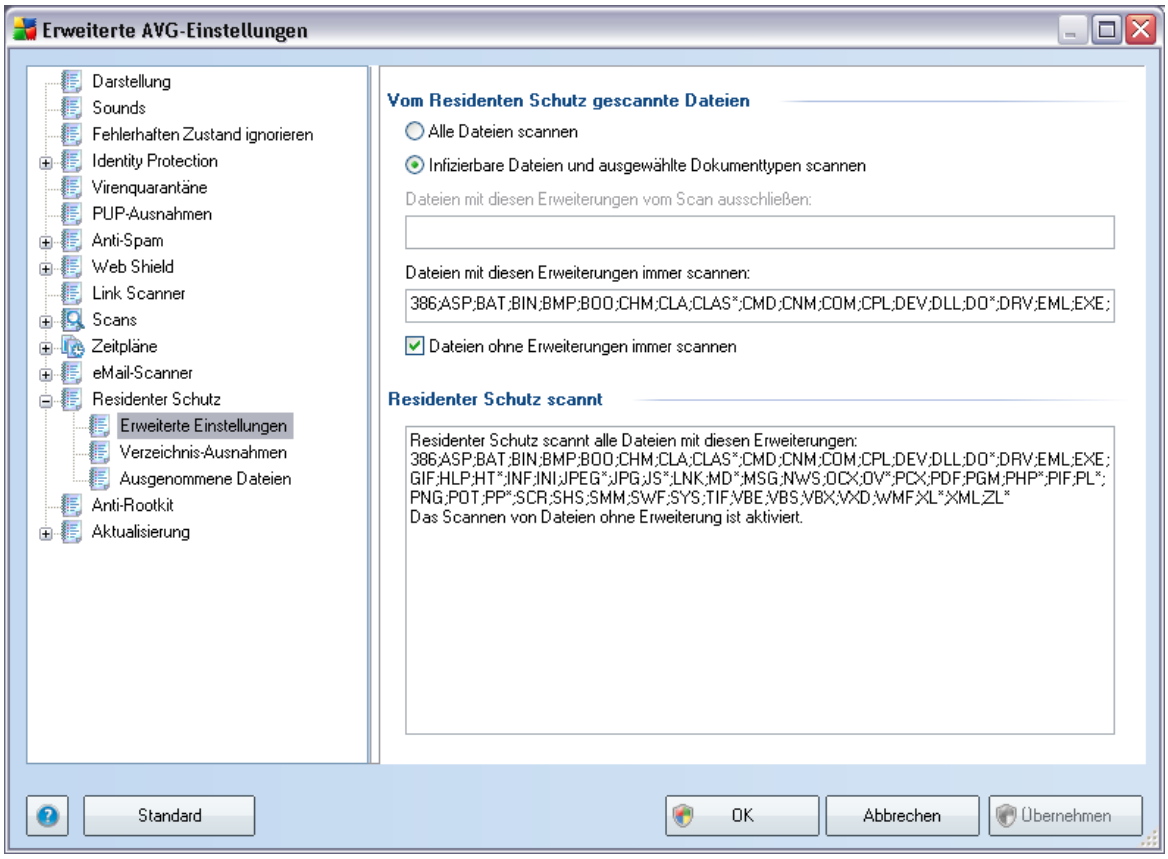
- ***Boot-Sektor des Wechselmediums scannen*** – (*standardmäßig aktiviert*)

- ***Heuristik verwenden*** – (*standardmäßig aktiviert*) Die heuristische Analyse wird zum Erkennen verwendet (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*)

- ***Automatisches Heilen*** – Jede erkannte Infektion wird automatisch geheilt, wenn eine Gegenmaßnahme verfügbar ist

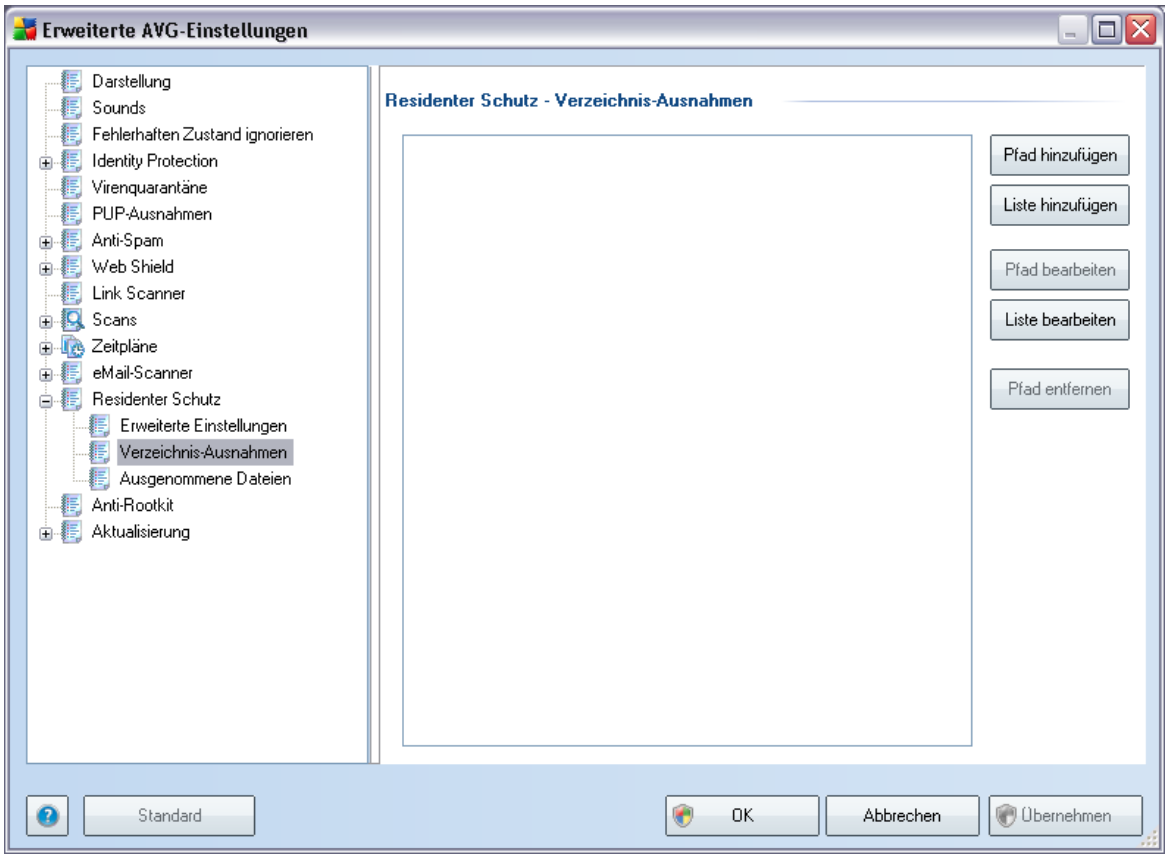
9.13.1. Erweiterte Einstellungen

Im Dialog ***Vom Residenten Schutz gescannte Dateien*** können Sie festlegen, welche Dateien gescannt werden sollen (*durch Angabe der Erweiterungen*):



Sie können festlegen, ob alle Dateien oder nur infizierbare Dateien gescannt werden sollen. Im letzteren Fall können Sie zwei Listen von Erweiterungen angeben, um zu bestimmen, welche Dateitypen vom Scan ausgeschlossen werden sollen und welche Dateitypen in jedem Fall gescannt werden sollen.

9.13.2. Verzeichnis-Ausnahmen



Im Dialog ***Residenter Schutz – Verzeichnis-Ausnahmen*** können Sie Ordner definieren, die von der Überprüfung durch den ***Residenten Schutz*** ausgeschlossen werden sollen.

Wenn dies nicht unbedingt notwendig ist, empfehlen wir dringend, keine Verzeichnisse auszuschließen!

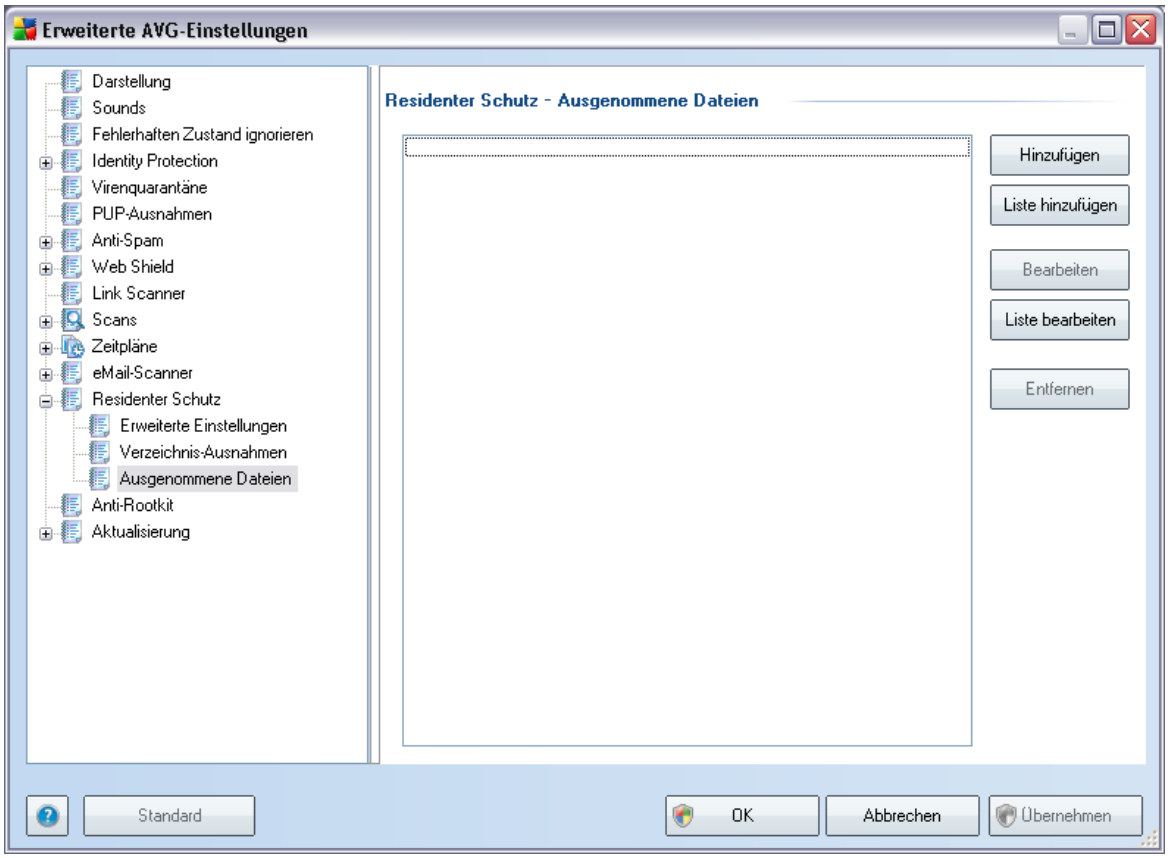
Der Dialog enthält folgende Schaltflächen:

- ***Pfad hinzufügen*** – Mit dieser Schaltfläche können Sie Verzeichnisse angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Liste hinzufügen*** – Mit dieser Schaltfläche können Sie eine ganze Liste von Verzeichnissen eingeben, die von der Überprüfung durch den ***Residenten***

Schutz ausgeschlossen werden sollen

- ***Pfad bearbeiten*** – Hier können Sie den festgelegten Pfad zu einem ausgewählten Verzeichnis bearbeiten
- ***Liste bearbeiten*** – Hier können Sie die Liste der Verzeichnisse bearbeiten
- ***Pfad entfernen*** – Mit dieser Schaltfläche können Sie den Pfad zu einem ausgewählten Verzeichnis aus der Liste löschen

9.13.3. Ausgenommene Dateien



Der Dialog ***Residenter Schutz – Ausgenommene Dateien*** weist das gleiche Verhalten auf wie der zuvor beschriebene Dialog ***Residenter Schutz – Verzeichnis-Ausnahmen*** , doch statt Verzeichnissen können Sie hier bestimmte Dateien auswählen, die von ***Residenter Schutz*** nicht überprüft werden.

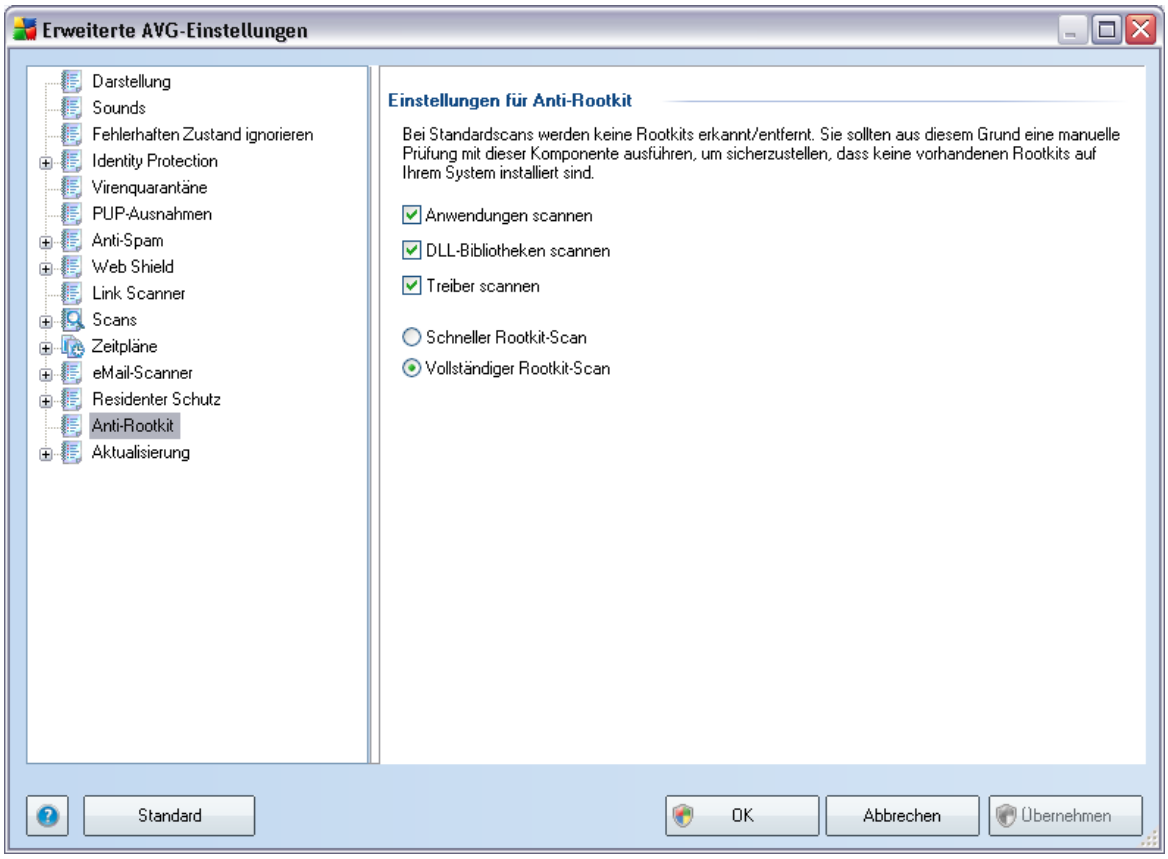
Wenn dies nicht unbedingt notwendig ist, empfehlen wir ausdrücklich, keine Dateien auszuschließen!

Der Dialog enthält folgende Schaltflächen:

- ***Hinzufügen*** – Mit dieser Schaltfläche können Sie Verzeichnisse angeben, die vom Scanvorgang ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Liste hinzufügen*** – Mit dieser Schaltfläche können Sie eine ganze Liste von Verzeichnissen eingeben, die von der Überprüfung durch ***Residenter Schutz*** ausgeschlossen werden
- ***Bearbeiten*** – Hier können Sie den festgelegten Pfad zu einem ausgewählten Verzeichnis bearbeiten
- ***Liste bearbeiten*** – Hier können Sie die Liste der Verzeichnisse bearbeiten
- ***Entfernen*** – Mit dieser Schaltfläche können Sie den Pfad zu einem ausgewählten Verzeichnis aus der Liste löschen

9.14. Anti-Rootkit

In diesem Dialog können Sie die Konfiguration der Komponente ***Anti-Rootkit*** bearbeiten:



Die Bearbeitung aller Funktionen der Komponente ***Anti-Rootkit*** kann auch direkt über die ***Benutzeroberfläche der Komponente Anti-Rootkit*** vorgenommen werden.

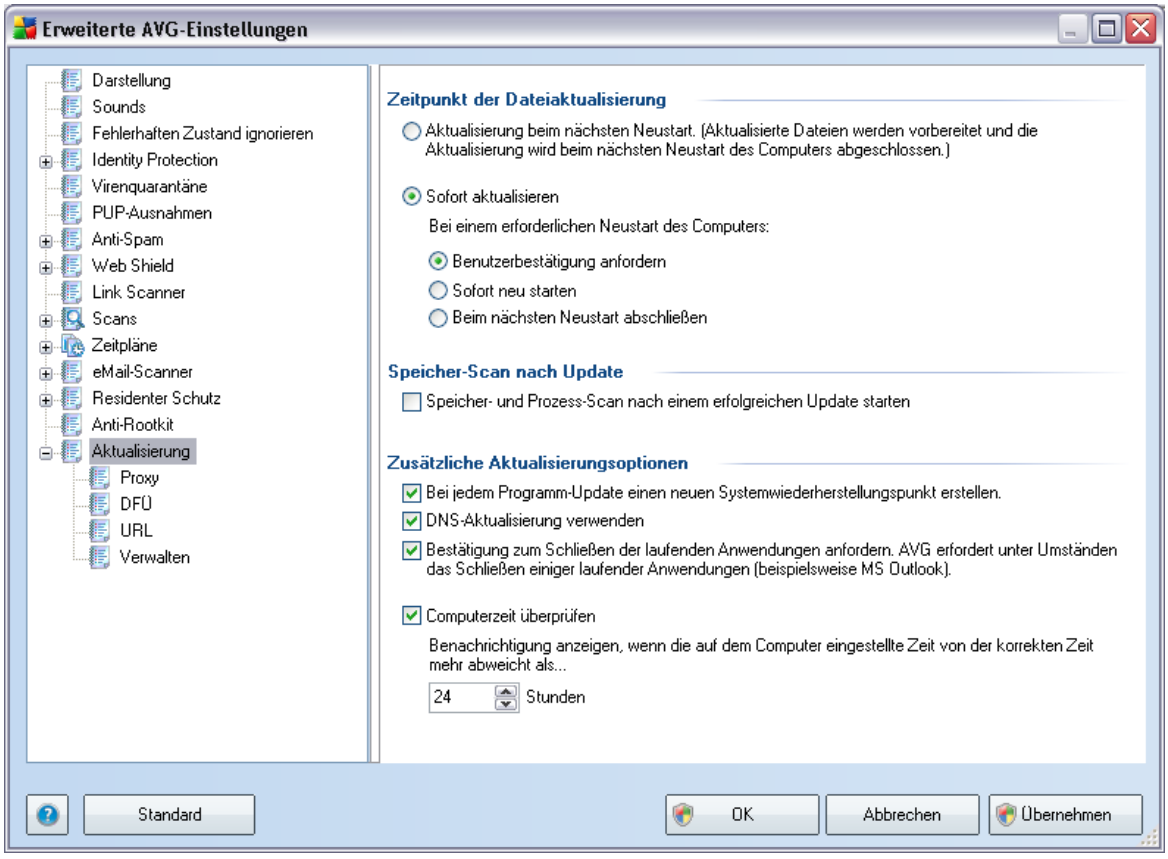
Aktivieren Sie die entsprechenden Kontrollkästchen, um festzulegen, welche Objekte gescannt werden sollen:

- ***Anwendungen scannen***
- ***DLL-Bibliotheken scannen***
- ***Treiber scannen***

Wählen Sie anschließend den Rootkit-Scanmodus aus:

- ***Schneller Rootkit-Scan*** – Nur der Systemordner wird gescannt (*normalerweise C:\Windows*)
- ***Vollständiger Rootkit-Scan*** – Alle verfügbaren Datenträger, mit Ausnahme von A: und B:, werden gescannt

9.15. Aktualisierung



Mit dem Navigationselement ***Aktualisierung*** wird ein neuer Dialog geöffnet, in dem Sie allgemeine Parameter hinsichtlich der Aktualisierung von AVG festlegen können:

Zeitpunkt der Dateiaktualisierung

In diesem Bereich können Sie zwischen zwei alternativen Optionen wählen: Aktualisierung beim nächsten Neustart oder Sie können die Aktualisierung sofort starten. Standardmäßig ist die Option zum sofortigen Aktualisieren ausgewählt, da AVG so die höchste Sicherheitsebene bieten kann. Das Planen einer Aktualisierung beim nächsten Neustart Ihres Computers ist nur empfohlen, wenn Sie sicher sind, dass der Computer regelmäßig, mindestens einmal täglich, neu gestartet wird.

Wenn Sie die Standardkonfiguration beibehalten und den Aktualisierungsprozess unmittelbar starten, können Sie die Umstände festlegen, unter denen ein möglicherweise notwendiger Neustart durchgeführt werden soll:

- ***Benutzerbestätigung anfordern*** – Sie werden aufgefordert, den Neustart Ihres Computers zu bestätigen, um den Aktualisierungsprozess abzuschließen
- ***Sofort neu starten*** – Der Computer wird automatisch neu gestartet, unmittelbar nachdem der Aktualisierungsprozess abgeschlossen ist. Sie müssen den Neustart nicht bestätigen
- ***Beim nächsten Neustart abschließen*** – Der Abschluss des Aktualisierungsprozesses wird bis zum nächsten Neustart des Computers verschoben – Bitte beachten Sie, dass diese Option nur empfohlen wird, wenn Sie sicher sind, dass der Computer regelmäßig, mindestens einmal täglich, neu gestartet wird

Speicher-Scan nach Update

Aktivieren Sie dieses Kontrollkästchen, um nach jedem erfolgreich abgeschlossenen Update einen Scan des Speichers durchzuführen. Das zuletzt heruntergeladene Update kann neue Virendefinitionen enthalten, die beim Scanvorgang umgehend angewendet werden.

