AVG Internet Security 2012

Benutzerhandbuch

Dokumentversion 2012.01 (1.9.2011)

Inhalt

1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG Internet Security 2012**.

AVG Internet Security 2012 bietet verschiedene Schutzebenen für all Ihre Online-Aktivitäten, so dass Sie sich über Identitätsdiebstahl, Viren oder schädliche Websites keine Sorgen mehr machen müssen. Das Programm enthält die AVG Protective Cloud-Technologie und das AVG Community-Schutznetzwerk, mittels derer wir Informationen zu den neuesten Bedrohungen sammeln und an die Community weitergeben, um sicherzustellen, dass Sie stets optimal geschützt sind:

- Gehen Sie sicher online einkaufen und tätigen Sie sichere Bankgeschäfte mit Firewall, Anti-Spam und Identitätsschutz von AVG
- Schützen Sie sich in sozialen Netzwerken mit dem Schutz in sozialen Netzwerken von AVG
- Surfen und suchen Sie sicher im Internet mit dem Echtzeitschutz von Link Scanner

2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG Internet Security 2012 wurde für den Schutz von Workstations mit den folgenden Betriebssystemen entwickelt:

- 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 unter Windows XP x64 nicht unterstützt. Bei diesem Betriebssystem können Sie AVG Internet Security 2012 installieren, jedoch ohne die Komponente „Identitätsschutz“.*

2.2. Minimale und empfohlene Hardware-Anforderungen

Minimale Hardware-Anforderungen für **AVG Internet Security 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM-Speicher
- 1000 MB freier Festplattenspeicher (für die Installation)

Empfohlene Hardware-Anforderungen für **AVG Internet Security 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-Speicher
- 1550 MB freier Festplattenspeicher (für die Installation)

3. Installationsvorgang bei AVG

Wo erhalte ich die Installationsdatei?

Für die Installation von **AVG Internet Security 2012** auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Um sicherzustellen, dass Sie die neueste Version von **AVG Internet Security 2012** installieren, wird empfohlen, die Installationsdatei von der Website von AVG (http://www.avg.com/de/) herunterzuladen. Der Bereich ***Support Center/Download*** enthält eine gegliederte Übersicht über die Installationsdateien von jeder AVG-Edition.

Wenn Sie sich nicht sicher sind, welche Dateien Sie herunterladen und installieren müssen, können Sie den Dienst ***Produkt wählen*** im unteren Teil der Webseite verwenden. Nachdem Sie drei einfache Fragen beantwortet haben, bestimmt dieser Dienst genau, welche Dateien Sie benötigen. Klicken Sie auf die Schaltfläche ***Weiter***, um zu einer vollständigen Liste mit Download-Dateien weitergeleitet zu werden, die auf Ihre Bedürfnisse zugeschnitten sind.

Wie läuft der Installationsvorgang ab?

Nachdem Sie die Installationsdatei heruntergeladen und auf Ihrer Festplatte gespeichert haben, können Sie den Installationsvorgang starten. Die Installation ist eine Abfolge von einfachen und leicht verständlichen Dialogen. Jeder Dialog beschreibt kurz, was bei jedem Schritt des Installationsvorgangs zu tun ist. Im Folgenden finden Sie eine detaillierte Erläuterung zu jedem Dialogfenster:

3.1. Willkommen

Der Installationsvorgang startet mit dem Dialog ***Willkommen im Installationsprogramm AVG***:

Wählen Sie eine Sprache für die Installation aus

In diesem Dialog können Sie die Sprache auswählen, die für den Installationsvorgang verwendet wird. Klicken Sie in der rechten Ecke des Dialogs auf das Kombinationsfeld, um das Sprachmenü zu öffnen. Wählen Sie die gewünschte Sprache aus, und der Installationsvorgang wird in der Sprache Ihrer Wahl fortgesetzt.

Achtung: Momentan wählen Sie nur die Sprache für den Installationsvorgang aus. Die Anwendung AVG Internet Security 2012 wird in der ausgewählten Sprache sowie in der immer automatisch installierten Sprache Englisch installiert. Es ist jedoch möglich, noch weitere Sprachen zu installieren und mit AVG Internet Security 2012 in jeder dieser Sprachen zu arbeiten. Sie können Ihre vollständige Auswahl alternativer Sprachen in einem der folgenden Dialoge mit dem Namen Benutzerdefinierte Optionen bestätigen.

Lizenzvereinbarung

Der Dialog ***Willkommen im Installationsprogramm AVG*** enthält auch den vollständigen Text der Lizenzvereinbarung von AVG. Lesen Sie das Dokument sorgfältig durch. Klicken Sie auf ***Akzeptieren***, um zu bestätigen, dass Sie die Vereinbarung gelesen, verstanden und akzeptiert haben. Falls Sie der Lizenzvereinbarung nicht zustimmen, klicken Sie auf ***Ablehnen***, und der Installationsvorgang wird abgebrochen.

Datenschutzrichtlinie von AVG

Dieser Setup-Dialog bietet neben der Lizenzvereinbarung auch die Option, mehr über die Datenschutzrichtlinie von AVG zu erfahren. In der unteren linken Ecke des Dialogs wird der Link ***Datenschutzrichtlinie von AVG***angezeigt. Klicken Sie darauf, um auf die Website von AVG (http://www.avg.com/de/) weitergeleitet zu werden. Dort finden Sie die vollständige Fassung der Datenschutzrichtlinie von AVG Technologies.

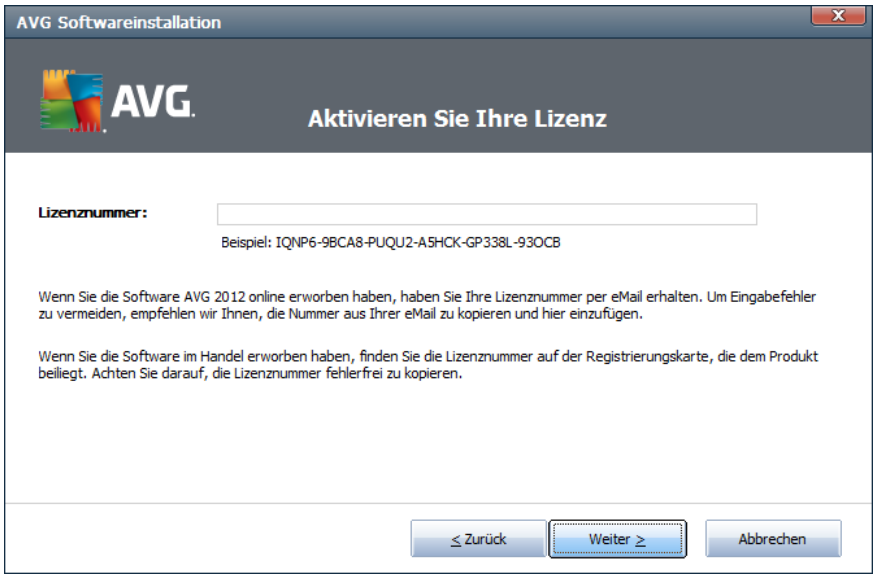
Schaltflächen

Im ersten Setup-Dialog stehen nur zwei Schaltflächen zur Verfügung:

- ***Zustimmen*** – Mit dieser Schaltfläche bestätigen Sie, dass Sie die Lizenzvereinbarung gelesen, verstanden und ihr zugestimmt haben. Die Installation wird fortgesetzt, und Sie gelangen einen Schritt weiter zum folgenden Setup-Dialog.
- ***Ablehnen*** – Mit dieser Schaltfläche lehnen Sie die Lizenzvereinbarung ab. Der Installationsvorgang wird sofort beendet. **AVG Internet Security 2012** wird nicht installiert.

3.2. Aktivieren Sie Ihre Lizenz

Im Dialog ***AVG-Lizenz aktivieren*** werden Sie dazu aufgefordert, Ihre Lizenznummer in das dafür vorgesehene Feld einzugeben:



Wo finde ich die Lizenznummer?

Die Vertriebsnummer finden Sie auf der CD-Verpackung Ihres **AVG Internet Security 2012**-Pakets. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von **AVG Internet Security 2012** 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.

So verwenden Sie die Methode „Kopieren & Einfügen“

Verwenden Sie die Methode ***Kopieren & Einfügen***, um Ihre Lizenznummer von **AVG Internet Security 2012** korrekt einzugeben. Gehen Sie wie folgt vor:

- Öffnen Sie die eMail mit Ihrer Lizenznummer.
- Klicken Sie mit der linken Maustaste an den Anfang der Lizenznummer, ziehen Sie die Maus bei gedrückter Maustaste bis zum Ende der Nummer, und lassen Sie die Maustaste los. Die Nummer ist jetzt markiert.
- Halten Sie die ***Strg***-Taste gedrückt, und drücken Sie die Taste ***C***. Damit wird die Nummer in den Zwischenspeicher verschoben.
- Positionieren Sie den Cursor an der Stelle, an der Sie die kopierte Nummer einfügen möchten.

- Halten Sie die ***Strg***-Taste gedrückt, und drücken Sie die Taste ***V***. Damit wird die Nummer an der gewünschten Stelle eingefügt.

Schaltflächen

Wie in den meisten Setup-Dialogen stehen die folgenden drei Schaltflächen zur Verfügung:

- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um einen Schritt zurück zum vorherigen Setup-Dialog zu gelangen.
- ***Weiter*** – Klicken Sie auf diese Schaltfläche, um die Installation fortzusetzen und einen Schritt weiter zu gelangen.
- ***Abbrechen*** – Klicken Sie auf diese Schaltfläche, um den Setup-Vorgang sofort zu beenden; **AVG Internet Security 2012** wird nicht installiert!

3.3. Wählen Sie die Installationsart aus

Installationsmöglichkeiten

Der Dialog ***Wählen Sie die Installationsart aus*** bietet zwei Installationsoptionen: ***Schnellinstallation*** und ***Benutzerdefinierte Installation***.

Den meisten Benutzern wird empfohlen, die standardmäßige Schnellinstallation beizubehalten, mit der **AVG Internet Security 2012** vollständig automatisch mit den vom Programmhersteller vordefinierten Einstellungen installiert wird. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration in Zukunft geändert werden muss, können Sie diese Änderung immer direkt in der Anwendung **AVG Internet Security 2012** vornehmen. Wenn Sie die Option ***Schnellinstallation*** ausgewählt haben, klicken Sie auf ***Weiter***, um mit dem Dialog AVG Security Toolbar installieren fortzufahren.

Die benutzerdefinierte Installation sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, **AVG Internet Security 2012** nicht mit den Standardeinstellungen zu installieren, beispielsweise um bestimmte Systemanforderungen zu erfüllen. Wenn Sie diese Option ausgewählt haben, klicken Sie auf ***Weiter***, um mit dem Dialog Benutzerdefinierte Optionen fortzufahren.

Installation von AVG-Gadget

Im rechten Bereich des Dialogs finden Sie das Kontrollkästchen zum AVG-Gadget (*unterstützt unter Windows Vista und Windows 7*). Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Gadget installieren möchten. Das AVG-Gadget wird daraufhin über die Windows-Sidebar verfügbar sein und bietet Ihnen Zugriff auf die wichtigsten Features von **AVG Internet Security 2012** wie Scans und Updates.

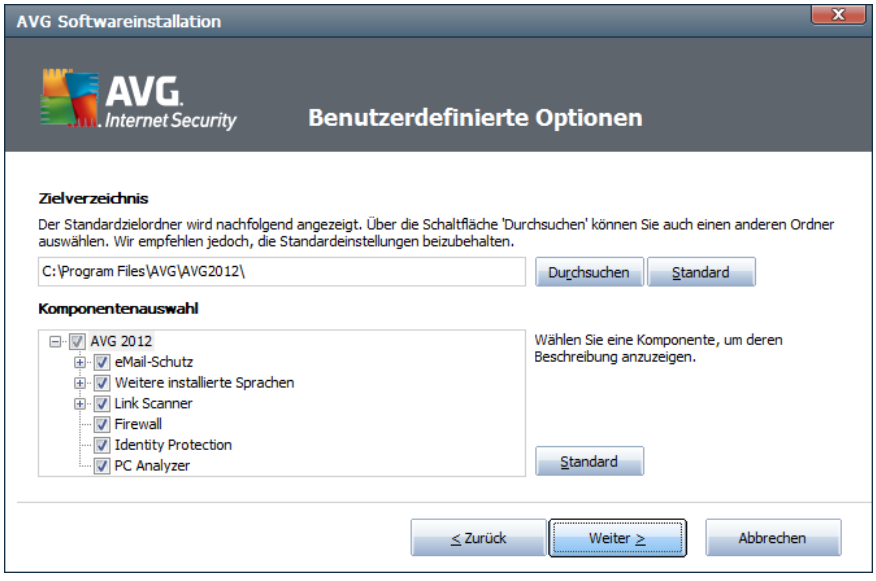
Schaltflächen

Wie in den meisten Setup-Dialogen stehen die folgenden drei Schaltflächen zur Verfügung:

- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um einen Schritt zurück zum vorherigen Setup-Dialog zu gelangen.
- ***Weiter*** – Klicken Sie auf diese Schaltfläche, um die Installation fortzusetzen und einen Schritt weiter zu gelangen.
- ***Abbrechen*** – Klicken Sie auf diese Schaltfläche, um den Setup-Vorgang sofort zu beenden; **AVG Internet Security 2012** wird nicht installiert!

3.4. Benutzerdefinierte Optionen

Im Dialog ***Benutzerdefinierte Optionen*** können Sie zwei Parameter für die Installation festlegen:



Zielverzeichnis

Im Dialogabschnitt ***Zielverzeichnis*** können Sie den Speicherort angeben, an dem **AVG Internet Security 2012** installiert werden soll. Standardmäßig wird **AVG Internet Security 2012** im Ordner C:/Programme installiert. Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf ***Durchsuchen***, um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus.

Komponentenauswahl

Im Abschnitt ***Komponentenauswahl*** wird eine Übersicht über alle Komponenten von **AVG Internet Security 2012** angezeigt, die installiert werden können. 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!

Markieren Sie einen Eintrag in der Liste ***Komponentenauswahl***, um eine kurze Beschreibung der entsprechenden Komponente auf der rechten Seite dieses Bereichs anzuzeigen. Weitere Informationen zu den Funktionen der einzelnen Komponenten finden Sie im Kapitel Komponentenübersicht in dieser Dokumentation. Klicken Sie auf die Schaltfläche ***Standard***, um die werkseitigen Standardeinstellungen wiederherzustellen.

Schaltflächen

Wie in den meisten Setup-Dialogen stehen die folgenden drei Schaltflächen zur Verfügung:

- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um einen Schritt zurück zum vorherigen Setup-Dialog zu gelangen.
- ***Weiter*** – Klicken Sie auf diese Schaltfläche, um die Installation fortzusetzen und zum nächsten Schritt zu gelangen.
- ***Abbrechen*** – Klicken Sie auf diese Schaltfläche, um den Setup-Vorgang sofort zu beenden; **AVG Internet Security 2012** wird nicht installiert.

3.5. AVG Security Toolbar installieren

Entscheiden Sie im Dialog ***AVG Security Toolbar installieren***, ob Sie die AVG Security Toolbar installieren möchten. Wenn Sie die Standardeinstellungen nicht ändern, wird die Komponente automatisch in Ihrem Internetbrowser installiert (*derzeit werden die Browser Microsoft Internet Explorer 6.0 oder höher, Mozilla Firefox 3.0 und höher unterstützt*), so dass Sie beim Surfen im Internet umfassend geschützt sind.

Sie können zudem entscheiden, ob Sie *AVG Secure Search (powered by Google)* als Ihren Standard-Suchanbieter festlegen möchten. Behalten Sie in diesem Fall die Aktivierung des entsprechenden Kontrollkästchens bei.

3.6. Installationsfortschritt

Im Dialog ***Installationsfortschritt*** wird der Fortschritt des Installationsvorgangs angezeigt. Hier ist keine Aktion erforderlich:

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

Schaltflächen

In diesem Dialog steht nur eine Schaltfläche zur Verfügung – ***Abbrechen***. Diese Schaltfläche sollte nur verwendet werden, wenn Sie den laufenden Installationsvorgang beenden möchten. Bitte beachten Sie, dass **AVG Internet Security 2012** in diesem Fall nicht installiert wird.

3.7. Die Installation wurde erfolgreich abgeschlossen

Der Dialog ***Die Installation wurde erfolgreich abgeschlossen*** bestätigt, dass **AVG Internet Security 2012** vollständig installiert und konfiguriert wurde:

Programm zur Produktverbesserung

In diesem Dialog können Sie festlegen, ob Sie am Programm zur Produktverbesserung teilnehmen möchten (*weitere Informationen finden Sie in Kapitel Erweiterte Einstellungen von AVG/Programm zur Produktverbesserung*), wobei anonyme Informationen zu erkannten Bedrohungen gesammelt werden, um die allgemeine Sicherheit im Internet zu verbessern. Wenn Sie dem Inhalt zustimmen, aktivieren Sie die Option ***Ich stimme der Teilnahme an AVG 2012-Websicherheit und am Programm zur Produktverbesserung zu*** *(die Option ist standardmäßig aktiviert)*.

Neustart des Computers

Starten Sie zum Abschließen des Installationsvorgang Ihren Computer neu: Wählen Sie entweder ***Jetzt neu starten*** oder ***Später neu starten*** aus.

Installation mit einer Firmenlizenz

Wenn Sie eine Firmenlizenz für AVG verwenden und bereits vorher ausgewählt haben, die Komponente „Remote-Verwaltung“ zu installieren *(siehe Benutzerdefinierte Optionen)*, wird in der folgenden Benutzeroberfläche der Dialog „Die Installation wurde erfolgreich abgeschlossen“ angezeigt:

Geben Sie AVG DataCenter-Parameter an – Geben Sie die Verbindungszeichenkette zum AVG DataCenter in der Form „Server:Port“ an. 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. Genaue Informationen zur Remote-Verwaltung von AVG erhalten Sie im Benutzerhandbuch der AVG Business Edition, das Sie von der AVG-Website (http://www.avg.com/de/) herunterladen können.

Lesen Sie im Kapitel Komponentenübersicht in dieser Dokumentation nach. Klicken Sie auf die Schaltfläche ***Standard***, um die werkseitigen Standardeinstellungen wiederherzustellen.

Schaltflächen

In diesem Dialog stehen folgende Schaltflächen zur Verfügung:

- ***Jetzt neu starten (empfohlen)*** – Der Neustart ist erforderlich, um den Installationsvorgang von **AVG Internet Security 2012** abzuschließen. Es wird empfohlen, den Computer sofort neu zu starten. Erst nach dem Neustart ist **AVG Internet Security 2012** vollständig installiert und der Schutz Ihres Systems gewährleistet.

- ***Später neu starten*** – Wenn Sie Ihren Computer aus bestimmten Gründen nicht sofort neu starten können, kann der Neustart auch auf einen späteren Zeitpunkt verschoben werden. Es wird jedoch empfohlen, den Neustart sofort auszuführen. Erst nach dem Neustart kann **AVG Internet Security 2012** Ihren Computer vollständig schützen.

4. Nach der Installation

4.1. Produktregistrierung

Nach Abschluss der Installation von **AVG Internet Security 2012** registrieren Sie bitte Ihr Produkt online auf der Website von AVG (http://www.avg.com/de/). Nach der Registrierung erhalten Sie vollen Zugriff auf Ihr AVG-Benutzerkonto, den AVG Update-Newsletter und andere exklusive Dienste für registrierte Benutzer.

Der einfachste Möglichkeit zur Registrierung bietet die Benutzeroberfläche von **AVG Internet Security 2012**. Wählen Sie im Hauptmenü den Eintrag Hilfe/Jetzt registrieren aus. Sie werden auf die ***Registrierungsseite*** der AVG-Website http://www.avg.com/de/) weitergeleitet. Bitte folgen Sie den Anweisungen auf dieser Seite.

4.2. Zugriff auf die Benutzeroberfläche

Der Hauptdialog von AVG kann auf mehrere Arten geöffnet werden:

- durch Doppelklicken auf das AVG-Symbol im Infobereich
- durch Doppelklicken auf das AVG-Symbol auf dem Desktop
- durch Doppelklicken auf die Statuszeile im unteren Bereich des AVG-Gadget (*falls installiert; wird unter Windows Vista und Windows 7 unterstützt*)
- über das Menü ***Start/Alle Programme/AVG 2012/Benutzeroberfläche von AVG***

4.3. Gesamten Computer scannen

Es besteht das potentielle Risiko, dass vor der Installation von **AVG Internet Security 2012** 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.

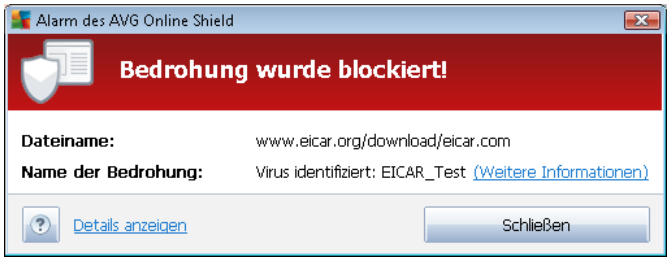
Eine Anleitung, wie Sie die Option Gesamten Computer scannen ausführen, finden Sie im Kapitel AVG-Scans.

4.4. Eicar-Test

Zur Überprüfung, ob **AVG Internet Security 2012** 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 nachdem Sie den Download der Testdatei bestätigt haben, reagiert Online Shield (*ein Teil der Komponente Link Scanner*) darauf mit einer Warnung. Diese Meldung zeigt an, dass AVG korrekt auf dem Computer installiert ist.



Von der Website http://www.eicar.com können Sie auch eine komprimierte Version des EICAR-‚Virus' herunterladen (*im Format eicar_com.zip*). Online Shield gibt Ihnen die Möglichkeit, diese Datei herunterzuladen und auf Ihrer Festplatte zu speichern. Beim Entpacken der Datei wird der ‚Virus' jedoch vom Residenten Schutz (*ein Teil der Komponente Anti-Virus*) erkannt.

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

4.5. Standardkonfiguration von AVG

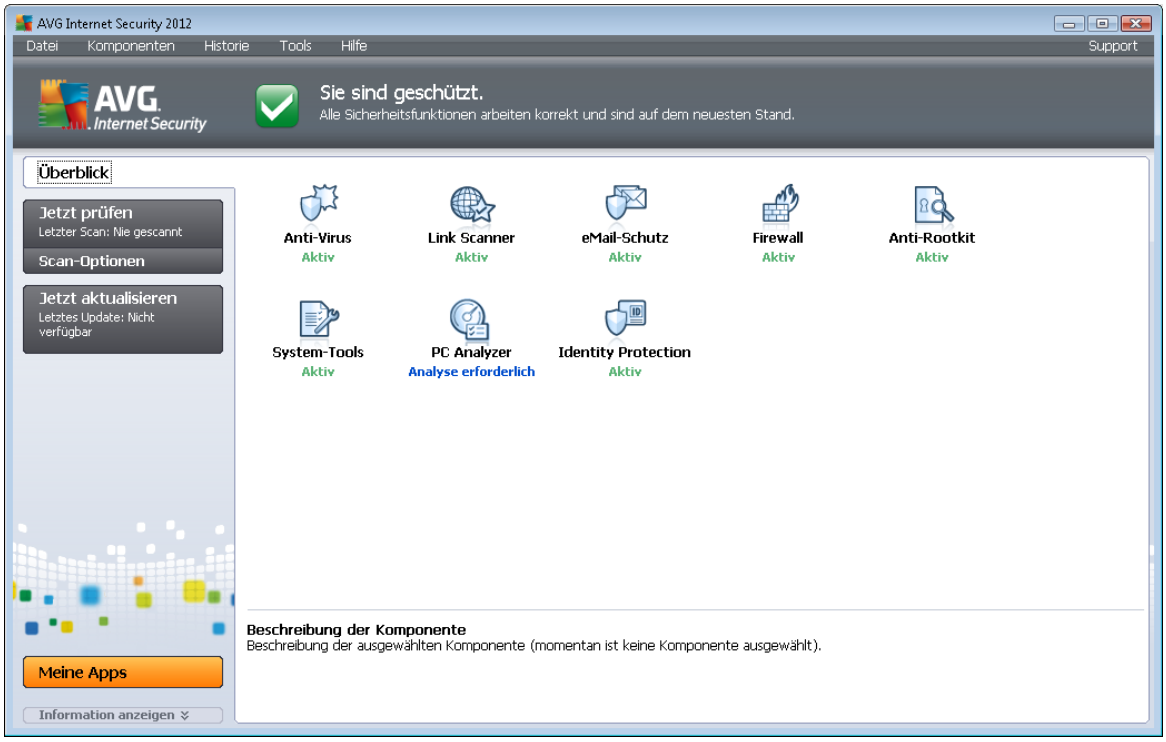
Die Standardkonfiguration (*Konfiguration der Anwendung unmittelbar nach der Installation*) von**AVG Internet Security 2012** ist vom Händler so eingestellt, dass alle Komponenten und Funktionen eine optimale Leistung erzielen.

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.

5. Benutzeroberfläche von AVG

AVG Internet Security 2012 wird mit dem Hauptfenster geöffnet:



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 Internet Security 2012** – Details >>
- ***Informationen zum Sicherheitsstatus*** *(oberer Bereich des Fensters)* enthält Informationen zum aktuellen Status Ihres **AVG Internet Security 2012** – Details >>
- ***Quick Links*** *(linker Bereich des Fensters)* ermöglichen das schnelle Aufrufen der wichtigsten und am häufigsten verwendeten Aufgaben von **AVG Internet Security 2012** – Details >>
- ***Meine Apps*** *(oberer linker Bereich des Fensters)* öffnet eine Übersicht über zusätzliche verfügbare Anwendungen für **AVG Internet Security 2012**: LiveKive, Family Safety und PC Tuneup
- ***Komponentenübersicht*** *(zentraler Bereich des Fensters)* zeigt eine Übersicht über alle installierten Komponenten von **AVG Internet Security 2012** – Details >>
- ***Infobereichsymbol*** *(untere rechte Ecke des Bildschirms, im Infobereich)* zeigt den aktuellen Status von **AVG Internet Security 2012** – Details >>
- Δασ ***AVG-Gadget*** *(Windows-Sidebar, wird unter Windows Vista und Windows 7 unterstützt)* ermöglicht schnellen Zugriff auf Scans und Updates von **AVG Internet**

Security 2012 – Details >>

5.1. Systemmenü

Das ***Systemmenü*** ist die Standardnavigation, die in allen Anwendungen von Windows verwendet wird. Es befindet sich horizontal im oberen Teil des Hauptfensters von **AVG Internet Security 2012**. Mit Hilfe des Systemmenüs können Sie auf bestimmte Komponenten, Funktionen und Dienste von AVG zugreifen.

Das Systemmenü ist in fünf Hauptbereiche eingeteilt:

5.1.1. Datei

- ***Beenden*** – Schließt die Benutzeroberfläche von **AVG Internet Security 2012**. Die AVG-Anwendung wird jedoch weiterhin im Hintergrund ausgeführt, damit Ihr Computer geschützt ist!

5.1.2. 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*** erkennt Viren, Spyware, Würmer, Trojaner und unerwünschte, ausführbare Dateien oder Bibliotheken in Ihrem System und schützt Sie vor schädlicher Adware – Details >>
- ***Link Scanner*** schützt Sie beim Surfen im Internet vor webbasierten Angriffen – Details >>
- ***eMail-Schutz*** überprüft Ihre eingehenden eMail-Nachrichten auf SPAM und blockiert Viren, Phishing-Angriffe und andere Bedrohungen – Details >>
- ***Die Firewall*** kontrolliert die Kommunikation an allen Netzwerkports, schützt Sie vor schädlichen Angriffen und verweigert dem Angreifer den Zugriff auf den Computer – Details >>
- ***Anti-Rootkit*** scannt auf gefährliche Rootkits, die sich in Anwendungen, Treibern oder Bibliotheken verstecken können – Details >>
- ***System-Tools*** bietet eine detaillierte Zusammenfassung der Umgebung von AVG und Informationen zum Betriebssystem – Details >>
- ***PC Analyzer*** bietet Informationen zum Status Ihres Computers – Details >>
- ***Identitätsschutz*** schützt permanent Ihre digitalen Daten vor neuen und unbekannten Bedrohungen – Details >>
- ***Security Toolbar*** ermöglicht es Ihnen, ausgewählte Funktion von AVG direkt in Ihrem Internetbrowser zu verwenden – Details >>

- ***Remote-Verwaltung*** wird nur in AVG Business Editionen angezeigt, wenn Sie während des Installationsvorgangs angegeben haben, dass diese Komponente installiert werden soll

5.1.3. Historie

- Scan-Ergebnisse – Wechsel zur Testoberfläche von AVG, und zwar zum Dialog Übersicht über Scan-Ergebnisse
- Residenter Schutz – Anzeigen eines Dialogs mit einer Übersicht über Bedrohungen, erkannt durch den Residenten Schutz
- eMail-Scanner – Öffnet einen Dialog mit einer Übersicht über eMail-Anhänge, die von der Komponente eMail-Schutz als gefährlich erkannt wurden
- Ergebnisse des Online Shield – Öffnet einen Dialog mit einer Übersicht über Bedrohungen, die von dem Dienst Online Shield der Komponente Link Scanner 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 von **AVG Internet Security 2012**
- Firewall – Öffnet die Benutzeroberfläche der Firewall-Einstellungen auf dem Reiter Protokolle mit einer detaillierten Übersicht über alle Firewall-Aktionen

5.1.4. 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 Internet Security 2012**.
- ***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 Internet Security 2012 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.

5.1.5. Hilfe

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

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

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

- ***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/de/) her. Bitte geben Sie Ihre Registrierungsdaten ein – Nur Kunden, die ihr AVG-Produkt registrieren, erhalten auch kostenlosen technischen Support.

Hinweis*: Wenn Sie die Testversion von* **AVG Internet Security 2012** *verwenden, werden die letzten zwei Einträge als* ***Jetzt kaufen*** *und* ***Aktivieren*** *angezeigt und ermöglichen es Ihnen, die Vollversion des Programms zu erwerben. Wenn* **AVG Internet Security 2012** *mit einer Vertriebsnummer installiert ist, werden die Einträge als* ***Registrieren*** *und* ***Aktivieren*** *angezeigt.*

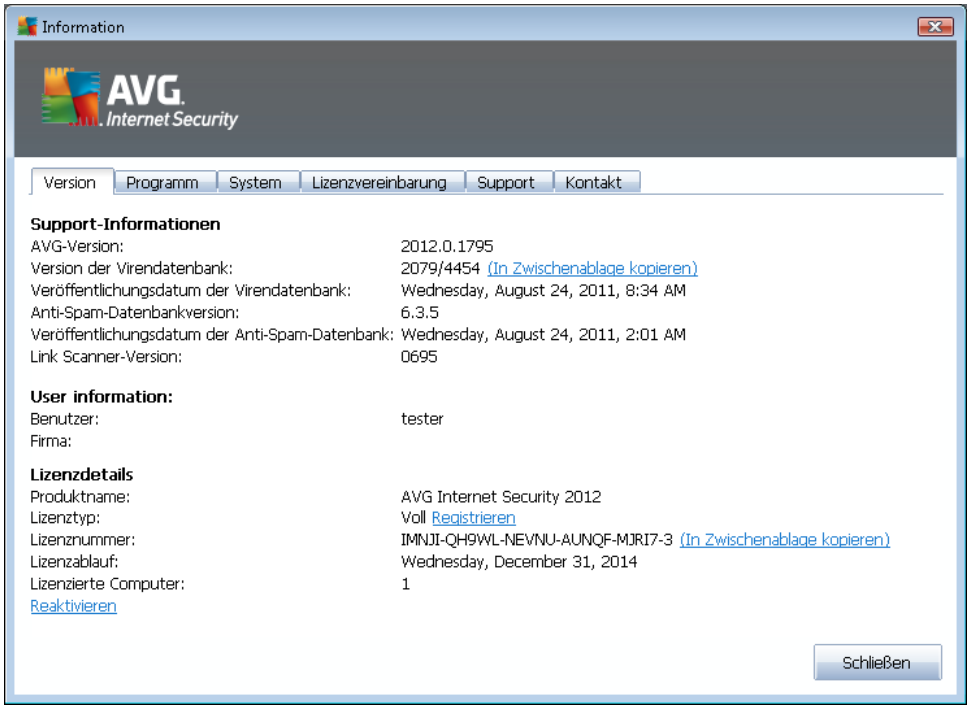
- ***Info zu AVG*** – öffnet den Dialog ***Information*** mit fünf Reitern, die Informationen über den Namen des Programms, das Programm selbst und die Version der Virendatenbank sowie Systeminformationen, die Lizenzvereinbarung und Kontaktdaten von ***AVG Technologies CZ***enthalten.

5.1.6. Support

Der Link ***Support*** öffnet einen neuen Dialog ***Informationen*** mit allen Arten von Informationen zur Unterstützung bei der Suche nach Hilfe. Der Dialog beinhaltet grundlegende Informationen zu Ihrem installierten AVG-Programm (*Programm-/Datenbankversion*), Lizenzdetails sowie eine Liste mit Schnell-Support-Links.

Der Dialog ***Informationen*** ist in sechs Reiter unterteilt:

Der Reiter ***Version*** ist in drei Bereiche gegliedert:



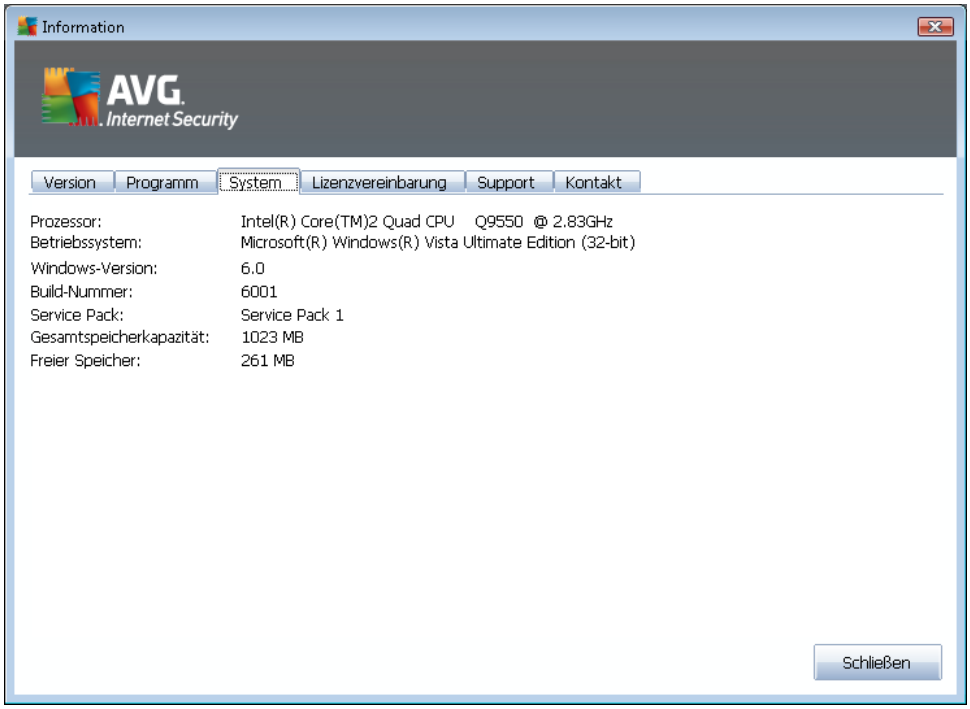
- ***Supportinformationen*** – Enthält Informationen zu den Versionen von**AVG Internet Security 2012**, der Virendatenbank, der Datenbank von Anti-Spam sowie von Link Scanner.

- ***Benutzerinformationen*** – Enthält Informationen über den lizenzierten Benutzer und die Firma.

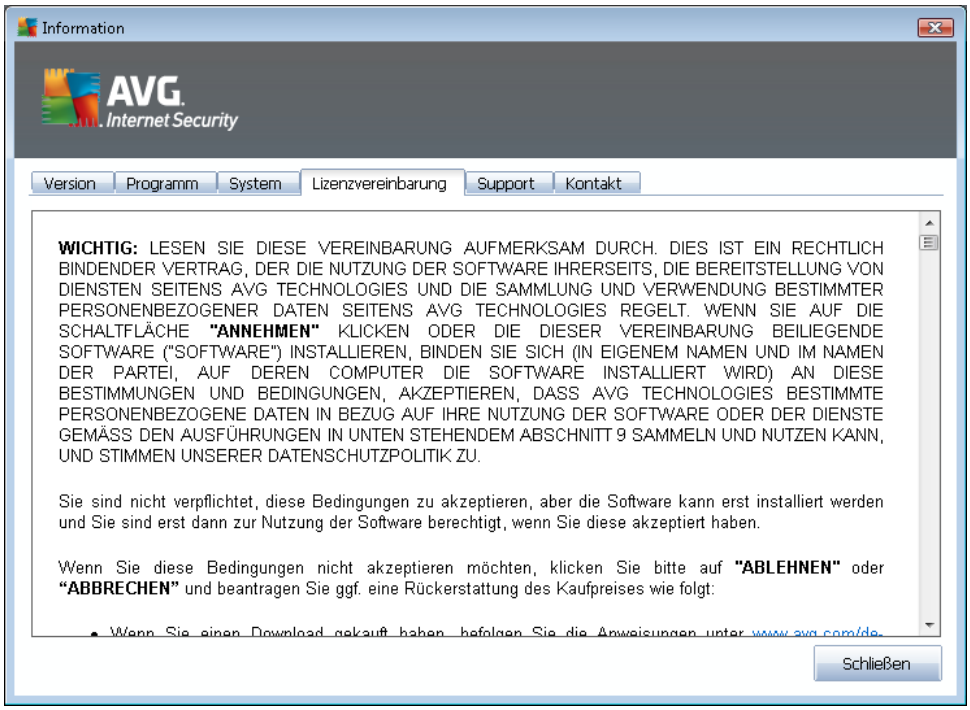
- ***Lizenzdetails*** – Enthält Informationen zu Ihrer Lizenz *(Produktname, Lizenzart, Lizenznummer, Ablaufdatum und Anzahl der Arbeitsplätze*). In diesem Bereich können Sie auch den Link ***Registrieren*** verwenden, um Ihr **AVG Internet Security 2012** online zu registrieren; anschließend können Sie den Technischen Support von AVG vollständig nutzen. Verwenden Sie auch den Link ***Reaktivieren*** , um den Dialog ***AVG aktivieren*** zu öffnen: Geben Sie Ihre Lizenznummer in das entsprechende Feld ein, um entweder die Vertriebsnummer *(die Sie während der AVG Internet Security 2012Installation verwenden)* zu ersetzen oder um Ihre aktuelle Lizenznummer durch eine andere zu ändern *(z. B. beim Upgrade zu einem höheren AVG-Produkt).*

Auf dem Reiter ***Programm*** finden Sie Informationen über die Programmdateiversion von **AVG Internet Security 2012** sowie über Code von anderen Herstellern, der in diesem Produkt verwendet wird:

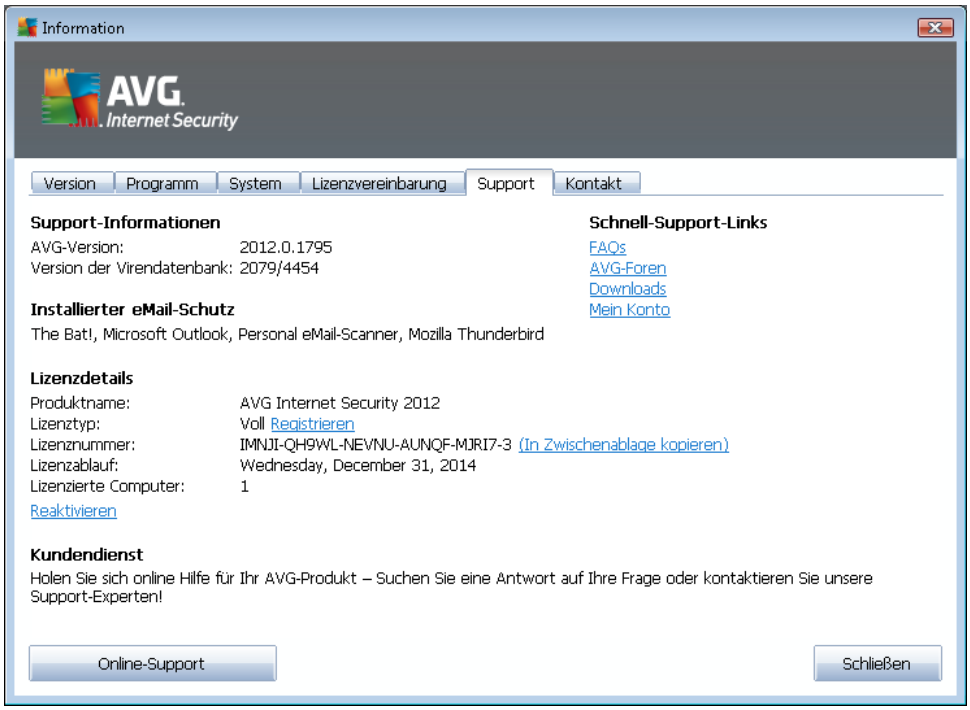
Der Reiter ***System*** enthält eine Liste mit Parametern Ihres Betriebssystems *(Prozessortyp, Betriebssystem und Version, Build-Nummer, verwendete Service Packs, Gesamtspeichergröße und freier Speicherplatz)*:



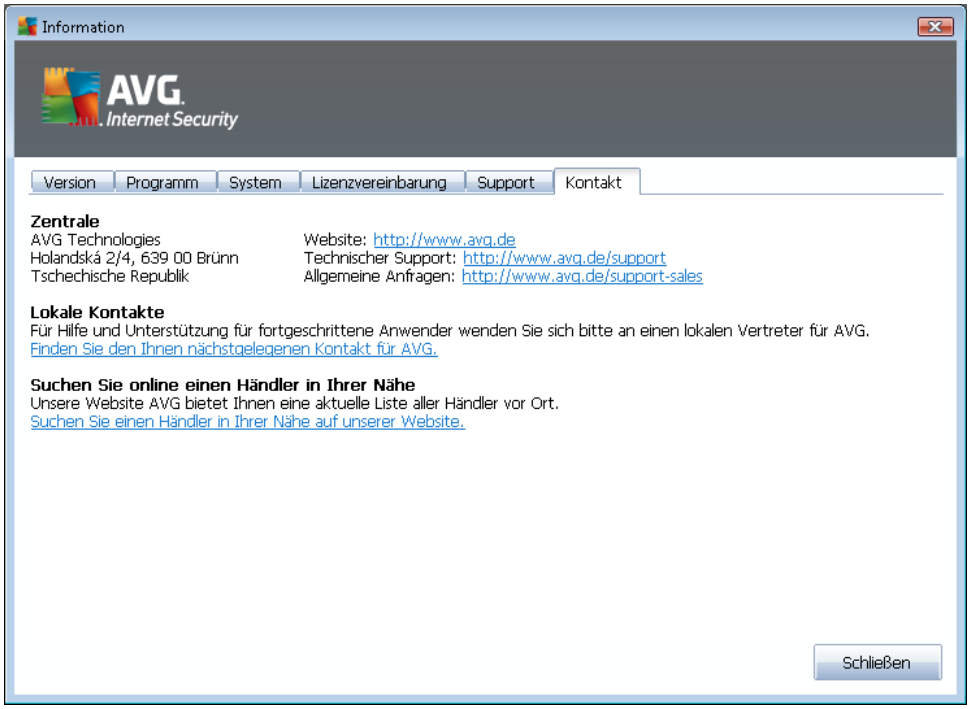
Auf dem Reiter ***Lizenzvereinbarung*** können Sie den vollständigen Text der Lizenzvereinbarung zwischen Ihnen und AVG Technologies lesen:



Der Reiter ***Support*** zeigt eine Liste mit allen Kontaktmöglichkeiten zum Kundendienst an. Er enthält zudem Links zur Website von AVG (http://www.avg.com/de/), zu AVG-Foren und FAQs usw. Außerdem finden Sie hilfreiche Informationen, die Sie für den Kontakt mit dem Kundendienst benötigen:



Der Reiter ***Kontakt*** enthält eine Liste aller Kontakte zu AVG Technologies sowie Kontaktinformationen lokaler Vertreter und Vertriebspartner von AVG:



5.2. Informationen zum Sicherheitsstatus

Der Bereich ***Informationen zum Sicherheitsstatus*** befindet sich im oberen Teil des Hauptfensters von **AVG Internet Security 2012**. In diesem Bereich finden Sie stets Informationen zum aktuellen Sicherheitsstatus von **AVG Internet Security 2012**. 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 Internet Security 2012 voll funktionsfähig ist***. Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

 – Das orangefarbene Symbol warnt Sie, wenn eine oder mehrere Komponenten falsch konfiguriert sind. Überprüfen Sie deren Eigenschaften/Einstellungen. Es besteht kein ernstes Problem in **AVG Internet Security 2012** und Sie haben sich wahrscheinlich aus einem bestimmten Grund dazu entschlossen, eine Komponente zu deaktivieren. Sie sind immer noch geschützt. Sie sollten jedoch die Einstellungen der problematischen Komponente überprüfen! Den Namen der Komponente finden Sie im Bereich ***Informationen zum Sicherheitsstatus***.

Das orangefarbene Symbol wird auch angezeigt, wenn Sie aus einem bestimmten Grund

festgelegt haben, den Fehlerstatus einer Komponente zu ignorieren. Die Option ***Komponentenstatus ignorieren*** ist über das Kontextmenü (*zu öffnen mit rechtem Mausklick*) des entsprechenden Komponentensymbols verfügbar, das sich in der Komponentenübersicht des Hauptfensters von **AVG Internet Security 2012** befindet. Wählen Sie diese Option, wenn Ihnen bekannt ist, dass die Komponente einen Fehlerstatus aufweist, aber **AVG Internet Security 2012** aus einem bestimmten Grund diesen Status beibehalten soll und Sie nicht über das Infobereichsymbol gewarnt werden möchten. 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 ***AVG Internet Security 2012 sich in einem kritischen Status befindet***. Eine oder mehrere Komponenten arbeiten nicht richtig und **AVG Internet Security 2012** 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.

Wenn AVG Internet Security 2012nicht für eine optimale Leistung konfiguriert ist, wird neben den Sicherheitsstatusinformationen eine neue Schaltfläche „Reparieren“ angezeigt (alternativ auch „Alles reparieren“, wenn das Problem mehrere Komponenten betrifft). Klicken Sie auf diese Schaltfläche, um einen automatischen Vorgang zur Programmüberprüfung und -konfiguration zu starten. Anhand dieser einfachen Methode können Sie die optimale Leistung von AVG Internet Security 2012 gewährleisten und maximale Sicherheit erzielen.

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 zu AVG Internet Security 2012 erhalten Sie auch jederzeit über das Symbol im Infobereich.*

5.3. Quick Links

Quick Links befinden sich auf der linken Seite der Benutzeroberfläche von **AVG Internet Security 2012**. Über diese Links können Sie sofort auf die wichtigsten und am häufigsten verwendeten Funktionen der Anwendung zugreifen, d. h. Scan und Update. Die Quick Links sind von allen Dialogen der Benutzeroberfläche aus verfügbar:

Die Quick Links sind grafisch in drei Bereiche unterteilt:

- ***Übersicht*** – Mit diesem Link können Sie von jedem aktuell geöffneten Dialog von AVG zum Standardfenster wechseln, in dem Sie eine Übersicht über alle installierten Komponenten erhalten. *(Weitere Informationen finden Sie im Kapitel Komponentenübersicht)*

- ***Jetzt prüfen*** – Diese Schaltfläche gibt standardmäßig Auskunft über den zuletzt gestarteten Scan *(d. h. Scantyp und Datum des letzten Starts)*. Klicken Sie auf den Befehl ***Jetzt prüfen***, um denselben Scan noch einmal zu starten. Wenn Sie einen anderen Scan starten möchten, klicken Sie auf den Link ***Scan-Optionen***. Auf diese Weise öffnen Sie die Scan-Benutzeroberfläche von AVG , über die Sie Scans ausführen, planen oder Scan-Parameter bearbeiten können. *(Weitere Informationen finden Sie im Kapitel AVG-Scans)*

- ***Jetzt aktualisieren*** – Dieser Link zeigt Ihnen Datum und Uhrzeit des letzten Updates an. Klicken Sie auf die Schaltfläche, um den Update-Vorgang sofort zu starten und seinen Fortschritt zu verfolgen. *(Weitere Informationen finden Sie im Kapitel AVG Updates)*

Auf die ***Quick Links*** können Sie jederzeit über die Benutzeroberfläche von AVG zugreifen. Wenn Sie einen Prozess (entweder einen Scan oder ein Update) über einen Quick Link ausführen, wechselt die Anwendung zu einem neuen Dialog, die Quick Links bleiben aber weiter verfügbar. Der laufende Prozess wird zudem grafisch in der Navigation angezeigt, so dass Sie die vollständige Kontrolle über alle gestarteten Prozesse haben, die momentan in **AVG Internet Security 2012** ausgeführt werden.

5.4. Komponentenübersicht

Bereiche der Komponentenübersicht

Der Bereich ***Komponentenübersicht*** befindet sich im mittleren Teil der Benutzeroberfläche von **AVG Internet Security 2012**. Er ist in zwei Teile gegliedert:

- ***In der Übersicht über alle installierten Komponenten*** werden alle installierten Komponenten grafisch dargestellt. Jedes Element besteht aus dem Symbol der Komponente und gibt Auskunft über den Status der jeweiligen Komponente (Aktiv oder Nicht aktiv).

- ***Die Komponentenbeschreibung*** befindet sich im unteren Teil dieses Dialogs. Die Beschreibung erläutert kurz die grundlegende Funktion der Komponente. Sie gibt außerdem Auskunft über den aktuellen Status der ausgewählten Komponente.

Liste der installierten Komponenten

In **AVG Internet Security 2012** enthält der Bereich ***Komponentenübersicht*** Informationen zu folgenden Komponenten:

- ***Anti-Virus*** erkennt Viren, Spyware, Würmer, Trojaner und unerwünschte, ausführbare Dateien oder Bibliotheken in Ihrem System und schützt Sie vor schädlicher Adware – Details >>

- ***Link Scanner*** schützt Sie beim Surfen im Internet vor webbasierten Angriffen – Details >>

- ***eMail-Schutz*** überprüft Ihre eingehenden eMail-Nachrichten auf SPAM und blockiert Viren, Phishing-Angriffe und andere Bedrohungen – Details >>
- ***Firewall*** kontrolliert jegliche Kommunikation an jedem Netzwerkanschluss, schützt Sie vor schädlichen Angriffen und blockiert alle Eindringungsversuche - Details >>
- ***Anti-Rootkit*** scannt auf gefährliche Rootkits, die sich in Anwendungen, Treibern oder Bibliotheken verstecken können – Details >>
- ***System-Tools*** bietet eine detaillierte Zusammenfassung der Umgebung von AVG und Informationen zum Betriebssystem – Details >>
- ***PC Analyzer*** bietet Informationen zum Status Ihres Computers – Details >>
- ***Identitätsschutz*** schützt permanent Ihre digitalen Daten vor neuen und unbekannten Bedrohungen –·Details >>
- ***Security Toolbar*** ermöglicht es Ihnen, ausgewählte Funktionen von AVG direkt in Ihrem Internetbrowser zu verwenden – Details >>

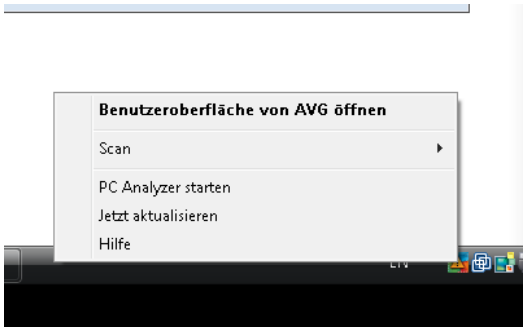
- ***Remote-Verwaltung*** wird nur in AVG Business Editionen angezeigt, wenn Sie während des Installationsvorgangs angegeben haben, dass diese Komponente installiert werden soll

Verfügbare Aktionen

- ***Bewegen Sie Ihre Maus über eines der Komponentensymbole***, um die Komponente in der Übersicht zu markieren. Im unteren Teil der Benutzeroberfläche wird eine kurze Funktionsbeschreibung der ausgewählten Komponente angezeigt.
- ***Klicken Sie auf ein Symbol***, um die Benutzeroberfläche der jeweiligen Komponente mit einer Auflistung von statistischen Basisdaten anzuzeigen.
- ***Klicken Sie mit der rechten Maustaste auf ein Komponentensymbol***, um das Kontextmenü mit weiteren Optionen anzuzeigen:
  - ***Öffnen*** – Klicken Sie auf diese Option, um den Dialog der Komponente zu öffnen *(genauso wie bei einem einfachen Klick auf das Komponentensymbol)*.
  - ***Komponentenstatus ignorieren*** – Wählen Sie diese Option, wenn Ihnen der Fehlerstatus der Komponente bekannt ist, Sie aber den Status beibehalten und nicht über das Infobereichsymbol gewarnt werden möchten.
  - ***In den erweiterten Einstellungen öffnen...*** – Diese Option ist nur für die Komponenten verfügbar, die die Option Erweiterte Einstellungen aufweisen.

5.5. Infobereichsymbol

Das ***Infobereichsymbol von AVG*** *(in Ihrer Windows-Taskleiste in der unteren rechte Ecke Ihres Monitors)* zeigt den aktuellen Status Ihres **AVG Internet Security 2012** an. Es wird immer in Ihrem Infobereich angezeigt, unabhängig davon, ob die Benutzeroberfläche von **AVG Internet Security 2012** geöffnet oder geschlossen ist:



Anzeige des Infobereichsymbols von AVG

- Wird das Symbol in Vollfarbe und ohne zusätzliche Elemente angezeigt, bedeutet dies, dass alle Komponenten von **AVG Internet Security 2012** aktiv und voll funktionsfähig sind. Das Symbol kann jedoch auch auf diese Weise angezeigt werden, wenn eine der Komponenten nicht voll funktionsfähig ist, der Benutzer aber festgelegt hat, den Komponentenstatus zu ignorieren. *(Wenn Sie die Option „Komponentenstatus ignorieren" bestätigen, ist Ihnen der Fehlerstatus der Komponente bekannt, Sie möchten aber aus einem bestimmten Grund den Status beibehalten und nicht über diese Situation gewarnt werden.)*

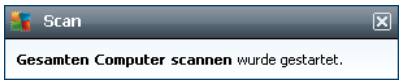
- Das Symbol mit einem Ausrufezeichen zeigt an, dass eine Komponente *(oder auch mehrere Komponenten)* einen Fehlerstatus aufweist. Bitte berücksichtigen Sie immer solche Warnungen und versuchen Sie, das Konfigurationsproblem einer Komponente, die nicht richtig eingestellt ist, zu beheben. Um Änderungen in der Konfiguration einer Komponente vorzunehmen, doppelklicken Sie auf das Infobereichsymbol, um die Benutzeroberfläche der Anwendung zu öffnen. Detaillierte Informationen darüber, welche Komponenten einen Fehlerstatus aufweisen, finden Sie im Abschnitt Informationen zum Sicherheitsstatus.

- Das Infobereichsymbol kann auch in Vollfarbe mit einem blinkenden und sich drehenden Lichtstrahl angezeigt werden. Diese grafische Anzeige signalisiert einen aktuell gestarteten Updatevorgang.

- Alternativ kann das Symbol auch in Vollfarbe mit einem Pfeil angezeigt werden; dies bedeutet, dass gerade ein **AVG Internet Security 2012**-Scan ausgeführt wird.

Informationen zum Infobereichsymbol von AVG

Das ***Infobereichsymbol von AVG*** gibt außerdem Auskunft über aktuelle Aktivitäten Ihres **AVG Internet Security 2012** sowie über mögliche Statusänderungen des Programms (*z. B. automatischer Start eines geplanten Scans oder Updates, Firewall-Profilwechsel, die Statusänderung einer Komponente, Auftreten eines Fehlerstatus usw.*). Dabei wird über das Infobereichsymbol ein Popup-Fenster geöffnet:



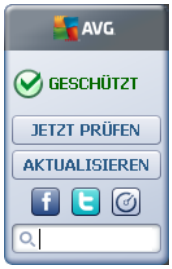
Über das Infobereichsymbol von AVG verfügbare Aktionen

Das ***Infobereichsymbol von AVG*** kann auch als Quick Link verwendet werden, um auf die Benutzeroberfläche von **AVG Internet Security 2012** zuzugreifen. Doppelklicken Sie dazu einfach auf das Symbol. Wenn Sie mit der rechten Maustaste auf das Symbol klicken, wird ein kurzes Kontextmenü mit den folgenden Optionen geöffnet:

- ***Benutzeroberfläche von AVG öffnen*** – Klicken Sie hierauf, um die Benutzeroberfläche von **AVG Internet Security 2012** zu öffnen.
- ***Scans*** – Klicken Sie auf diese Option, um das Kontextmenü Vordefinierte Scans zu öffnen (*Scan des gesamten Computers*, *Bestimmte Dateien/Ordner scannen*, *Anti-Rootkit-Scan*), und wählen Sie den erforderlichen Scan aus, der daraufhin sofort gestartet wird.
- ***Firewall*** – Klicken Sie auf diese Option, um das Kontextmenü mit den Einstellungsoptionen der Firewall zu öffnen, wo Sie die folgenden Parameter bearbeiten können:Firewall-Status (*Firewall aktiviert/Firewall deaktiviert/Notfallmodus*), Spielmoduswechsel und Firewall-Profile.
- ***PC Analyzer*** ausführen – Klicken Sie auf diese Option, um die Komponente PC Analyzer aufzurufen.
- ***Scans werden durchgeführt*** – Dieser Hinweis wird nur angezeigt, wenn auf Ihrem Computer gerade ein Scan ausgeführt wird. Sie können den Scan unterbrechen, anhalten oder eine Priorität festlegen. Außerdem stehen folgenden Aktionen zur Verfügung:*Priorität für alle Scans festlegen, Alle Scans unterbrechen* oder *Alle Scans anhalten*.
- ***Jetzt aktualisieren*** – Startet ein sofortiges Update.
- ***Hilfe*** –·Die Hilfedatei wird auf der Startseite geöffnet.

5.6. AVG-Gadget

Das ***AVG-Gadget*** wird auf dem Windows-Desktop angezeigt (*Windows-Sidebar*). Diese Anwendung wird nur in den Betriebssystemen Windows Vista und Windows 7 unterstützt. Über das ***AVG-Gadget*** können Sie direkt auf die wichtigsten Funktionen von **AVG Internet Security 2012** zugreifen, wie Scans und Updates:



Schnellzugriff auf Scan- und Update-Vorgänge

Das ***AVG-Gadget*** ermöglicht Ihnen, unmittelbar einen Scan- oder Update-Vorgang zu starten:

- ***Jetzt scannen*** –·Klicken Sie auf den Link ***Jetzt scannen***, um sofort einen Scan des gesamten Computers zu starten. Sie können den Scanvorgang in der geänderten Benutzeroberfläche des Gadget nachvollziehen. Eine Übersicht bietet Informationen über die Anzahl der gescannten Objekte, erkannten Bedrohungen und geheilten Bedrohungen.

  Sie können den Scanvorgang jederzeit unterbrechen  oder anhalten  . Weitere Informationen zu den Scan-Ergebnissen finden Sie im Standarddialog Übersicht über Scan-Ergebnisse, der direkt vom Gadget aus über die Option ***Details anzeigen*** geöffnet werden kann *(die entsprechenden Scan-Ergebnisse werden unter Scan der Sidebar-Gadgets)* aufgelistet.

- ***Jetzt aktualisieren*** – Klicken Sie auf den Link ***Jetzt aktualisieren***, um das **AVG Internet Security 2012**-Update direkt über das Gadget zu starten:

Zugriff auf soziale Netzwerke

Das ***AVG-Gadget*** bietet außerdem einen Quick Link für den Zugriff auf die größten sozialen

Netzwerke. Verwenden Sie die entsprechende Schaltfläche, um eine Verbindung mit den AVG-Communitys auf Twitter, Facebook oder LinkedIn herzustellen:

- ***Twitter-Link*** – Öffnet eine neue Benutzeroberfläche des ***AVG-Gadget*** mit einer Übersicht über die neuesten Twitter-Feeds zu AVG. Klicken Sie auf den Link ***Alle Twitter-Feeds von AVG anzeigen***, um die speziell auf AVG bezogene Twitter-Website in einem neuen Fenster Ihres Internetbrowsers zu öffnen:

- ***Facebook-Link*** – Öffnet in Ihrem Internetbrowser die Seite der ***AVG Community*** auf Facebook

- ***LinkedIn*** – Diese Option ist nur innerhalb der Netzwerkinstallation verfügbar (*d. h. vorausgesetzt, dass AVG mit einer Lizenz für AVG Business Edition installiert wurde*) und öffnet Ihren Internet-Browser mit der Website ***AVG SMB Community*** des sozialen Netzwerks „LinkedIn“

Andere über das Gadget verfügbare Funktionen

- ***PC Analyzer*** – Öffnet die Benutzeroberfläche in der Komponente PC Analyzer

- ***Suchfeld*** – Geben Sie ein Schlüsselwort ein, und Sie erhalten die Suchergebnisse sofort in einem neu geöffneten Fenster Ihres Standardwebbrowsers

6. Komponenten von AVG

6.1. Anti-Virus

Die Komponente ***Anti-Virus*** ist ein Grundstein Ihres **AVG Internet Security 2012** und vereint mehrere grundlegende Funktionen eines Sicherheitsprogramms:

- Scan-Engine
- Residenter Schutz
- Anti-Spyware-Schutz

6.1.1. Scan-Engine

Die Scan-Engine ist der Grundstein der Komponente ***Anti-Virus*** und scannt 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 Virenquarantäne verschoben.

