



AVG File Server 2011

Benutzerhandbuch

Dokumentversion 2011.01 (20. 9. 2010)

Copyright AVG Technologies CZ, s.r.o. Alle Rechte vorbehalten.
Alle anderen Markenzeichen sind das Eigentum der jeweiligen Inhaber.

Dieses Produkt verwendet RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Erstellt 1991.

Dieses Produkt verwendet Code aus der Bibliothek C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Dieses Produkt verwendet die Kompressionsbibliothek zlib, Copyright © 1995-2002 Jean-Loup Gailly und Mark Adler.

Dieses Produkt verwendet die Kompressionsbibliothek libbzip2, Copyright © 1996-2002 Julian R. Seward.



Inhalt

1. Einleitung	6
2. Installationsvoraussetzungen für AVG	7
2.1 Unterstützte Betriebssysteme	7
2.2 Minimale und empfohlene Hardware-Anforderungen	7
3. Optionen für die Installation von AVG	8
4. Installationsvorgang bei AVG	9
4.1 Willkommen	9
4.2 AVG-Lizenz aktivieren	10
4.3 Wählen Sie die Installationsart aus	11
4.4 Benutzerdefinierte Optionen	12
4.5 Installationsfortschritt	13
4.6 Die Installation wurde erfolgreich abgeschlossen	13
5. Nach der Installation	15
5.1 Produktregistrierung	15
5.2 Zugriff auf die Benutzeroberfläche	15
5.3 Gesamten Computer scannen	15
5.4 Standardkonfiguration von AVG	15
6. Benutzeroberfläche von AVG	16
6.1 Systemmenü	17
6.1.1 Datei	17
6.1.2 Komponenten	17
6.1.3 Historie	17
6.1.4 Tools	17
6.1.5 Hilfe	17
6.2 Informationen zum Sicherheitsstatus	19
6.3 Quick Links	20
6.4 Komponentenübersicht	21
6.5 Server-Komponenten	22
6.6 Statistik	23
6.7 Infobereich-Symbol	23
7. Komponenten von AVG	25



7.1 Anti-Virus	25
7.1.1 Grundlagen zu Anti-Virus	25
7.1.2 Benutzeroberfläche des Anti-Virus	25
7.2 Anti-Spyware	26
7.2.1 Grundlagen zu Anti-Spyware	26
7.2.2 Benutzeroberfläche der Anti-Spyware	26
7.3 Residenter Schutz	28
7.3.1 Grundlagen zu Residenter Schutz	28
7.3.2 Benutzeroberfläche des Residenten Schutzes	28
7.3.3 Erkennungen durch den Residenten Schutz	28
7.4 Updatemanager	33
7.4.1 Grundlagen zum Updatemanager	33
7.4.2 Benutzeroberfläche des Updatemanagers	33
7.5 Lizenz	36
7.6 Remote-Verwaltung	37
7.7 Anti-Rootkit	38
7.7.1 Grundlagen zu Anti-Rootkit	38
7.7.2 Benutzeroberfläche von Anti-Rootkit	38
8. AVG Einstellungsmanager	41
9. AVG Server-Komponenten	44
9.1 Document Scanner für MS SharePoint	44
9.1.1 Grundlagen zu Document Scanner	44
9.1.2 Benutzeroberfläche von Document Scanner	44
10. AVG für SharePoint Portal Server	46
10.1 Programmwartung	46
10.2 AVG für SPPS-Konfiguration – SharePoint 2007	46
10.3 AVG für SPPS-Konfiguration – SharePoint 2003	48
11. Erweiterte Einstellungen von AVG	50
11.1 Darstellung	50
11.2 Sounds	52
11.3 Fehlerhaften Zustand ignorieren	54
11.4 Virenquarantäne	55
11.5 PUP-Ausnahmen	55
11.6 Scans	57
11.6.1 Gesamten Computer scannen	57



11.6.2	Shell-Erweiterungs-Scan	57
11.6.3	Bestimmte Dateien/Ordner scannen	57
11.6.4	Scan des Wechseldatenträgers	57
11.7	Zeitpläne	63
11.7.1	Geplanter Scan	63
11.7.2	Zeitplan für Update der Virendatenbank	63
11.7.3	Zeitplan für Update des Programms	63
11.8	Residenter Schutz	73
11.8.1	Erweiterte Einstellungen	73
11.8.2	Ausgeschlossene Einträge	73
11.9	Cache-Server	77
11.10	Anti-Rootkit	78
11.11	Aktualisierung	79
11.11.1	Proxy	79
11.11.2	DFÜ	79
11.11.3	URL	79
11.11.4	Verwalten	79
11.12	Remote-Verwaltung	86
11.13	Server-Komponenten	87
11.13.1	Document Scanner für MS SharePoint	87
11.13.2	Erkennungsaktionen	87
11.14	AVG-Schutz vorübergehend deaktivieren	90
11.15	Programm zur Produktverbesserung	91
12.	AVG-Scans	93
12.1	Benutzeroberfläche für Scans	93
12.2	Vordefinierte Scans	94
12.2.1	Scan des gesamten Computers	94
12.2.2	Bestimmte Dateien/Ordner scannen	94
12.2.3	Anti-Rootkit-Scan	94
12.3	Scans aus dem Windows Explorer	104
12.4	Scannen von Befehlszeilen	105
12.4.1	Parameter für CMD-Scan	105
12.5	Scans planen	108
12.5.1	Einstellungen für den Zeitplan	108
12.5.2	Vorgehensweise beim Scannen	108
12.5.3	Zu testende Objekte	108
12.6	Übersicht über Scan-Ergebnisse	117



12.7 Details zu den Scan-Ergebnissen	118
12.7.1 Reiter „Ergebnisübersicht“	118
12.7.2 Reiter „Infektionen“	118
12.7.3 Reiter „Spyware“	118
12.7.4 Reiter „Warnungen“	118
12.7.5 Reiter „Rootkits“	118
12.7.6 Reiter „Informationen“	118
12.8 Virenquarantäne	126
13. AVG Updates	128
13.1 Updatestufen	128
13.2 Updatetypen	128
13.3 Updatevorgang	128
14. Ereignisprotokoll	130
15. FAQ und technischer Support	132



1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG File Server 2011**.

Herzlichen Glückwunsch zum Kauf von AVG File Server 2011!

AVG File Server 2011 zählt zu einer Reihe von preisgekrönten AVG-Produkten, die vollständige Sicherheit für Ihren PC bieten, damit Sie in Ruhe arbeiten können. Wie alle AVG-Produkte wurde **AVG File Server 2011** von Grund auf vollkommen neu gestaltet, um den anerkannten Schutz von AVG noch benutzerfreundlicher und effizienter bereitzustellen. Ihr neues **AVG File Server 2011**-Produkt verfügt über eine optimierte Benutzeroberfläche sowie aggressivere und schnellere Scans. Die Anzahl der automatisierten Sicherheitsfunktionen wurde zu Ihrer Unterstützung erhöht und neue ‚intelligente‘ Benutzeroptionen hinzugefügt, damit Sie unsere Sicherheitsfunktionen besser an Ihre Bedürfnisse anpassen können. Einfache Verwendung und hohe Sicherheit schließen einander nicht aus!

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

Alle AVG-Produkte bieten folgende Vorteile:

- Schutz für den individuellen Umgang mit Ihrem Computer und dem Internet: Banking, Shopping, Surfen und Suchen, Chatten, Mailen, Dateien herunterladen oder Aktivitäten in sozialen Netzwerken – AVG liefert das richtige Produkt für Ihren individuellen Bedarf
- Sorgenfreier Schutz, dem mehr als 110 Millionen Menschen auf der ganzen Welt vertrauen und der ständig von einem globalen Netzwerk erfahrener Researcher weiterentwickelt wird
- Schutz mit Experten-Support rund um die Uhr



2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG File Server 2011 wurde für den Schutz von Workstations/Servern mit den folgenden Betriebssystemen entwickelt:

- Windows 2003 Server und Windows 2003 Server x64 Edition
- Windows 2008 Server und Windows 2008 Server x64 Edition

(sowie ggf. höhere Service Packs für bestimmte Betriebssysteme)

2.2. Minimale und empfohlene Hardware-Anforderungen

Minimale Hardware-Anforderungen für **AVG File Server 2011**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM-Speicher
- 470 MB an freiem Festplattenplatz (für die Installation)

Empfohlene Hardware-Anforderungen für **AVG File Server 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-Speicher
- 600 MB an freiem Festplattenplatz (für die Installation)



3. Optionen für die Installation von AVG

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

Vor der Installation von AVG sollten Sie auf jeden Fall prüfen, ob auf der Website von AVG (<http://www.avg.com/de>) eine neue Installationsdatei verfügbar ist. Auf diese Weise können Sie sicher sein, dass Sie die neueste verfügbare Version von AVG File Server 2011 installieren.

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



4. Installationsvorgang bei AVG

Für die Installation von **AVG File Server 2011** auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei online herunterzuladen. Sie können die Datei von der Website von AVG (<http://www.avg.com/de>) im Bereich **Support Center / Downloads** herunterladen.

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

4.1. Willkommen

Zu Beginn des Installationsvorgangs wird das Dialogfenster **Willkommen** angezeigt. Hier können Sie die Sprache für die Installation und die Standardsprache für die Benutzeroberfläche von AVG auswählen. Im oberen Bereich des Dialogs befindet sich ein Dropdown-Menü mit den zur Auswahl stehenden Sprachen:



Achtung: Hier wählen Sie nur die Sprache für den Installationsvorgang aus. Die ausgewählte Sprache wird als Standardsprache für die Benutzeroberfläche von AVG installiert. Daneben wird Englisch immer automatisch installiert. Wenn Sie weitere Sprachen für die Benutzeroberfläche installieren möchten, geben Sie die gewünschten Sprachen im Setup-Dialog **Benutzerdefinierte Optionen** an.

Dieser Dialog 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.



4.2. AVG-Lizenz aktivieren

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

Die Vertriebsnummer finden Sie auf der CD-Verpackung Ihres **AVG File Server 2011**-Pakets. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von **AVG File Server 2011** 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.

The screenshot shows a window titled "AVG-Installationsprogramm" with a close button in the top right corner. The window has a dark header bar containing the AVG logo and the text "Aktivieren Sie Ihre Lizenz". Below the header, there is a label "Lizenznummer:" followed by a text input field. Underneath the input field, a sample license number is provided: "Beispiel: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3". Two paragraphs of text provide instructions: the first paragraph explains that for online purchases, the license number is received via email and should be copied; the second paragraph explains that for retail purchases, the license number is on a registration card and should be copied accurately. At the bottom of the window, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

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

4.3. Wählen Sie die Installationsart aus



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

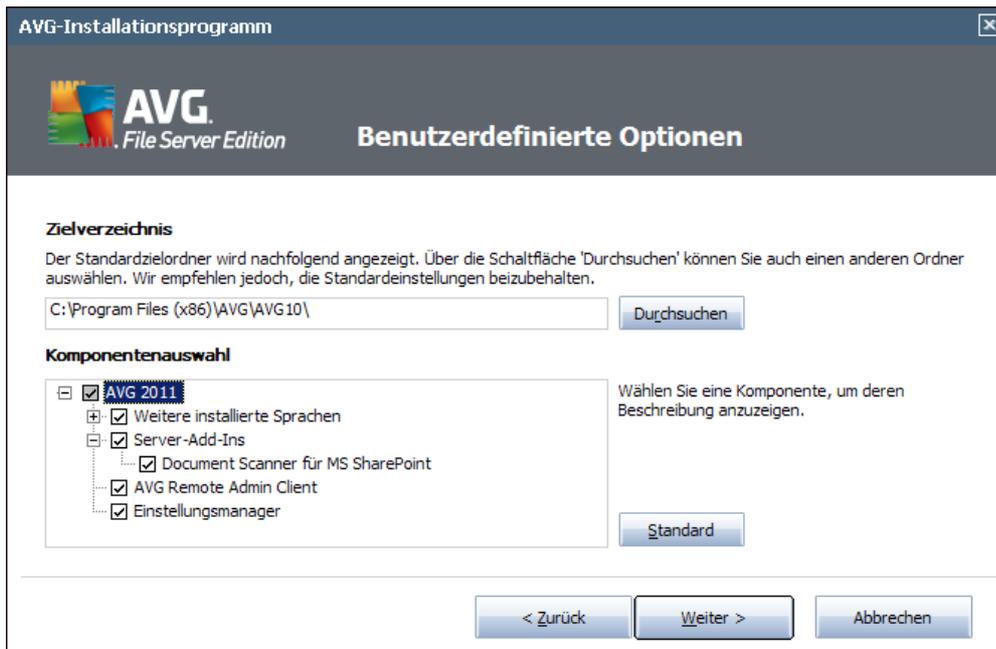
Den meisten Benutzern wird empfohlen, die standardmäßige **Schnellinstallation** beizubehalten, mit der AVG vollständig automatisch mit den vom Programmhersteller vordefinierten Einstellungen installiert wird. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration zukünftig geändert werden muss, können Sie diese Änderungen immer direkt in der Anwendung AVG vornehmen. Wenn Sie die Option **Schnellinstallation** ausgewählt haben, klicken Sie auf **Weiter**, um mit dem Dialog [Installationsfortschritt](#) fortzufahren.

Die **Benutzerdefinierte Installation** sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, AVG 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.



4.4. 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 File Server 2011** installiert werden soll. Standardmäßig wird AVG im Ordner C:/Programme installiert. Wenn der Ordner noch nicht existiert, werden Sie in einem Dialog dazu aufgefordert, der Erstellung dieses Ordners durch AVG zuzustimmen. Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf **Durchsuchen**, um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus.

Komponentenauswahl

Im Abschnitt **Komponentenauswahl** wird eine Übersicht über alle Komponenten von **AVG File Server 2011** 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.



- **Sprachauswahl**

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

- **Server-Add-Ins – Document Scanner für MS SharePoint**

Diese Komponente scannt in MS SharePoint gespeicherte Dokumente und schützt vor möglichen Bedrohungen. Es wird dringend empfohlen, diese Komponente zu installieren, da sie ein wichtiger Teil von **AVG File Server 2011** ist.

- **AVG Remote Admin Client**

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

- **Einstellungsmanager**

AVG Einstellungsmanager ist eine kleine Anwendung, mit der lokale Installationen von AVG schnell und einfach konfiguriert werden können (dazu gehören auch Installationen, die nicht unter Remote-Verwaltung ausgeführt werden). Diese Anwendung nutzt Konfigurationsdateien (im Format .pck), die mit AVG Einstellungsmanager einfach auf jedem Computer erstellt werden können, auf dem AVG installiert ist. Diese Dateien können anschließend auf einen Wechseldatenträger kopiert und auf jedem Computer verwendet werden. Dasselbe gilt natürlich auch für AVG Einstellungsmanager. Weitere Informationen zu dieser Anwendung finden Sie [hier](#).

Klicken Sie zum Fortfahren auf **Weiter**.