Zusätzliche Aktualisierungsoptionen

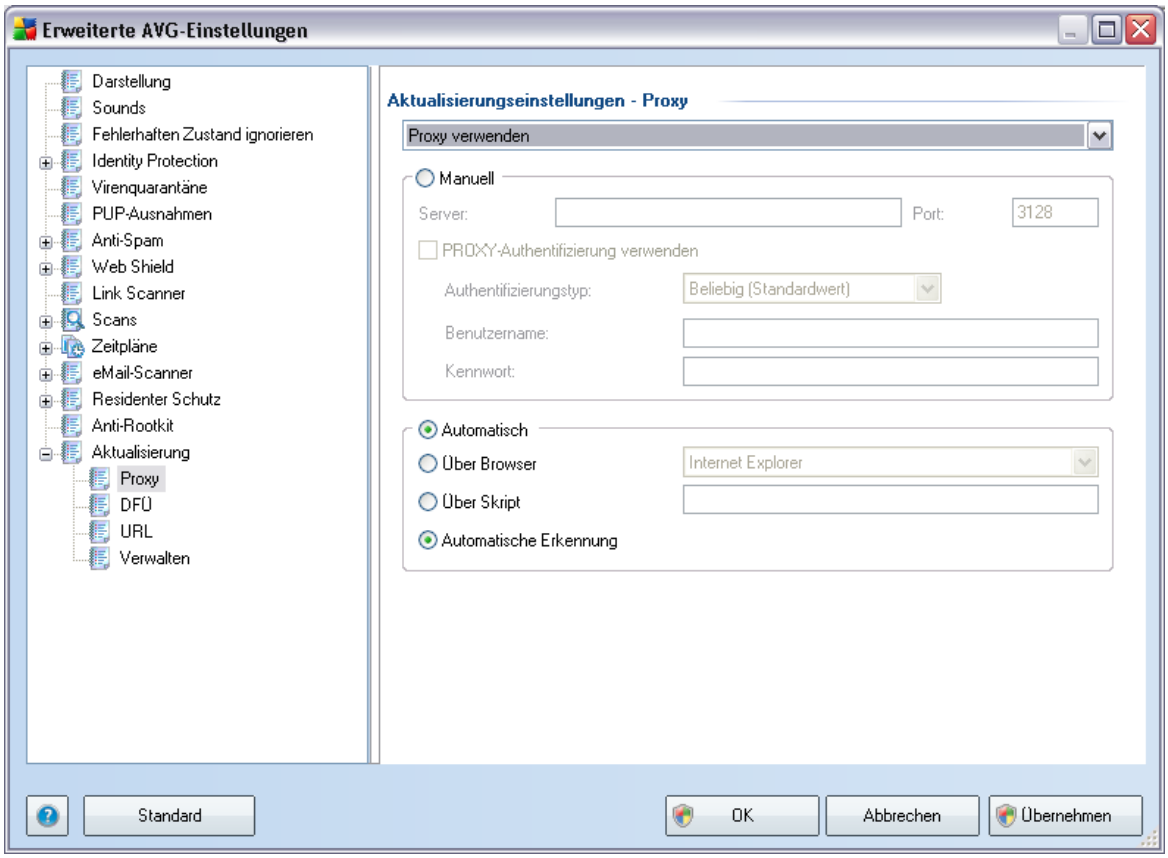
- ***Nach jedem Programmupdate einen neuen Systemwiederherstellungspunkt erstellen*** – Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen Konfiguration wiederherstellen. Diese Option kann über Start/Programme/Zubehör/ Systemprogramme/Systemwiederherstellung aufgerufen werden. Änderungen sollten jedoch nur von erfahrenen Benutzern vorgenommen werden! Wenn Sie diese Funktion nutzen möchten, lassen Sie dieses Kontrollkästchen aktiviert.

- ***DNS-Aktualisierung verwenden*** – Aktivieren Sie dieses Kontrollkästchen, um zu bestätigen, dass Sie die Erkennungsmethode für Update-Dateien verwenden möchten, durch welche die zwischen dem Update-Server und dem AVG-Client übertragene Datenmenge verringert wird.

- ***Mithilfe der Option „Bestätigung zum Schließen der laufenden Anwendungen anfordern"*** (*standardmäßig aktiviert*) können Sie dafür sorgen, dass keine aktuell ausgeführten Anwendungen ohne Ihre Genehmigung geschlossen werden. Dies kann zum Abschluss des Updatevorgangs erforderlich sein;

- ***Computerzeit überprüfen*** – Aktivieren Sie diese Option, wenn eine Benachrichtigung angezeigt werden soll, falls die Computerzeit um mehr als die angegebene Anzahl an Stunden von der korrekten Zeit abweicht.

9.15.1. Proxy



Ein Proxy-Server ist ein unabhängiger Server oder Dienst, der auf einem PC ausgeführt wird und für eine sicherere Verbindung mit dem Internet sorgt. Sie können auf das Internet entsprechend den festgelegten Netzwerkregeln entweder direkt oder über den Proxy-Server zugreifen. Es können auch beide Möglichkeiten gleichzeitig zugelassen sein. Wählen Sie anschließend im Dialog ***Aktualisierungseinstellungen – Proxy*** aus dem Dropdown-Menü eine der folgenden Optionen aus:

- ***Proxy verwenden***
- ***Keinen Proxy verwenden***
- ***Versuchen Sie zuerst, eine Proxy-Verbindung herzustellen. Sollte dieser Versuch fehlschlagen, stellen Sie eine direkte Verbindung her*** – Standardeinstellungen

Wenn Sie eine Option mit Proxy-Server ausgewählt haben, müssen Sie weitere Angaben machen. Die Servereinstellungen können entweder manuell oder automatisch vorgenommen werden.

Manuelle Konfiguration

Wenn Sie die manuelle Konfiguration auswählen (aktivieren Sie *die Option* ***Manuell*** *, um den jeweiligen Dialog zu aktivieren*), müssen Sie folgende Angaben machen:

- ***Server*** – Geben Sie die IP-Adresse oder den Namen des Servers an.
- ***Port*** – Geben Sie die Portnummer für den Internetzugriff an (*Standardmäßig ist die Portnummer 3128 zugewiesen. Sie können diese aber ändern. Wenn Sie sich nicht sicher sind, wenden Sie sich an Ihren Netzwerkadministrator*)

Auf dem Proxy-Server können auch besondere Regeln für jeden Benutzer festgelegt sein. Aktivieren Sie in diesem Fall das Kontrollkästchen ***PROXY-Authentifizierung verwenden***, um zu bestätigen, dass Ihr Benutzername und Ihr Kennwort für die Verbindung mit dem Internet über den Proxy-Server gültig sind.

Automatische Konfiguration

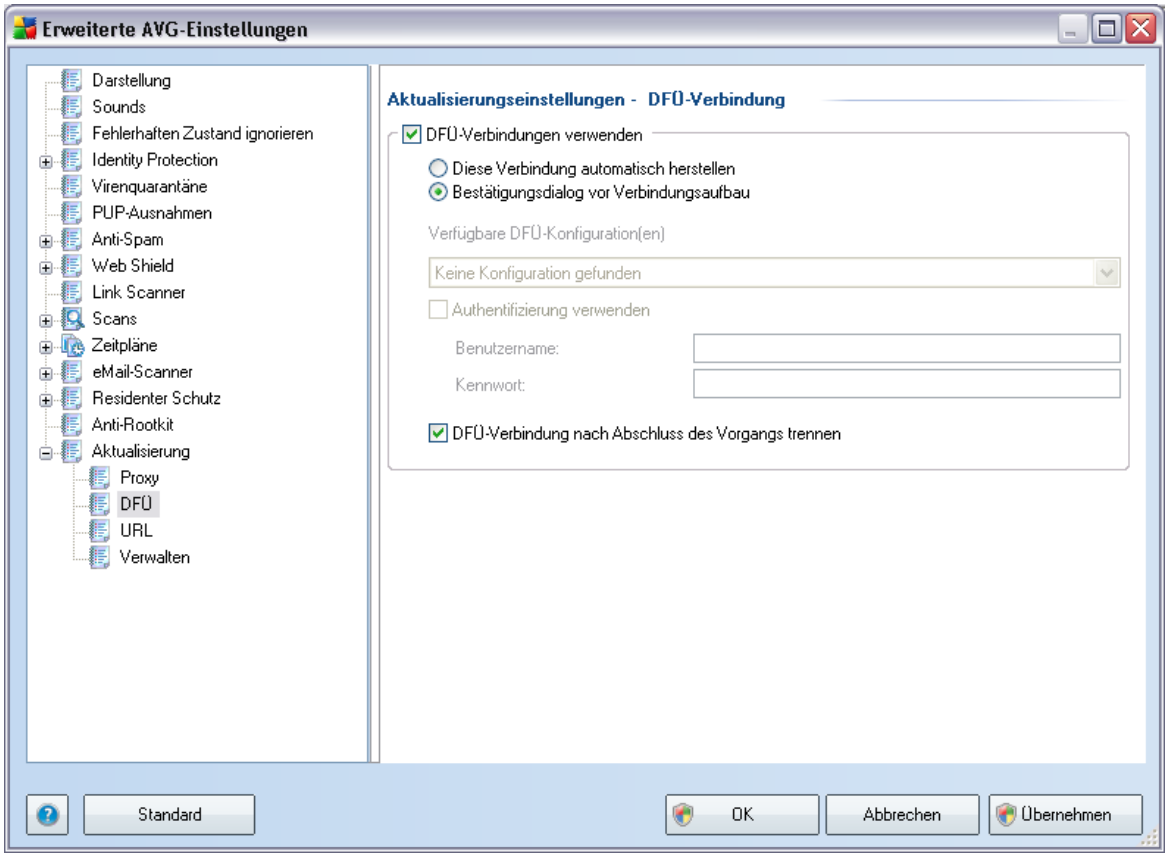
Wenn Sie die automatische Konfiguration auswählen (*Aktivieren Sie die Option* ***Automatisch****, um den Dialog zu aktivieren*), wählen Sie bitte aus, von wo die Konfiguration des Proxy vorgenommen werden soll:

- ***Über Browser*** – Die Konfiguration wird von Ihrem Standard-

Internetbrowsers gelesen

- ***Über Skript*** – Die Konfiguration wird von einem heruntergeladenen Skript gelesen, das die Proxy-Adresse wiedergibt
- ***Automatische Erkennung*** – Die Konfiguration wird automatisch direkt vom Proxy-Server erkannt

9.15.2. DFÜ

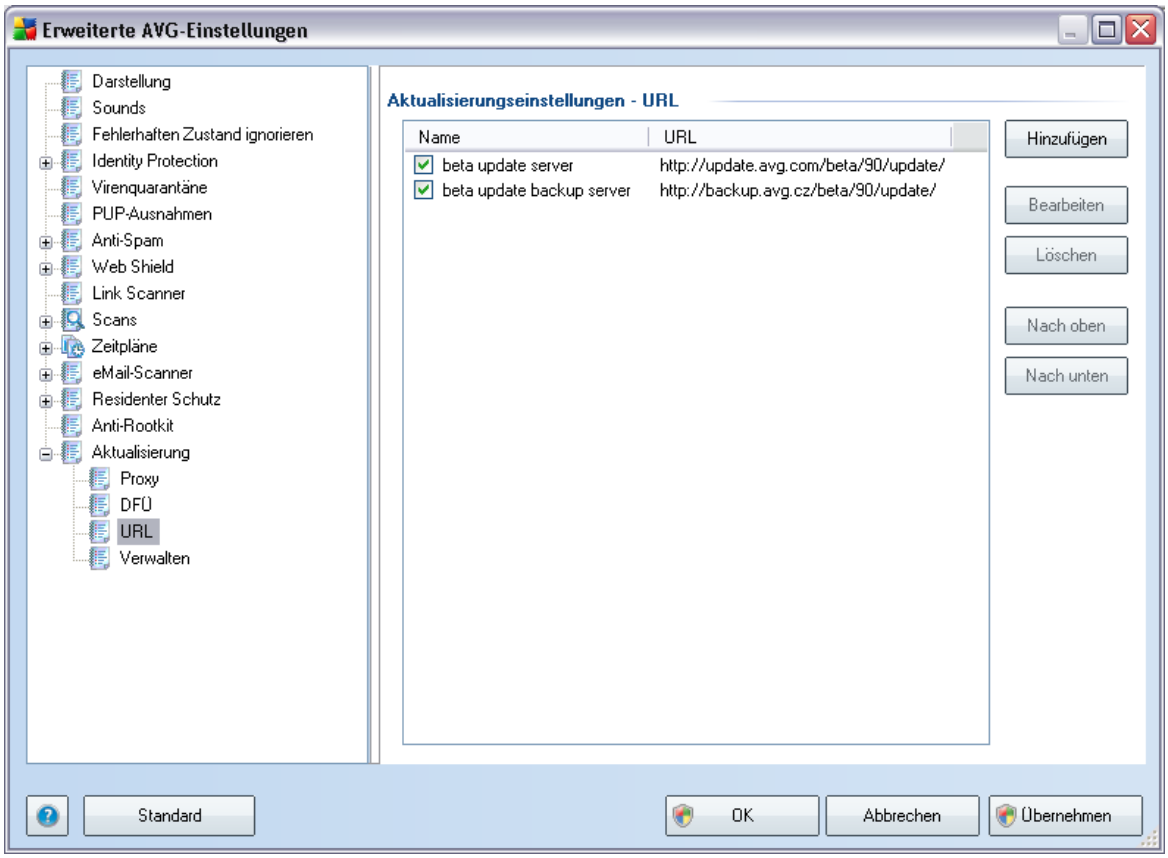


Die optional im Dialog ***Aktualisierungseinstellungen – DFÜ-Verbindung*** definierten Parameter beziehen sich auf die Einwahlverbindung mit dem Internet. Die Felder des Dialogs werden erst aktiviert, wenn Sie die Option ***DFÜ-Verbindungen verwenden*** auswählen.

Geben Sie an, ob die Verbindung mit dem Internet automatisch hergestellt werden soll (***Diese Verbindung automatisch herstellen***) oder ob Sie die Verbindung jedes

Mal bestätigen möchten (***Bestätigungsdialog vor Verbindungsaufbau***). Bei der automatischen Verbindungsherstellung sollten Sie zudem auswählen, ob die Verbindung nach Abschluss der Aktualisierung getrennt werden soll (***DFÜ-Verbindung nach Abschluss des Vorgangs trennen***).

9.15.3. URL



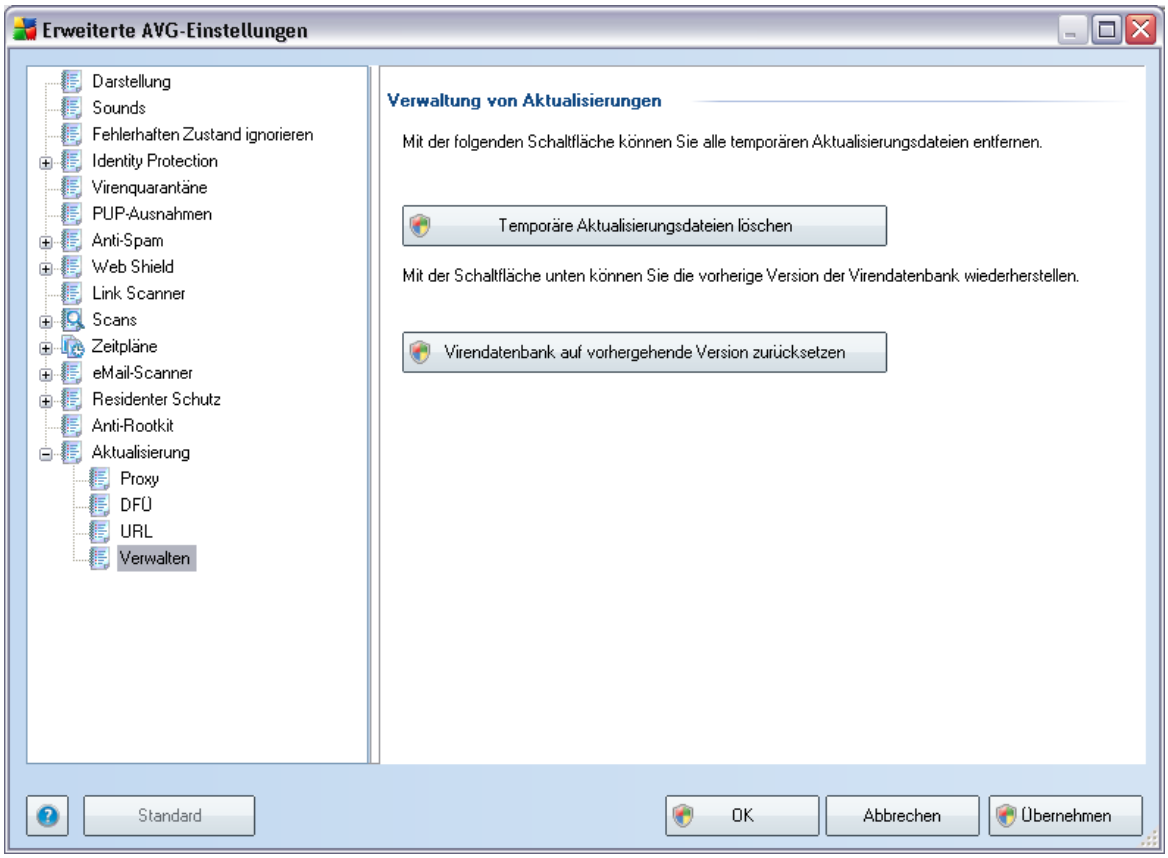
Der Dialog ***URL*** zeigt eine Liste von Internetadressen an, von denen Updates heruntergeladen werden können. Die Liste kann über die folgenden Schaltflächen geändert werden:

- ***Hinzufügen*** – Ein Dialog wird geöffnet, in dem Sie der Liste eine neue URL hinzufügen können
- ***Bearbeiten*** – Ein Dialog wird geöffnet, in dem Sie die Parameter der ausgewählten URL bearbeiten können

- ***Löschen*** – Die ausgewählte URL wird aus der Liste gelöscht
- ***Nach oben*** – Die ausgewählte URL wird in der Liste eine Position nach oben verschoben
- ***Nach unten*** – Die ausgewählte URL-Adresse wird in der Liste eine Position nach unten verschoben

9.15.4. Verwalten

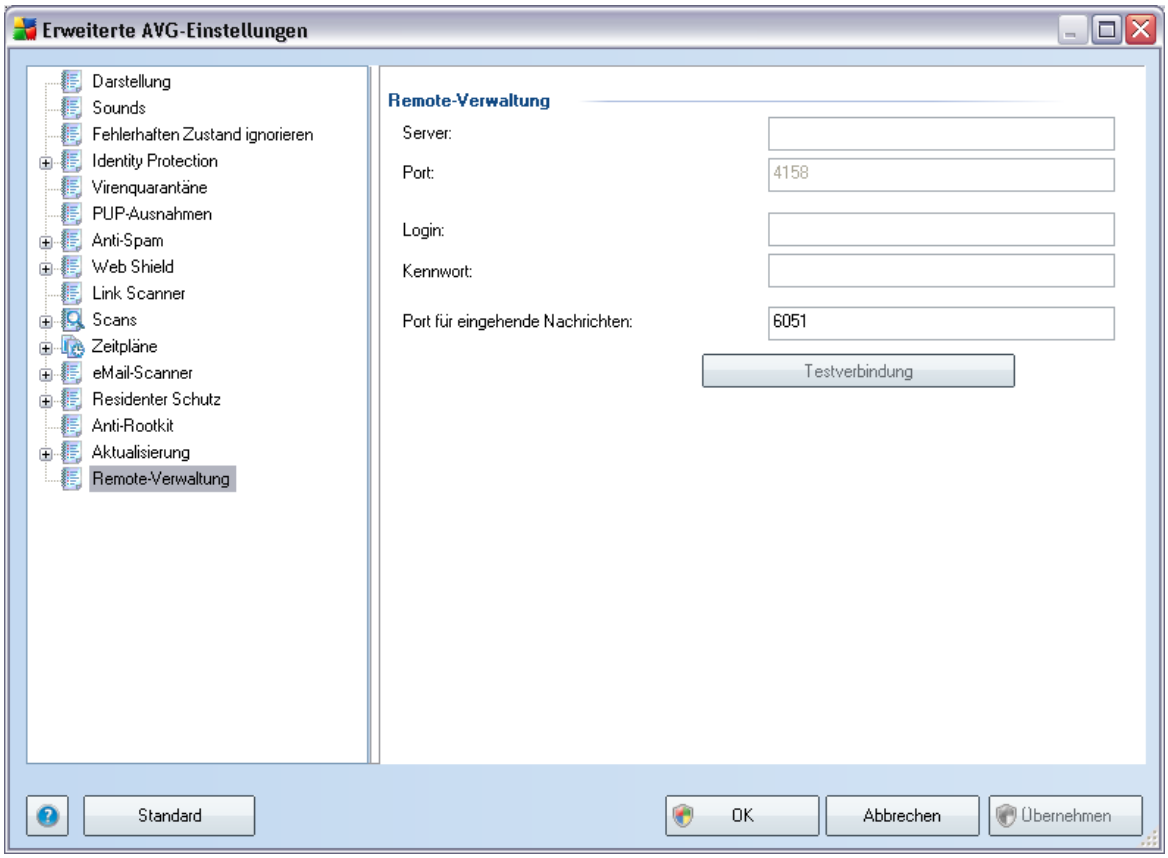
Im Dialog ***Verwalten*** stehen zwei Optionen über zwei Schaltflächen zur Verfügung:



- ***Temporäre Aktualisierungsdateien löschen*** – Klicken Sie auf diese Schaltfläche, wenn Sie alle redundanten Update-Dateien von Ihrer Festplatte löschen möchten (*standardmäßig werden diese Dateien 30 Tage gespeichert*)
- ***Virendatenbank auf vorhergehende Version zurücksetzen*** – Klicken Sie

auf diese Schaltfläche, um die letzte Version der Virendatenbank auf Ihrer Festplatte zu löschen und zur vor diesem Update gespeicherten Version zurückzukehren (*Die neue Version der Virendatenbank ist Teil des nächsten Update*)

9.16. Remote-Verwaltung



Die Einstellungen der ***Remote-Verwaltung*** dienen der Verbindung der AVG-Clients mit dem Remote-Verwaltungssystem. Wenn Sie vorhaben, die jeweilige Station mit der Remote-Verwaltung zu verbinden, geben Sie bitte folgende Parameter an:

- ***Server*** – Name oder IP-Adresse des Servers, auf dem der AVG Admin-Server installiert ist
- ***Port*** – Geben Sie die Nummer des Ports an, über den der AVG-Client mit dem AVG Admin-Server kommuniziert (*Standard-Port ist 4158. Wenn Sie diesen Port verwenden, müssen Sie ihn gesondert angeben*)

- ***Login*** – Wenn die Kommunikation zwischen dem AVG-Client und dem AVG Admin-Server gesichert ist, geben Sie bitte Ihren Benutzernamen ...
- ***Kennwort*** – ... und Ihr Kennwort an
- ***Port für eingehende Nachrichten*** – Nummer des Ports, auf dem der AVG-Client vom AVG Admin-Server eingehende Nachrichten empfängt

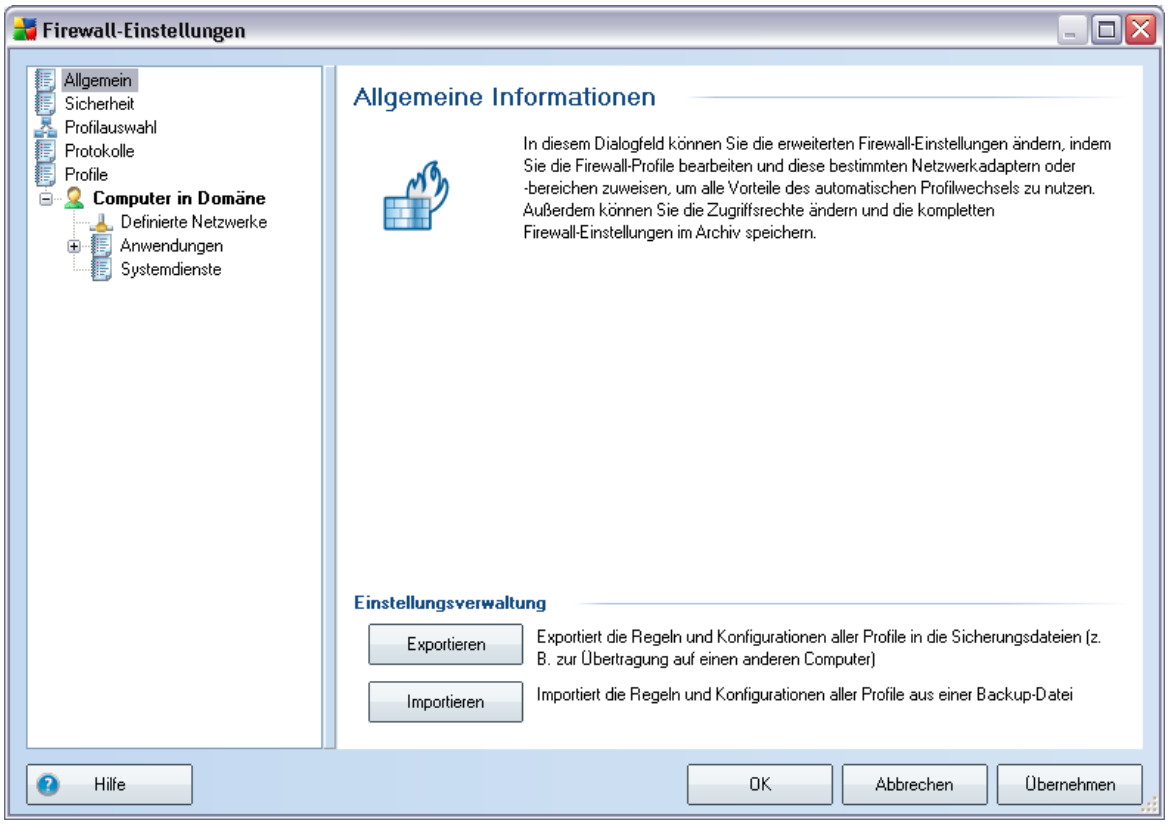
Über die Schaltfläche ***Testverbindung*** können Sie überprüfen, ob alle oben genannten Daten gültig sind und für eine erfolgreiche Verbindung zum DataCenter genutzt werden können.