Die zentrale Funktion des Schutzes von AVG Internet Security 2012 besteht darin, das Ausführen bekannter Viren auf dem Computer zu verhindern.

Erkennungsmethoden

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. ***Anti-Virus*** verwendet die folgenden Erkennungsmethoden:

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

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. **AVG Internet Security 2012** kann zudem ausführbare Anwendungen oder DLL-Bibliotheken, die im System potentiell unerwünscht sind, erkennen und analysieren. Diese Bedrohungen bezeichnen wir als potentiell unerwünschte Programme *(verschiedene Arten von Spyware, Adware usw.)*.. Außerdem durchsucht **AVG Internet Security 2012** Ihre System-Registrierung nach verdächtigen Einträgen, temporären Internetdateien und Tracking Cookies und ermöglicht Ihnen, mit allen potentiell schädlichen Elementen wie mit jeder anderen Infektion zu verfahren.

AVG Internet Security 2012 bietet permanenten Schutz für Ihren Computer.

6.1.2. Residenter Schutz

AVG Internet Security 2012 bietet Ihnen einen kontinuierlichen Schutz in Form des so genannten Residenten Schutzes. Die Komponente ***Anti-Virus*** scannt jede einzelne Datei *(mit bestimmten Erweiterungen oder ohne jegliche Erweiterungen)*, die geöffnet, gespeichert oder kopiert wird. Sie überwacht sowohl die Systembereiche des Computers als auch Wechseldatenträger (*Flash-Laufwerke usw.).*). Wird in einer Datei, auf die zugegriffen wird, ein Virus entdeckt, stoppt die Komponente den aktuell ausgeführten Vorgang und hindert den Virus daran, sich zu aktivieren. Normalerweise nehmen Sie diesen Vorgang nicht wahr, da der Residente Schutz „im Hintergrund“ läuft. Sie werden nur benachrichtigt, wenn Bedrohungen gefunden werden; gleichzeitig blockiert ***Anti-Virus*** die Aktivierung der Bedrohung und entfernt sie.

Der Residente Schutz wird beim Systemstart in den Speicher Ihres Computers geladen. Es wird dringend davon abgeraten, den Residenten Schutz zu deaktivieren.

6.1.3. Anti-Spyware-Schutz

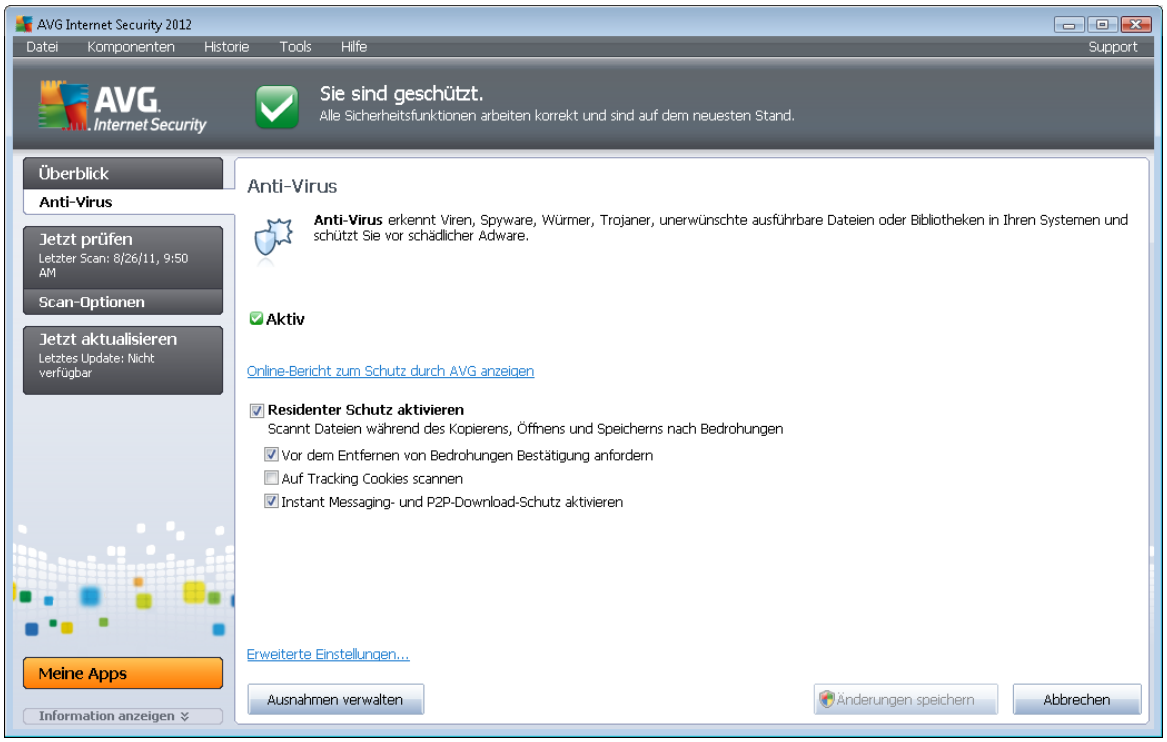
Anti-Spyware besteht aus einer Spyware-Datenbank, die zur Erkennung bekannter Spyware-Definitionstypen verwendet wird. Die Spyware-Experten von AVG arbeiten unermüdlich daran, die neuesten Spyware-Muster zu erkennen, zu beschreiben und die Definitionen zur Datenbank hinzuzufügen, sobald diese Muster auftauchen. Mittels des Update-Prozesses werden diese Definitionen auf Ihren Computer heruntergeladen, so dass Sie stets zuverlässig selbst gegen die neuesten Spyware-Typen geschützt sind. ***Mit Anti-Spyware*** können Sie Ihren Computer vollständig nach Malware/Spyware durchsuchen. Außerdem erkennt die Komponente ruhende und nicht aktive Malware, d. h. Malware, die heruntergeladen, aber noch nicht aktiviert wurde.

Was ist Spyware?

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.

6.1.4. Benutzeroberfläche des Anti-Virus

Die Benutzeroberfläche der Komponente ***Anti-Virus*** enthält kurze Informationen über die Funktionen der Komponente, über ihren aktuellen Status *(Aktiv)* und ihre grundlegenden Konfigurationsoptionen:



Konfigurationsoptionen

Der Dialog enthält einige grundlegende Konfigurationsoptionen der für die Komponente ***Anti-Virus*** verfügbaren Funktionen. Nachfolgend finden Sie eine kurze Beschreibung dieser Optionen:

- ***Online-Bericht zum Schutz durch AVG anzeigen*** – Über diesen Link werden Sie auf eine bestimmte Seite auf der Website von AVG (http://www.avg.com/de/) weitergeleitet. Auf dieser Seite finden Sie eine detaillierte statistische Übersicht über alle Aktivitäten, die **AVG Internet Security 2012** auf Ihrem Computer in einem bestimmten Zeitraum bzw. insgesamt durchgeführt hat.

- ***Residenter Schutz aktivieren*** – Mit dieser Option können Sie den Residenten Schutz leicht ein-/ausschalten. Residenter Schutz scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden. Wenn ein Virus oder eine andere Bedrohung erkannt wird, werden Sie unmittelbar gewarnt. Diese Funktion ist standardmäßig aktiviert, und es wird empfohlen, dies nicht zu ändern! Mit dem Residenten Schutz können Sie zudem festlegen, wie mit Infektionen umgegangen werden soll:

  - ***Alle Bedrohungen automatisch entfernen*** / ***Vor dem Entfernen von Bedrohungen Bestätigung anfordern*** – Wählen Sie wahlweise eine dieser Optionen. Diese Auswahl hat keinen Einfluss auf die Sicherheitsstufe und kann

beliebig festgelegt werden.

- ***Auf Tracking Cookies scannen*** – Unabhängig von den vorherigen Optionen können Sie entscheiden, ob Sie auf Tracking Cookies scannen möchten. *(Cookies sind 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.)* In bestimmten Fällen kann es sinnvoll sein, diese Option zu aktivieren, um maximale Sicherheit zu erzielen, sie ist jedoch standardmäßig deaktiviert.

- ***Instant Messaging-Schutz aktivieren*** – Aktivieren Sie diese Option, um festzulegen, dass die Kommunikation über Instant Messenger (*z. B. ICQ, MSN Messenger usw.*) auf Viren überprüft werden soll.

- ***Erweiterte Einstellungen***... – Klicken Sie auf den Link, um zum entsprechenden Dialog der Erweiterten Einstellungen von **AVG Internet Security 2012** zu gelangen. Dort können Sie die Konfiguration der Komponente im Detail bearbeiten. Beachten Sie jedoch, dass die Standardkonfiguration aller Komponenten so eingestellt wurde, dass **AVG Internet Security 2012** eine optimale Leistung und maximale Sicherheit gewährleistet. Es wird empfohlen, die Standardkonfiguration nicht zu ändern, es sei denn, Sie haben einen besonderen Grund dazu!

Schaltflächen

Im Dialogs stehen die folgenden Schaltflächen zur Verfügung:

- ***Ausnahmen verwalten*** – Öffnet einen neuen Dialog mit dem Namen Residenter Schutz – Ausnahmen. Der Dialog ist auch über das Hauptmenü verfügbar; klicken Sie dazu auf Erweiterte Einstellungen/Anti-Virus/Residenter Schutz/Ausnahmen *(siehe entsprechendes Kapitel für eine detaillierte Beschreibung)*. In dem Dialog können Sie Dateien und Ordner festlegen, die vom Scan durch den Residenten Schutz ausgeschlossen werden sollen. Wenn dies nicht unbedingt notwendig ist, empfehlen wir dringend, keine Einträge auszuschließen! Der Dialog enthält folgende Schaltflächen:

  - *Pfad hinzufügen* – Mit dieser Schaltfläche können Sie ein Verzeichnis *(oder mehrere Verzeichnisse)* angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen.

  - *Datei hinzufügen* – Mit dieser Schaltfläche können Sie Dateien angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen.

  - *Eintrag bearbeiten* – Hier können Sie den festgelegten Pfad zu einer ausgewählten Datei oder einem ausgewählten Ordner bearbeiten.

  - *Eintrag entfernen* – Mit dieser Schaltfläche können Sie den Pfad zu einem ausgewählten Eintrag aus der Liste löschen.

- ***Änderungen speichern*** – Mit dieser Schaltfläche können Sie alle Änderungen der in diesem Dialog vorgenommenen Einstellungen der Komponente speichern und zur Haupt-Benutzeroberfläche von **AVG Internet Security 2012** (*Komponentenübersicht*) zurückkehren.

- ***Abbrechen*** – Alle Änderungen der in diesem Dialog vorgenommenen Einstellungen der Komponente werden widerrufen. Es werden keine Änderungen gespeichert. Sie kehren zur Haupt-Benutzeroberfläche von **AVG Internet Security 2012** (*Komponentenübersicht*) zurück.

6.1.5. Erkennungen durch den Residenten Schutz

Bedrohung gefunden!

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:

In diesem Warndialog finden Sie Informationen zu der Datei, die als infiziert erkannt wurde (*Dateiname*), den Namen der erkannten Bedrohung (*Name der Bedrohung*) und einen Link zur Virenenzyklopädie, wo Sie weitere Informationen zur erkannten Infektion finden, falls bekannt (*Weitere Informationen*).

Sie müssen außerdem entscheiden, welche Maßnahmen ergriffen werden sollten. Mehrere Optionen stehen zur Verfügung. ***Beachten Sie, dass unter bestimmten Bedingungen (Art und Speicherort der infizierten Datei) nicht immer alle Optionen verfügbar sind.***

- ***Bedrohung als Hauptbenutzer entfernen*** – Aktivieren Sie das Kontrollkästchen, falls Sie der Meinung sind, dass Sie als normaler Benutzer nicht genügend Rechte zum Entfernen der Datei haben. Hauptbenutzer verfügen über umfassende Zugriffsrechte. Falls sich die Bedrohung·in einem bestimmten Systemordner befindet, müssten Sie, wenn nötig, das Kontrollkästchen für ein erfolgreiches Entfernen aktivieren.

- ***Heilen*** – Diese Schaltfläche wird nur angezeigt, wenn die erkannte Infektion geheilt werden kann. Daraufhin wird die Infektion aus der Datei entfernt, und der ursprüngliche Zustand der Datei wird wiederhergestellt. Wenn es sich bei der Datei selbst um einen Virus handelt, verwenden Sie diese Schaltfläche, um sie zu löschen (*d. h. in die Virenquarantäne verschieben)*

- ***In Quarantäne verschieben*** – Der Virus wird in die -Virenquarantäne verschoben

- ***Gehe zu Datei*** – Mit dieser Option werden Sie zum genauen Speicherort des verdächtigen Objekts weitergeleitet (*öffnet ein neues Fenster von Windows Explorer*)

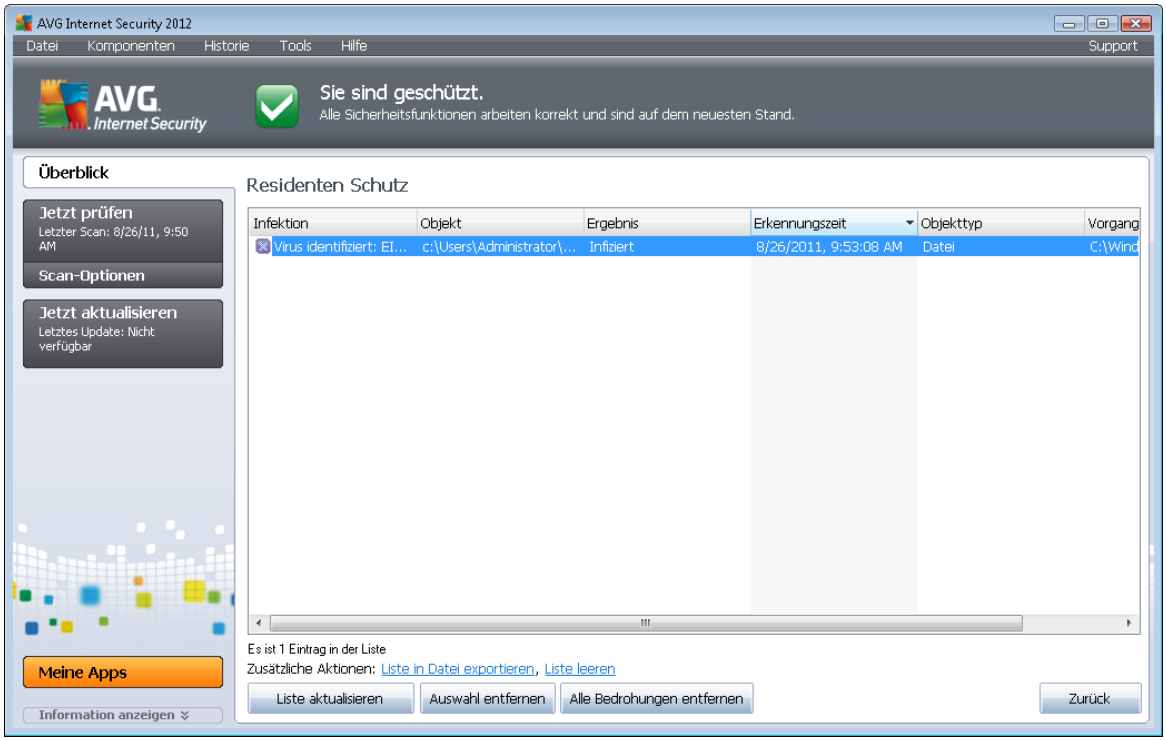
- ***Ignorieren*** – Es wird dringend empfohlen, diese Option NICHT zu verwenden, wenn Sie keinen wirklich guten Grund dazu haben!

Hinweis: *Die Größe des entdeckten Objektes kann gegebenenfalls den verfügbaren Speicherplatz der Virenquarantäne überschreiten. In diesem Fall erscheint eine Warnmeldung, die Sie über das Problem informiert, wenn Sie versuchen, das infizierte Objekt in die Quarantäne zu verschieben. Die Größe des Quarantänespeichers kann jedoch angepasst werden. Sie ist als einstellbarer Prozentsatz der tatsächlichen Größe Ihrer Festplatte definiert. Um die Größe Ihres Quarantänespeichers zu erhöhen, rufen Sie den Quarantäne-Dialog innerhalb der Erweiterten Einstellungen für AVG auf und ändern Sie die Option 'Größe der Quarantäne begrenzen'.*

Im unteren Abschnitt des Dialogs finden Sie den Link ***Details anzeigen*** – Klicken Sie auf diesen Link, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess zu öffnen, der beim Erkennen der Infektion ausgeführt wurde.

Übersicht über Erkennungen durch den Residenten Schutz

Die Gesamtübersicht über alle vom Residenten Schutz gefundenen Bedrohungen können Sie im Dialog ***Erkennung durch den Residenten Schutz*** aufrufen, und zwar im Systemmenü unter der Option Historie/Ergebnisse des Residenten Schutzes:



Der Bereich ***Erkennung durch den 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 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
- ***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*** kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*) zurück.

6.2. Link Scanner

Link Scanner schützt vor den akuten kurzlebigen Bedrohungen aus dem Internet. Gefahren lauern auf allen möglichen Webseiten, egal ob es sich um Seiten von Regierungsbehörden, großen und bekannten Markenfirmen oder Kleinbetrieben handelt. Und sie verweilen dort selten länger als 24 Stunden. ***Link Scanner*** sorgt für den nötigen Schutz durch Analyse aller sich hinter einem Link verbergenden Webseiten. Das garantiert den gewünschten Schutz im entscheidenden Moment: nämlich kurz bevor Sie auf den Link klicken.

Link Scanner ist nicht für den Schutz von Serverplattformen vorgesehen!

Die ***Link Scanner***-Technologie umfasst folgende Funktionen:

- Search-Shield enthält eine Liste von Websites (URL-Adressen), deren Gefährlichkeit bekannt ist. Wenn Sie eine Internetsuche mit Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask oder Seznam durchführen, werden alle Suchergebnisse gemäß dieser Liste überprüft. Jedes Ergebnis erhält anschließend ein Zertifikatssymbol *(für Suchergebnisse von Yahoo! werden nur die Zertifikatssymbole für „Website-Exploits“ angezeigt)*.

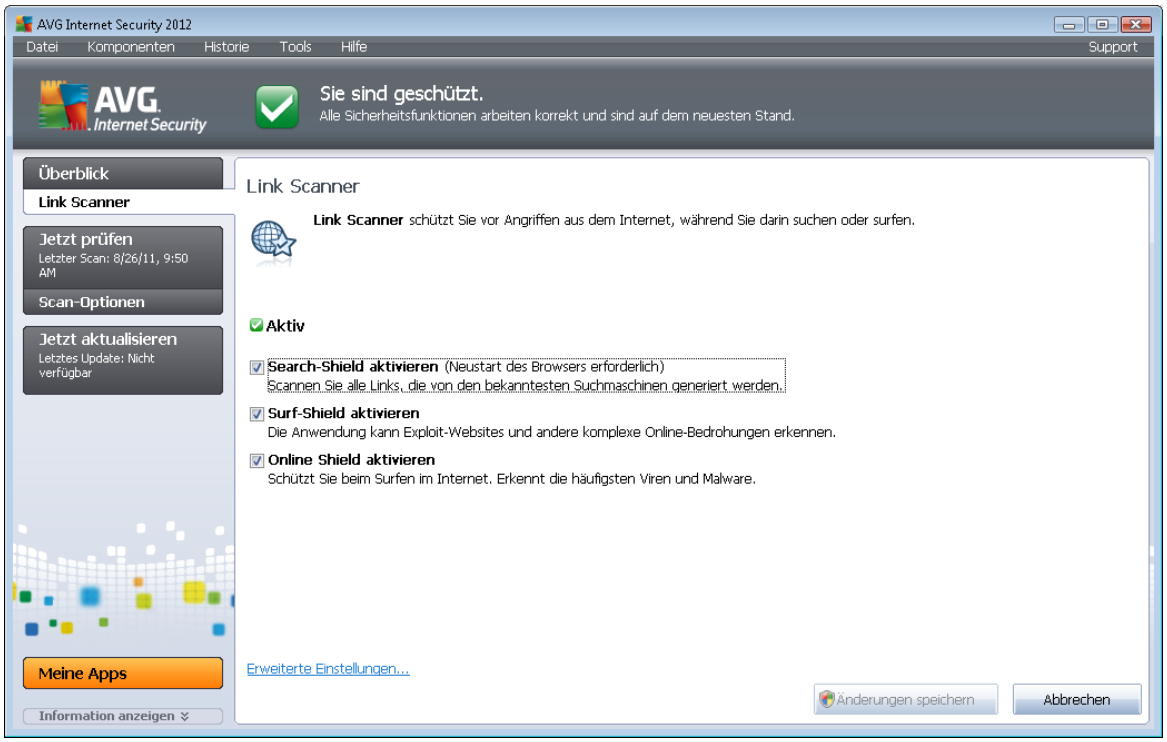
- Surf-Shield scannt die Inhalte der von Ihnen besuchten Websites unabhängig von deren Adresse. Selbst wenn eine Website nicht von Search-Shield *erkannt wird (z. B. wenn eine neue verseuchte Website erstellt wird oder wenn eine bisher saubere Website jetzt Malware enthält)*, wird diese von Surf-Shield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

- Online Shield bietet einen Echtzeitschutz beim Surfen im Internet. Die Inhalte besuchter Webseiten (und möglicher enthaltener Dateien) werden gescannt, noch bevor diese in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen werden. Online Shield erkennt Viren und Spyware auf der Seite, die Sie besuchen möchten, und hält den Download sofort an, so dass erst gar keine Bedrohungen auf Ihren Computer gelangen.

- ***AVG Accelerator*** ermöglicht eine gleichmäßigere Online-Videowiedergabe und vereinfacht das zusätzliche Herunterladen. Wenn der Video-Beschleunigungsvorgang ausgeführt wird, werden Sie über das Popup-Fenster im Infobereich benachrichtigt.

6.2.1. Benutzeroberfläche des Link Scanners

Der Hauptdialog der Komponente Link Scanner enthält eine kurze Beschreibung der Funktionen der Komponente sowie Informationen über ihren aktuellen Status *(Aktiv)*:



Im unteren Bereich des Dialogs können einige grundlegenden Funktionen der Komponente konfiguriert werden:

- ***Search-Shield*** aktivieren – (*standardmäßig aktiviert*): Deaktivieren Sie das Kontrollkästchen nur, wenn Sie einen besonderen Grund haben, die Funktion von Search-Shield zu deaktivieren.

- ***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.

- ***Online Shield*** aktivieren – (*standardmäßig aktiviert*): Scannt Webseiten, die Sie besuche möchten, auf Viren oder Spyware in Echtzeit. Beim Erkennen von Viren und Spyware wird der Download sofort angehalten, so dass erst gar keine Bedrohungen auf Ihren Computer gelangen.

6.2.2. Erkennungen durch Search-Shield

Wenn das Internet mit aktiviertem ***Search-Shield*** durchsucht wird, werden alle angezeigten Suchergebnisse der bekanntesten Suchmaschinen (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg und SlashDot*) auf gefährliche oder verdächtige Links hin untersucht. Da Link Scanner 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 ist sicher (*dieses Symbol wird nicht bei sicheren Suchergebnissen von Yahoo! JP angezeigt*).

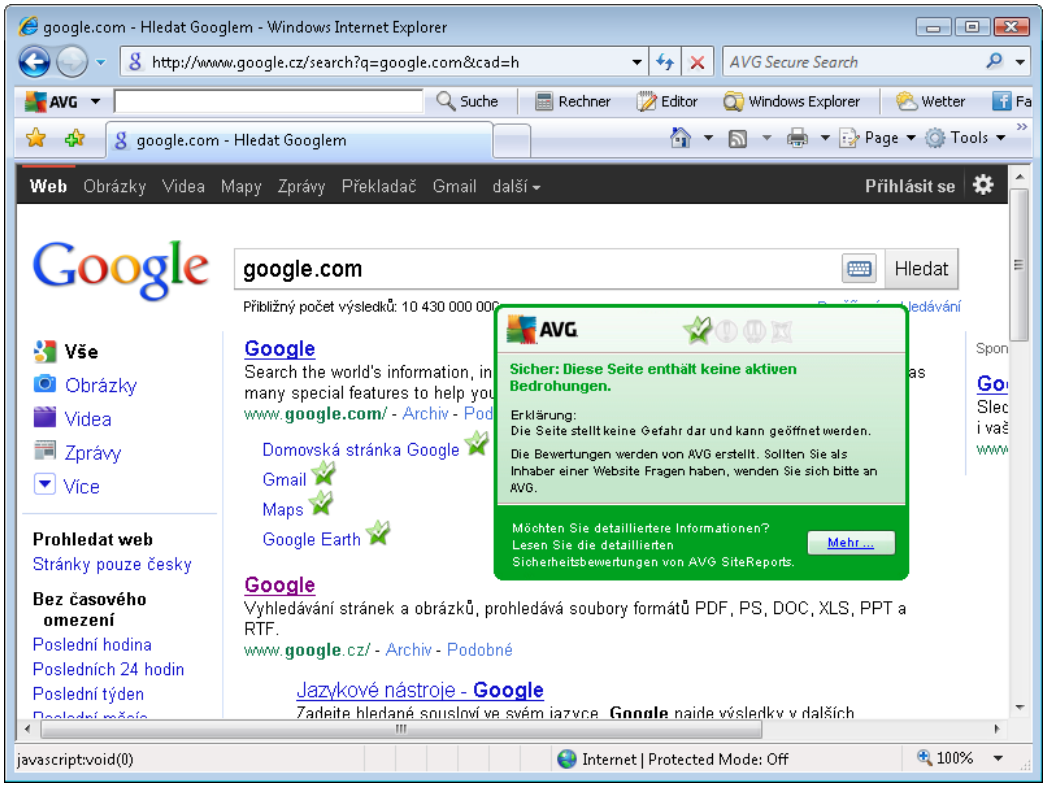
 Die verlinkte Seite enthält keine Bedrohungen, wird aber als verdächtig eingestuft (*die Herkunft/der Zweck der Seite ist fragwürdig, weshalb von Online-Einkäufen abgeraten wird usw.*).

 Die verlinkte Seite stellt momentan kein Sicherheitsrisiko dar, kann aber Links zu eindeutig gefährlichen Seiten oder verdächtigen Code enthalten.

 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.

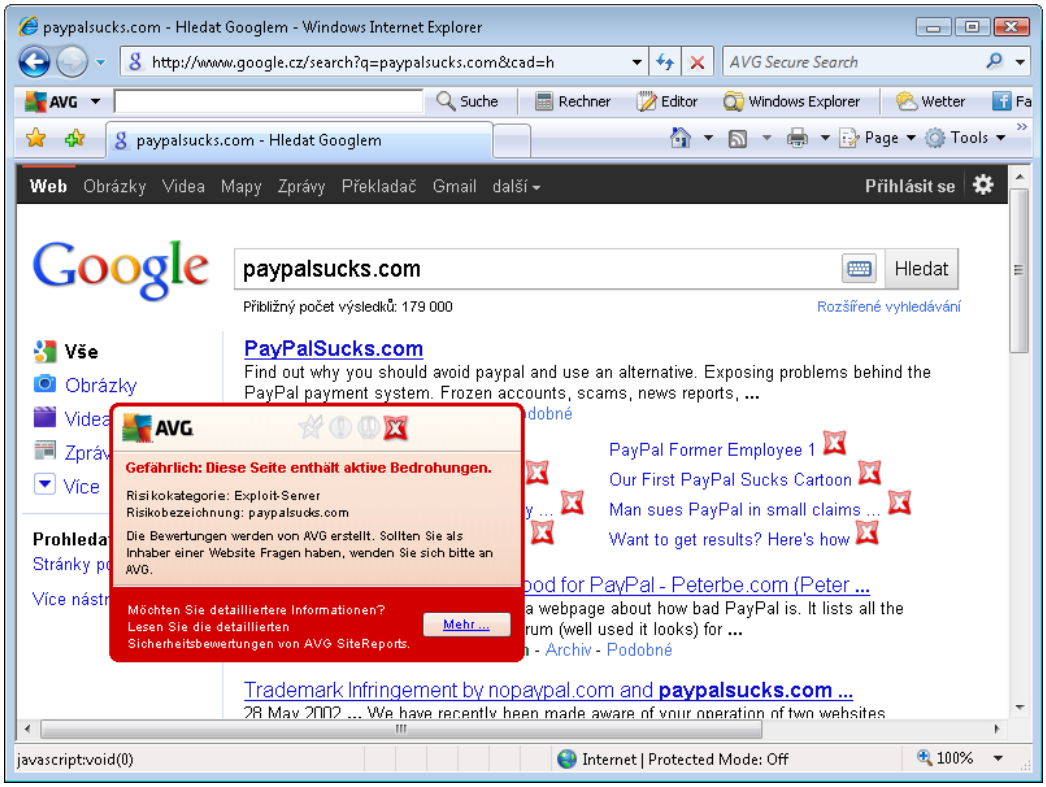
Wenn Sie mit der Maus über ein bestimmtes Bewertungssymbol fahren, werden Details zu dem entsprechenden Link angezeigt. Zu den Informationen gehören Details über die Art der Gefahr (*sofern vorhanden*):



6.2.3. Erkennungen durch 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 Link Scanner Ihren Browser davon ab, die Seite zu öffnen.

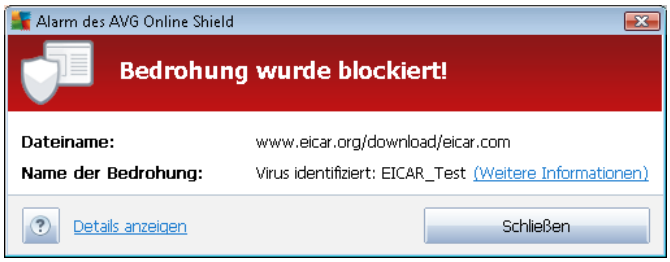
Wenn Sie in Ihrem Webbrowser auf eine gefährliche Website stoßen, werden Sie von Link Scanner mit einem Fenster gewarnt, das in etwa wie folgt aussieht:



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

6.2.4. Erkennungen durch Online Shield

Online 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:

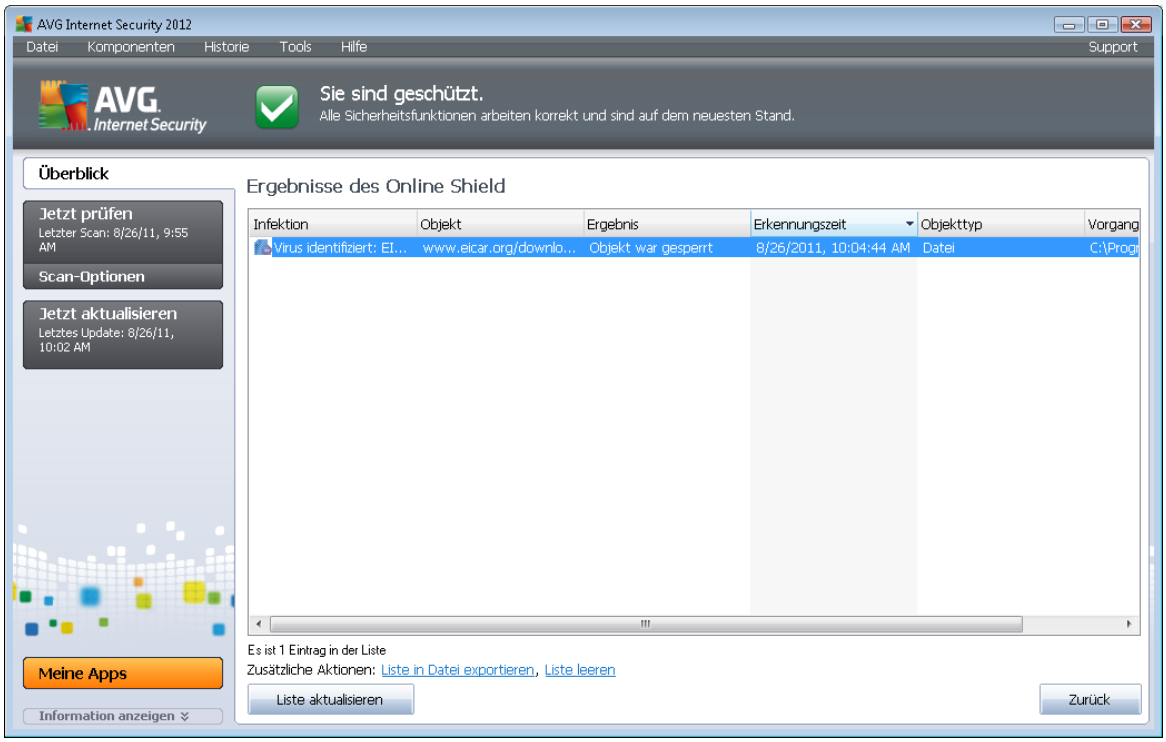


In diesem Warndialog finden Sie Informationen zu der Datei, die als infiziert erkannt wurde (*Dateiname*), den Namen der erkannten Bedrohung (*Name der Bedrohung*) und einen Link zur Virenenzyklopädie, wo Sie weitere Informationen zur erkannten Infektion finden (*falls bekannt*). Der Dialog enthält folgende Schaltflächen:

- ***Details anzeigen*** – Klicken Sie auf ***Details anzeigen***, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess anzuzeigen, der beim Erkennen der Infektion ausgeführt wurde.

- ***Schließen*** – Klicken Sie auf diese Schaltfläche, um den Warndialog zu schließen.

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

Schaltflächen

- ***Liste aktualisieren*** – aktualisiert die Liste der von ***Online Shield***
- ***Zurück*** – Hiermit kehren Sie zum Hauptdialog von AVG *(Komponentenübersicht)*

6.3. eMail-Schutz

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 Benutzer 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.

Die Komponente ***eMail-Schutz*** scannt jede eMail-Nachricht, die Sie senden oder empfangen. Wenn in einer eMail ein Virus erkannt wird, wird sie sofort in die Virenquarantäne verschoben. Die Komponente kann auch bestimmte Arten von eMail-Anhängen filtern und einen Zertifizierungstext zu infektionsfreien Nachrichten hinzufügen. Der ***eMail-Schutz*** vereint zwei Hauptfunktionen:

- eMail-Scanner
- Anti-Spam

6.3.1. eMail-Scanner

Der ***Personal eMail-Scanner*** prüft eingehende und ausgehende eMails automatisch. Sie können ihn für eMail-Clients verwenden, die über kein eigenes Plugin in AVG verfügen (*kann aber auch zum Scannen von eMails für eMail-Clients verwendet werden, die von AVG mit einem bestimmten Plugin unterstützt werden, z. B. Microsoft Outlook und The Bat*). Der eMail-Scanner ist hauptsächlich für die Verwendung mit Anwendungen wie Outlook Express, Mozilla, Incredimail usw. vorgesehen.

Während der Installation von 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 Quarantäne 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).

eMail-Scanner ist nicht für Serverplattformen vorgesehen!

6.3.2. Anti-Spam

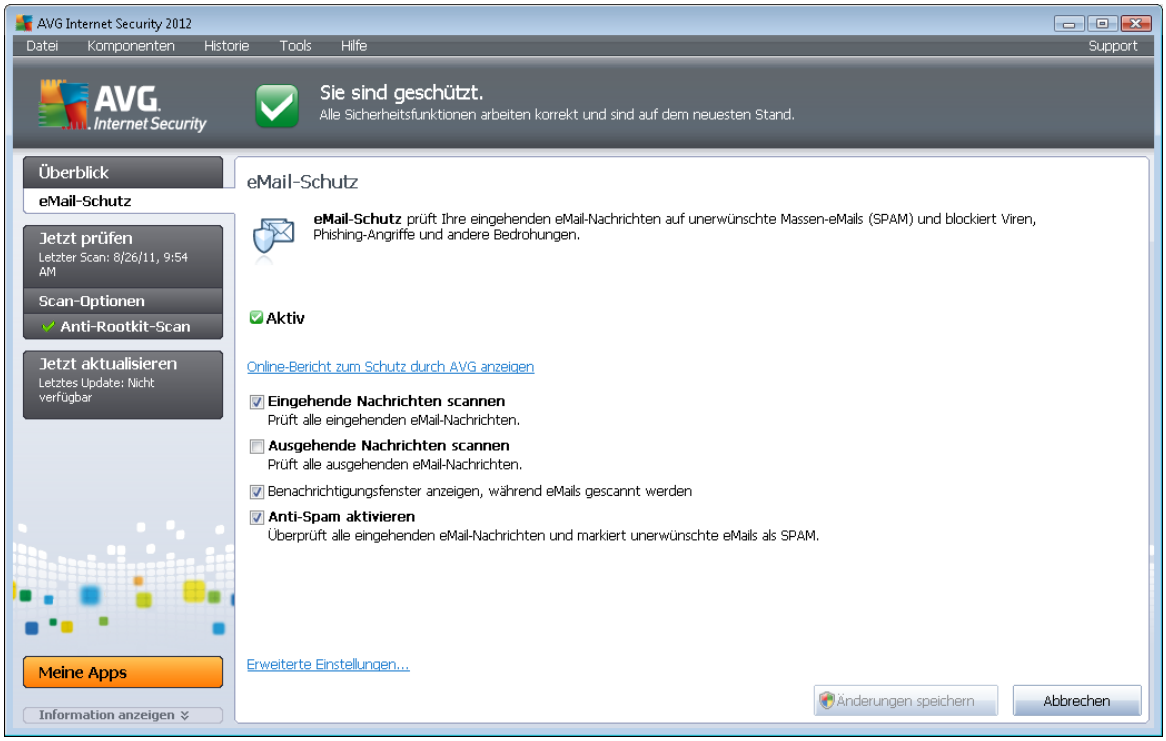
Wie funktioniert Anti-Spam?

Anti-Spam überprüft alle eingehenden eMails und markiert unerwünschte Nachrichten als Spam. ***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. ***Anti-Spam*** verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit optimalen Schutz vor unerwünschten eMail-Nachrichten. ***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.

Was ist 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.

6.3.3. Benutzeroberfläche des eMail-Schutzes



Der Dialog der Komponente ***eMail-Schutz*** enthält eine kurze Funktionsbeschreibung der Komponente und Informationen über den aktuellen Status *(Aktiv).* Verwenden Sie den Link ***Online-Bericht über den Schutz durch AVG anzeigen***, um detaillierte Statistiken zu den Aktivitäten und Erkennungen von **AVG Internet Security 2012** auf einer gesonderten Seite der Website von AVG (http://www.avg.com/de/) anzuzeigen.

Basiseinstellungen für den eMail-Schutz

Im Dialog ***eMail-Schutz*** können Sie zudem einige grundlegende Optionen der Komponentenfunktionen bearbeiten:

- ***Eingehende Nachrichten scannen*** *(standardmäßig aktiviert)* – Aktivieren Sie diesen Eintrag, damit alle in Ihrem Konto eingehenden eMails auf Viren überprüft werden.
- ***Ausgehende Nachrichten scannen*** *(standardmäßig deaktiviert)* – Aktivieren Sie diesen Eintrag, damit alle von Ihrem Konto ausgehenden eMails auf Viren überprüft werden.
- ***Benachrichtigungsfenster anzeigen, während eMails gescannt werden*** *(standardmäßig aktiviert)* – Aktivieren Sie diesen Eintrag, wenn Sie beim Scannen Ihrer eMails über den Benachrichtigungsdialog, der über dem AVG-Symbol im Infobereich angezeigt wird, benachrichtigt werden möchten.
- ***Anti-Spam*** aktivieren *(standardmäßig aktiviert)* – Aktivieren Sie diesen Eintrag, um anzugeben, ob Sie Ihre eingehenden eMails nach unerwünschten Junk-eMails filtern

möchten.

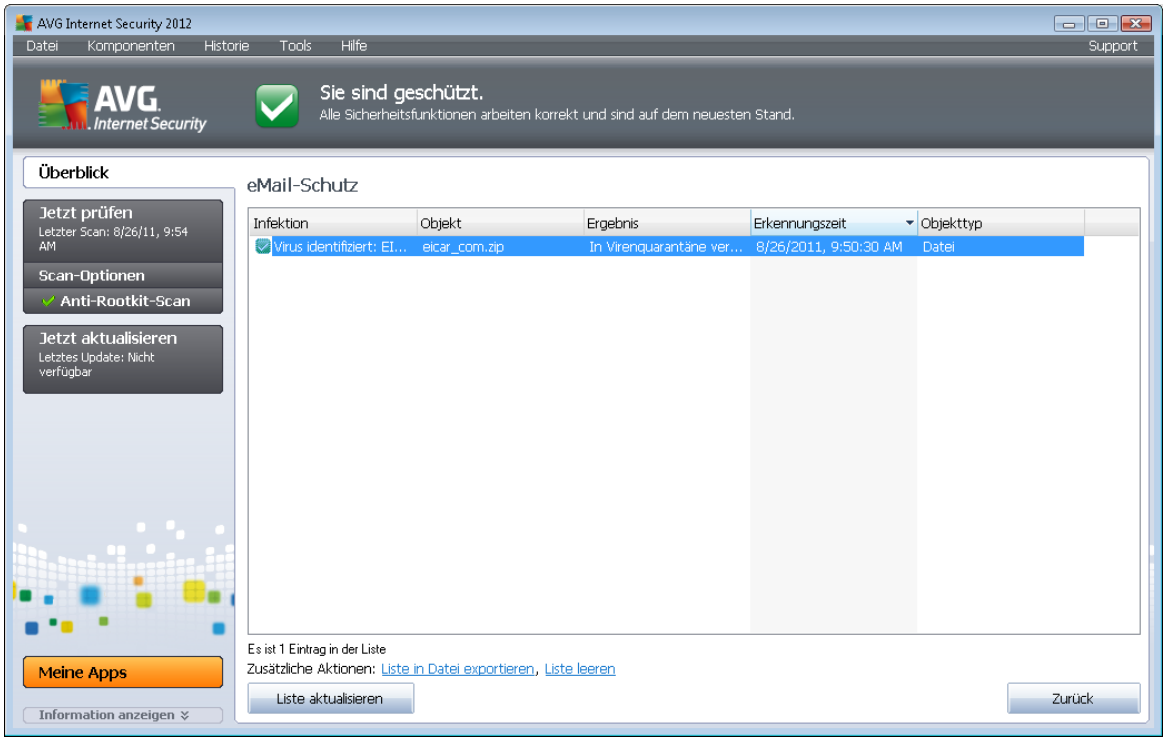
Alle Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie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

Schaltflächen

Im Dialog ***eMail-Schutz*** 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 kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*) zurück.

6.3.4. Erkennungen durch den eMail-Schutz



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-Schutz 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*** – Führt Sie zum zuvor angezeigten Dialog

6.4. Firewall

Die Firewall ist ein System, das Richtlinien für die Zugangskontrolle zwischen mehreren Netzwerken durch das Blockieren und Zulassen von Datenverkehr durchsetzt. Die Firewall verfügt über Regelsätze, die das interne Netzwerk vor Angriffen von außen *(normalerweise aus dem Internet)* schützen und die Kommunikation an jedem einzelnen Netzwerkport 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 vor Angriffen, die von internen Benutzern anderer Computer im Netzwerk ausgehen.

Computer, die nicht durch die Firewall geschützt sind, werden zu einem leichten Ziel für Computer-Hacker und Datendiebe.

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.*

6.4.1. Firewall-Richtlinien

In **AVG Internet Security 2012** kontrolliert die ***Firewall*** den Datenverkehr an jedem Netzwerkport Ihres Computers. Abhängig von den definierten Regeln wertet die ***Firewall*** Anwendungen aus, die entweder auf Ihrem Computer ausgeführt werden *(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.

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
- Automatischer Profilwechsel beim Herstellen einer Verbindung zu wechselnden Netzwerken oder bei Verwendung verschiedener Netzwerkadapter

6.4.2. 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*** – Dies 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*** – Dies 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*** – Mithilfe von benutzerdefinierten Profilen können Sie auch den automatischen Profilwechsel nutzen; dies kann insbesondere dann hilfreich sein, wenn Sie häufig Verbindungen mit wechselnden Netzwerken herstellen *(beispielsweise mit einem Notebook).* Benutzerdefinierte Profile werden nach der Installation von **AVG Internet Security 2012** automatisch erstellt und erfüllen individuelle Bedürfnisse an Firewall-Richtlinien. Die folgenden benutzerdefinierten Profile stehen zur Verfügung:

    - ***Direkt mit dem Internet verbunden*** – Geeignet für alle gängigen Heimcomputer oder Notebooks, die ohne zusätzlichen Schutz direkt mit dem Internet verbunden sind. Diese Option wird auch empfohlen, wenn Sie mit Ihrem Notebook mit verschiedenen unbekannten und möglicherweise unsicheren Netzwerken eine Verbindung herstellen (*z. B. im Internetcafé, Hotelzimmer usw.*).Die striktesten Firewall-Regeln dieses Profils gewährleisten, dass Computer dieser Kategorie ausreichend geschützt sind.

    - ***Computer in Domäne*** – Geeignet für Computer in einem lokalen Netzwerk, normalerweise an Schulen oder in einem Unternehmen. Hierbei wird angenommen, dass das Netzwerk professionell verwaltet und durch zusätzliche Maßnahmen geschützt wird. Die Sicherheitsstufe kann in diesem Fall niedriger sein als in den zuvor erwähnten Konfigurationen und muss den Zugriff auf gemeinsame Ordner, Festplatten usw. gewährleisten.

    - ***Heim- oder Büronetzwerk*** – Geeignet für Computer in einem kleinen Netzwerk, normalerweise Zu Hause oder in einem kleinen Unternehmen. Diese Art von Netzwerk verfügt über keinen „zentralen Administrator“ und besteht nur aus einer kleinen Anzahl von Computern, die miteinander verbunden sind und häufig Drucker, Scanner oder ähnliche Geräte gemeinsam nutzen. Die Firewall-Regeln müssen diese Konfiguration berücksichtigen.

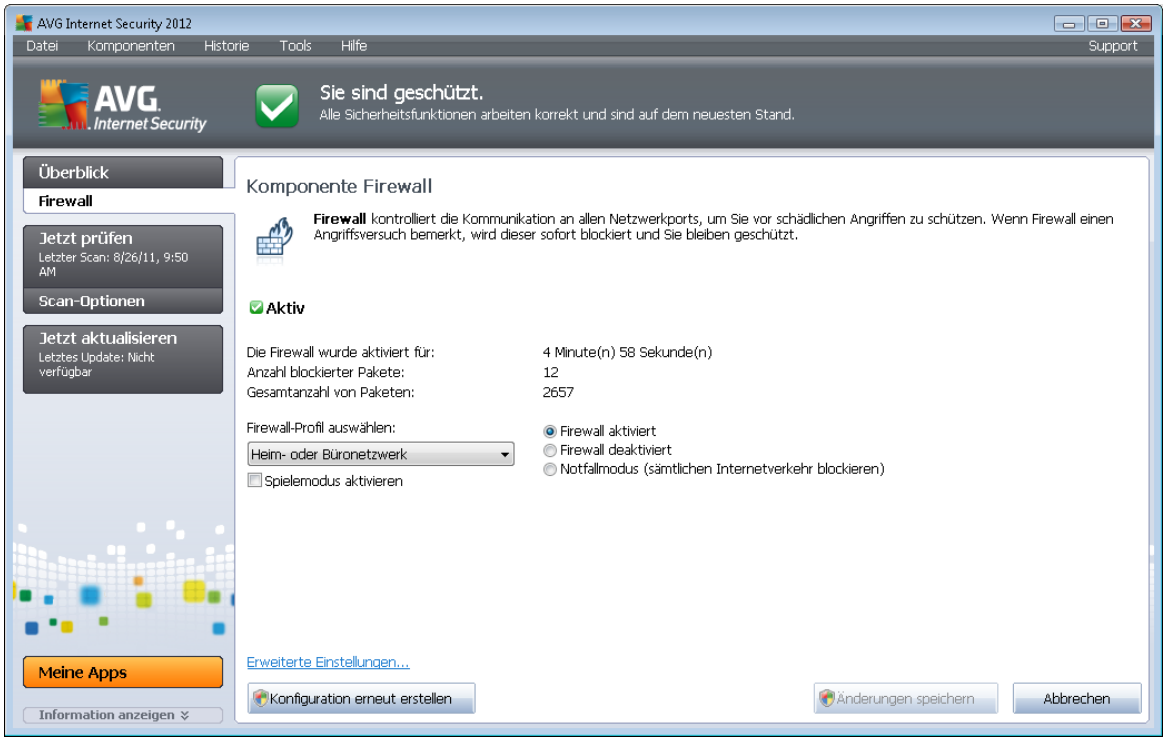
Profilwechsel

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.

6.4.3. Benutzeroberfläche der Firewall



Der Hauptdialog ***Komponente Firewall*** enthält einige grundlegende Informationen zur Funktion der Komponente, zu ihrem Status *(Aktiv)*sowie eine kurze Übersicht über die statistischen Daten der Komponente:

- ***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

Basiseinstellungen der Firewall

- ***Firewall-Profil auswählen*** – Wählen Sie aus dem Dropdown-Menü eines der definierten Profile aus (*für eine detaillierte Beschreibung jedes Profils und seine empfohlene Verwendung siehe Kapitel Firewall-Profile*)
- ***Spielmodus aktivieren*** – Aktivieren Sie diese Option, um zu gewährleisten, dass beim Ausführen von Vollbildanwendungen (*Spiele, Präsentationen, Filme usw.*) die Firewall keine Dialoge anzeigt, mit denen Sie darum gebeten werden, Kommunikation mit unbekannten

Anwendungen zu erlauben 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. ***Hinweis:*** Wenn der Spielmodus aktiviert ist, werden alle geplanten Aufgaben (Scans, Updates) bis zum Schließen der Anwendung aufgeschoben.

- In diesem Abschnitt der Basiseinstellungen können Sie auch zwischen drei alternativen Optionen auswählen, die den aktuellen Status der Komponente Firewall definieren:
  - ***Firewall aktiviert*** *(standardmäßig 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 aus, 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 Internet Security 2012 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

- ***Konfiguration erneut erstellen*** – Klicken Sie auf diese Schaltfläche, um die aktuelle Firewall-Konfiguration zu überschreiben und die Standardkonfiguration anhand einer automatischen Erkennung wiederherzustellen.
- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen.
- ***Abbrechen*** – Mit dieser Schaltfläche kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*) zurück.

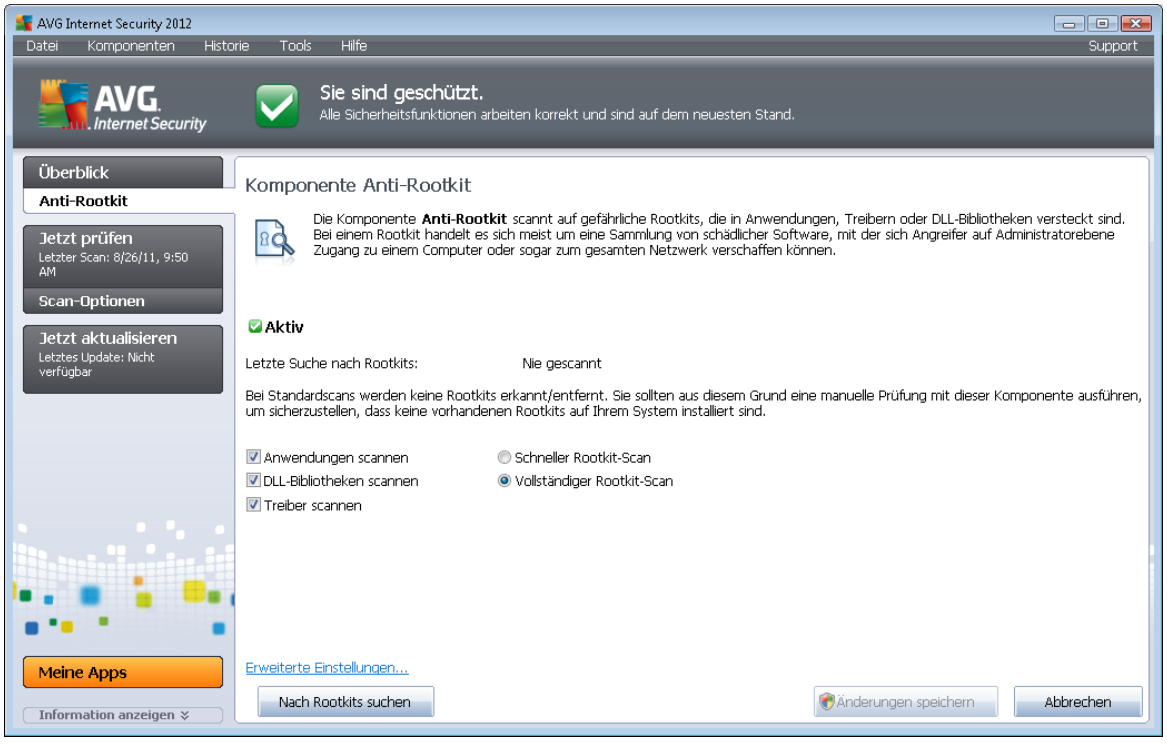
6.5. Anti-Rootkit

Anti-Rootkit ist ein spezielles Tool zur Erkennung und effektiven Entfernung von gefährlichen Rootkits, wie z. B. Programmen und Technologien, die das Vorhandensein von schädlicher Software auf Ihrem Computer verschleiern können. ***Anti-Rootkit*** erkennt Rootkits auf Basis eines vordefinierten Regelsatzes. Bitte beachten Sie, dass alle Rootkits erkannt werden *(nicht nur die infizierten)*. Wenn ***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.

Was ist ein Rootkit?

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.

6.5.1. Benutzeroberfläche von Anti-Rootkit



Der Dialog ***Anti-Rootkit*** enthält eine kurze Beschreibung der Funktionen der Komponente, gibt Auskunft über den aktuellen Status der Komponente *(Aktiv)* und enthält Informationen über den Zeitpunkt des letzten mit ***Anti-Rootkit*** durchgeführten Tests (***Letzte Suche nach Rootkits***). Der Dialog ***Anti-Rootkit*** enthält außerdem den Link Tools/Erweiterte Einstellungen. Klicken Sie auf diesen Link, um erweiterte Konfigurationen für die Komponente ***Anti-Rootkit*** vorzunehmen.

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.

Basiseinstellungen von Anti-Rootkit

Im unteren Teil des Dialogs können Sie einige grundlegende Funktionen für das Scannen nach vorhandenen Rootkits einstellen. 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*** – Prüft alle laufenden Prozesse, geladenen Treiber und den Systemordner (*typischerweise C:\Windows*).
- ***Vollständiger Rootkit-Scan*** – Prüft alle laufenden Prozesse, geladenen Treiber, den Systemordner (*typischerweise C:\Windows*) und zusätzlich alle lokalen Festplatten (*einschließlich Flash-Laufwerke, aber keine Disketten-/CD-Laufwerke*).

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 zum standardmäßigen Hauptdialog von AVG (*Komponentenübersicht*) zurückkehren.
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zum standardmäßigen Hauptdialog von AVG (*Komponentenübersicht*) zurückkehren, ohne Ihre Änderungen zu speichern.

6.6. System-Tools

System-Tools sind Tools, die eine detaillierte Zusammenfassung der Umgebung von **AVG Internet Security 2012** und des Betriebssystems zur Verfügung stellen. Die Komponente zeigt eine Übersicht über:

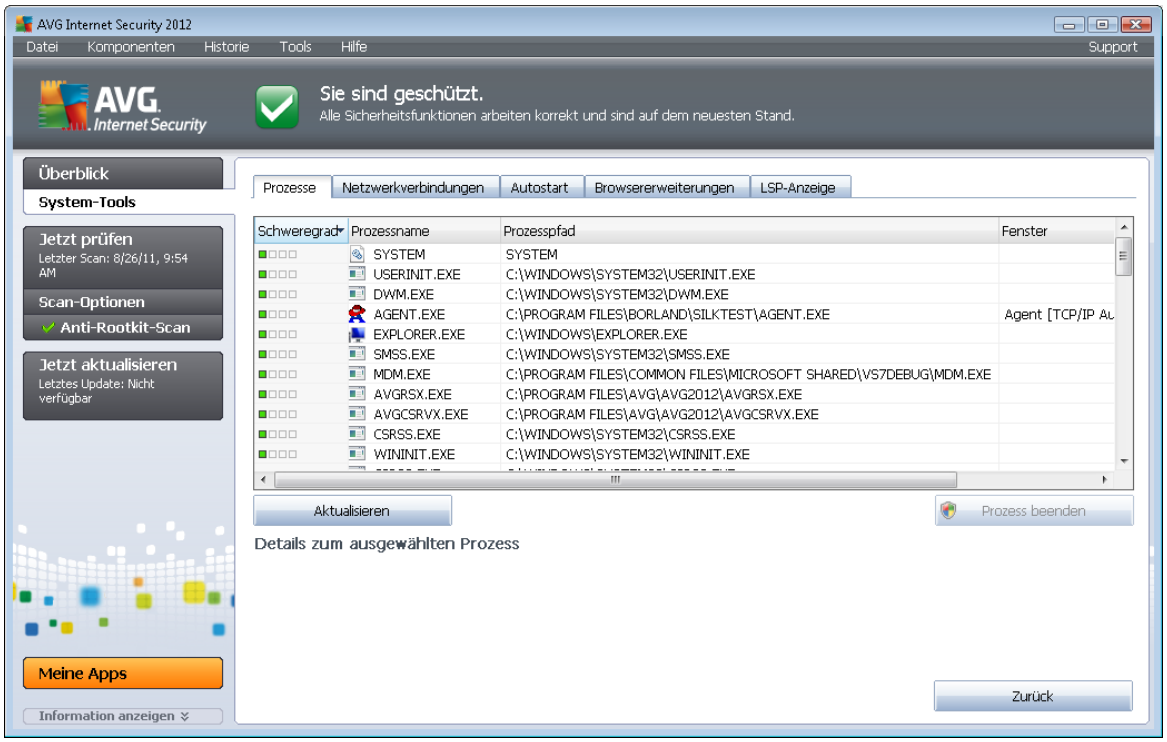
- Prozesse – Eine Liste der Prozesse (*d. h. ausgeführte Anwendungen*), die auf Ihrem Computer gerade aktiv sind
- Netzwerkverbindungen – Eine Liste der momentan aktiven Verbindungen
- Autostart – Eine Liste aller Anwendungen, die während des Starts von Windows ausgeführt werden

- 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!