4.5. Installationsfortschritt

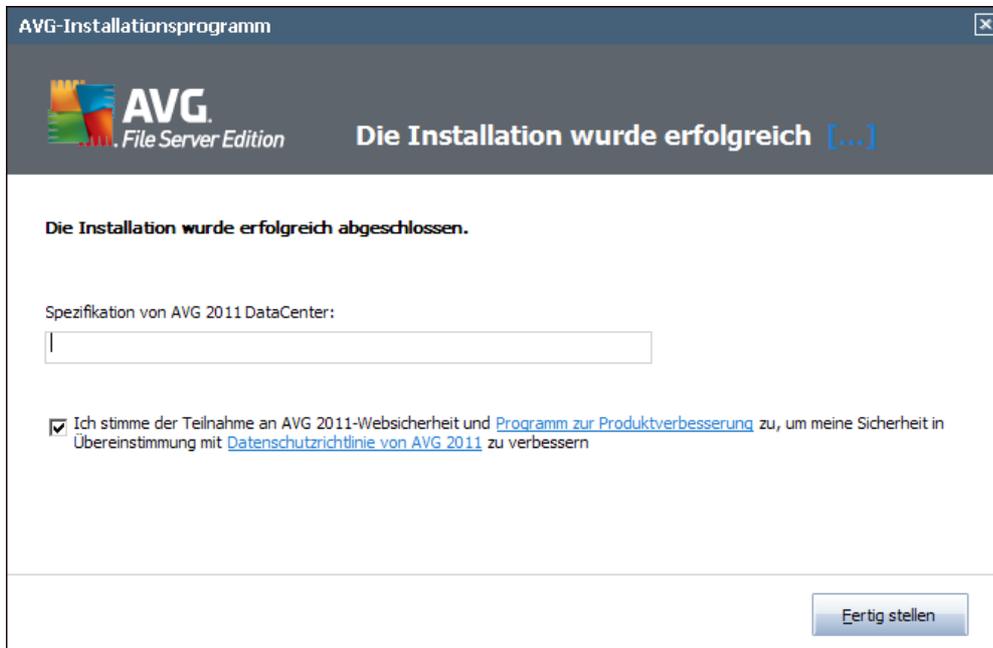
Im Dialog **Installationsfortschritt** wird der Fortschritt des Installationsvorgangs angezeigt. Hier ist keine Aktion erforderlich.

Nach Abschluss des Installationsvorgangs werden das Programm und die Virendatenbank automatisch aktualisiert. Anschließend werden Sie zum nächsten Dialog weitergeleitet.

4.6. Die Installation wurde erfolgreich abgeschlossen

Der Dialog **Die Installation wurde erfolgreich abgeschlossen** bestätigt, dass **AVG File Server 2011** vollständig installiert und konfiguriert wurde.

Wenn Sie zuvor den AVG Remote Admin Client für die Installation ausgewählt haben (siehe [Benutzerdefinierte Optionen](#)), wird der Dialog mit der folgenden Oberfläche 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. Genauer 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.

Ich stimme der Teilnahme an AVG 2011-Websicherheit und am Programm zur Produktverbesserung zu – Aktivieren Sie dieses Kontrollkästchen, wenn 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.



5. Nach der Installation

5.1. Produktregistrierung

Nach Abschluss der Installation von **AVG File Server 2011** registrieren Sie bitte Ihr Produkt, indem Sie auf der Website von AVG (<http://www.avg.com/de>) die Seite **Registrierung** aufrufen (*folgen Sie den Anweisungen auf dieser Seite*). Nach der Registrierung erhalten Sie vollen Zugriff auf Ihr AVG-Benutzerkonto, den AVG Update-Newsletter und andere exklusive Dienste für registrierte Benutzer.

5.2. Zugriff auf die Benutzeroberfläche

Die **Benutzeroberfläche 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
- über das Menü **Start/Alle Programme/AVG 2011/Benutzeroberfläche von AVG**

5.3. Gesamten Computer scannen

Es besteht das potentielle Risiko, dass vor der Installation von **AVG File Server 2011** 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**.

5.4. Standardkonfiguration von AVG

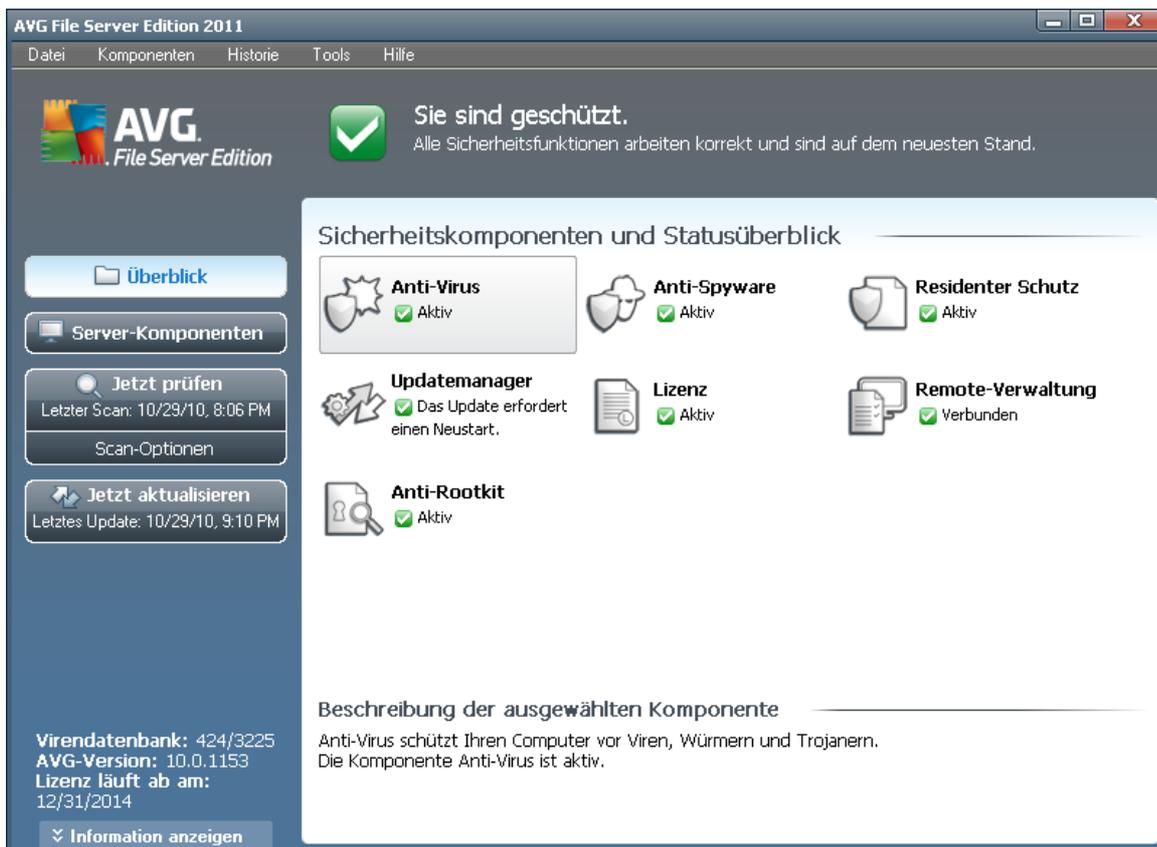
Die Standardkonfiguration (*Konfiguration der Anwendung unmittelbar nach der Installation*) von **AVG File Server 2011** ist vom Händler so eingestellt, dass alle Komponenten und Funktionen eine optimale Leistung erzielen.

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.

6. Benutzeroberfläche von AVG

AVG File Server 2011 öffnet das Hauptfenster:



Das Hauptfenster ist in mehrere Bereiche gegliedert:

- **Systemmenü** (Leiste an der Oberseite des Fensters) dient zur Standardnavigation für den Zugriff auf alle Komponenten, Dienste und Funktionen von AVG - [Details >>](#)
- **Informationen zum Sicherheitsstatus** (oberer Bereich des Fensters) enthält Informationen zum aktuellen Status Ihres AVG-Programms - [Details >>](#)
- **Quick Links** (linker Bereich des Fensters) ermöglichen das schnelle Aufrufen der wichtigsten und am häufigsten verwendeten AVG-Aufgaben - [Details >>](#)
- **Komponentenübersicht** (zentraler Bereich des Fensters) zeigt eine Übersicht über alle installierten Komponenten von AVG - [Details >>](#)
- **Statistik** (linker unterer Bereich des Fensters) enthält alle statistischen Daten zur Programmnutzung - [Details >>](#)
- **Infobereich-Symbol** (untere rechte Ecke des Bildschirms, im Infobereich) zeigt den aktuellen Status von AVG - [Details >>](#)



6.1. 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 File Server 2011**. Mit Hilfe des Systemmenüs können Sie auf bestimmte Komponenten, Funktionen und Dienste von AVG zugreifen.

Das Systemmenü ist in fünf Hauptbereiche eingeteilt:

6.1.1. Datei

- **Beenden** – Schließt die Benutzeroberfläche von **AVG File Server 2011**. Die AVG-Anwendung wird jedoch weiterhin im Hintergrund ausgeführt, damit Ihr Computer geschützt ist!

6.1.2. 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](#)
- **Server-Komponenten** – Zeigt die verfügbaren Sicherheitskomponenten und deren Status in einer Übersicht an – [Details >>](#)
- **Anti-Virus** stellt sicher, dass Ihr Computer vor Viren geschützt wird – [Details >>](#)
- **Anti-Spyware** gewährleistet, dass Ihr Computer vor Spyware und Adware geschützt ist – [Details >>](#)
- **Residenter Schutz** wird im Hintergrund ausgeführt und scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden – [Details >>](#)
- **Updatemanager** kontrolliert alle Aktualisierungen von AVG – [Details >>](#)
- **Lizenz** zeigt die Lizenznummer, den Lizenztyp und das Ablaufdatum an – [Details >>](#)
- **Remote-Verwaltung** wird nur angezeigt, wenn Sie während des [***](#) Installationsvorgangs angegeben haben, dass diese Komponente installiert werden soll.
- **Anti-Rootkit** erkennt Programme und Technologien, die darauf abzielen, Malware zu verbergen – [Details >>](#)



6.1.3. Historie

- **[Scan-Ergebnisse](#)** - Wechsel zur Testoberfläche von AVG, und zwar zum Dialog **[Übersicht über Scan-Ergebnisse](#)**
- **[Residenter Schutz](#)** - Anzeigen einen Dialogs mit einer Übersicht über Bedrohungen, erkannt durch den **[Residenten Schutz](#)**
- **[Virenquarantäne](#)** - Anzeige der Oberfläche der Virenquarantäne (**[Virenquarantäne](#)**), in die AVG alle erkannten Infektionen verschiebt, die nicht automatisch geheilt werden können. Innerhalb dieser Quarantäne werden die infizierten Dateien isoliert, so das die Sicherheit Ihres Computers gewährleistet ist. Gleichzeitig werden die infizierten Dateien für eine mögliche Reparatur gespeichert.
- **[Ereignisprotokoll](#)** - Anzeige der Ereignisprotokoll Oberfläche mit einer Übersicht über alle protokollierten Aktionen **AVG File Server 2011** .

6.1.4. 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 File Server 2011**
- **[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 File Server 2011** bearbeiten können. Im Allgemeinen empfehlen wir Ihnen, die Standardeinstellungen der Software beizubehalten, die vom Software-Hersteller festgelegt wurden.

6.1.5. 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
- **AVG Rescue CD herunterladen** – Öffnet im Webbrowser die Seite zum Herunterladen der AVG Rescue CD.
- **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 kostenlosen technischen Support.

Hinweis: Wenn Sie die Testversion von **AVG File Server 2011** verwenden, werden die letzten zwei Einträge als **Jetzt kaufen** und **Aktivieren** angezeigt und ermöglichen es Ihnen, die Vollversion des Programms zu erwerben. Wenn **AVG File Server 2011** mit einer Vertriebsnummer installiert ist, werden die Einträge als **Registrieren** und **Aktivieren** angezeigt. Weitere Informationen finden Sie im Abschnitt [Lizenz](#) dieser Dokumentation.

- **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.

6.2. Informationen zum Sicherheitsstatus

Der Bereich **Informationen zum Sicherheitsstatus** befindet sich im oberen Teil des Hauptfensters von AVG. In diesem Bereich finden Sie stets Informationen zum aktuellen Sicherheitsstatus von **AVG File Server 2011**. Bitte verschaffen Sie sich eine Übersicht über Symbole, die in diesem Bereich möglicherweise angezeigt werden und über ihre Bedeutung:



- Das grüne Symbol zeigt an, dass Ihr AVG vollständig funktioniert. 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 grundlegendes Problem in AVG, und Sie haben sich wahrscheinlich entschieden, einige Komponenten aus bestimmten Gründen zu deaktivieren. Sie sind immer noch durch AVG geschützt. Sie sollten jedoch die Einstellungen der problematischen Komponente überprüfen! Den Namen der Komponente finden Sie im Bereich **Informationen zum Sicherheitsstatus**.

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



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

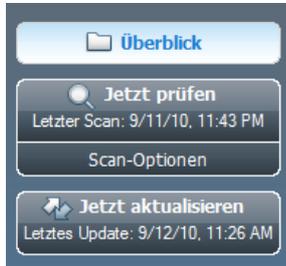
Wenn AVG nicht für eine optimale Leistung konfiguriert ist, wird neben den Sicherheitsstatusinformationen eine neue Schaltfläche „Reparieren“ angezeigt (alternativ auch „Alles reparieren“, wenn das Problem mehrere Komponenten betrifft). Klicken Sie auf diese Schaltfläche, um einen automatischen Vorgang zur Programmüberprüfung und -konfiguration zu starten. Anhand dieser einfachen Methode können Sie AVG für eine optimale Leistung optimieren 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 von AVG erhalten Sie auch jederzeit über das [Symbol im Infobereich](#).

6.3. Quick Links

Mithilfe der Quick Links (im linken Bereich der [Benutzeroberfläche von AVG](#)) können Sie sofort auf die wichtigsten und am häufigsten verwendeten Features von AVG zugreifen:



- **Überblick** – Mit diesem Link können Sie von jeder aktuell geöffneten Oberfläche von AVG zur Standardoberfläche wechseln, auf der Sie eine Übersicht über alle installierten Komponenten erhalten. Siehe Kapitel [Komponentenübersicht >>](#)
- **Jetzt scannen** – Über diese Schaltfläche erhalten Sie standardmäßig Informationen (*Scan-Typ, Datum des letzten Scans*) zum letzten, durchgeführten Scan. Verwenden Sie den Befehl **Jetzt scannen**, um denselben Scan erneut auszuführen, oder klicken Sie auf den Link **Computer-Scanner**, um die Scanoberfläche von AVG zu öffnen, von der Sie Scans ausführen, planen oder Scan-Parameter bearbeiten können – siehe Kapitel [AVG-Scans >>](#)
- **Jetzt aktualisieren** – über diesen Link erhalten Sie das Datum des letzten, durchgeführten Updatevorgangs. Klicken Sie auf diese Schaltfläche, um die Updateoberfläche zu öffnen und den Updatevorgang sofort zu starten – siehe Kapitel [AVG Updates >>](#)
- **Server-Komponenten** – Dieser Link öffnet die [Übersicht über Server-Komponenten](#).