Hinweis: *Eine genauere Beschreibung der Remote-Verwaltung finden Sie in der Dokumentation zur AVG Netzwerk Edition.*

10. Firewall-Einstellungen

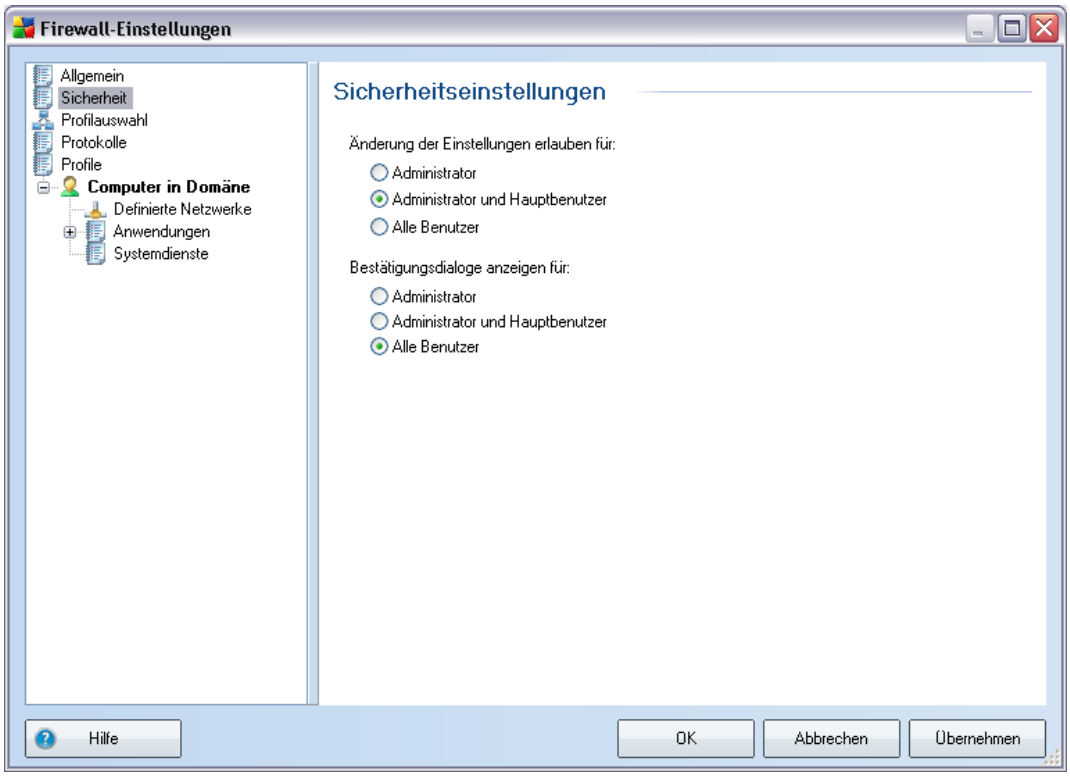
Für die Konfiguration der ***Firewall*** wird ein neues Fenster geöffnet, wo in verschiedenen Dialogen sehr detaillierte Parameter der Komponente eingestellt werden können. ***Eine erweiterte Bearbeitung der Konfiguration wird jedoch nur für Experten und erfahrene Benutzer empfohlen.***

10.1. Allgemein



In den ***Allgemeinen Informationen*** können Sie Firewall-Konfigurationen ***Exportieren*** oder ***Importieren***; das heißt, dass Sie die festgelegten ***Firewall***-Regeln und -Einstellungen in die Sicherungsdateien exportieren oder eine vollständige Sicherungsdatei importieren können.

10.2. Sicherheit



Im Dialog ***Sicherheitseinstellungen***können Sie die allgemeinen Regeln der ***Firewall*** unabhängig vom ausgewählten Profil festlegen:

- ***Änderung von Einstellungen erlauben für*** – legt fest, wer die Konfiguration der ***Firewall*** ändern darf
- ***Bestätigungsdialog anzeigen für*** – legt fest, wem die Bestätigungsdialoge angezeigt werden sollen (*Dialoge, in denen nach einer Entscheidung gefragt wird, wenn eine bestimmte Situation nicht von einer definierten* ***Firewall-*** *Regel* abgedeckt wird)

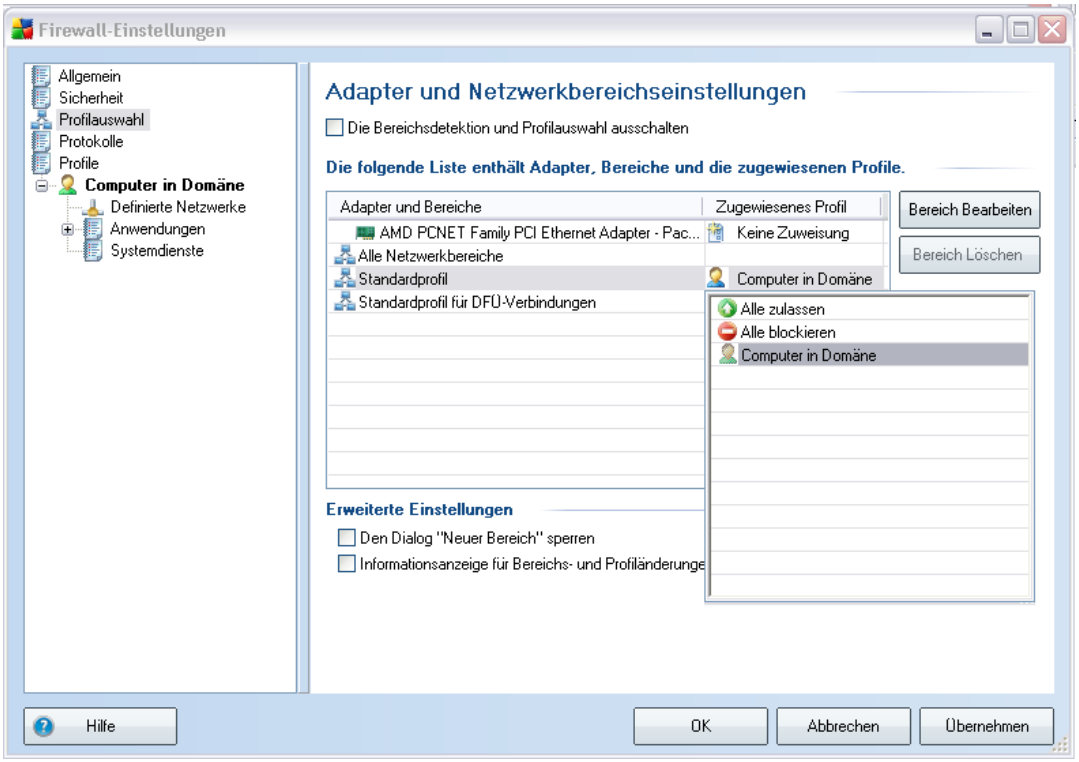
In beiden Fällen können Sie die spezifische Berechtigung einer der folgenden Benutzergruppen zuweisen:

  - ***Administrator*** – hat vollständige Kontrolle über den Computer und ist berechtigt, jeden Benutzer in Gruppen mit speziell definierten Berechtigungen zuzuweisen.

- ***Administrator und Hauptbenutzer*** – Der Administrator kann jeden Benutzer einer bestimmten Gruppe zuweisen (*Hauptbenutzer*) und die Berechtigungen der Gruppenmitglieder festlegen

- ***Alle Benutzer*** – Andere Benutzer, die keiner bestimmten Gruppe zugewiesen sind

10.3. Profilauswahl



In den Dialogen ***Adapter- und Netzwerkbereichseinstellungen***können Sie die Einstellung bearbeiten, die sich auf das Zuweisen von definierten Profilen zu bestimmten Adaptern und auf das Verweisen der entsprechenden Netzwerke bezieht:

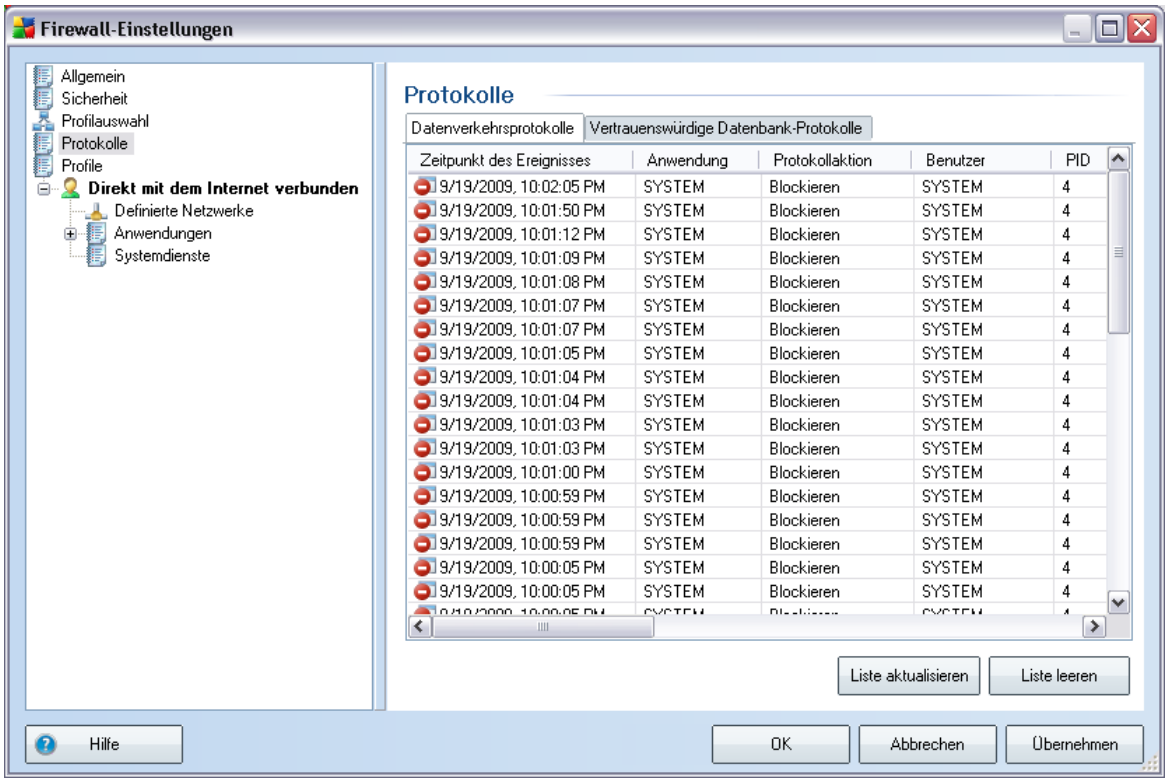
- ***Die Bereichsdetektion und Profilauswahl ausschalten***– Jedem Netzwerkschnittstellentyp bzw. jedem Bereich kann eines der definierten Profile zugewiesen werden. Wenn Sie keine spezifischen Profile festlegen möchten, wird während des ***Installationsvorgangs*** ein allgemeines Profil verwendet, das auf Ihrer Auswahl für die Elemente Computernutzung und Netzwerkdesign Ihres Computers basiert. Wenn Sie jedoch Profile unterscheiden und bestimmten Adaptern und Bereichen zuweisen möchten

und die Zuweisung später aus irgendeinem Grund zeitweise ändern möchten, aktivieren Sie die Option ***Die Bereichsdetektion und Profilauswahl ausschalten***.

- ***Liste der Adapter, Bereiche und zugewiesenen Profile*** – Diese Liste enthält einen Überblick über die erkannten Adapter und Bereiche. Jedem Adapter oder Bereich können Sie aus dem Menü der definierten Profile ein bestimmtes Profil zuweisen. Um das Menü zu öffnen, klicken Sie auf den entsprechenden Eintrag in der Liste der Adapter, und wählen Sie das Profil aus.

- ***Erweiterte Einstellungen***– Durch das Aktivieren der entsprechenden Option wird die Anzeige von Informationsmeldungen deaktiviert.

10.4. Protokolle



Im Dialog ***Protokolle*** können Sie auf zwei Reitern die Liste aller protokollierten ***Firewall***-Aktivitäten und Ereignisse mit einer genauen Beschreibung der jeweiligen Parameter aufrufen (*Zeitpunkt des Ereignisses, Name der Anwendung, jeweilige*

Protokollaktion, Benutzername, PID, Richtung des Datenverkehrs, Protokolltyp, Zahl der lokalen und Remote-Ports usw.):

- ***Datenverkehrsprotokolle*** – Umfassen Informationen über die Aktivitäten aller Anwendungen, die versucht haben, eine Verbindung mit dem Netzwerk herzustellen.

- ***Protokolle zu vertrauenswürdigen Datenbanken***– Die *Vertrauenswürdige Datenbank* ist eine interne Datenbank von AVG, in der Informationen über zertifizierte und vertrauenswürdige Anwendungen gesammelt werden, die jederzeit online kommunizieren dürfen. Wenn eine neue Anwendung erstmalig versucht, eine Verbindung zum Netzwerk herzustellen (*d. h. es wurde noch keine Firewall-Regel für diese Anwendung erstellt*), muss ermittelt werden, ob die Netzwerkkommunikation für die entsprechende Anwendung zugelassen werden soll oder nicht. Zunächst durchsucht AVG die *Vertrauenswürdige Datenbank*; wenn die Anwendung darin enthalten ist, erhält sie automatisch Zugang zum Netzwerk. Wenn in der Datenbank keine Informationen zur Anwendung verfügbar sind, werden Sie in einem gesonderten Dialog gefragt, ob Sie der Anwendung Zugang zum Netzwerk gewähren möchten.

Schaltflächen

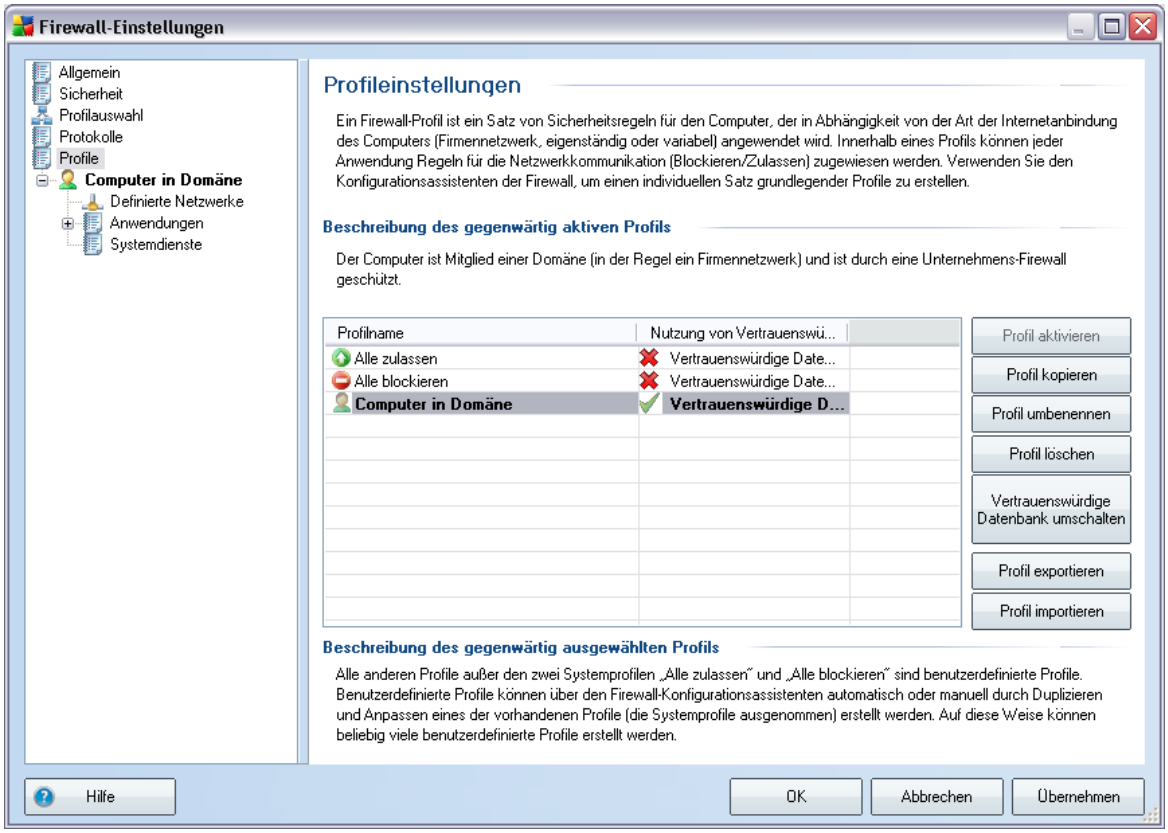
- ***Hilfe*** – Der Dialog zur Hilfe wird geöffnet.

- ***Liste aktualisieren*** – Die protokollierten Parameter können nach dem ausgewählten Attribut angeordnet werden: chronologisch (*Datum*) oder alphabetisch (*andere Spalten*) – klicken Sie einfach auf die entsprechende Spaltenüberschrift. Aktualisieren Sie die angezeigten Informationen mit der Schaltfläche ***Liste aktualisieren***.

- ***Liste leeren*** – Alle Einträge in der Liste können gelöscht werden.

10.5. Profile

Im Dialog***Profileinstellungen*** finden Sie eine Liste aller verfügbaren Profile.



Alle anderen bestehenden Systemprofile können mit den folgenden Schaltflächen direkt in diesem Dialog bearbeitet werden:

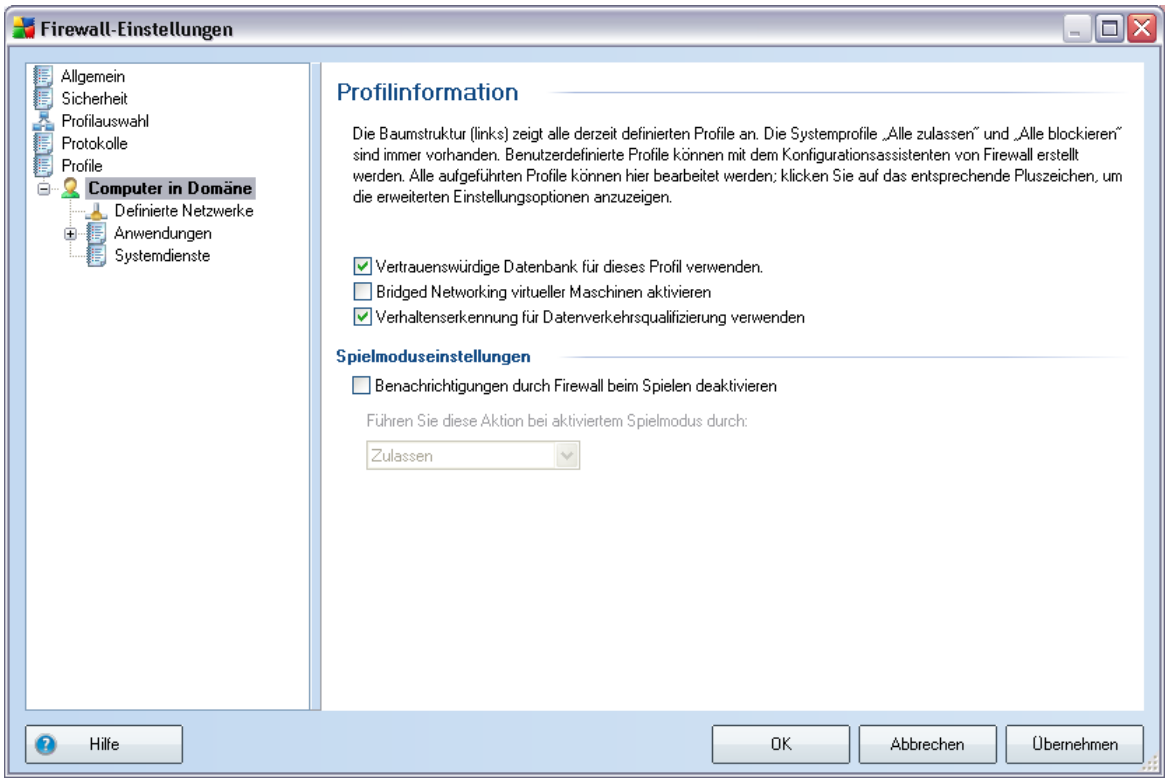
- ***Profil aktivieren*** – Mit dieser Schaltfläche können Sie das ausgewählte Profil als aktiv markieren; das heißt, dass die ausgewählte Profilkonfiguration von der ***Firewall*** zur Kontrolle des Netzwerkverkehrs verwendet wird
- ***Profil kopieren*** – Erstellt eine identische Kopie des ausgewählten Profils; Sie können die Kopie später bearbeiten und umbenennen, um auf der Basis des duplizierten Originals ein neues Profil zu erstellen
- ***Profil umbenennen*** – Hiermit können Sie einen neuen Namen für das ausgewählte Profil festlegen

- ***Profil löschen*** – Löscht das ausgewählte Profil aus der Liste
- ***Vertrauenswürdige Datenbank umschalten*** – Sie können für das ausgewählte Profil festlegen, ob Sie Informationen der *Vertrauenswürdigen Datenbank* nutzen möchten (*Die vertrauenswürdige Datenbank ist eine interne Datenbank von AVG, in der Informationen über zertifizierte und vertrauenswürdige Anwendungen gesammelt werden, die jederzeit online kommunizieren dürfen.*)
- ***Profil exportieren*** – Speichert die Konfiguration des ausgewählten Profils in einer Datei zur weiteren Verwendung
- ***Profil importieren***– Konfiguriert die Einstellungen des ausgewählten Profils auf Basis der Daten, die aus der Backup-Konfigurationsdatei exportiert wurden
- ***Hilfe*** – Die Hilfe zu dem Dialog wird geöffnet

Im unteren Abschnitt des Dialogs finden Sie die Beschreibung eines Profils, das gegenwärtig in der Liste oben ausgewählt ist.