6.6.1. 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 des ausgeführten Prozesses

- ***Fenster*** – Zeigt den Namen des Anwendungsfensters an, falls verfügbar

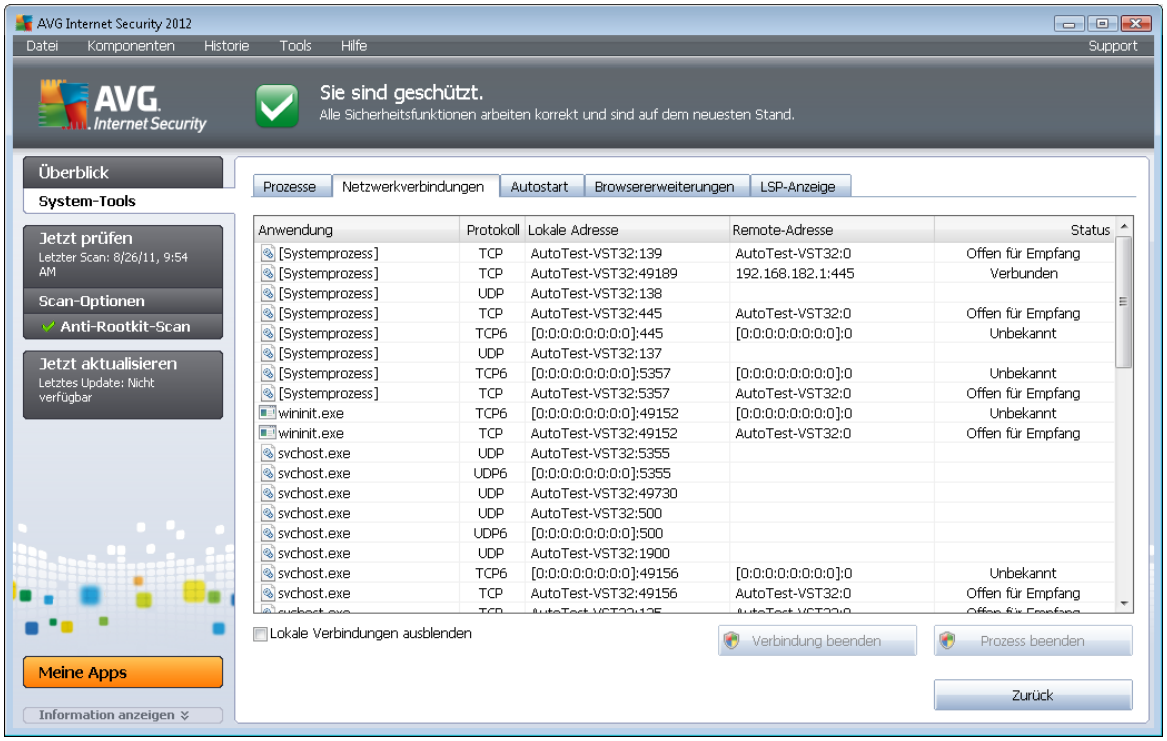
- ***PID*** – Die Prozesskennung ist eine eindeutige Windows-interne Prozesskennung

Schaltflächen

Auf dem Reiter ***Prozesse*** 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 kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht)* zurück.

6.6.2. 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 (*mit Ausnahme von Windows 2000, bei dem keine Informationen zur Verfügung stehen*)
- ***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***.

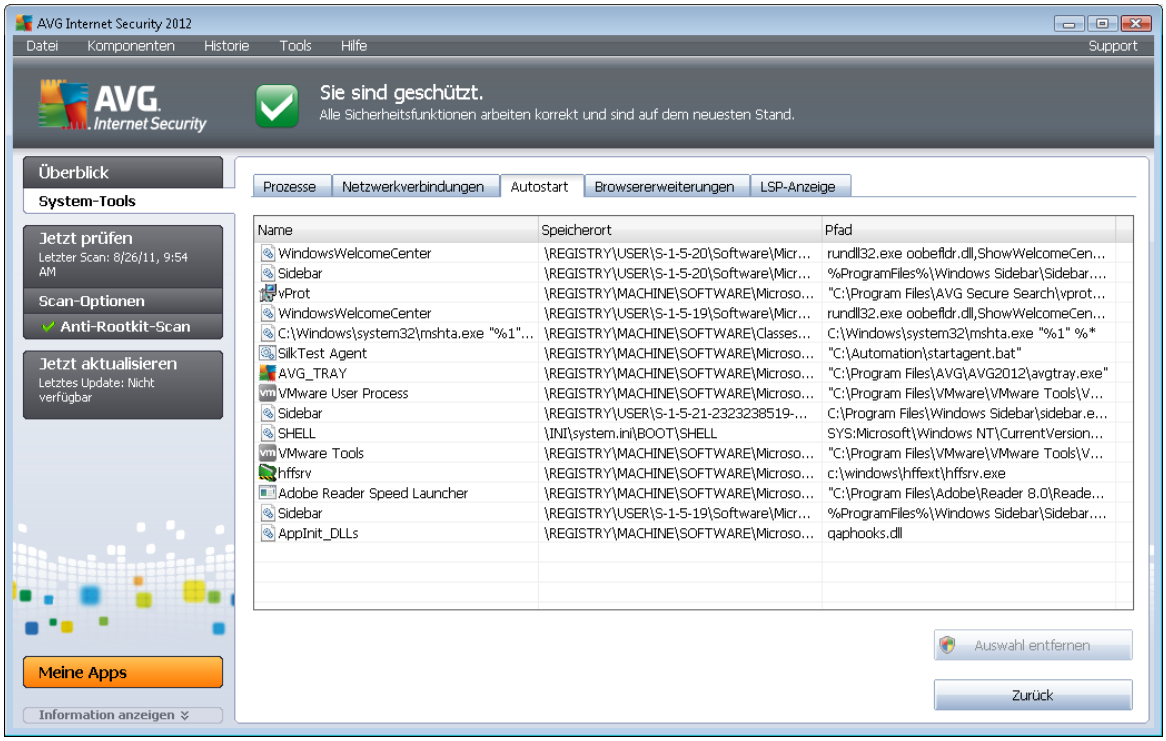
Schaltflächen

Auf dem Reiter ***Netzwerkverbindungen*** stehen folgende Schaltflächen zur Verfügung:

- ***Verbindung beenden*** – schließt eine oder mehrere in der Liste ausgewählte Verbindungen
- ***Prozess beenden*** – Schließt eine oder mehrere Anwendungen, die mit in der Liste ausgewählten Verbindungen verknüpft sind
- ***Zurück*** – Hiermit kehren Sie zum Hauptdialog 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!

6.6.3. 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.

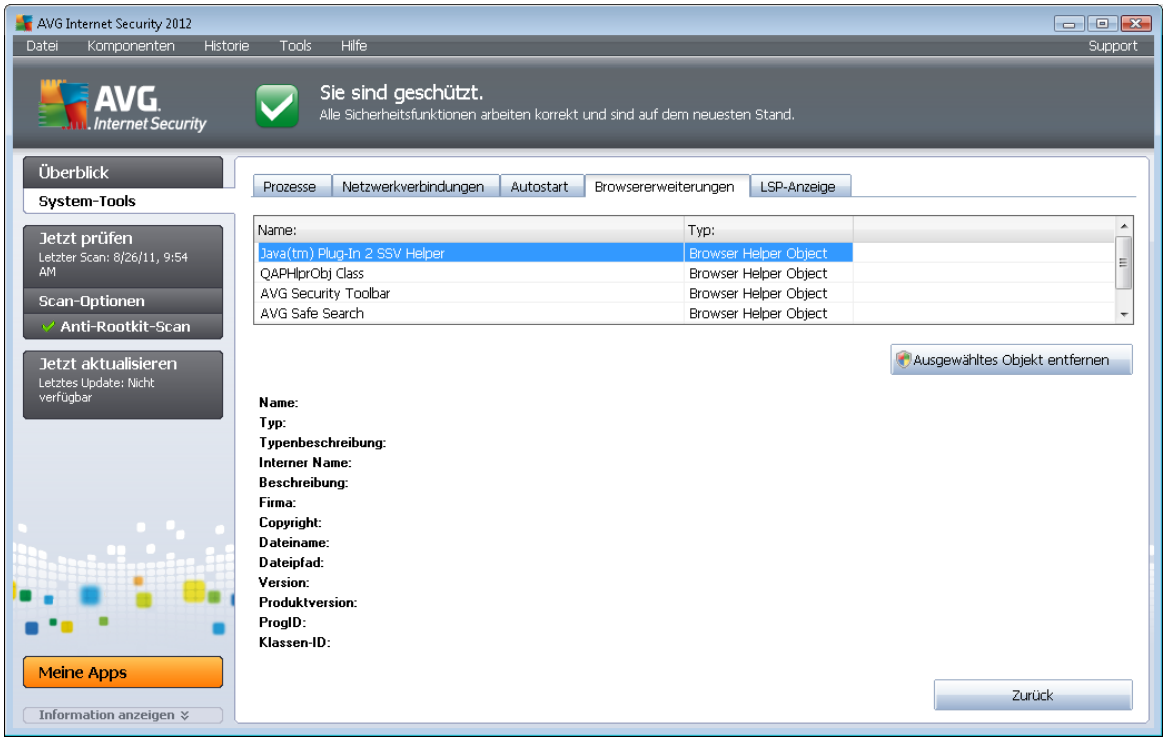
Schaltflächen

Auf dem Reiter ***Autostart*** stehen folgende Schaltflächen zur Verfügung:

- ***Auswahl entfernen*** – Klicken Sie auf diese Schaltfläche, um einen oder mehrere ausgewählte Einträge zu entfernen.
- ***Zurück*** – Mit dieser Schaltfläche kehren Sie zum Hauptdialog von AVG *(Komponentenübersicht) zurück*.

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

6.6.4. 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.

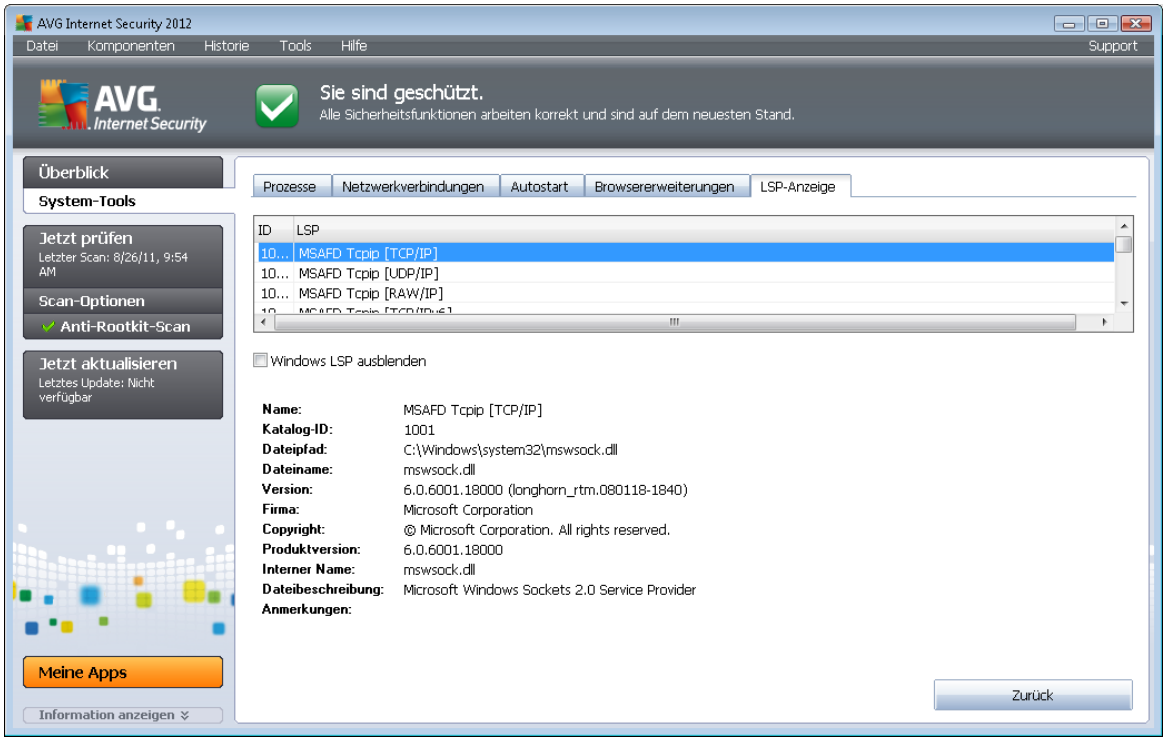
Schaltflächen

Auf dem Reiter ***Browsererweiterungen*** stehen folgende 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 kehren Sie zum Hauptdialog von AVG *(Komponentenübersicht) zurück*.

6.6.5. 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.

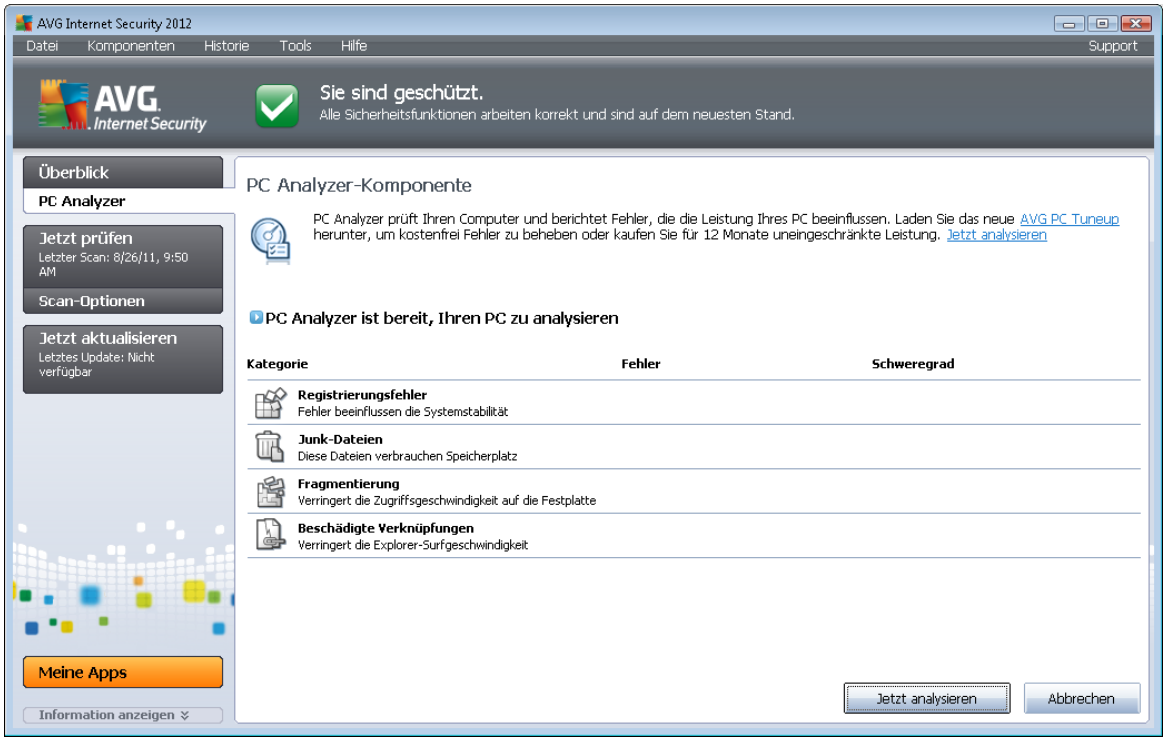
Schaltflächen

Auf dem Reiter ***LSP-Anzeige*** stehen folgende Schaltflächen zur Verfügung:

- ***Windows LSP ausblenden*** – Deaktivieren Sie das Kontrollkästchen Windows-LSP ausblenden, um den Windows-LSP in die Liste aufzunehmen.
- ***Zurück*** – Mit dieser Schaltfläche kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*) zurück.

6.7. PC Analyzer

Die Komponente ***PC Analyzer*** überprüft Ihren Computer auf Systemprobleme und zeigt anschließend in einer Übersicht mögliche Gründe für die beeinträchtigte Leistung Ihres Computers an. Auf der Benutzeroberfläche der Komponente wird ein Diagramm angezeigt, das in die folgenden vier Kategorien eingeteilt ist: Registrierungsfehler, Junk-Dateien, Fragmentierung und beschädigte Verknüpfungen:



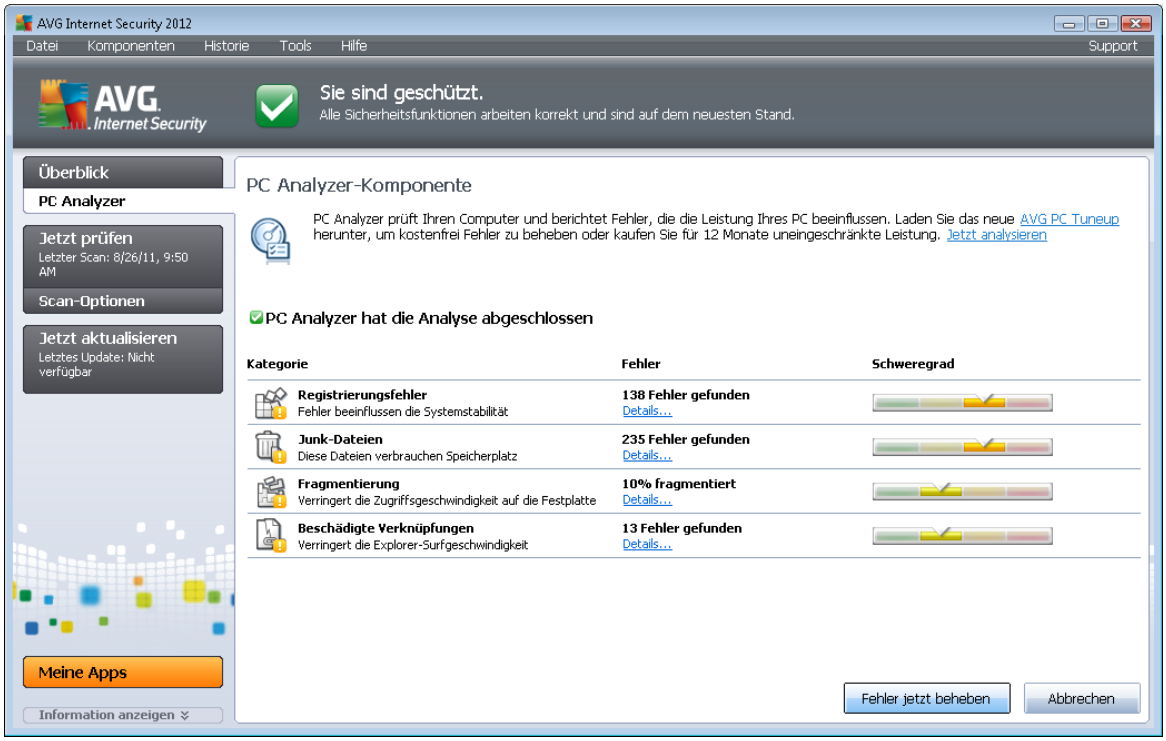
- ***Registrierungsfehler***: Gibt die Anzahl der Fehler in der Windows-Registrierung an. Da die Fehlerbehebung der Registrierung spezifische Kenntnisse erfordert, wird die selbständige Reparatur der Registrierung nicht empfohlen.

- ***Junk-Dateien***: Gibt die Anzahl der Dateien an, die mit großer Wahrscheinlichkeit nicht benötigt werden. Dazu gehören typischerweise temporäre Dateien und Dateien, die sich im Papierkorb befinden.

- ***Fragmentierung***: Berechnet die Fragmentierung Ihrer Festplatte in Prozent. Mit Fragmentierung bezeichnet man die Speicherung von Datenbeständen, die nach einem langen Zeitraum über die gesamte Festplatte verteilt sind. Sie können dieses Problems mit einem Defragmentierungs-Tool beheben.

- ***Beschädigte Verknüpfungen***: Benachrichtigt Sie über Verknüpfungen, die nicht mehr funktionieren oder auf nicht vorhandene Speicherorte verweisen usw.

Klicken Sie auf ***Jetzt analysieren***, um eine Analyse Ihres Systems zu starten. Sie können den Analysefortschritt nachvollziehen und die Ergebnisse der Analyse direkt im Diagramm sehen:



In der Ergebnisübersicht werden die erkannten Systemprobleme (***Fehler***) in den entsprechenden, überprüften Kategorien aufgelistet. Die Ergebnisse der Analyse werden außerdem grafisch auf einer Achse in der Spalte ***Schweregrad*** angeordnet.

Schaltflächen

- ***Jetzt analysieren*** (*wird vor dem Start der Analyse angezeigt*) – Klicken Sie auf diese Schaltfläche, um eine sofortige Analyse Ihres Computer zu starten
- ***Fehler jetzt beheben***(*wird nach Abschluss der Analyse angezeigt*) – Klicken Sie auf diese Schaltfläche, um eine Seite der Website von AVG (http://www.avg.com/de/) aufzurufen, auf der Sie genaue und aktuelle Informationen zur Komponente ***PC Analyzer*** erhalten.
- ***Abbrechen*** – Klicken Sie auf diese Schaltfläche, um die Analyse abzubrechen oder um nach Abschluss der Analyse zum Hauptdialog von AVG (*Komponentenübersicht*) zurückzukehren.

6.8. Identity Protection

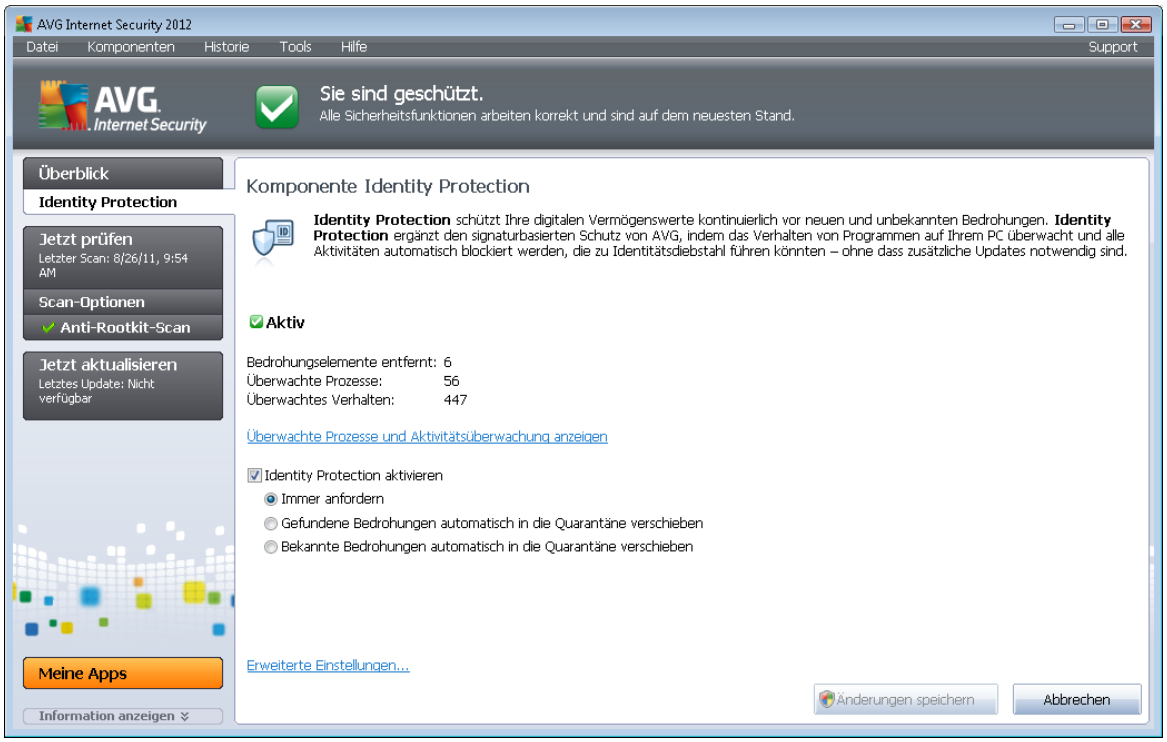
Identitätsschutz ist eine Anti-Malware-Komponente, die Sie mithilfe von Verhaltenstechnologien vor allen Arten von Malware schützt(*Spyware, Bots, Identitätsdiebstahl usw.*) und mit dem Zero-Day-Schutz vor neuen Viren bewahrt. ***Identitätsschutz*** ist darauf ausgerichtet, Identitätsdiebe daran zu hindern, Ihre Kennwörter, die Zugangsdaten zu Ihrem Bankkonto, Kreditkartennummern und andere persönliche und vertrauliche Daten mithilfe verschiedener schädlicher Software (*Malware*) von Ihrem PC zu stehlen. Es sorgt sicher, dass alle auf Ihrem Computer ausgeführten Programme ordnungsgemäß funktionieren. ***Identitätsschutz*** erkennt und blockiert kontinuierlich verdächtiges

Verhalten und schützt Ihren Computer vor neuer Malware.

Identitätsschutz gewährt Ihrem Computer Echtzeitschutz vor neuen und unbekannten Bedrohungen. Die Komponente überwacht alle *(auch versteckte)* Prozesse und mehr als 285 verschiedene Verhaltensmuster. Außerdem kann sie erkennen, wenn auf Ihrem Computer ein schädlicher Vorgang ausgeführt wird. Aus diesem Grund kann die Komponente Bedrohungen erkennen, noch bevor sie in der Virendatenbank beschrieben sind. Jedes Mal, wenn ein unbekannter Code auf Ihrem Computer auftritt, wird er sofort auf schädliches Verhalten überprüft und aufgezeichnet. Falls die Datei als schädlich erachtet wird, verschiebt ***Identitätsschutz*** den Code in die Virenquarantäne und macht alle Änderungen rückgängig, die im System durchgeführt wurden *(Codeeinschleusungen, Registrierungsänderungen, Öffnen von Ports usw.)*. Sie müssen keinen Scan starten, um geschützt zu sein. Diese Technologie ist sehr proaktiv, muss selten aktualisiert werden und ist immer aktiv.

Identitätsschutz ist ein ergänzender Schutz zu Anti-Virus. Es wird dringend empfohlen, beide Komponenten zu installieren, um Ihren Computer umfassend zu schützen.

6.8.1. Benutzeroberfläche des Identitätsschutzes



Der Dialog ***Identitätsschutz*** enthält eine kurze Beschreibung der Grundfunktionen der Komponente, ihren Status *(Aktiv)* sowie einige statistische Daten:

- ***Bedrohungselemente entfernt*** – 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

Nachfolgend finden Sie den Link Überwachte Prozesse und Aktivitätsüberwachung anzeigen, über den Sie zur Benutzeroberfläche der Komponente System-Tools geleitet werden und wo Sie eine detaillierte Übersicht über alle überwachten Prozesse finden.

Basiseinstellungen für den Identitätsschutz

Im unteren Bereich des Dialogs können Sie einige Grundfunktionen der Komponente bearbeiten:

- ***Identitätsschutz aktivieren*** – (*standardmäßig aktiviert*): Aktivieren 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:

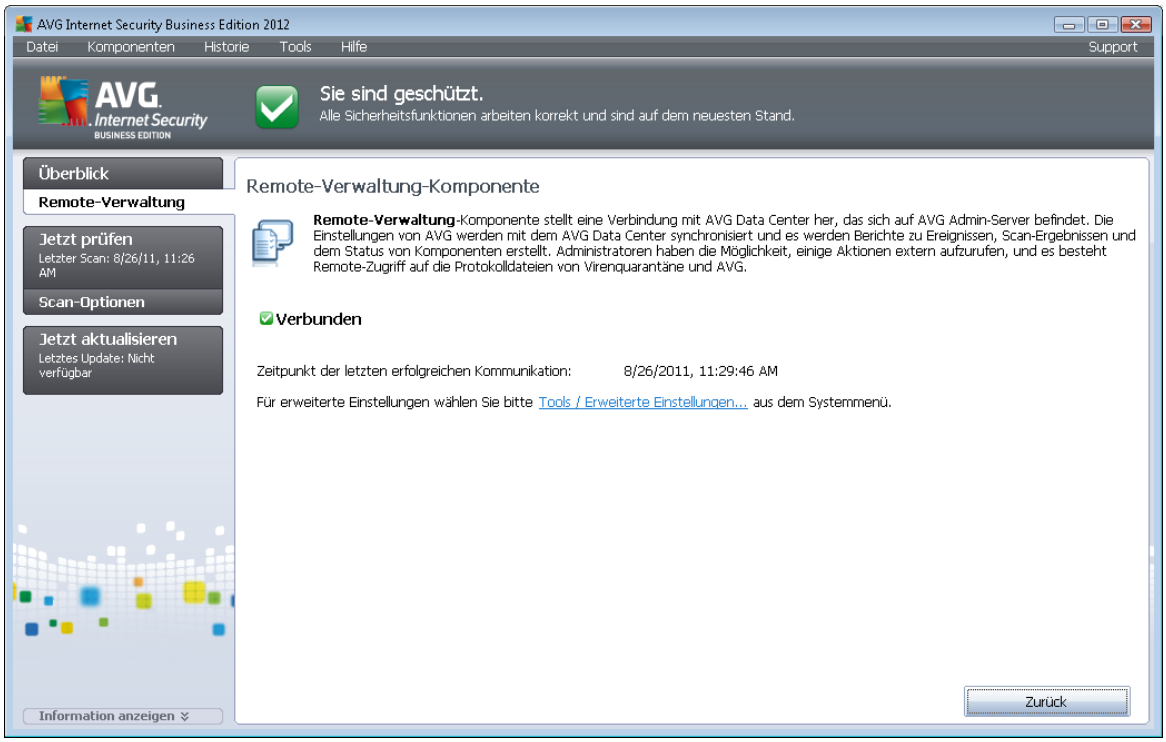
  - ***Immer anfordern*** – Wenn eine Anwendung als Malware erkannt wird, werden Sie gefragt, ob diese blockiert werden soll (*diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Einstellung nur dann zu ändern, wenn Sie einen guten Grund dafür haben*)
  - ***Gefundene Bedrohungen automatisch 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

Schaltflächen

Auf der Benutzeroberfläche von ***Identitätsschutz*** 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 kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*)

6.9. Remote-Verwaltung



Die Komponente ***Remote-Verwaltung*** wird nur auf der Benutzeroberfläche von **AVG Internet Security 2012** angezeigt, wenn Sie die Business Edition des Produkts installiert haben *(weitere Informationen über die für die Installation verwendete Lizenz finden Sie auf dem Reiter Version des Dialogs Informationen, der über den Systemmenüeintrag Support geöffnet werden kann)*. Im Dialog der Komponente ***Remote-Verwaltung*** wird angezeigt, ob die Komponente aktiv und mit dem Server verbunden ist. Alle Einstellungen der Komponente ***Remote-Verwaltung*** werden in den ***Erweiterten Einstellungen/Remote-Verwaltung*** vorgenommen.

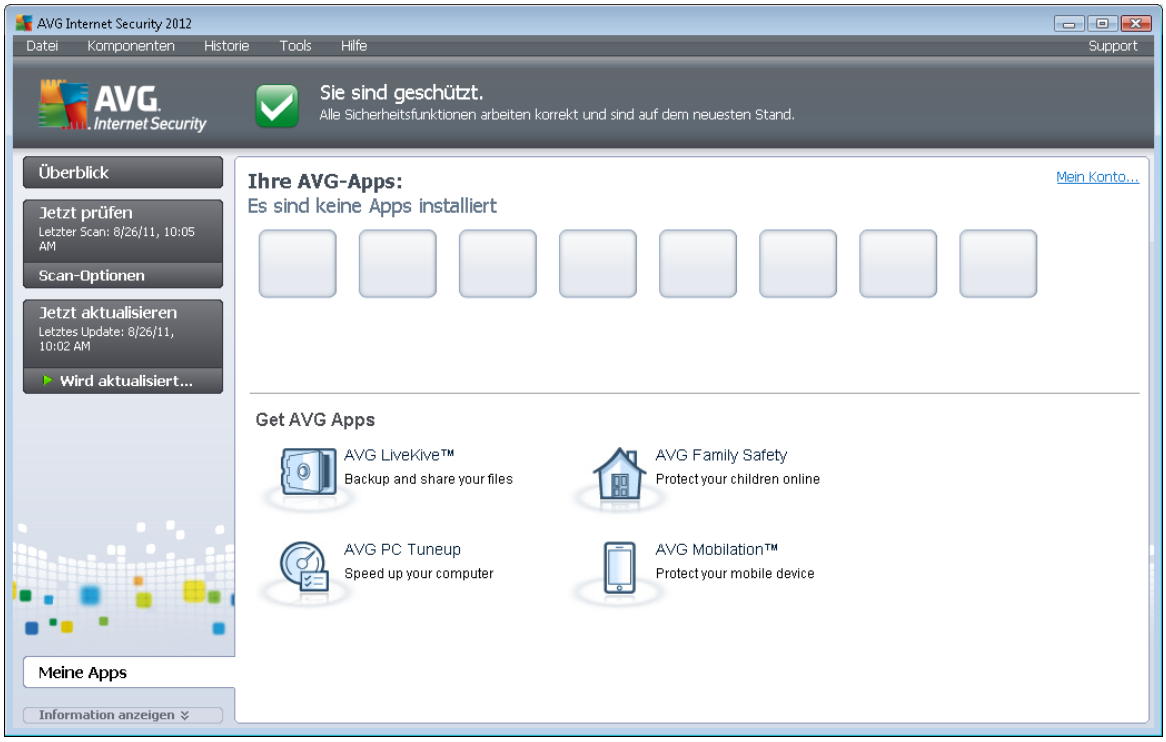
Eine genaue Beschreibung der Optionen und Funktionen der Komponente im System von AVG Remote-Verwaltung finden Sie in der Dokumentation speziell und ausschließlich zu diesem Thema. Diese Dokumentation kann von der AVG-Website (http://www.avg.com/de/)) im Bereich ***Support Center/Download/Dokumentation*** heruntergeladen werden.

Schaltflächen

- ***Abbrechen*** – Mit dieser Schaltfläche kehren Sie zum Hauptdialog von AVG (*Komponentenübersicht*) zurück.

7. Meine Apps

Jede der drei Anwendungen, LiveKive, Family Safety und PC Tuneup, ist als eigenständiges AVG-Produkt erhältlich und ein optionaler Teil Ihrer Installation von **AVG Internet Security 2012**. Im Dialog ***Ihre AVG-Apps*** *(verfügbar direkt im Hauptdialog von AVG über die Schaltfläche „Meine Apps“)* finden Sie eine Übersicht über alle bereits installierten Anwendungen sowie Anwendungen, die optional installiert werden können:



7.1. LiveKive

LiveKive ist für die Online-Datensicherung auf abgesicherten Servern vorgesehen. ***LiveKive*** sichert automatisch Ihre gesamten Dateien, Fotos und Musik an einem sicheren Ort und ermöglicht es Ihnen, diese mit Ihrer Familie und Ihren Freunden gemeinsam zu nutzen. Sie haben von allen internetfähigen Geräten, einschließlich iPhones und Android-Geräten, Zugriff auf diese. Zu den Funktionen von ***LiveKive*** gehören:

- Sicherheitsmaßnahme für den Fall, dass Ihr Computer und/oder Ihre Festplatte beschädigt werden
- Zugang zu Ihren Daten über ein beliebiges mit dem Internet verbundenes Gerät
- Einfache Organisation
- Gemeinsame Nutzung mit allen, die Sie dazu berechtigen

Weitere Informationen finden Sie auf der Website von AVG, auf der Sie auch die Komponente sofort herunterladen können. Alternativ können Sie auch den LiveKive-Link im Dialog Meine

***Apps* verwenden.**

7.2. Family Safety

Family Safety unterstützt Sie beim Schutz Ihrer Kinder vor unangemessenen Websites, Medieninhalten und Online-Suchergebnissen und bietet Ihnen Berichte zu ihren Online-Aktivitäten. Sie können für jedes Ihrer Kinder die angemessene Schutzstufe einstellen und sie einzeln über eindeutige Anmeldedaten überwachen.

Weitere Informationen finden Sie auf der Website von AVG, auf der Sie auch die Komponente sofort herunterladen können. Alternativ können Sie auch den Family Safety-Link im Dialog Meine Apps verwenden.

7.3. PC Tuneup

Die Anwendung ***PC Tuneup*** ist ein leistungsstarkes Tool zur detaillierten Systemanalyse und Optimierung der Geschwindigkeit und Gesamtleistung Ihres Computers. Zu den Funktionen von ***PC Tuneup*** gehören:

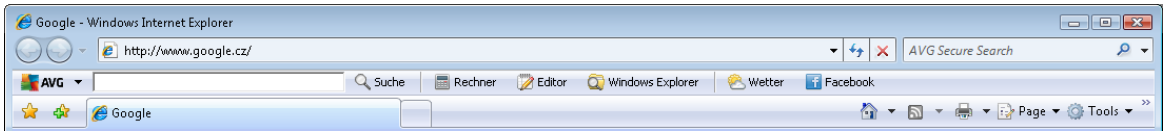
- Disk Cleaner – Entfernt Junk-Dateien, die den Computer verlangsamen.
- Disk Defrag – Defragmentiert Laufwerke und optimiert die Anordnung von Systemdateien.
- Registry Cleaner – Repariert Fehler in der Registrierung, um die PC-Stabilität zu verbessern.
- Registry Defrag – Komprimiert die Registrierung durch das Entfernen speicherintensiver Lücken.
- Disk Doctor – Findet defekte Sektoren, verlorene Cluster und Fehler in der Verzeichnisstruktur und repariert sie.
- Internet Optimizer – Passt die Standardeinstellungen an die jeweilige Internetverbindung an.
- Track Eraser – Entfernt die Historie der Computer- und Internetaktivitäten.
- Disk Wiper – Überschreibt freien Speicherplatz auf Festplatten, um die Wiederherstellung sensibler Daten zu vermeiden.
- File Shredder – Löscht ausgewählte Dateien von einer Festplatte oder einem USB-Stick permanent, so dass sie nicht wiederhergestellt werden können.
- File Recovery – Stellt versehentlich gelöschte Dateien von Festplatten, USB-Sticks oder Kameras wieder her.
- Duplicate File Finder – Findet und entfernt doppelte Dateien, die den Festplattenspeicher verschwenden.
- Services Manager – Deaktiviert unnötige Dienste, die den Computer verlangsamen.

- Startup Manager – Ermöglicht die Verwaltung von Programmen, die beim Starten von Windows automatisch gestartet werden.
- Uninstall Manager – Deinstalliert nicht mehr benötigte Softwareprogramme.
- Tweak Manager – Ermöglicht dem Benutzer, versteckte Windows-Einstellungen anzupassen.
- Task Manager – Führt alle laufenden Prozesse, Dienste und gesperrten Dateien auf.
- Disk Explorer – Zeigt an, welche Dateien den meisten Speicherplatz auf dem Computer einnehmen.
- Systeminformationen – Enthält detaillierte Informationen über die installierte Hardware und Software.

Weitere Informationen finden Sie auf der Website von AVG, auf der Sie auch die Komponente sofort herunterladen können. Alternativ können Sie auch den PC Tuneup-Link im Dialog Meine Apps verwenden.

8. AVG Security Toolbar

Das Tool ***AVG Security Toolbar*** arbeitet eng mit der Komponente Link Scanner zusammen und bietet Ihnen maximalen Schutz beim Surfen im Internet. Bei **AVG Internet Security 2012** ist die Installation der ***AVG Security Toolbar*** optional; beim Installationsvorgang wurden Sie gefragt, ob diese Komponente installiert werden soll. ***AVG Security Toolbar*** ist direkt in Ihrem Internetbrowser verfügbar. Derzeit werden die Internetbrowser Internet Explorer (*Version 6.0 und höher*) und/oder Mozilla Firefox (*Version 3.0 und höher*) unterstützt. Es werden keine anderen Browser unterstützt *(Wenn Sie einen alternativen Browser verwenden, z. B. Avant, kann unerwartetes Verhalten auftreten)*.



AVG Security Toolbar enthält die folgenden Elemente:

- ***AVG-Logo*** mit dem Dropdown-Menü:
  - ***AVG Secure Search verwenden*** – Ermöglicht Ihnen die direkte Suche über die ***AVG Security Toolbar*** mit der ***AVG Secure Search***-Engine. Alle Suchergebnisse werden kontinuierlich vom Dienst Search-Shield überprüft, so dass Sie sich online absolut sicher fühlen können.
  - ***Aktuelle Bedrohungsstufe*** – Öffnet die Webseite des Virenlabors mit einer grafischen Darstellung der aktuellen Bedrohungslage im Internet.
  - ***AVG Threat Labs*** – Öffnet die Seite ***SiteReport*** auf der Website von AVG(http://www.avg.com/de/), auf der Sie bestimmte Bedrohungen nach Namen suchen können und weitere Informationen zu den einzelnen Bedrohungen erhalten.
  - ***Toolbar-Hilfe*** – Öffnet die Onlinehilfe, in der Sie Informationen über alle Funktionen der ***AVG Security Toolbar*** erhalten.
  - ***Produkt-Feedback einsenden*** – Öffnet eine Webseite, auf der Sie ein Formular mit Ihrer Meinung zur ***AVG Security Toolbar***ausfüllen können.
  - ***Über...*** – Öffnet ein neues Fenster mit Informationen über die aktuell installierten Version der ***AVG Security Toolbar***.
- ***Suchfeld*** – Führen Sie Suchanfragen im Internet geschützt und bequem mit der ***AVG Security Toolbar*** durch, denn alle angezeigten Suchergebnisse sind hundertprozentig sicher. Geben Sie den Suchbegriff oder Ausdruck in das Suchfeld ein, und klicken Sie auf die Schaltfläche ***Suche*** *(oder drücken Sie die Eingabetaste)*. Alle Suchergebnisse werden kontinuierlich vom Dienst Search-Shield *(in der Komponente Link Scanner) überprüft*.
- Verknüpfungsschaltflächen für den Schnellzugriff auf diese Anwendungen: ***Rechner***, ***Notepad***, ***Windows Explorer***
- ***Wetter*** – Diese Schaltfläche öffnet einen neuen Dialog mit Informationen zum aktuellen

Wetter an Ihrem Standort und der Wettervorhersage für die nächsten zwei Tage. Diese Informationen werden regelmäßig alle 3–6 Stunden aktualisiert. In diesem Dialog können Sie den gewünschten Standort manuell ändern und festlegen, ob die Temperatur in Celsius oder Fahrenheit angezeigt werden soll.

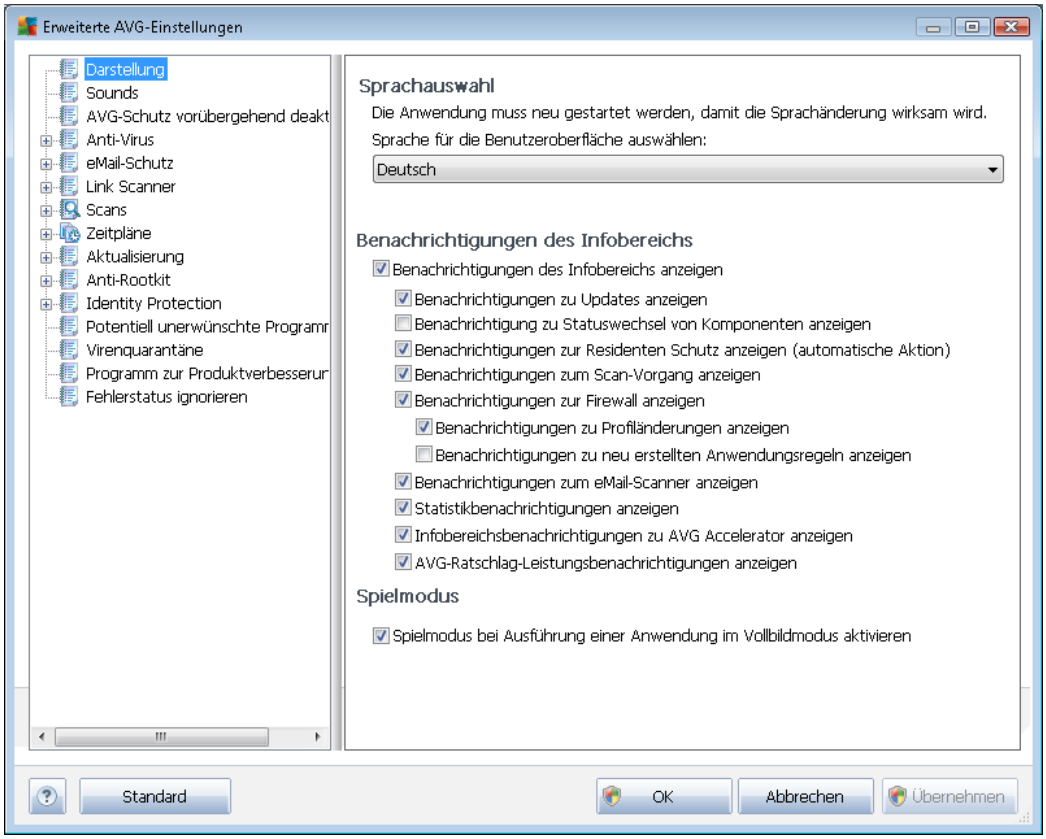
- ***Facebook*** – Mit dieser Schaltfläche können Sie sich mit dem sozialen Netzwerk Facebook direkt über die ***AVG Security Toolbar*** verbinden. *Verhalten.*

9. Erweiterte Einstellungen von AVG

Der Dialog zur erweiterten Konfiguration von **AVG Internet Security 2012** wird in einem neuen Fenster mit dem Namen ***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 **AVG Internet Security 2012**-Benutzeroberfläche und beinhaltet einige grundlegende Optionen für das Verhalten der Anwendung:

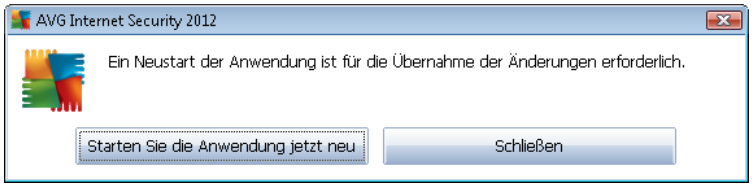


Sprachauswahl

Im Abschnitt ***Sprachauswahl*** können Sie Ihre gewünschte Sprache aus dem Dropdown-Menü auswählen. Die ausgewählte Sprache wird dann für die gesamte **AVG Internet Security 2012**-Benutzeroberfläche verwendet. Im Dropdown-Menü sind nur die Sprachen verfügbar, die zuvor beim Installationsvorgang ausgewählt wurden (*siehe Kapitel Benutzerdefinierte Optionen*) sowie die Benutzersprache Englisch (*wird standardmäßig installiert*). Um die Umstellung von **AVG Internet Security 2012** auf eine andere Sprache abzuschließen, müssen Sie die Anwendung neu starten.

Gehen Sie wie folgt vor:

- Wählen Sie im Dropdown-Menü die gewünschte Sprache der Anwendung aus
- Bestätigen Sie Ihre Auswahl durch Klicken auf die Schaltfläche ***Übernehmen*** *(untere rechte Ecke des Dialogs)*
- Klicken Sie zum Bestätigen auf die Schaltfläche ***OK***
- Ein neuer Dialog wird angezeigt, der Sie darüber informiert, dass Sie **AVG Internet Security 2012**
- Klicken Sie auf die Schaltfläche ***Starten Sie die Anwendung jetzt neu***, um den Programmneustart zu bestätigen, und warten Sie eine Sekunde, damit die Sprache übernommen wird:



Benachrichtigungen des Infobereichs

In diesem Bereich können Sie die Anzeige von Benachrichtigungen des Infobereichs über den Status der Anwendung **AVG Internet Security 2012**deaktivieren. In der Standardeinstellung werden die Benachrichtigungen des Infobereichs angezeigt. Es wird dringend empfohlen, diese Konfiguration beizubehalten. Systembenachrichtigungen geben beispielsweise Auskunft über den Start von Scan- oder Update-Vorgängen oder über die Veränderung des Status einer Komponente von **AVG Internet Security 2012**. Sie sollten diese Benachrichtigungen unbedingt beachten!

Wenn Sie dennoch nicht auf diese Art informiert werden möchten oder möchten, dass nur bestimmte Benachrichtigungen *(zu einer bestimmten Komponente von AVG Internet Security 2012)* angezeigt werden, können Sie dies durch Aktivieren/Deaktivieren der folgenden Optionen festlegen:

- ***Benachrichtigungen des Infobereichs anzeigen*** *(standardmäßig aktiviert)* – Standardmäßig werden alle Benachrichtigungen angezeigt. Heben Sie die Markierung dieses Eintrags auf, um die Anzeige aller Systembenachrichtigungen zu deaktivieren. Wenn diese Funktion aktiviert ist, können Sie auswählen, welche Benachrichtigungen angezeigt werden sollen:
  - ***Benachrichtigungen des Infobereichs zu Updates*** anzeigen*(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zum Start, Fortschritt und Abschluss des Updatevorgangs von **AVG Internet Security 2012** angezeigt werden sollen.
  - ***Benachrichtigungen zum Statuswechsel von Komponenten anzeigen*** *(standardmäßig deaktiviert)* – Legen Sie fest, ob Informationen zur Aktivität/Inaktivität von Komponenten angezeigt werden sollen und ob Sie über möglicherweise auftretende Probleme informiert werden möchten. Die Option zur Benachrichtigung

über den fehlerhaften Status einer Komponente entspricht der Informationsfunktion des Infobereichsymbols, das auf Probleme aufmerksam macht, die im Zusammenhang mit Komponenten von **AVG Internet Security 2012** auftreten.

- ***Benachrichtigungen des Infobereichs zu Residenter Schutzanzeigen (automatische Aktion)*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zum Speichern, Kopieren und Öffnen von Dateien angezeigt werden sollen (*diese Konfiguration zeigt nur an, ob die Option Automatisches Heilen des Residenten Schutzes aktiviert ist*).

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

- ***Benachrichtigungen des Infobereichs zur Firewall anzeigen*** *(standardmäßig aktiviert)* – 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. Dieser Eintrag beinhaltet zwei weitere Auswahloptionen *(für eine detaillierte Erläuterung dieser Optionen siehe Kapitel Firewall in diesem Dokument)*:

  - ***Benachrichtigungen zu Profiländerungen anzeigen*** *(standardmäßig aktiviert)* – Benachrichtigt Sie über automatische Änderungen der Firewall-Profile.

  - ***Benachrichtigungen zu neu erstellten Anwendungsregeln anzeigen*** *(standardmäßig deaktiviert)* – Benachrichtigt Sie über die automatische Erstellung von Firewall-Regeln für neue Anwendungen basierend auf einer Liste der sicheren Anwendungen.

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

- ***Statistische Benachrichtigungen anzeigen*** *(standardmäßig aktiviert)* – Lassen Sie diese Option aktiviert, damit regelmäßige statistische Prüfbenachrichtigungen im Infobereich angezeigt werden.

- ***Benachrichtigungen des Infobereichs zum AVG Accelerator anzeigen*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zu den Aktivitäten von ***AVG Accelerator*** angezeigt werden sollen. ***AVG Accelerator*** ermöglicht eine gleichmäßigere Online-Videowiedergabe und vereinfacht das zusätzliche Herunterladen.

- ***AVG Advice-Leistungsbenachrichtigungen anzeigen*** *(standardmäßig aktiviert)* – ***AVG Advice*** überwacht die Leistung der unterstützten Internetbrowser *(Internet Explorer, Chrome, Firefox, Opera und Safari)* und benachrichtigt Sie, sobald Ihr Browser mehr als den empfohlenen Arbeitsspeicher verwendet. In solch einem Fall nimmt die Leistung Ihres Computers deutlich ab, und es wird empfohlen, Ihren Internetbrowser neu zu starten, um die Prozesse zu beschleunigen. Lassen Sie den Eintrag ***AVG Advice-Leistungsbenachrichtigungen anzeigen*** aktiviert, um

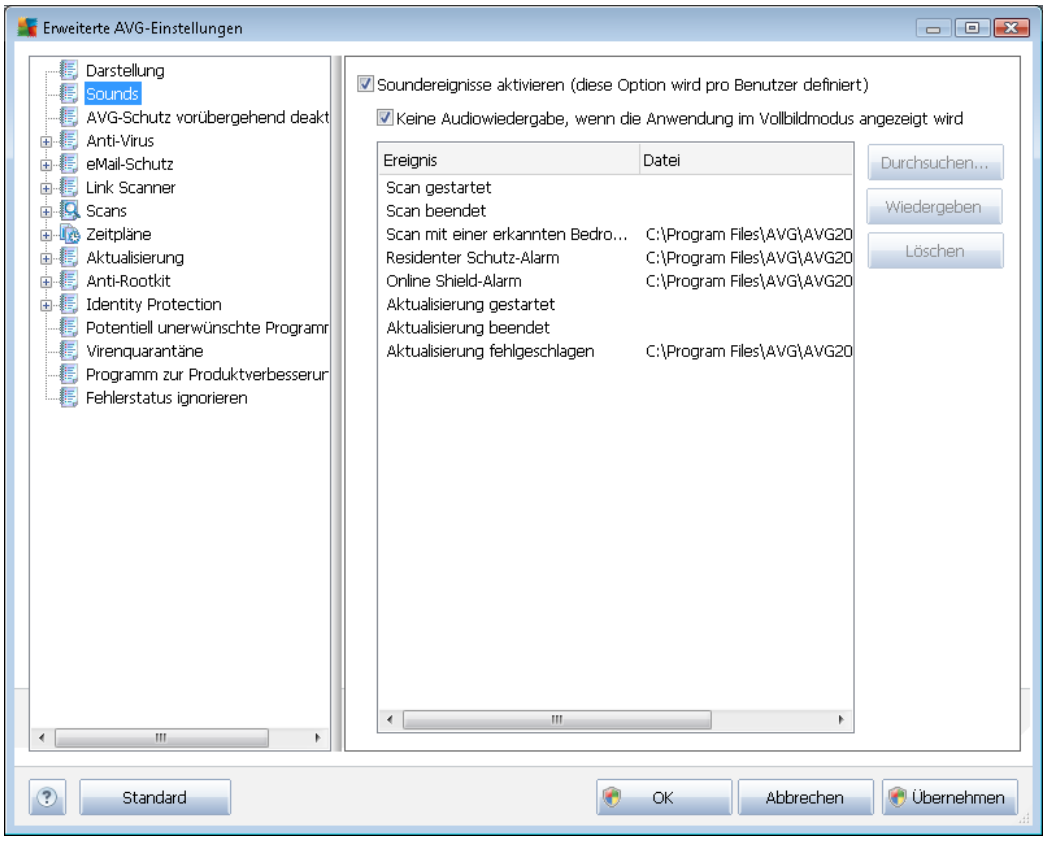
Benachrichtigungen zu erhalten.

Spielmodus

Diese Funktion von AVG wurde für Anwendungen mit Vollbildmodus entwickelt, bei denen Informationsfenster von AVG (*z. B. beim Start eines geplanten Scans*) stören könnten (*eine Anwendung könnte minimiert oder ihre Grafiken könnten beschädigt werden*). 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 Internet Security 2012** per Soundbenachrichtigung informiert werden möchten:



Diese Einstellungen gelten nur für das aktuelle Benutzerkonto. Das heißt, jeder Benutzer auf dem Computer kann eigene Soundeinstellungen vornehmen. Wenn Sie per Soundbenachrichtigung informiert werden möchten, behalten Sie die Aktivierung der Option ***Soundereignisse aktivieren*** bei (*die Option ist standardmäßig aktiviert*), um die Liste aller relevanten Aktionen zu aktivieren. Sie können zudem die Option ***Keine Sounds wiedergeben, wenn eine Vollbildanwendung aktiv ist*** aktivieren, um die Soundbenachrichtigungen in Situationen zu unterdrücken, in denen sie störend sein könnten *(siehe auch Abschnitt „Spielmodus“ im Kapitel Erweiterte Einstellungen/Darstellung in dieser Dokumentation)*.

Schaltflächen

- ***Durchsuchen*** – Nachdem Sie das entsprechende Ereignis aus der Liste ausgewählt haben, verwenden Sie die Schaltfläche ***Durchsuchen***, um Ihr Laufwerk nach der gewünschten Sounddatei zu durchsuchen, die Sie dem Ereignis zuweisen möchten. *(Bitte beachten Sie, dass momentan nur *.wav Sounddateien unterstützt werden.)*

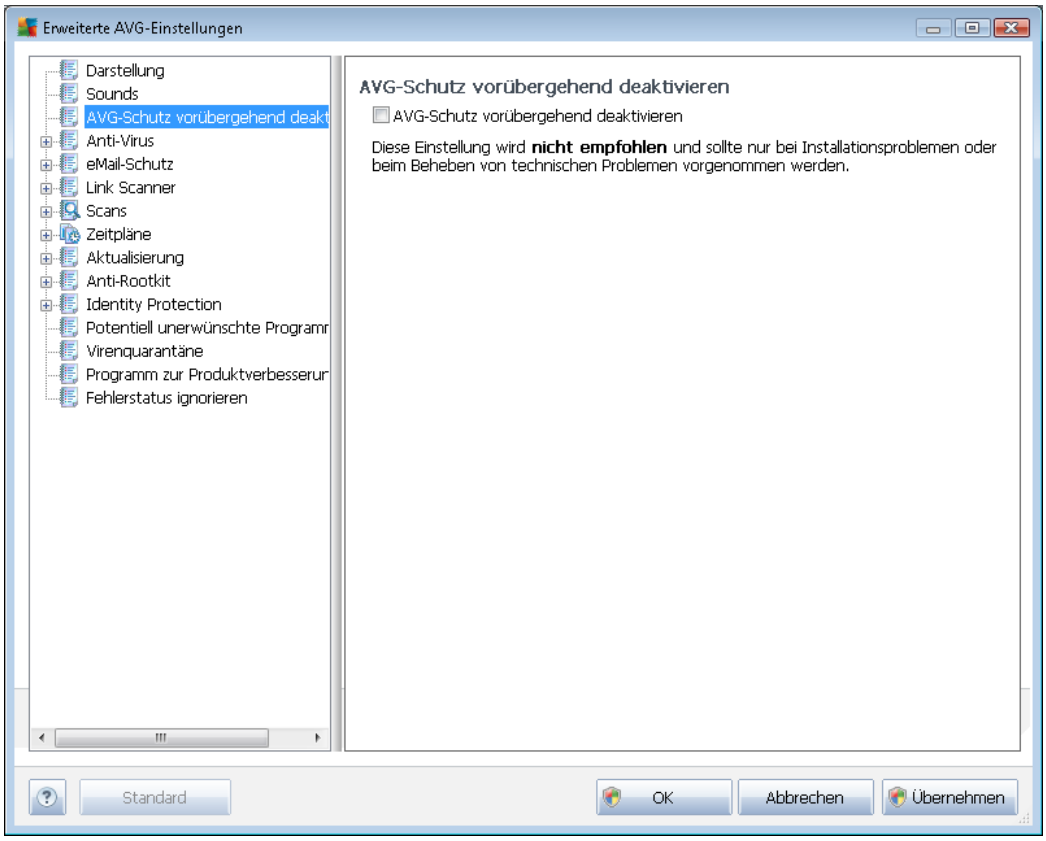
- ***Wiedergeben*** – Um den ausgewählten Sound anzuhören, markieren Sie das Ereignis in der Liste, und klicken Sie auf die Schaltfläche ***Wiedergeben***.

- ***Löschen*** – Verwenden Sie die Schaltfläche ***Löschen***, um den einem Ereignis zugewiesenen Sound zu entfernen.

9.3. AVG-Schutz vorübergehend deaktivieren

Im Dialog ***AVG-Schutz vorübergehend deaktivieren*** können Sie alle Schutzfunktionen von **AVG Internet Security 2012** gleichzeitig deaktivieren.

Verwenden Sie diese Option nur, wenn es unbedingt erforderlich ist.

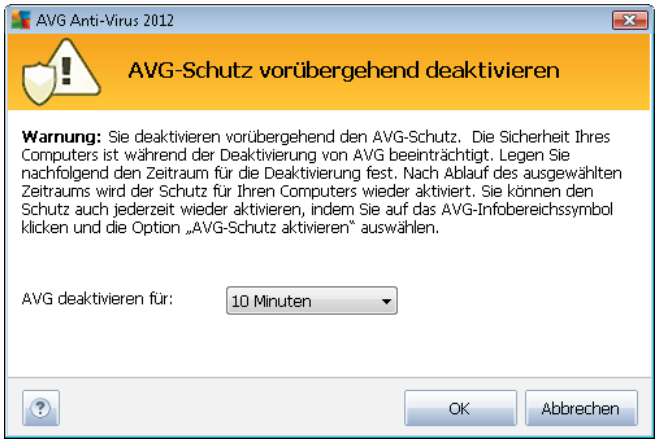


In der Regel ***müssen Sie*** **AVG Internet Security 2012** nicht deaktivieren, bevor Sie neue Software oder Treiber installieren, auch wenn das Installationsprogramm oder der Software-Assistent darauf hinweist, dass laufende Programme und Anwendungen beendet werden sollten, um den Installationsvorgang ohne Unterbrechungen abzuschließen. Wenn Sie während der Installation jedoch ein Problem feststellen, deaktivieren Sie zuerst den Residenten Schutz (*(Residenten Schutz aktivieren*) . Wenn Sie **AVG Internet Security 2012** vorübergehend deaktivieren müssen, sollten Sie es so bald wie möglich wieder aktivieren. Ihr Computer ist Bedrohungen ausgesetzt, wenn Sie bei deaktivierter Virenschutz-Software mit dem Internet oder einem Netzwerk verbunden sind.

So können Sie den AVG-Schutz deaktivieren

- Aktivieren Sie das Kontrollkästchen ***AVG-Schutz vorübergehend deaktivieren***, und bestätigen Sie Ihre Auswahl mit der Schaltfläche ***Übernehmen*** .

- Legen Sie im neu geöffneten Dialog ***AVG-Schutz vorübergehend deaktivieren*** fest, wie lange Sie **AVG Internet Security 2012** deaktivieren möchten. Der Schutz wird standardmäßig für 10 Minuten deaktiviert, was für allgemeine Aufgaben wie die Installation neuer Software usw. ausreichend sein sollte. Beachten Sie, dass das anfängliche Zeitlimit möglicherweise auf 15 Minuten festgelegt ist und aus Sicherheitsgründen nicht durch Ihren eigenen Wert überschrieben werden kann. Nach Ablauf des festgelegten Zeitraums werden alle deaktivierten Komponenten automatisch wieder aktiviert.