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

6.4. Komponentenübersicht

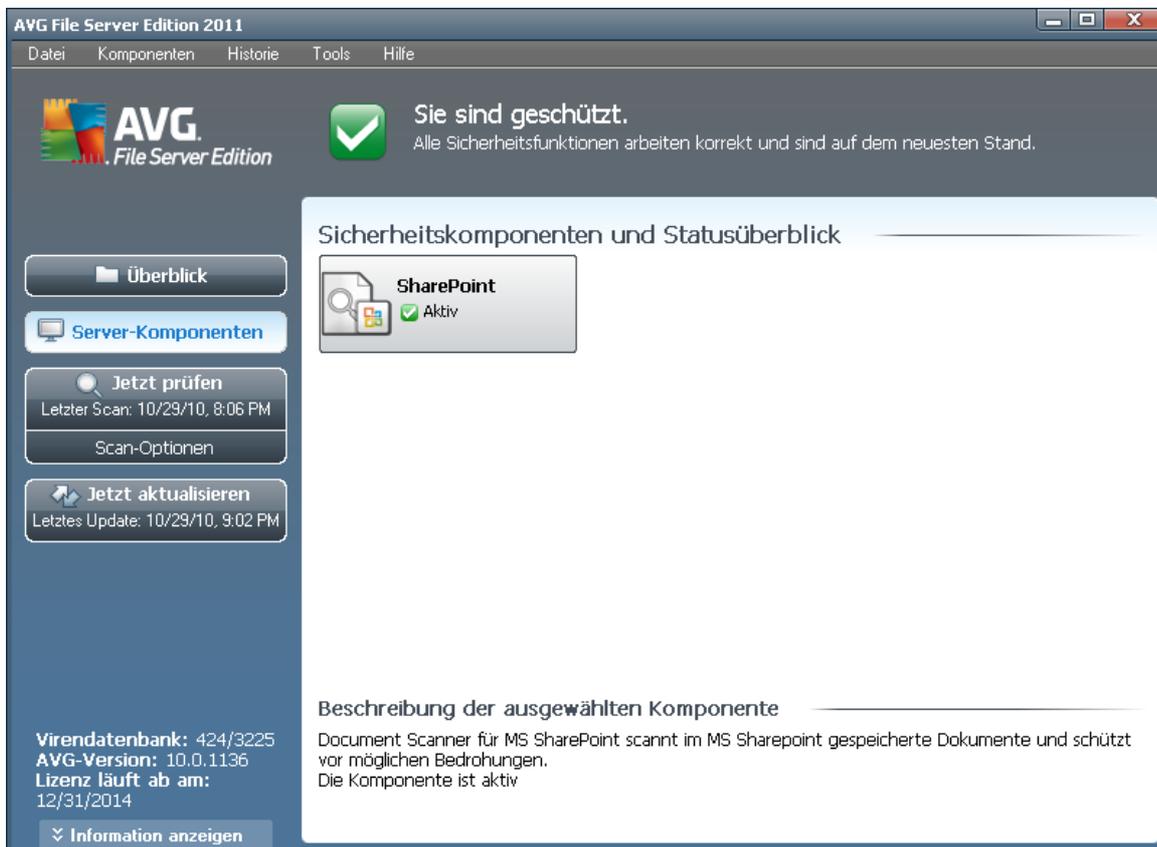
Der Bereich **Sicherheitskomponenten und Statusüberblick** befindet sich in der Mitte der [Benutzeroberfläche von AVG](#). Er ist in zwei Teile gegliedert:

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

In **AVG File Server 2011** enthält der Bereich **Komponentenübersicht** Informationen zu folgenden Komponenten:

- **Anti-Virus** stellt sicher, dass Ihr Computer vor Viren geschützt wird – [Details >>](#)
- **Anti-Spyware** gewährleistet, dass Ihr Computer vor Spyware und Adware geschützt ist – [Details >>](#)

6.5. Server-Komponenten



Der Bereich **Server-Komponenten** befindet sich in der Mitte der [Benutzeroberfläche von AVG](#). Er ist in zwei Teile gegliedert:

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

In **AVG File Server 2011** enthält der Bereich **Server-Komponenten** Informationen zu folgenden Komponenten:

- **SharePoint** scannt in MS SharePoint gespeicherte Dokumente und schützt vor möglichen Bedrohungen.- [Details >>](#)

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

Klicken Sie mit der rechten Maustaste auf das Komponentensymbol, um das



Kontextmenü einzublenden: Darüber können Sie nicht nur die grafische Benutzeroberfläche der Komponente öffnen, sondern auch die Option **Komponentenstatus ignorieren** auswählen. Wählen Sie diese Option aus, wenn Ihnen bekannt ist, dass die [Komponente einen Fehlerstatus aufweist](#), AVG aber aus einem bestimmten Grund aktiviert bleiben soll und Sie nicht anhand der Farbänderung des [Symbols im Infobereich](#) gewarnt werden möchten.

6.6. Statistik

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

- **Virendatenbank** – Hier wird die aktuell installierte Version der Virendatenbank angegeben
- **AVG-Version** – Hier erhalten Sie Informationen zur installierten AVG-Version (*die Versionsnummer wird im Format 10.0.xxxx angegeben, wobei 10.0 die Version der Produktlinie ist, und xxxx für die Build-Nummer steht*)
- **Lizenz läuft ab am:** – Hier wird das Ablaufdatum Ihrer Lizenz von AVG angegeben

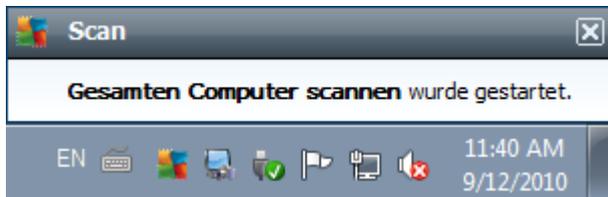
6.7. Infobereich-Symbol

Infobereichsymbol (auf Ihrer Taskleiste von Windows) zeigt den aktuellen Status von **AVG File Server 2011** an. Es wird immer in Ihrem Infobereich angezeigt, unabhängig davon, ob Ihr Hauptfenster von AVG geöffnet oder geschlossen ist:



Durch die Vollfarbe  des **Infobereichsymbols** wird angezeigt, dass alle Komponenten von AVG aktiv und voll funktionsfähig sind. Das AVG-Symbol im Infobereich wird auch dann in Vollfarbe angezeigt, wenn AVG einen Fehlerstatus aufweist und Sie sich absichtlich dafür entschieden haben, den [Komponentenstatus zu ignorieren](#). Ein Symbol mit einem Ausrufezeichen  zeigt an, dass ein Problem vorliegt (*inaktive Komponente, Fehlerstatus etc.*). Doppelklicken Sie auf das **Infobereich-Symbol**, um das Hauptfenster zu öffnen und eine Komponente zu bearbeiten.

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



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

- **Benutzeroberfläche von AVG öffnen** – Klicken Sie hierauf, um die [Benutzeroberfläche von AVG zu öffnen](#)
- **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
- **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



7. Komponenten von AVG

7.1. Anti-Virus

7.1.1. Grundlagen zu Anti-Virus

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

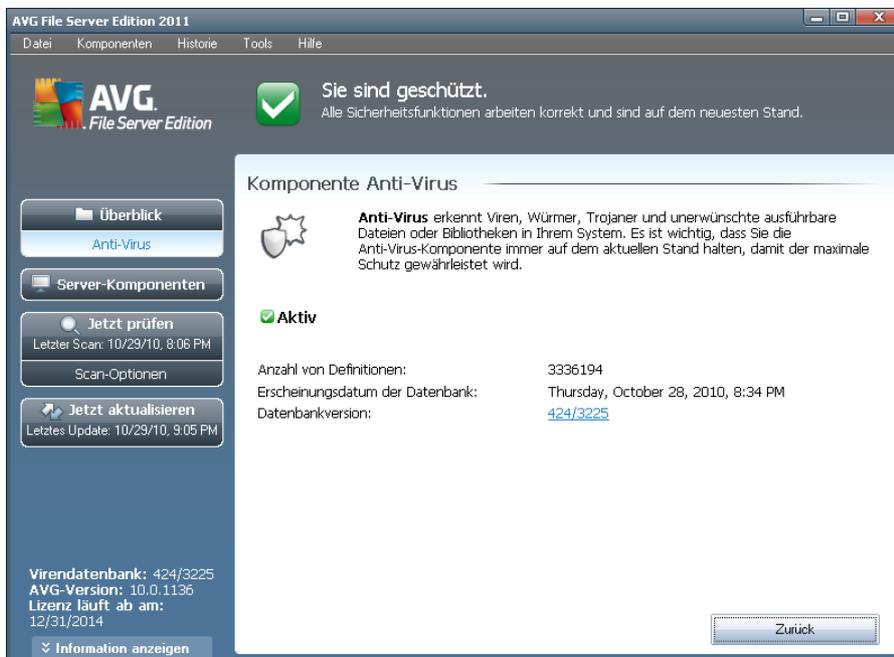
Die wichtigste Funktion des Virenschutzes ist, sicherzustellen, dass keine bekannten Viren auf dem Computer ausgeführt werden können!

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

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

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

7.1.2. Benutzeroberfläche des Anti-Virus



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

- **Anzahl von Definitionen** – Anzahl der in der aktuellen Version der Virendatenbank definierten Viren
- **Erscheinungsdatum der Datenbank** – Datum und Uhrzeit des letzten Updates der Viren-Datenbank
- **Datenbankversion** – Versionsnummer der aktuell installierten Virendatenbank; wird bei jedem Update der Virendatenbank erhöht

Die Benutzeroberfläche der Komponente enthält nur eine Schaltfläche (**Zurück**), mit der Sie zum Hauptfenster der [Benutzeroberfläche von AVG](#) (*Komponentenübersicht*) zurückkehren können.

7.2. Anti-Spyware

7.2.1. Grundlagen zu Anti-Spyware

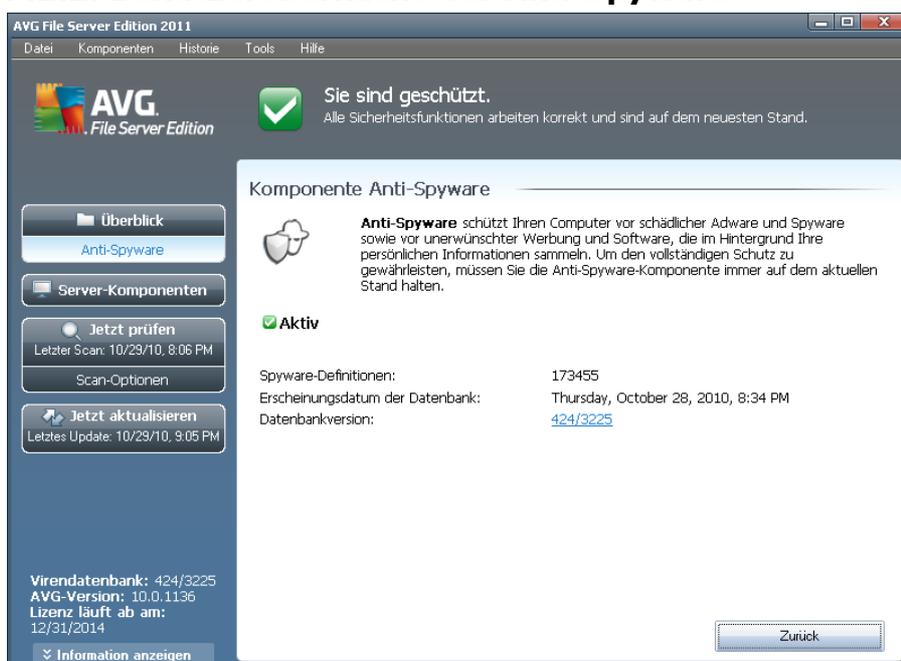
Spyware wird normalerweise als eine Art Malware definiert, d. h. Software, die ohne Wissen und Zustimmung des Benutzers Informationen auf dem Computer sammelt. Einige Spyware-Programme können bewusst installiert werden und enthalten häufig Werbung, Pop-up-Fenster oder ähnlich unerfreuliche Software.



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 residerter Schutz funktioniert und Ihre Anwendungen während der Arbeit im Hintergrund überprüft.

Es ist allerdings möglich, dass Malware bereits vor der Installation von AVG auf den Computer übertragen wurde oder dass Sie **AVG File Server 2011** nicht mit den neuesten [Datenbank- und Programmaktualisierungen](#) ausgestattet haben. Daher können Sie mit AVG Ihren Computer mithilfe der Scan-Funktion vollständig auf Malware bzw. Spyware überprüfen. Außerdem erkennt die Komponente ruhende und nicht aktive Malware, d. h. Malware, die heruntergeladen, aber noch nicht aktiviert wurde.

7.2.2. Benutzeroberfläche der Anti-Spyware



Die Benutzeroberfläche von **Anti-Spyware** enthält eine Übersicht über die Funktionsweise der Komponente, Informationen zum aktuellen Status sowie einige Statistiken zu **Anti-Spyware**:

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

Die Benutzeroberfläche der Komponente enthält nur eine Schaltfläche (**Zurück**), mit



der Sie zum Hauptfenster der [Benutzeroberfläche von AVG](#) (*Komponentenübersicht*) zurückkehren können.