Das Navigationsmenü links wird an die Zahl der definierten Profile angepasst, die in der Liste des Dialogs ***Profil*** enthalten sind. Mit jedem definierten Profil wird im Element ***Profil*** ein spezieller Zweig erstellt. Spezifische Profile können in den folgenden Dialogen bearbeitet werden (*diese sind für alle Profile gleich*):

10.5.1. Profilinformationen



Der Dialog ***Profilinformationen*** ist der ersten Dialog eines Abschnitts, in dem Sie die Konfiguration der einzelnen Profile in separaten Dialogen für bestimmte Parameter des jeweiligen Profils bearbeiten können.

- ***Pro tento profil použít Duveryhodnou databázi*** – (*standardmäßig aktiviert*) – Markieren Sie diese Option, um die *Vertrauenswürdige Datenbank* zu aktivieren (*d. h. die interne Datenbank von AVG, die Informationen über vertrauenswürdige und zertifizierte Anwendungen sammelt, die online kommunizieren. Wenn für die entsprechende Anwendung noch keine Regel festgelegt wurde, müssen Sie herausfinden, ob die Anwendung Zugang zum Netzwerk erhalten darf. AVG durchsucht zuerst die vertrauenswürdige Datenbank; wenn die Anwendung darin aufgeführt ist, wird sie als sicher eingestuft und darf über das Netzwerk kommunizieren. Ansonsten werden Sie aufgefordert, zu entscheiden, ob die Anwendung über das Netzwerk kommunizieren darf*) – und zwar für das jeweilige Profil

- ***Bridged Networking virtueller Maschinen aktivieren*** – (*standardmäßig deaktiviert*) – Aktivieren Sie diesen Eintrag, damit virtuelle Computer in

VMware direkt eine Verbindung mit dem Netzwerk herstellen können

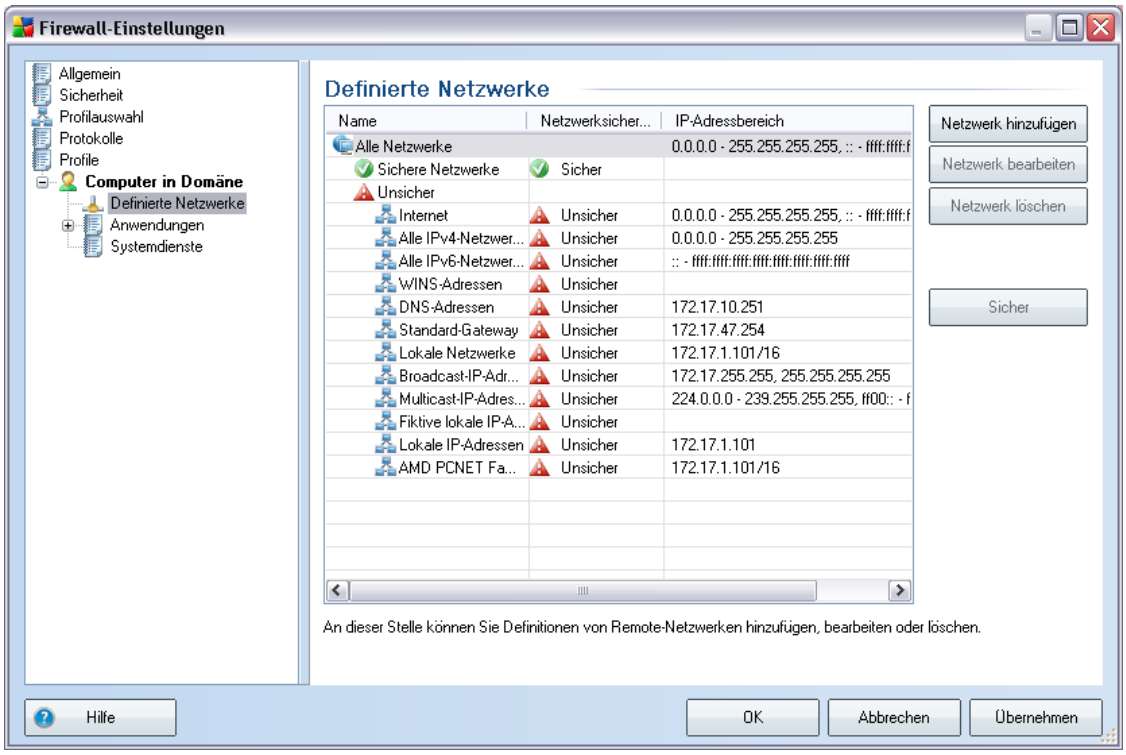
- ***Verhaltenserkennung für Datenverkehrsqualifizierung verwenden*** – (*standardmäßig aktiviert*) Markieren Sie diese Option, damit die ***Firewall*** die Funktionen von ***Link Scanner*** bei der Bewertung von Anwendungen nutzen kann – ***Link Scanner*** kann feststellen, ob die Anwendung verdächtiges Verhalten an den Tag legt oder vertrauenswürdig ist und online kommunizieren darf.

Spielmoduseinstellungen

Im Bereich ***Spielmoduseinstellungen*** können Sie durch Aktivierung der entsprechenden Optionen festlegen, ob Informationsmeldungen der ***Firewall*** auch angezeigt werden sollen, während auf dem Computer eine Vollbildanwendung ausgeführt wird (*meist Spiele, aber auch andere Anwendungen, wie z. B. PPT-Präsentationen*). Informationsmeldungen können unter Umständen als störend empfunden werden.

Wenn Sie die Option ***Benachrichtigung durch Firewall beim Spielen deaktivieren*** markieren, wählen Sie anschließend im Dropdown-Menü die Aktion aus, die ausgeführt werden soll, wenn eine neue Anwendung, für die noch keine Regeln definiert sind, versucht, über das Netzwerk zu kommunizieren. (*Anwendungen, bei denen normalerweise ein Fragedialog angezeigt wird*). Derartige Anwendungen können entweder zugelassen oder blockiert werden.

10.5.2. Definierte Netzwerke

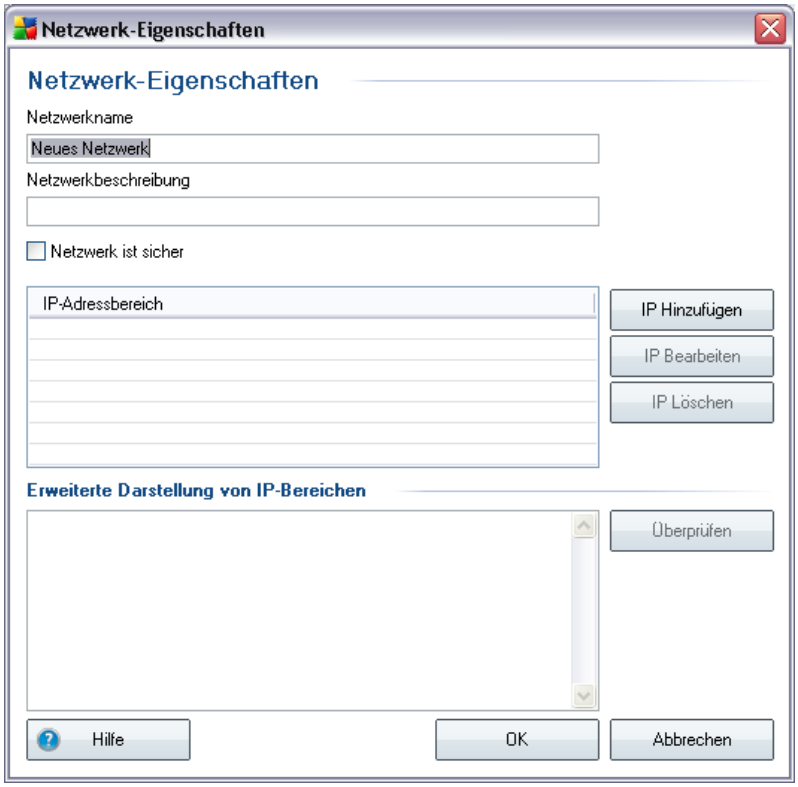


Der Dialog ***Definierte Netzwerke*** enthält eine Liste aller Netzwerke, mit denen Ihr Computer verbunden ist. Zu jedem erkannten Netzwerk werden folgende Informationen angegeben:

- ***Name*** - Namensliste aller Netzwerke, mit denen der Computer verbunden ist
- ***Netzwerksicherheit*** - Standard ist, alle Netzwerke als unsicher einzustufen. Nur wenn Sie sicher sind, dass ein Netzwerk sicher ist, können Sie es entsprechend kennzeichnen (*klicken Sie auf den Eintrag für das entsprechende Netzwerk. Wählen Sie im Kontextmenü die Option „Sicher" aus*). Alle sicheren Netzwerke werden in die Gruppe der Netzwerke aufgenommen, über welche die Anwendung mit folgender Anwendungsregel kommunizieren kann: ***Sichere zulassen***
- ***IP-Adressbereich***- Jedes Netzwerk wird automatisch als IP-Adressbereich angegeben und erkannt

Schaltflächen

- ***Netzwerk hinzufügen*** - Der Dialog ***Netzwerk-Eigenschaften*** wird geöffnet, und Sie können darin Parameter des neu definierten Netzwerks bearbeiten:



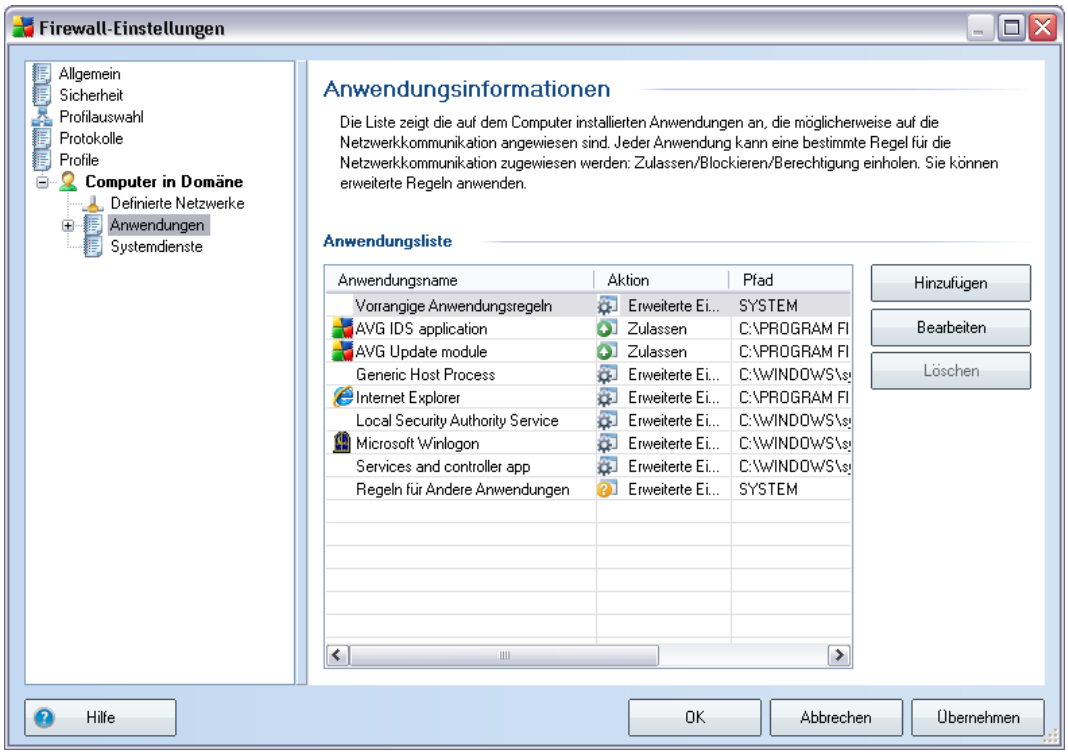
In diesem Dialog können Sie den ***Netzwerknamen*** sowie eine ***Netzwerkbeschreibung*** angeben und ggf. das Netzwerk als sicher kennzeichnen. Das neue Netzwerk kann manuell in einem separaten Dialog definiert werden, der über die Schaltfläche ***IP hinzufügen*** geöffnet wird (oder auch über ***IP bearbeiten*** / ***IP löschen***). In diesem Dialog können Sie das Netzwerk durch Angabe des IP-Bereichs oder der Maske definieren.

Für eine größere Anzahl von Netzwerken, die als Teil des neu erstellten Netzwerks definiert werden sollen, können Sie die Option ***Erweiterte Darstellung von IP-Bereichen*** verwenden: Geben Sie die Liste der Netzwerke in das entsprechende Textfeld ein (*alle Standardformate*

werden unterstützt). Klicken Sie auf ***Überprüfen*** , um sicherzustellen, dass das Format erkannt wird. Klicken Sie anschließend auf ***OK***, um die Daten zu bestätigen und zu speichern.

- ***Netzwerk bearbeiten*** - Der Dialog ***Netzwerk-Eigenschaften*** wird geöffnet (*siehe oben*). Sie können darin Parameter eines bereits definierten Netzwerks bearbeiten (*der Dialog ist identisch mit dem Dialog für das Hinzufügen eines neuen Netzwerks, beachten Sie daher die Beschreibung im vorherigen Absatz*)
- ***Netzwerk löschen*** - Der Eintrag des ausgewählten Netzwerks wird aus der Liste der Netzwerke gelöscht
- ***Sicher*** - Standard ist, alle Netzwerke als unsicher einzustufen. Nur wenn Sie sicher sind, dass ein Netzwerk sicher ist, können Sie dieses mit dieser Schaltfläche entsprechend kennzeichnen
- ***Hilfe*** – Die Hilfe zu dem Dialog wird geöffnet

10.5.3. Anwendungen

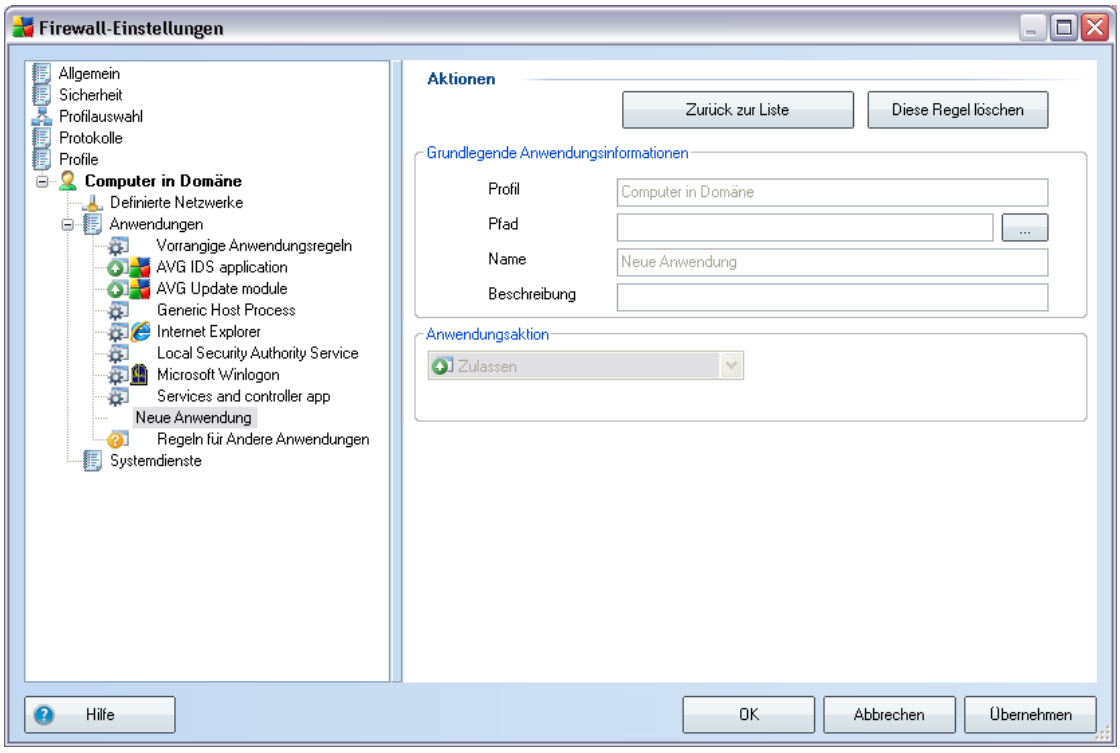


Im Dialog ***Anwendungsinformationen*** finden Sie eine Übersicht aller

Anwendungen, die über das Netzwerk kommunizieren. Die Liste kann mit den folgenden Schaltflächen bearbeitet werden:

- ***Hinzufügen*** - Der Dialog zur Definition des Regelsatzes einer neuen Anwendung wird geöffnet
- ***Bearbeiten*** - Der Dialog zur Bearbeitung des Regelsatzes einer vorhandenen Anwendung wird geöffnet
- ***Löschen*** - Die ausgewählte Anwendung wird aus der Liste gelöscht
- ***Hilfe*** – Die Hilfe zu dem Dialog wird geöffnet

Mit Hilfe der Schaltfläche ***Hinzufügen*** des Dialogs ***Anwendungen*** der ***Firewall-Einstellungen*** können Sie den Dialog zum Festlegen der Regeln einer neuen Anwendung öffnen.



In diesem Dialog können Sie die folgenden Optionen festlegen:

- ***Grundlegende Anwendungsinformationen*** – Name der Anwendung, eine kurze Beschreibung und ein Pfad zum Speicherort auf dem Laufwerk

- ***Anwendungsaktion*** – Wählen Sie aus dem Dropdown-Menü eine Regel, um das Verhalten der Anwendung festzulegen:

  - ***Erweiterte Einstellungen –*** Mit dieser Option können Sie die Details der Regeln bearbeiten, die im unteren Abschnitt des Dialogs angezeigt werden; *eine Beschreibung dieses Abschnitts finden Sie im Kapitel* ***Anwendung bearbeiten***

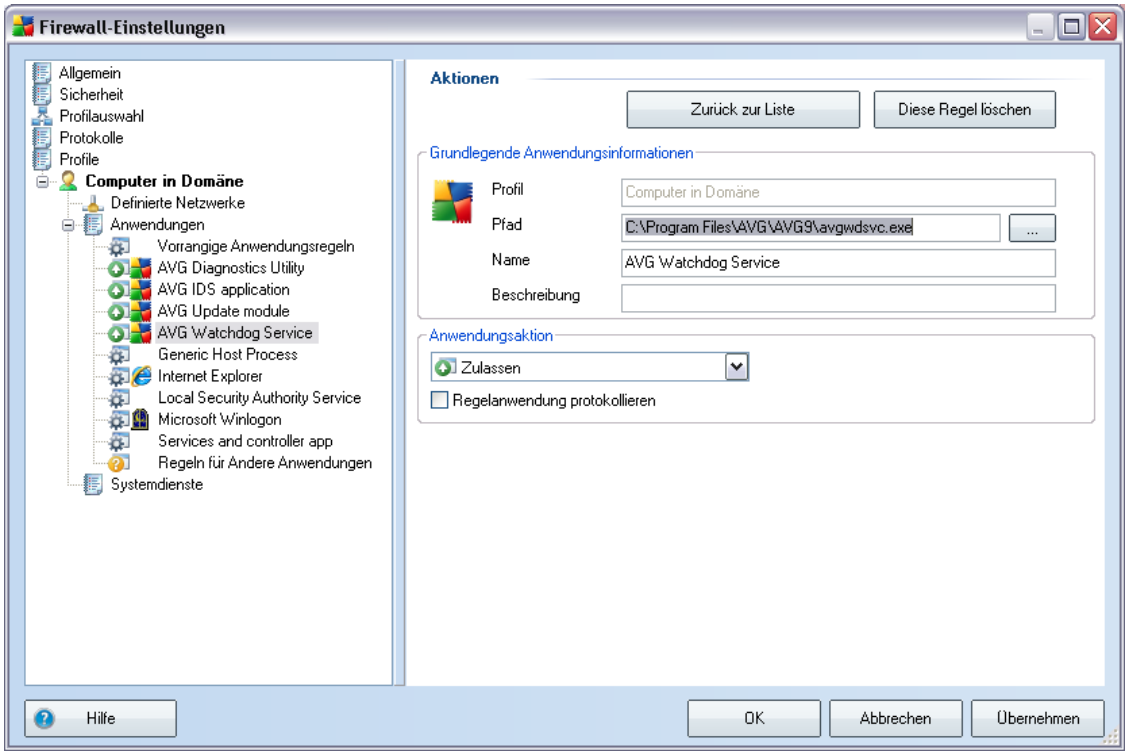
  - ***Zulassen –*** Alle Kommunikationsversuche der Anwendung werden zugelassen

  - ***Sichere zulassen –*** Die Anwendung darf nur mit sicheren Netzwerken kommunizieren (*Kommunikation mit dem geschützten Unternehmensnetzwerk zum Beispiel wird zugelassen, während Kommunikation mit dem Internet blockiert wird*); einen Überblick und eine Beschreibung sicherer Netzwerke finden Sie im Dialog ***Definierte Netzwerke***

  - ***Fragen –*** Jedes Mal, wenn die Anwendung versucht, mit dem Netzwerk zu kommunizieren, werden Sie gefragt, ob die Kommunikation zugelassen oder blockiert werden soll

  - ***Blockieren –*** Alle Kommunikationsversuche der Anwendung werden blockiert

Mit Hilfe der Schaltfläche ***Bearbeiten*** im Dialog ***Anwendungen*** der ***Firewall-Einstellungen*** können Sie den Dialog zur Bearbeitung der Regeln einer vorhandenen Anwendung aufrufen:



In diesem Dialog können Sie alle Parameter der Anwendung bearbeiten:

- ***Grundlegende Anwendungsinformationen***– Name der Anwendung, eine kurze Beschreibung sowie der Pfad zum Speicherort auf der Festplatte
- ***Anwendungsaktion***– Wählen Sie aus dem Dropdown-Menü eine Regel, um das Verhalten der Anwendung festzulegen:
  - ***Erweiterte Einstellungen –*** Mit dieser Option können Sie die Details der Regeln ändern, die im unteren Abschnitt des Dialogs angezeigt werden
  - ***Zulassen –*** Alle Kommunikationsversuche der Anwendung werden zugelassen
  - ***Sichere zulassen –*** Die Anwendung darf nur mit sicheren Netzwerken kommunizieren (*Kommunikation mit dem geschützten Unternehmensnetzwerk zum Beispiel wird zugelassen, während Kommunikation mit dem Internet blockiert wird*); einen Überblick und eine Beschreibung sicherer Netzwerke finden Sie im Dialog ***Definierte***

Netzwerke

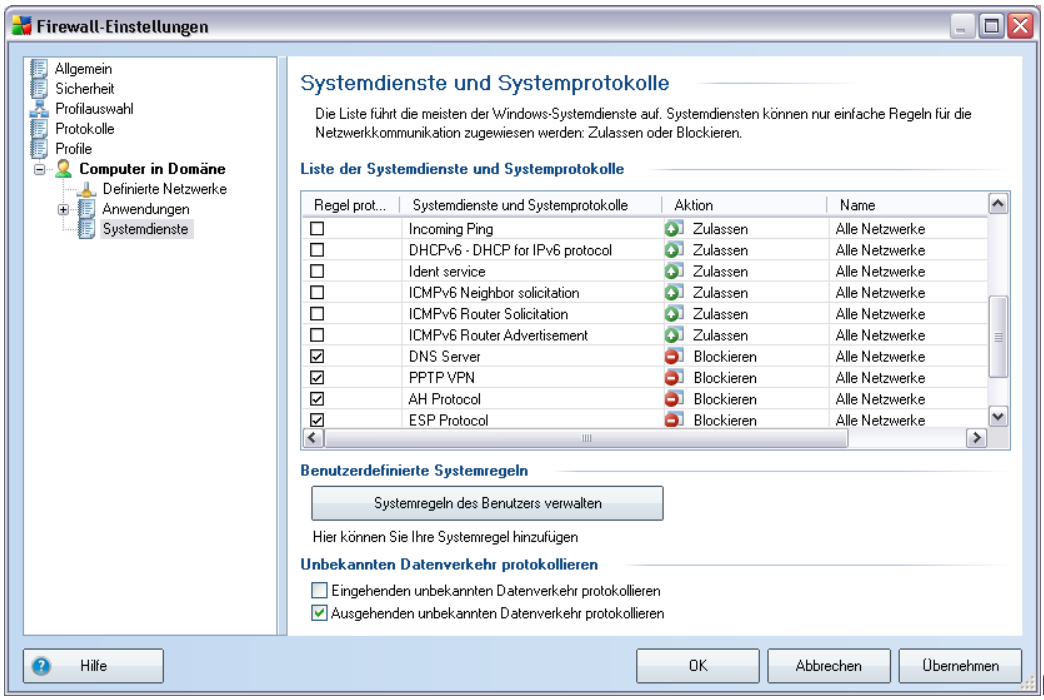
- ***Fragen –*** Jedes Mal, wenn die Anwendung versucht, mit dem Netzwerk zu kommunizieren, werden Sie gefragt, ob die Kommunikation zugelassen oder blockiert werden soll

- ***Blockieren –*** Alle Kommunikationsversuche der Anwendung werden blockiert

- ***Regelanwendung protokollieren***– Aktivieren Sie diese Aktion, wenn Sie möchten, dass alle Aktionen der ***Firewall*** in Bezug auf die Anwendung protokolliert werden sollen, für die Sie die Regeln erstellt haben. Die entsprechenden Protokolleinträge finden Sie anschließend im Dialog ***Protokolle***.