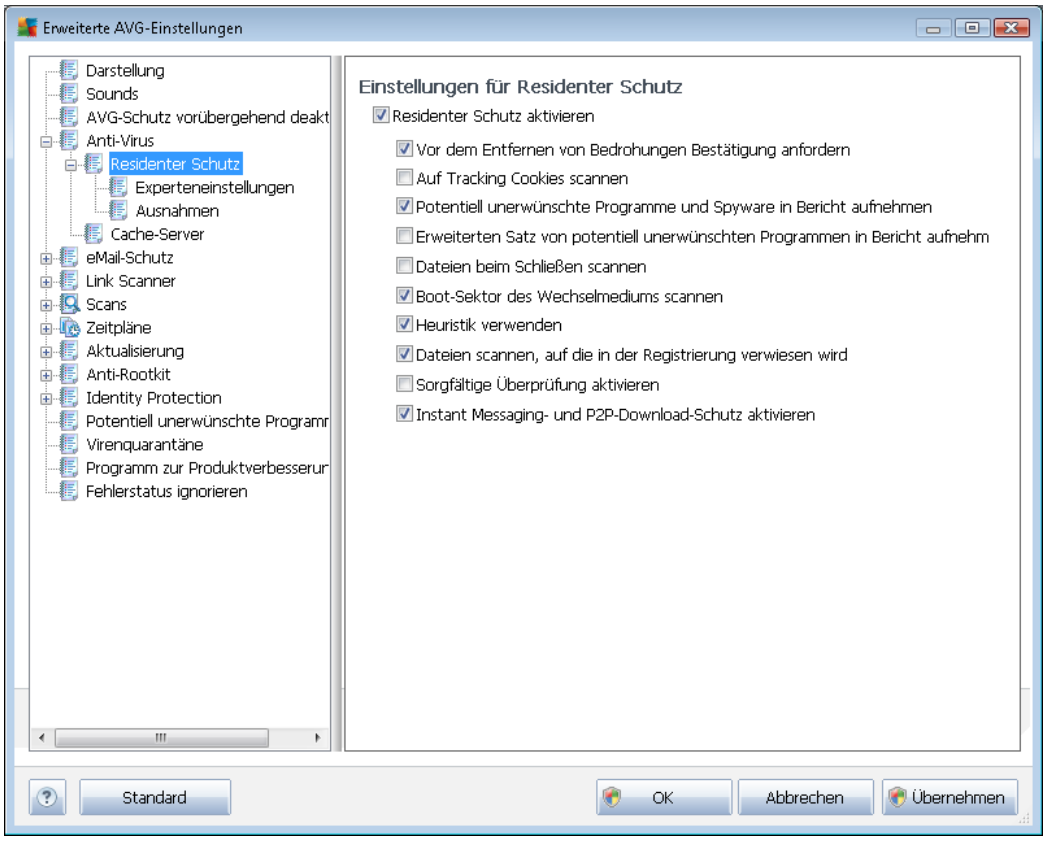


9.4. Anti-Virus

Geben Sie hier ein Thema ein.

9.4.1. Residenter Schutz

Der Residente Schutz schützt Dateien und Ordner vor Viren, Spyware und anderer Malware in Echtzeit.



Im Dialog ***Einstellungen für Residenter Schutz*** können Sie den Residenten Schutz vollständig aktivieren oder deaktivieren, indem Sie den Eintrag ***Residenter Schutz aktivieren*** aktivieren oder deaktivieren (*standardmäßig ist diese Option aktiviert*). Zusätzlich können Sie auswählen, welche Funktionen des Residenten Schutzes aktiviert werden sollen:

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – 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*) – Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von

Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Dateien beim Schließen scannen*** (*standardmäßig deaktiviert*) – Diese Option sorgt dafür, dass AVG aktive Objekte (z. B. Anwendungen oder Dokumente) sowohl beim Öffnen als auch beim Schließen scannt. Durch dieses Feature ist Ihr Computer auch vor einigen fortschrittlichen 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*).

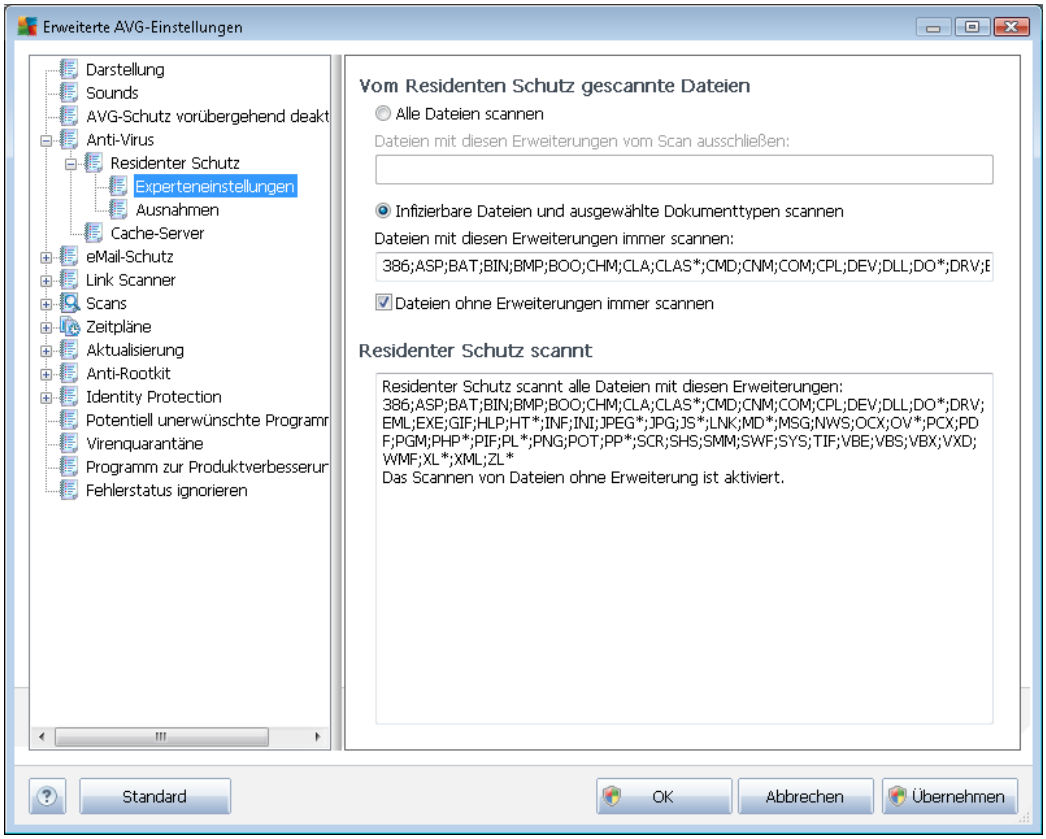
- ***Alle Bedrohungen automatisch entfernen*** (*standardmäßig deaktiviert*) – Jede erkannte Infektion wird automatisch geheilt, wenn eine Gegenmaßnahme verfügbar ist. Infektionen, die nicht geheilt werden können, werden entfernt.

- ***Dateien scannen, auf die in der Registrierung verwiesen wird*** (*standardmäßig aktiviert*) – Mit diesem Parameter wird festgelegt, dass AVG alle ausführbaren Dateien der Startup-Registrierung scannt, um zu verhindern, dass eine bekannte Infektion beim nächsten Computerstart ausgeführt wird.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*in extremen Notfällen*), um einen sorgfältigen Scan zu starten, bei dem alle möglichen, bedrohlichen Objekte genauestens überprüft werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

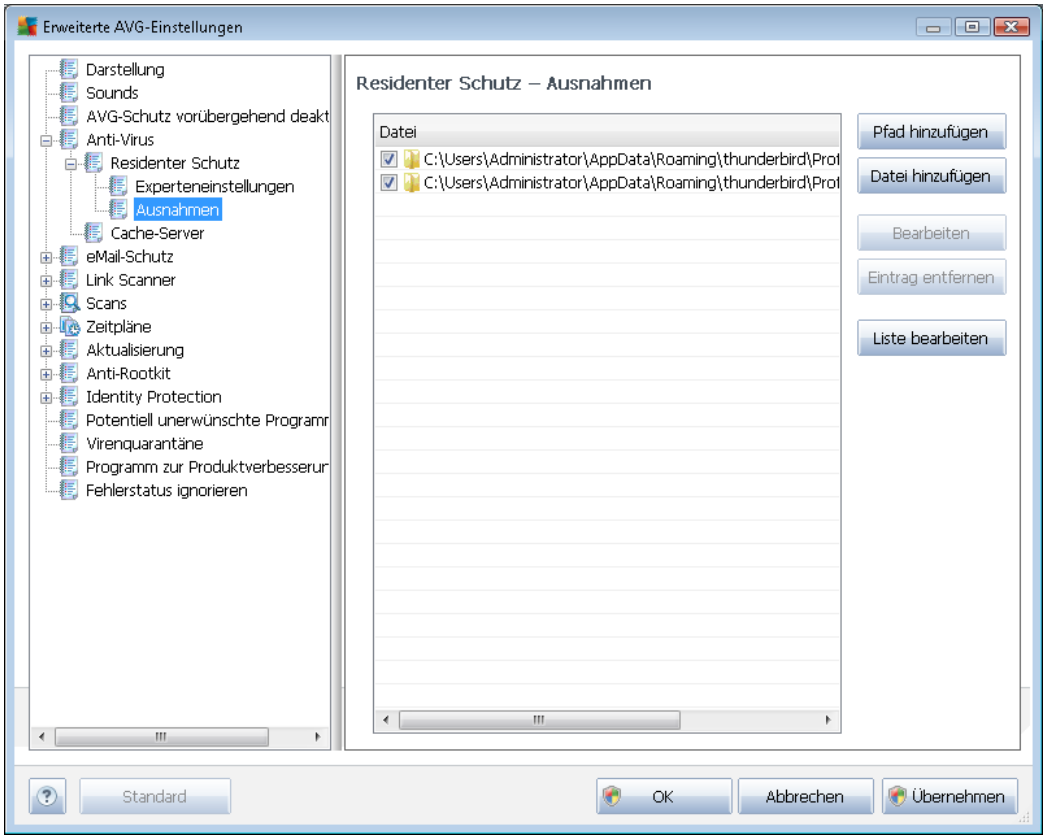
- ***Instant Messaging-Schutz und P2P-Downloadschutz aktivieren*** (*standardmäßig aktiviert*) – Aktivieren Sie diesen Eintrag, wenn Sie überprüfen möchten, ob die Kommunikation über Instant Messenger (*z.B. ICQ, MSN Messenger usw.*) und P2P-Downloads virenfrei sind.

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



Aktivieren Sie das entsprechende Kontrollkästchen, um festzulegen, ob Sie ***Alle Dateien scannen*** oder nur ***Infizierbare Dateien und ausgewählte Dokumenttypen scannen*** möchten. 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.

Im unteren Bereich ***Residenter Schutz scannt*** werden die aktuellen Einstellungen zusammengefasst und detailliert angezeigt, was vom ***Residenten Schutz*** tatsächlich gescannt wird.



Im Dialog ***Residenter Schutz – Ausnahmen*** können Sie Dateien und/oder Ordner definieren, die von der Überprüfung durch den ***Residenten Schutz***ausgeschlossen werden sollen.

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

Schaltflächen

Der Dialog enthält folgende Schaltflächen:

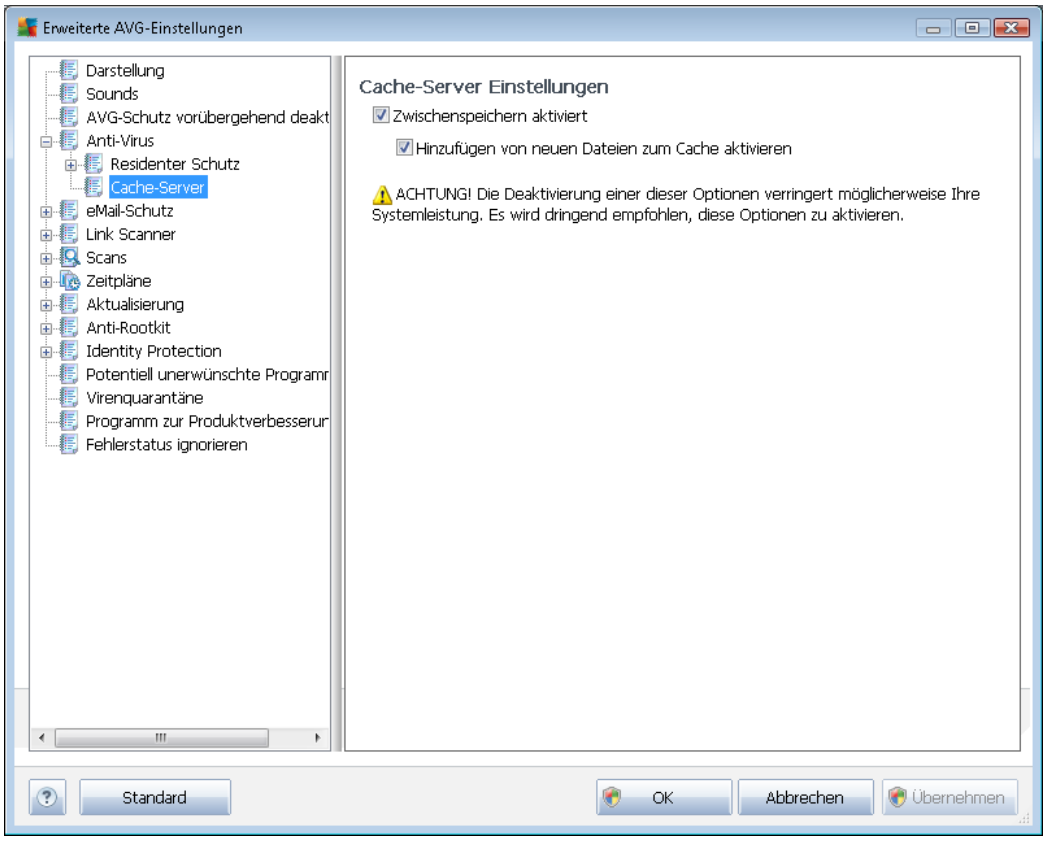
- ***Pfad hinzufügen*** – Mit dieser Schaltfläche können Sie ein oder mehrere Verzeichnisse angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Datei hinzufügen*** – Mit dieser Schaltfläche können Sie Dateien angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Bearbeiten*** – Hier können Sie den festgelegten Pfad zu einer ausgewählten Datei oder einem ausgewählten Ordner bearbeiten
- ***Eintrag entfernen***– Mit dieser Schaltfläche können Sie den Pfad zu einem ausgewählten

Eintrag aus der Liste löschen

- ***Liste bearbeiten*** – Mit dieser Schaltfläche können Sie die gesamte Liste der definierten Ausnahmen in einem neuen Dialog bearbeiten, der wie ein Standardtexteditor funktioniert

9.4.2. Cache-Server

Der Dialog ***Cache-Servereinstellungen*** bezieht sich auf den Cache-Server-Vorgang, der alle Arten von Scans von **AVG Internet Security 2012** beschleunigt:



Der Cache-Server sammelt und speichert Informationen von vertrauenswürdigen Dateien (*eine Datei wird als vertrauenswürdig eingestuft, wenn sie mit einer digitalen Signatur einer vertrauenswürdigen Quelle versehen ist*). Diese Dateien werden damit automatisch als sicher angesehen und müssen nicht erneut geprüft werden; daher werden diese Dateien beim Scan-Vorgang übersprungen.

Im Dialog ***Cache-Servereinstellungen*** stehen folgende Konfigurationsoptionen zur Verfügung:

- ***Zwischenspeichern aktiviert*** (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, um den ***Cache-Server*** zu deaktivieren und den Zwischenspeicher zu leeren. Beachten Sie, dass Scans möglicherweise langsamer ablaufen und die Gesamtleistung des Computers beeinträchtigt wird, da jede einzelne verwendete Datei zunächst auf Viren und Spyware gescannt wird.

- ***Hinzufügen von neuen Dateien zum Cache aktivieren*** (*standardmäßig aktiviert*) –

Deaktivieren Sie dieses Kontrollkästchen, und dem Zwischenspeicher werden keine weiteren Dateien hinzugefügt. Dateien, die sich bereits im Zwischenspeicher befinden, bleiben darin enthalten und werden bis zum nächsten Update der Virendatenbank oder bis zum vollständigen Ausschalten des Zwischenspeichers weiter verwendet.

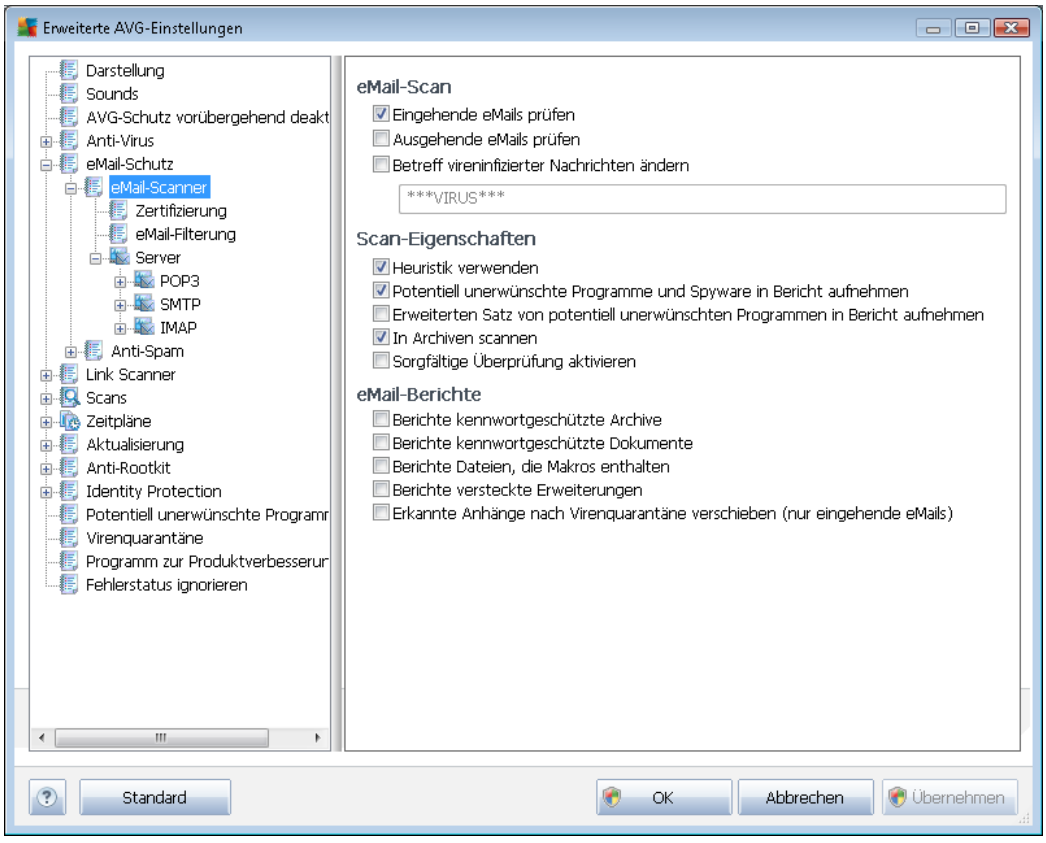
Wir empfehlen dringend, die Standardeinstellungen beizubehalten und beide Optionen aktiviert zu lassen, sofern Sie keinen wichtigen Grund haben, den Cache-Server zu deaktivieren. Andernfalls können Leistung und Geschwindigkeit Ihres Systems deutlich abnehmen.

9.5. eMail-Schutz

In dem Bereich ***eMail-Schutz*** können Sie die detaillierte Konfiguration von eMail-Scanner und Anti-Spam bearbeiten:

9.5.1. eMail-Scanner

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



eMail-Scan

In diesem Abschnitt können Sie folgende Basiseinstellungen für ein- und ausgehende eMail-Nachrichten vornehmen:

- ***Eingehende eMails überprüfen*** (*standardmäßig aktiviert*) – Aktivieren/Deaktivieren Sie diese Option, um alle an Ihren eMail-Client gesendeten Nachrichten zu scannen bzw. nicht zu scannen

- ***Ausgehende eMails überprüfen*** (*standardmäßig deaktiviert*) – Aktivieren/Deaktivieren Sie diese Option, um alle von Ihrem Konto gesendeten eMails zu scannen bzw. nicht zu scannen

- ***Betreff vireninfizierter Nachrichten ändern*** (*standardmäßig deaktiviert*) – Wenn Sie gewarnt werden möchten, dass beim Scannen eine infizierte eMail erkannt wurde, aktivieren Sie diesen Eintrag, und geben Sie im Textfeld den gewünschten Text ein. Dieser Text wird dem Betreff jeder infizierten eMail-Nachricht hinzugefügt , um die Identifikation und Filterung zu erleichtern. Der Standardtext lautet ***VIRUS***. Wir empfehlen, diesen beizubehalten.

Scan-Eigenschaften

In diesem Abschnitt können Sie festlegen, wie die eMail-Nachrichten gescannt werden sollen:

- ***Heuristik verwenden*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, um als Erkennungsmethode beim Scannen der eMail-Nachrichten die Heuristik zu verwenden. Wenn diese Option aktiviert ist, werden·eMail-Anhänge nicht nur anhand ihrer Dateierweiterungen gefiltert. Der eigentliche Inhalt des Anhangs wird ebenfalls betrachtet. Die Filterung kann im Dialog eMail-Filterung eingestellt werden.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** *(standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***In Archiven scannen*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, um den Inhalt von Archiven zu scannen, die an eMail-Nachrichten angehängt sind.

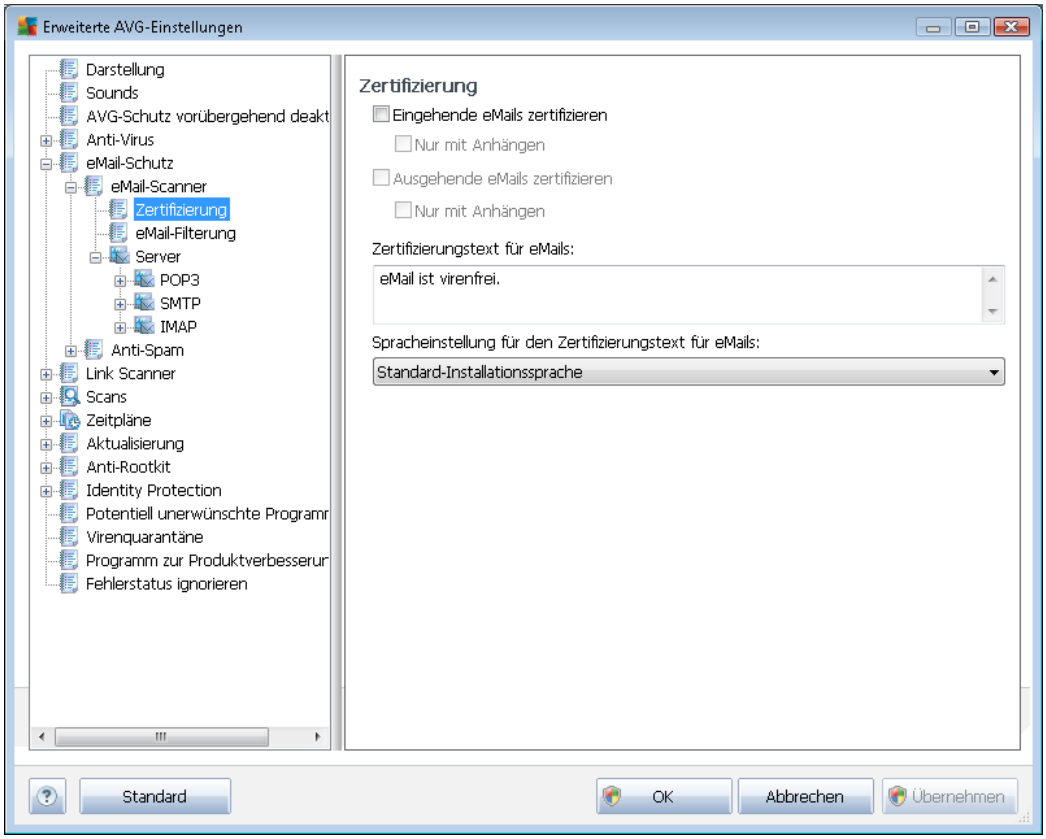
- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer durch ein Virus oder ein Exploit infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

Berichte über eMail-Anhänge

In diesem Bereich können Sie zusätzliche Berichte über Dateien einrichten, die potentiell gefährlich oder verdächtig sein können. Bitte beachten Sie, dass keine Warnung angezeigt wird. Es wird lediglich ein Zertifizierungstext am Ende der eMail-Nachricht angehängt. Alle derartigen Berichte werden im Dialog eMail-Scanner-Erkennung aufgelistet:

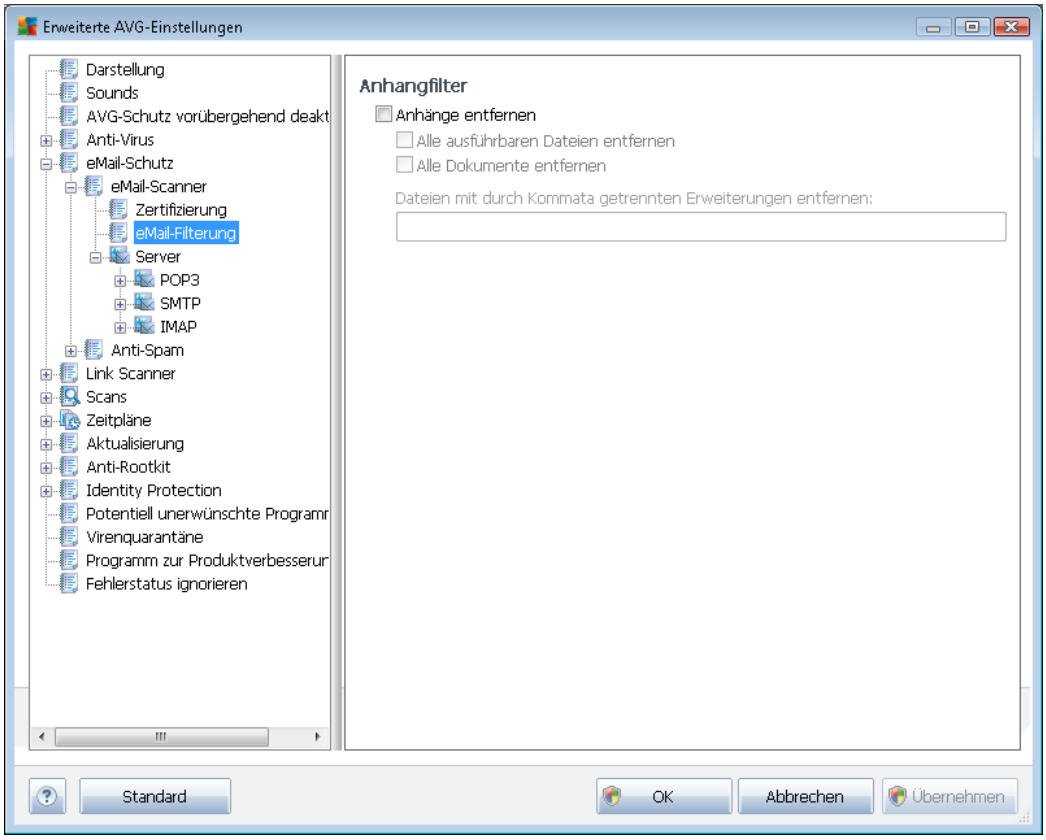
- ***Berichte kennwortgeschützte Archive*** – Archive (*ZIP, RAR usw.*) die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Archive als potentiell gefährlich anzuzeigen.
- ***Kennwortgeschützte Dokumente*** – Dokumente, die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Dokumente als potentiell gefährlich anzuzeigen.
- ***Dateien, die Makros enthalten*** – Ein Makro ist eine vordefinierte Abfolge von Schritten, die bestimmte Aufgaben für den Benutzer vereinfachen (*Makros in MS Word sind weitgehend bekannt*). Ein Makro kann z.B. potentiell gefährliche Anweisungen enthalten und durch Aktivieren dieses Kontrollkästchens wird sichergestellt, dass Dateien mit Makros als verdächtig eingestuft werden.
- ***Berichte versteckte Erweiterungen*** – Durch versteckte Erweiterungen kann beispielsweise eine verdächtige ausführbare Datei wie „abcdef.txt.exe“ als eine harmlose Textdatei „abcdef.txt“ angezeigt werden. Aktivieren Sie das Kontrollkästchen, um diese Dateien als potentiell gefährlich anzuzeigen.
- ***Erkannte Anhänge in die Virenquarantäne verschieben*** – 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.

Im Dialog ***Zertifizierung*** können Sie die entsprechenden Kontrollkästchen aktivieren, um festzulegen, ob Sie Ihre eingehenden Mails (***Eingehende eMail zertifizieren***) und/oder ausgehenden Mails (***Ausgehende eMail zertifizieren***) zertifizieren möchten. Für jede dieser Optionen können Sie zudem den Parameter ***Nur mit Anhängen*** angeben, so dass die Zertifizierung nur zu eMail-Nachrichten mit Anhängen hinzugefügt wird:



Standardmäßig enthält der Zertifizierungstext nur die allgemeine Information *Die Nachricht ist virenfrei.* Diese Information kann jedoch nach Ihren Wünschen erweitert oder verändert werden: Geben Sie im Feld ***Zertifizierungstext für eMails*** den gewünschten Zertifizierungstext ein. Im Abschnitt ***Spracheinstellung für den Zertifizierungstext für eMails*** können Sie zudem festlegen, in welcher Sprache der automatisch erstellte Teil der Zertifizierung (*Die Nachricht ist virenfrei*) angezeigt werden soll.

Hinweis: *Bitte beachten Sie, dass nur der Standardtext in der gewünschten Sprache angezeigt und Ihr benutzerdefinierter Text nicht automatisch übersetzt wird.*



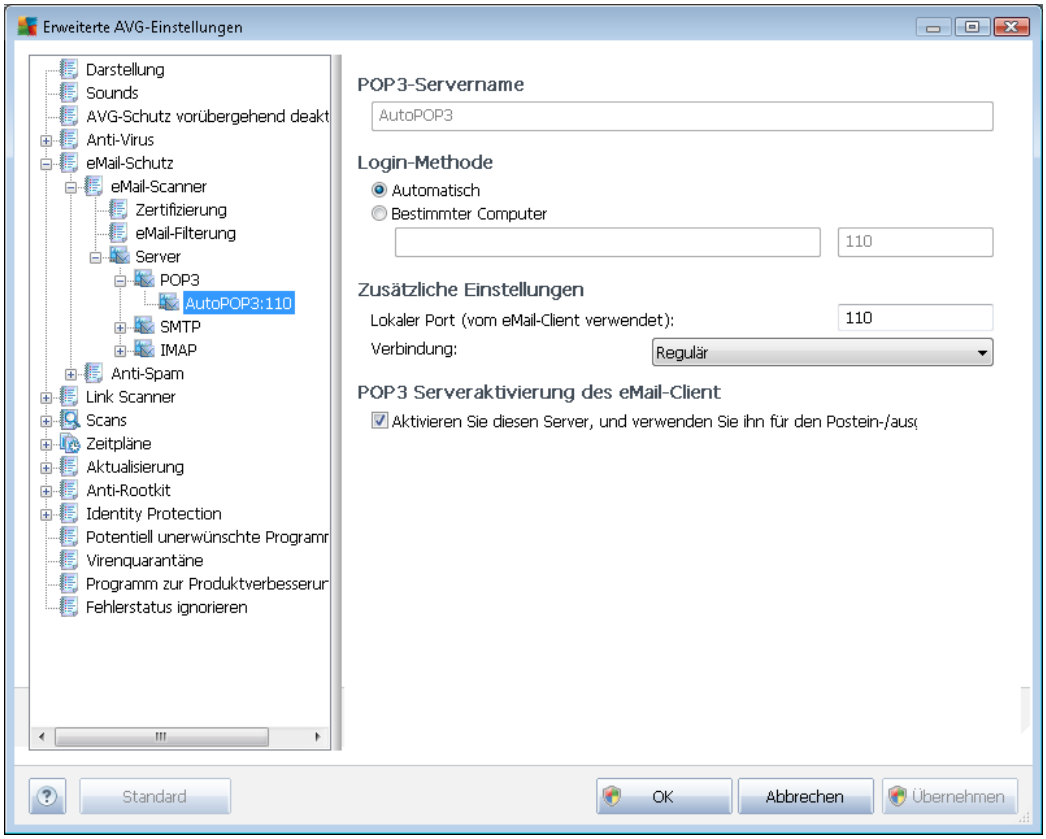
Im Dialog ***Anhangfilter*** können Sie Parameter für das Scannen von eMail-Anhängen festlegen. Standardmäßig ist die Option ***Anhänge entfernen*** deaktiviert. Wenn Sie die Option aktivieren, werden alle eMail-Anhänge, die als infektiös oder potentiell gefährlich erkannt werden, automatisch entfernt. 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 mit den folgenden Erweiterungen werden entfernt: *.doc, *.docx, *.xls, *.xlsx
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Alle Dateien mit den definierten Erweiterungen werden entfernt

Im Bereich ***Server*** können Sie die Parameter der eMail Scanner-Server bearbeiten:

- POP3-Server
- SMTP-Server
- IMAP-Server

Sie können auch neue Server für eingehende oder ausgehende eMails über die Schaltfläche***Neuen Server hinzufügen*** festlegen.



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

- ***POP3-Servername*** – In diesem Feld können sie den Namen des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines POP3-Servers mit der rechten Maustaste auf den POP3-Eintrag im linken Navigationsmenü*). Bei einem automatisch erstellten „AutoPOP3"-Server ist dieses Feld deaktiviert.

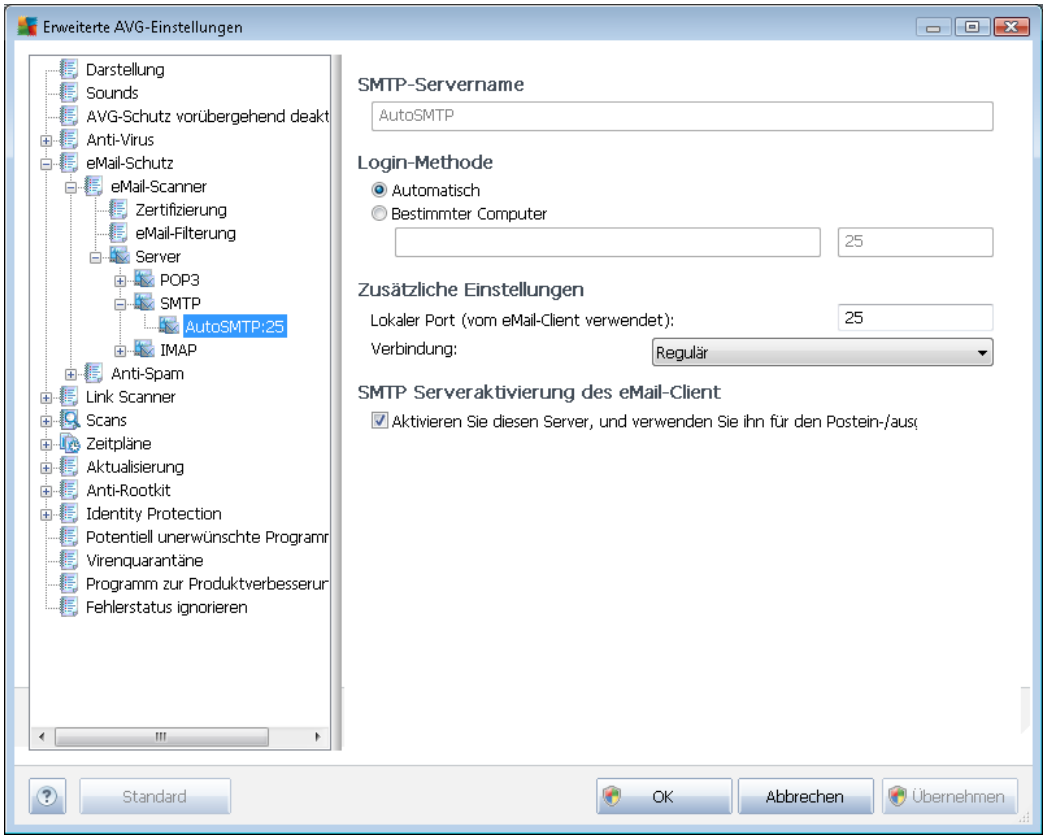
- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für eingehende eMails bestimmt werden soll:

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

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

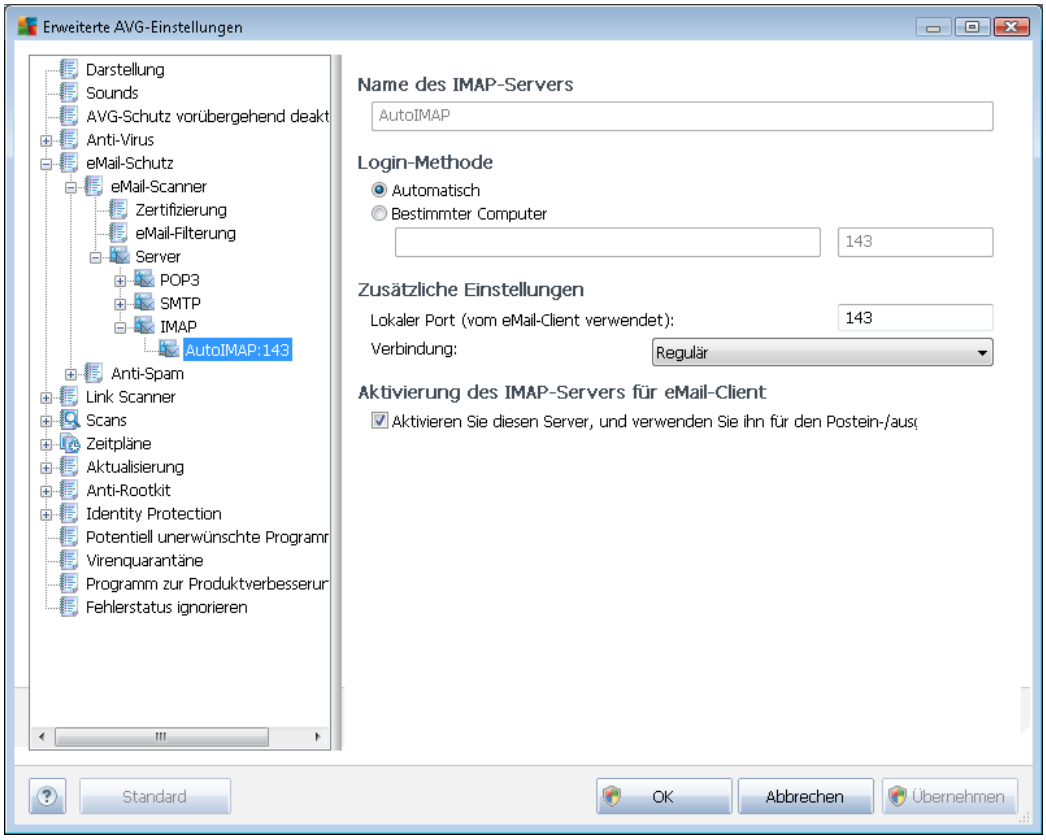


In diesem Dialog (*wird über **Server/SMTP*** geöffnet) können Sie einen neuen eMail-Scanner-Server einrichten, der das SMTP-Protokoll für ausgehende eMails verwendet:

- ***SMTP-Servername*** – In diesem Feld können sie den Name des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines SMTP-Servers mit der rechten Maustaste auf*

den SMTP-Eintrag im linken Navigationsmenü). Bei einem automatisch erstellten „AutoSMTP“-Server ist dieses Feld deaktiviert.

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für ausgehende eMails bestimmt werden soll:
    - ***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 Mailserver 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 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 SMTP-Kommunikation angeben.
    - ***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.
- ***SMTP-Serveraktivierung des eMail-Client*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten SMTP-Server zu aktivieren/deaktivieren



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

- ***IMAP-Servername*** – In diesem Feld können sie den Name des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines IMAP-Servers mit der rechten Maustaste auf den IMAP-Eintrag im linken Navigationsmenü*). Bei einem automatisch erstellten „AutoIMAP"-Server ist dieses Feld deaktiviert.

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für ausgehende eMails bestimmt werden soll:

    - ***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. imap.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. imap.acme.com:8200*). Der Standardport für die IMAP-Kommunikation ist 143.

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

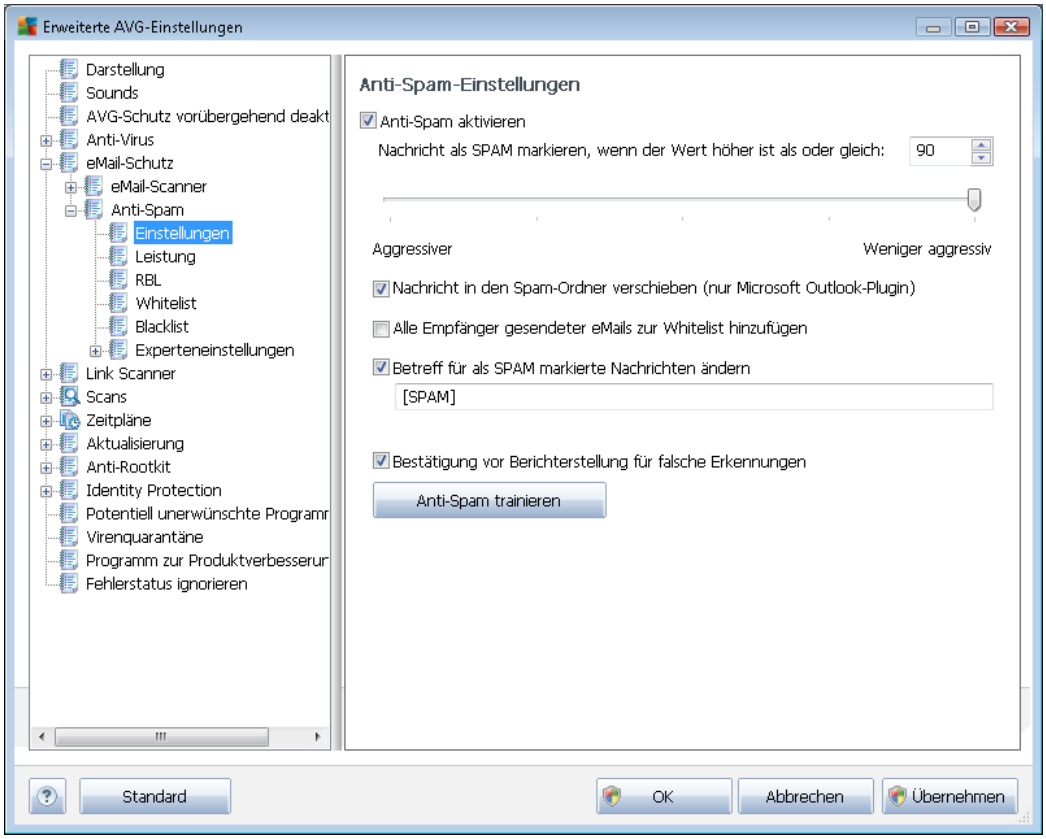
- ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung ankommen soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die IMAP-Kommunikation angeben.

- ***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.

- ***IMAP-Serveraktivierung des eMail-Clients*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten IMAP-Server zu aktivieren/deaktivieren

9.5.2. Anti-Spam

Geben Sie hier ein Thema ein.



Im Dialog ***Anti-Spam-Einstellungen*** können Sie das Kontrollkästchen ***Anti-Spam aktivieren*** aktivieren bzw. deaktivieren, um festzulegen, ob eMails auf Spam gescannt 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 eingeben oder den Schieberegler nach links oder rechts verschieben (*es 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 80–90*** – 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 50–59*** – 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.

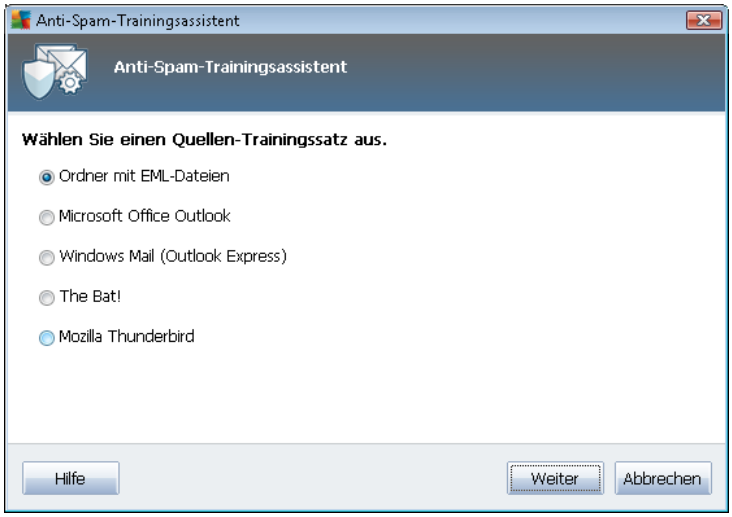
Im Dialog ***Anti-Spam-Einstellungen*** können Sie außerdem festlegen, wie mit den erkannten Spam-eMail-Nachrichten verfahren werden soll:

- ***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.
- ***Bestätigung vor Berichterstellung für falsche Erkennungen*** − Setzt voraus, dass Sie während des Installationsvorgangs zugestimmt haben, am Programm zur Produktverbesserung teilzunehmen. Wenn dies der Fall ist, haben Sie die Berichterstellung über erkannte Bedrohungen an AVG zugelassen. Die Berichterstellung erfolgt automatisch. Sie können das Kontrollkästchen jedoch aktivieren, wenn Sie benachrichtigt werden möchten, bevor ein Bericht über erkannten Spam an AVG gesendet wird, wobei sichergestellt werden soll, dass es sich bei der Nachricht wirklich um Spam handelt.

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 aufgefordert, die Quelle der eMail-Nachrichten auszuwählen, die für das Training verwendet werden sollen. In der Regel wählen Sie eMails aus, die nicht als Spam erkannt oder fälschlicherweise als Spam eingestuft worden sind.



Folgende Optionen stehen zur Auswahl:

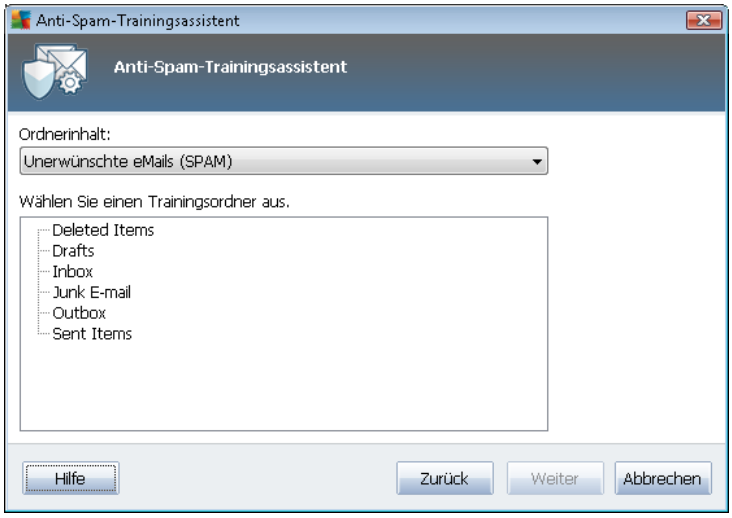
- ***Spezifischer eMail-Client*** – Wenn Sie einen der aufgelisteten eMail-Clients verwenden (*MS Outlook, Outlook Express, The Bat! oder*), wählen Sie einfach die entsprechende Option aus
- ***Ordner mit EML-Dateien*** – Wenn Sie ein anderes eMail-Programm verwenden, sollten Sie die Nachrichten zunächst 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 Training zu erleichtern und zu beschleunigen, empfiehlt sich eine entsprechende Vorsortierung, so dass der Ordner nur noch die (erwünschten bzw. unerwünschten) eMails für das Training enthält. 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



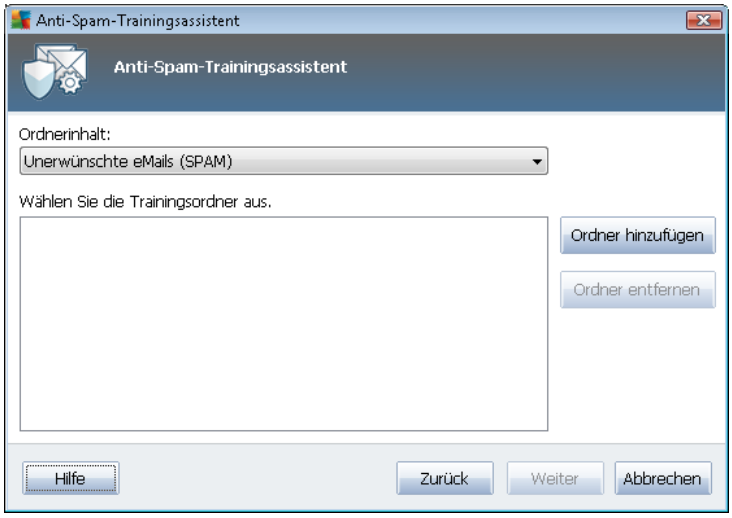
Wählen Sie in diesem Dialog bitte den Ordner mit den Nachrichten aus, den Sie für Trainingszwecke verwenden möchten. Klicken Sie auf die Schaltfläche ***Ordner hinzufügen***, um den Ordner mit den EML-Dateien zu suchen (*gespeicherte eMail-Nachrichten*). Der ausgewählte Ordner wird anschließend im Dialog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

Wählen Sie im Dropdown-Menü ***Ordnerinhalt***eine der 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. 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***, und fahren Sie fort mit den Filteroptionen für Nachrichten.

Ein bestimmter eMail-Client

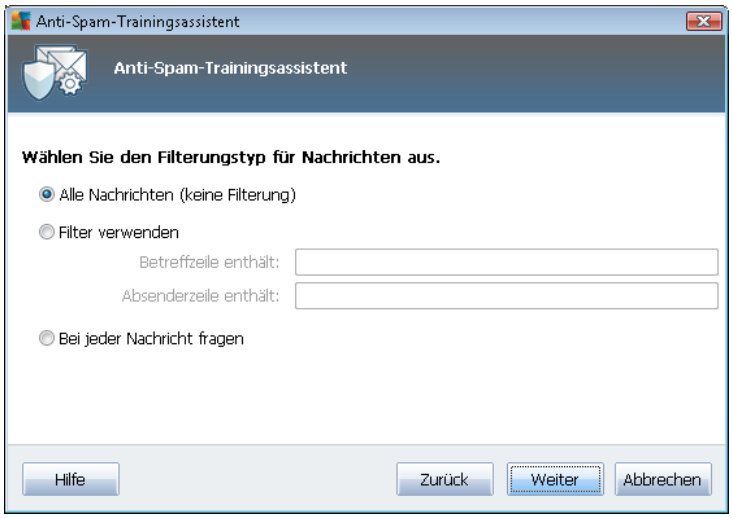
Sobald Sie eine der Optionen bestätigen, wird ein neuer Dialog angezeigt.



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. Suchen Sie den gewünschten Ordner, und wählen Sie diesen 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 Filter für eMail-Nachrichten konfigurieren.

- ***Alle Nachrichten (keine Filterung)*** – Wenn Sie sicher sind, dass der ausgewählte Ordner

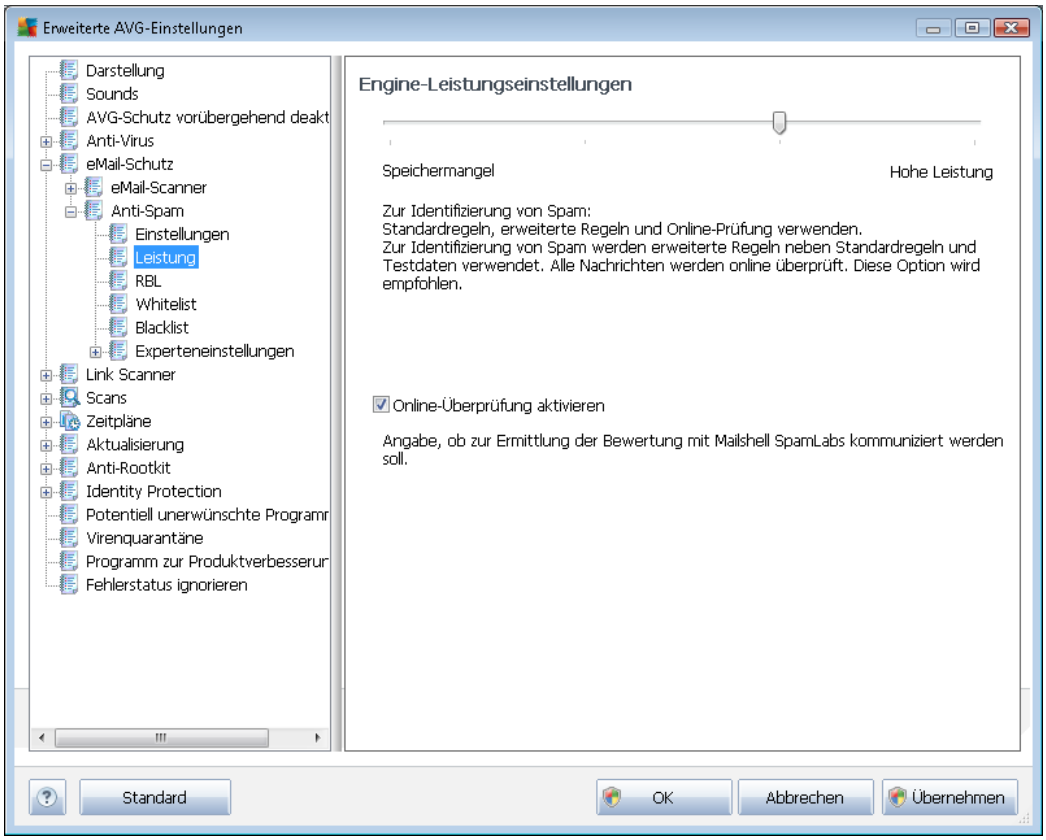
ausschließlich Nachrichten enthält, die Sie für das Training verwenden möchten, wählen Sie die Option ***Alle Nachrichten (keine Filterung)*** .

- ***Filter verwenden*** – Um eine erweiterte Filterung anzuwenden, wählen Sie die Option ***Filter verwenden***aus. 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 exakt mit den Suchkriterien übereinstimmen, werden unmittelbar·für das Training verwendet. Wenn Sie beide Textfelder ausfüllen, werden auch Adressen verwendet, für die nur eines der beiden Suchkriterien zutrifft!

- ***Bei jeder Nachricht fragen*** – Wenn Sie sich angesichts der im Ordner enthaltenen Nachrichten nicht sicher sind, kann Sie der Assistent bei 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***.

Nachdem Sie die gewünschte Option ausgewählt 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.

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.

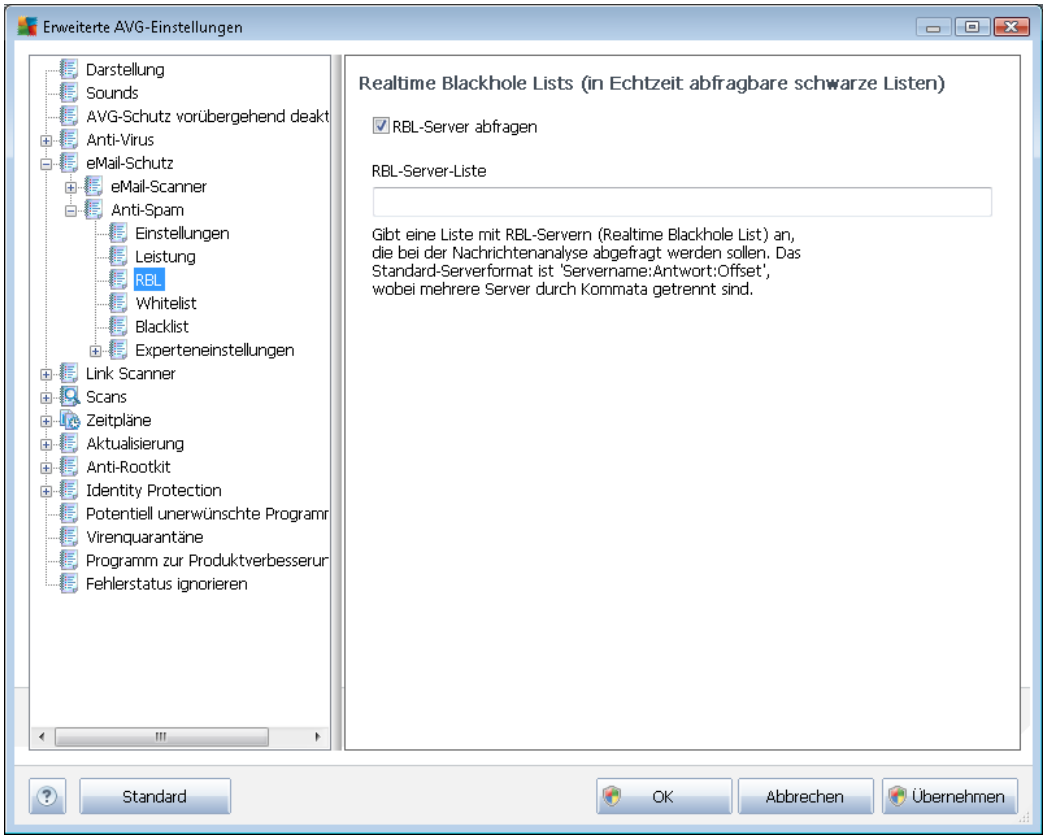
- ***Speichermangel*** – Beim Scanvorgang werden zur Identifizierung von Spam keine Regeln verwendet. Zur Identifizierung werden nur Testdaten verwendet. Dieser Modus ist nicht für den allgemeinen Gebrauch empfohlen, es sei denn, die Computer-Hardware ist wirklich sehr langsam.

- ***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!

Der Eintrag ***RBL*** öffnet den Bearbeitungsdialog ***Realtime Blackhole Lists (in Echtzeit abfragbare schwarze Listen)***, in dem Sie die Funktion ***RBL-Server abfragen*** aktivieren bzw. deaktivieren können:

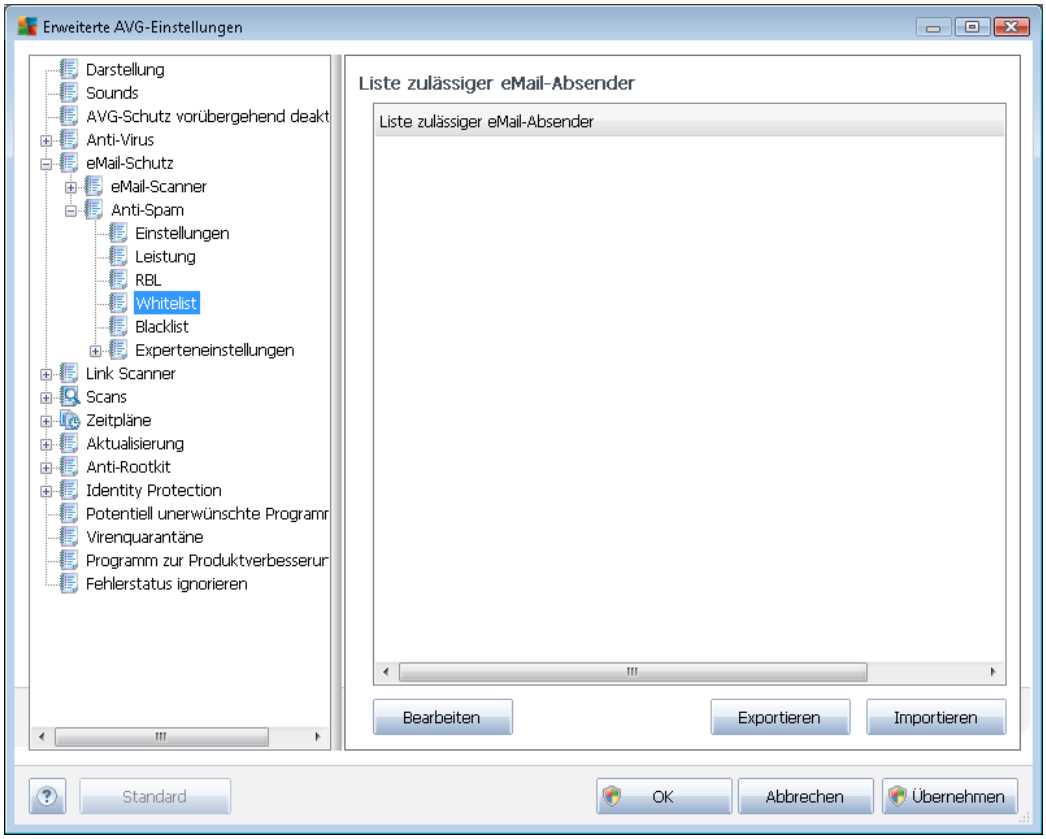


Der RBL-Server (*Realtime Blackhole Lists (in Echtzeit abfragbare schwarze Listen)*) ist ein DNS-Server mit einer umfangreichen Datenbank bekannter Spam-Sender. Bei Aktivierung dieser Funktion werden alle eMails mit den Adressen der RBL-Serverdatenbank verglichen und als Spam markiert, wenn Sie einem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

In der ***RBL-Serverliste*** können Sie bestimmte RBL-Serverstandorte definieren (*Bitte beachten Sie, dass die Aktivierung dieser Funktion den eMail-Empfang für einige Systeme und Konfigurationen verlangsamen kann, da jede einzelne Nachricht mit der RBL-Serverdatenbank abgeglichen werden muss).*

Es werden keine persönlichen Daten an den Server gesendet!