7.3. Residenter Schutz

7.3.1. Grundlagen zu Residenter Schutz

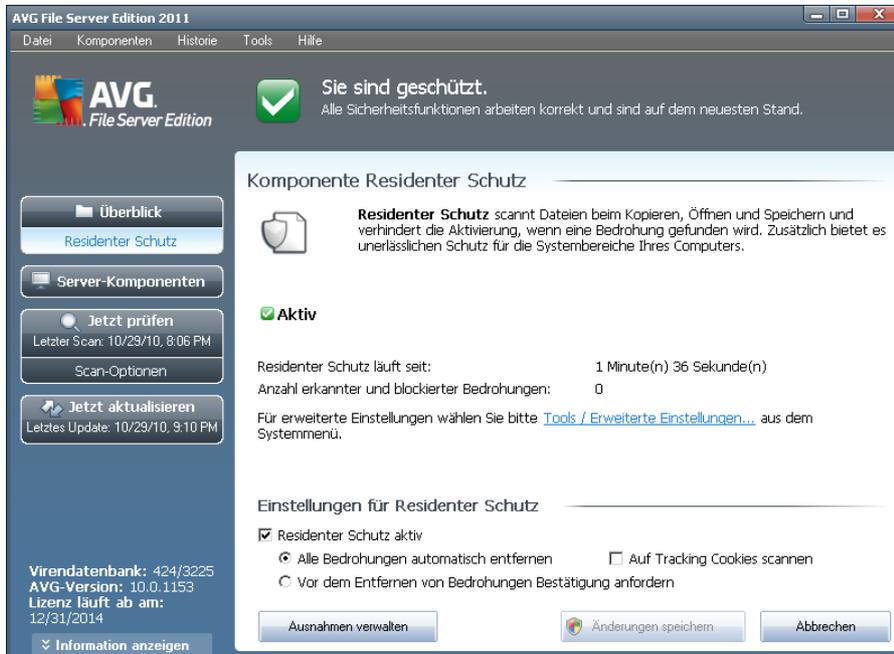
Die Komponente **Residenter Schutz** gewährt Ihrem Computer dauerhaften Schutz. Sie scannt jede einzelne Datei, die geöffnet, gespeichert oder kopiert wird und überwacht die Systembereiche Ihres Computers. Wenn der **Residente Schutz** in einer Datei, auf die zugegriffen wird, ein Virus entdeckt, stoppt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

Aufgaben des Residenten Schutzes

- Scannen auf bestimmte mögliche Bedrohungen
- Scannen von Wechseldatenträgern (*Flash-Disks usw.*)
- Scannen von Dateien mit bestimmten Erweiterungen oder Dateien ohne Erweiterungen
- Festlegen von Ausnahmen für Scans (bestimmte Dateien oder Ordner, die nie gescannt werden sollen)

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

7.3.2. Benutzeroberfläche des Residenten Schutzes



Neben einer Übersicht über die Funktionen des **Residenten Schutzes** und Informationen zum Status der Komponente enthält die Benutzeroberfläche des **Residenten Schutzes** auch einige statistische Daten:

- **Residenter Schutz läuft seit** – Abgelaufene Zeit seit dem letzten Start der Komponenten
- **Anzahl erkannter und blockierter Bedrohungen** – Anzahl der erkannten Infektionen, deren Ausführung/Öffnen verhindert wurde (*wenn nötig kann dieser Wert zurückgesetzt werden, z. B. für statistische Zwecke – Wert zurücksetzen*)

Einstellungen für Residenter Schutz

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

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

- entweder automatisch (**Alle Bedrohungen automatisch entfernen**)



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

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

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

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

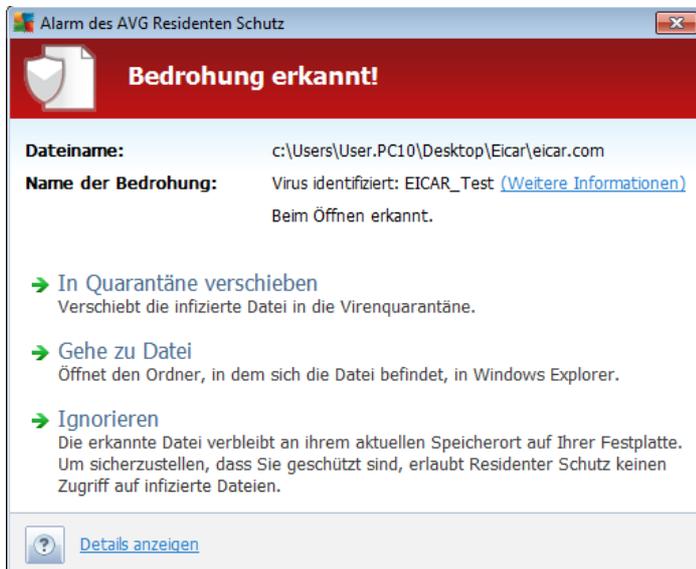
Schaltflächen

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

- **Ausnahmen verwalten** – Öffnet den Dialog [Residenter Schutz – Ausgeschlossene Einträge](#), in dem Sie Ordner und Dateien festlegen können, die vom [Residenten Schutz](#) nicht durchsucht werden sollen
- **Änderungen speichern** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen
- **Abbrechen** – Mit dieser Schaltfläche können Sie zur [Benutzeroberfläche von AVG](#) (Komponentenübersicht) zurückkehren

7.3.3. Erkennungen durch den Residenten Schutz

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



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 [Virenzyklopädie](#), wo Sie weitere Informationen zur erkannten Infektion finden, falls bekannt ([Weitere Informationen](#)).

Zudem müssen Sie die erforderliche Aktion auswählen – die folgenden 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 AVG-[Virenquarantäne verschoben](#)
- **Gehe zu Datei** – Mit dieser Option werden Sie zum genauen Speicherort des verdächtigen Objekts weitergeleitet (*öffnet ein neues Fenster von Windows Explorer*)
- **Ignorieren** – Es wird dringend empfohlen, diese Option NICHT zu verwenden,



wenn Sie keinen wirklich guten Grund dazu haben!

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.

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**:

The screenshot shows the AVG File Server Edition 2011 interface. At the top, it says "Sie sind geschützt." (You are protected). Below this, the "Residenten Schutz" (Resident Protection) section is active, displaying a table of detected threats. The table has four columns: Infektion (Infection), Objekt (Object), Ergebnis (Result), and Erkennungszeit (Detection time). The table contains six entries, with the first three being Trojaners and the last two being viruses. The interface also includes buttons for "Liste aktualisieren", "Auswahl entfernen", "Alle Bedrohungen entfernen", and "Zurück".

Infektion	Objekt	Ergebnis	Erkennungszeit
Trojaner: BackDoor...	c:\Documents and Set...	In Virenquarantäne ver...	10/19/2010, 10:39:
Trojaner: BackDoor...	c:\Documents and Set...	In Virenquarantäne ver...	10/19/2010, 10:39:
Virus identifiziert: EI...	c:\Documents and Set...	In Virenquarantäne ver...	10/19/2010, 10:39:
Trojaner: BackDoor...	c:\Documents and Set...	In Virenquarantäne ver...	10/19/2010, 10:38:
Virus identifiziert: EI...	c:\Documents and Set...	Infiziert	10/19/2010, 10:38:
Virus identifiziert: EI...	c:\Documents and Set...	Infiziert	10/19/2010, 10:37:

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** können Sie zur Hauptseite der [Benutzeroberfläche von AVG](#) (*Komponentenübersicht*) zurückkehren.

7.4. Updatemanager

7.4.1. Grundlagen zum Updatemanager

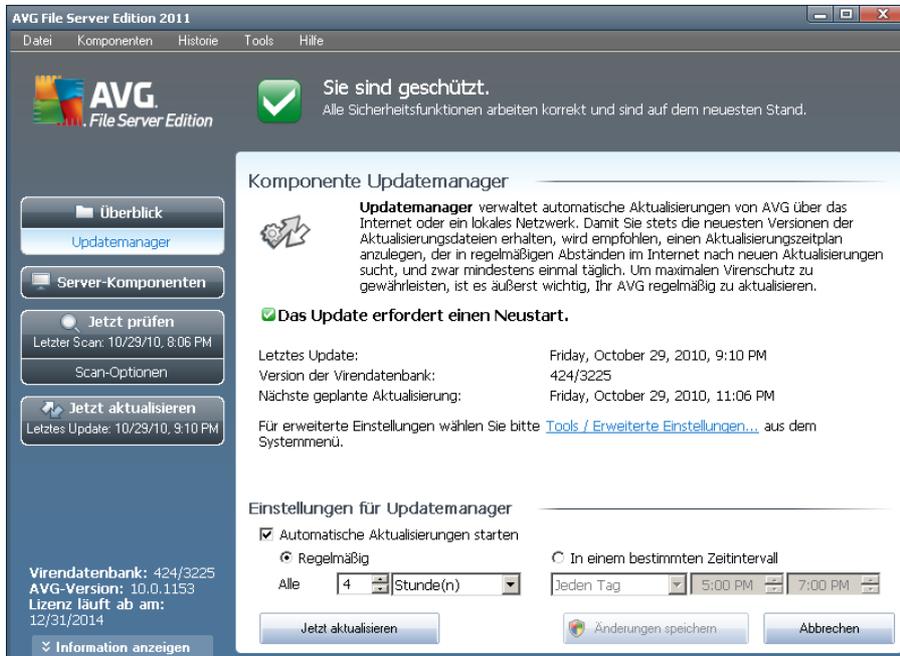
Keine Sicherheits-Software kann einen wirksamen Schutz gegen verschiedene Bedrohungen bieten, wenn sie nicht regelmäßig aktualisiert wird! Verfasser von Viren suchen stets nach neuen Lücken in Software und Betriebssystemen, die sie ausnutzen können. Jeden Tage gibt es neue Viren, neue Malware und neue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

Es ist entscheidend, dass Sie AVG regelmäßig aktualisieren!

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

Hinweis: Im Kapitel [AVG Updates](#) finden Sie weitere Informationen zu Aktualisierungsstufen und -arten!

7.4.2. Benutzeroberfläche des Updatemanagers



Die Oberfläche des **Updatemanagers** enthält Informationen zu den Funktionen der Komponente, ihren aktuellen Status und bietet wichtige statistische Daten:

- **Letztes Update** – Hier werden Datum und Uhrzeit der Datenbankaktualisierung angegeben
- **Version der Virendatenbank** – gibt die Versionsnummer der aktuell installierten Virendatenbank an; wird bei jedem Update der Virendatenbank erhöht
- **Nächstes geplantes Update** – Gibt an, wann die Datenbank laut Zeitplan erneut aktualisiert werden soll

Einstellungen für Update Manager

Im unteren Teil des Dialogs finden Sie den Bereich **Einstellungen für Updatemanager**, in dem Sie einige Regeln des Aktualisierungsstarts ändern können. Sie können festlegen, ob die Aktualisierungsdateien automatisch (**Automatische Aktualisierungen starten**) oder On-Demand heruntergeladen werden sollen. Standardmäßig ist die Option **Automatische Aktualisierungen starten** aktiviert, und wir empfehlen, dies auch so zu belassen! Das regelmäßige Herunterladen der aktuellsten Updatedateien ist entscheidend für das Funktionieren jeder Sicherheits-Software!

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

- **Regelmäßig** – Hier können Sie das Zeitintervall festlegen



- **In einem bestimmten Zeitintervall** – geben Sie die Startzeit für die Durchführung des Updates an

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

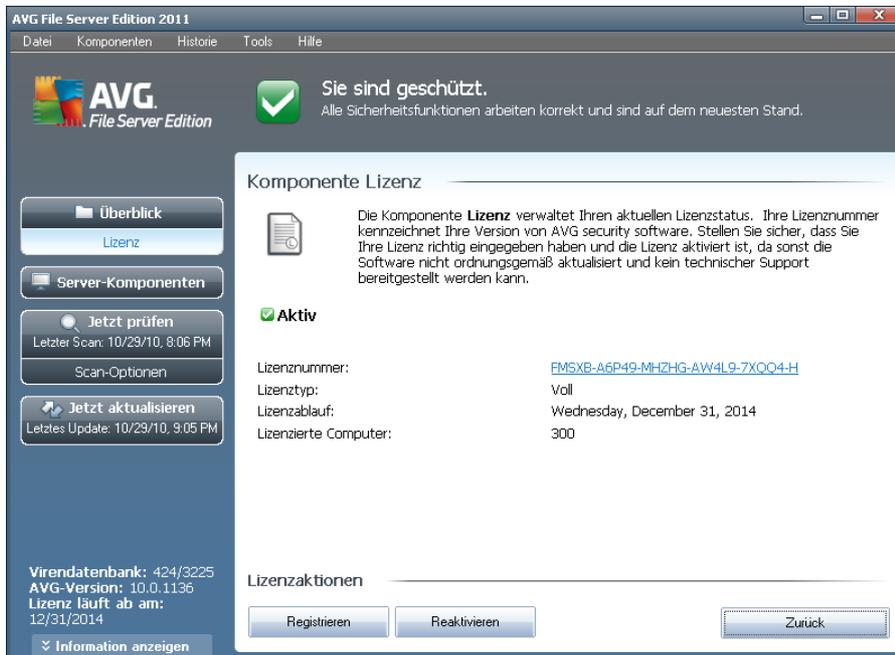
Hinweis: Alle Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.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

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

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

7.5. Lizenz



Auf der Benutzeroberfläche der Komponente **Lizenz** finden Sie eine kurze Beschreibung der Funktionsweise der Komponente, Informationen zum aktuellen Status sowie die folgenden Informationen:

- **Lizenznummer** – bietet die verkürzte Form Ihrer Lizenznummer (*aus Sicherheitsgründen wurden die letzten vier Ziffern weggelassen*). Wenn Sie die Lizenznummer eingeben, müssen Sie diese absolut präzise und exakt wie angezeigt eingeben. Aus diesem Grund empfehlen wir ausdrücklich, zur Verwendung der Lizenznummer die Methode „Kopieren und Einfügen“ zu nutzen.
- **Lizenztyp** – Gibt den installierten Produkttyp an.
- **Lizenzablauf** – Dieses Datum zeigt, wie lange Ihre Lizenz gültig ist. Wenn Sie **AVG File Server 2011** über dieses Datum hinaus weiter verwenden möchten, müssen Sie Ihre Lizenz verlängern. Die Verlängerung der Lizenz kann online auf der [Website von AVG](http://www.avg.com/de) durchgeführt werden.
- **Lizenzierte Computer** – Gibt an, auf wie vielen Workstations **AVG File Server 2011** installiert werden darf.

Schaltflächen

- **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 kostenlosen technischen Support.

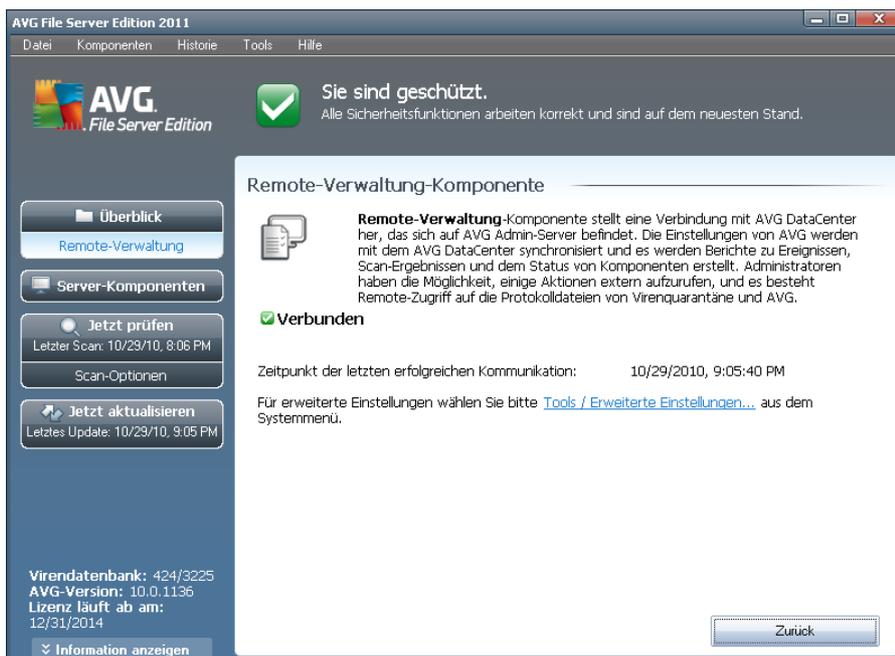


- **Reaktivieren** – Öffnet den Dialog **AVG aktivieren** mit den Daten, die Sie im Dialog **AVG personalisieren** des **Installationsvorgangs** eingegeben haben. In diesem Dialog können Sie Ihre Lizenznummer eingeben, um entweder die Vertriebsnummer (*die Nummer, mit der Sie AVG installiert haben*)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

Hinweis: Wenn Sie die Testversion von **AVG File Server 2011** verwenden, werden die Schaltflächen als **Jetzt kaufen** und **Aktivieren** angezeigt und ermöglichen es Ihnen, die Vollversion des Programms zu erwerben. Wenn **AVG File Server 2011** mit einer Vertriebsnummer installiert ist, werden die Schaltflächen als **Registrieren** und **Aktivieren** angezeigt.