10.5.4. Systemdienste

Systemdienste und Protokolldialoge sollten NUR von erfahrenen Benutzern bearbeitet werden!



Der Dialog ***Systemdienste und Systemprotokolle*** enthält eine Übersicht über Systemdienste und Protokolle, die über das Netzwerk kommunizieren. Unter der Liste stehen zwei Optionen zur Auswahl: Aktivieren/deaktivieren Sie diese, um festzulegen,

ob der gesamte unbekannte Datenverkehr in beide Richtungen (*eingehend oder ausgehend*) protokolliert werden soll.

Schaltflächen

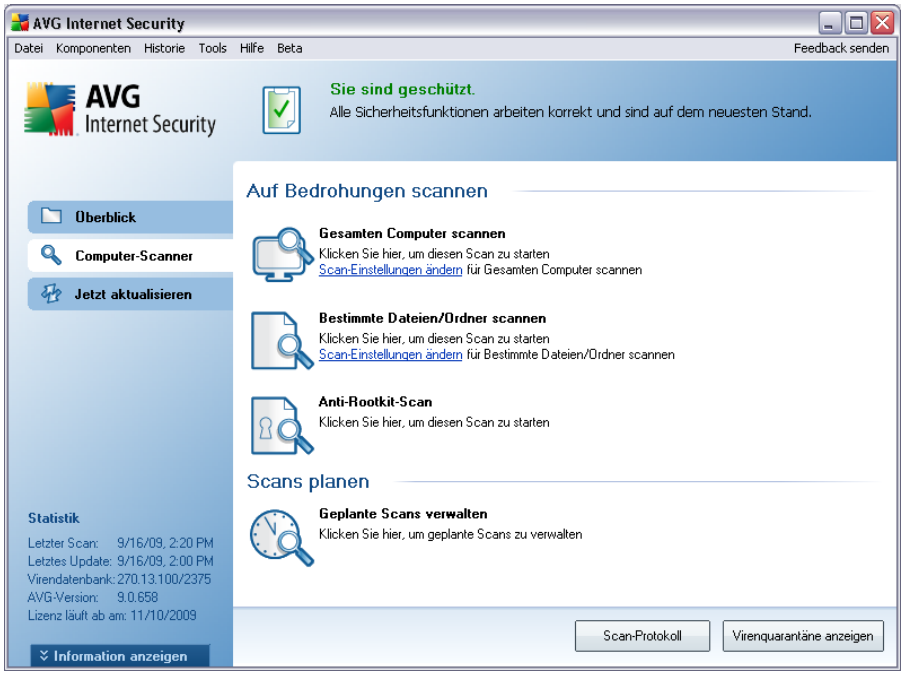
- ***Hinzufügen / Bearbeiten*** - Mit beiden Schaltflächen wird derselbe Dialog geöffnet, in dem Sie die Parameter für den jeweiligen Systemdienst bearbeiten können. Mit ***Hinzufügen*** wird ein leerer Dialog im Basismodus geöffnet (*kein Bereich für erweiterte Einstellungen, dieser kann jedoch durch Auswahl der erweiterten Einstellungen für die Anwendungsaktion geöffnet werden*); mit der Schaltfläche ***Bearbeiten*** wird derselbe Dialog mit bereits eingegebenen Daten zum ausgewählten Systemdienst geöffnet.

Systemdienste und Protokolldialoge sollten NUR von erfahrenen Benutzern bearbeitet werden!

11. AVG-Scans

Scans sind eine der wichtigsten Funktionen von **AVG 9 Internet Security**. Sie können Scans nach Bedarf (on-Demand) ausführen oder geplant regelmäßig nach einem festgelegten Zeitplan, der Ihren Anforderungen entspricht.

11.1. Benutzeroberfläche für Scans



Auf die Scan-Oberfläche von AVG kann über den Quick Link ***Computer-Scanner*** zugegriffen werden. Klicken Sie auf den Link, um zum Dialog ***Auf Bedrohungen scannen*** zu wechseln. Im Dialog finden Sie Folgendes:

- Übersicht über vordefinierte Scans – Drei verschiedene vom Softwarehersteller definierte Scans, die sich On-Demand oder in Zeitplänen verwenden lassen:
  - ***Gesamten Computer scannen***
  - ***Bestimmte Dateien/Ordner scannen***
  - ***Anti-Rootkit-Scan***

- Scans planen – Hier können Sie gegebenenfalls neue Scans definieren und neue Zeitpläne erstellen.

Schaltflächen

Auf der Scan-Oberfläche stehen Ihnen folgende Schaltflächen zur Verfügung:

- ***Scan-Protokoll*** – Hiermit wird der Dialog Übersicht über Scan-Ergebnisse mit dem gesamten Protokoll der Scans angezeigt
- ***Virenquarantäne anzeigen*** – Hiermit wird ein neues Fenster mit der Virenquarantäne geöffnet – ein Bereich, in dem erkannte Infektionen unter Quarantäne gestellt werden

11.2. Vordefinierte Scans

Eine der Hauptfunktionen von **AVG 9 Internet Security** ist ein bedarfsorientierter Scan. Tests On-Demand wurden entwickelt, um verschiedene Teile eines Computers zu scannen, wenn der Verdacht einer Virusinfektion besteht. Es wird dringend empfohlen, derartige Tests regelmäßig durchzuführen, auch wenn Sie denken, dass sich auf dem Computer kein Virus befinden kann.

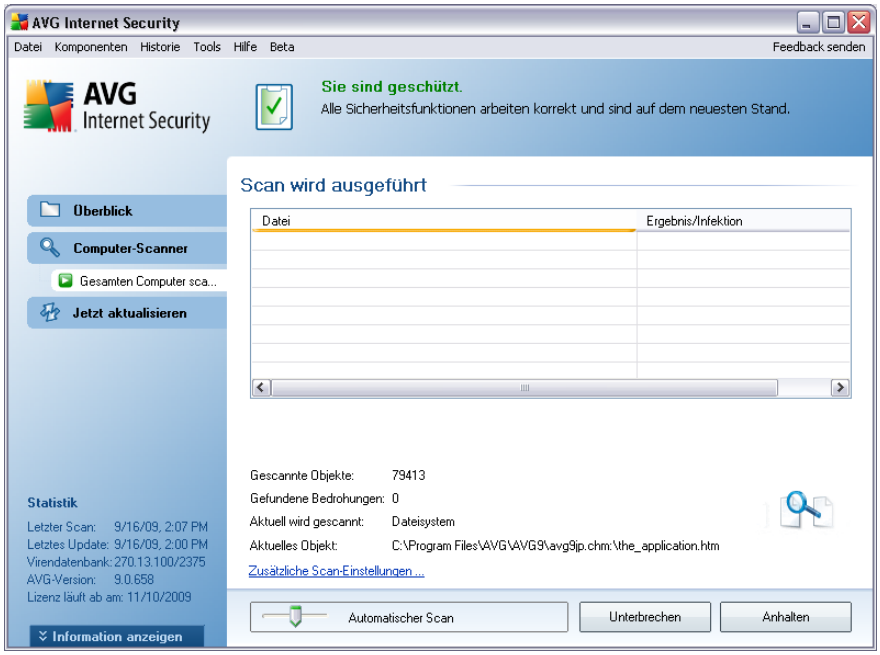
In **AVG 9 Internet Security** gibt es zwei vordefinierte Arten von Scans:

11.2.1. Gesamten Computer scannen

Gesamten Computer scannen – Hiermit wird Ihr gesamter Computer nach möglichen Infektionen und/oder potentiell unerwünschter Programmen durchsucht. Bei diesem Scan werden alle Festplatten Ihres Computers gescannt, gefundene Viren werden geheilt oder erkannte Infektionen in die ***Virenquarantäne*** verschoben. Ein Scan des gesamten Computers sollte auf einer Workstation mindestens einmal pro Woche geplant werden.

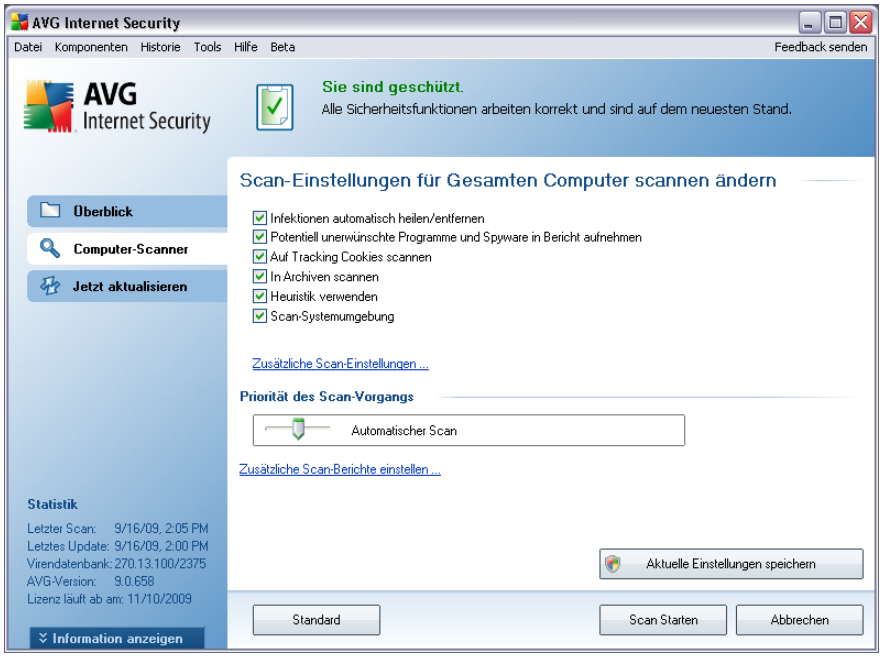
Start von Scans

Die Option ***Gesamten Computer scannen*** kann direkt von der Benutzeroberfläche für Scans durch Klicken auf das Symbol des Scans gestartet werden. Es müssen für diesen Scan keine weiteren Einstellungen vorgenommen werden. Der Scan startet sofort im Dialog ***Scan wird ausgeführt*** (*siehe Screenshot*). Der Scanvorgang kann bei Bedarf unterbrochen (***Unterbrechen***) oder abgebrochen (***Anhalten***) werden.



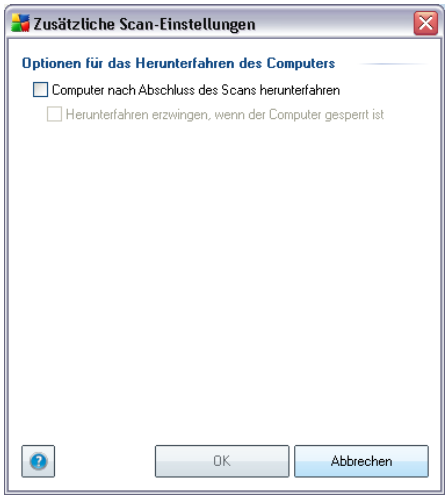
Bearbeitung der Scan-Konfiguration

Sie können die vordefinierten Standardeinstellungen der Option ***Gesamten Computer scannen*** bearbeiten. Klicken Sie auf den Link ***Scan-Einstellungen ändern*** , um den Dialog ***Scan-Einstellungen für Gesamten Computers scannen ändern*** zu öffnen. ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, Sie haben einen wichtigen Grund, sie zu ändern!***



- ***Scan-Parameter*** – In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter ein- bzw. ausschalten. Standardmäßig sind die meisten Parameter aktiviert und werden während des Scans verwendet.

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog ***Zusätzliche Scan-Einstellungen*** geöffnet, in dem Sie die folgenden Parameter festlegen können:



- ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).

- ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:

  - ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen; oder

  - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

  - Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Priorität des Scan-Vorgangs*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die mittlere Stufe eingestellt (*Automatischer Scan*), wodurch die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog ***Scan-Berichte***, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:

Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel* ***AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen*** *beschrieben. Wenn Sie die Standardkonfiguration der Option* ***Gesamten Computer scannen*** *ändern, können Sie Ihre neuen Einstellungen als Standardkonfiguration speichern, die für alle weiteren Scans des gesamten Computers verwendet wird.*

11.2.2. Bestimmte Dateien/Ordner scannen

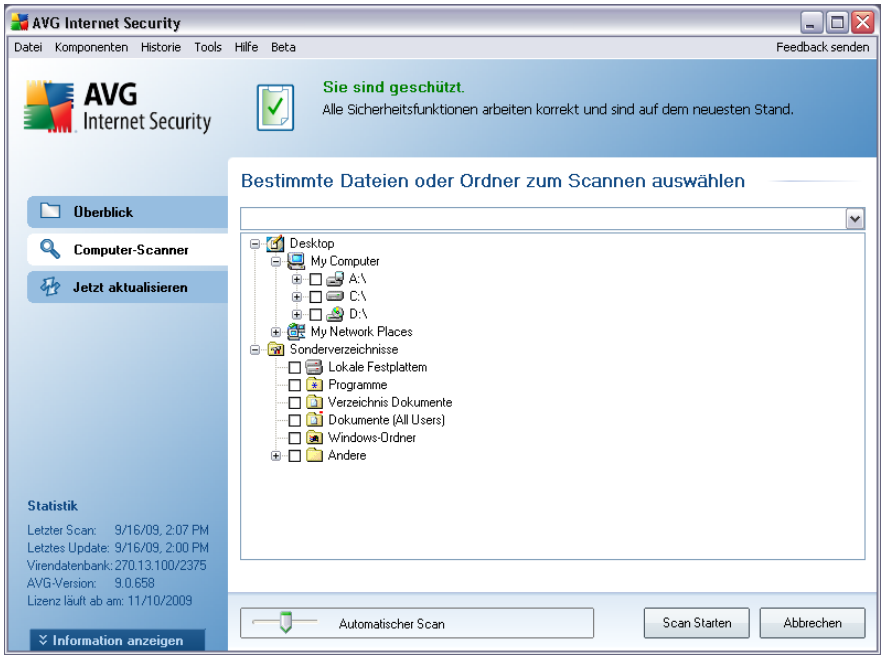
Bestimmte Dateien oder Ordner scannen – Scannt ausschließlich die Bereiche Ihres Computers, die Sie zum Scannen ausgewählt haben (*ausgewählte Ordner, Festplatten, Wechseldatenträger, CDs usw.*). Der Scan-Verlauf bei einer Virenerkennung sowie die Behandlung des Virus entsprechen dem Scan des gesamten Computers ***: Jedes gefundene Virus wird geheilt oder in die Virenquarantäne verschoben***. Das Scannen bestimmter Dateien oder Ordner kann verwendet werden, um eigene Scans und deren Zeitpläne nach Ihren Bedürfnissen einzurichten.

Start von Scans

Die Option ***Bestimmte Dateien/Ordner scannen*** kann direkt von der Benutzeroberfläche für Scans durch Klicken auf das Symbol des Scans gestartet werden. Es öffnet sich der Dialog ***Bestimmte Dateien oder Ordner zum Scannen auswählen***. Wählen Sie in der Baumstruktur Ihres Computers den zu scannenden Ordner aus. Der Pfad zu jedem Ordner wird automatisch generiert und wird in dem Textfeld im oberen Bereich dieses Dialogs angezeigt.

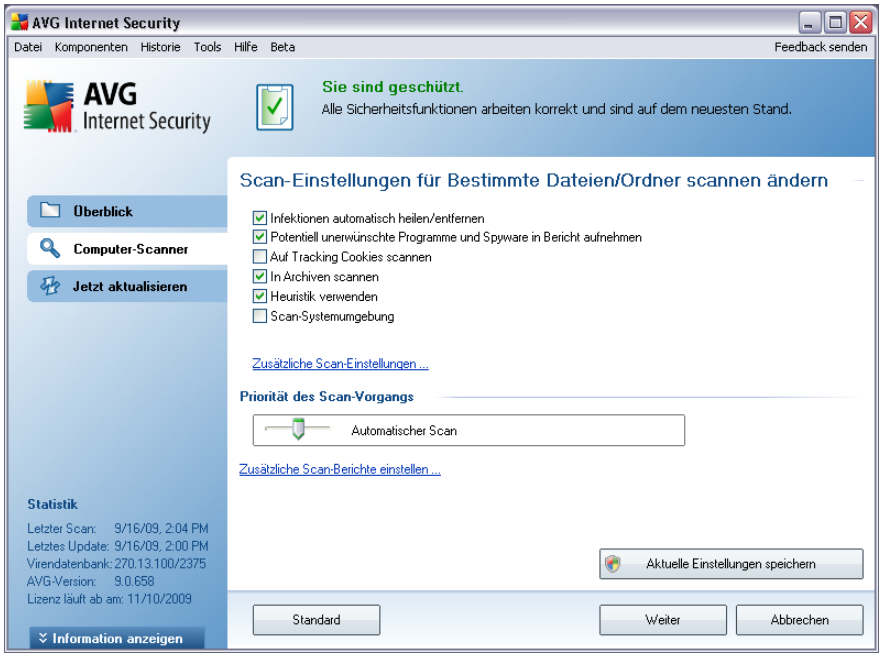
Es ist möglich, einen bestimmten Ordner zu scannen, jedoch seine Unterordner vom Scan auszuschließen. Setzen Sie dafür ein Minuszeichen „**-**" vor den automatisch generierten Pfad (*siehe Screenshot*). Um den gesamten Ordner vom Scan auszuschließen, verwenden Sie das Ausrufezeichen "!" parameter.

Klicken Sie zum Starten des Scans auf die Schaltfläche ***Scan starten***. Der Scanvorgang gleicht im Grunde genommen dem Scan des gesamten Computers.



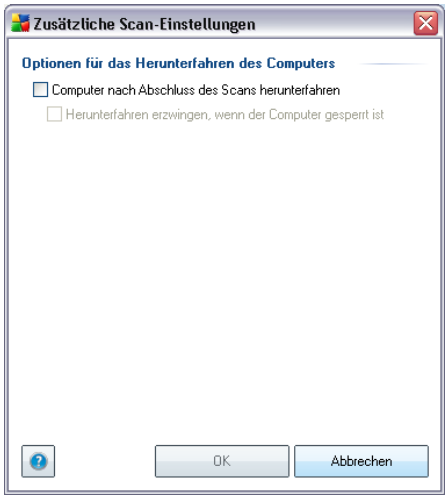
Bearbeitung der Scan-Konfiguration

Sie können die vordefinierten Standardeinstellungen der Option ***Bestimmte Dateien oder Ordner scannen*** bearbeiten. Klicken Sie auf den Link ***Scan-Einstellungen ändern*** , um den Dialog ***Scan-Einstellungen für Bestimmte Dateien/Ordner scannen ändern*** zu öffnen. ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, Sie haben einen wichtigen Grund, sie zu ändern!***



- ***Scan-Parameter*** – In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter aktivieren bzw. deaktivieren(*Weitere Informationen zu diesen Einstellungen finden Sie im Kapitel Erweiterte AVG-Einstellungen / Scans / Bestimmte Dateien/Ordner scannen*).

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog „Zusätzliche Scan-Einstellungen" geöffnet, in dem Sie die folgenden Parameter festlegen können:



- ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).

- ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:

  - ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen; oder

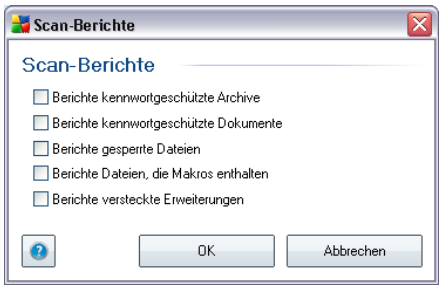
  - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

  - Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir

empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Priorität des Scan-Vorgangs*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die mittlere Stufe eingestellt (*Automatischer Scan*), wodurch die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog ***Scan-Berichte***, wo Sie wählen können, welche Scan-Ergebnisse berichtet werden sollen:



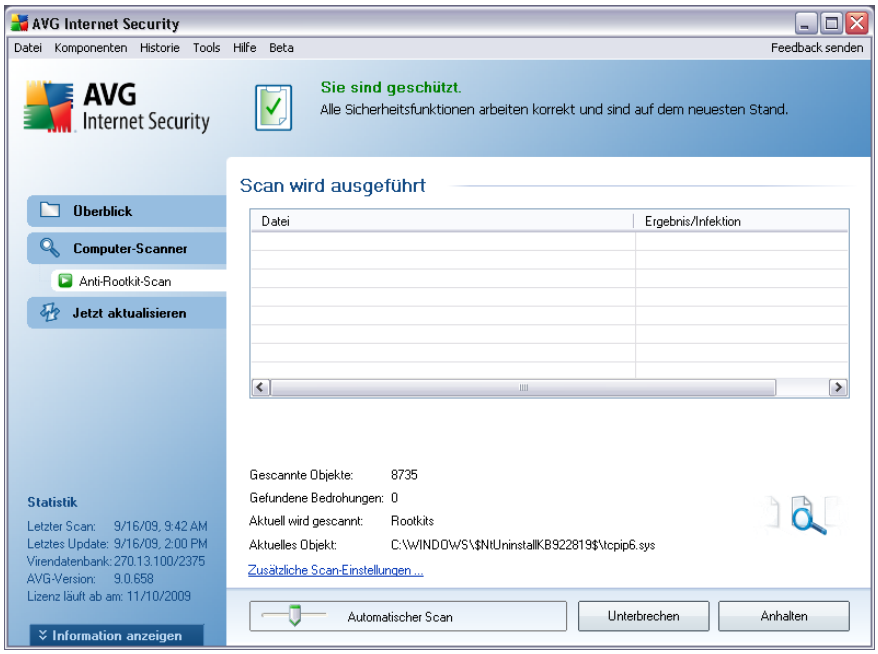
Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel* ***AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen*** *beschrieben. Wenn Sie die Standardkonfiguration der Option* ***Bestimmte Dateien oder Ordner scannen*** *ändern, können Sie Ihre neuen Einstellungen als Standardkonfiguration speichern, die für alle weiteren Scans bestimmter Dateien oder Ordner verwendet wird. Diese Konfiguration wird auch als Vorlage für alle Ihre neuen geplanten Scans verwendet (alle benutzerdefinierten Scans basieren auf der aktuellen Konfiguration des Scans bestimmter Dateien oder Ordner).*

11.2.3. Anti-Rootkit-Scan

Anti-Rootkit-Scan überprüft Ihren Computer auf mögliche Rootkits (*Programme und Technologien, die Aktivitäten von Malware auf Ihrem Computer verbergen können*). Wenn ein Rootkit erkannt wird, heißt das nicht unbedingt, dass Ihr Computer infiziert ist. In manchen Fällen können bestimmte Treiber oder Abschnitte zulässiger Anwendungen fälschlicherweise als Rootkits erkannt werden.