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.



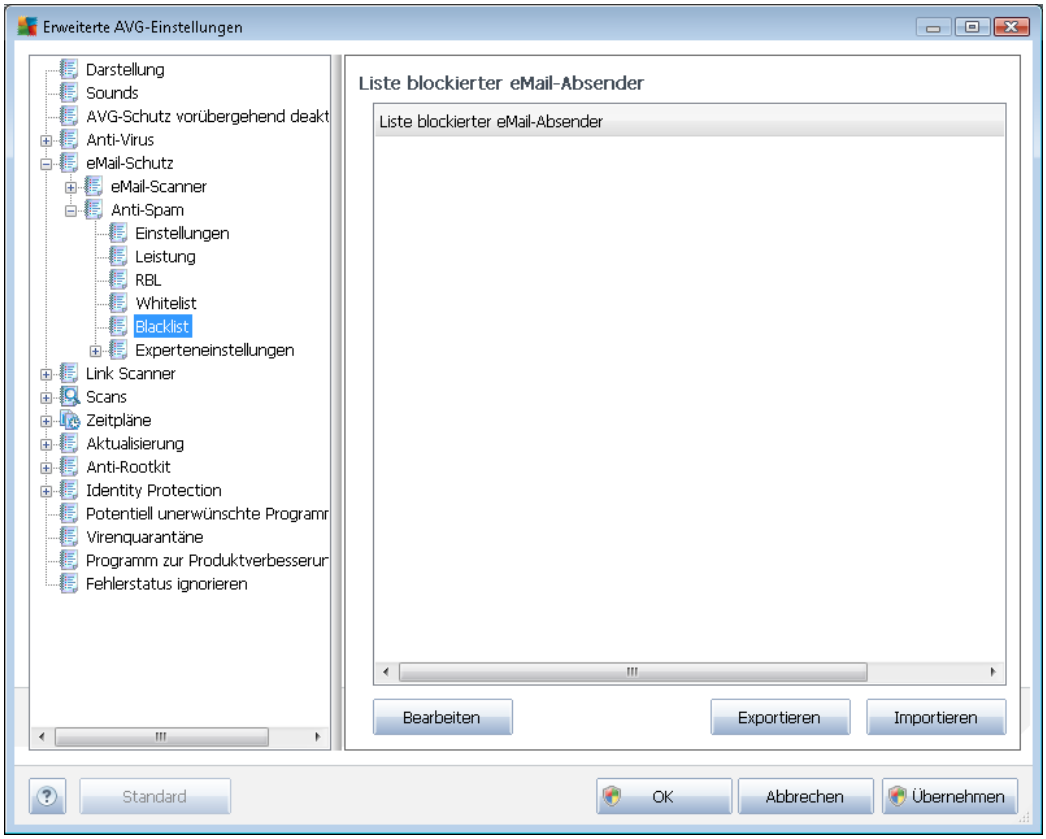
In der Bearbeitungsoberfläche können Sie eine Liste mit Absendern erstellen, bei denen Sie sicher sind, dass sie Ihnen nie unerwünschte Nachrichten (Spam) senden werden. Sie können auch eine Liste mit vollständigen Domainnamen erstellen (*z. B. avg.com*), von denen Sie wissen, dass sie keine Spam-Nachrichten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

Schaltflächen

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 Datei darf nur ein Element *(Adresse, Domainname)* pro Zeile enthalten.

Wenn Sie den Eintrag ***Blacklist*** wählen, 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.

Schaltflächen

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.

Der Zweig Erweiterte Einstellungen enthält zahlreiche Optionen, die für die Komponente Anti-Spam festgelegt werden können. Diese Einstellungen sind ausschließlich für erfahrene Benutzer vorgesehen, normalerweise Netzwerk-Administratoren, die den Spam-Schutz detailliert konfigurieren müssen, um den besten Schutz für eMail-Server zu gewährleisten. Daher steht für die einzelnen Dialoge keine weitere Hilfe zur Verfügung. Auf der Benutzeroberfläche finden Sie jedoch eine kurze Beschreibung der jeweiligen Option.

Wir empfehlen ausdrücklich, keine Einstellungen zu ändern, es sei denn, Sie sind wirklich mit den erweiterten Einstellungen von SpamCatcher (Mailshell Inc.) vertraut. Andernfalls kann es zu Leistungseinbußen oder Fehlfunktionen der Komponente kommen.

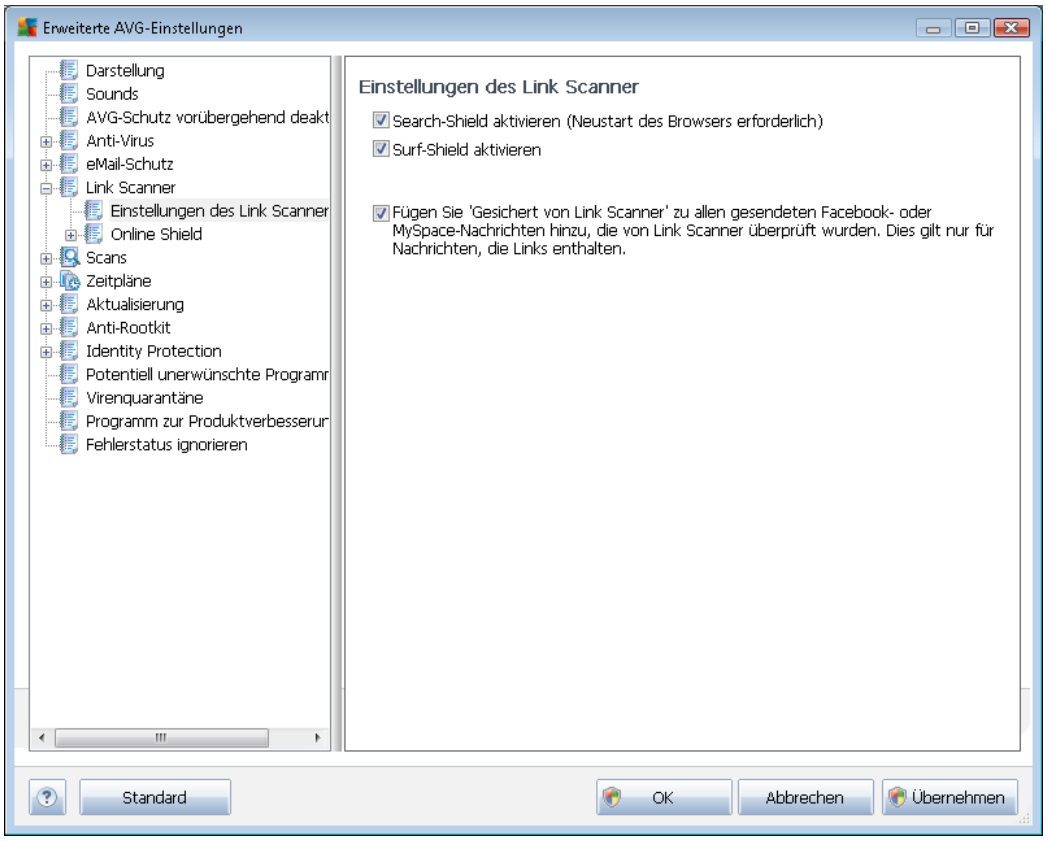
Wenn Sie dennoch der Meinung sind, dass Sie die Konfiguration von Anti-Spam im Detail ändern müssen, folgen Sie den Anweisungen direkt auf der Benutzeroberfläche. Im Allgemeinen finden Sie in jedem Dialog eine bestimmte Funktion, die Sie bearbeiten können, sowie die zugehörige Beschreibung:

- ***Cache*** – Fingerabdruck, Domainprüfung, LegitRepute
- ***Training*** – maximale Worteinträge, Schwellenwert für Autotraining, Gewicht
- ***Filtern*** – Sprachenliste, Länderliste, genehmigte IPs, blockierte IPs, blockierte Länder, blockierte Zeichensätze, gefälschte Absender
- ***RBL*** – RBL-Server, Mehrfachtreffer, Schwellenwert, Timeout, maximale IPs
- ***Internetverbindung*** – Timeout, Proxyserver, Proxyauthentifizierung

9.6. Link Scanner

9.6.1. Einstellungen für Link Scanner

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

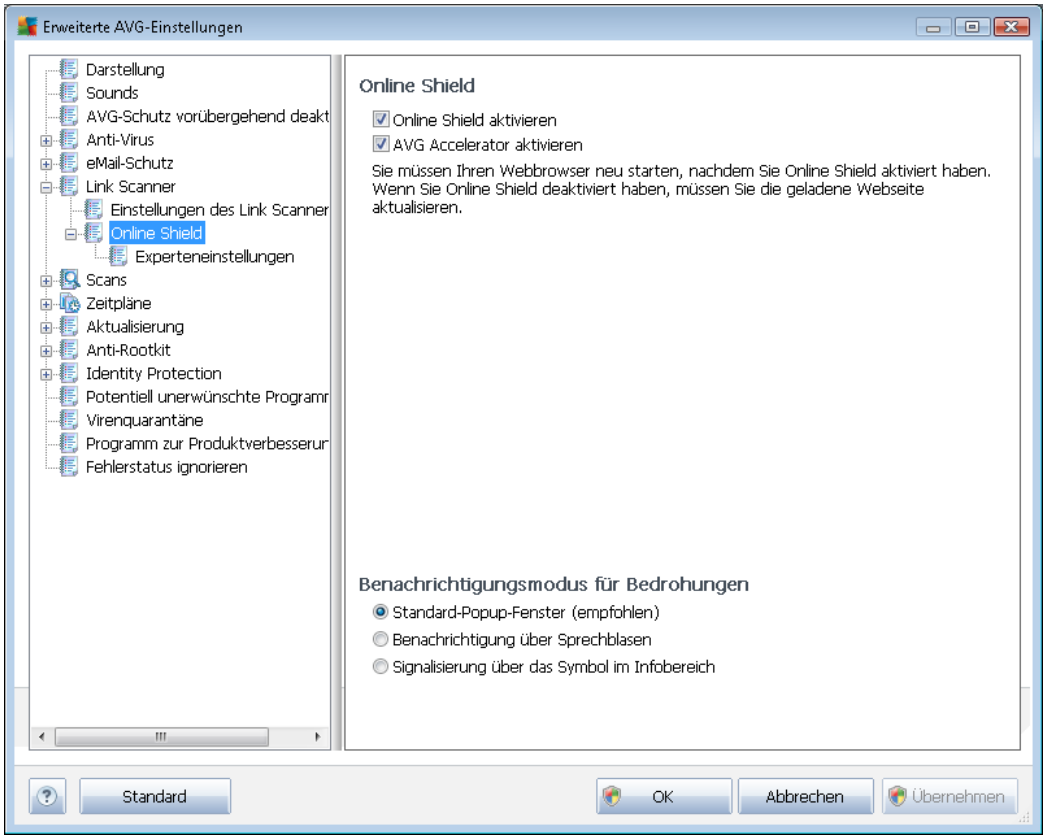


- ***Search-Shield aktivieren*** – (*standardmäßig aktiviert*): Benachrichtigungssymbole zu Suchabfragen in Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg und Slashdot weisen darauf hin, dass der Inhalt der als Suchergebnis angezeigten Sites überprüft wurde.

- ***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.

- ***„Gesichert von Link Scanner" hinzufügen*** – (*standardmäßig aktiviert*): Aktivieren Sie diesen Eintrag, wenn Sie zu allen von Link Scanner überprüften Nachrichten, die einen Link enthalten und von Facebook oder MySpace gesendet wurden, eine Zertifizierungsbenachrichtigung hinzufügen möchten.

9.6.2. Online Shield



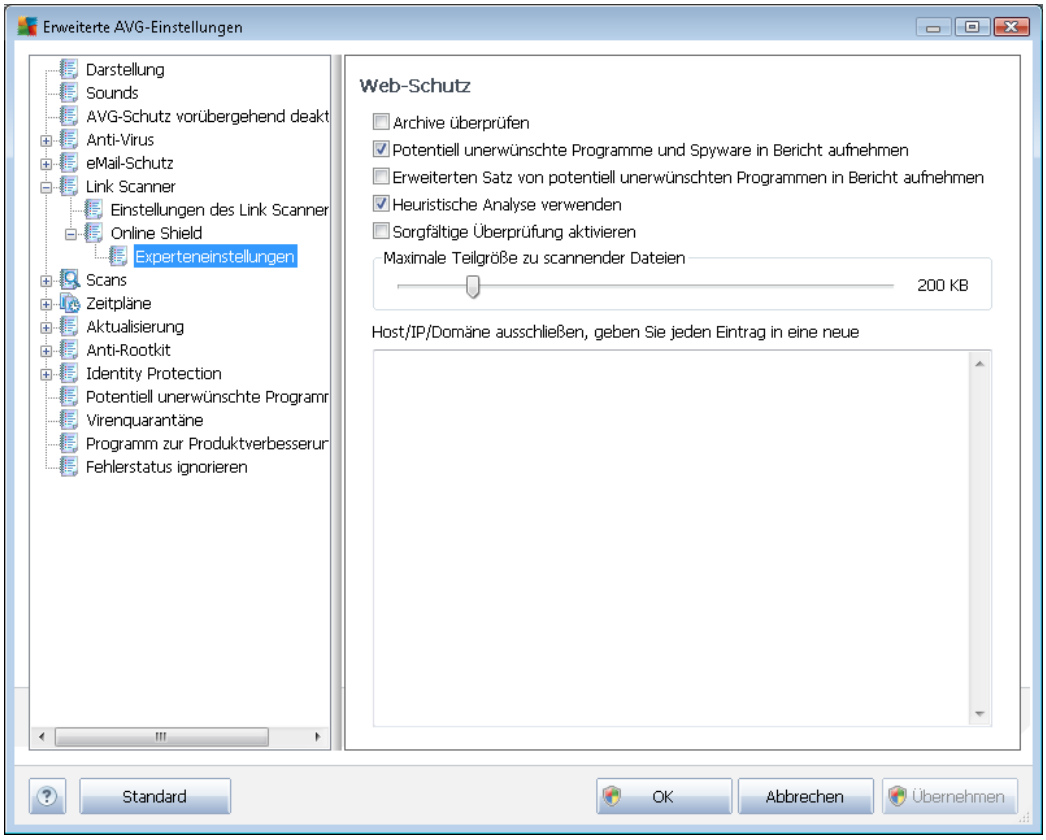
Der Dialog ***Online Shield*** enthält die folgenden Optionen:

- ***Online Shield aktivieren****(standardmäßig aktiviert)* – Aktivieren bzw. deaktivieren Sie den gesamten Dienst ***Online Shield***. Für weitere erweiterte Einstellungen von ***Online Shield*** fahren Sie bitte mit dem nachfolgenden Dialog Web-Schutz fort.

- ***AVG Accelerator aktivieren*** *(standardmäßig aktiviert)* – Aktivieren bzw. deaktivieren Sie den Dienst ***AVG Accelerator***, der eine gleichmäßigere Online-Videowiedergabe ermöglicht und zusätzliches Herunterladen vereinfacht.

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.



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 ***Online 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*** – (*standardmäßig deaktiviert*): Archivinhalte, die möglicherweise auf einer anzuzeigenden Webseite enthalten sind, werden ebenfalls gescannt.
    - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert*): Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
    - ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** – (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn

Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

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

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***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. Mithilfe des Schiebereglers können Sie die maximale Größe einer Datei festlegen, die noch mit ***Online Shield*** gescannt werden soll. Selbst wenn die heruntergeladene Datei größer als festgelegt ist und daher nicht mit Online 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 ***Online Shield*** *gescannt werden sollen.* Schließen Sie daher nur Hosts aus, die mit Sicherheit keine gefährlichen Webinhalte bereitstellen.

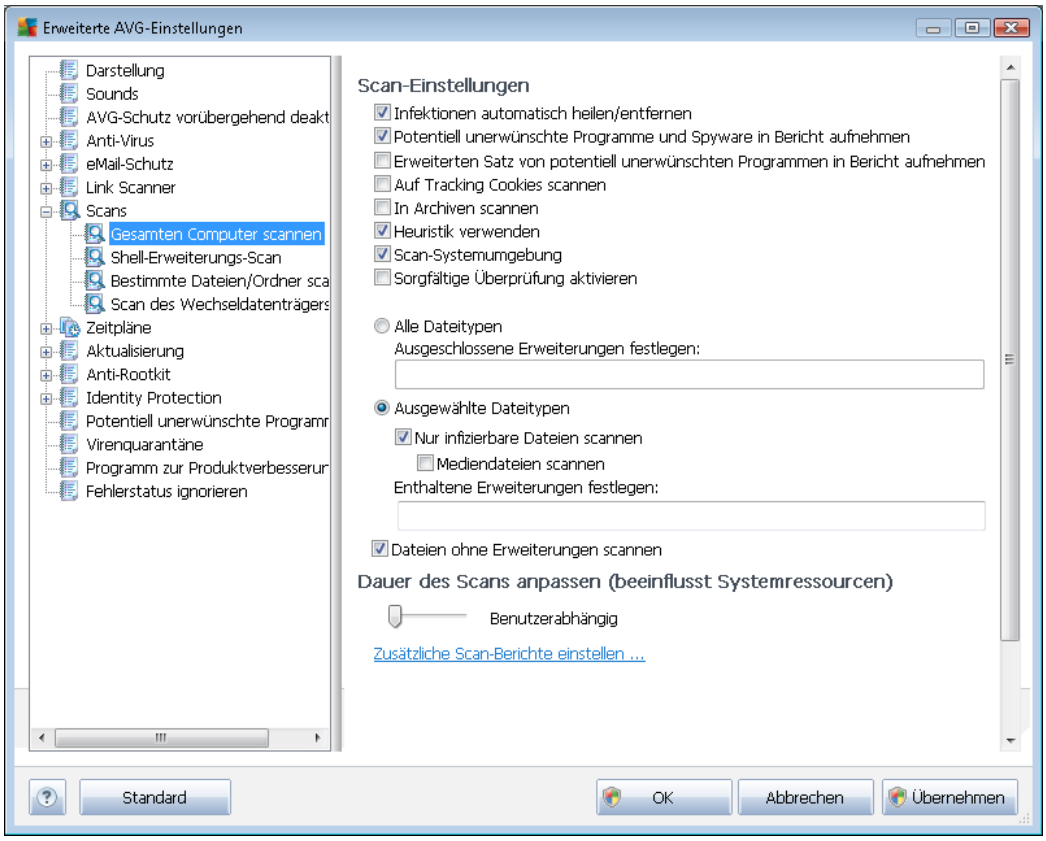
9.7. Scans

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

- ***Scan des gesamten Computers*** – 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

9.7.1. Gesamten Computer scannen

Mit der Option ***Scan des gesamten Computers*** können Sie die Parameter eines Scans bearbeiten, der vom Software-Hersteller vordefiniert wurde, Scan des gesamten Computers:



Scan-Einstellungen

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

- ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (

standardmäßig deaktiviert) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

- ***In Archiven scannen*** (*standardmäßig deaktiviert*) – 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*** (*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.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wird*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die kaum einer Infektion zum Opfer fallen. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

Außerdem sollten Sie entscheiden, welche Elemente gescannt werden

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen (*beim Speichern werden ändern sich die Kommata in Semikola*), die nicht gescannt werden sollen;

- ***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.

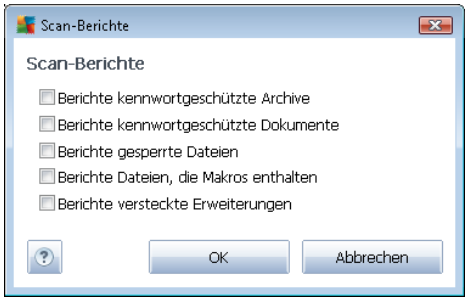
- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt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

Dauer des Scans anpassen

Im Bereich ***Dauer des Scans anpassen*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* 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.

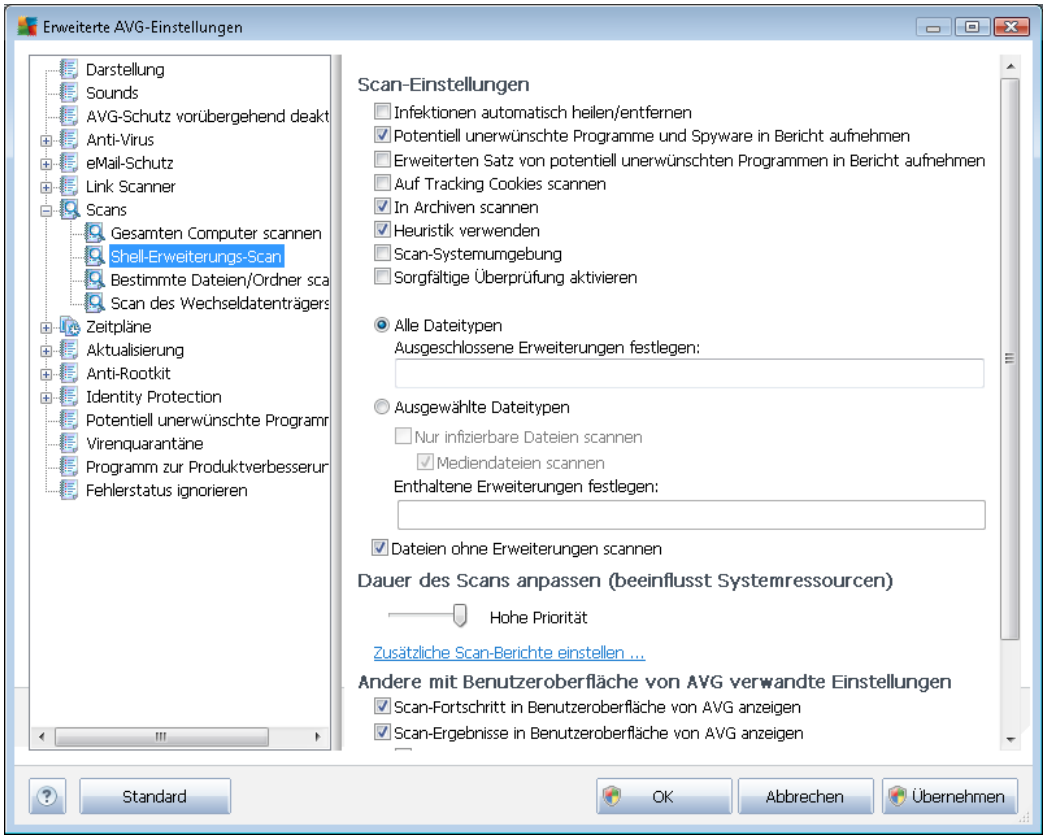
Zusätzliche Scan-Berichte einstellen ...

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:



9.7.2. Shell-Erweiterungs-Scan

Ähnlich der vorhergehenden Option Scan des gesamten Computers enthält die Option ***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:



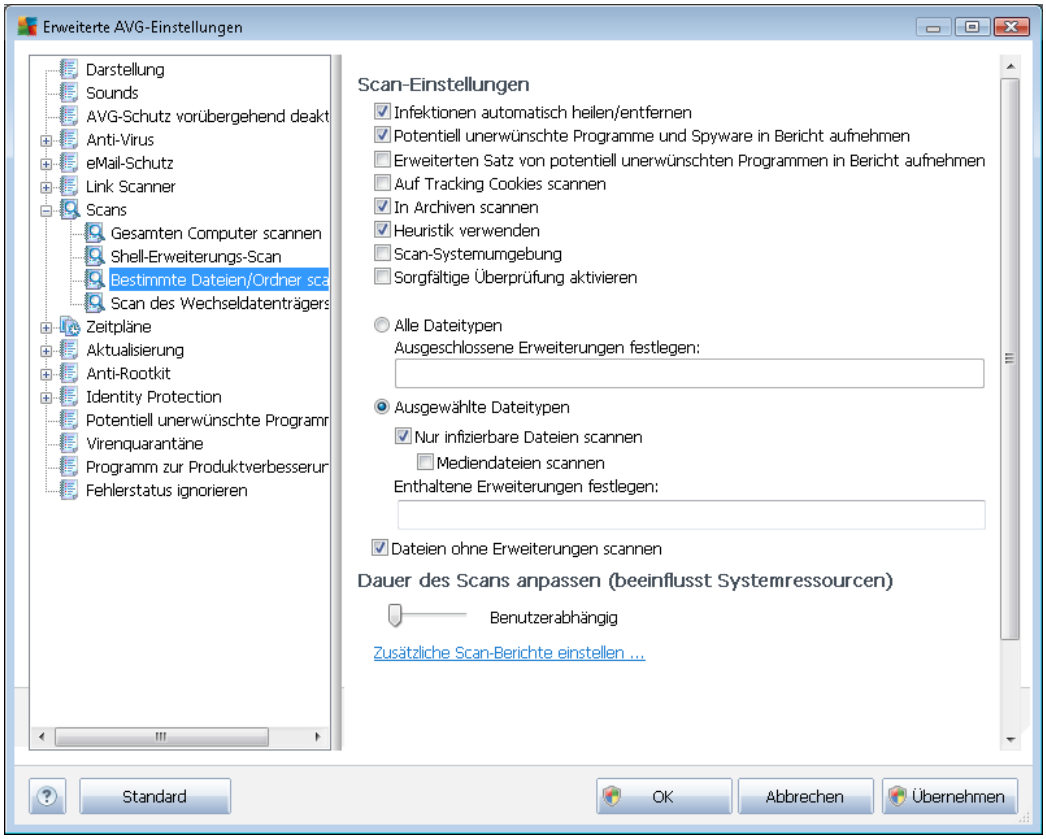
Die Parameterliste stimmt mit der Parameterliste der Option Gesamten Computer scannen überein. Die Standardeinstellungen unterscheiden sich jedoch: (*Während beim Scan des gesamten Computers standardmäßig keine Archive, aber die Systemumgebung gescannt wird, verhält es sich beim Shell-Extension-Scan umgekehrt*).

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel Erweiterte Einstellungen von AVG/ Scans/Scan des gesamten Computers.*

Im Vergleich zum Dialog Scan des gesamten Computers enthält der Dialog ***Shell-Erweiterungs-Scan*** auch den Bereich ***Andere Einstellungen bezüglich der Benutzeroberfläche von AVG***, in dem Sie festlegen können, dass der Scan-Fortschritt und die Scan-Ergebnisse auch über die Benutzeroberfläche von AVG aufgerufen werden können. Sie können außerdem festlegen, dass Scan-Ergebnisse nur bei einer beim Scan erkannten Infektion angezeigt werden sollen.

9.7.3. Bestimmte Dateien/Ordner scannen

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

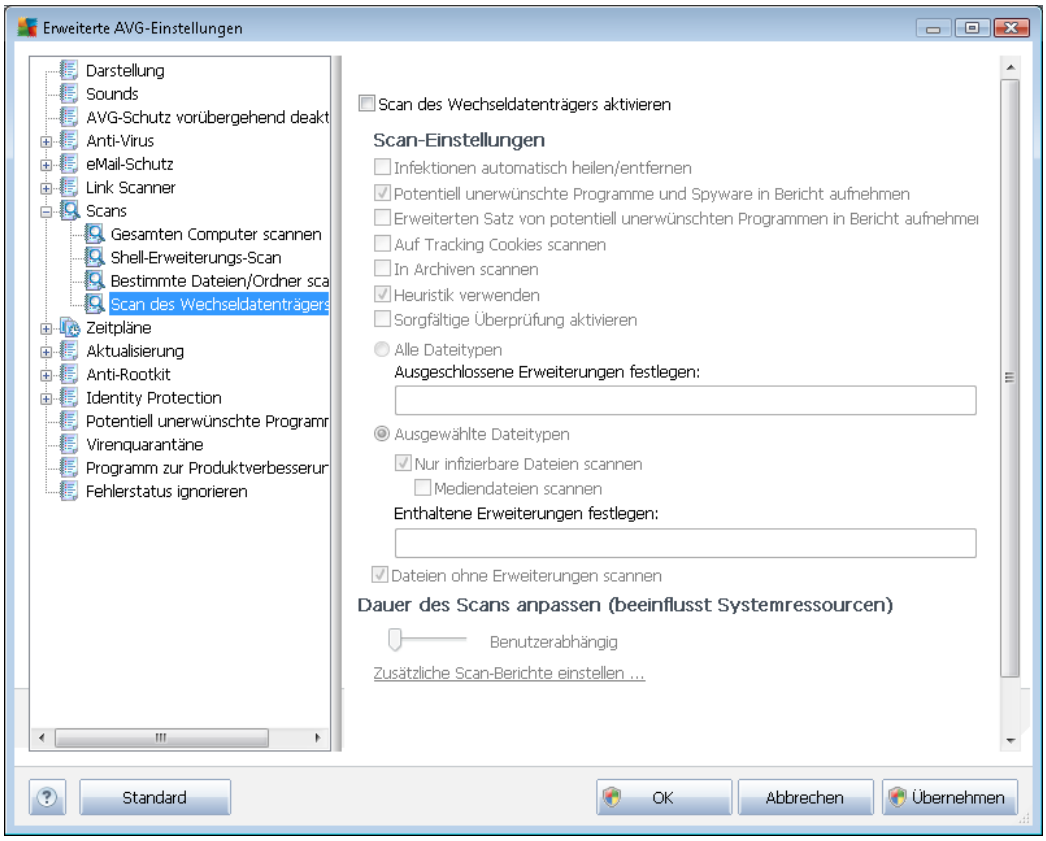


Alle Parameter, die in diesem Konfigurationsdialog festgelegt werden, gelten nur für die Scan-Bereiche, die unter der Option Bestimmte Dateien oder Ordner scannen ausgewählt wurden!

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel Erweiterte Einstellungen von AVG/ Scans/Scan des gesamten Computers.*

9.7.4. Scan des Wechseldatenträgers

Die Bearbeitungsoberfläche für die Option ***Scan des Wechseldatenträgers*** ist auch dem Bearbeitungsdialog der Option Scan des gesamten Computers 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 Erweiterte Einstellungen von AVG/Scans/Scan des gesamten Computers.*

9.8. Zeitpläne

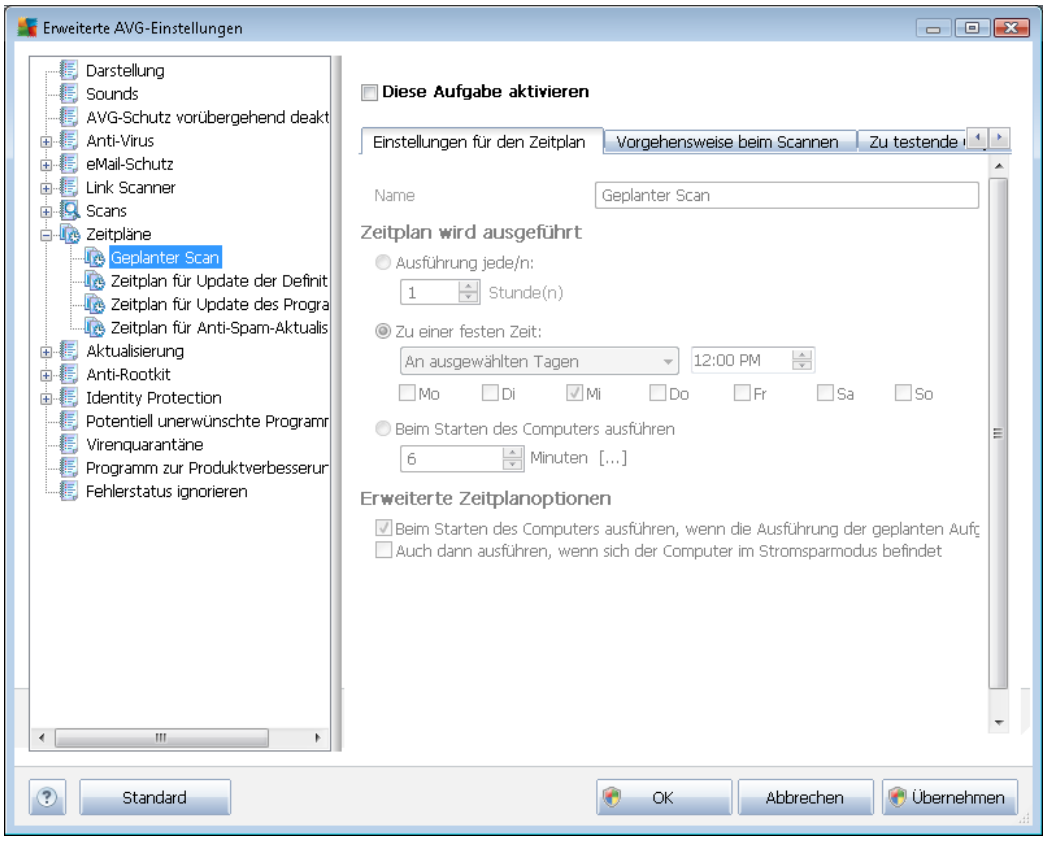
Im Bereich ***Zeitpläne*** können Sie die Standardeinstellungen für folgende Zeitpläne bearbeiten:

- Geplanter Scan
- Zeitplan für Update der Definitionen
- Zeitplan für Update des Programms

- Zeitplan für Anti-Spam-Aktualisierung

9.8.1. Geplanter Scan

Auf drei Reitern können die Parameter für den geplanten Scan bearbeitet (*oder ein neuer Zeitplan erstellt*) werden. Sie können den Eintrag ***Diese Aufgabe aktivieren*** auf jedem Reiter aktivieren oder deaktivieren, um den geplanten Test vorübergehend zu deaktivieren. Anschließend können Sie den Eintrag bei Bedarf hier 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.*

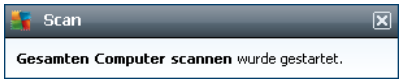
In diesem Dialog können Sie weiterhin folgende Parameter für den Scan festlegen:

Zeitplan wird ausgeführt

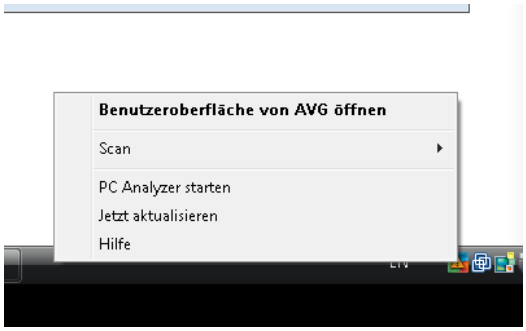
Hier können Sie die Zeitintervalle für den Start des neu geplanten Scans festlegen. Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum ausführen (***Ausführung jede/n ...***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit ...***) oder ein Ereignis festlegen,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

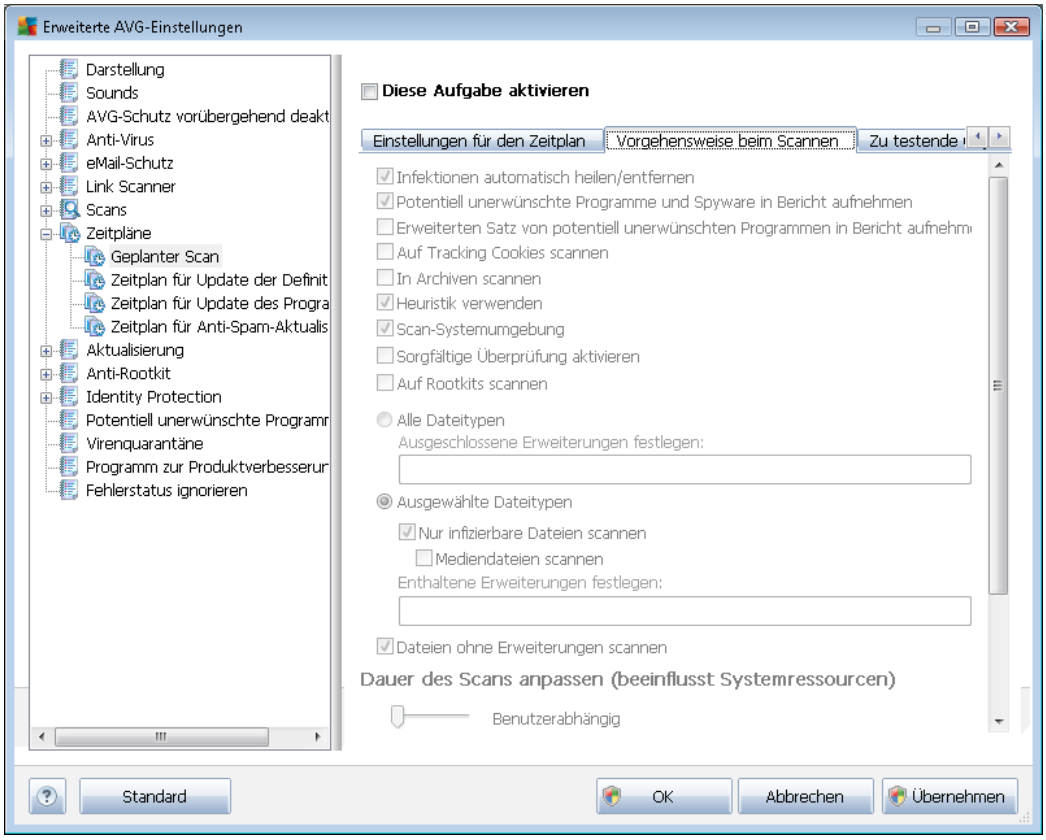
Erweiterte Zeitplanoptionen

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 einer Ampel*), das Sie darauf hinweist, dass gerade ein geplanter Scan durchgeführt wird. Klicken Sie mit der rechten Maustaste auf das AVG-Symbol für einen laufenden Scan, um ein Kontextmenü zu öffnen, über das Sie den Scan unterbrechen oder auch anhalten können sowie die Priorität des momentan ausgeführten Scans ändern 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, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert):* Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres

Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*): Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*)

- ***In Archiven scannen*** (*standardmäßig deaktiviert*): 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*** (*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.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***Auf Rootkits scannen*** (*standardmäßig deaktiviert*): 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 vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen (*beim Speichern ändern sich die Kommata in Semikola*), die nicht gescannt werden sollen;

- ***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.

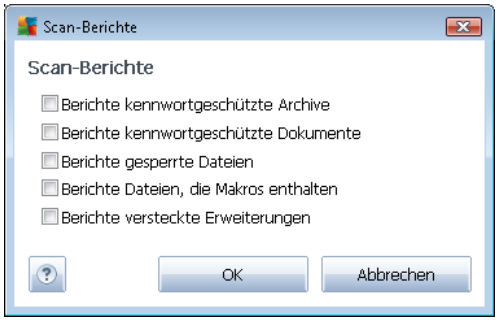
- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt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

Dauer des Scans anpassen

Im Bereich ***Dauer des Scans anpassen*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* 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.

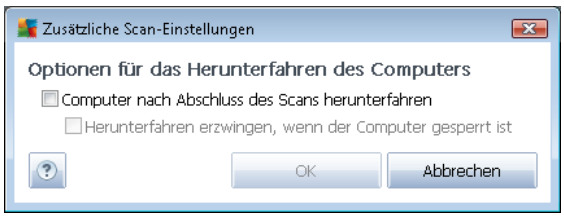
Zusätzliche Scan-Berichte einstellen

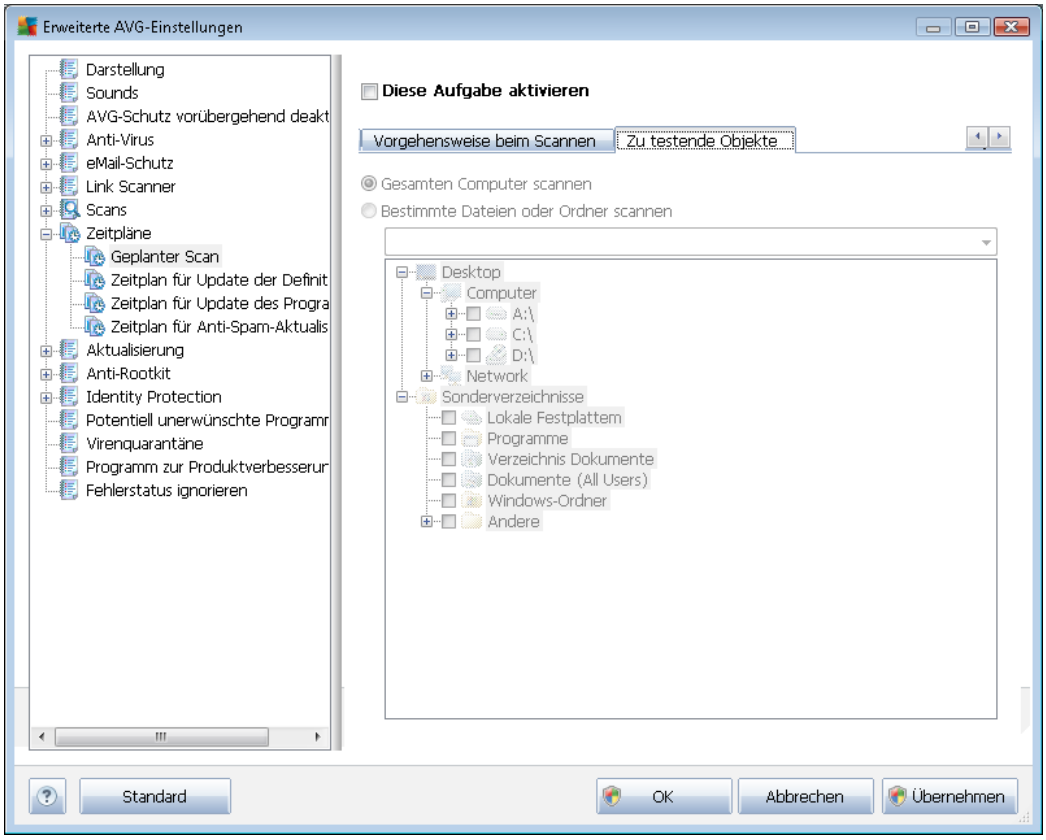
Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen ...***, um den separaten Dialog ***Scan-Berichte*** zu öffnen, wo Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



Zusätzliche Scan-Einstellungen

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***).

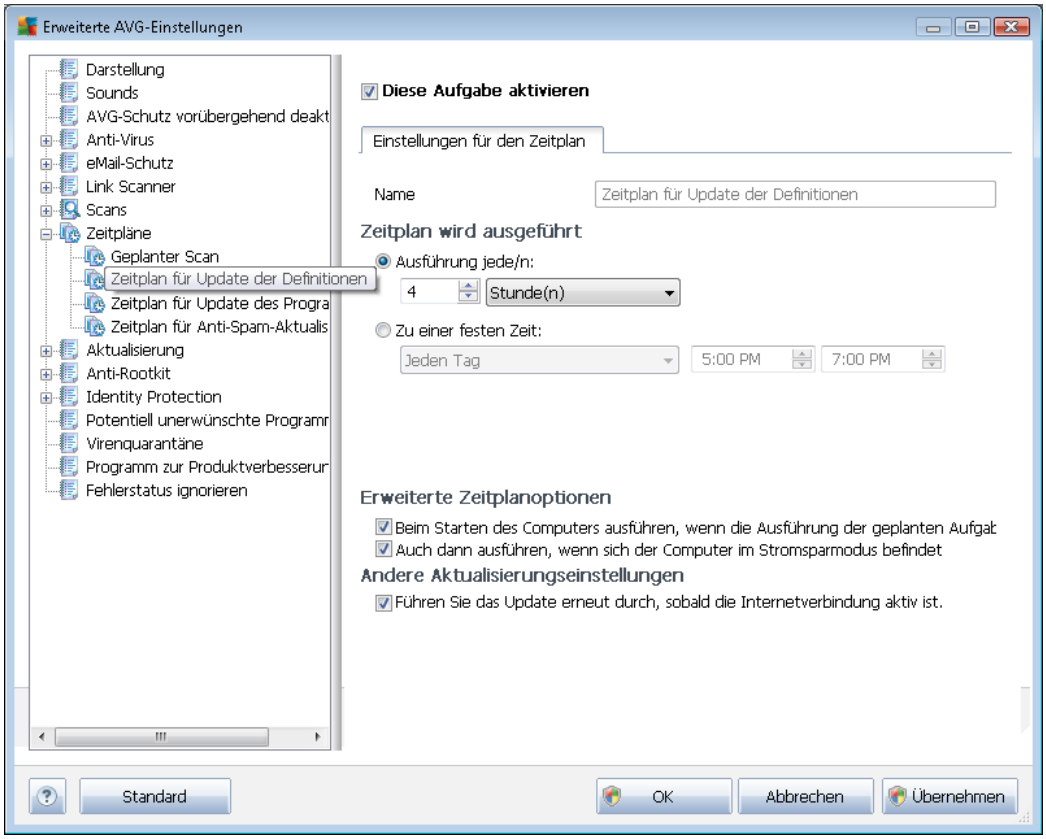




Auf dem Reiter ***Scan-Umfang*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien oder Ordner scannen planen möchten. Wenn Sie die Option „Bestimmte Dateien oder Ordner scannen“ auswählen, wird im unteren Bereich dieses Dialogs die angezeigte Baumstruktur aktiviert,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

9.8.2. Zeitplan für Update der Definitionen

Falls ***wirklich erforderlich***, können Sie den Eintrag ***Diese Aufgabe aktivieren*** deaktivieren, um das geplante Update der Definitionen vorübergehend zu deaktivieren bzw. später erneut zu aktivieren:



In diesem Dialog können Sie genauere Parameter für den Zeitplan des Definitionsupdates festlegen. Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

Zeitplan wird ausgeführt

Legen Sie in diesem Bereich die Zeitintervalle fest, in denen das neu geplante Update der Definitionen durchgeführt werden soll.
Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum (***Ausführung jede/n ...***) oder ein genaues Datum und eine Uhrzeit (***Ausführung zu einer bestimmten Zeit ...***) festlegen.

Erweiterte Zeitplanoptionen

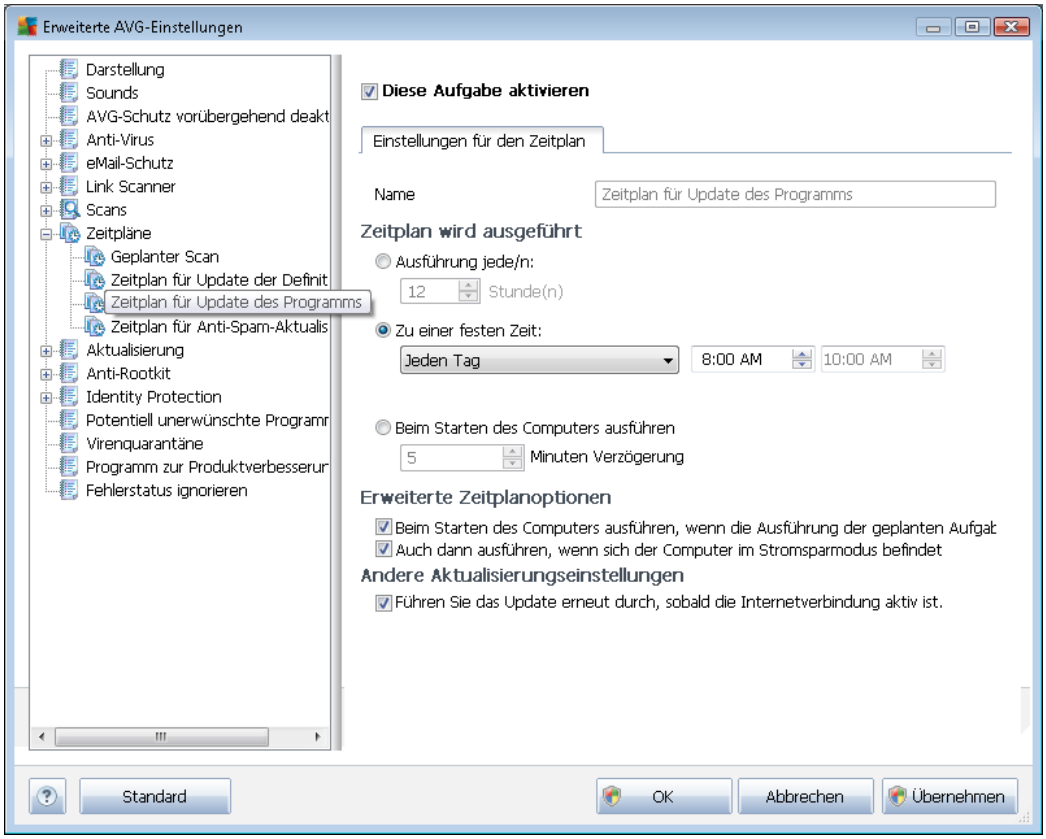
In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen das Update der Definitionen gestartet werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder komplett ausgeschaltet ist).

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

9.8.3. Zeitplan für Update des Programms

Falls ***wirklich erforderlich***, können Sie den Eintrag ***Diese Aufgabe aktivieren*** deaktivieren, um das geplante Programm-Update vorübergehend zu deaktivieren bzw. später erneut zu aktivieren:



Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

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).

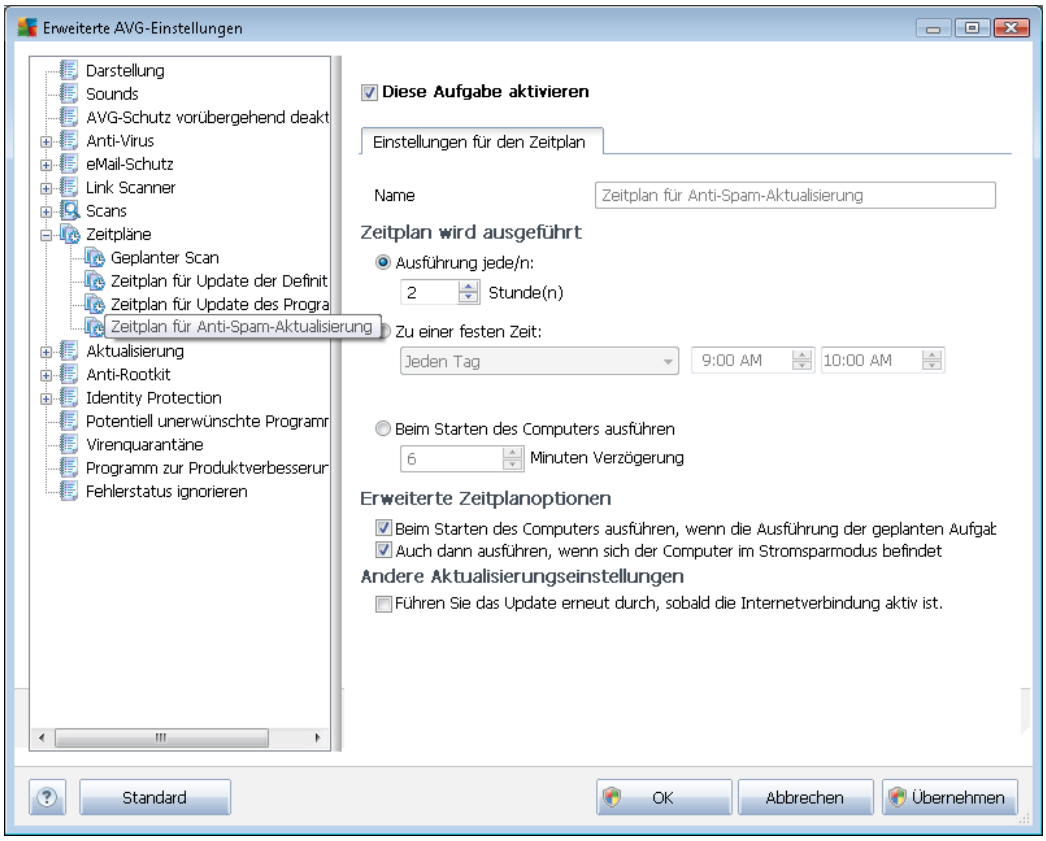
Andere Aktualisierungseinstellungen

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 darüber in einem Popup-Fenster informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog Erweiterte Einstellungen/Darstellung beibehalten)*.

Hinweis: *Wenn sich ein geplantes Programm-Update und ein geplanter Scan zeitlich überschneiden, wird der Scan unterbrochen, da das Update eine höhere Priorität hat.*

9.8.4. Zeitplan für Anti-Spam-Aktualisierung

Falls wirklich erforderlich, können Sie den Eintrag ***Diese Aufgabe aktivieren*** deaktivieren, um das geplante Update für Anti-Spam vorübergehend zu deaktivieren bzw. später erneut zu aktivieren:



In diesem Dialog können Sie genauere Parameter für den Updatezeitplan festlegen. Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

Zeitplan wird ausgeführt

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

Erweiterte Zeitplanoptionen

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

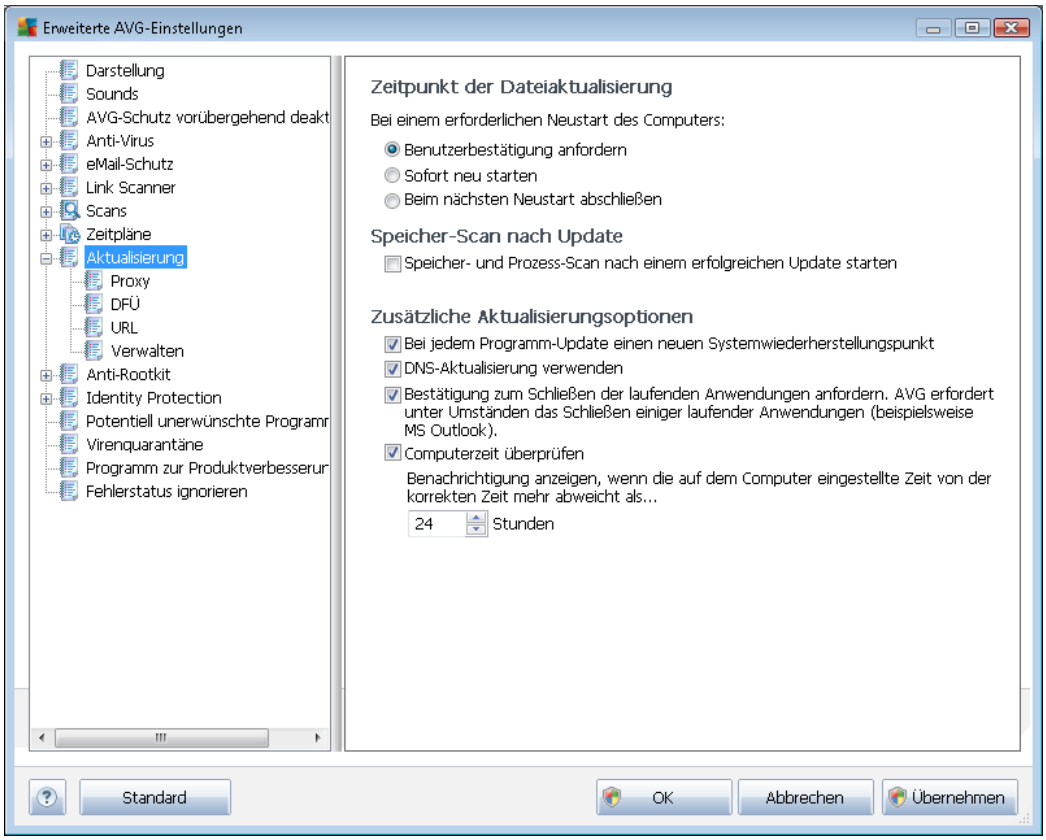
Andere Aktualisierungseinstellungen

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

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

9.9. Aktualisierung

Mit dem Navigationselement ***Update*** 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 drei alternativen Optionen wählen, wenn der Update-Vorgang einen Neustart des Computers erfordert. Der Abschluss des Updates kann für den nächsten Neustart des Computers geplant werden, oder Sie können den Neustart sofort durchführen:

- ***Benutzerbestätigung anfordern*** *(standardmäßig aktiviert)*– Sie werden aufgefordert, den Neustart Ihres Computers zu bestätigen, um den Updatevorgang abzuschließen

- ***Sofort neu starten*** – der Computer wird automatisch neu gestartet, unmittelbar nachdem der Updatevorgang abgeschlossen ist. Sie müssen den Neustart nicht bestätigen.

- ***Beim nächsten Neustart abschließen*** – der Abschluss des Updatevorgangs 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

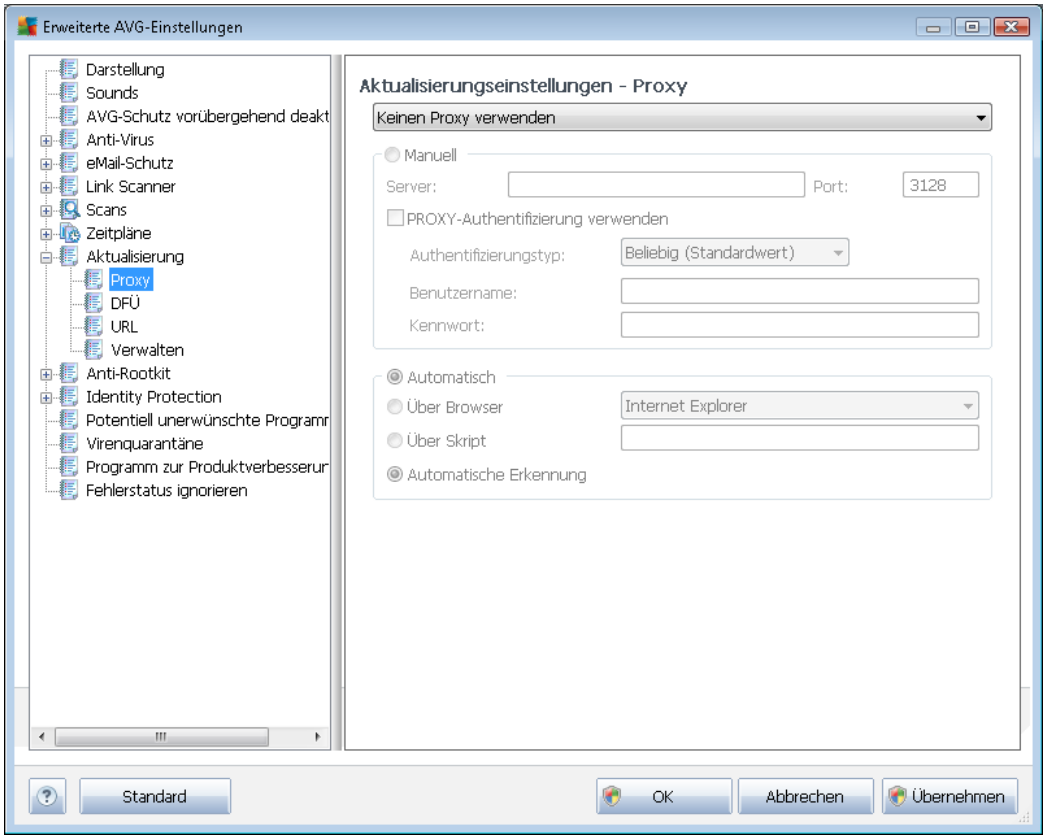
- ***Bei jedem Programmupdate einen neuen Systemwiederherstellungspunkt erstellen*** – Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen 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-Update verwenden*** (*Standard*) – Ist diese Option aktiviert, sucht Ihr **AVG Internet Security 2012** die Informationen der neuesten Version der Virendatenbank auf dem DNS-Server, sobald das Update gestartet wird. Dann werden nur die kleinsten unabdingbar erforderlichen Aktualisierungsdateien heruntergeladen und ausgeführt. Auf diese Weise wird die heruntergeladene Datenmenge auf einem Minimum gehalten und der Aktualisierungsprozess ist schneller.

- ***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.

9.9.1. 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***
- ***Proxy nicht verwenden*** – Standardeinstellungen
- ***Stellen Sie eine direkte Verbindung her, wenn eine Proxy-Verbindung fehlschägt***

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.