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

7.6. Remote-Verwaltung



Die Komponente **Remote-Verwaltung** wird nur in der Benutzeroberfläche von **AVG File Server 2011** angezeigt, wenn Sie die Netzwerk-Edition Ihres Produkts installiert haben (*siehe Komponente [Lizenz](#)*). Im Dialog **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.de) (www.avg.de) unter **Support Center > Download > Dokumentation** heruntergeladen



werden.

Schaltflächen

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

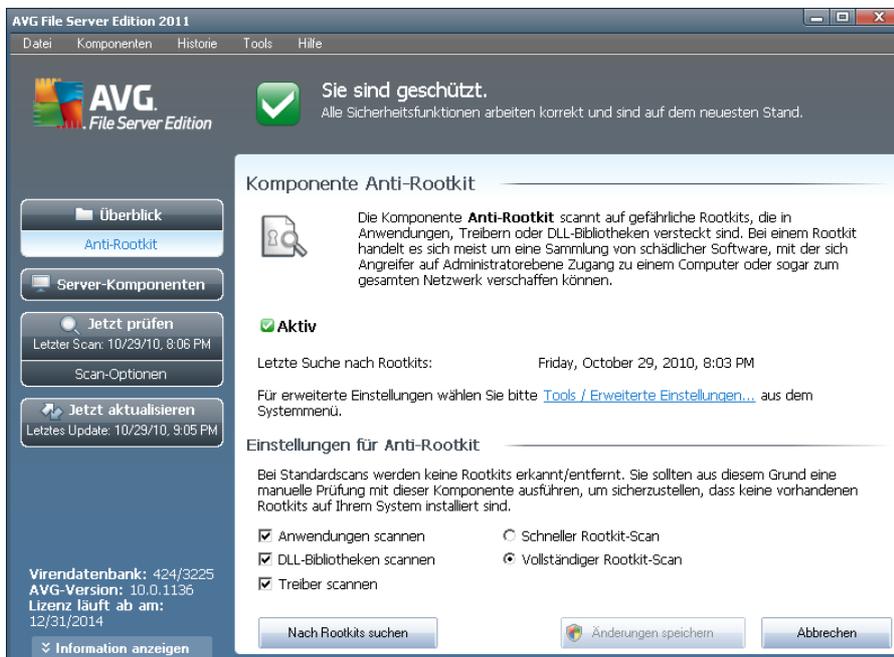
7.7. Anti-Rootkit

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.

7.7.1. Grundlagen zu Anti-Rootkit

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

7.7.2. Benutzeroberfläche von Anti-Rootkit



Die Benutzeroberfläche von **Anti-Rootkit** enthält eine kurze Beschreibung der Funktionen der Komponente, gibt Auskunft über den Status der Komponente und enthält Informationen über den Zeitpunkt des letzten mit **Anti-Rootkit (Letzte Suche nach Rootkits)** durchgeführten Tests. 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.

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

Einstellungen für Anti-Rootkit

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

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

Wählen Sie anschließend den Rootkit-Scanmodus aus:



- **Schneller Rootkit-Scan** – 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*)

Schaltflächen

- **Nach Rootkits suchen** – Da der Rootkit-Scan kein integrierter Bestandteil des [Scans für den gesamten Computer](#) ist, können Sie den Rootkit-Scan mit dieser Schaltfläche direkt über die Benutzeroberfläche von **Anti-Rootkit** ausführen
- **Änderungen speichern** – Mit dieser Schaltfläche können Sie alle auf dieser Benutzeroberfläche vorgenommenen Änderungen speichern und zur [Benutzeroberfläche von AVG](#) (*Komponentenübersicht*) zurückkehren
- **Abbrechen** – Mit dieser Schaltfläche können Sie zur [Benutzeroberfläche von AVG](#) (*Komponentenübersicht*) zurückkehren, ohne Ihre Änderungen zu speichern

8. AVG Einstellungsmanager

AVG Einstellungsmanager ist besonders für kleinere Netzwerke geeignet. Mit dieser Komponente können Sie die Konfiguration von AVG kopieren, bearbeiten und bereitstellen. Die Konfiguration kann auf einem Wechseldatenträger (USB-Flash-Laufwerk usw.) gespeichert und anschließend für die ausgewählte Station manuell übernommen werden.

Das Tool ist standardmäßig in der Installation von AVG enthalten und kann über das Startmenü von Windows aufgerufen werden:

Alle Programme/AVG 2011/AVG Einstellungsmanager



- **Konfiguration von AVG für diesen Computer bearbeiten**

Mit dieser Schaltfläche öffnen Sie einen Dialog mit erweiterten Einstellungen für Ihre lokale Installation von AVG. Alle hier vorgenommenen Änderungen zeigen sich auch in der lokalen Installation von AVG.

- **AVG Konfigurationsdatei laden und bearbeiten**

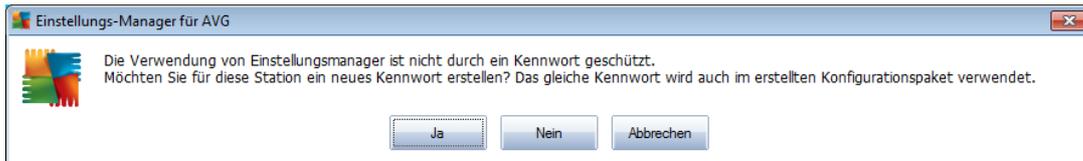
Wenn Sie bereits eine AVG Konfigurationsdatei (.pck) besitzen, können Sie sie durch Klicken auf diese Schaltfläche öffnen und bearbeiten. Wenn Sie Ihre Änderungen durch Klicken auf **OK** oder **Übernehmen** bestätigen, wird die Datei durch die neuen Einstellungen ersetzt!

- **Konfiguration für AVG aus Datei übernehmen**

Über diese Schaltfläche können Sie eine AVG Konfigurationsdatei (.pck) öffnen und für die lokale Installation von AVG übernehmen.

- **Lokale Konfiguration von AVG in einer Datei speichern**

Über diese Schaltfläche können Sie eine AVG Konfigurationsdatei (.pck) der lokalen Installation von AVG speichern. Wenn Sie kein Kennwort für die Zugelassenen Aktionen angeben, wird möglicherweise folgender Dialog angezeigt:



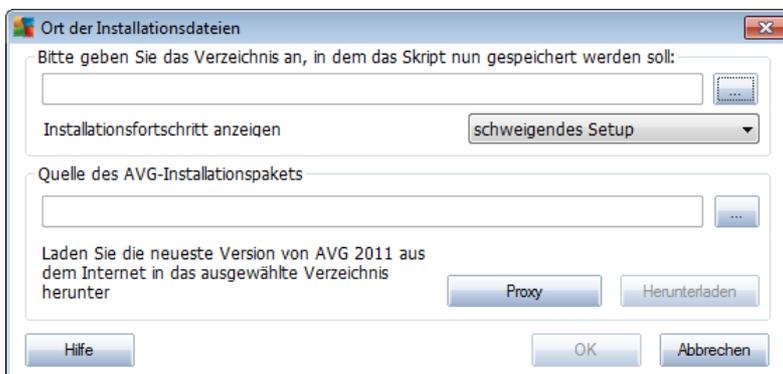
Antworten Sie mit **Ja**, wenn Sie das Kennwort für den Zugriff auf die zugelassenen Elemente jetzt festlegen möchten, geben Sie anschließend die notwendigen Informationen ein und bestätigen diese. Antworten Sie mit **Nein**, um die Kennworterstellung zu überspringen und die lokale Konfiguration von AVG in einer Datei zu speichern.

- **Installation von AVG klonen**

Mit dieser Option können Sie eine Kopie der lokalen Installation von AVG erstellen, indem Sie ein Installationspaket mit individuellen Optionen erzeugen. Die Kopie umfasst den Großteil der AVG-Einstellungen mit folgenden Ausnahmen:

- Spracheinstellungen
- Soundeinstellungen
- Firewall-Konfiguration
- Liste „Zugelassen“ und Ausnahmen der potentiell unerwünschten Programme der Komponente „Identitätsschutz“.

Wählen Sie dazu zuerst den Ordner aus, in dem das Installationskript gespeichert werden soll.



Wählen Sie anschließend aus dem Dropdownmenü eine der folgenden Optionen:



- **Versteckte Installation** – während der Installation werden keine Informationen angezeigt.
- **Nur Installationsfortschritt anzeigen** – während der Installation sind keine Benutzereingaben erforderlich, es wird jedoch der Installationsfortschritt angezeigt.
- **Installationsassistent anzeigen** – der Installationsfortschritt wird angezeigt, und der Benutzer muss alle Schritte bestätigen.

Verwenden Sie entweder die Schaltfläche **Herunterladen**, um das neueste verfügbare Installationspaket von AVG direkt von der Website in den gewählten Ordner herunterzuladen, oder verschieben Sie das Installationspaket manuell in diesen Ordner.

Sie können über die Schaltfläche **Proxy** Einstellungen für einen Proxy-Server angeben, falls dies in Ihrem Netzwerk notwendig ist.

Klicken Sie auf **OK**, um den Klonvorgang zu starten. Möglicherweise wird ein Dialog angezeigt, in dem Sie dazu aufgefordert werden, ein Kennwort für die zugelassenen Elemente festzulegen (siehe oben). Sobald der Vorgang abgeschlossen ist, sollte sich im gewählten Ordner die Datei **AvgSetup.bat** befinden. Wenn Sie die Datei **AvgSetup.bat** ausführen, wird AVG entsprechend den oben gewählten Parametern installiert.



9. AVG Server-Komponenten

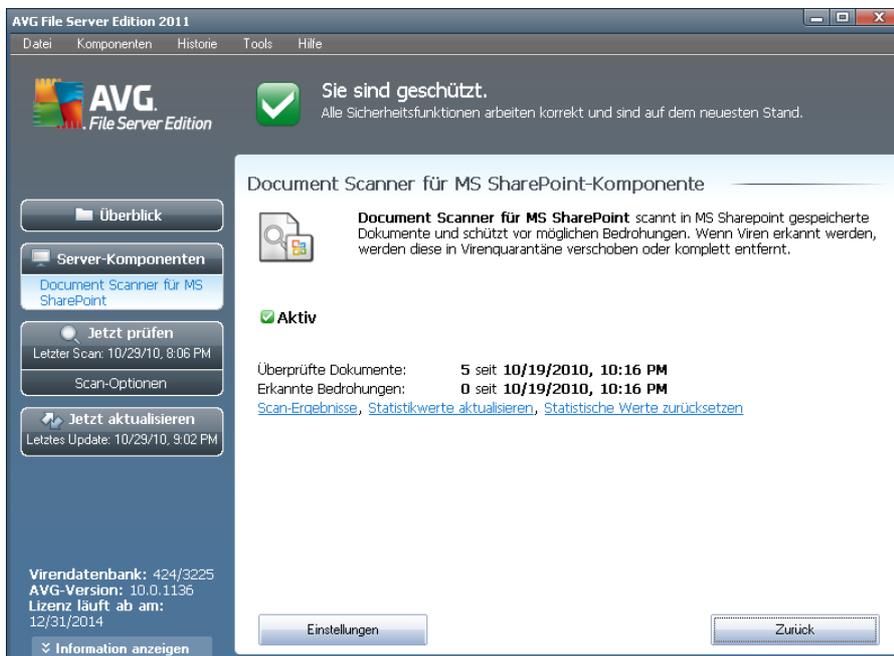
9.1. Document Scanner für MS SharePoint

9.1.1. Grundlagen zu Document Scanner

Die Server-Komponente **Document Scanner für MS SharePoint** scannt Dokumente, die in MS SharePoint gespeichert sind. Erkannte Viren werden in die [Virenquarantäne](#) verschoben oder vollständig entfernt.

Microsoft SharePoint ist eine Zusammenfassung von Produkten und Software und beinhaltet neben einer wachsenden Anzahl an Komponenten z. B. folgende Komponenten: Internet Explorer-basierte Kollaborationsfunktionen, Prozessverwaltungsmodule, Suchmodule sowie eine Dokumentenverwaltungsplattform. SharePoints können für das Hosting von Websites verwendet werden, die auf gemeinsame Arbeitsbereiche, Informationsspeicher und Dokumente zugreifen.

9.1.2. Benutzeroberfläche von Document Scanner



Neben einer Übersicht über die wichtigsten statistischen Daten und Informationen zum aktuellen Status der Komponente (*Die Komponente ist aktiv*) enthält die Benutzeroberfläche des **Document Scanner für MS SharePoint** eine kurze Übersicht über Statistiken der Komponente:

- **Überprüfte Dokumente** – Anzahl der überprüften Dokumente ab einem bestimmten Datum



- **Erkannte Bedrohungen** – Anzahl der erkannten Bedrohungen ab einem bestimmten Datum

Sie können diese statistischen Daten jederzeit aktualisieren, indem Sie auf den Link **Statistikwerte aktualisieren** klicken. Daraufhin werden umgehend aktualisierte Daten angezeigt. Wenn Sie alle statistischen Daten auf null setzen möchten, klicken Sie auf den Link **Statistische Daten zurücksetzen**. Durch Klicken auf den Link **Scan-Ergebnis** wird ein neuer Dialog mit aufgelisteten Scan-Ergebnissen angezeigt. Mithilfe von Optionsfeldern und/oder Reitern können Sie die Daten in der Liste sortieren.

Schaltflächen

Auf der Benutzeroberfläche des **Document Scanner für MS SharePoint** sind folgende Schaltflächen verfügbar:

- **Einstellungen** – öffnet ein neues Dialogfeld, in dem Sie verschiedene Parameter anpassen können, die die Viren-Scan-Leistung von **Document Scanner für MS SharePoint** betreffen (weitere Informationen zu diesem Dialogfeld finden Sie in den Kapiteln [Erweiterte Einstellungen für Document Scanner für MS SharePoint](#) und/oder [Erkennungsaktionen](#)).
- **Zurück** – Klicken Sie auf diese Schaltfläche, um zur [Standardoberfläche der Server-Komponenten](#) zurückzukehren.