Start von Scans

Anti-Rootkit-Scan können Sie direkt über die Benutzeroberfläche für Scans starten, indem Sie auf das Scan-Symbol klicken. Für diesen Scantyp müssen keine weiteren Einstellungen vorgenommen werden. Der Scan startet sofort im Dialog ***Scan wird ausgeführt*** (*siehe Screenshot*). Der Scanvorgang kann bei Bedarf unterbrochen (***Unterbrechen***) oder abgebrochen (***Anhalten***) werden.



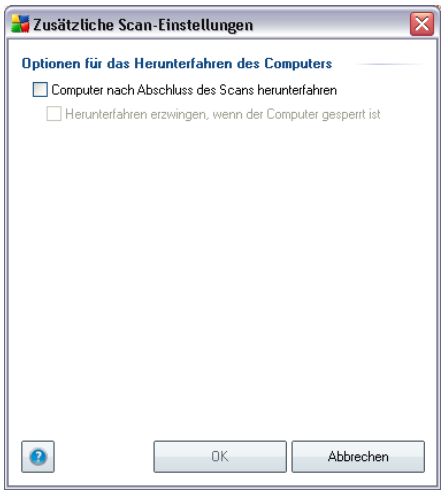
Bearbeitung der Scan-Konfiguration

Anti-Rootkit-Scan wird stets mit den Standardeinstellungen gestartet; die Scanparameter können nur im Dialog ***Erweiterte Einstellungen von AVG/Anti-Rootkit*** bearbeitet werden. Auf der Benutzeroberfläche für Scans steht lediglich die folgende Konfiguration zur Verfügung:

- ***Automatischer Scan*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die mittlere Stufe eingestellt (*Automatischer Scan*), wodurch die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer*

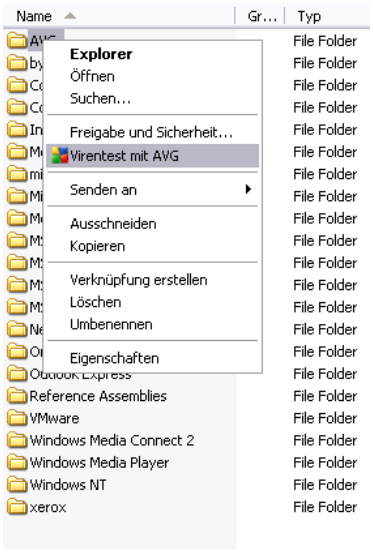
arbeiten und Ihnen die Dauer des Scans nicht wichtig ist). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link lässt sich der Dialog ***Zusätzliche Scan-Einstellungen*** öffnen, in dem Sie mögliche Bedingungen für ein Herunterfahren des Computers im Hinblick auf den ***Anti-Rootkit-Scan*** festlegen können (***Computer nach Abschluss des Scans herunterfahren***, *möglicherweise* ***Herunterfahren erzwingen, wenn der Computer gesperrt ist***):



11.3. Scans aus dem Windows Explorer

Neben den vordefinierten Scans, die für den gesamten Computer oder ausgewählte Bereiche gestartet werden, umfasst **AVG 9 Internet Security** auch eine Option für die Schnellprüfung eines bestimmten Objekts direkt in Windows Explorer. Wenn Sie eine unbekannte Datei öffnen und ihren Inhalt nicht genau kennen, möchten Sie sie möglicherweise On-Demand überprüfen. Gehen Sie dazu wie folgt vor:



- Markieren Sie im Windows Explorer die Datei (oder den Ordner), die Sie überprüfen möchten
- Klicken Sie mit der rechten Maustaste auf das Objekt, um das Kontextmenü zu öffnen
- Wählen Sie die Option ***Virentest mit AVG Anti-Virus***, um die Datei mit AVG zu scannen

11.4. Scannen von Befehlszeilen

Mit **AVG 9 Internet Security** haben Sie die Möglichkeit, einen Scan von der Befehlszeile aus durchzuführen. Diese Option kann beispielsweise für Server oder für die Erstellung eines Batch-Skripts angewendet werden, das nach dem Hochfahren des Computers automatisch gestartet werden soll. Wenn Sie einen Scan von der Befehlszeile aus durchführen, können Sie einen Großteil der Parameter anwenden, die auch in der Benutzeroberfläche von AVG zur Verfügung stehen.

Um einen AVG-Scan von der Befehlszeile aus zu starten, führen Sie den folgenden Befehl in dem Ordner aus, in dem AVG installiert wurde:

- ***avgscanx*** für 32-Bit-Betriebssysteme
- ***avgscana*** für 64-Bit-Betriebssysteme

Syntax des Befehls

Die Syntax des Befehls lautet:

- ***avgscanx /Parameter*** ... z. B. ***avgscanx /comp***, um den gesamten Computer zu scannen
- ***avgscanx /Parameter /Parameter*** ... Wenn mehrere Parameter verwendet werden, müssen diese in einer Reihe geschrieben und mit einem Leerzeichen und einem Schrägstrich getrennt werden.
- Wenn ein Parameter einen bestimmten Wert erfordert (der Parameter ***/scan*** benötigt z. B. Informationen über die Bereiche Ihres Computers, die gescannt werden sollen, und die genaue Pfadangabe zum ausgewählten Bereich), werden die einzelnen Werte durch Kommata getrennt, z. B.: ***avgscanx /scan=C:\,D:***

Scan-Parameter

Um eine vollständige Übersicht der verfügbaren Parameter anzuzeigen, geben Sie den entsprechenden Befehl mit dem Parameter /? oder /HELP ein (z. B. ***avgscanx /?***). Der einzige obligatorische Parameter ist /SCAN, mit dem festgelegt wird, welche Bereiche des Computers gescannt werden sollen. Eine genauere Erläuterung der Optionen finden Sie in der Übersicht zu Befehlszeilenparametern.

Drücken Sie die ***Eingabetaste***, um den Scan auszuführen. Der Scan-Vorgang kann mit den Tastenkombinationen ***Strg+C*** oder ***Strg+Pause*** abgebrochen werden.

CMD-Scan über die Benutzeroberfläche starten

Wenn Ihr Computer im abgesicherten Modus arbeitet, können Sie den Befehlszeilen-Scan auch über die grafische Benutzeroberfläche starten. Der Scan selbst wird von der Befehlszeile aus gestartet. Im Dialog ***Erstellungshilfe über die Befehlszeile*** können Sie nur die meisten Scan-Parameter in der übersichtlichen Benutzeroberfläche festlegen.

Da der Zugriff auf diesen Dialog nur im abgesicherten Modus von Windows möglich ist, können Sie sich genauere Informationen zu diesem Dialog in der Hilfedatei ansehen, die direkt in diesem Dialog geöffnet werden kann.

11.4.1. Parameter für CMD-Scan

Die folgende Liste enthält alle Parameter, die zum Scannen von der Befehlszeile aus zur Verfügung stehen:

- ***/SCAN*** Bestimmte Dateien/ Ordner scannen /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- ***/COMP*** Gesamten Computer scannen
- ***/HEUR*** Heuristische Analyse verwenden
- ***/EXCLUDE*** Pfad oder Datei(en) vom Scan ausschließen
- ***/@*** Befehlsdatei /Dateiname/
- ***/EXT*** Diese Erweiterungen scannen /z. B. EXT=EXE,DLL/
- ***/NOEXT*** Diese Erweiterungen nicht scannen /z. B. NOEXT=JPG/
- ***/ARC*** Archive scannen
- ***/CLEAN*** Automatisch bereinigen
- ***/TRASH*** Infizierte Dateien in die Virenquarantäne verschieben
- ***/QT*** Schnelltest
- ***/MACROW*** Makros in Bericht aufnehmen
- ***/PWDW*** Kennwortgeschützte Dateien in Bericht aufnehmen
- ***/IGNLOCKED*** Gesperrte Dateien ignorieren
- ***/REPORT*** Bericht in Datei /Dateiname/
- ***/REPAPPEND*** An die Berichtsdatei anhängen
- ***/REPOK*** Nicht infizierte Dateien als OK in Bericht aufnehmen
- ***/NOBREAK*** Kein Abbrechen mit STRG-PAUSE
- ***/BOOT*** MBR/BOOT-Test aktivieren
- ***/PROC*** Aktive Prozesse scannen

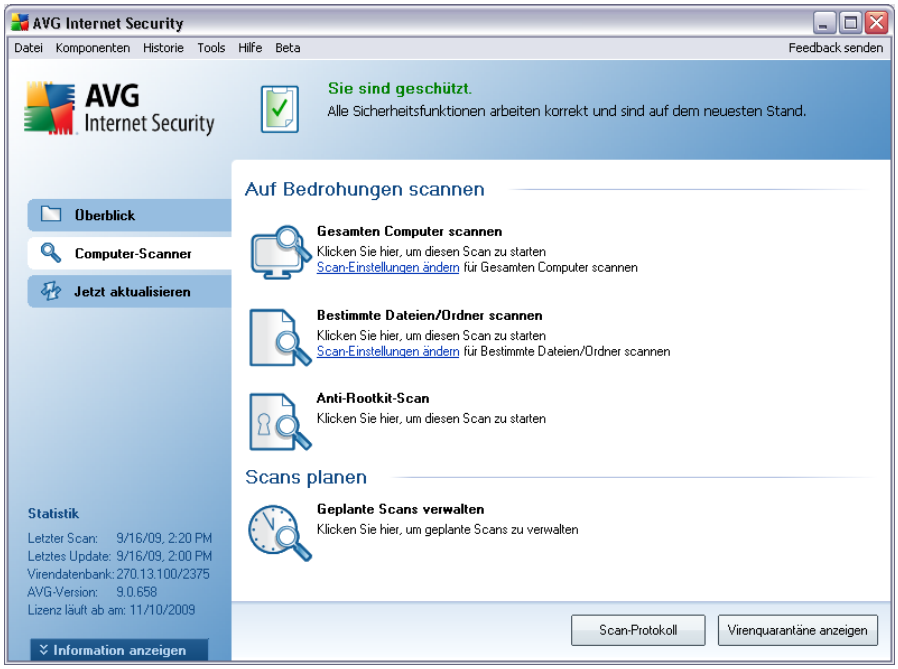
- ***/PUP*** „Potentiell unerwünschte Programme“ in Bericht aufnehmen
- ***/REG*** Registry scannen
- ***/COO*** Cookies scannen
- ***/?*** Hilfe zu diesem Thema anzeigen
- ***/HELP*** Hilfe zu diesem Thema anzeigen
- ***/PRIORITY*** Scan-Priorität einstellen /Low, Auto, High/ (siehe Erweiterte Einstellungen/Scans)
- ***/SHUTDOWN*** Computer nach Abschluss des Scans herunterfahren
- ***/FORCESHUTDOWN*** Herunterfahren erzwingen, wenn der Scan abgeschlossen ist
- ***/ADS*** Alternative Datenströme scannen (nur NTFS)

11.5. Scans planen

Mit **AVG 9 Internet Security** können Sie On-Demand-Scans (z. B. wenn Sie befürchten, dass Ihr Computer infiziert wurde) oder einen geplanten Scan ausführen. Es wird dringend empfohlen, geplante Scans auszuführen. Auf diese Weise sorgen Sie dafür, dass Ihr Computer gegen Infektionen geschützt ist, und Sie müssen sich nicht darum kümmern, ob und wann ein Scan gestartet werden soll.

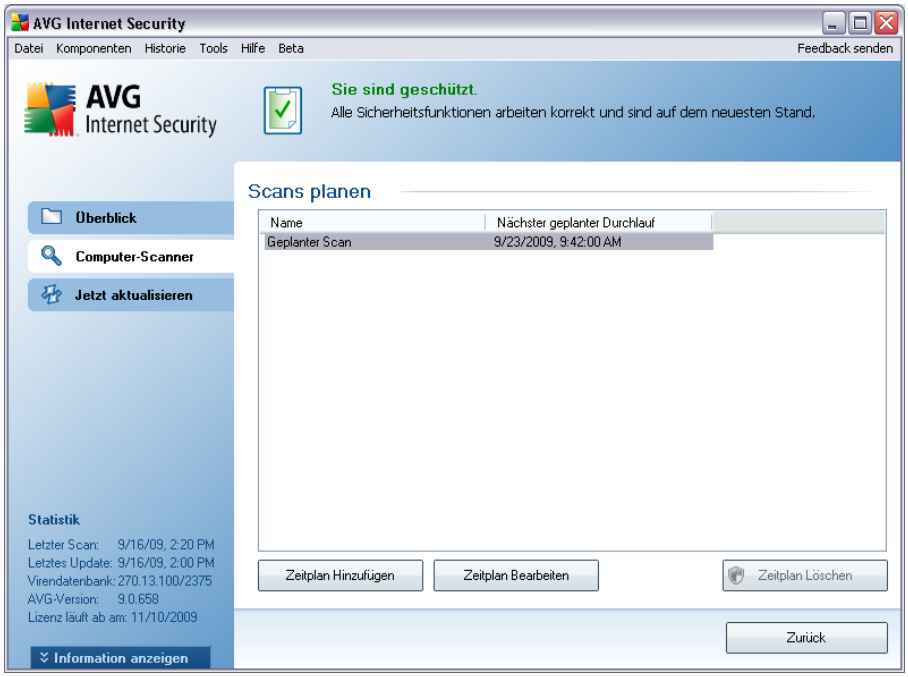
Sie sollten die Funktion ***Gesamten Computer scannen*** regelmäßig, mindestens einmal pro Woche, starten. Wenn möglich, sollten Sie Ihren gesamten Computer täglich scannen. Dies ist auch die Standardkonfiguration für geplante Scans. Wenn der Computer immer eingeschaltet ist, können Sie die Scans für Zeiten außerhalb der Arbeitszeit planen. Wenn der Computer manchmal ausgeschaltet ist, werden die geplanten Scans beim Start des Computers ausgeführt, wenn eine Aufgabe verpasst wurde.

Um neue Span-Pläne zu erstellen, gehen Sie auf der Scan-Oberfläche von AVG unten zum Abschnitt ***Scans planen***:



Scans planen

Klicken Sie im Bereich ***Scans planen*** auf das grafische Symbol, um den Dialog ***Scans planen*** zu öffnen, in dem eine Liste aller gegenwärtig geplanten Scans angezeigt wird:



Sie können Scans mithilfe der folgenden Schaltflächen bearbeiten oder hinzufügen:

- ***Zeitplan Hinzufügen*** – Mit dieser Schaltfläche wird der Dialog ***Einstellungen für geplanten Scan*** auf dem Reiter ***Einstellungen für den Zeitplan*** geöffnet. In diesem Dialog können Sie die Parameter für den neu definierten Scan festlegen.

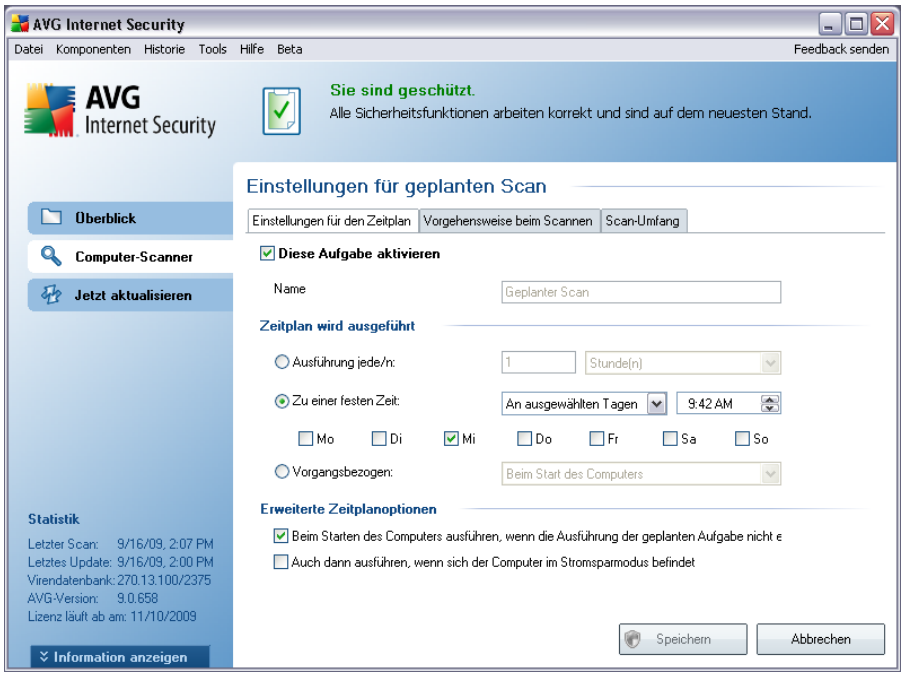
- ***Zeitplan Bearbeiten*** – Diese Schaltfläche steht nur zur Verfügung, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. In diesem Fall ist die Schaltfläche aktiv, und Sie können darauf klicken, um zum Dialog ***Einstellungen für geplanten Scan*** auf dem Reiter ***Einstellungen für den Zeitplan*** zu wechseln. Hier sind bereits Parameter des ausgewählten Scans festgelegt und können bearbeitet werden.

- ***Zeitplan Löschen*** – Diese Schaltfläche ist ebenfalls nur aktiv, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. Dieser Scan wird durch Klicken auf die Schaltfläche aus der Liste gelöscht. Sie können jedoch nur Ihre eigenen Scans entfernen. Der ***Zeitplan für Scans des gesamten Computers***, der in den Standardeinstellungen vordefiniert ist, kann nicht gelöscht werden.

- ***Zurück*** – Zurück zur Scan-Oberfläche von AVG

11.5.1. Einstellungen für den Zeitplan

Wenn Sie einen neuen Test und dessen regulären Start planen möchten, machen Sie im Dialog ***Einstellungen für geplanten Test*** die entsprechenden Angaben (*klicken Sie auf die Schaltfläche* ***Scan-Zeitplan hinzufügen*** *im Dialog* ***Scans planen***). Der Dialog ist in drei Reiter unterteilt:***Einstellungen für den Zeitplan*** *– siehe Bild unten* (*der Standardreiter, zu dem Sie automatisch zurückgeführt werden*), ***Vorgehensweise beim Scannen*** und ***Scan-Umfang***.



Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um den geplanten Scan vorübergehend zu deaktivieren. Anschließend können Sie den Zeitplan bei Bedarf hier wieder aktivieren.

Geben Sie anschließend dem zu erstellenden und zu planenden Scan einen Namen. Geben Sie den Namen im Textfeld ***Name*** ein. Wählen Sie nach Möglichkeit kurze, beschreibende Namen für Ihre Scans, damit Sie die einzelnen Scans später leichter unterscheiden und wiederfinden können.

Beispiel: *Sie sollten einen Scan nicht „Neuer Scan" oder „Mein Scan" nennen, da diese Namen nichts darüber aussagen, was der Scan tatsächlich überprüft. Ein Beispiel für einen guten, beschreibenden Namen wäre andererseits „Scan von Systembereichen" usw. Es ist auch nicht erforderlich, im Namen des Scans*

anzugeben, ob es sich um einen Scan des gesamten Computers handelt oder lediglich um den Scan bestimmter Dateien oder Ordner. Ihre eigenen Scans sind immer bestimmte Versionen eines Scans bestimmter Dateien oder Ordner.

In diesem Dialog können Sie weiterhin folgende Parameter für den Scan festlegen:

- ***Zeitplan wird ausgeführt*** – Legen Sie das Zeitintervall für den Start des neu geplanten Scans fest. Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum (***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Scans auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

- ***Erweiterte Zeitplanoptionen*** – In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist.

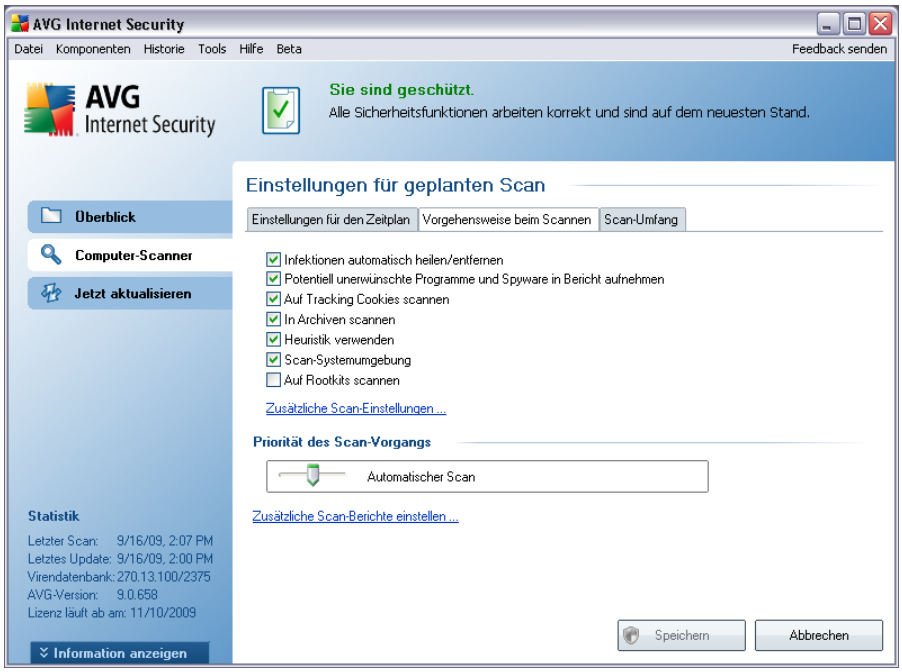
Schaltflächen im Dialog „Einstellungen für geplanten Scan"

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Zu testende Objekte***) zwei Schaltflächen zur Verfügung, die auf allen Reitern die gleichen Funktionen haben:

- ***Speichern*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.