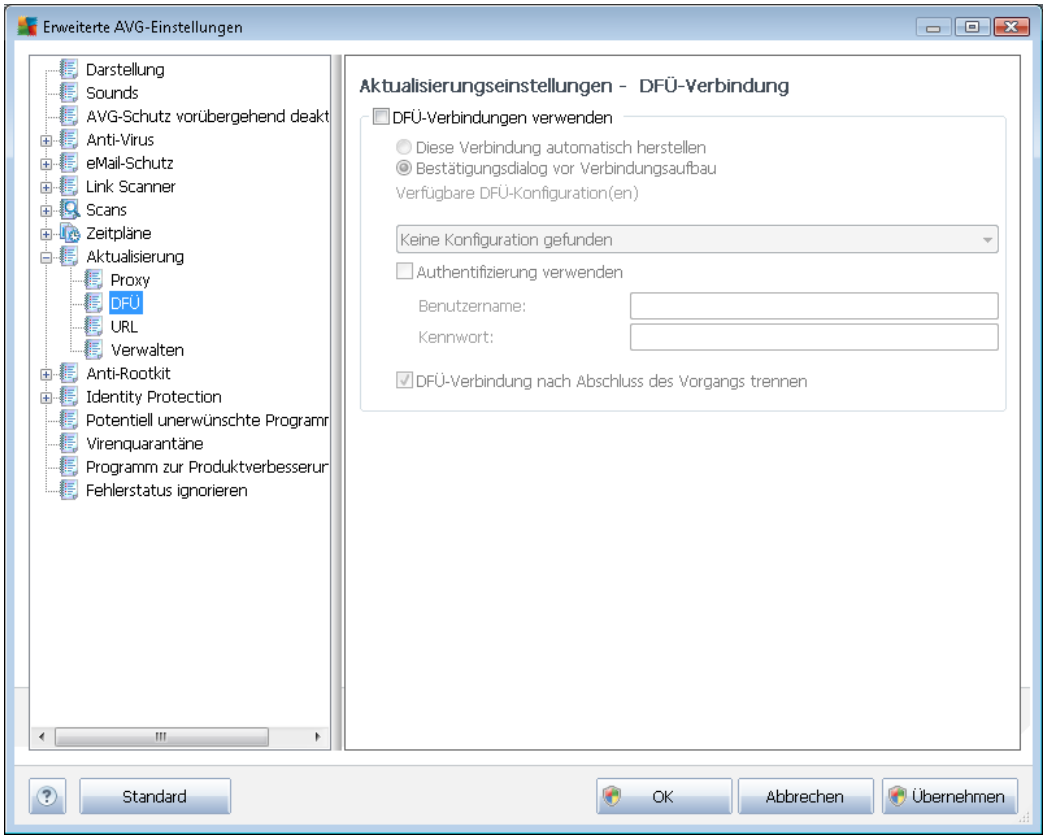
Automatische Konfiguration

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

9.9.2. DFÜ

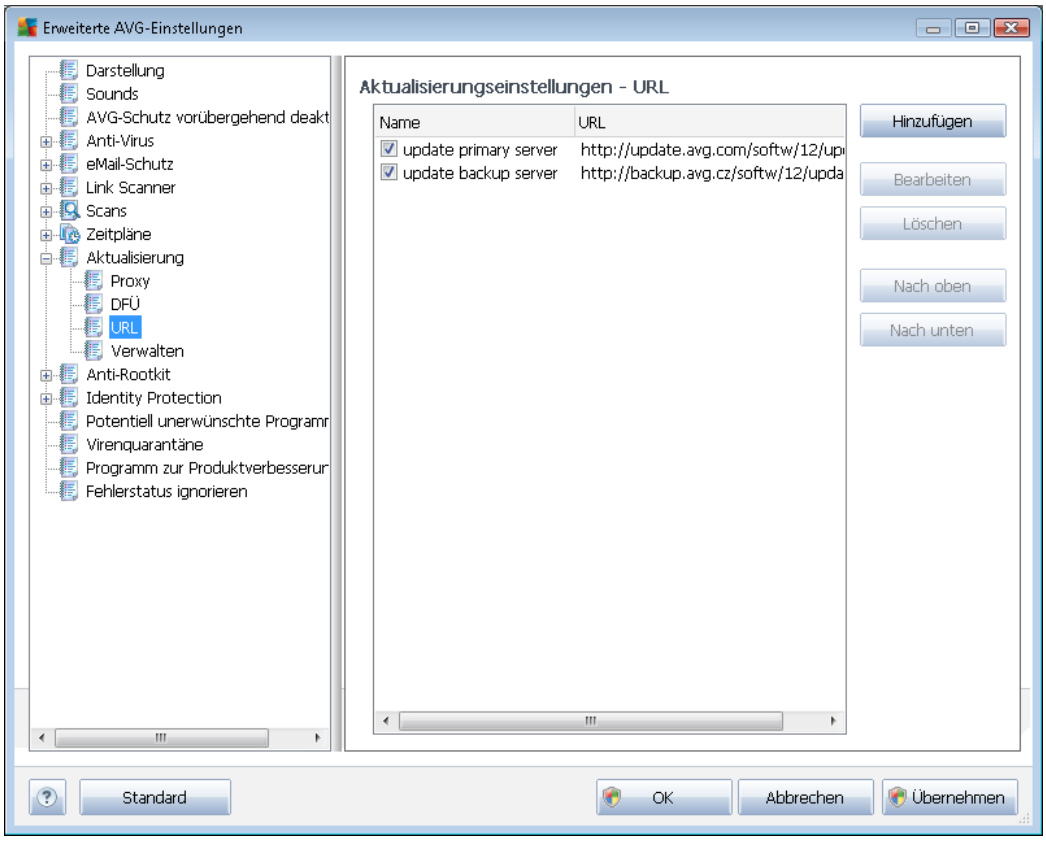
Die optional im Dialog ***Aktualisierungseinstellungen – DFÜ-Verbindung*** definierten Parameter beziehen sich auf die Einwahlverbindung mit dem Internet. Die Felder des Dialogs werden erst aktiviert, wenn Sie die Option ***DFÜ-Verbindungen verwenden*** auswählen:



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***).

9.9.3. URL

Der Dialog ***URL*** zeigt eine Liste von Internetadressen an, von denen Updates heruntergeladen werden können:



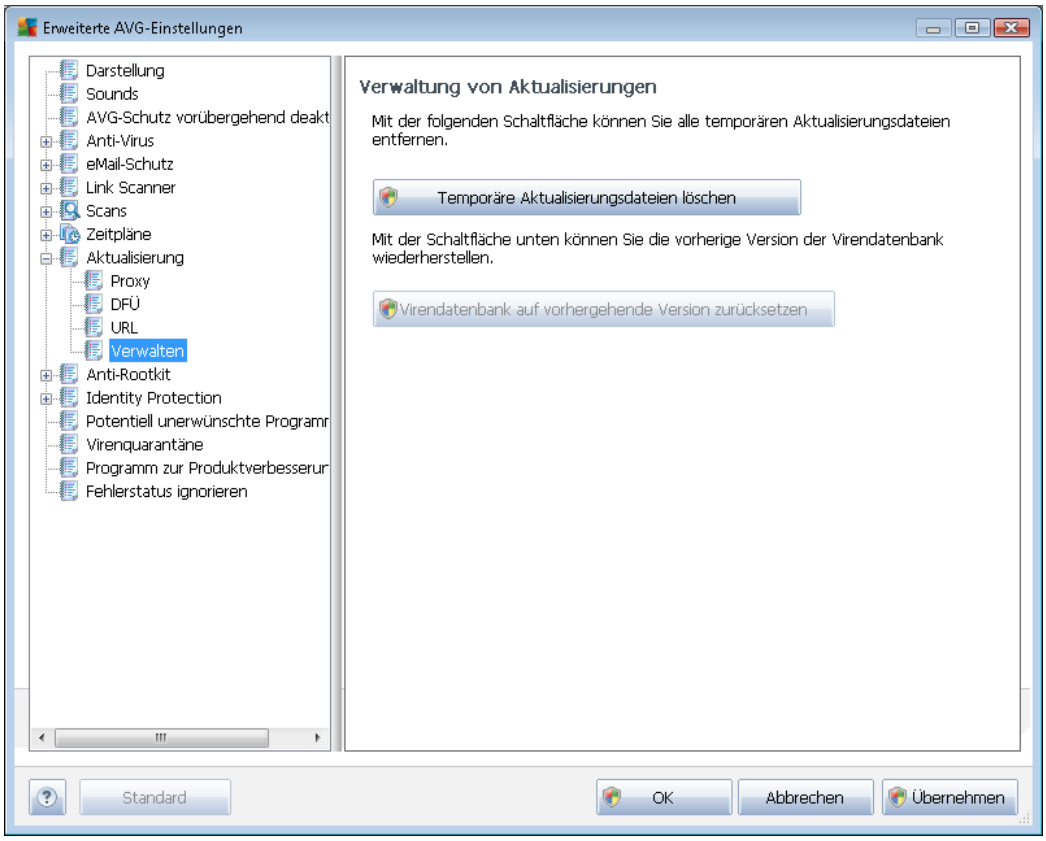
Schaltflächen

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

9.9.4. Verwalten

Im Dialog ***Verwaltung von Aktualisierungen*** stehen zwei Optionen über zwei Schaltflächen zur Verfügung:

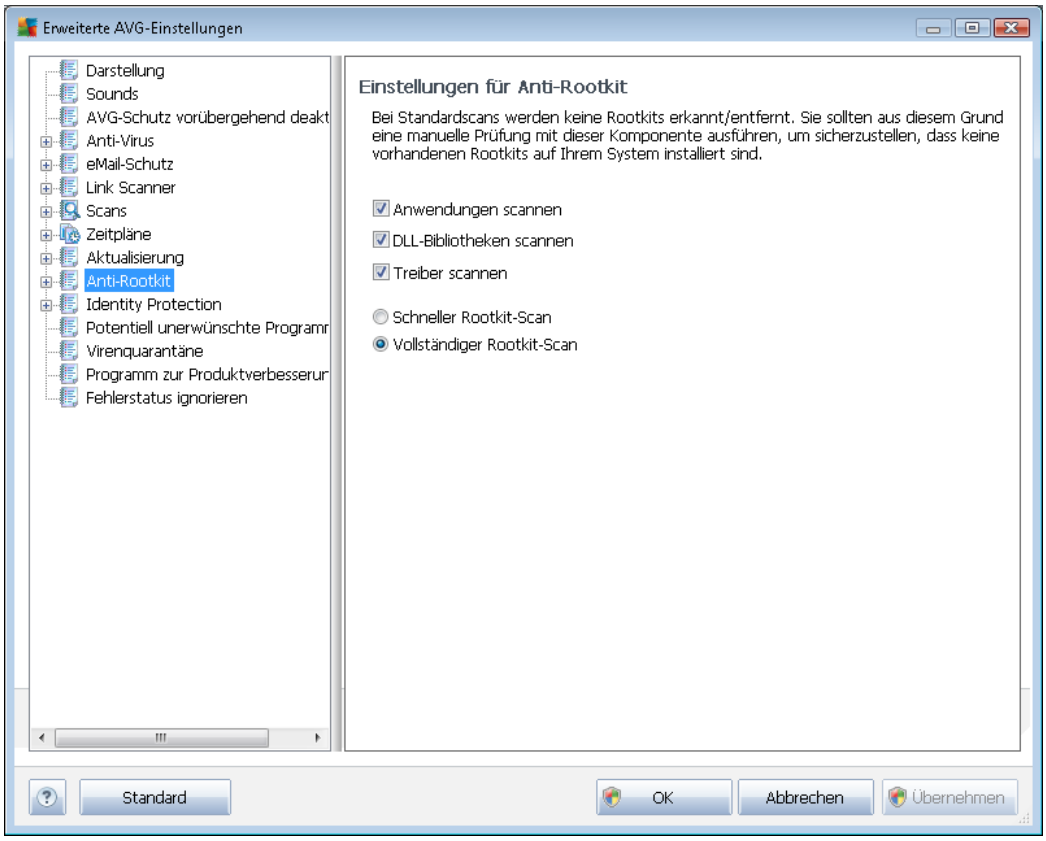


- ***Temporäre Aktualisierungsdateien löschen*** – Klicken Sie auf diese Schaltfläche, wenn Sie alle redundanten Update-Dateien von Ihrer Festplatte löschen möchten (*standardmäßig werden diese Dateien 30 Tage gespeichert*)

- ***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*)

9.10. Anti-Rootkit

Im Dialog ***Einstellungen für Anti-Rootkit*** 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***

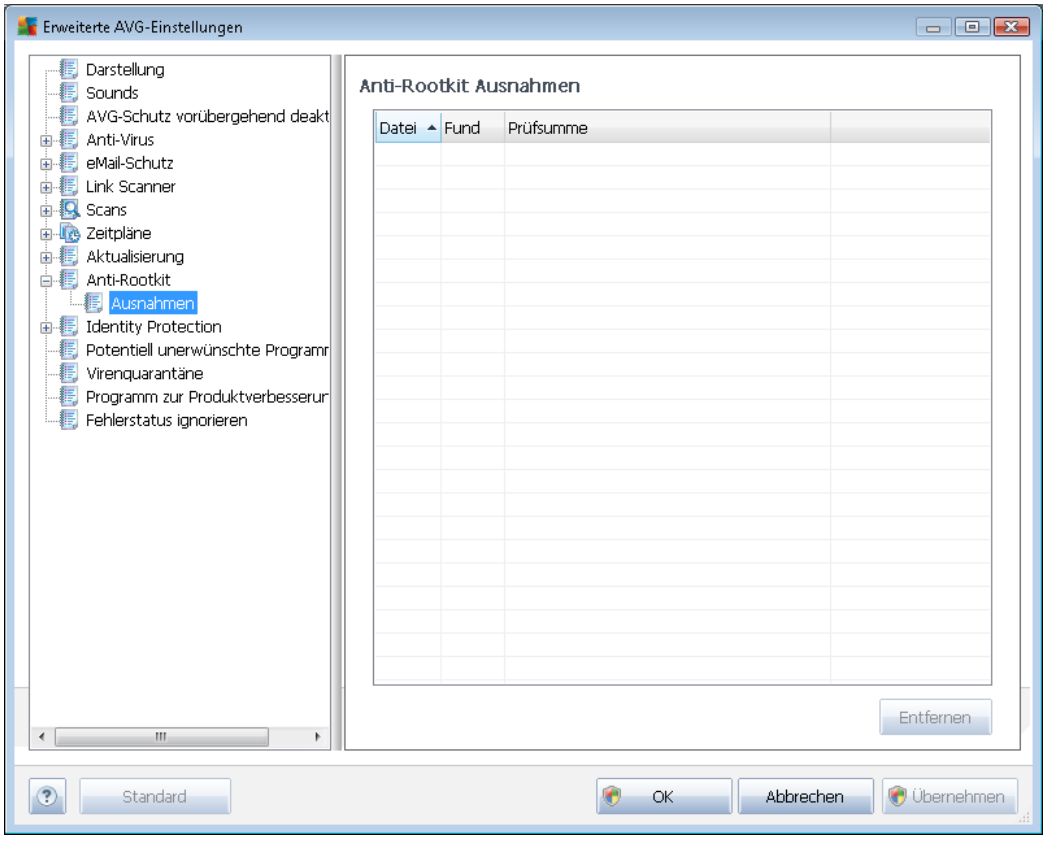
Wählen Sie anschließend den Rootkit-Scanmodus aus:

- ***Schneller Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber und den Systemordner (*typischerweise C:\WINDOWS*)
- ***Vollständiger Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber, den Systemordner (*typischerweise C:\WINDOWS*) und zusätzlich alle lokalen Festplatten (

einschließlich Flash-Disks, aber keine Disketten-/CD-Laufwerke)

9.10.1. Ausnahmen

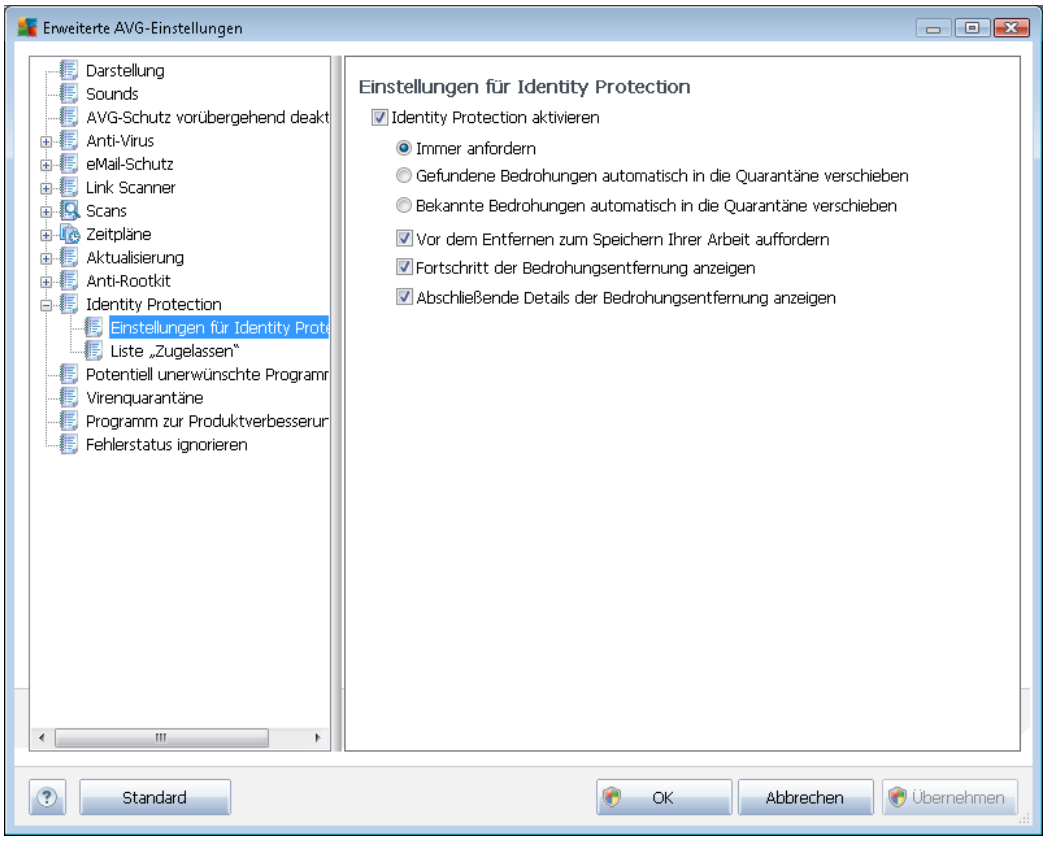
Im Dialog ***Anti-Rootkit-Ausnahmen*** können Sie bestimmte Dateien definieren *(z. B. einige Treiber, die fälschlicherweise als Rootkit erkannt werden können)*, die von diesem Scan ausgeschlossen werden sollen:



9.11. Identitätsschutz

9.11.1. Einstellungen des Identitätsschutzes

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



Identitätsschutz aktivieren (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, um die Komponente Identitätsschutz zu deaktivieren.

Es wird dringend empfohlen, dies nur in Ausnahmesituationen zu tun!

Wenn Identitätsschutz aktiviert ist, können Sie festlegen, was im Falle einer erkannten Bedrohung geschehen soll:

- ***Immer anfordern*** (*standardmäßig aktiviert*) – Sie werden 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.
- ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** – Aktivieren Sie dieses Kontrollkästchen, um alle potentiell gefährlichen Bedrohungen umgehend in die sichere Virenquarantäne zu verschieben. 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.
- ***Bekannte Bedrohungen automatisch in die Quarantäne verschieben*** – Behalten Sie die

Aktivierung dieses Eintrags bei, wenn Sie möchten, dass alle Anwendungen mit Verdacht auf Malware automatisch und sofort in die Virenquarantäne verschoben werden sollen.

Darüber hinaus können Sie bestimmte Elemente zuweisen, die optional weitere Funktionen von Identitätsschutz aktivieren:

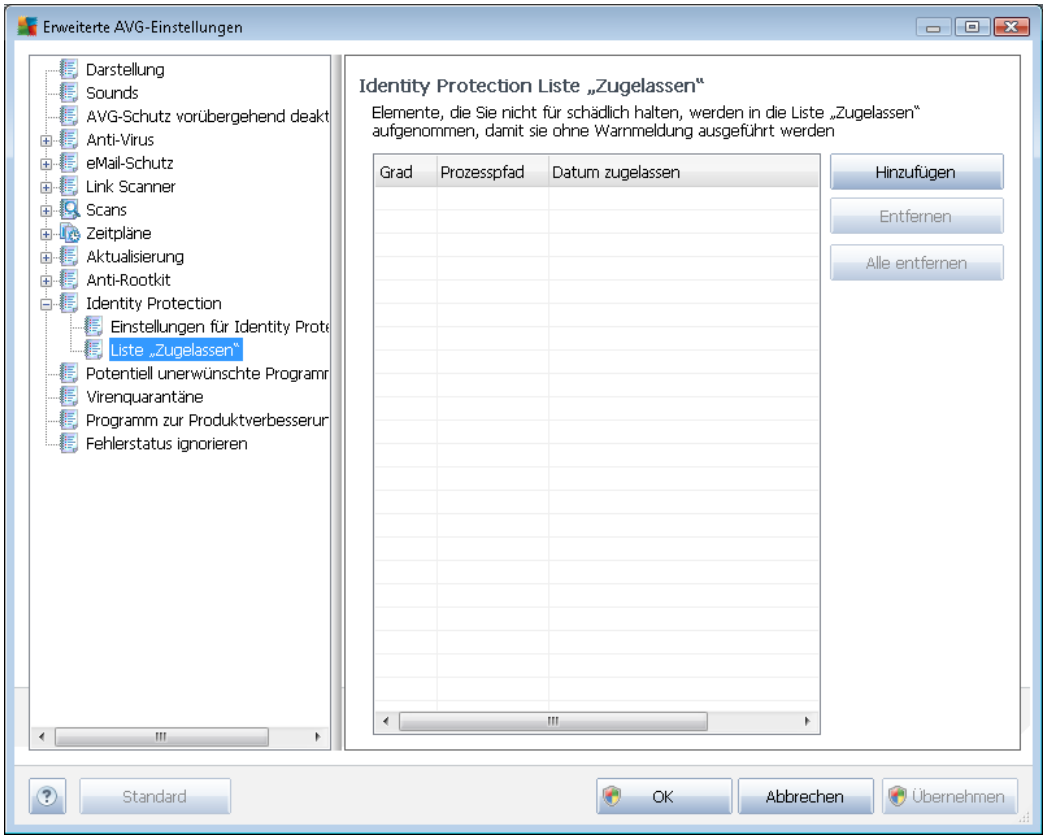
- ***Vor dem Entfernen zum Speichern Ihrer Arbeit auffordern*** (*standardmäßig aktiviert*) – Behalten Sie die Aktivierung dieses Eintrags bei, wenn Sie eine Warnung für eine Anwendung mit Verdacht auf Malware erhalten möchten, bevor diese in die Virenquarantäne verschoben wird. Wenn Sie gerade mit der Anwendung arbeiten, könnte Ihr Projekt verlorengehen, und Sie müssen es zuerst speichern. Dieser Eintrag ist standardmäßig aktiviert, und wir empfehlen, diese Einstellung beizubehalten.

- ***Fortschritt der Malware-Entfernung anzeigen*** – (*standardmäßig aktiviert*) – wenn dieser Eintrag aktiviert ist, wird bei Erkennung einer potentiellen Malware ein neuer Dialog geöffnet, der Fortschritt beim Verschieben der Malware in die Virenquarantäne angezeigt.

- ***Abschließende Details der Malware-Entfernung anzeigen*** (*standardmäßig aktiviert*) – Wenn dieser Eintrag aktiviert ist, zeigt ***Identitätsschutz*** detaillierte Informationen für jedes Objekt an, das in die Virenquarantäne verschoben wird (*Schweregrad, Speicherort usw.*).

9.11.2. 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 so genannten ***Liste „Zugelassen" in Identitätsschutz*** hinzugefügt und nicht mehr als potentiell gefährlich gekennzeichnet:



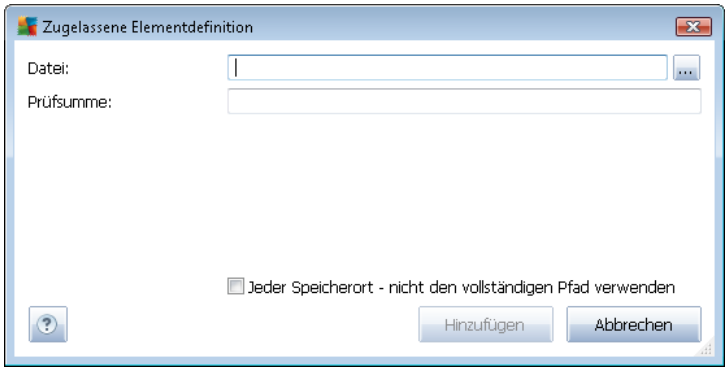
Die ***Liste „Zugelassen“ in Identitätsschutz*** enthält für jede Anwendung die folgenden Informationen:

- ***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“ in Identitätsschutz***stehen folgende 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.

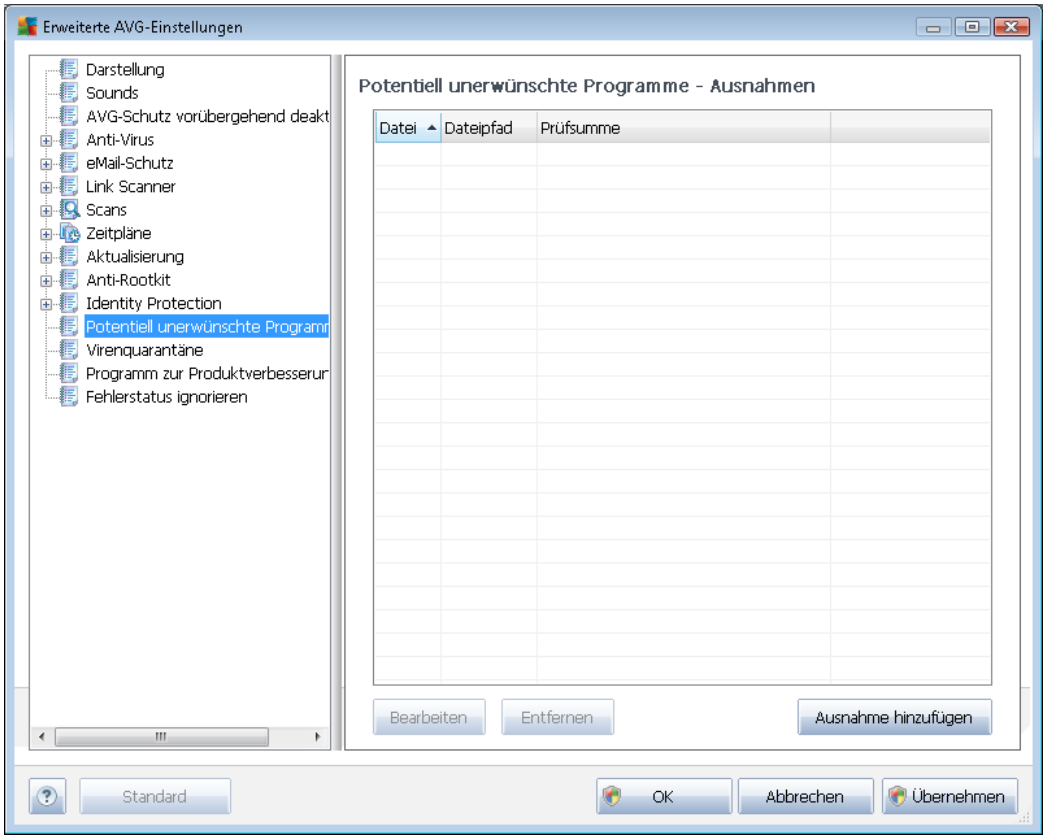
- Jeder Speicherort – nicht den vollständigen Pfad verwenden – Wenn Sie diese Datei nur für diesen bestimmten Speicherort als Ausnahme festlegen möchten, lassen Sie das Kontrollkästchen deaktiviert

- ***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

9.12. Potentiell unerwünschte Programme

AVG Internet Security 2012 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. Solche Adware wird möglicherweise von **AVG Internet Security 2012** als *potentiell unerwünschtes Programm* erkannt und gemeldet. Wenn Sie ein derartiges Programm auf Ihrem Computer behalten möchten, können Sie es als Ausnahme eines potentiell unerwünschten Programms definieren:



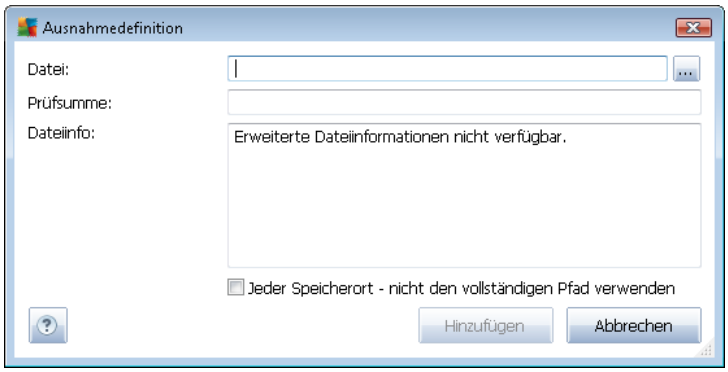
Im Dialog ***Potentiell unerwünschten Programmen - Ausnahmen*** wird eine Liste der bereits definierten und aktuell gültigen Ausnahmen an potentiell unerwünschten Programmen angezeigt. Sie können die Liste bearbeiten, vorhandene Einträge löschen oder neue Ausnahmen hinzufügen. Für jede einzelne Ausnahme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

- ***Datei*** – Gibt den genauen 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:



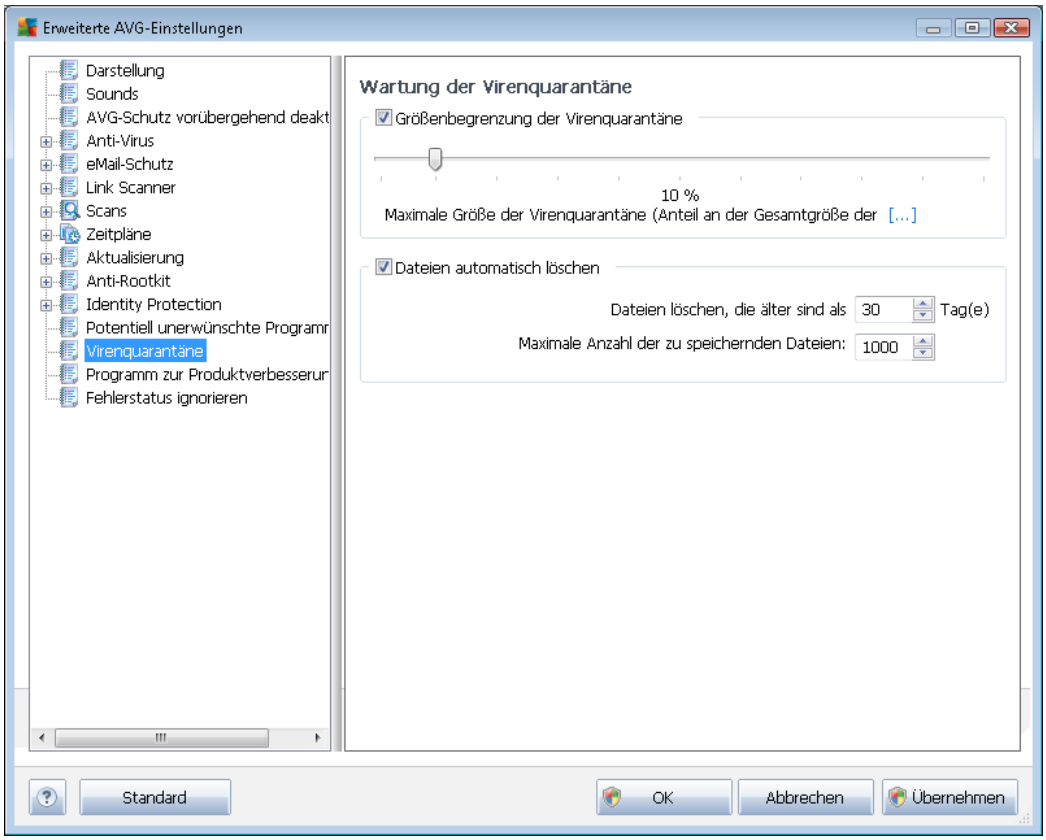
- ***Datei*** – Geben Sie den vollständigen Pfad zu der Datei ein, die Sie als Ausnahme definieren möchten

- ***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. Wenn das Kontrollkästchen aktiviert ist, wird die angegebene Datei (unabhängig von ihrem Speicherort) als Ausnahme definiert *(Sie müssen trotzdem den vollständigen Pfad der Datei angeben; die Datei wird dann als Beispiel dafür verwendet, dass sich zwei Dateien mit demselben Namen auf Ihrem System befinden können)*.

9.13. 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.

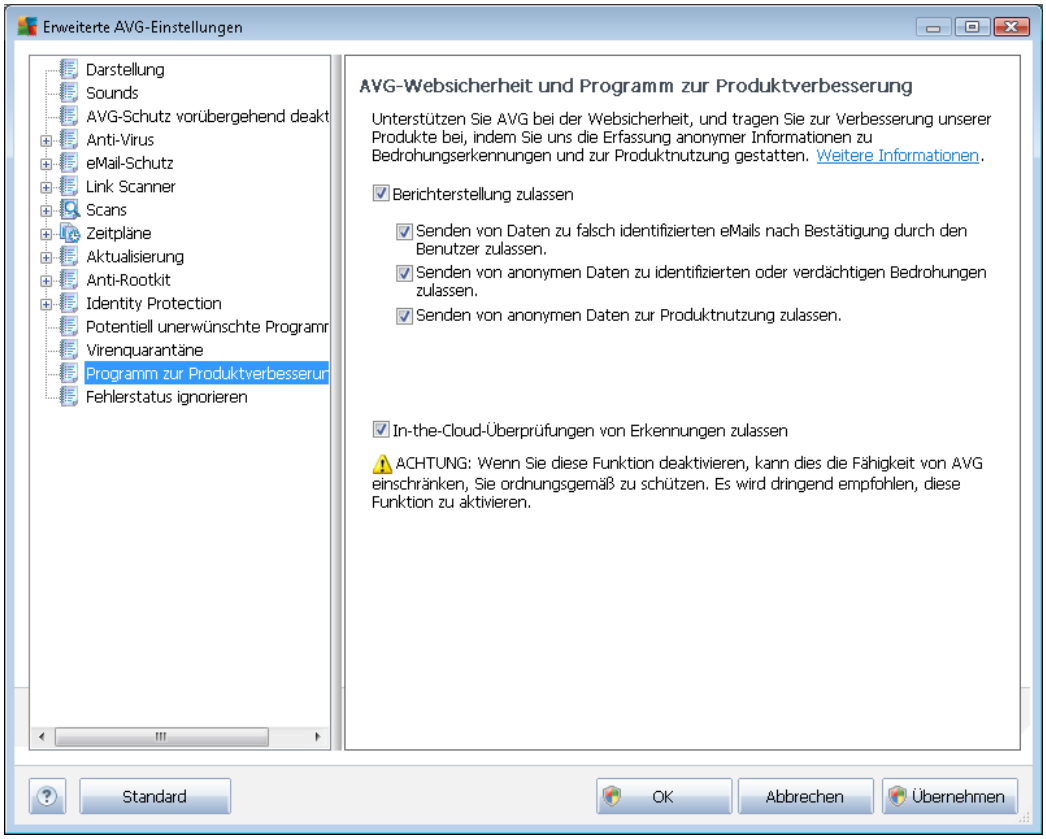
- ***Dateien automatisch löschen*** – In diesem Bereich wird die maximale Dauer festgelegt, die Objekte in der Virenquarantäne gespeichert werden (***Dateien löschen, die älter sind als ... Tage***), und die maximale Anzahl der in der Virenquarantäne gespeicherten Dateien (***Maximale Anzahl der zu speichernden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

9.14. Programm zur Produktverbesserung

Der Dialog ***AVG-Websicherheit und Programm zur Produktverbesserung*** lädt Sie zur Teilnahme an der AVG-Produktverbesserung ein, wodurch Sie uns bei der Verbesserung der allgemeinen Internetsicherheit unterstützen. Behalten Sie die Markierung der Option ***Berichterstellung zulassen*** bei, um die Berichterstattung über erkannte Bedrohungen an die AVG-Labore zu aktivieren. Auf diese Weise erhalten wir aktuelle Informationen über Bedrohungen von allen Benutzern auf der ganzen Welt und können im Gegenzug unseren Schutz für alle noch weiter verbessern.

Die Berichterstattung erfolgt automatisch und ohne Beeinträchtigungen. In den Berichten sind

keine persönlichen Daten enthalten. Die Berichterstattung über erkannte Bedrohungen ist optional; dennoch bitten wir Sie, die Aktivierung dieser Option beizubehalten. Sie hilft uns, den Schutz für Sie und andere Benutzer von AVG weiter zu verbessern.



Es gibt heutzutage weit mehr Bedrohungen als reine Viren. Urheber von schädlichen Codes und gefährlichen Websites zeigen sich stets einfallsreich, und neue Bedrohungen tauchen immer wieder auf, die meisten davon im Internet. Im Folgenden werden einige der häufigsten beschrieben:

- ***Ein Virus*** ist ein schädlicher Code, der sich selbst vervielfältigt und sich ohne Erlaubnis und Wissen der Benutzer auf Computern verbreitet und Schäden anrichtet. Einige Viren stellen ernstere Bedrohungen dar, da sie Dateien löschen oder manipulieren können; andere Viren hingegen sind eher harmlos und spielen beispielsweise nur eine Musikdatei ab. Unabhängig von der Gefährlichkeit können alle Viren jedoch aufgrund ihrer Fähigkeit zur Vervielfältigung rasch den gesamten Speicher in Beschlag nehmen und den Computer zum Absturz bringen.

- ***Würmer*** sind eine Unterkategorie von Viren, die jedoch kein Trägerobjekt zur Verbreitung benötigen. Sie verbreiten sich ohne Zutun des Benutzers. In aller Regel geschieht dies per eMail, und es kommt zu Überlastungen von eMail-Servern und Netzwerksystemen.

- ***Spyware*** ist eine Malware-Kategorie (*Malware = jede schädliche Software, einschließlich Viren*), eingebunden in Programme (üblicherweise Trojaner), die persönliche Informationen, Kennwörter, Kreditkartennummern stehlen oder in einen Computer eindringen und es dem Angreifer ermöglichen, die Kontrolle über den Computer zu übernehmen, natürlich ohne das

Wissen oder die Einwilligung des Computerbesitzers.

- ***Potentiell unerwünschte Programme*** sind eine Art Spyware, die eine Gefahr für Ihren Computer darstellen können, aber nicht müssen. Ein typisches Beispiel für ein PUP ist Adware, eine Software zur Verteilung von Werbung, die meist in störenden Popup-Fenstern angezeigt wird, aber keinen Schaden anrichten.

- ***Auch Tracking Cookies*** sind eine Art Spyware, da diese kleinen Dateien im Webbrowser gespeichert werden und automatisch an eine Stamm-Website gesendet werden, wenn diese Seite noch einmal besucht wird. Sie enthalten dann Daten wie das Surfverhalten und andere ähnlicher Informationen.

- ***Exploit*** ist ein gefährlicher Code, der Schlupflöcher oder Schwachstellen im Betriebssystem, Internetbrowser oder in anderen wichtigen Programmen ausnutzt.

- ***Mit Phishing*** bezeichnet man den Versuch, an sensible persönliche Daten heranzukommen, indem vorgetäuscht wird, dass es sich um eine vertrauenswürdige und bekannte Organisation handelt. Normalerweise werden die potentiellen Opfer über eine Massen-eMail gebeten, z. B. die Zugangsdaten zu ihrem Bankkonto zu aktualisieren. Sie sollen dazu dem angegebenen Link folgen, der sie dann auf eine gefälschte Website der Bank führt.

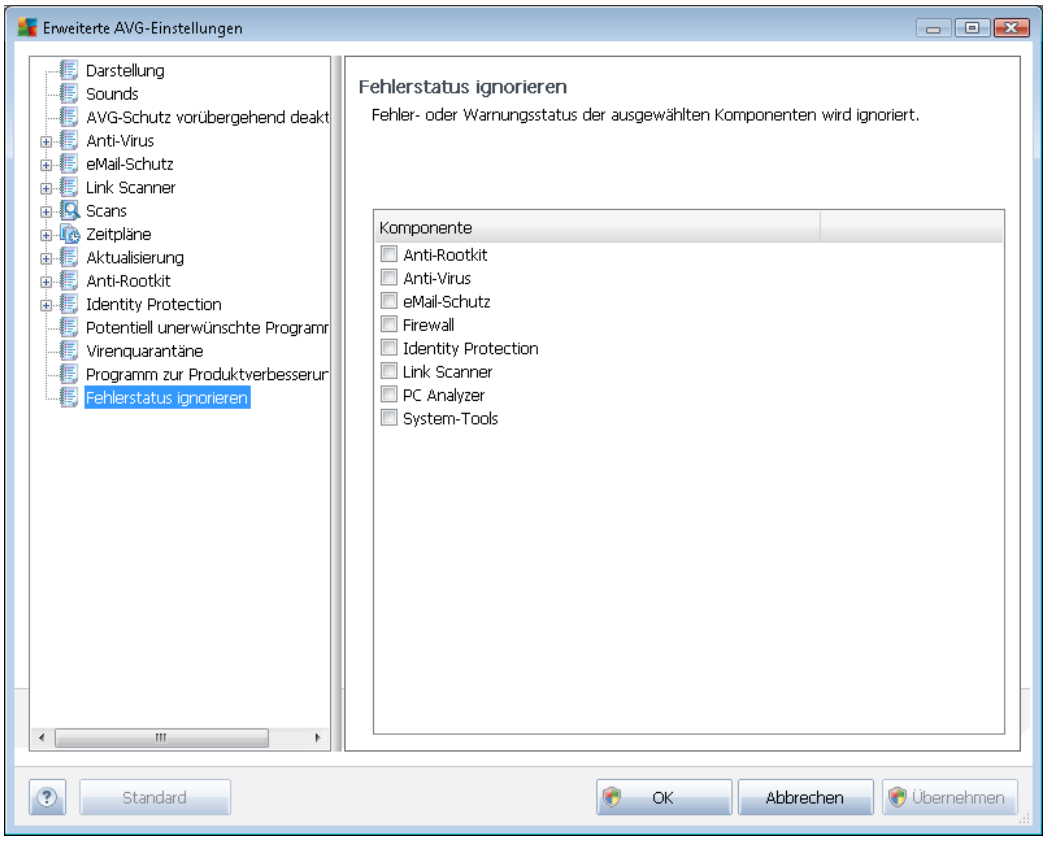
- ***Hoax bezeichnet eine Massen-eMail, die gefährliche, alarmierende oder einfach belästigende und nutzlose Informationen enthält.*** Viele der oben genannten Bedrohungen verwenden Hoax-eMails als Verbreitungsmethode.

- ***Verseuchte Websites*** sind Websites, durch die gefährliche Software auf Ihrem Computer installiert wird, sowie infizierte Seiten, die dasselbe tun, wobei es sich in diesem Fall um legitime Websites handelt, die beschädigt wurden und dazu benutzt werden, Besucher zu infizieren.

Um Sie vor diesen verschiedenen Bedrohungen zu schützen, bietet AVG Internet Security 2012 besondere Komponenten. Eine kurze Beschreibung der Komponenten finden Sie im Kapitel Komponentenübersicht.

9.15. Fehlerstatus ignorieren

Im Dialog ***Fehlerstatus 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.

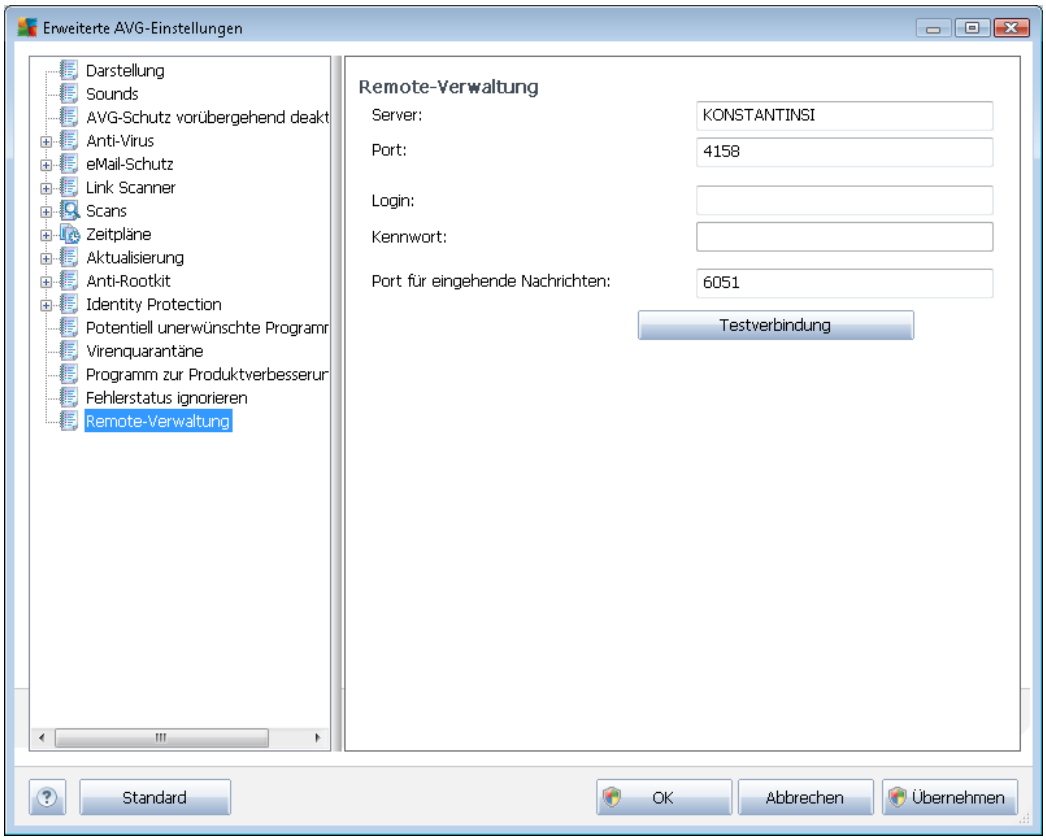
Es kann vorkommen, dass Sie aus bestimmten Gründen eine Komponente vorübergehend deaktivieren möchten. (*Die Deaktivierung einer Komponente wird nicht empfohlen. Achten Sie darauf, dass alle Komponenten aktiviert und die jeweiligen Standardeinstellungen vorgenommen sind*). In diesem Fall zeigt das Symbol 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. Dieselbe Option *(Komponentenstatus ignorieren)* steht auch für bestimmte Komponenten direkt über die Komponentenübersicht im Hauptfenster von AVG zur Verfügung.

9.16. Remote-Verwaltung

Der Eintrag ***Remote-Verwaltung*** und der entsprechende Dialog werden in der Navigationsstruktur nur angezeigt, wenn Sie Ihr **AVG Internet Security 2012** mit einer Lizenz für die AVG Business Edition installiert und während des Installationsvorgangs bestätigt haben, dass die Komponente ***Remote-Verwaltung*** installiert werden soll. Weitere Informationen zur Installation und Konfiguration der Remote-Verwaltung finden Sie in der entsprechenden Dokumentation der AVG Network Edition, die auf der Website von AVG (http://www.avg.com/de/) im Bereich Support Center/Download heruntergeladen werden kann.



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

Schaltflächen

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

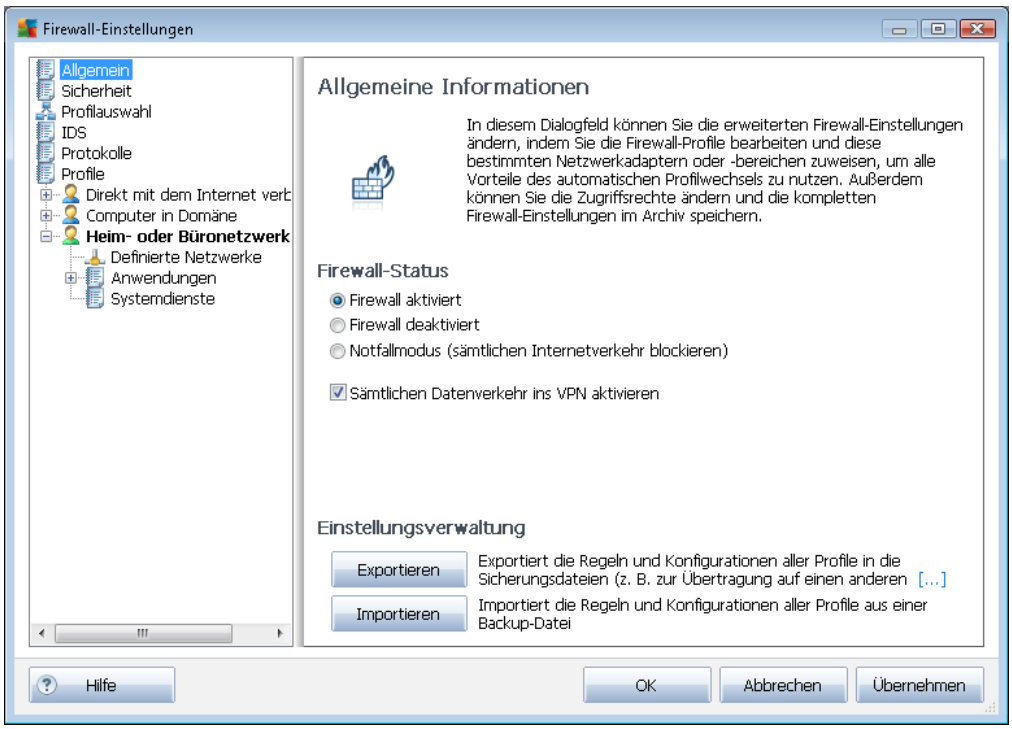
10. Firewall-Einstellungen

Für die Konfiguration der Firewall wird ein neues Fenster geöffnet, wo in verschiedenen Dialogen sehr detaillierte Parameter der Komponente eingestellt werden können.

Alle Komponenten von AVG Internet Security 2012 sind dennoch standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Standardkonfiguration nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

10.1. Allgemein

Der Dialog ***Allgemeine Informationen*** besteht aus zwei Bereichen:



Firewall-Status

Im Abschnitt ***Firewall*** können Sie den Status der Firewall nach Bedarf ändern:

- ***Firewall aktiviert*** – Wählen Sie diese Option aus, um die Kommunikation der Anwendungen zuzulassen, 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 aus,

um den gesamten Datenverkehr an jedem einzelnen Netzwerkport zu blockieren; die Firewall wird weiterhin ausgeführt, aber der gesamte Netzwerkverkehr ist gestoppt.

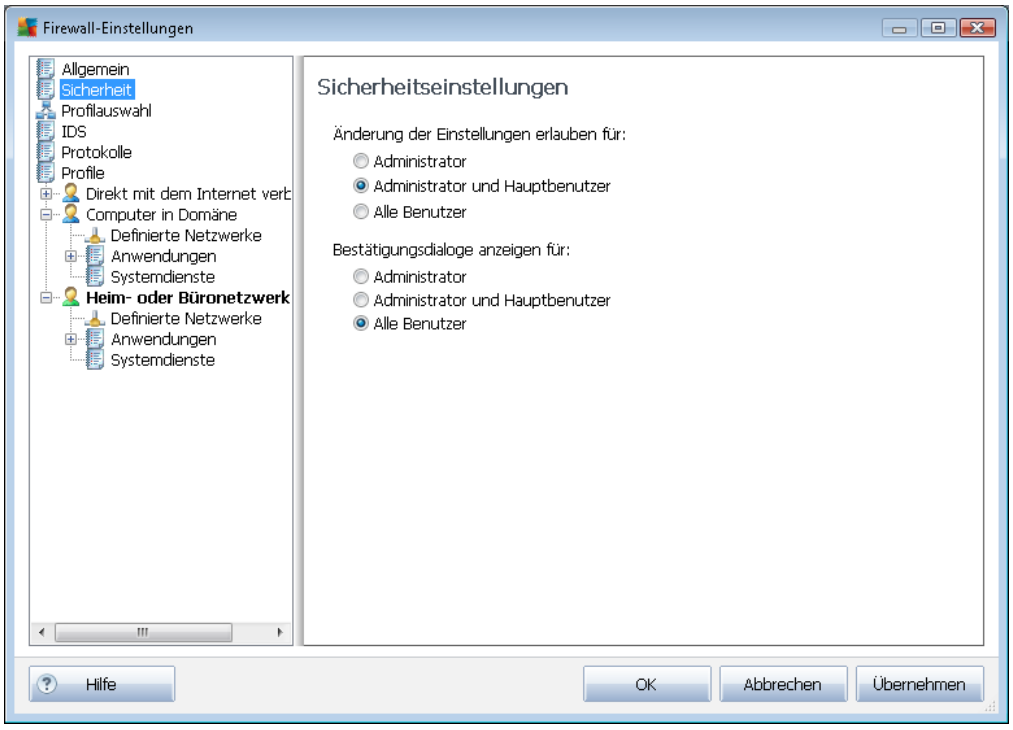
- ***Sämtlichen Datenverkehr ins VPN aktivieren*** *(standardmäßig aktiviert)* – Wenn Sie eine VPN-Verbindung *(Virtual Private Network)* verwenden, beispielsweise, um von zu Hause eine Verbindung mit Ihrem Büro herzustellen, empfehlen wir, das Kontrollkästchen zu aktivieren. ***AVG Firewall*** durchsucht automatisch Ihre Netzwerkadapter, findet diejenigen für VPN-Verbindungen und ermöglicht allen Anwendungen die Verbindung mit dem Zielnetzwerk *(gilt nur für Anwendungen, für die keine besondere Firewall-Regel festgelegt wurde)*. In einem Standardsystem mit allgemeinen Netzwerkadaptern erspart Ihnen dieser einfache Schritt die Einrichtung einer detaillierten Regel für jede Anwendung, die Sie über VPN verwenden müssen.

Hinweis: *Um eine VPN-Verbindung überhaupt zu ermöglichen, müssen Sie die Kommunikation mit den folgenden Systemprotokollen zulassen: GRE, ESP, L2TP, PPTP. Dies kann über den Dialog Systemdienste erfolgen.*

Einstellungsverwaltung

Im Abschnitt ***Einstellungsverwaltung*** 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:

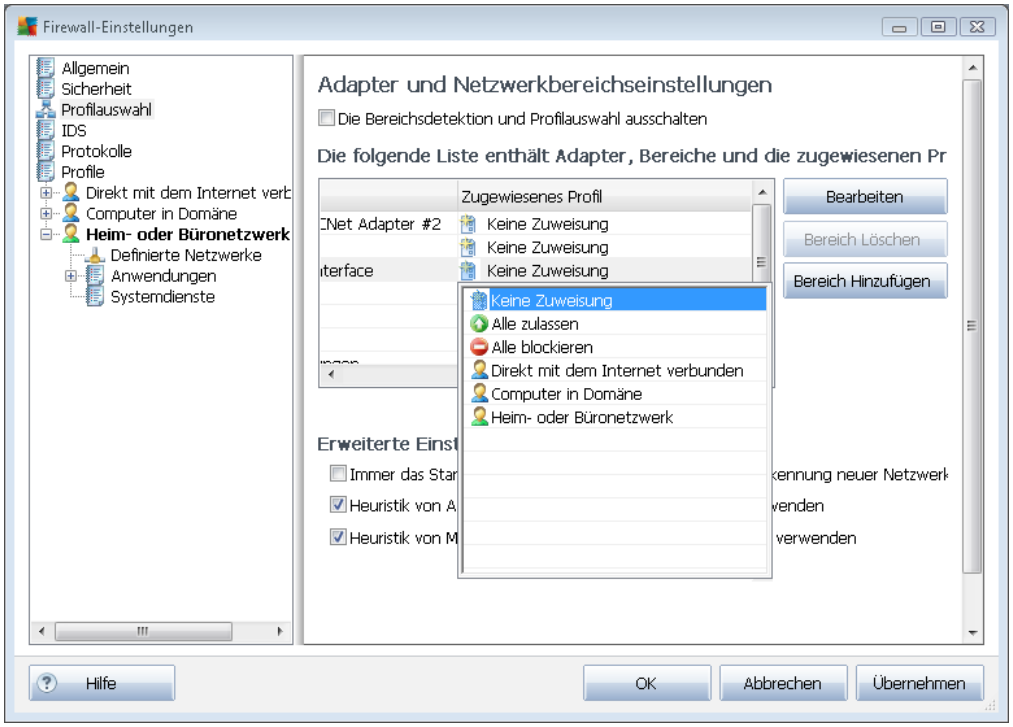
- ***Änderung von Einstellungen erlauben für*** – legt fest, wer die Konfiguration der Firewall ändern darf.
- ***Bestätigungsdialoge anzeigen für*** – Legt fest, wem die Bestätigungsdialoge angezeigt werden sollen *(Dialoge, in denen nach einer Entscheidung gefragt wird, wenn eine bestimmte Situation 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*** *(standardmäßig deaktiviert)* – Jedem Netzwerkschnittstellentyp bzw. jedem Bereich kann eines der definierten Profile zugewiesen werden. Wenn Sie keine bestimmten Profile festlegen möchten, wird ein allgemeines Profil verwendet. 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. Klicken Sie zum Öffnen dieses Menüs mit der linken Maustaste auf den entsprechenden Eintrag in der Liste der Adapter *(in der Spalte „zugewiesene Profile“)*, und wählen Sie das Profil aus dem Kontextmenü aus.

Erweiterte Einstellungen

- ***Immer das Standardprofil verwenden und den Dialog zur Erkennung neuer Netzwerke nicht anzeigen*** – Wenn eine Verbindung zwischen Ihrem Computer und einem neuen Netzwerk hergestellt wird, werden Sie von der Firewall darauf aufmerksam gemacht, und es wird ein Dialog angezeigt, in dem Sie die Art der Netzwerkverbindung auswählen und dieser ein Firewall-Profilzuweisen müssen. Wenn der Dialog nicht angezeigt werden soll, aktivieren Sie dieses Kontrollkästchen.

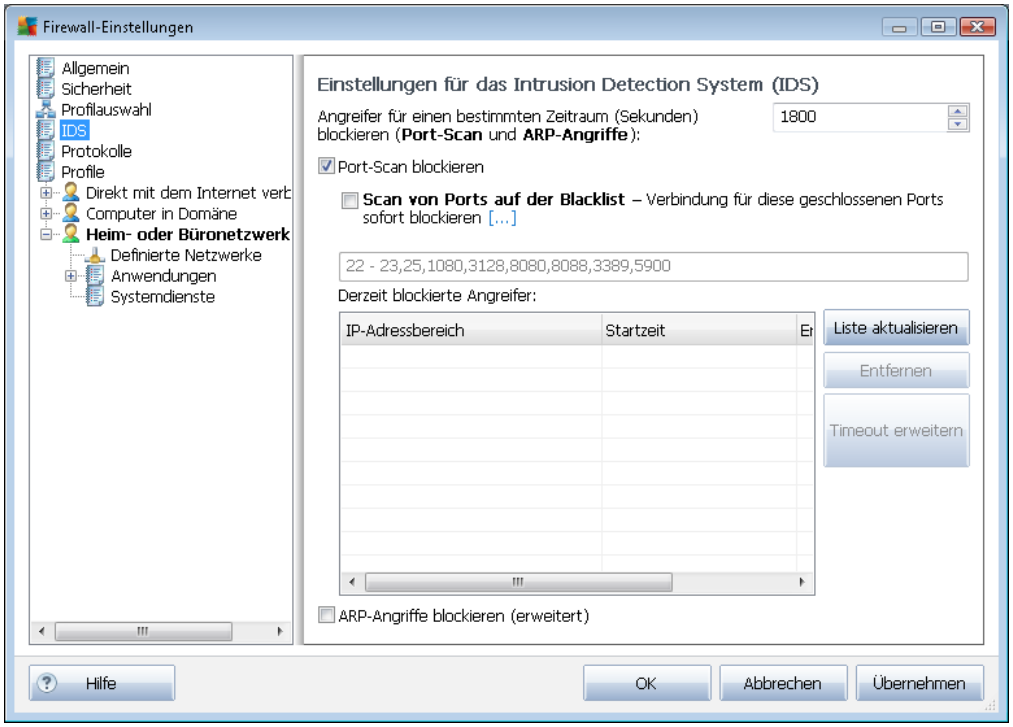
- ***Heuristik von AVG für die Erkennung neuer Netzwerke verwenden*** – Ermöglicht das Abrufen von Informationen über neu erkannte Netzwerke mithilfe einer AVG-

eigenen Methode (*diese Option ist jedoch nur unter dem Betriebssystem Vista und höher verfügbar*).

- ***Heuristik von Microsoft für die Erkennung neuer Netzwerke verwenden*** – Ermöglicht das Abrufen von Informationen über neue erkannte Netzwerke mithilfe des Windows-Dienstes (*diese Option ist nur unter Windows Vista oder höher verfügbar*).