10. AVG für SharePoint Portal Server

Dieses Kapitel beschäftigt sich mit der Wartung von AVG auf einem speziellen Fileserver-Typ, dem **MS SharePoint Portal Server**.

10.1. Programmwartung

AVG für SharePoint Portal Server verwendet die Virenskan-Benutzeroberfläche von Microsoft SP VSAPI 1.4, um Ihren Server vor Vireneinfektionen zu schützen. Die Objekte auf dem Server werden beim Up- bzw. Download auf den Server bzw. vom Server auf Malware gescannt. Die Konfiguration des Virenschutzes kann über die Benutzeroberfläche der **Zentralen Verwaltung** des SharePoint Portal Server durchgeführt werden. Über die Benutzeroberfläche der **Zentraladministration** können Sie auch die Protokolldatei von **AVG für SharePoint Portal Server** verwalten und anzeigen.

Sie können die **Zentrale Verwaltung des SharePoint Portal Server** starten, wenn Sie auf dem Computer angemeldet sind, der als Server dient. Die Verwaltungsoberfläche ist webbasiert (*so wie die Benutzeroberfläche von SharePoint Portal Server*) und kann geöffnet werden, indem Sie die Option **SharePoint Central Administration** im Windows-**Startmenü** unter **Programm/Microsoft Office Server** (abhängig von Ihrer Version von **SharePoint Portal Server**) verwenden oder indem Sie die **Verwaltung** öffnen und die Option **SharePoint Central Administration** auswählen.

Mit entsprechenden Zugriffsrechten und der entsprechenden URL können Sie die Webseite **Zentrale Verwaltung des SharePoint Portal Server** auch per Remote-Zugriff öffnen.

10.2. AVG für SPPS-Konfiguration – SharePoint 2007

Über die Benutzeroberfläche der **Zentralen Verwaltung von SharePoint 3.0** können Sie die Leistungsparameter und Aktionen für den **AVG für SharePoint Portal Server-Scanner** problemlos konfigurieren. Wählen Sie die Option **Operations** im Abschnitt **Central Administration**. Ein neuer Dialog wird angezeigt. Wählen Sie die Option **Antivirus** im Bereich **Security Configuration**.

Security Configuration

- ▣ Service accounts
- ▣ Information Rights Management
- ▣ Antivirus
- ▣ Blocked file types
- ▣ Update farm administrator's group
- ▣ Information management policy configuration
- ▣ Manage settings for single sign-on

Das folgende Fenster wird angezeigt:



Central Administration > Operations > Antivirus

Antivirus

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Learn about configuring antivirus settings.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents.

- Scan documents on upload
- Scan documents on download
- Allow users to download infected documents
- Attempt to clean infected documents

Antivirus Time Out

You can specify how long the virus scanner should run before timing out. If server response time is slow while scanning, you may want to decrease the number of seconds.

Time out duration (in seconds):

Antivirus Threads

You can specify the number of execution threads on the server that the virus scanner may use. If server response time is slow while scanning, you may want to decrease the number of threads allowed for virus scanning.

Number of threads:

OK

Cancel

Hier können Sie verschiedene Leistungsfunktionen und Scanaktionen für den Virenschutz von **AVG für SharePoint Portal Server** konfigurieren:

- **Scan documents on upload** – Aktivieren/deaktivieren Sie den Scan von Dokumenten, die gerade hochgeladen werden.
- **Scan documents on download** – Aktivieren/deaktivieren Sie den Scan von Dokumenten, die gerade heruntergeladen werden.
- **Allow users to download infected documents** – Gestatten/verweigern Sie Benutzern das Herunterladen infizierter Dokumente.
- **Versuchen, infizierte Dokumente zu löschen** – Aktivieren/deaktivieren Sie das automatische Löschen infizierter Dokumente (wenn möglich)
- **Zeitbegrenzung für den Scan in Sekunden** – Maximale Anzahl an Sekunden, die der Scanvorgang nach einem Einzelstart ausgeführt wird (Setzen Sie den Wert herab, wenn der Server beim Scannen von Dokumenten sehr langsam zu sein scheint.)
- **Anzahl an Threads** – Maximale Anzahl der Virenskan-Threads, die gleichzeitig ausgeführt werden. Wenn die Anzahl erhöht wird, werden mehrere Threads parallel ausgeführt, wodurch der Scan beschleunigt wird. Andererseits wird jedoch eventuell die Reaktionszeit des Servers verlängert.

10.3. AVG für SPPS-Konfiguration – SharePoint 2003

Über die Benutzeroberfläche der **Zentralen Verwaltung des SharePoint Portal Servers** können Sie die Leistungsparameter und Aktionen für den **AVG für SharePoint Portal Server**-Scanner problemlos konfigurieren. Wählen Sie die Option **Antivirus Actions Configuration** im Abschnitt **Security Configuration**:

Security Configuration

Use these links to update the security options which impact all virtual servers, and to add, update, or change user information for a single top-level Web site.

- Set SharePoint administration group
- Manage site collection owners
- Manage Web site users
- Manage blocked file types
- Configure antivirus settings

Das folgende Fenster wird angezeigt:

Windows SharePoint Services
Configure Antivirus Settings

Use this page to configure settings for virus scanning. You must install virus scanning software on all Web servers that are hosting documents before these settings can take effect. [Show me more information.](#)

Antivirus Settings

Specify when you want documents stored in document libraries and lists to be virus scanned, and whether you want your virus scanner to attempt to clean infected documents. You can also specify how long the virus scanner should run before timing out, and the number of execution threads on the server that it may use. If server response time is slow while scanning, you may want to decrease the number of seconds and threads allowed for virus scanning.

Scan documents on upload

Scan documents on download

Allow users to download infected documents

Attempt to clean infected documents

Time out scanning after seconds

Allow scanner to use up to threads

Hier können Sie verschiedene Leistungsfunktionen und Scanaktionen für den Virenschutz von **AVG für SharePoint Portal Server** konfigurieren:

- **Scan documents on upload** – Aktivieren/deaktivieren Sie den Scan von Dokumenten, die gerade hochgeladen werden.
- **Scan documents on download** – Aktivieren/deaktivieren Sie den Scan von Dokumenten, die gerade heruntergeladen werden.



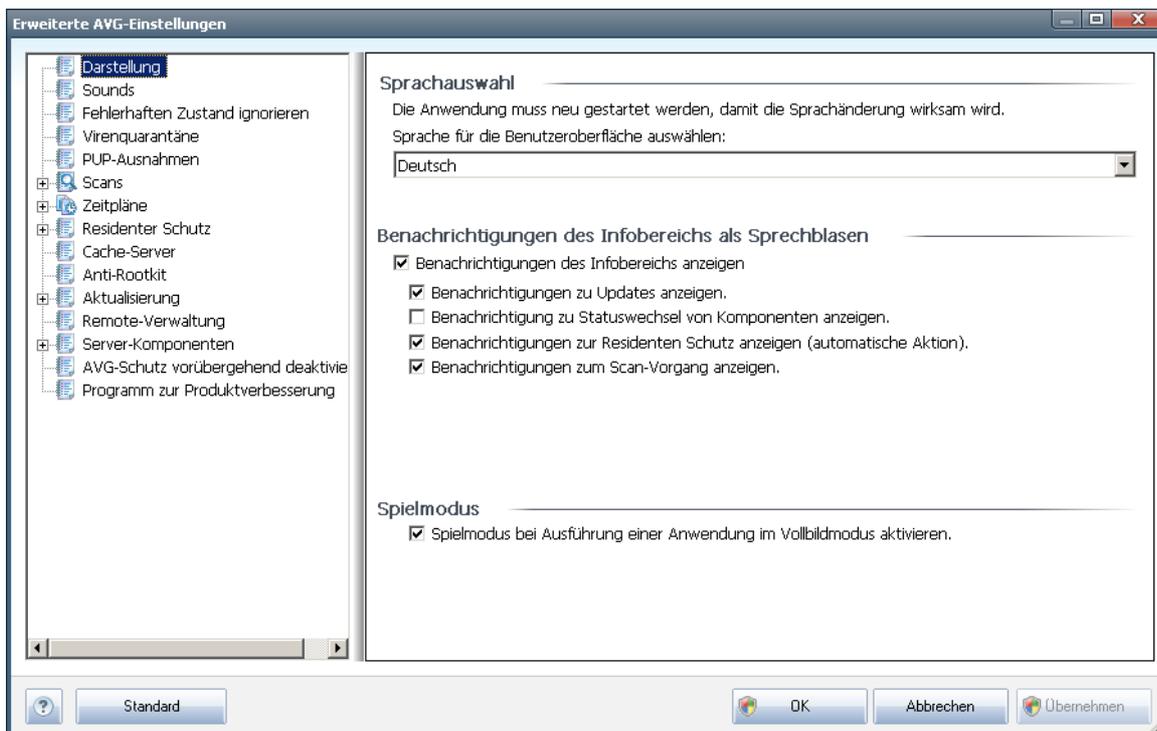
- **Allow users to download infected documents** – Gestatten/verweigern Sie Benutzern das Herunterladen infizierter Dokumente.
- **Versuchen, infizierte Dokumente zu löschen** – Aktivieren/deaktivieren Sie das automatische Löschen infizierter Dokumente (wenn möglich)
- **Zeitbegrenzung für den Scan** – Maximale Anzahl an Sekunden, die der Scanvorgang nach einem Einzelstart ausgeführt wird (*Setzen Sie den Wert herab, wenn die Serverantwort beim Scannen von Dokumenten sehr langsam zu sein scheint*)
- **Maximal: X Teilvorgänge beim Scannen von Dokumenten ausführen** – Das X steht für die Anzahl der Virensan-Threads, die gleichzeitig ausgeführt werden können. Wenn die Anzahl erhöht wird, werden mehrere Threads parallel ausgeführt, wodurch der Scan beschleunigt wird. Andererseits wird jedoch eventuell die Reaktionszeit des Servers verlängert.

11. Erweiterte Einstellungen von AVG

Der Dialog zur erweiterten Konfiguration von **AVG File Server 2011** 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.

11.1. Darstellung

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



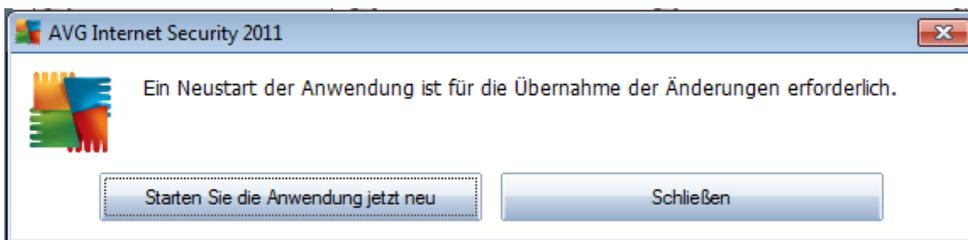
Sprachauswahl

Im Bereich **Sprachauswahl** kann aus dem Dropdown-Menü die gewünschte Sprache ausgewählt werden. Diese Sprache wird dann für die gesamte [Benutzeroberfläche von AVG](#) verwendet. 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 den Wechsel zur ausgewählten Sprache abzuschließen, müssen Sie die Benutzeroberfläche wie folgt neu starten:

- Wählen Sie die gewünschte Sprache aus, und bestätigen Sie Ihre Auswahl mit

der Schaltfläche **Übernehmen** (rechte untere Ecke)

- Klicken Sie zum Bestätigen auf die Schaltfläche **OK**
- Es wird ein Dialog angezeigt, in dem Sie darüber informiert werden, dass nach einer Sprachänderung der Benutzeroberfläche von AVG ein Neustart der Anwendung erforderlich ist:



Benachrichtigungen des Infobereichs als Sprechblasen

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

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

- **Benachrichtigungen des Infobereichs anzeigen** – Diese Option ist standardmäßig (*aktiviert*), so dass die Benachrichtigungen angezeigt werden. Wenn Sie die Markierung dieser Option aufheben, wird die Anzeige von Benachrichtigungen in Sprechblasen vollständig deaktiviert. Wenn diese Funktion aktiviert ist, können Sie auswählen, welche Benachrichtigungen angezeigt werden sollen:
 - **Benachrichtigungen des Infobereichs zu Updates** anzeigen – Legen Sie fest, ob Informationen zum Start, Fortschritt und Abschluss des Aktualisierungsvorgangs von AVG angezeigt werden sollen;
 - **Benachrichtigungen zum Statuswechsel von Komponenten anzeigen** – Legen Sie fest, ob Informationen zur Aktivität/Inaktivität der Komponenten angezeigt werden sollen und ob Sie über auftretende Probleme informiert werden möchten. Die Option zur Benachrichtigung über den fehlerhaften Status einer Komponente entspricht der Informationsfunktion des [Infobereichsymbols](#), das (durch einen Farbwechsel) auf Probleme aufmerksam macht, die im Zusammenhang mit AVG-Komponenten auftreten;



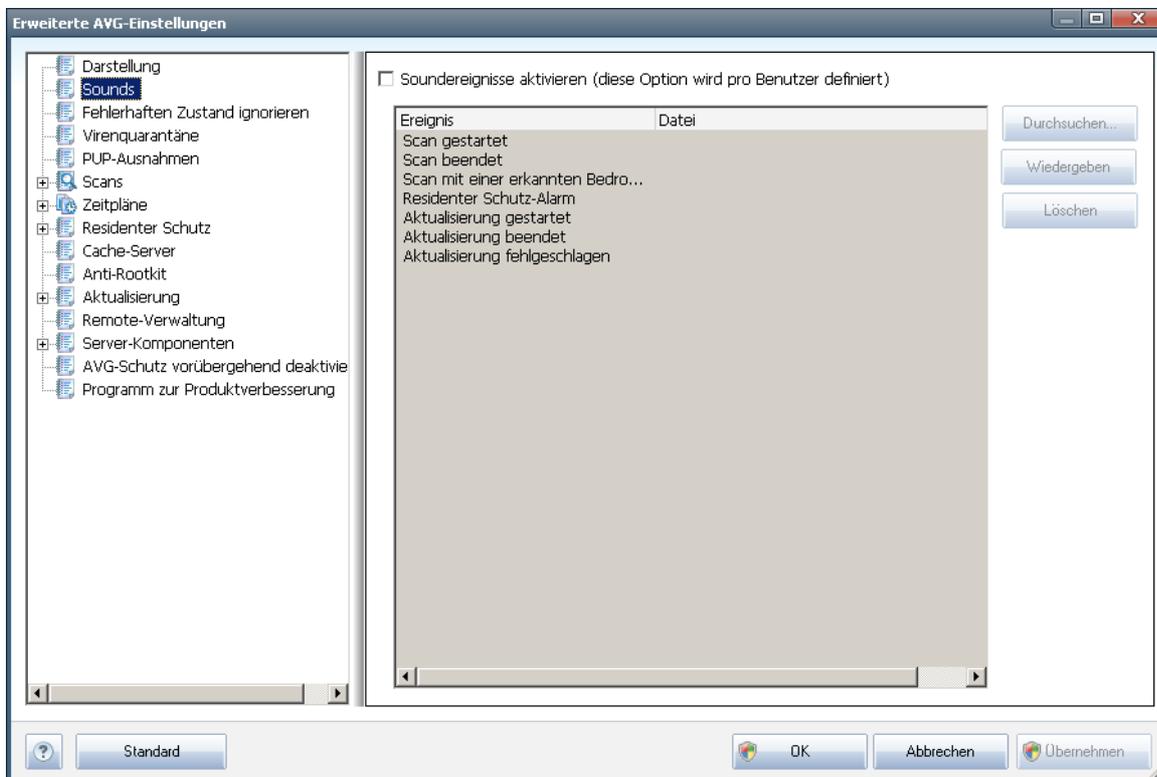
- **Benachrichtigungen des Infobereichs zu Residenter Schutz anzeigen (automatische Aktion)** – Legen Sie fest, ob Informationen zum Speichern, Kopieren und Öffnen von Dateien angezeigt werden sollen (diese Konfiguration zeigt an, ob die Option Automatisches Heilen des Residenten Schutzes aktiviert ist);
- **Benachrichtigungen des Infobereichs zum Scan-Vorgang anzeigen** – Legen Sie fest, ob Informationen zum automatischen Start, Fortschritt und Abschluss des geplanten Scan-Vorgangs angezeigt werden sollen;

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).