11.5.2. Vorgehensweise beim Scannen



Der Reiter ***Vorgehensweise beim Scannen*** enthält eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. Standardmäßig sind die meisten Parameter aktiviert und ihre Funktionen werden während des Scans angewandt. Wenn Sie keinen wichtigen Grund haben, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten:

- ***Infektionen automatisch heilen/entfernen*** – (*standardmäßig aktiviert*): Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch geheilt werden kann oder wenn Sie diese Option deaktivieren, werden Sie über einen Virenfund unterrichtet, und Sie können entscheiden, was mit der erkannten Infektion geschehen soll. Es wird empfohlen, die infizierte Datei in die ***Virenquarantäne*** zu verschieben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert* ***): Dieser Parameter steuert die Funktion von*** Anti-Virus, mit der potentiell unerwünschte Programme (*ausführbare Dateien, die Spyware oder Adware sein können*) erkannt und blockiert oder entfernt werden können;

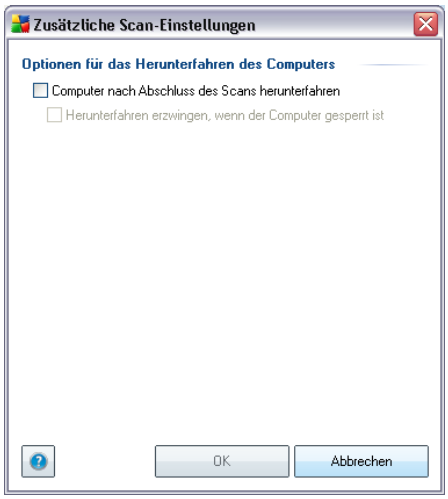
- ***Auf Tracking Cookies scannen*** – (*standardmäßig aktiviert*): Dieser

Parameter der Komponente ***Anti-Spyware*** legt fest, dass beim Scan Cookies erkannt werden (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und zum Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte ihrer Warenkörbe*);

- ***In Archiven scannen*** – (*standardmäßig aktiviert*): Dieser Parameter legt fest, dass Scans alle Dateien überprüfen sollen, selbst wenn sie in Archiven wie ZIP, RAR usw. gespeichert sind.
- ***Heuristik verwenden*** – (*standardmäßig aktiviert*): Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet.
- ***Scan-Systemumgebung*** – (*standardmäßig aktiviert*): Beim Scan werden auch die Systembereiche Ihres Computers überprüft;
- ***Auf Rootkits scannen*** – Aktivieren Sie diese Option, wenn die Rootkit-Erkennung während des Scans des gesamten Computers durchgeführt werden soll. Die Rootkit-Erkennung kann über die Komponente ***Anti-Rootkit*** auch separat durchgeführt werden;

Anschließend können Sie die Scan-Konfiguration wie folgt ändern:

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog ***Zusätzliche Scan-Einstellungen*** geöffnet, in dem Sie die folgenden Parameter festlegen können:



- ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).

- ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:

  - ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen; oder

  - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

  - Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Priorität des Scan-Vorgangs*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die mittlere Stufe eingestellt (*Automatischer Scan*), wodurch die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog ***Scan-Berichte***, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:

Hinweis: *Standardmäßig ist die Scan-Konfiguration so eingestellt, dass eine optimale Leistung erzielt wird. Wenn Sie keinen wichtigen Grund haben, die Scan-Einstellungen zu ändern, wird dringend empfohlen, die vordefinierte Konfiguration beizubehalten. Änderungen an der Konfiguration sollten nur von erfahrenen Benutzern durchgeführt werden. Weitere Optionen für die Scan-Konfiguration finden Sie im Dialog* ***Erweiterte Einstellungen****, den Sie über das Systemmenü mit* ***Tools/ Erweiterte Einstellungen*** *aufrufen können.*

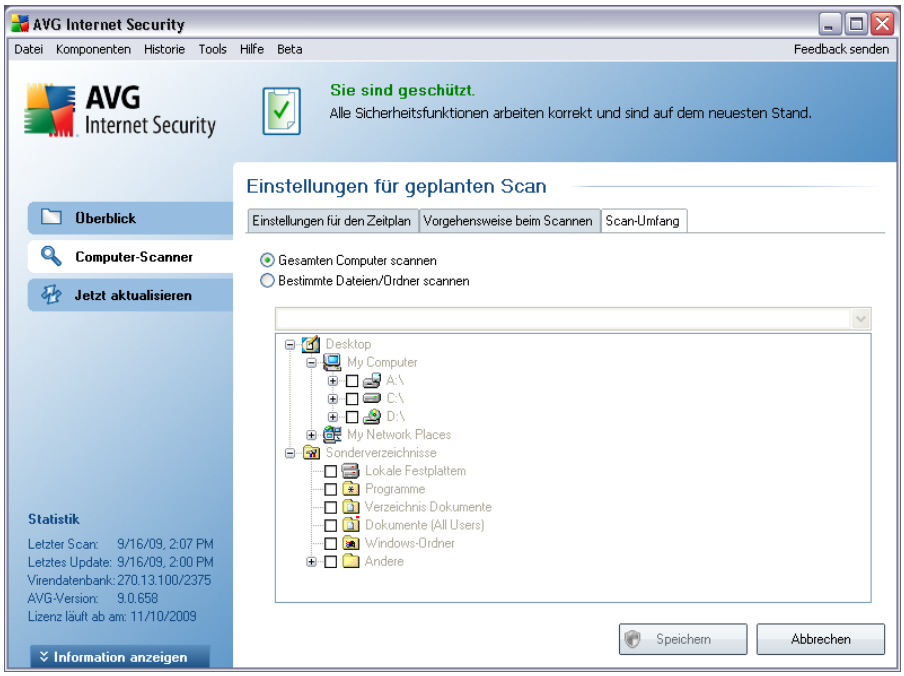
Schaltflächen

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Zu testende Objekte***) zwei Schaltflächen zur Verfügung, die auf allen Reitern dieselbe Funktion haben:

- ***Übernehmen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.

11.5.3. Zu testende Objekte



Auf dem Reiter ***Zu testende Objekte*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien/Ordner scannen planen möchten. Wenn Sie die Option „Bestimmte Dateien/Ordner scannen" auswählen, wird im unteren Bereich dieses Dialogs die angezeigte Baumstruktur aktiviert, und Sie können die zu scannenden Ordner festlegen.

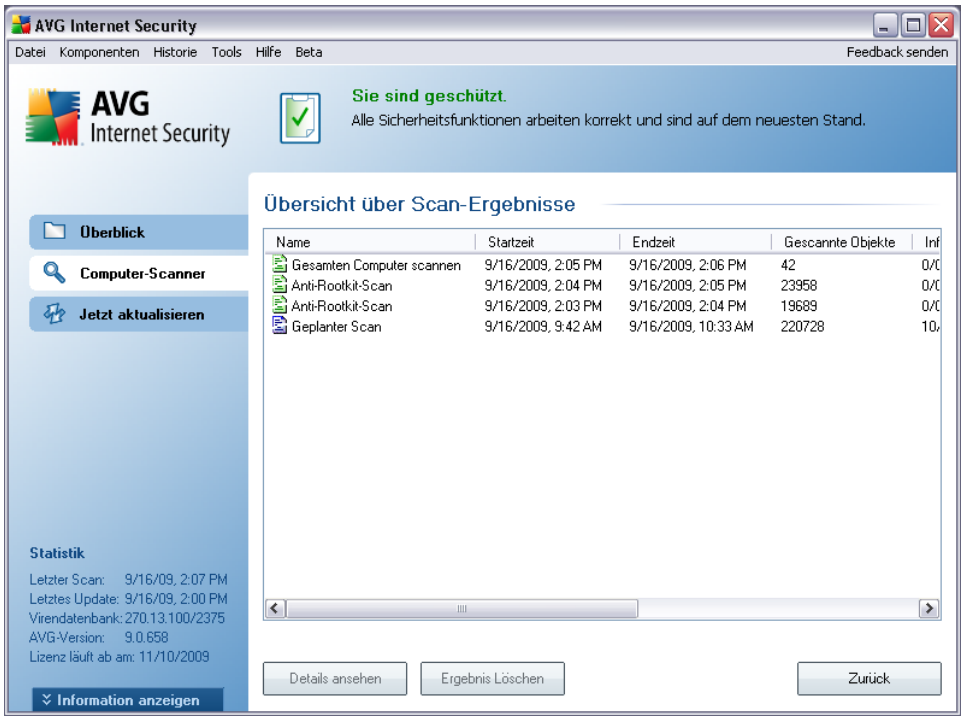
Schaltflächen im Dialog „Einstellungen für geplanten Scan"

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Zu testende Objekte***) zwei Schaltflächen zur Verfügung, die auf allen Reitern die gleichen Funktionen haben:

- ***Speichern*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.

11.6. Übersicht über Scan-Ergebnisse



Der Dialog ***Übersicht über Scan-Ergebnisse*** ist über die Scan-Oberfläche von AVG über die Schaltfläche ***Scan-Ergebnisse*** verfügbar. Im Dialog wird eine Liste aller vorher gestarteten Scans und Informationen zu deren Ergebnissen angezeigt:

- ***Name*** – Scan-Ziel. Dabei kann es sich entweder um den Namen eines vordefinierten Scans oder um einen Namen handeln, den Sie Ihrem eigenen geplanten Scan gegeben haben. Jeder Name enthält ein Symbol, das das Scan-Ergebnis anzeigt:

  – Ein grünes Symbol zeigt an, dass beim Scan keine Infektion gefunden wurde

  – Ein blaues Symbol zeigt an, dass beim Scan eine Infektion gefunden, das infizierte Objekt jedoch automatisch entfernt wurde

 – Ein rotes Symbol zeigt an, dass beim Scan eine Infektion gefunden wurde, die nicht entfernt werden konnte!

Jedes Symbol kann entweder ganz oder halb angezeigt werden. Ein vollständig angezeigtes Symbol zeigt an, dass ein Scan vollständig abgeschlossen und korrekt beendet wurde. Ein unvollständig angezeigtes Symbol zeigt an, dass der Scan unterbrochen oder abgebrochen wurde.

Hinweis: *Genauere Informationen zu jedem Scan finden Sie im Dialog* ***Scan-Ergebnisse****, auf den Sie über die Schaltfläche* ***Details ansehen*** *(im unteren Teil des Dialogs) zugreifen können.*

- ***Startzeit*** – Datum und Uhrzeit des gestarteten Scans
- ***Endzeit*** – Datum und Uhrzeit des Scan-Endes
- ***Gescannte Objekte*** – Anzahl der gescannten Objekte
- ***Infektionen*** – Anzahl der erkannten/entfernten Vireninfektionen
- ***Spyware*** – Anzahl der erkannten/entfernten Spyware
- ***Informationen zum Scan-Protokoll*** – Information zum Ablauf und zum Ergebnis des Scans (normalerweise nach dessen Abschluss oder bei Unterbrechung)

Schaltflächen

Im Dialog ***Übersicht über Scan-Ergebnisse*** stehen folgende Schaltflächen zur Verfügung:

- ***Details ansehen*** – Diese Schaltfläche ist nur aktiv, wenn in der oben genannten Übersicht ein bestimmter Scan ausgewählt wurde. Klicken Sie darauf, um zum Dialog ***Scan-Ergebnisse*** zu gelangen, wo Sie detaillierte Daten zum ausgewählten Scan erhalten
- ***Ergebnis löschen*** – Diese Schaltfläche ist nur aktiv, wenn in der oben genannten Übersicht ein bestimmter Scan ausgewählt wurde. Klicken Sie darauf, um das ausgewählte Element aus der Übersicht über die Scan-Ergebnisse zu entfernen
- ***Zurück*** – Mit dieser Schaltfläche gelangen Sie zurück zum Standarddialog

der Scan-Oberfläche von AVG

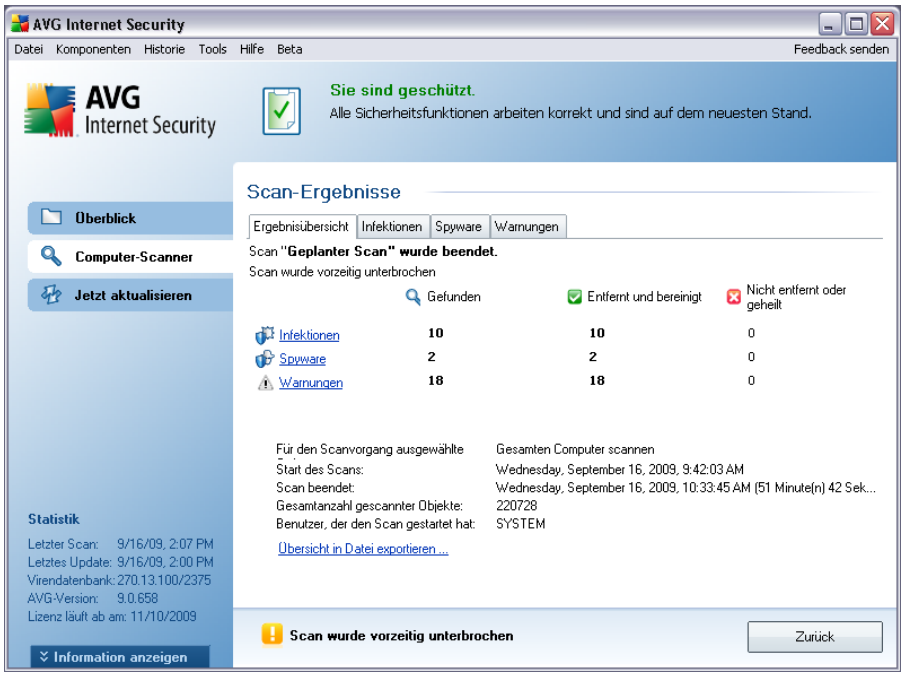
11.7. Details zu den Scan-Ergebnissen

Wenn im Dialog ***Übersicht über Scan-Ergebnisse*** ein bestimmter Scan ausgewählt wurde, können Sie anschließend auf ***Details ansehen*** klicken und so zum Dialog ***Scan-Ergebnisse*** wechseln, in dem Sie genauere Informationen zum Ablauf und dem Ergebnis des ausgewählten Scans erhalten.

Dieser Dialog ist weiter in mehrere Reiter unterteilt:

- ***Ergebnisübersicht*** – Dieser Reiter wird immer angezeigt und enthält statistische Daten zum Scan-Verlauf
- ***Infektionen*** – Dieser Reiter wird nur angezeigt, wenn beim Scan eine Vireninfektion erkannt wurde
- ***Spyware*** – Dieser Reiter wird nur angezeigt, wenn beim Scan Spyware erkannt wurde
- ***Warnungen*** – Dieser Reiter wird nur angezeigt, wenn beim Scan einige Objekte erkannt wurden, die nicht gescannt werden konnten
- ***Rootkits*** – Dieser Reiter wird nur angezeigt, wenn beim Scan Rootkits erkannt wurden
- ***Information*** **–** Dieser Reiter wird nur angezeigt, wenn potentielle Bedrohungen erkannt wurden und diese nicht in einer der oben genannten Kategorien eingeordnet werden konnten; der Reiter zeigt dann eine Warnbenachrichtigung zu diesem Fund an

11.7.1. Reiter „Ergebnisübersicht“



Auf dem Reiter ***Scan-Ergebnisse*** finden Sie eine genauere Statistik mit folgenden Informationen:

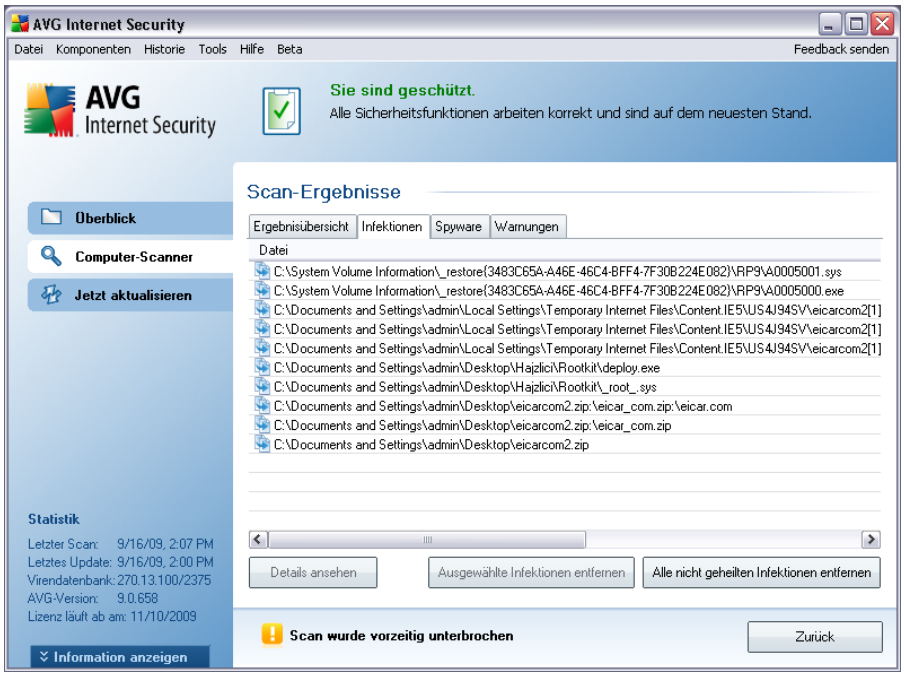
- Erkannte Vireninfektionen / Spyware
- Entfernte Vireninfektionen / Spyware
- Anzahl der Vireninfektionen / Spyware, die nicht entfernt oder geheilt werden konnte

Darüber hinaus erhalten Sie Informationen zu Datum und Uhrzeit des gestarteten Scans, zur Gesamtanzahl der gescannten Objekte, zur Scan-Dauer sowie zur Anzahl der Fehler, die beim Scan auftraten.

Schaltflächen

In diesem Dialog steht lediglich eine Schaltfläche zur Verfügung. Mit der Schaltfläche ***Ergebnisse schließen*** kehren Sie zum Dialog ***Übersicht über Scan-Ergebnisse*** zurück.

11.7.2. Reiter „Infektionen"



Der Reiter ***Infektionen*** wird nur dann im Dialog ***Scan-Ergebnisse*** angezeigt, wenn während des Scans eine Vireninfektion erkannt wurde. Dieser Reiter ist in drei Bereiche mit folgenden Informationen unterteilt:

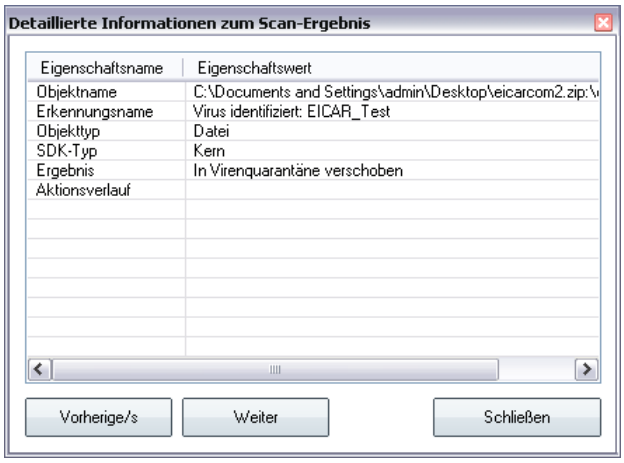
- ***Datei*** – Der vollständige Pfad zum ursprünglichen Speicherort des infizierten Objekts
- ***Infektion*** – Name des erkanntenVirus (*genauere Informationen zu bestimmten Viren finden Sie online in der Virenenzyklopädie*)
- ***Ergebnis*** – Hier wird der aktuelle Status des beim Scan erkannten Objekts definiert:
  - ***Infiziert*** – Das infizierte Objekt wurde erkannt und an seinem ursprünglichen Ort belassen (beispielsweise, wenn Sie die *Option für automatisches Heilen in bestimmten Scan-Einstellungen deaktiviert haben)*
  - ***Geheilt*** – Das infizierte Objekt wurde automatisch geheilt und an seinem ursprünglichen Ort belassen

- ***In Virenquarantäne verschoben*** – Das infizierte Objekt wurde in die ***Virenquarantäne*** verschoben
- ***Gelöscht*** – Das infizierte Objekt wurde gelöscht
- ***Zu PUP-Ausnahmen hinzugefügt*** – Der Fund wurde als Ausnahme eingestuft und zur Liste der PUP-Ausnahmen hinzugefügt (*konfiguriert im Dialog **PUP-Ausnahmen** in den erweiterten Einstellungen*)
- ***Gesperrte Datei – nicht getestet*** – Das betreffende Objekt ist gesperrt und kann daher nicht von AVG gescannt werden
- ***Potentiell gefährliches Objekt*** – Das Objekt wurde als potentiell gefährlich, aber nicht als infiziert erkannt (*es könnte zum Beispiel Makros enthalten*); diese Information dient lediglich als Warnung
- ***Neustart erforderlich, um die Aktion abzuschließen*** – Das infizierte Objekt kann nicht entfernt werden; zur vollständigen Entfernung müssen Sie den Computer neu starten

Schaltflächen

In diesem Dialog stehen drei Schaltflächen zur Verfügung:

- ***Details ansehen – Diese Schaltfläche öffnet einen neuen Dialog*** Detaillierte Informationen über das Scan-Ergebnis :



In diesem Dialog finden Sie Informationen zum Ort des erkannten

infizierten Objekts (***Eigenschaftsname***). Mit den Schaltflächen ***Vorherige/s*** bzw. ***Weiter*** können Sie Informationen zu bestimmten Funden anzeigen. Klicken Sie auf die Schaltfläche ***Schließen***, um den Dialog zu verlassen.