10.4. IDS

Das Intrusion Detection System ist ein Verhaltensanalyse-Tool zur Erkennung und Blockierung verdächtiger Kommunikationsversuche über bestimmte Ports auf Ihrem Computer. Im Dialog ***Einstellungen für das Intrusion Detection System (IDS)*** können Sie IDS-Parameter konfigurieren:



Der Dialog ***Einstellungen für das Intrusion Detection System (IDS)*** bietet folgende Konfigurationsoptionen:

- ***Angreifer für einen bestimmten Zeitraum blockieren (Port-Scan und ARP-Angriffe)*** – Hier können Sie die Anzahl an Sekunden festlegen, die ein Port blockiert sein soll, wenn ein verdächtiger Kommunikationsversuch an diesem Port erkannt wird. Standardmäßig ist das Intervall auf 1800 Sekunden (*30 Minuten*) festgelegt.

- ***Port-Scan blockieren*** *(standardmäßig aktiviert)* – Aktivieren Sie dieses Kontrollkästchen, um alle eingehenden Kommunikationsversuche über TCP- und UDP-Ports auf Ihren Computer zu blockieren. Für Verbindungen dieser Art werden fünf Versuche zugelassen; beim sechsten Versuch wird die Verbindung blockiert. Dieser Eintrag ist standardmäßig aktiviert, und es wird empfohlen, diese Einstellung beizubehalten. Wenn Sie die Aktivierung der Option ***Port-Scan blockieren*** beibehalten, sind weitere detaillierte Konfigurationen

verfügbar *(andernfalls wird der folgende Eintrag deaktiviert)*:

- ***Scan von Ports auf der Blacklist*** – Aktivieren Sie dieses Kontrollkästchen, um Kommunikationsversuche von den im nachfolgenden Textfeld angegebenen Ports sofort zu blockieren. Einzelne Ports und Portbereiche müssen durch Kommas getrennt eingegeben werden. Bei Bedarf steht eine vordefinierte Liste mit empfohlenen Ports zur Verfügung.

- Derzeit blockierte Angreifer – In diesem Abschnitt sind alle Kommunikationsversuche aufgelistet, die momentan von der Firewall blockiert werden. Eine vollständige Historie aller blockierten Versuche kann im Dialog Protokolle (*auf dem Reiter „Port-Scan-Protokolle“*) angezeigt werden.

- ***ARP-Angriffe blockieren (erweitert)*** *(standardmäßig deaktiviert)* – Aktivieren Sie diese Option, um bestimmte Kommunikationsversuche innerhalb eines lokalen Netzwerks blockieren zu können, die vom ***IDS*** als potenziell gefährlich erkannt werden. Die in ***Angreifer für einen bestimmten Zeitraum blockieren festgelegte Zeit gilt hier ebenfalls.*** Dieses Feature wird nur für erfahrene Benutzer empfohlen, die sich mit der Art und der Risikostufe ihres lokalen Netzwerks auskennen.

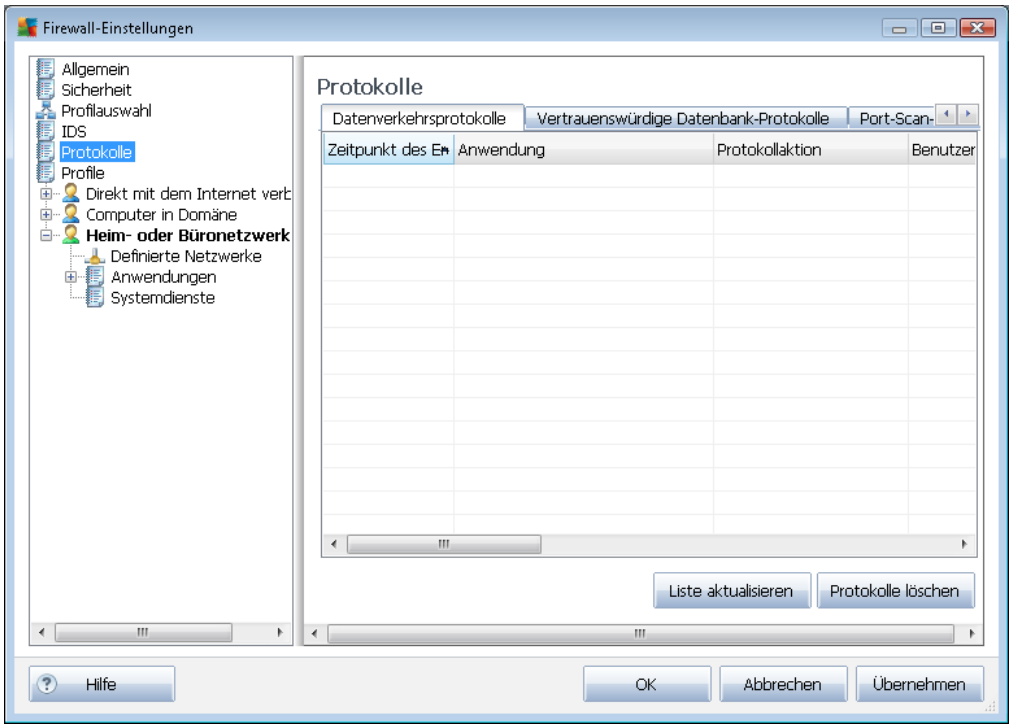
Schaltflächen

- ***Liste aktualisieren*** – Klicken Sie auf diese Schaltfläche, um die Liste zu aktualisieren (*Erfassen der neuesten blockierten Versuche*)

- ***Entfernen*** – Klicken Sie auf diese Schaltfläche, um eine ausgewählte Blockierung aufzuheben

- ***Timeout erweitern*** – Klicken Sie auf diese Schaltfläche, um den Blockierungszeitraum für eine ausgewählte Blockierung zu verlängern. Daraufhin wird ein neuer Dialog mit erweiterten Optionen angezeigt, in dem Sie eine bestimmte Uhrzeit und ein bestimmtes Datum oder einen unbegrenzten Zeitraum festlegen können.

10.5. Protokolle



Im Dialog ***Protokolle*** können Sie die Liste aller protokollierten Firewall-Aktivitäten und -Ereignisse mit einer genauen Beschreibung der jeweiligen Parameter überprüfen (*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.
- ***Port-Scan-Protokolle*** – bietet ein Protokoll aller Aktivitäten des Intrusion Detection Systems.
- ***ARP-Protokolle*** – Protokollinformationen zur Blockierung bestimmter Kommunikationsversuche innerhalb eines lokalen Netzwerks (Option *ARP-Angriffe blockieren*), die vom Intrusion Detection System als potentiell gefährlich eingestuft wurden.

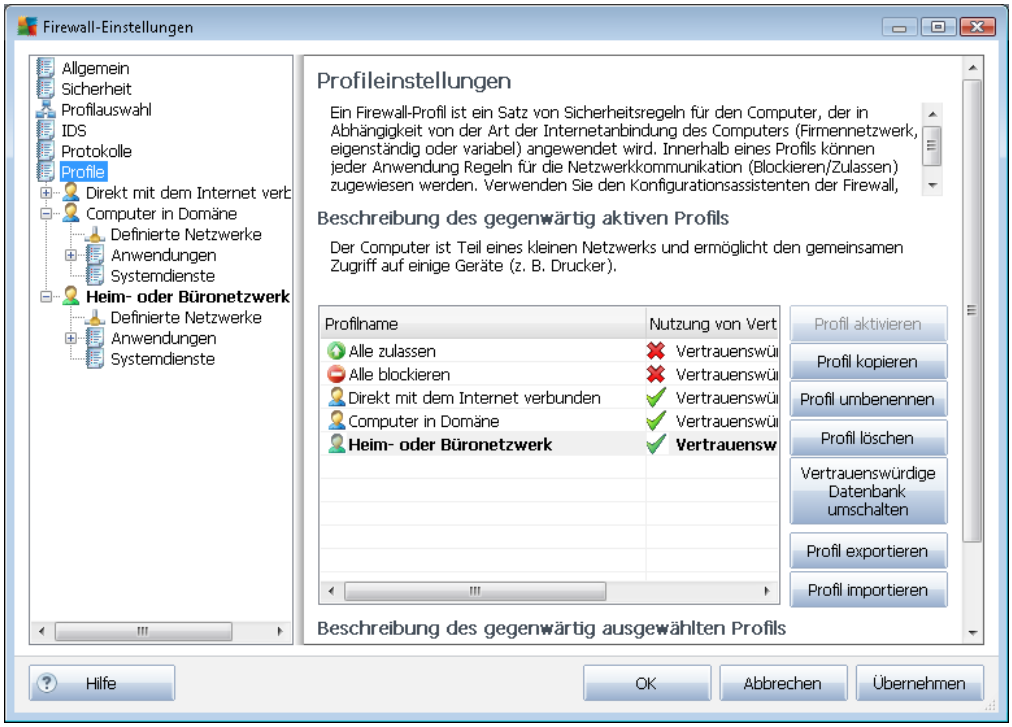
Schaltflächen

- ***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***.

- ***Protokolle löschen*** – Mit dieser Schaltfläche löschen Sie alle Einträge in der Tabelle.

10.6. Profile

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



Systemprofile *(Alle zulassen, Alle blockieren)* können nicht bearbeitet werden. Alle benutzerdefinierten Profile *(Direkt mit dem Internet verbunden, Computer in Domäne, Heim- oder Büronetzwerk)* können jedoch direkt in diesem Dialog mit den folgenden Schaltflächen 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.

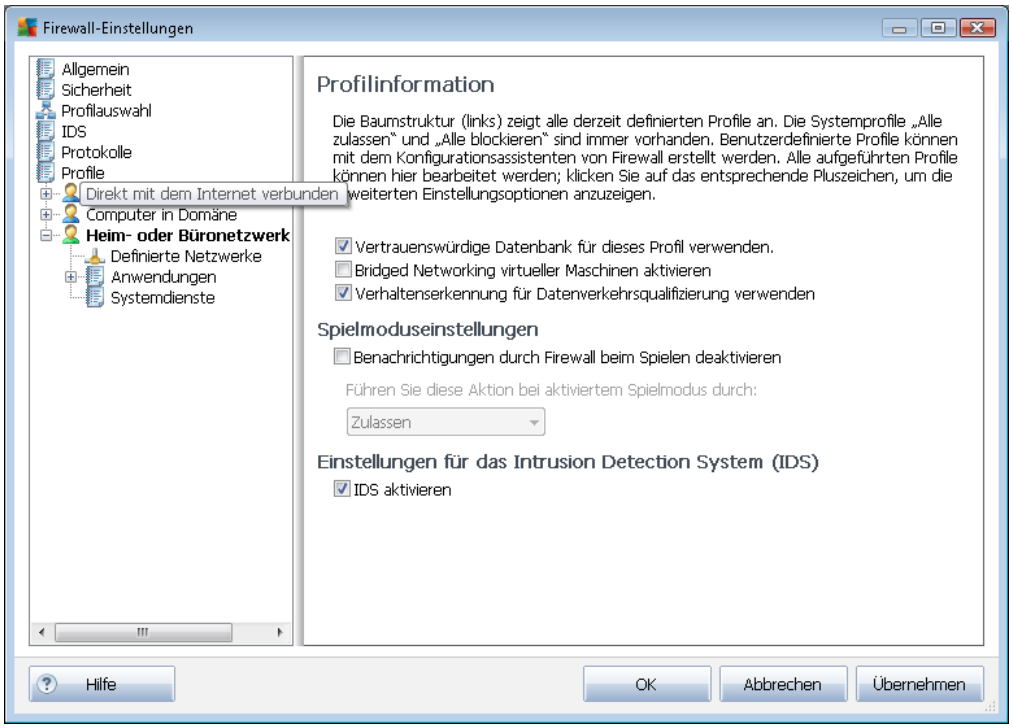
- ***Profil kopieren*** – Erstellt eine identische Kopie des ausgewählten Profils; Sie können die Kopie später bearbeiten und umbenennen, um auf der Basis des duplizierten Originals ein neues Profil zu erstellen.

- ***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.

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*):

10.6.1. 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.

- ***Vertrauenswürdige Datenbank für dieses Profil verwenden*** (*standardmäßig aktiviert*) – Aktivieren 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 Maschinen in VMware direkt eine Verbindung mit dem Netzwerk herstellen können.

- ***Verhaltenserkennung für Datenverkehrsqualifizierung verwenden*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, damit die Firewall die Funktionen von Identitätsschutz bei der Bewertung von Anwendungen nutzen kann – Identitätsschutz 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. PowerPoint-Präsentationen*), da die Informationsmeldungen störend sein können.

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.

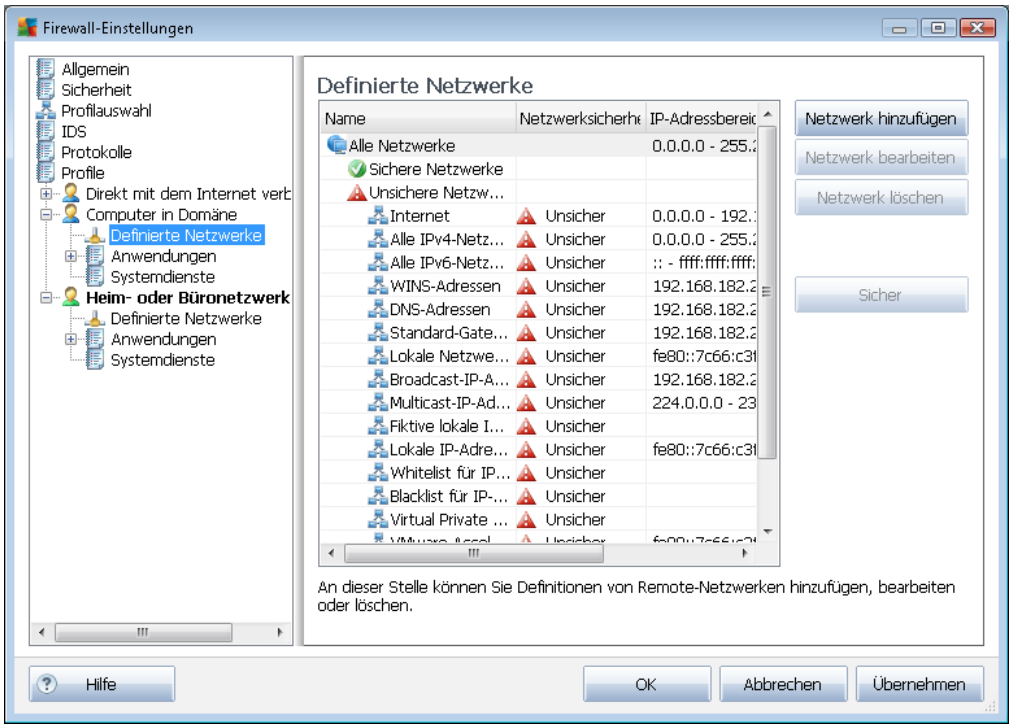
Wenn der Spielemodus aktiviert ist, werden alle geplanten Aufgaben (*Scans, Updates*) bis zum Schließen der Anwendung aufgeschoben.

Einstellungen für das Intrusion Detection System (IDS)

Aktivieren Sie das Kontrollkästchen ***IDS aktivieren***, um ein Verhaltensanalyse-Tool zur Erkennung und Blockierung verdächtiger Kommunikationsversuche über bestimmte Ports auf Ihrem Computer zu aktivieren *(weitere Informationen zu den Einstellungen dieses Tools finden Sie im Kapitel IDS dieser Dokumentation).*

10.6.2. Definierte Netzwerke

Der Dialog ***Definierte Netzwerke*** enthält eine Liste aller Netzwerke, mit denen Ihr Computer verbunden ist.

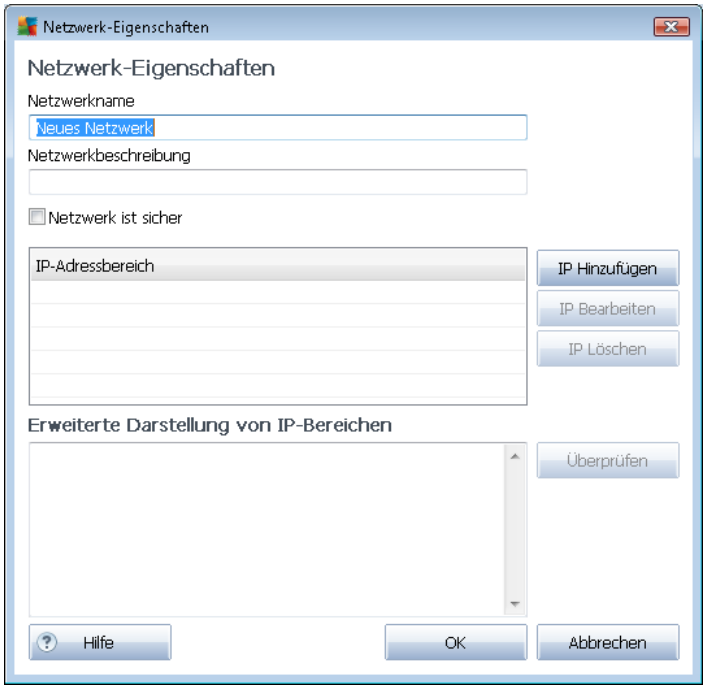


Die Liste enthält die folgenden Informationen über jedes erkannte Netzwerk:

- ***Netzwerke*** – Zeigt eine Namensliste aller Netzwerke, mit denen der Computer verbunden ist.
- ***Netzwerksicherheit*** – Standardmäßig werden alle Netzwerke als unsicher eingestuft. Nur wenn Sie sicher sind, dass ein Netzwerk sicher ist, können Sie es entsprechend kennzeichnen (*Klicken Sie auf den Eintrag für das entsprechende Netzwerk, und 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.

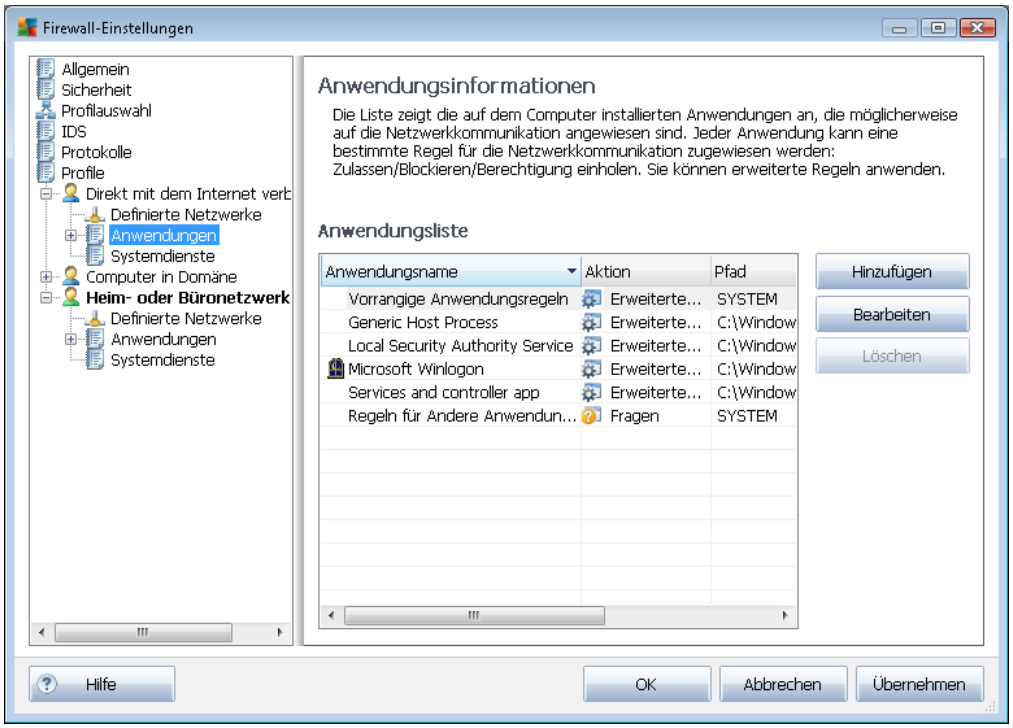
- ***Netzwerk bearbeiten*** – Der Dialog ***Netzwerk-Eigenschaften*** wird geöffnet (*siehe oben*). Sie können darin Parameter eines bereits definierten Netzwerks bearbeiten (*der Dialog ist identisch mit dem Dialog für das Hinzufügen eines neuen Netzwerks, beachten Sie daher die Beschreibung im vorherigen Absatz*).

- ***Netzwerk löschen*** – Der Eintrag des ausgewählten Netzwerks wird aus der Liste der Netzwerke gelöscht.

- ***Als Sicher markieren*** – Standardmäßig werden alle Netzwerke als unsicher eingestuft. Nur wenn Sie sicher sind, dass ein Netzwerk sicher ist, können Sie es entsprechend kennzeichnen (*und umgekehrt, die Schaltfläche ändert sich in „Als unsicher markieren“, wenn das Netzwerk als sicher gekennzeichnet ist*).

10.6.3. Anwendungen

Im Dialog ***Anwendungsinformationen*** sind alle installierten Anwendungen aufgeführt, die möglicherweise eine Netzwerkkommunikation erfordern, sowie Symbole für die jeweils zugeordnete Aktion:



Die in der ***Anwendungsliste*** angezeigten Anwendungen wurden auf Ihrem Computer erkannt (*und ihnen wurden die entsprechenden Aktionen zugewiesen*). Die folgenden Aktionstypen können verwendet werden:

- - Kommunikation für alle Netzwerke zulassen
- - Kommunikation nur für Netzwerke zulassen, die als „sicher“ definiert wurden
- - Kommunikation blockieren
- - Bestätigungsdialog anzeigen (*Benutzer können hier entscheiden, ob sie die Kommunikation zulassen oder blockieren möchten, wenn die Anwendung versucht, eine Verbindung mit dem Netzwerk herzustellen*)
- - Erweiterte Einstellungen definiert

Bitte beachten Sie, dass nur Anwendungen erkannt werden, die zum Zeitpunkt der Ausführung bereits auf dem Computer installiert waren; bei der späteren Installation weiterer Anwendungen müssen nachträglich entsprechende Firewall-Regeln definiert werden. Wenn die neu installierte Anwendung erstmals versucht, eine Netzwerkverbindung herzustellen, erstellt die Firewall standardmäßig entweder automatisch eine entsprechende Regel gemäß der Vertrauenswürdigen Datenbank, oder Sie werden von der Firewall gefragt, ob Sie die

Kommunikation zulassen oder blockieren möchten. Im letzteren Fall können Sie Ihre Entscheidung als dauerhafte Regel speichern (die dann in diesem Dialog angezeigt wird).

Natürlich können Sie entsprechende Regeln für Anwendungen auch direkt definieren: Klicken Sie dazu in diesem Dialog auf ***Hinzufügen***, und geben Sie die jeweiligen Informationen für die Anwendung an.

Neben den Anwendungen enthält diese Liste noch zwei spezielle Elemente:

- ***Vorrangige Anwendungsregeln*** (*oben in der Liste*) haben Vorrang vor individuellen Anwendungsregeln.
- ***Regeln für andere Anwendungen*** (*unten in der Liste*) werden als „letzte Instanz" verwendet, wenn keine spezifischen Anwendungsregeln Verwendung finden, beispielsweise bei unbekannten und nicht definierten Anwendungen.

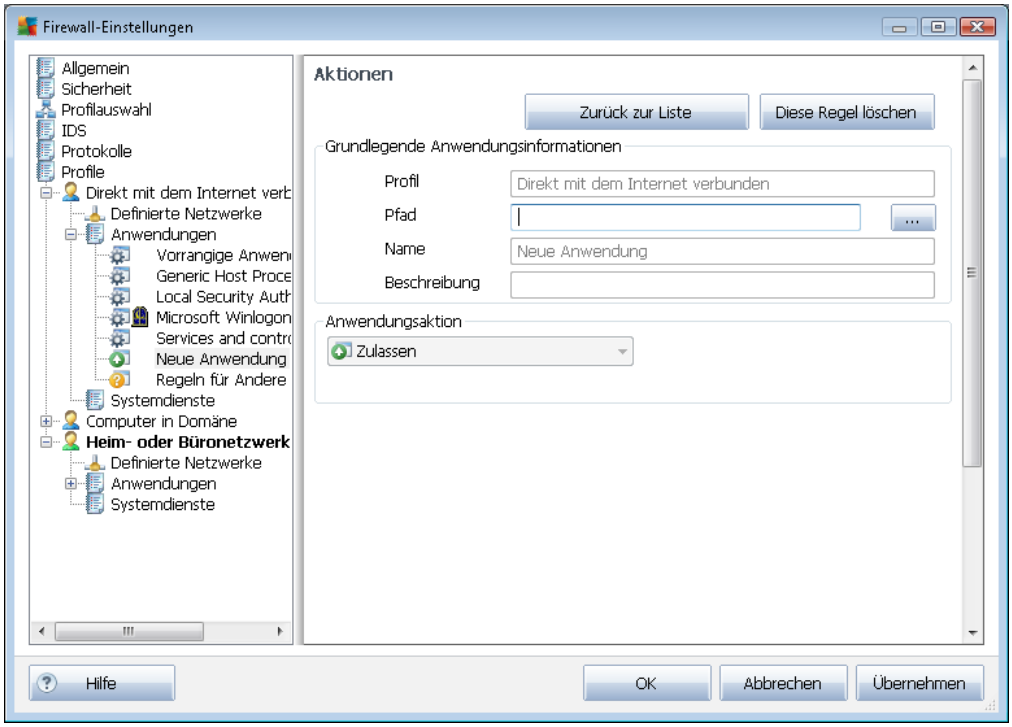
Die Einstellungsoptionen dieser Elemente unterscheiden sich von den Standardanwendungen und sind nur für erfahrene Benutzer gedacht. Wir empfehlen dringend, die Einstellungen beizubehalten!

Schaltflächen

Die Liste kann mit den folgenden Schaltflächen bearbeitet werden:

- ***Hinzufügen*** – Öffnet einen leeren Dialog Aktionen zum Festlegen neuer Anwendungsregeln.
- ***Bearbeiten*** – Öffnet denselben Dialog Aktionen mit Daten zur Bearbeitung eines vorhandenen Regelsatzes einer Anwendung.
- ***Löschen*** – Entfernt die ausgewählte Anwendung aus der Liste.

Im Dialog ***Aktionen*** können Sie detaillierte Einstellungen für die jeweilige Anwendung vornehmen:



Schaltflächen

Im oberen Bereich des Dialogs stehen zwei Schaltflächen zur Verfügung:

- ***Zurück zur Liste*** – Klicken Sie auf die Schaltfläche, um eine Übersicht aller definierten Anwendungsregeln anzuzeigen.
- ***Diese Regel löschen*** – Klicken Sie auf die Schaltfläche, um die aktuell angezeigte Anwendungsregel zu löschen. ***Bitte beachten Sie, dass diese Aktion nicht rückgängig gemacht werden kann.***

Grundlegende Anwendungsinformationen

Geben Sie in diesem Abschnitt den ***Namen*** der Anwendung sowie optional eine ***Beschreibung*** (*ein kurzer Kommentar zu Ihrer eigenen Information*) ein. Geben Sie im Feld ***Pfad*** den vollständigen Pfad für die Anwendung (*die ausführbare Datei*) auf dem Datenträger ein. Sie können die Anwendung auch einfach in der Baumstruktur auswählen, indem Sie auf die Schaltfläche „***...***“ klicken.

Anwendungsaktion

Im Dropdown-Menü können Sie die Firewall-Regel für die Anwendung auswählen, Sie können also

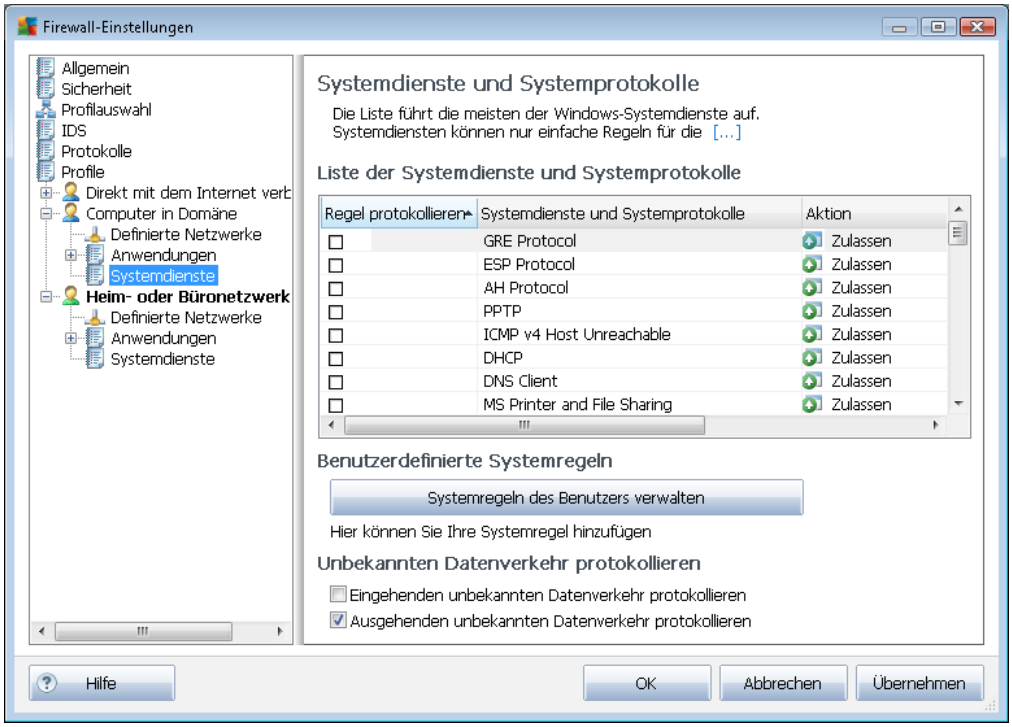
auswählen, was die Firewall tun soll, wenn die Anwendung versucht, über das Netzwerk zu kommunizieren:

- ***Zulassen*** – Ermöglicht der Anwendung die Kommunikation über alle definierten Netzwerke und Adapter ohne Einschränkungen.
- ***Sichere zulassen*** – Ermöglicht der Anwendung die Kommunikation nur über als sicher *(vertrauenswürdig)* definierte Netzwerke.
- ***Blockieren*** – Unterbindet die Kommunikation automatisch; die Anwendung kann keine Netzwerkverbindungen herstellen.
- ***Fragen*** – Zeigt einen Dialog an, in dem Sie jeweils entscheiden können, ob die Kommunikation über das Netzwerk für die Anwendung zugelassen oder blockiert werden soll.
- ***Erweiterte Einstellungen*** – Zeigt im unteren Bereich des Dialogs im Abschnitt ***Detailregeln für die Anwendung*** weitere umfangreiche Einstellungsoptionen an. Die detaillierten Regeln werden entsprechend der Listenreihenfolge angewendet, und Sie können die Regeln in der Liste je nach Priorität***Nach oben*** oder ***Nach unten*** verschieben. Wenn Sie auf eine bestimmte Regel in der Liste klicken, wird die Übersicht über die Regeldetails im unteren Abschnitt des Dialogs angezeigt. Jeder blau unterstrichene Wert kann durch Anklicken des entsprechenden Einstellungsdialogs geändert werden. Um die hervorgehobene Regel zu löschen, klicken Sie auf ***Entfernen***. Um eine neue Regel zu definieren, klicken Sie auf ***Hinzufügen***, um den Dialog ***Regeldetail ändern***zu öffnen, in dem Sie alle erforderlichen Details angeben können.

10.6.4. Systemdienste

Systemdienste und Protokolldialoge sollten NUR VON ERFAHRENEN BENUTZERN bearbeitet werden!

Im Dialog ***Systemdienste und Systemprotokolle*** werden die Standardsystemdienste und -protokolle von Windows aufgeführt, die möglicherweise über das Netzwerk kommunizieren müssen:



Liste der Systemdienste und Systemprotokolle

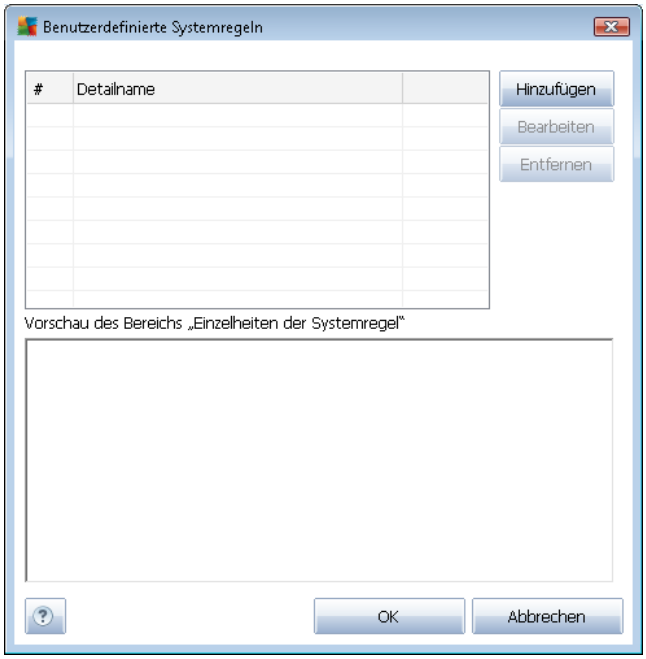
Das Diagramm enthält die folgenden Spalten:

- ***Regel protokollieren*** – Mit diesem Kontrollkästchen können Sie das Erfassen jeder Regelanwendung in den Protokollen einschalten.
- ***Systemdienste und Systemprotokolle*** – Diese Spalte zeigt den Namen des entsprechenden Systemdienstes an.
- ***Aktion*** – Diese Spalte zeigt das Symbol für die zugewiesene Aktion an:
  - Kommunikation für alle Netzwerke zulassen
  - Kommunikation nur für Netzwerke zulassen, die als „sicher“ definiert wurden
  - Kommunikation blockieren
- ***Netzwerke*** – Diese Spalte gibt an, für welches spezielle Netzwerk die Systemregel gilt.

Um die Einstellungen eines Eintrags in der Liste (*einschließlich der zugehörigen Aktionen*) zu bearbeiten, klicken Sie mit der rechten Maustaste auf den entsprechenden Eintrag, und wählen Sie die Option ***Bearbeiten*** aus. ***Systemregeln sollten jedoch nur von erfahrenen Benutzern bearbeitet werden; wir raten ausdrücklich von einer Bearbeitung der Systemregeln ab!***

Benutzerdefinierte Systemregeln

Um einen neuen Dialog für das Definieren Ihrer eigenen Systemdienstregel zu öffnen (*siehe Bild unten*), klicken Sie auf die Schaltfläche ***Systemregeln des Benutzers verwalten***. Im oberen Abschnitt des Dialogs ***Benutzerdefinierte Systemregeln*** wird eine Übersicht mit allen Details der aktuell bearbeiteten Systemregel angezeigt, im unteren Abschnitt dagegen das entsprechende Detail. Benutzerdefinierte Systemregeln können bearbeitet, hinzugefügt oder gelöscht werden (über die entsprechende Schaltfläche). Vom Hersteller definierte Regeldetails können nur bearbeitet werden:



Bitte beachten Sie, dass es sich bei Detailregeleinstellungen um erweiterte Einstellungen handelt, die hauptsächlich für Netzwerkadministratoren vorgesehen sind, die über eine vollständige Kontrolle der Firewall-Konfiguration verfügen müssen. Sollten Sie mit den verschiedenen Kommunikationsprotokollen, Portnummern der Netzwerke, Definitionen der IP-Adressen usw. nicht vertraut sein, ändern Sie diese Einstellungen bitte nicht! Wenn Sie die Konfiguration jedoch ändern müssen, finden Sie genaue Informationen in den Hilfedateien des entsprechenden Dialogs.

Unbekannten Datenverkehr protokollieren

- ***Eingehenden unbekannten Datenverkehr protokollieren*** *(standardmäßig deaktiviert)* – Aktivieren Sie dieses Kontrollkästchen, um mithilfe der Protokolle alle unbekannten Versuche zu erfassen, von einem externen Netzwerk aus eine Verbindung mit Ihrem Computer herzustellen.

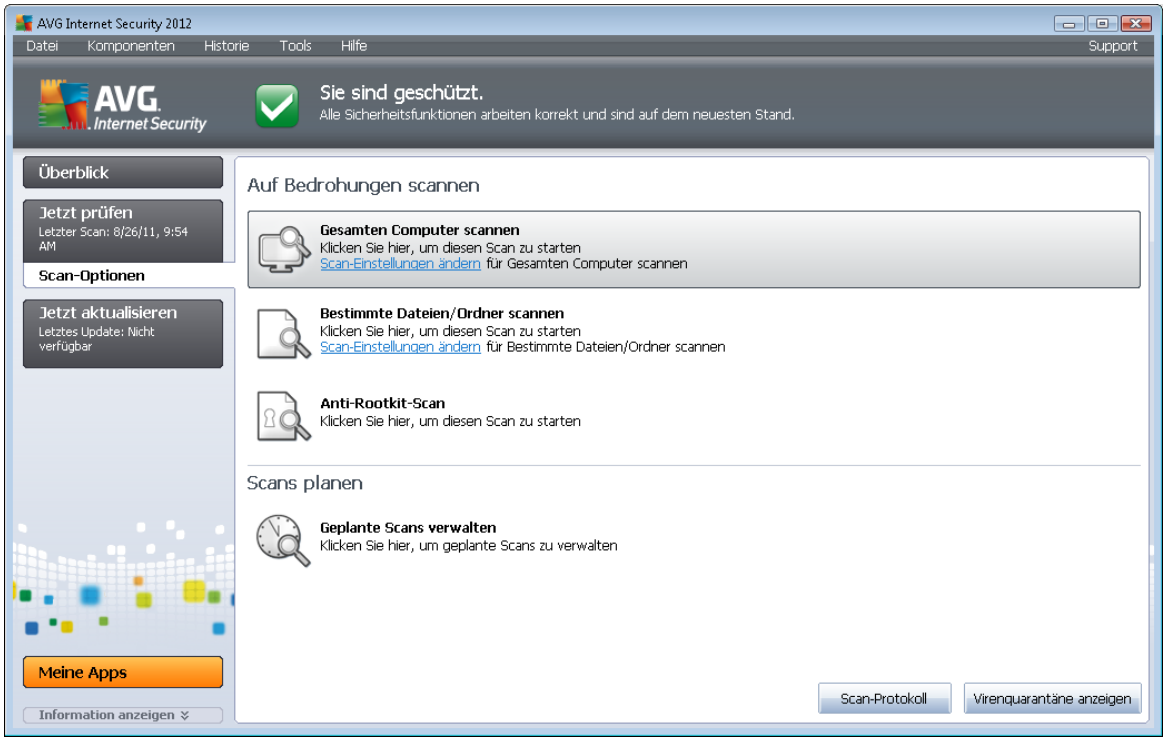
- ***Ausgehenden unbekannten Datenverkehr protokollieren*** *(standardmäßig aktiviert)* – Aktivieren Sie dieses Kontrollkästchen, um mithilfe der Protokolle alle Versuche zu

erfassen, eine unbekannte Verbindung von Ihrem Computer zu einem externen Netzwerk herzustellen.

11. AVG-Scans

Standardmäßig führt **AVG Internet Security 2012** keine Scans aus, da Sie nach dem ersten Scan perfekt durch die residenten Komponenten von **AVG Internet Security 2012** geschützt sein sollten, die stets wachsam sind und keinerlei schädlichen Code in Ihren Computer eindringen lassen. Selbstverständlich können Sie einen Scan planen, der in regelmäßigen Abständen ausgeführt wird, oder auch jederzeit ganz nach Ihrem Bedarf einen Scan starten.

11.1. Benutzeroberfläche für Scans



Auf die Benutzeroberfläche für Scans von AVG kann über den Quick Link ***Scan-Optionen*** 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
- Bereich Einstellungen für geplanten Scan“ – 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 Internet Security 2012** ist der On-Demand-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.

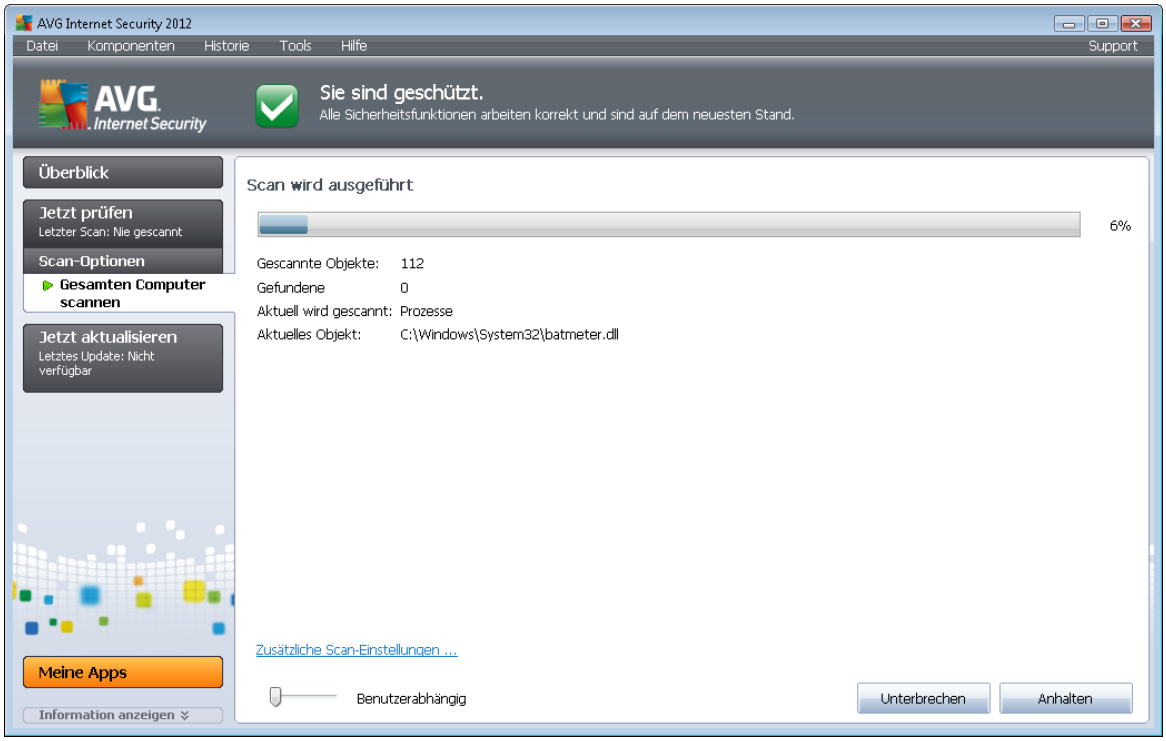
In **AVG Internet Security 2012** stehen die folgenden vom Software-Hersteller vordefinierten Arten von Scans zur Verfügung:

11.2.1. Scan des gesamten Computers

Scan des gesamten Computers – Hiermit wird Ihr gesamter Computer nach möglichen Infektionen und/oder potentiell unerwünschten Programmen gescannt. 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.

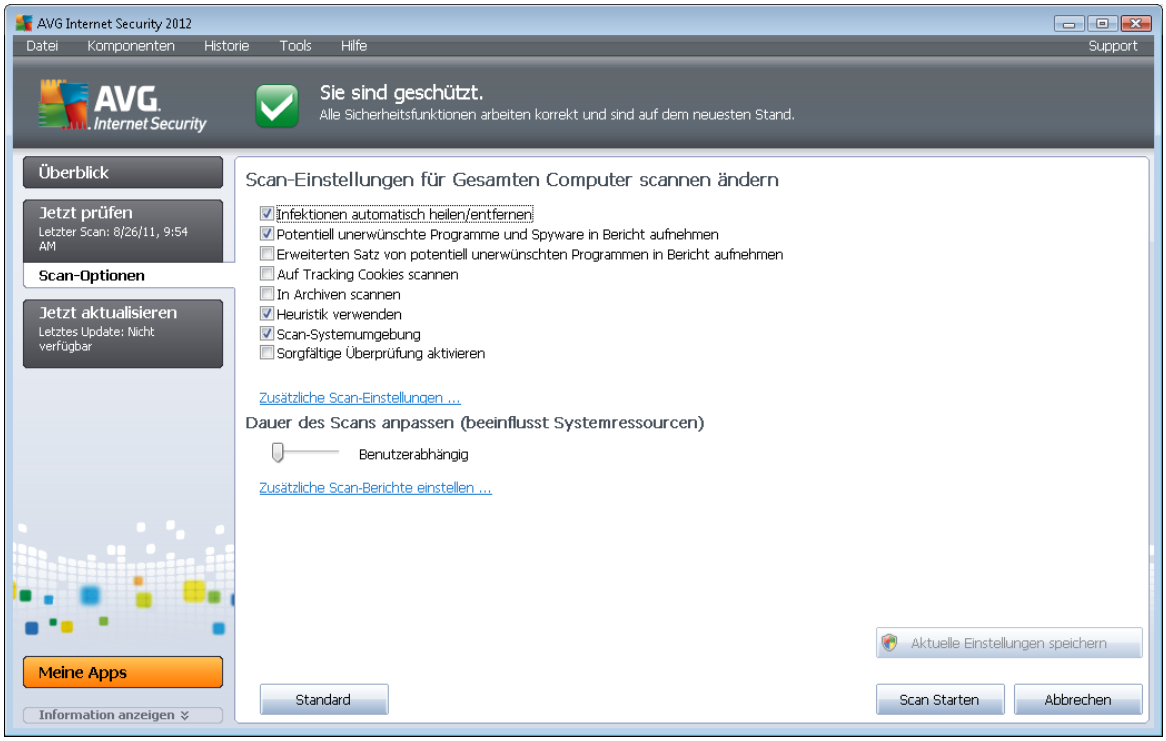
Start von Scans

Sie können den ***Scan des gesamten Computers*** direkt über die Benutzeroberfläche für Scans starten, indem Sie auf das Scan-Symbol klicken. Für diesen Scan-Typ 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

Sie können die vordefinierten Standardeinstellungen der Option ***Scan des gesamten Computers*** bearbeiten. Klicken Sie auf den Link ***Scan-Einstellungen ändern***, um den Dialog ***Scan-Einstellungen für Scan des gesamten Computers ändern*** *zu öffnen (Zugriff über Benutzeroberfläche für Scans über den Link „Scan-Einstellungen ändern“ für Scan des gesamten Computers).* ***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:

  - ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

  - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

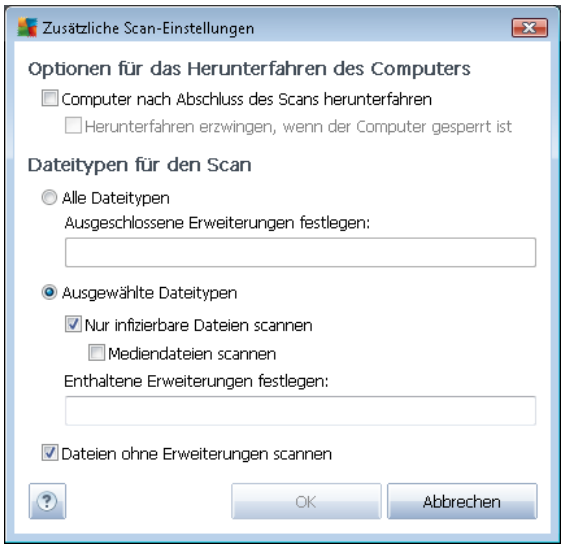
  - ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

  - ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen

(*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

- ***In Archiven scannen*** (*standardmäßig deaktiviert*) – 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*** (*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.
- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***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*** – Außerdem sollten Sie bestimmen, welche Elemente

überprüft werden:

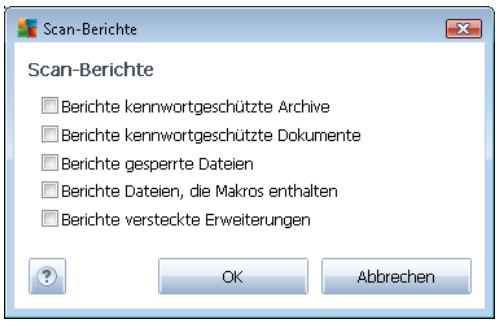
- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;

- ***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.

- ***Dauer des Scans anpassen*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. 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

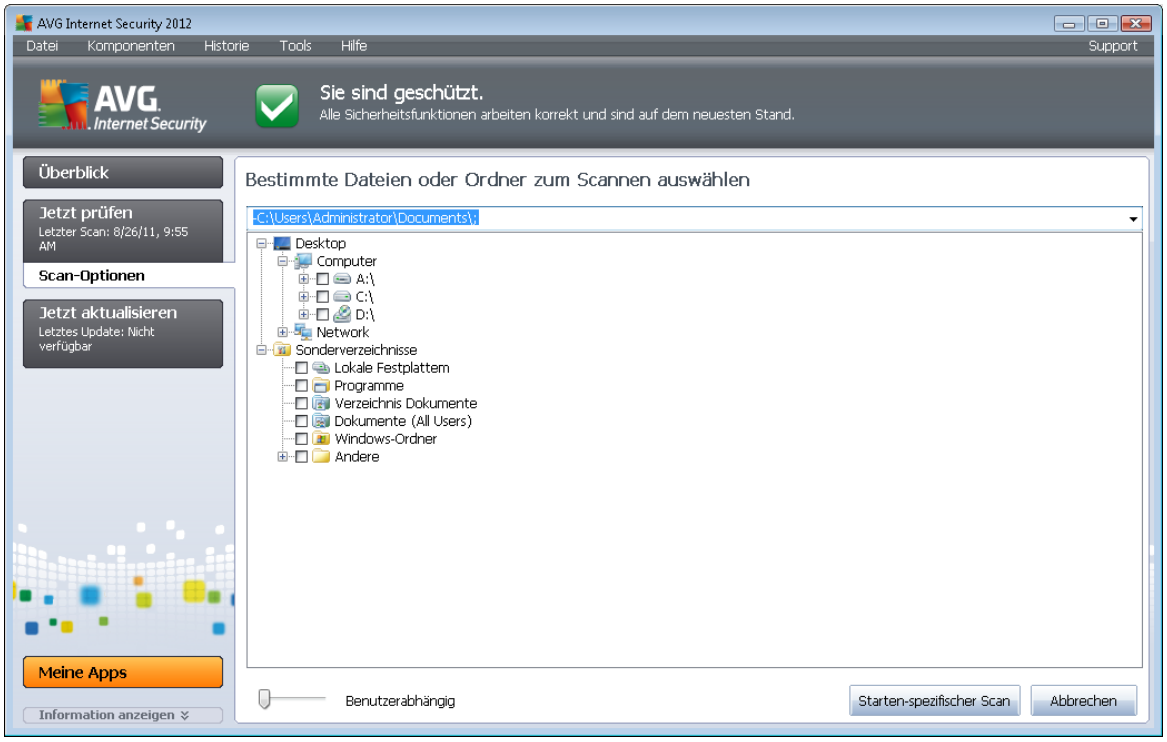
Bestimmte Dateien oder Ordner scannen – Scannt ausschließlich die Bereiche Ihres Computers, die Sie zum Scannen ausgewählt haben (*ausgewählte Ordner, Festplatten, Wechseldatenträger, CDs usw.*). Der Scan-Verlauf bei einer Virenerkennung sowie die Behandlung des Virus entsprechen dem Scan des gesamten 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.

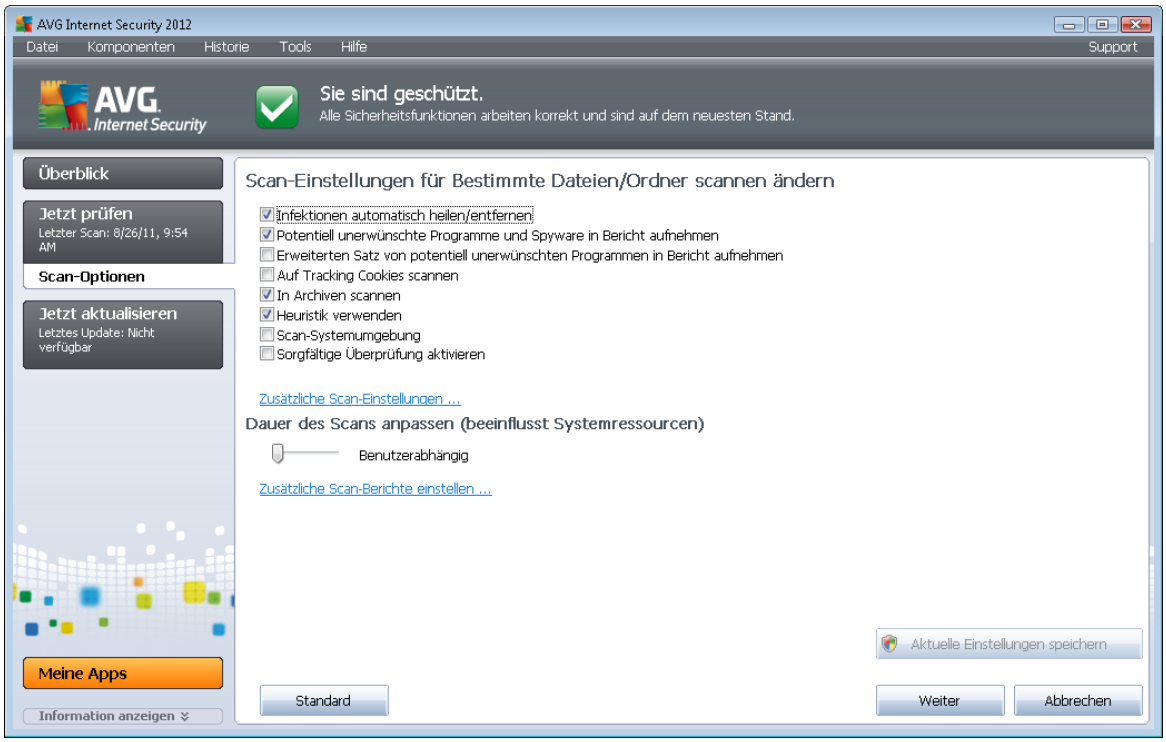
Es ist möglich, einen bestimmten Ordner zu scannen, jedoch seine Unterordner vom Scan auszuschließen. Setzen Sie dafür ein Minuszeichen „**-**“ vor den automatisch generierten Pfad (*siehe Screenshot*). Um den gesamten Ordner vom Scan auszuschließen, verwenden Sie das Ausrufezeichen "!" parameter.

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 ein- bzw. ausschalten:
    - ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.
    - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
    - ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** *(standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein

erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

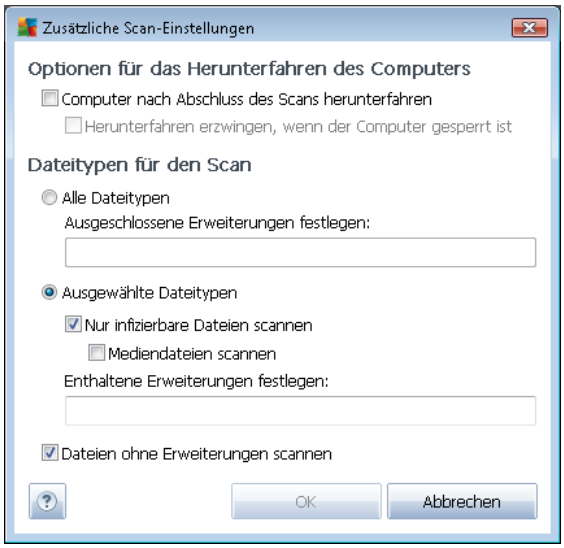
- ***In Archiven scannen*** (*standardmäßig aktiviert*) – Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

- ***Heuristik verwenden*** (*standardmäßig deaktiviert*) – 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 deaktiviert*) –·Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***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*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:

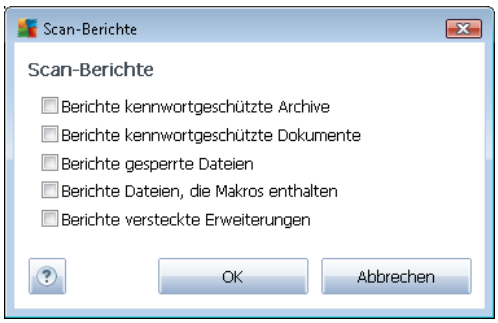
  - ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;

  - ***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 dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. 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:



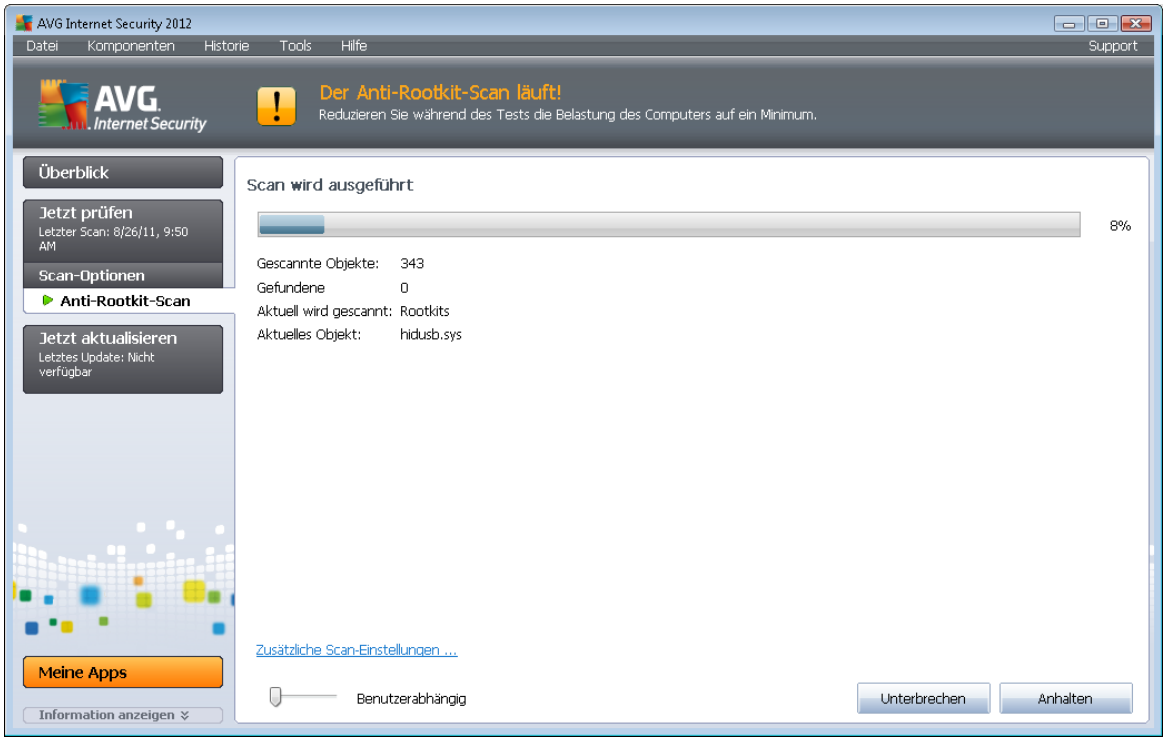
Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen beschrieben. Wenn Sie die Standardkonfiguration der Option* ***Bestimmte Dateien oder Ordner scannen*** *ändern, können 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 Scan-Typ 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.