11.2. Sounds

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

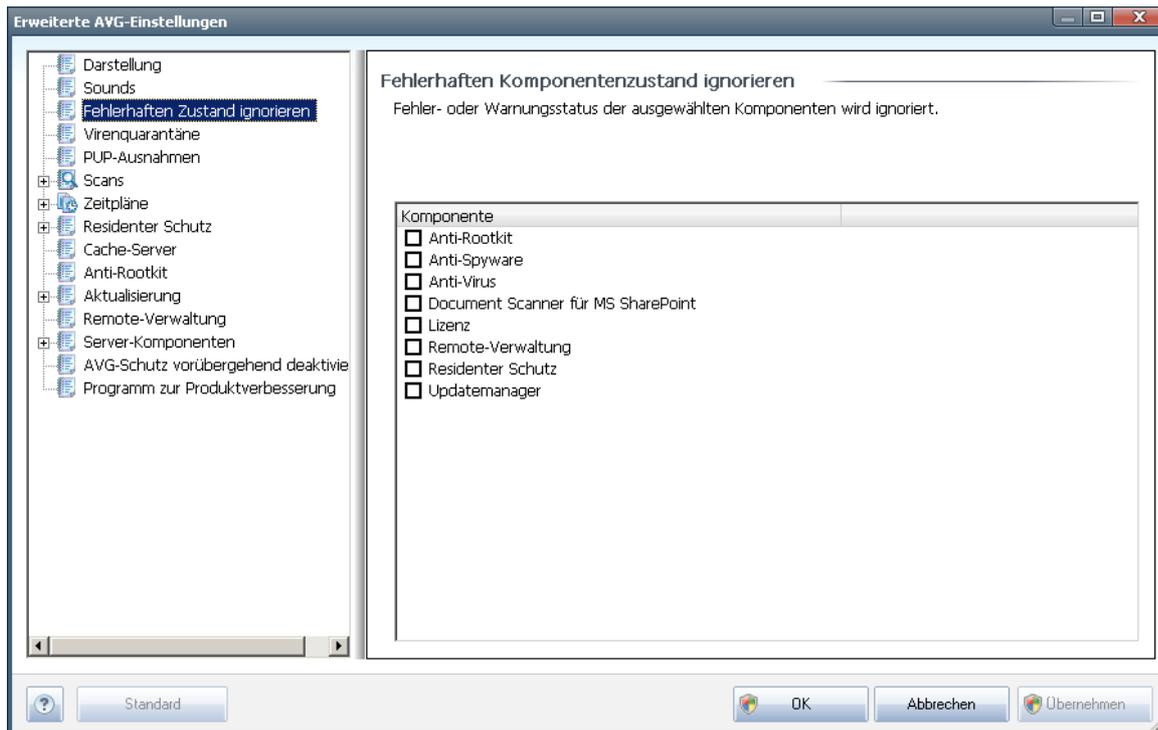


Wählen Sie nun aus der Liste das gewünschte Ereignis aus, und suchen Sie auf Ihrem Datenträger nach einem Sound (**Durchsuchen**), den Sie diesem Ereignis zuweisen möchten. Um den ausgewählten Sound anzuhören, markieren Sie das Ereignis in der Liste, und klicken Sie auf die Schaltfläche **Wiedergeben**.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

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

11.3. Fehlerhaften Zustand ignorieren

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



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

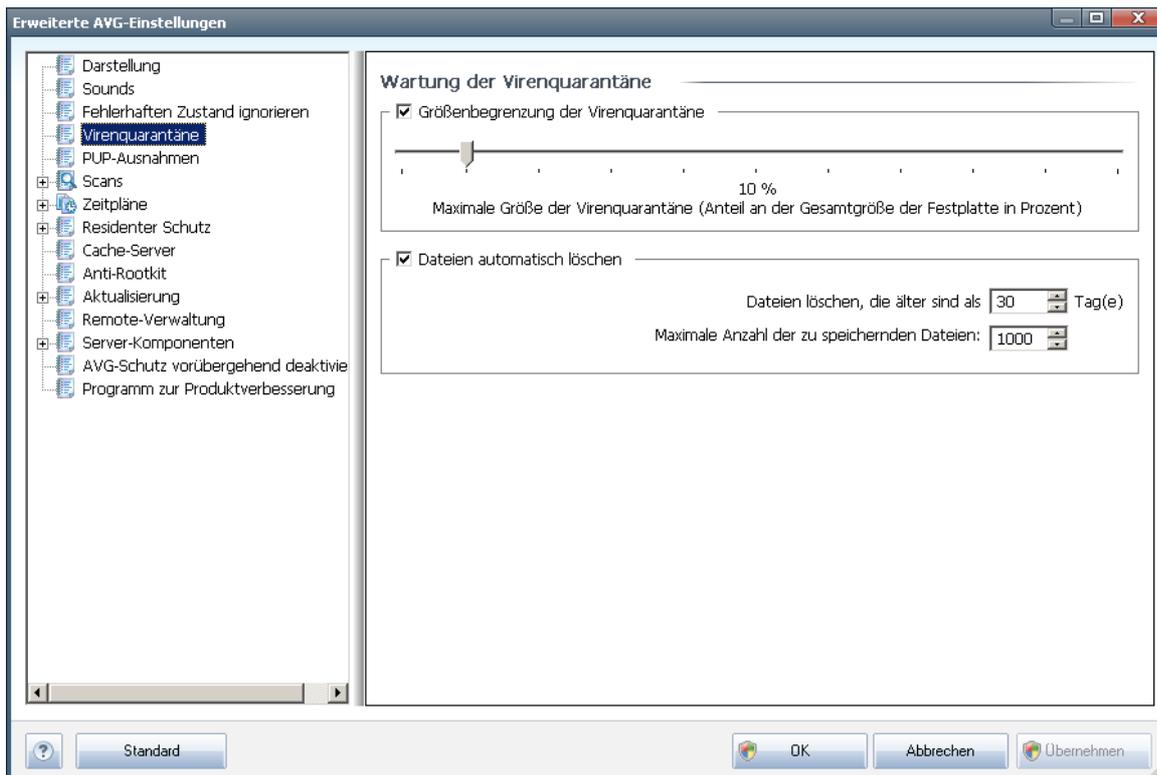
- **Symbol im Infobereich** – Wenn alle Teile von AVG ordnungsgemäß funktionieren, wird das Symbol in vier Farben dargestellt. Tritt ein Fehler auf, wird das Symbol mit einem gelben Ausrufezeichen angezeigt
- und eine Beschreibung zum bestehenden Problem wird im Bereich **Informationen zum Sicherheitsstatus**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

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

Für diesen Fall können Sie im oben angezeigten Dialog Komponenten auswählen, die eventuell einen fehlerhaften Status aufweisen (*oder deaktiviert sind*) oder über die Sie

keine Informationen erhalten möchten. Alternativ steht für einige Komponenten die Option **Komponentenstatus ignorieren** zur Verfügung, die über die Komponentenübersicht im [Hauptfenster von AVG](#) festgelegt werden kann.

11.4. Virenquarantäne



Im Dialog **Wartung der Virenquarantäne** können Sie mehrere Parameter hinsichtlich der Verwaltung der in der [Virenquarantäne](#) gespeicherten Objekte festlegen:

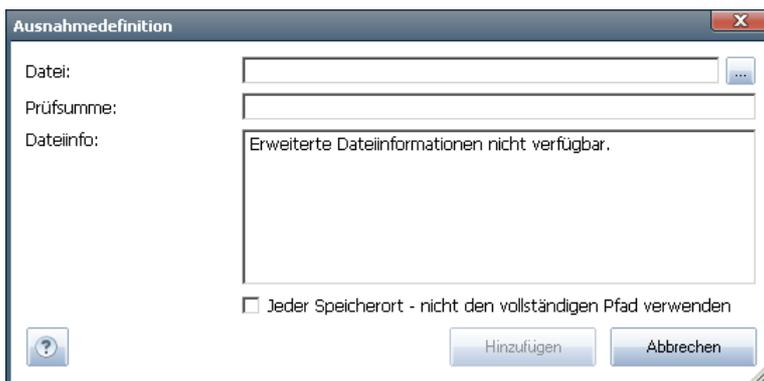
- **Größenbegrenzung der Virenquarantäne** – Mithilfe des Schiebereglers können Sie die maximale Größe der [Virenquarantäne](#) festlegen. Die Größe wird proportional zur Größe Ihrer lokalen Festplatte angegeben.
- **Dateien automatisch löschen** – In diesem Bereich wird die maximale Dauer festgelegt, 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

11.5. PUP-Ausnahmen

AVG File Server 2011 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*

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*).

11.6. Scans

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

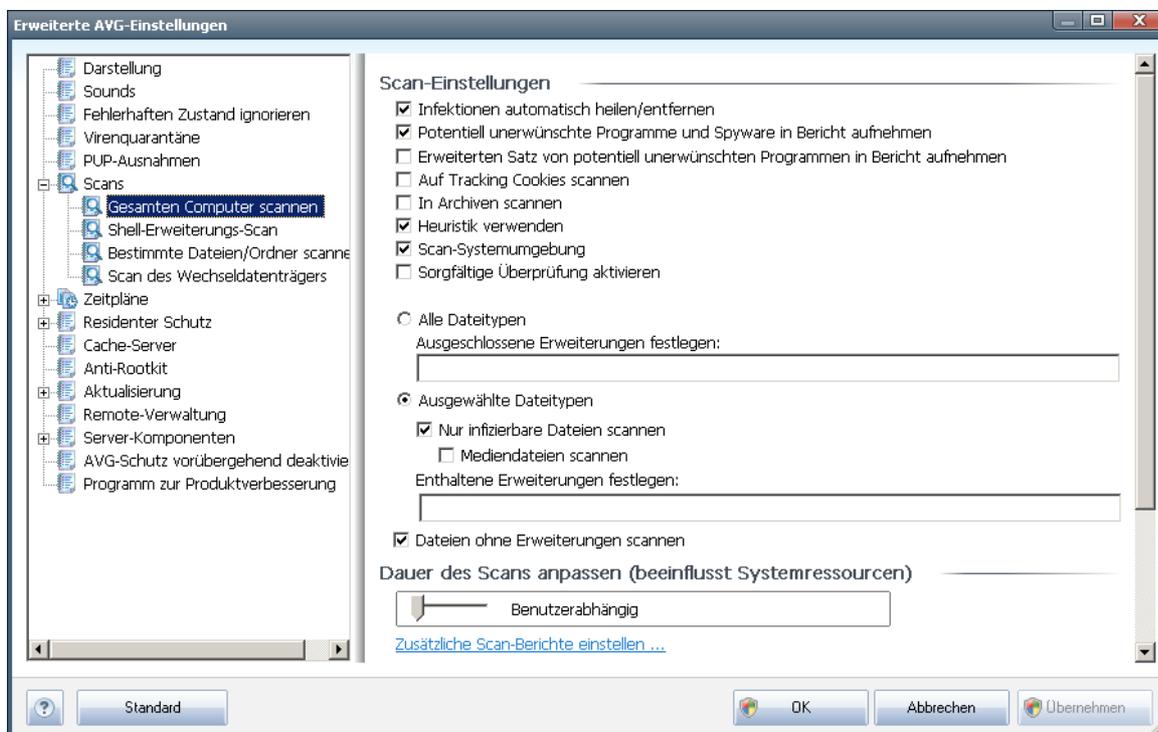
- **Scan des gesamten Computers** – Vordefinierter Standard-Scan des gesamten Computers
- **Shell-Erweiterungs-Scan** – Bestimmter Scan eines ausgewählten Objekts direkt von der Umgebung des Windows Explorer aus



- **Bestimmte Dateien/Ordner scannen** – Vordefinierter Standard-Scan ausgewählter Bereiche Ihres Computers
- **Scan des Wechseldatenträgers** – Bestimmter Scan der Wechseldatenträger, die an Ihren Computer angeschlossen sind

11.6.1. 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.

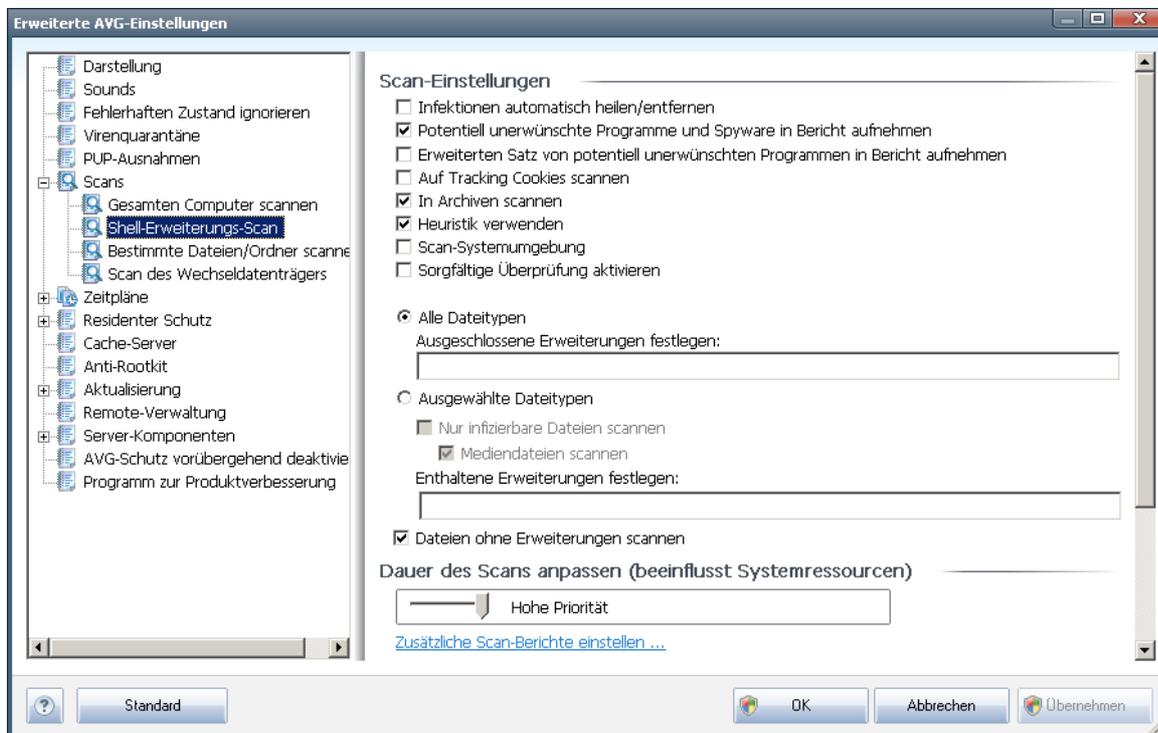
Zusätzliche Scan-Berichte einstellen ...