- ***Ausgewählte Infektionen entfernen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Fund in die ***Virenquarantäne zu verschieben***
- ***Alle nicht geheilten Infektionen entfernen*** – Diese Schaltfläche löscht alle Funde, die nicht geheilt oder in die ***Virenquarantäne verschoben werden können***
- ***Zurück*** – Die detaillierte Informationsübersicht wird geschlossen, und Sie gelangen zurück zum Dialog ***Übersicht über Scan-Ergebnisse***

11.7.3. Reiter „Spyware"

Der Reiter ***Spyware*** wird nur dann im Dialog ***Scan-Ergebnisse*** angezeigt, wenn beim Scan Spyware erkannt wurde. Dieser Reiter ist in drei Bereiche unterteilt, die folgende Informationen enthalten:

- ***Datei*** – Der vollständige Pfad zum ursprünglichen Standort des infizierten Objekts
- ***Infektion*** – Name der erkanntenSpyware (*genauere Informationen zu bestimmten Viren finden Sie in der* ***Virenenzyklopädie*** *online*)
- ***Ergebnis*** – Hier wird der aktuelle Status des beim Scan erkannten Objekts definiert:
  - ***Infiziert*** – Das infizierte Objekt wurde erkannt und an seinem ursprünglichen Ort belassen (beispielsweise, wenn Sie die Option für automatisches Heilen in bestimmten Scan-Einstellungen deaktiviert haben)
  - ***Geheilt*** – Das infizierte Objekt wurde automatisch geheilt und an seinem ursprünglichen Ort belassen
  - ***In Virenquarantäne verschoben*** – Das infizierte Objekt wurde in die ***Virenquarantäne*** ***verschoben***
  - ***Gelöscht*** – Das infizierte Objekt wurde gelöscht
  - ***Zu PUP-Ausnahmen hinzugefügt*** – Der Fund wurde als Ausnahme eingestuft und zur Liste der PUP-Ausnahmen hinzugefügt (*konfiguriert*

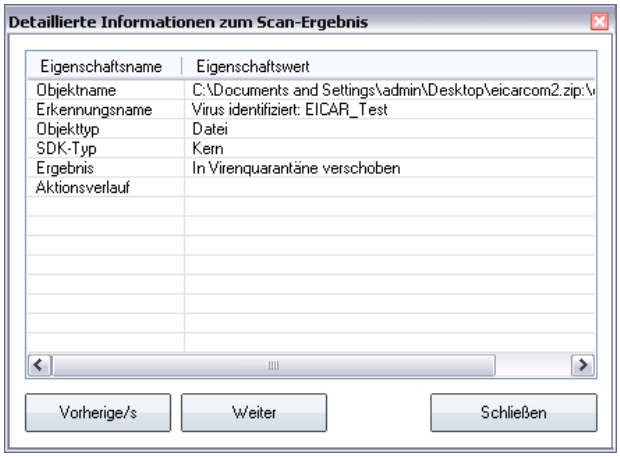
*im Dialog **PUP-Ausnahmen** in den erweiterten Einstellungen*)

- ***Gesperrte Datei – nicht getestet*** – Das betreffende Objekt ist gesperrt und kann daher nicht von AVG gescannt werden
- ***Potentiell gefährliches Objekt*** – Das Objekt wurde als potentiell gefährliches Objekt, aber nicht als infiziert erkannt (es enthält zum Beispiel möglicherweise Makros); diese Information dient lediglich als Warnung
- ***Neustart erforderlich, um die Aktion abzuschließen*** – Das infizierte Objekt kann nicht entfernt werden. Um es vollständig zu entfernen, müssen Sie Ihren Computer neu starten

Schaltflächen

In diesem Dialog stehen drei Schaltflächen zur Verfügung:

- ***Details ansehen*** – Diese Schaltfläche öffnet einen neuen Dialog ***Detaillierte Informationen zum Scan-Ergebnis***:



In diesem Dialog finden Sie Informationen zum Ort des erkannten infizierten Objekts (***Eigenschaftsname***). Mit den Schaltflächen ***Vorheriges*** / ***Weiter*** können Sie Informationen zu bestimmten Funden anzeigen. Klicken Sie auf die Schaltfläche ***Schließen***, um den Dialog zu verlassen.

- ***Ausgewählte Infektionen entfernen*** – Klicken Sie auf diese Schaltfläche,

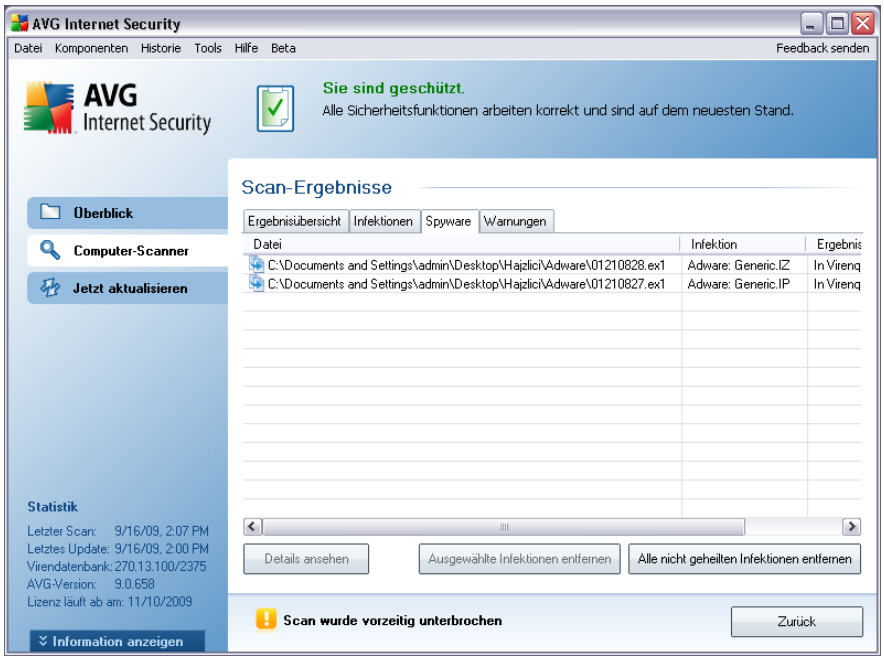
um den ausgewählten Fund in die ***Virenquarantäne zu verschieben***

- ***Alle nicht geheilten Infektionen entfernen*** – Diese Schaltfläche löscht alle Funde, die nicht geheilt oder in die ***Virenquarantäne verschoben werden können***

- ***Zurück*** – Die detaillierte Informationsübersicht wird geschlossen, und Sie gelangen zurück zum Dialog ***Übersicht über Scan-Ergebnisse***

11.7.4. Reiter „Warnungen"

Auf dem Reiter ***Warnungen*** werden Informationen zu „verdächtigen" Objekten (*normalerweise Dateien*) angezeigt, die beim Scan erkannt wurden. Wenn diese Dateien von ***Residenter Schutz*** erkannt werden, wird der Zugriff auf diese Dateien blockiert. Typische Funde dieser Art sind beispielsweise folgende: Versteckte Dateien, Cookies, verdächtige Registrierungsschlüssel, kennwortgeschützte Dokumente oder Archive usw. Diese Dateien stellen keine direkte Bedrohung für Ihren Computer oder Sicherheit dar. Informationen zu diesen Dateien können bei der Erkennung von Adware oder Spyware auf Ihrem Computer nützlich sein. Wenn diese Warnungen nur nach einem AVG-Scan ausgegeben werden, ist keine Aktion nötig.



Dies ist eine kurze Beschreibung der bekanntesten Beispiele solcher Objekte:

- ***Versteckte Dateien*** – Versteckte Dateien sind in Windows standardmäßig

nicht sichtbar, und bestimmte Viren oder andere Bedrohungen können versuchen, der Erkennung durch das Speichern ihrer Dateien mit diesem Attribut zu umgehen. Wenn Ihr AVG eine versteckte Datei meldet, die verseucht sein könnte, können Sie diese in die ***AVG Virenquarantäne*** verschieben.

- ***Cookies*** – Cookies sind reine Textdateien, die von Webseiten dazu verwendet werden, benutzerbezogene Informationen zu speichern. Diese Informationen werden später verwendet, um benutzerdefinierte Layouts von Websites zu laden, Benutzernamen einzutragen usw.

- ***Verdächtige Registrierungsschlüssel*** – Manche Malware speichert Informationen in der Windows-Registrierung, um sicherzustellen, dass sie beim Hochfahren geladen wird oder um ihre Auswirkung auf das Betriebssystem zu erweitern.

11.7.5. Reiter „Rootkits"

Auf dem Reiter ***Rootkits*** werden Informationen zu während des Scanvorgangs entdeckten Rootkits angezeigt, wenn Sie den ***Anti-Rootkit-Scan*** gestartet oder die Option für den Anti-Rootkit-Scan dem Element ***Gesamten Computer scannen*** manuell hinzugefügt haben (*diese Option ist standardmäßig deaktiviert*).

Ein ***Rootkit*** ist ein Programm, das ohne Genehmigung der Systembesitzer oder berechtigten Manager die Kontrolle über ein Computersystem übernimmt. Ein Zugriff auf die Hardware ist meist nicht erforderlich, da ein Rootkit darauf abzielt, die Kontrolle über das Betriebssystem, das auf der Hardware ausgeführt wird, zu übernehmen. Rootkits verbergen ihre Existenz auf dem System üblicherweise, indem sie die standardmäßigen Sicherheitsmechanismen des Betriebssystems außer Kraft setzen oder umgehen. Oft handelt es sich bei diesen Programmen gleichzeitig um Trojaner, die bei Benutzern den Eindruck erwecken, sie könnten ohne Risiko auf ihren Systemen ausgeführt werden. Dies wird mit Techniken wie dem Verbergen von ausgeführten Prozessen vor Überwachungsprogrammen oder dem Verbergen von Dateien oder Systemdaten vor dem Betriebssystem erzielt.

Dieser Reiter ist ähnlich aufgebaut wie der Reiter ***Infektionen*** oder ***Spyware***.

11.7.6. Reiter „Informationen"

Der Reiter ***Informationen*** enthält Daten über „Funde", die nicht als Infektionen, Spyware usw. eingestuft werden können. Sie können nicht eindeutig als gefährlich klassifiziert werden, müssen jedoch trotzdem beachtet werden. AVG-Scan kann Dateien erkennen, die möglicherweise nicht infiziert, aber verdächtig sind. Diese Dateien werden entweder als ***Warnung*** oder ***Information*** gemeldet.

Die ***Information*** zum Schweregrad kann aus einem der folgenden Gründe angezeigt werden:

- ***Run-time packed*** – Die Datei wurde mit einem unüblichen Run-Time-Packer gepackt, was auf einen Versuch hinweisen kann, den Scan der Datei zu verhindern. Nicht jeder Bericht über eine solche Datei weist jedoch auf ein Virus hin.

- ***Run-time packed recursive*** – Ähnlich wie oben, jedoch weniger häufig unter gebräuchlicher Software. Solche Dateien sind verdächtig und sollten entfernt oder zur Analyse eingesendet werden.

- ***Kennwortgeschützte Dokumente oder Archive*** – Kennwortgeschützte Dateien können von AVG (*bzw. anderen Anti-Malware-Programmen*) nicht gescannt werden.

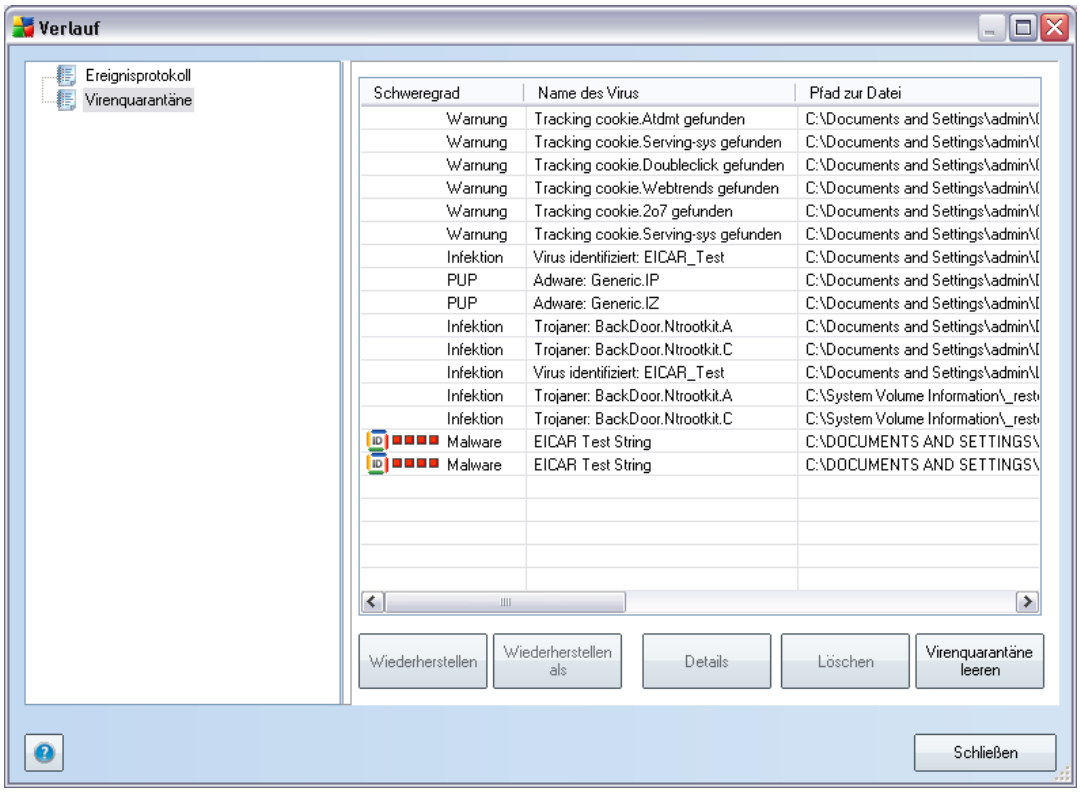
- ***Dokument mit Makros*** – Das gemeldete Dokument enthält Makros, die möglicherweise schädlich sind.

- ***Versteckte Erweiterung*** – Dateien mit versteckten Erweiterungen können beispielsweise wie Bilder aussehen, sind jedoch in Wahrheit ausführbare Dateien (*z. B. bild.jpg.exe*). Die zweite Erweiterung ist standardmäßig in Windows nicht sichtbar. AVG berichtet solche Dateien, um ein versehentliches Öffnen dieser Dateien zu verhindern.

- ***Falscher Dateipfad*** – Wenn eine wichtige Systemdatei nicht vom Standardpfad ausgeführt wird (*winlogon.exe wird z. B. nicht aus dem Windows-Ordner ausgeführt*), meldet AVG diese Unstimmigkeit. In einigen Fällen verwenden Viren die Namen von Standardsystemprozessen, damit ihr Vorhandensein im System weniger auffällt.

- ***Gesperrte Datei*** – Die gemeldete Datei ist gesperrt und kann von AVG nicht gescannt werden. Das bedeutet üblicherweise, dass diese Datei dauerhaft vom System verwendet wird (*z. B. Auslagerungsdateien*).

11.8. Virenquarantäne



Virenquarantäne ist eine sichere Umgebung zur Verwaltung von verdächtigen und infizierten Objekten, die von AVG beim Scan erkannt wurden. Sobald beim Scan ein infiziertes Objekt erkannt wird und AVG dieses nicht automatisch heilen kann, werden Sie gefragt, wie dieses verdächtige Objekt behandelt werden soll. Es wird empfohlen, das Objekt zur weiteren Behandlung in die ***Virenquarantäne*** zu verschieben.

Die Oberfläche der ***Virenquarantäne*** wird in einem eigenen Fenster geöffnet, in dem eine Informationsübersicht über infizierte Objekte angezeigt wird, die sich in der Quarantäne befinden:

- ***Schweregrad*** – Die grafische Darstellung des entsprechenden Schweregrads des Prozesses auf einer vierstufigen Skala von unbedenklich (■□□□) bis sehr gefährlich (■■■■)
- ***Infektionsart*** – Funde werden aufgrund ihrer Infektionsstufe in zwei Typen eingeteilt (*alle aufgeführten Objekte können tatsächlich oder potentiell infiziert sein*)

- ***Name des Virus*** – Der Name der erkannten Infektion wird entsprechend der Virenenzyklopädie (online) angegeben

- ***Pfad zur Datei*** – Der vollständige Pfad zum ursprünglichen Standort der infizierten Datei

- ***Ursprünglicher Objektname*** – Alle hier aufgelisteten Objekte wurden von AVG während des Scanvorgangs mit dem Standardnamen gekennzeichnet. Wenn das Objekt einen bekannten ursprünglichen Namen hat (*z. B. der Name eines eMail-Anhangs, der nicht mit dem eigentlichen Inhalt des Anhangs übereinstimmt*), wird der Name in dieser Spalte angegeben.

- ***Speicherdatum*** – Datum und Uhrzeit, zu dem die verdächtige Datei erkannt und in die ***Virenquarantäne verschoben wurde***

Schaltflächen

Auf der Oberfläche der ***Virenquarantäne*** stehen folgende Schaltflächen zur Verfügung:

- ***Wiederherstellen*** – Die infizierte Datei wird zurück zu ihrem ursprünglichen Standort auf Ihrer Festplatte verschoben

- ***Wiederherstellen als*** – Wenn Sie das erkannte infizierte Objekt aus der ***Virenquarantäne*** in einen ausgewählten Ordner verschieben möchten, klicken Sie auf diese Schaltfläche, und das verdächtige und erkannte Objekt wird mit seinem ursprünglichen Namen gespeichert. Wenn der ursprüngliche Name nicht bekannt ist, wird stattdessen der Standardname verwendet.

- ***Löschen*** – Die infizierte Datei wird vollständig aus der ***Virenquarantäne*** gelöscht

- ***Virenquarantäne leeren*** - Alle Objekte werden vollständig aus der ***Virenquarantäne*** entfernt

12. AVG Updates

Die regelmäßige Aktualisierung von AVG ist entscheidend, damit alle neu entdeckten Viren so früh wie möglich erkannt werden. Da AVG-Updates nicht nach einem festen Zeitplan, sondern entsprechend der Anzahl und des Schweregrads neuer Bedrohungen zur Verfügung gestellt werden, wird empfohlen, mindestens einmal täglich eine Prüfung auf neue Updates durchzuführen. Durch eine alle vier Stunden erfolgende Prüfung wird sichergestellt, dass Ihre AVG-Virendatenbank auch tagsüber auf den neuesten Stand gebracht wird.

12.1. Updatestufen

Sie können in AVG eine von zwei Updatestufen auswählen:

- ***Definitionsupdates*** umfassen Änderungen, die für zuverlässigen Viren-, Spam- und Malware-Schutz erforderlich sind. In der Regel umfasst sie keine Änderungen am Code und es wird nur die Virendatenbank aktualisiert. Dieses Update sollte durchgeführt werden, sobald es verfügbar ist.

- ***Das Programmupdate*** enthält verschiedene Programmänderungen, -ausbesserungen und -verbesserungen.

Beim Planen von Updates können Sie auswählen, welche Prioritätsstufe heruntergeladen und angewendet werden soll.

12.2. Updatetypen

Sie können zwischen zwei Aktualisierungstypen wählen:

- ***Eine Aktualisierung On-Demand*** ist ein sofortiges Update von AVG, das bei Bedarf jederzeit durchgeführt werden kann.

- ***Geplante Aktualisierung*** – Innerhalb von AVG können Sie auch einen Aktualisierungsplan voreinstellen. Die geplante Aktualisierung wird dann regelmäßig zu den festgelegten Zeiten ausgeführt. Immer wenn neue Aktualisierungsdateien an dem angegebenen Speicherort verfügbar sind, werden sie entweder direkt über das Internet oder das Netzwerkverzeichnis heruntergeladen. Wenn keine neuen Aktualisierungen verfügbar sind, passiert nichts.

12.3. Updatevorgang

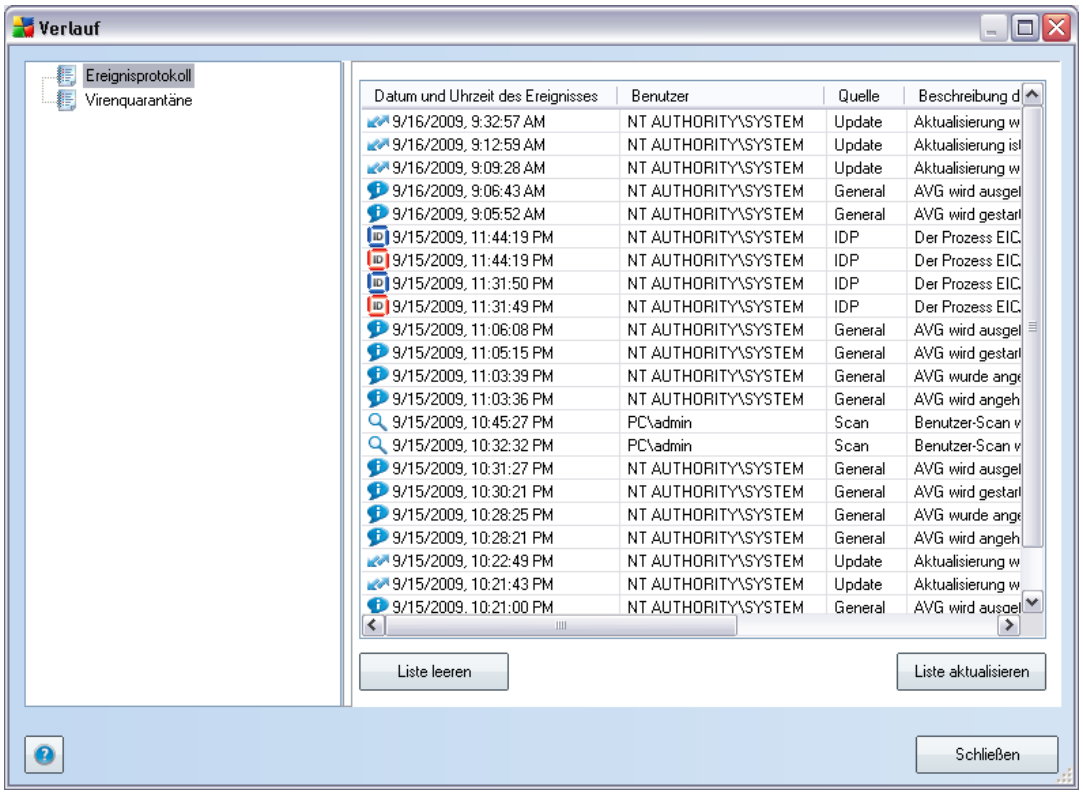
Der Updateprozess kann bei Bedarf unmittelbar gestartet werden, indem Sie auf den Quick Link ***Jetzt aktualisieren*** klicken. Dieser Link steht Ihnen jederzeit in allen Dialogen der Benutzeroberfläche von AVG zur Verfügung. Es empfiehlt sich jedoch,

Updates regelmäßig entsprechend dem Updatezeitplan durchzuführen, der in der Komponente Updatemanager bearbeitet werden kann.

Wenn Sie das Update starten, überprüft AVG zunächst, ob neue Updatedateien zur Verfügung stehen. Wenn dies der Fall ist, lädt AVG diese eigenständig herunter und startet den Updateprozess. Während des Updateprozesses werden Sie zur Oberfläche ***Fortschritt beim Update*** zurückgeführt, wo der Fortschritt der Aktualisierung grafisch dargestellt wird, ebenso wie eine Übersicht über die statistischen Parameter (*Größe der Aktualisierungsdatei, empfangene Daten, Download-Geschwindigkeit, verstrichene Zeit usw.*).

Hinweis*: Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen Konfiguration wiederherstellen. Diese Option kann über Start/ Programme/Zubehör/Systemprogramme/Systemwiederherstellung aufgerufen werden. Eine Änderung dieser Einstellungen wir nur erfahrenen Benutzern empfohlen!*

13. Ereignisprotokoll



Der Dialog ***Ereignisprotokoll*** kann im Systemmenü über die Optionen ***Historie/ Ereignisprotokoll*** geöffnet werden. In diesem Dialog finden Sie eine Zusammenfassung aller wichtigen Ereignisse, die während der Ausführung von **AVG 9 Internet Security** aufgetreten sind. Das ***Ereignisprotokoll*** zeichnet folgende Ereignistypen auf:

- Informationen über Updates der AVG-Anwendung
- Start, Ende oder Unterbrechung des Scans (einschließlich automatisch ausgeführter Tests)
- Ereignisse in Verbindung mit der Virenerkennung (durch Residenten Schutz oder Scan), einschließlich der Quelle, an dem das Ereignis aufgetreten ist
- Andere wichtige Ereignisse

Schaltflächen

- ***Liste leeren*** – Alle Einträge der Ereignisliste werden gelöscht
- ***Liste aktualisieren*** – Alle Einträge der Ereignisliste werden aktualisiert

14. FAQ und technischer Support

Bei Problemen mit AVG, egal ob diese geschäftlicher oder technischer Art sind, konsultieren Sie bitte den Abschnitt ***FAQ*** auf der Website von AVG (http://www.avg.com/).

Falls Sie auf diese Weise keine Lösung für Ihr Problem finden, wenden Sie sich bitte per eMail an den technischen Support. Verwenden Sie bitte das Kontaktformular, das im Systemmenü unter ***Hilfe/Onlinehilfe*** zur Verfügung steht.