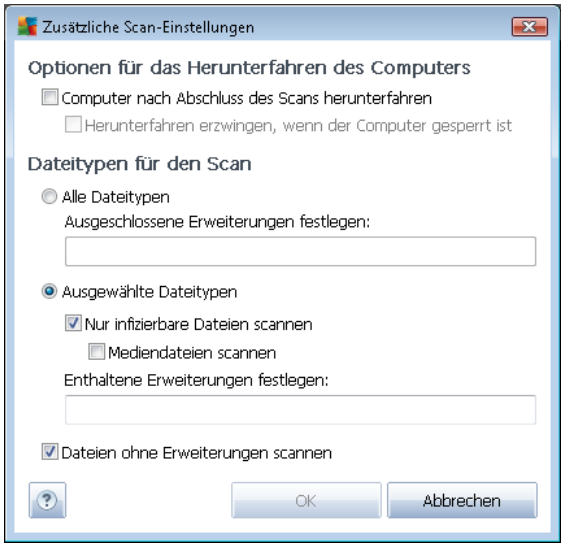
Bearbeitung der Scan-Konfiguration

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 Scan-Oberfläche steht während der Ausführung eines Scans die folgende Konfiguration zur Verfügung:

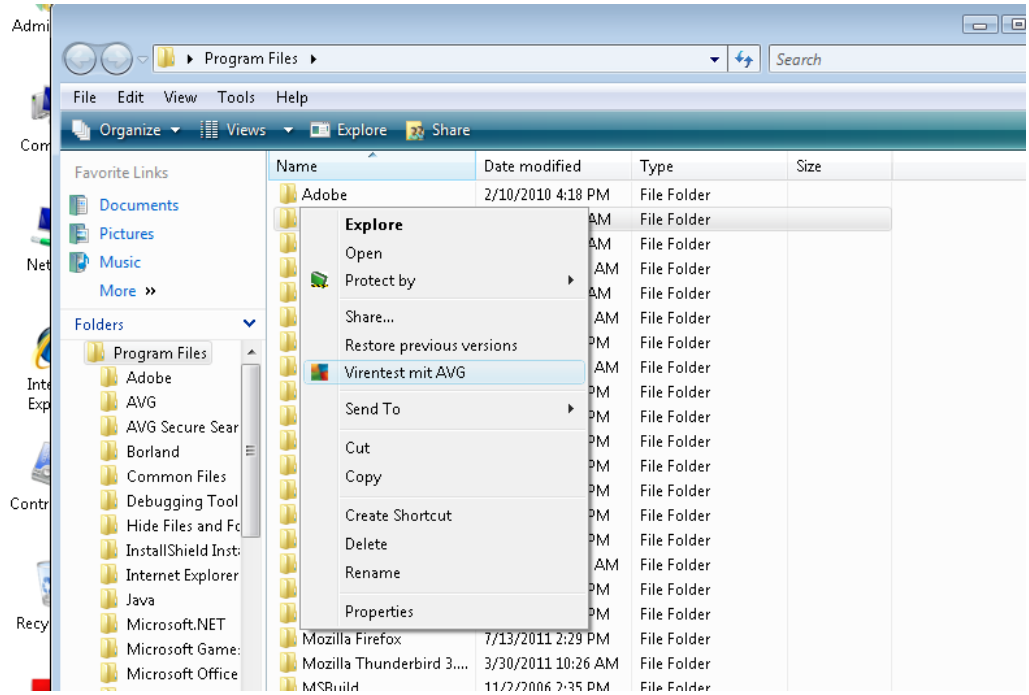
- ***Automatischer Scan*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die 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 Internet Security 2012** 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 Anti-Virus***, um die Datei mit AVG zu scannen**AVG Internet Security 2012**

11.4. Scannen von Befehlszeilen

Mit **AVG Internet Security 2012** 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 Semikola 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 Scanvorgang 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*** Scan des gesamten Computers
- ***/HEUR*** Heuristische Analyse verwenden
- ***/EXCLUDE*** Pfad oder Datei(en) vom Scan ausschließen
- ***/@*** Befehlsdatei /Dateiname/

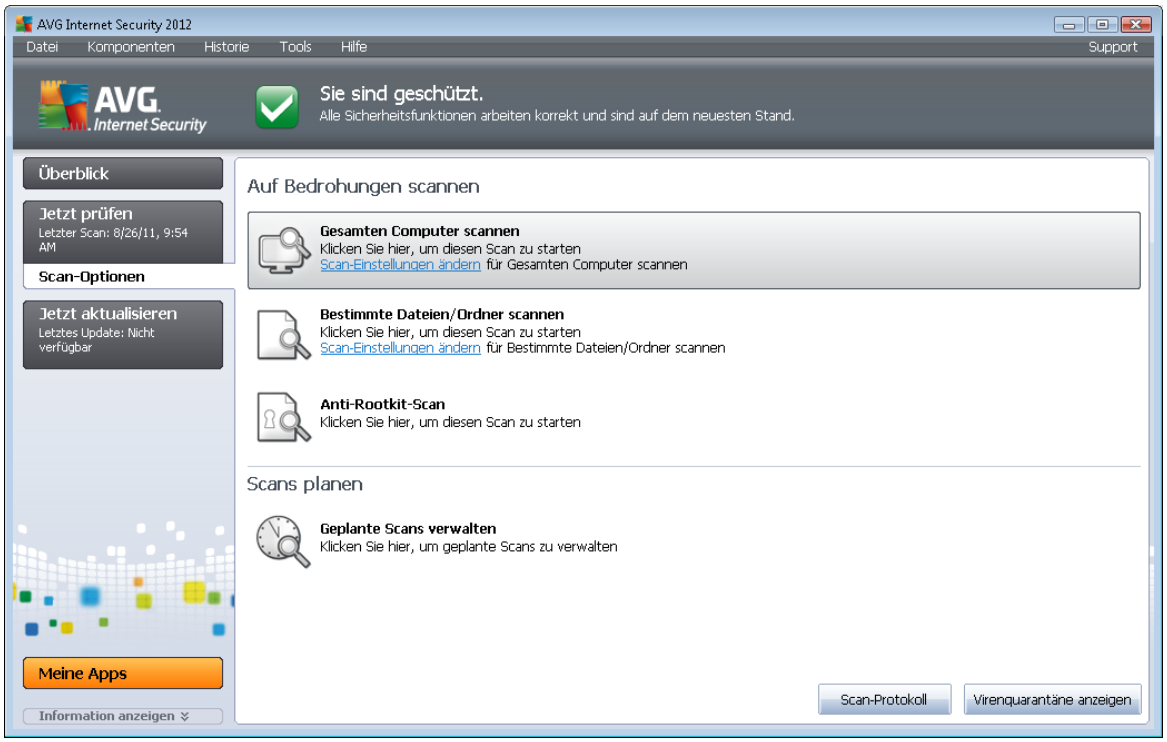
- ***/EXT*** Diese Erweiterungen scannen /z. B. EXT=EXE,DLL/
- ***/NOEXT*** Diese Erweiterungen nicht scannen /z. B. NOEXT=JPG/
- ***/ARC*** Archive scannen
- ***/CLEAN*** Automatisch bereinigen
- ***/TRASH*** Infizierte Dateien in die Virenquarantäne verschieben
- ***/QT*** Schnelltest
- ***/MACROW*** 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 /niedrig, automatisch, hoch/ *(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)*
- ***/ARCBOMBSW*** Erneut komprimierte Archivdateien melden

11.5. Scans planen

Mit **AVG Internet Security 2012** 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.

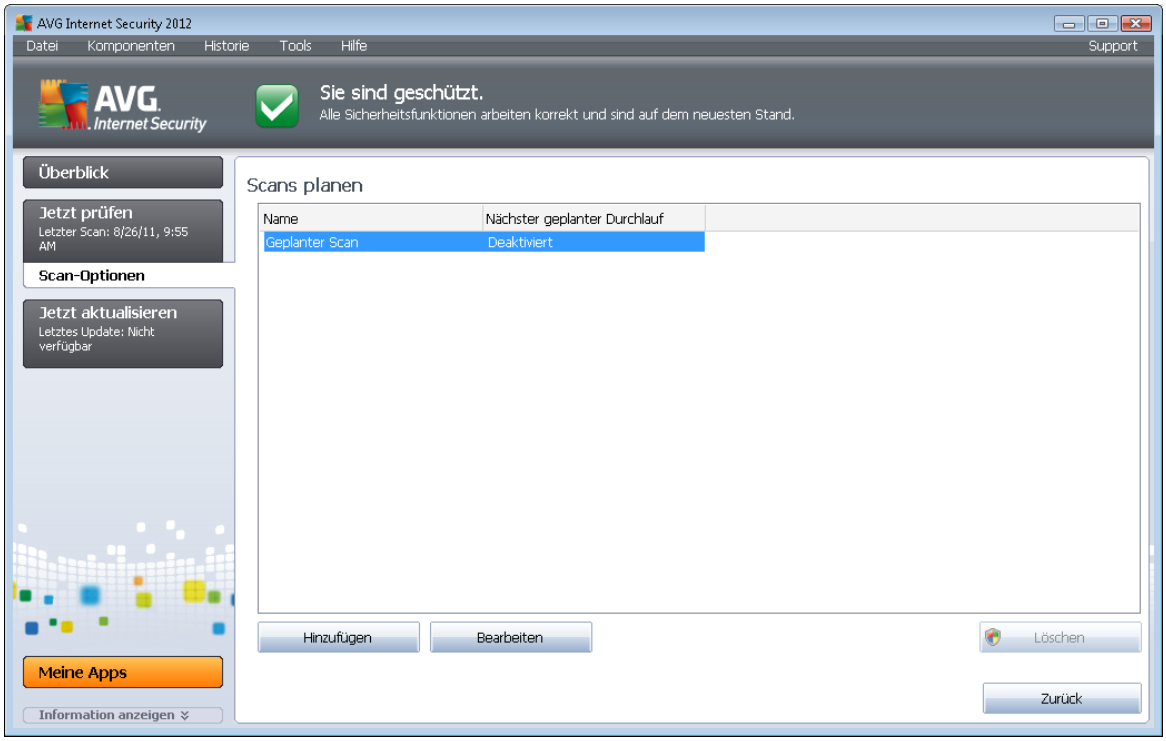
Sie sollten die Funktion Scan des gesamten Computers regelmäßig, mindestens einmal pro Woche, starten. Wenn möglich, sollten Sie Ihren gesamten Computer täglich scannen. Dies ist auch die Standardkonfiguration für geplante Scans. Wenn der Computer immer eingeschaltet ist, können Sie die Scans für Zeiten 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 einen neuen 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.

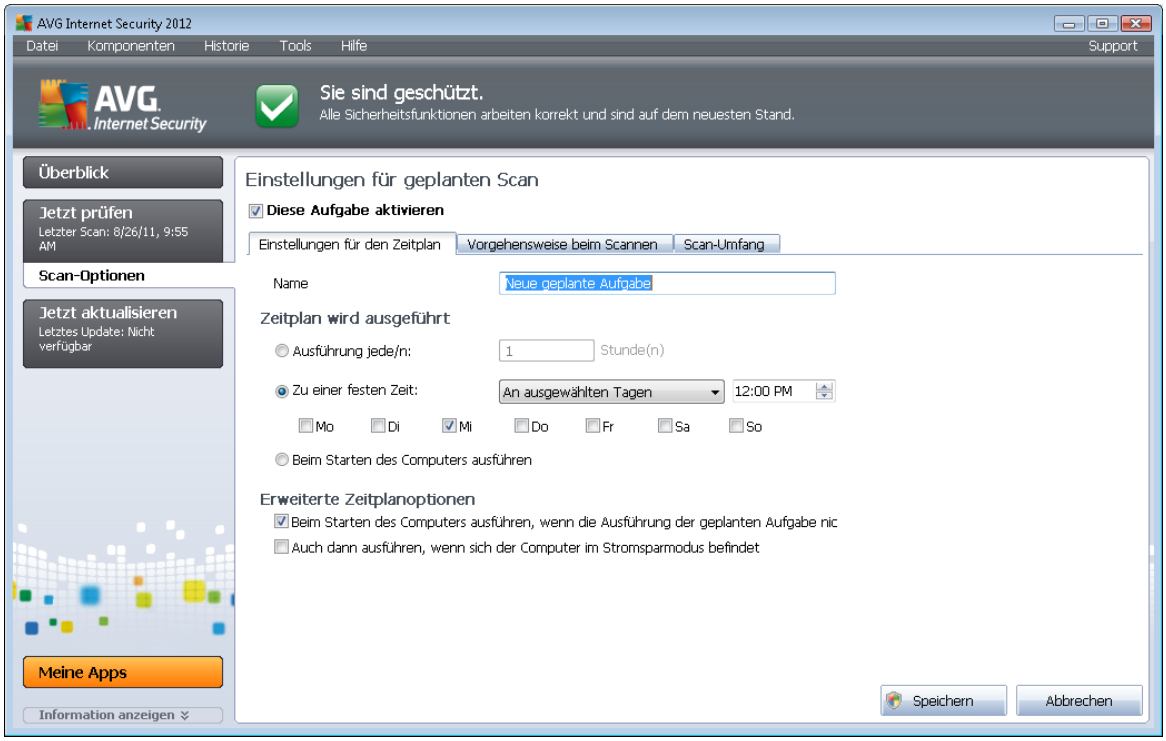
- ***Zeitplan Bearbeiten*** – Diese Schaltfläche steht nur zur Verfügung, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. In diesem Fall ist die Schaltfläche aktiv, und Sie können darauf klicken, um zum Dialog ***Einstellungen für geplanten Scan*** auf 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 im Dialog* ***Scans planen*** *auf die Schaltfläche* ***Scan-Zeitplan hinzufügen***). Der Dialog ist in drei Reiter unterteilt: ***Einstellungen für den Zeitplan*** *(siehe Bild unten; der Standardreiter, zu dem Sie automatisch weitergeleitet 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 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.

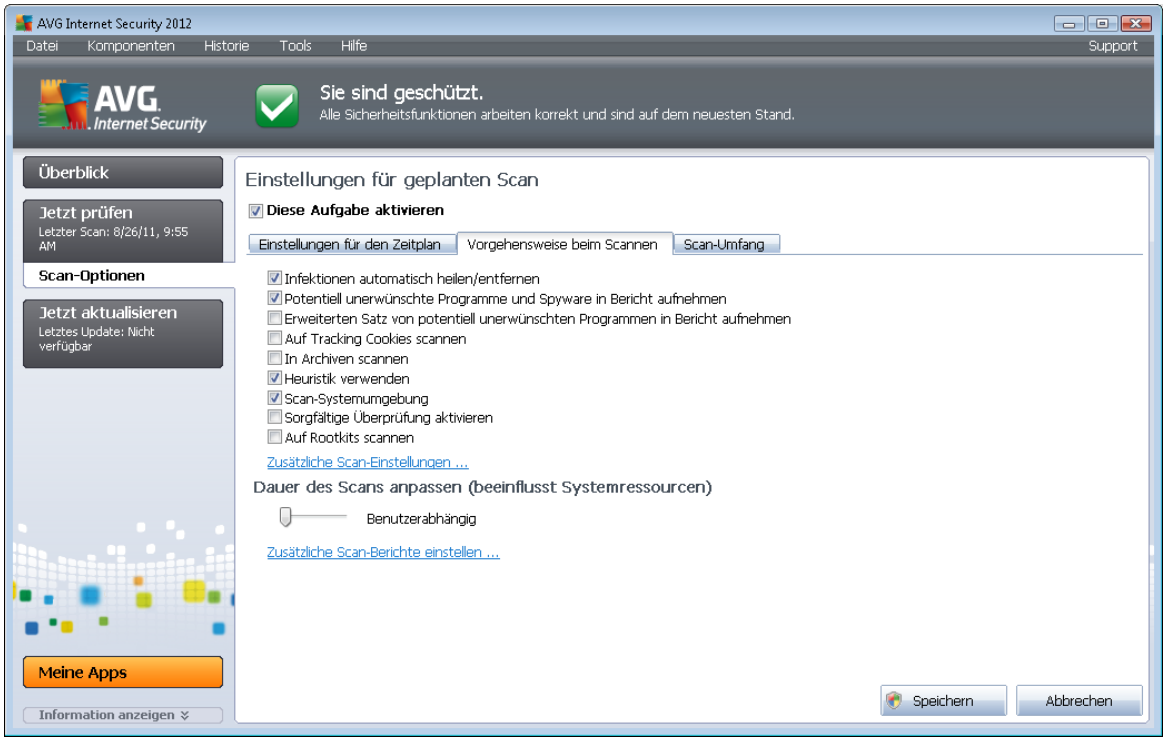
Schaltflächen im Dialog „Einstellungen für geplanten Scan“

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern *(Einstellungen für den Zeitplan, Vorgehensweise beim Scannen und Scan-Umfang)* zwei Schaltflächen zur Verfügung, die auf allen Reitern die gleichen Funktionen 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.

11.5.2. 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 zur Verfügung steht. 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*): Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*): Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

- ***In Archiven scannen*** (*standardmäßig deaktiviert*): Dieser Parameter legt fest, dass bei Scans alle Dateien überprüft werden sollen, selbst solche, die 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.

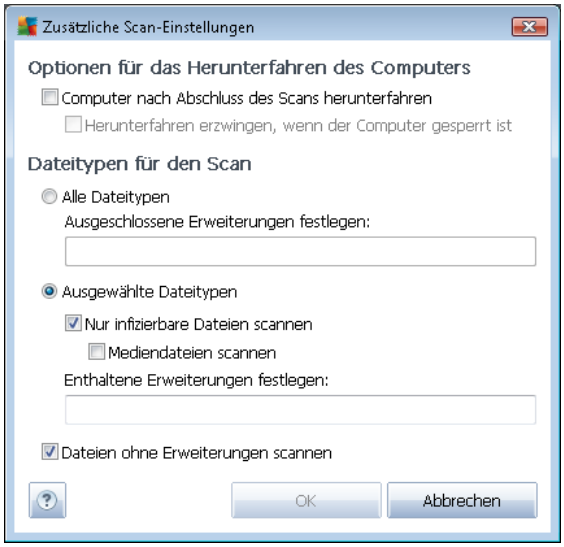
- ***Scan-Systemumgebung*** (*standardmäßig aktiviert*): Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***Auf Rootkits scannen*** (*standardmäßig deaktiviert*): 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*** – 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;

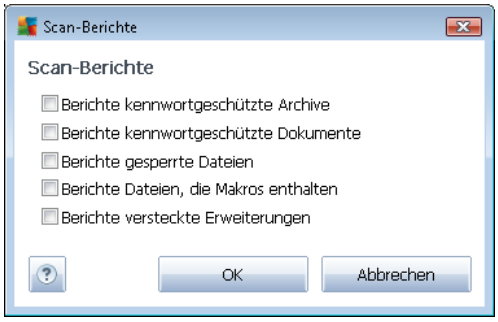
  - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien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

- ***Dauer des Scans anpassen*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. 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:



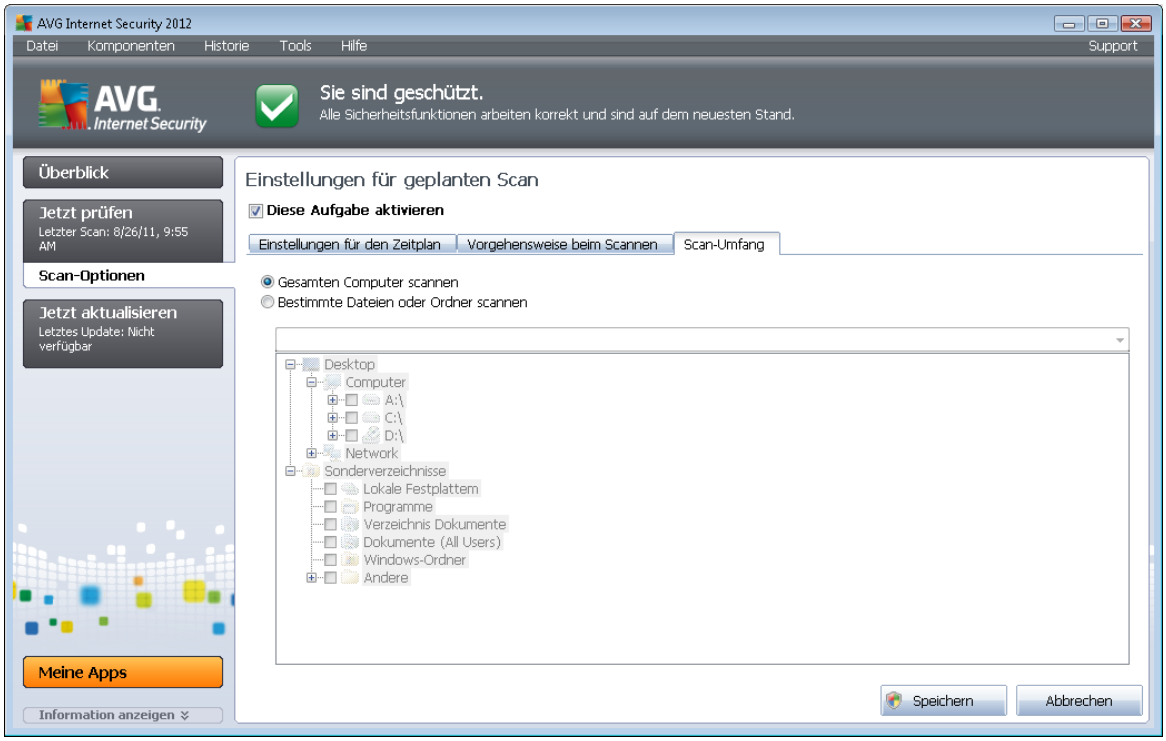
Schaltflächen

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (*Einstellungen für den Zeitplan, Vorgehensweise beim Scannen und Zu scannende Objekte*) zwei Schaltflächen zur Verfügung, die auf allen Reitern die gleichen Funktionen 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 ***Scan-Umfang*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien oder 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. (*Sie können Elemente einblenden, indem Sie auf das Plus-Zeichen klicken, bis Sie den zu scannenden Ordner finden.*) Sie können mehrere Ordner auswählen, indem Sie die entsprechenden Kästchen aktivieren. Die ausgewählten Ordner erscheinen im Textfeld im oberen Bereich des Dialogs. Im Dropdown-Menü wird Ihr Scanverlauf für einen späteren Gebrauch festgehalten. Alternativ können Sie den vollständigen Pfad zu dem gewünschten Ordner manuell eingeben (*bei mehreren Pfaden müssen diese mit einem Semikolon ohne Leerzeichen voneinander getrennt werden*).

Innerhalb der Baumstruktur sehen Sie einen Zweig namens ***Spezielle Speicherorte***. Im Folgenden wird eine Liste mit Speicherorten aufgeführt, die nach Aktivierung des entsprechenden Kontrollkästchens gescannt werden:

- ***Lokale Festplatten*** – alle Festplatten Ihres Computers
- ***Programmdateien***
  - C:\Programme\
  - *in 64-Bit-Versionen* C:\Programme (x86)

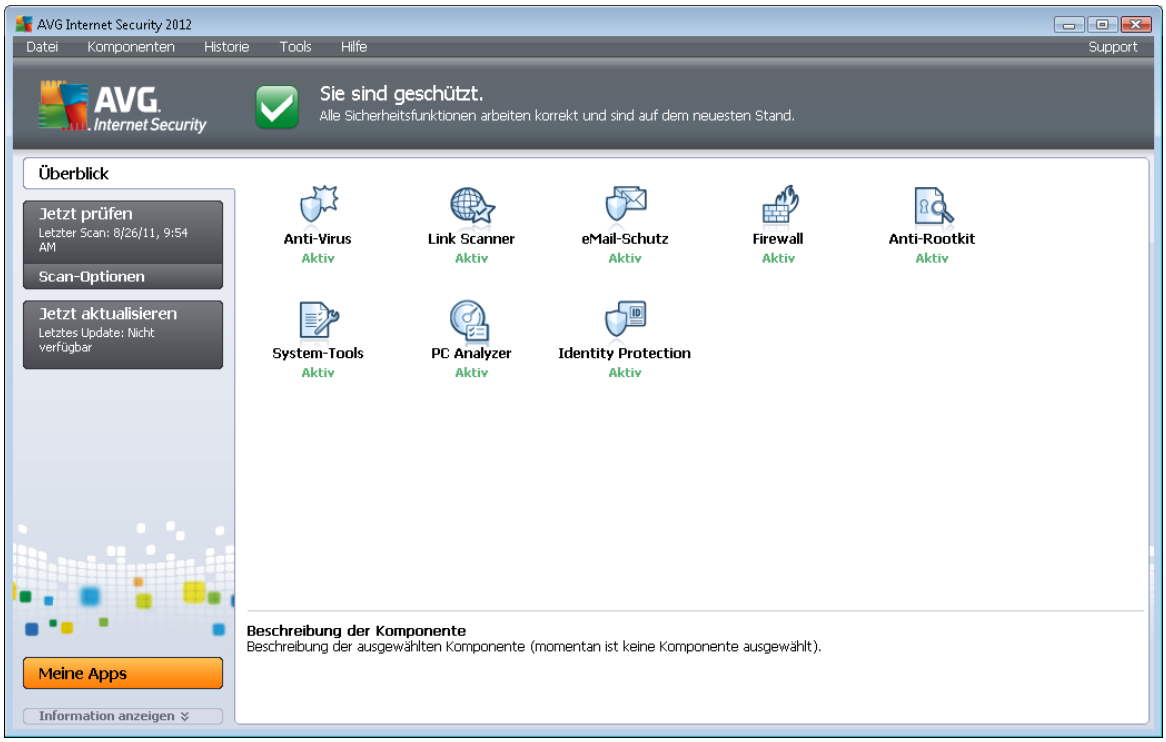
- ***Ordner „Eigene Dateien“***
    - *unter Windows XP*: C:\Dokumente und Einstellungen\Standardbenutzer\Eigene Dateien\
    - *unter Windows Vista/7*: C:\Benutzer\"Benutzername"\Dokumente\
- ***Gemeinsame Dokumente***
    - *unter Windows XP:* : C:\Dokumente und Einstellungen\Alle Benutzer\Dokumente\
    - *unter Windows Vista/7*: C:\Benutzer\Öffentlich\Dokumente\
- ***Windows-Ordner*** – C:\Windows\
- ***Andere***
    - *Systemlaufwerk* – die Festplatte, auf der das Betriebssystem installiert ist (normalerweise C:)
    - *Systemordner* – C:\Windows\System32\
    - *Ordner „Temporäre Dateien“* – C:\Dokumente und Einstellungen\Benutzer\Lokal (*Windows XP*oder C:\Benutzer\"Benutzername"\AppData\Local\Temp *Windows Vista/7*)
    - *Temporäre Internetdateien* – C:\Dokumente und Einstellungen\Benutzer\Lokale Einstellungen\Temporäre Internetdateien\ (*Windows XP*) oder C:\Benutzer\"Benutzername"\AppData\Local\Microsoft\Windows\Temporäre Internetdateien (*Windows Vista/7*)

Schaltflächen

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern *(Einstellungen für den Zeitplan, Vorgehensweise beim Scannen und Scan-Umfang)* dieselben zwei Schaltflächen zur Verfügung:

- ***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.

11.6. 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 SchaltflächeDetails 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
- ***Warnungen*** – Anzahl der erkannten verdächtigen Objekte
- ***Rootkits*** – Anzahl der erkannten Rootkits
- ***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*** – Klicken Sie auf diese Schaltfläche, um in den Dialog Scan-Ergebnisse zu wechseln und genaue Daten zu einem ausgewählten Scan anzuzeigen
- ***Ergebnis löschen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Eintrag aus der Übersicht der Scan-Ergebnisse zu löschen
- ***Zurück*** – Mit dieser Schaltfläche gelangen Sie zurück zum Standarddialog der Scan-Oberfläche von AVG

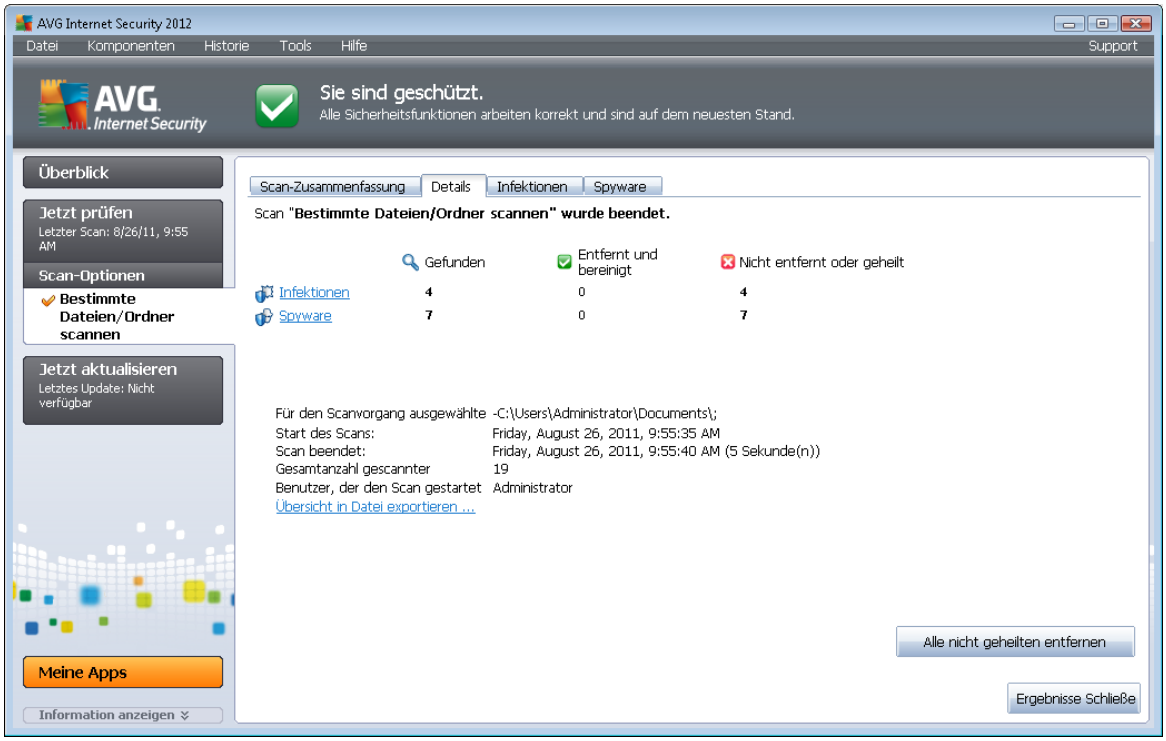
11.7. Details zu den Scan-Ergebnissen

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 angezeigt, wenn während eines Scans Cookies erkannt wurden
- 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. Sie finden dort auch Informationen zu Objekten, die nicht gescannt werden können *(z. B. kennwortgeschützte Archive)*.

11.7.1. Reiter „Ergebnisübersicht"



Auf dem Reiter ***Scan-Ergebnisse*** finden Sie eine genauere Statistik mit folgenden Informationen:

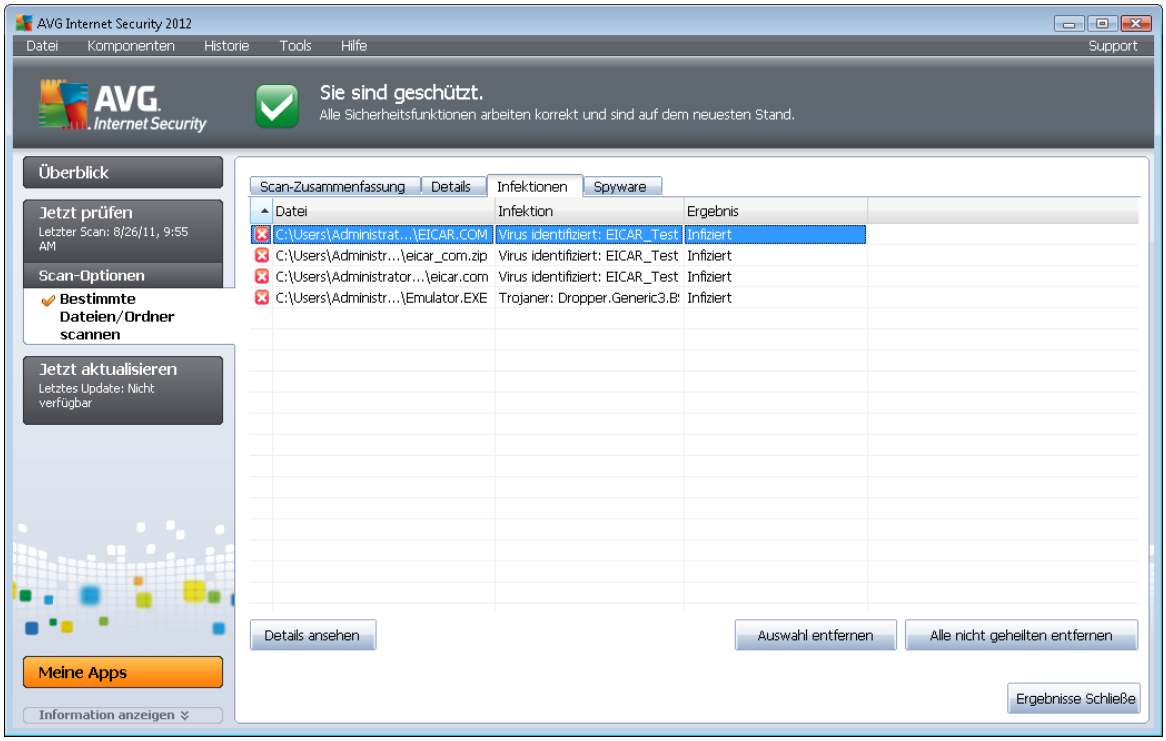
- Erkannte Vireninfektionen / Spyware
- Entfernte Vireninfektionen / Spyware
- Anzahl der Vireninfektionen / Spyware, die nicht entfernt oder geheilt werden konnte

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 unterteilt, die folgende Informationen enthalten:

- ***Datei*** – Der vollständige Pfad zum ursprünglichen Standort 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*

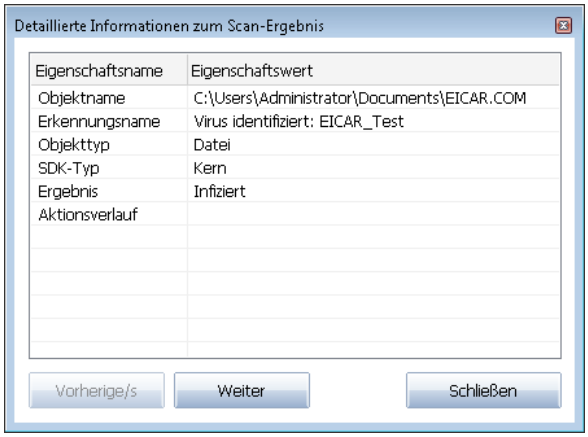
in den erweiterten Einstellungen)

- ***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. Um es vollständig zu entfernen, müssen Sie Ihren Computer neu starten

Schaltflächen

In diesem Dialog stehen drei Schaltflächen zur Verfügung:

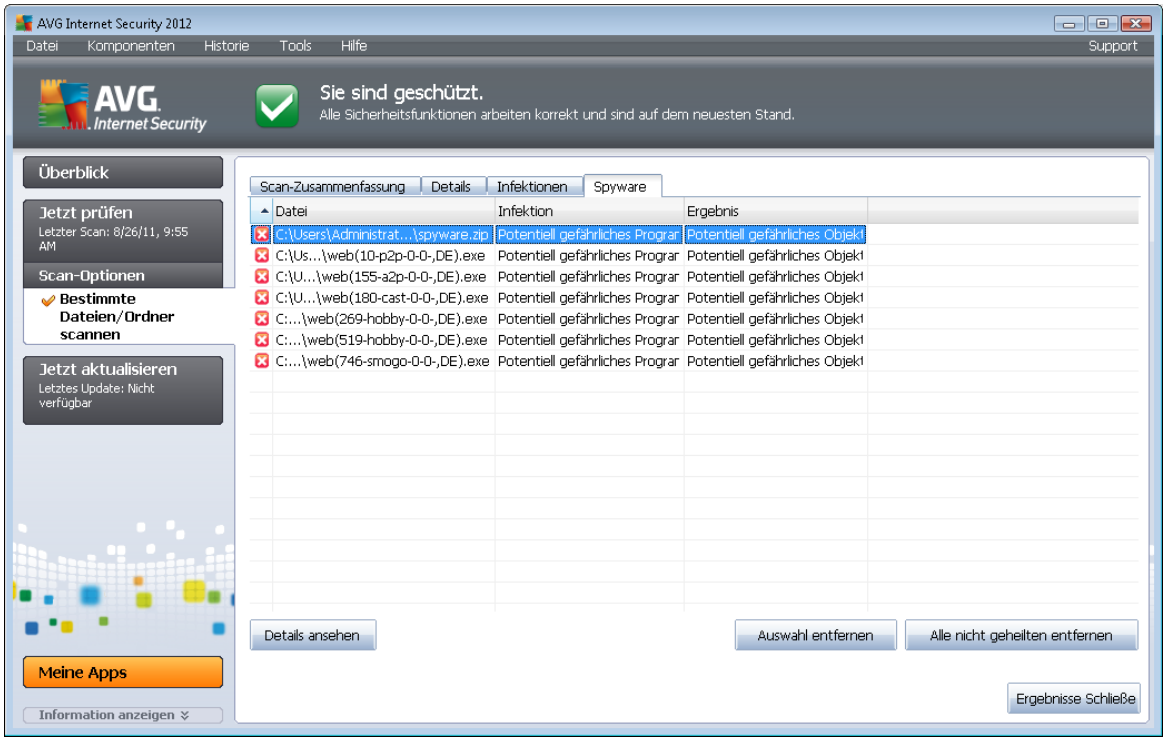
- ***Details ansehen*** – Diese Schaltfläche öffnet einen neuen Dialog ***Detaillierte Objektinformationen***:



  In diesem Dialog finden Sie weitere Informationen zum erkannten, infizierten Objekt (*z. B. Name und Speicherort des infizierten Objekts, Objekttyp, SDK-Typ, Erkennungsergebnis und Aktionsverlauf des infizierten Objekts*). 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.

- ***Auswahl entfernen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Fund in die Virenquarantäne zu verschieben
- ***Alle nicht geheilten 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:

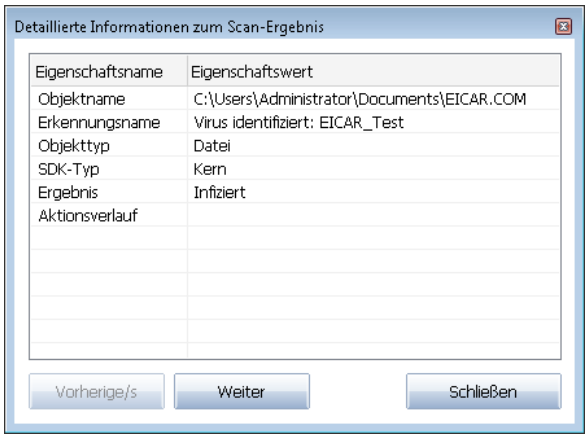
- ***Datei*** – Der vollständige Pfad zum ursprünglichen Standort des infizierten Objekts
- ***Infektionen*** – Name der erkannten Spyware *(genauere Informationen zu bestimmten Viren finden Sie in der Virenenzyklopädie online)*
- ***Ergebnis*** – Hier wird der aktuelle Status des beim Scan erkannten 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 Objektinformationen***:



  In diesem Dialog finden Sie weitere Informationen zum erkannten, infizierten Objekt (*z. B. Name und Speicherort des infizierten Objekts, Objekttyp, SDK-Typ, Erkennungsergebnis und Aktionsverlauf des infizierten Objekts*). 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.

- ***Auswahl entfernen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Fund in die Virenquarantäne zu verschieben
- ***Alle nicht geheilten entfernen*** – Diese Schaltfläche löscht alle Funde, die nicht geheilt oder in die Virenquarantäne
- ***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 in den Testergebnissen nur Warnungen vorkommen, die von **AVG Internet Security 2012** erkannt wurden, ist keine Aktion notwendig.

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 **AVG Internet Security 2012** eine versteckte Datei meldet, die verseucht sein könnte, können Sie diese in die 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 Rootkits angezeigt, die beim Anti-Rootkit-Scan erkannt wurden.

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"

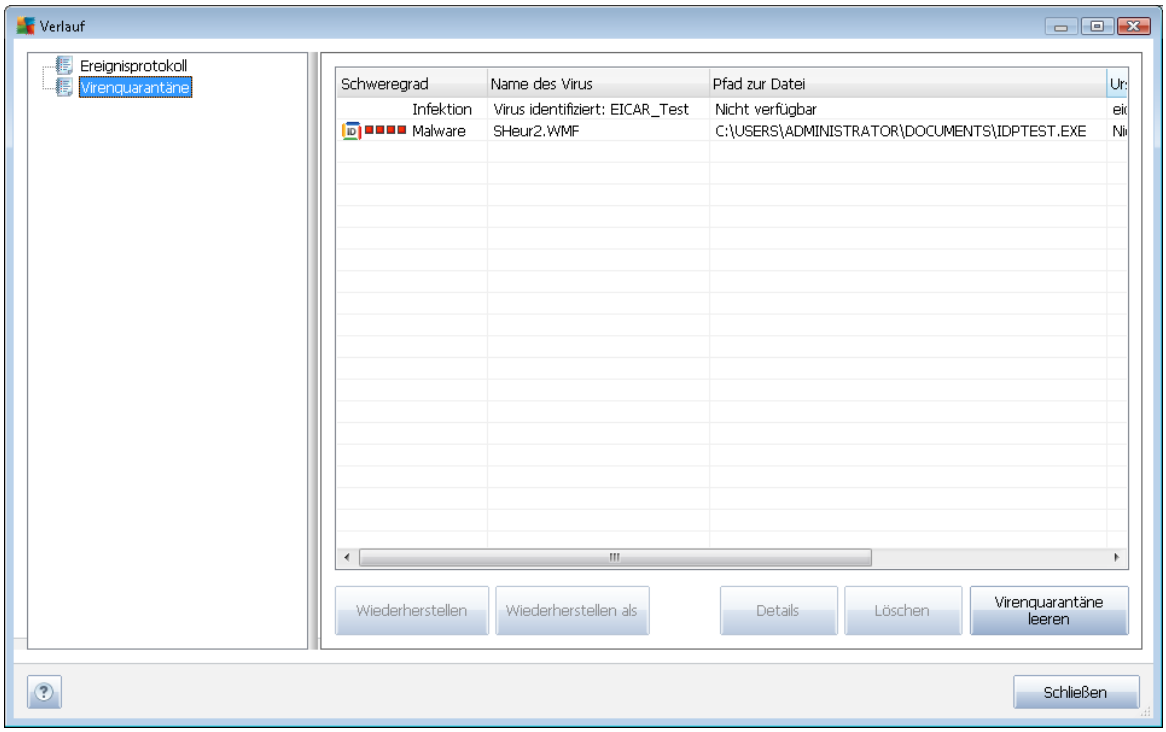
Der Reiter ***Informationen*** enthält Daten über „Funde", die nicht als Infektionen, Spyware usw. eingestuft werden können. Sie können nicht eindeutig als gefährlich klassifiziert werden, müssen jedoch trotzdem beachtet werden. Der Scan von **AVG Internet Security 2012** kann auch Dateien

erkennen, die zwar nicht infiziert, aber dennoch 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 Internet Security 2012** (*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 Internet Security 2012** 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 diese Unstimmigkeit. **AVG Internet Security 2012** 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 Internet Security 2012** 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 ***Virenquarantäne*** ist in erster Linie dazu da, entfernte Dateien so lange zu speichern, bis sie an ihrem ursprünglichen Speicherort nicht mehr benötigt werden. Wenn das Fehlen der Datei Probleme bereitet, können Sie die fragliche Datei zur Analyse senden oder sie an ihrem ursprünglichen Speicherort wiederherstellen.

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*** – Wenn Sie sich zur Installation der Komponente Identitätsschutz in **AVG Internet Security 2012** entschieden haben, wird eine grafische Identifizierung des entsprechenden Schweregrads des Prozesses auf einer vierstufigen Skala von unbedenklich (■□□□) bis sehr gefährlich (■■■■) angezeigt sowie die Informationen zur Infektionsart (*basierend auf ihrer Infektionsstufe – alle aufgelisteten 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

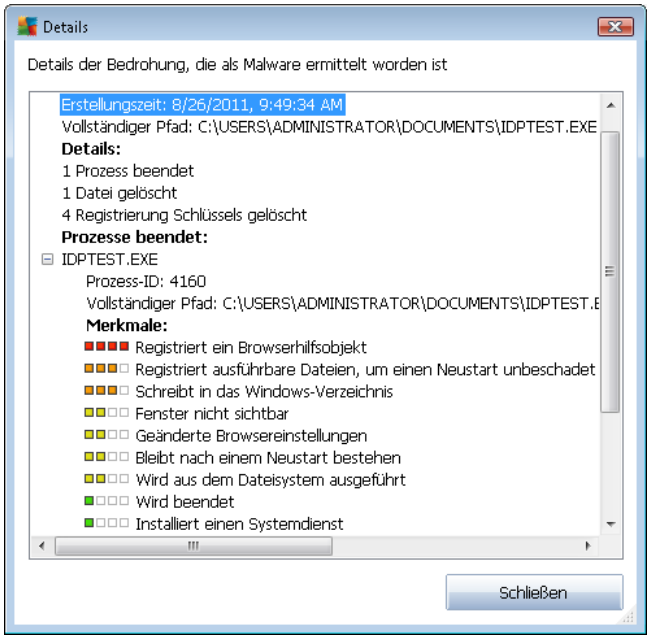
des Scanvorgangs mit dem Standardnamen gekennzeichnet. Wenn das Objekt einen bekannten ursprünglichen Namen hat (*z. B. der Name eines eMail-Anhangs, der nicht mit dem eigentlichen Inhalt des Anhangs übereinstimmt*), wird der Name in dieser Spalte angegeben.

- ***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*** – Die infizierte Datei wird in den ausgewählten Ordner verschoben
- ***Details*** – Diese Schaltfläche gilt nur für Bedrohungen, die von Identitätsschutz gefunden wurden. Nach dem Anklicken wird eine zusammenfassende Übersicht über die Bedrohungsdetails angezeigt (*welche Dateien/Prozesse sind betroffen, Merkmale des Prozesses usw.*). Bitte beachten Sie, dass die Schaltfläche bei allen anderen Bedrohungen, die nicht von Identitätsschutz entdeckt wurden, ausgegraut und inaktiv ist!



- ***Löschen*** – Die infizierte Datei wird vollständig und unwiederbringlich aus der ***Virenquarantäne*** gelöscht
- ***Virenquarantäne leeren*** - Alle Objekte werden vollständig aus der ***Virenquarantäne*** entfernt. Durch das Entfernen der Dateien aus der ***Virenquarantäne*** werden diese Dateien unwiderruflich von der Festplatte entfernt (*sie werden nicht in den Papierkorb verschoben*).

12. AVG Updates

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.

Angesichts der vielen neuen Computerbedrohungen und der Geschwindigkeit, mit der sie sich verbreiten, ist es besonders wichtig, dass Sie Ihr **AVG Internet Security 2012** regelmäßig aktualisieren. Am besten ist es, die Standardeinstellungen des Programms beizubehalten, in denen das automatische Update konfiguriert ist. Bitte beachten Sie, dass das Programm die neuesten Bedrohungen nicht erkennen kann, wenn die Virendatenbank von **AVG Internet Security 2012** nicht auf dem neuesten Stand ist.

Es ist entscheidend, dass Sie AVG regelmäßig aktualisieren! Wenn möglich, sollten Virendefinitionen täglich aktualisiert werden. Weniger dringende Programmupdates können wöchentlich gestartet werden.

12.1. Update-Start

Um die größtmögliche Sicherheit zu gewährleisten, sucht **AVG Internet Security 2012** in der Standardeinstellung alle vier Stunden nach neuen Updates. Da AVG-Updates nicht nach einem festen Zeitplan, sondern entsprechend der Anzahl und des Schweregrads neuer Bedrohungen zur Verfügung gestellt werden, ist diese Überprüfung äußerst wichtig, um sicherzustellen, dass Ihre Virendatenbank von AVG jederzeit auf dem neuesten Stand ist.

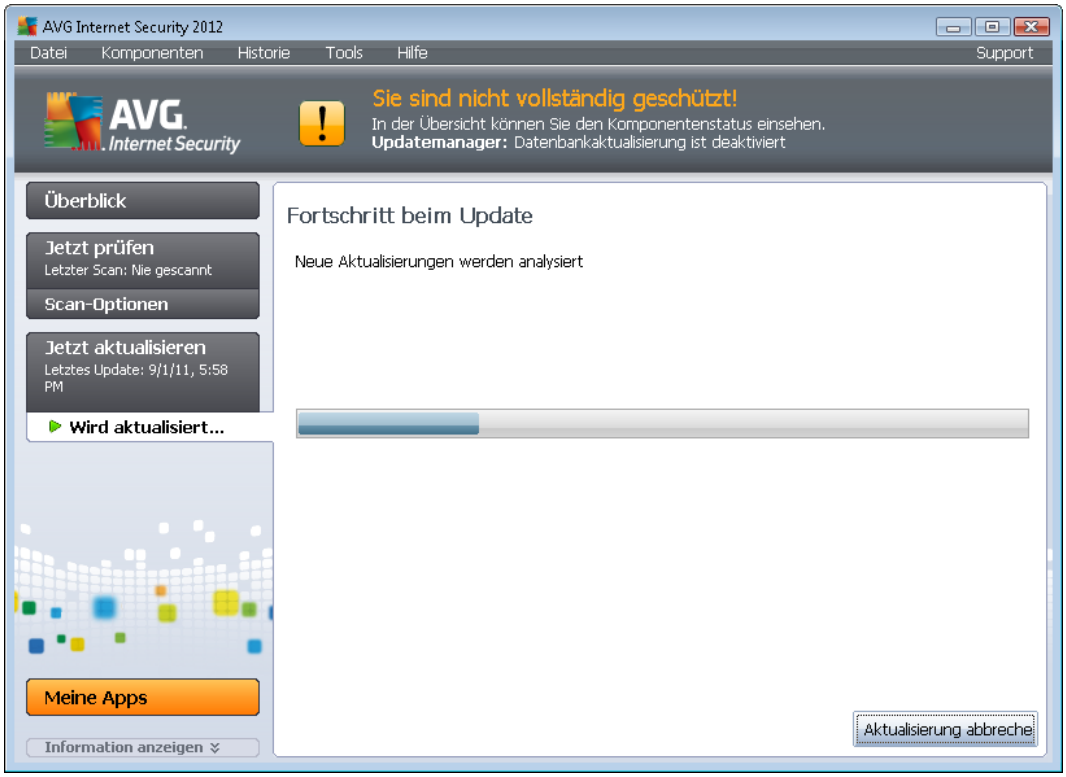
Wenn Sie die Anzahl solcher Update-Starts reduzieren möchten, können Sie Ihre eigenen Parameter für den Update-Start festlegen. Es wird jedoch dringend empfohlen, mindestens einmal täglich ein Update auszuführen! Die Konfiguration kann im Bereich Erweiterte Einstellungen/ Zeitpläne bearbeitet werden, insbesondere in den folgenden Dialogen:

- Zeitplan für Update der Definitionen
- Zeitplan für Update des Programms
- Zeitplan für Anti-Spam-Aktualisierung

Wenn Sie die neuen Updatedateien sofort überprüfen möchten, verwenden Sie den Quick Link Jetzt aktualisieren auf der Hauptbenutzeroberfläche. Dieser Link steht Ihnen jederzeit in allen Dialogen der Benutzeroberfläche von zur Verfügung.

12.2. Updatefortschritt

Wenn Sie das Update starten, überprüft AVG zunächst, ob neue Updatedateien zur Verfügung stehen. Ist dies der Fall, startet **AVG Internet Security 2012** den Download dieser Dateien und ruft auch selbst den Updatevorgang auf. Während des Updatevorgangs werden Sie zur Benutzeroberfläche ***Update*** weitergeleitet, wo der Fortschritt des Updates grafisch dargestellt und eine Übersicht über die statistischen Parameter (*Größe der Updatedatei, empfangene Daten, Download-Geschwindigkeit, verstrichene Zeit usw.*) angezeigt wird:



***Hinweis**: Vor jedem 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 das Windows-Menü Start/Programme/Zubehör/Systemprogramme/Systemwiederherstellung aufgerufen werden. Eine Änderung dieser Einstellungen wir nur erfahrenen Benutzern empfohlen!*

12.3. Updatestufen

Bei **AVG Internet Security 2012** können Sie zwischen zwei Updatestufen wählen:

- ***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.

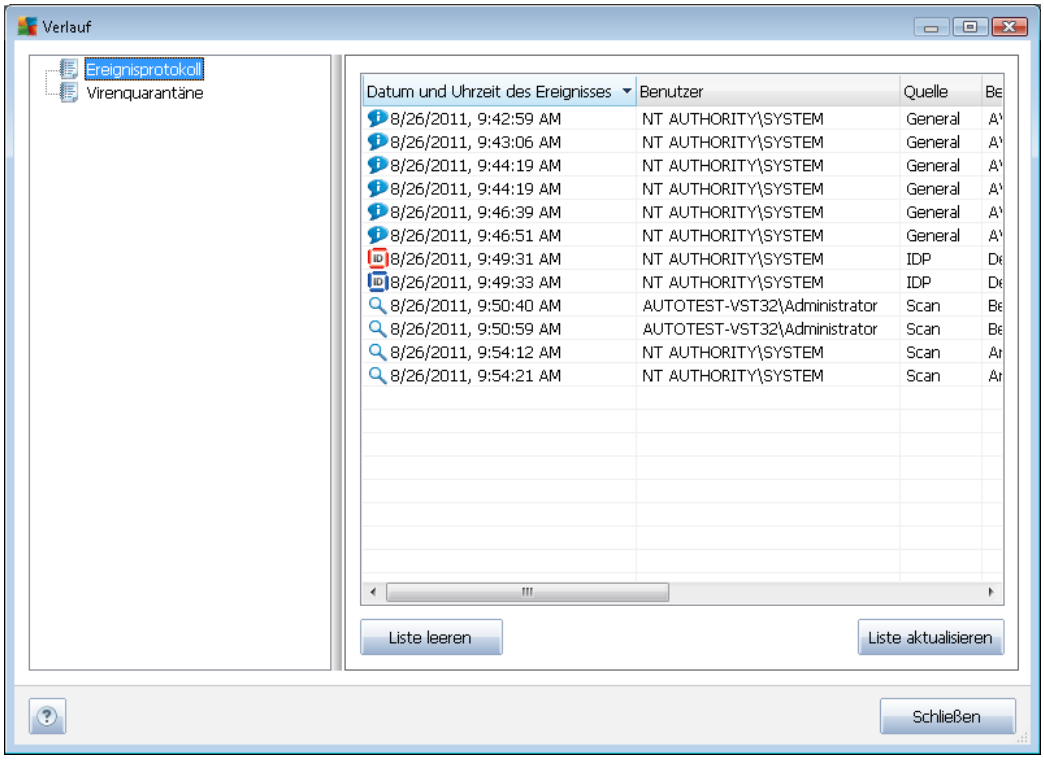
Beim Planen von Updates können Sie bestimmte Parameter für beide Updatestufen definieren:

- Zeitplan für Update der Definitionen

- Zeitplan für Update des Programms

***Hinweis:** Wenn sich ein geplantes Programm-Update und ein geplanter Scan zeitlich überschneiden, wird der Scan unterbrochen, da das Update eine höhere Priorität hat.*

13. Ereignisprotokoll



Der Dialog ***Historie*** 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 Internet Security 2012** aufgetreten sind. In der ***Historie*** werden folgende Ereignistypen aufgezeichnet:

- Informationen über Updates der AVG-Anwendung
- Informationen über Start, Ende oder Unterbrechung des Scans (*einschließlich automatisch ausgeführter Tests*)
- Ereignisse in Verbindung mit der Virenerkennung (*entweder durch den Residenten Schutz oder einen Scan*), einschließlich des Ortes, an dem das Ereignis aufgetreten ist
- Andere wichtige Ereignisse

Für jedes Ereignis werden die folgenden Informationen aufgelistet:

- ***Datum und Uhrzeit des Ereignisses*** gibt das Datum und die exakte Uhrzeit des Ereignisses an
- ***Benutzer*** nennt den Namen des Benutzers, der zur Zeit des Ereignisses angemeldet war
- ***Quelle*** gibt Informationen zu einer Quellkomponente oder einem anderen Teil des AVG-Systems an, von der bzw. dem das Ereignis ausgelöst wurde

- ***Beschreibung des Ereignisses*** gibt eine kurze Zusammenfassung der tatsächlichen Geschehnisse.

Schaltflächen

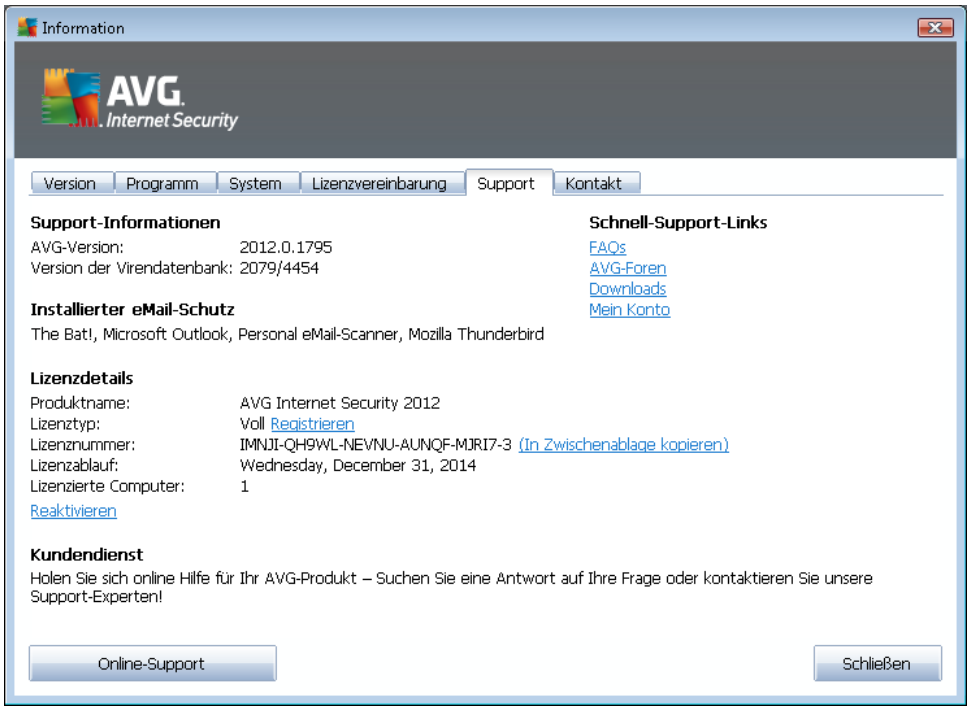
- ***Liste leeren***– Klicken Sie auf die Schaltfläche, um alle Einträge in der Ereignisliste zu löschen
- ***Liste aktualisieren***– Klicken Sie auf die Schaltfläche, um alle Einträge in der Ereignisliste zu aktualisieren

14. FAQ und technischer Support

Wenn Probleme mit dem Vertrieb oder technische Probleme mit Ihrer Anwendung **AVG Internet Security 2012** auftreten, stehen verschiedene Möglichkeiten zur Verfügung, Hilfe in Anspruch zu nehmen. Bitte wählen Sie eine der folgenden Optionen:

- ***Kundendienst kontaktieren***: Sie können sich direkt von der AVG-Anwendung aus an unseren professionellen Kundendienst wenden. Wählen Sie im Hauptmenü den Eintrag ***Hilfe/Onlinehilfe*** aus, um zum Online-Kontaktformular weitergeleitet zu werden. Darüber steht Ihnen der Kundendienst von AVG rund um die Uhr zur Verfügung. Ihre Lizenznummer wird automatisch eingefügt. Folgen Sie zum Fortfahren den Anweisungen auf der Webseite.

- ***Support (Link im Hauptmenü)***: Das Menü der AVG-Anwendung (*im oberen Bereich der Hauptbenutzeroberfläche*) enthält den Link ***Support***, der einen neuen Dialog mit Informationen öffnet, die Sie bei der Suche nach Hilfe unterstützen. Der Dialog beinhaltet grundlegende Informationen über Ihr installiertes AVG-Programm (*Programm-/ Datenbankversion*), Lizenzdetails sowie eine Liste mit Schnell-Support-Links:



- ***Problembehandlung in der Hilfedatei***: Ein neuer Abschnitt ***Problembehandlung*** steht direkt in der Hilfedatei von **AVG Internet Security 2012**zur Verfügung. Dieser Abschnitt enthält eine Liste der häufigsten Situationen, in denen ein Benutzer professionelle Hilfe zu einem technischen Problem sucht. Bitte wählen Sie die Situation aus, die Ihr Problem am besten beschreibt, und klicken Sie darauf, um detaillierte Anweisungen zur Lösung des Problems zu anzuzeigen.

- ***Support Center auf der Website von AVG***: Alternativ können Sie die Lösung zu Ihrem Problem auch auf der Website von AVG suchen (http://www.avg.com/de/). Im Bereich ***Support Center*** finden Sie eine gegliederte Übersicht mit thematischen Gruppen zu Problemen mit dem Vertrieb und technischen Problemen.

- ***Häufig gestellte Fragen***: Auf der Website von AVG (http://www.avg.com/de/) finden Sie außerdem einen gesonderten und klar strukturierten Abschnitt mit häufig gestellten Fragen. Dieser Abschnitt kann über die Menüoption ***Support Center/FAQ*** aufgerufen werden. Alle Fragen sind hier übersichtlich in die Kategorien Vertriebs-FAQ, Technische FAQ und FAQ zu Viren gegliedert.

- ***Infos zu Viren und Bedrohungen***: Dieser Bereich auf der Website von AVG (http://www.avg.com/de/) befasst sich mit dem Thema Viren. Wählen Sie im Menü ***Support Center/ Infos zu Viren und Bedrohungen*** aus, um zu einer Seite mit übersichtlichen Informationen zu Online-Bedrohungen zu gelangen. Dort finden Sie außerdem Anweisungen zum Entfernen von Viren und Spyware sowie Ratschläge zur Aufrechterhaltung Ihres Schutzes.

- ***Diskussionsforum***: Sie können auch das Benutzerdiskussionsforum von AVG unter http:// http://forums.avg.com/eu-de verwenden.