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:



11.6.2. 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](#):



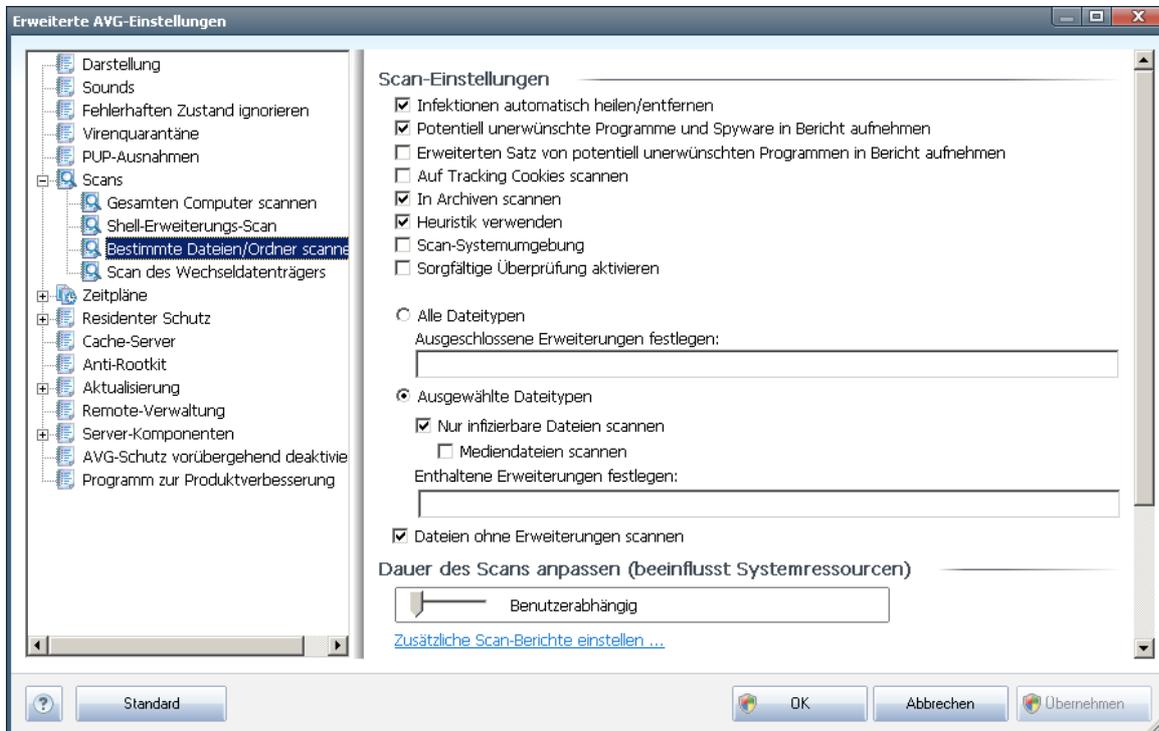
Die Parameterliste stimmt mit der Parameterliste der Option **Gesamten Computer scannen** überein. Die Standardeinstellungen unterscheiden sich jedoch: (Während beim Scan des gesamten Computers standardmäßig keine Archive, aber die Systemumgebung gescannt wird, verhält es sich beim Shell-Extension-Scan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

11.6.3. Bestimmte Dateien/Ordner scannen

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

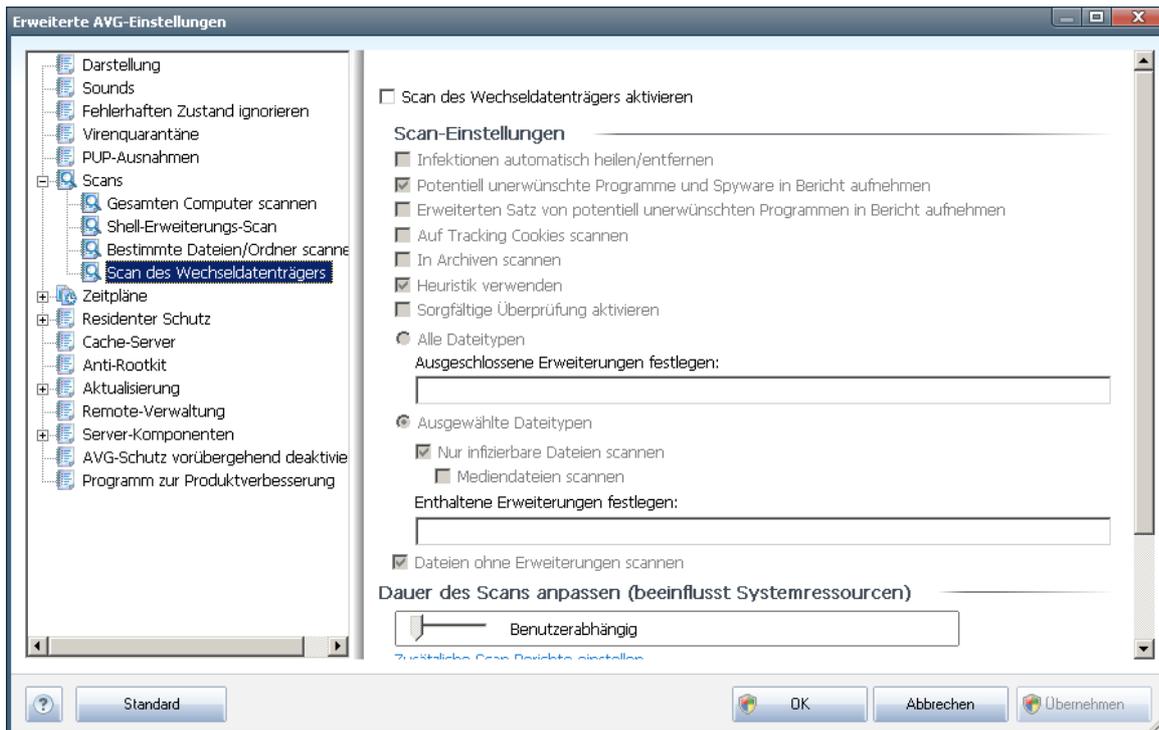


Alle Parameter, die in diesem Konfigurationsdialog festgelegt werden, gelten nur für die Scan-Bereiche, die unter der Option **Bestimmte Dateien oder Ordner scannen** ausgewählt wurden!

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

11.6.4. 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](#).

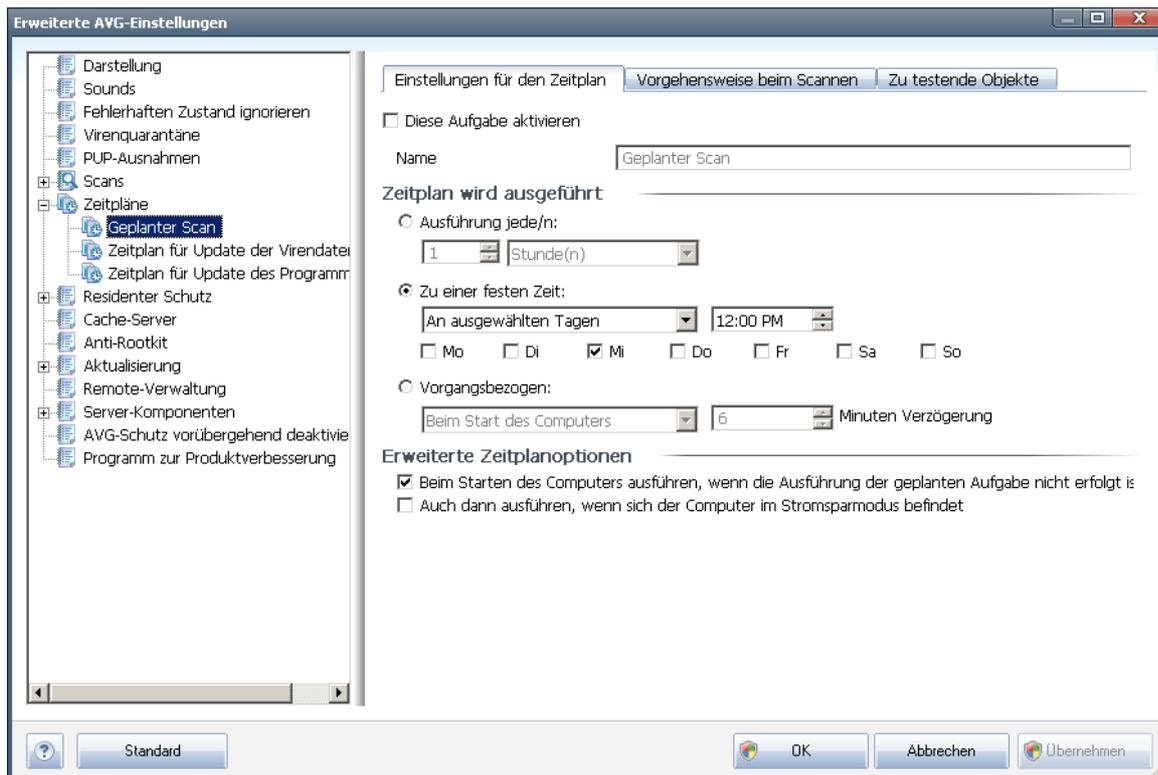
11.7. Zeitpläne

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

- [Geplanter Scan](#)
- [Zeitplan für Update der Virendatenbank](#)
- [Zeitplan für Update des Programms](#)

11.7.1. Geplanter Scan

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



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

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

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



bestimmte Versionen eines [Scans bestimmter Dateien oder Ordner](#).

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

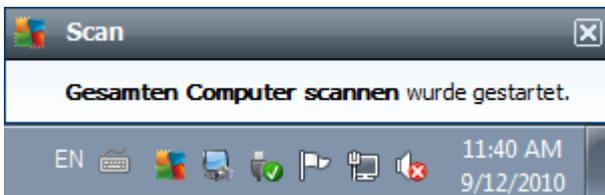
Zeitplan wird ausgeführt

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

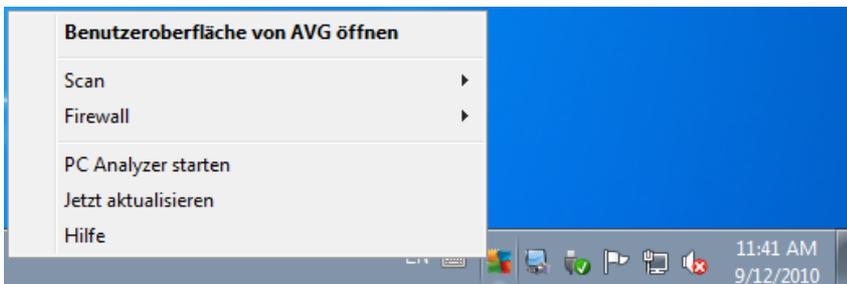
Erweiterte Zeitplanoptionen

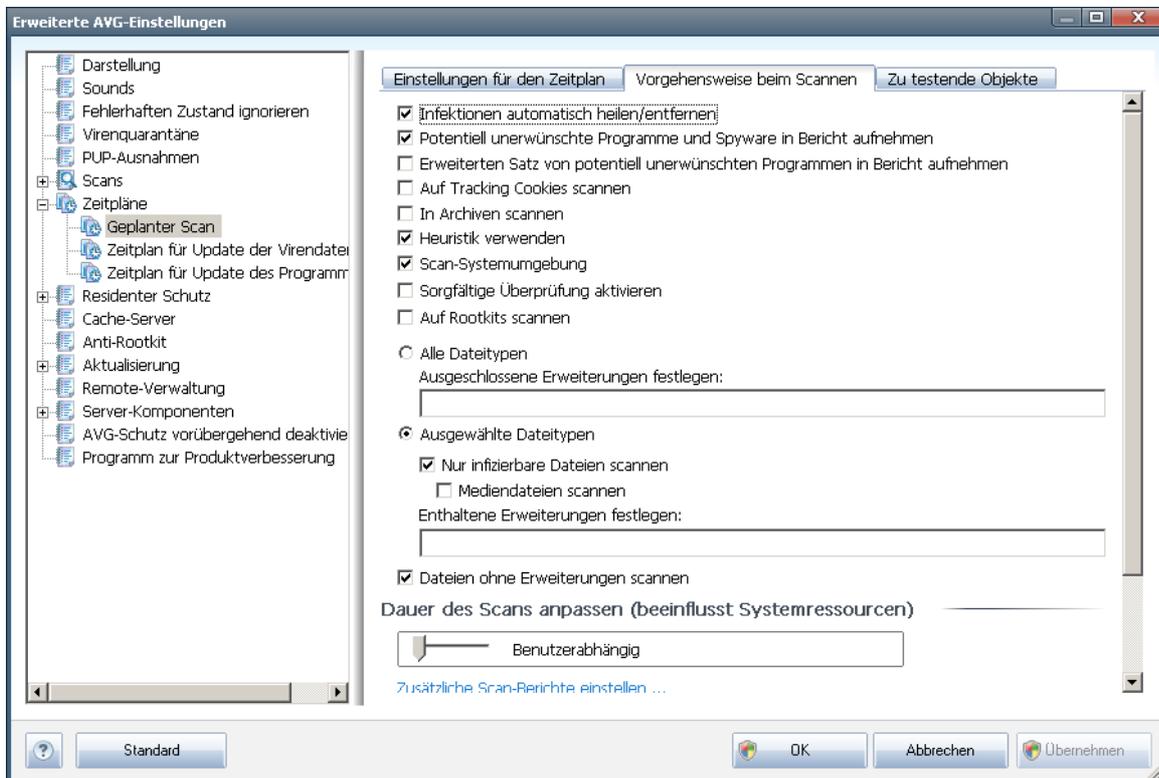
In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist.

Sobald der geplante Scan zu der von Ihnen festgelegten Zeit startet, werden Sie darüber über ein Popup-Fenster 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 angewendet. 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 diese Option 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.

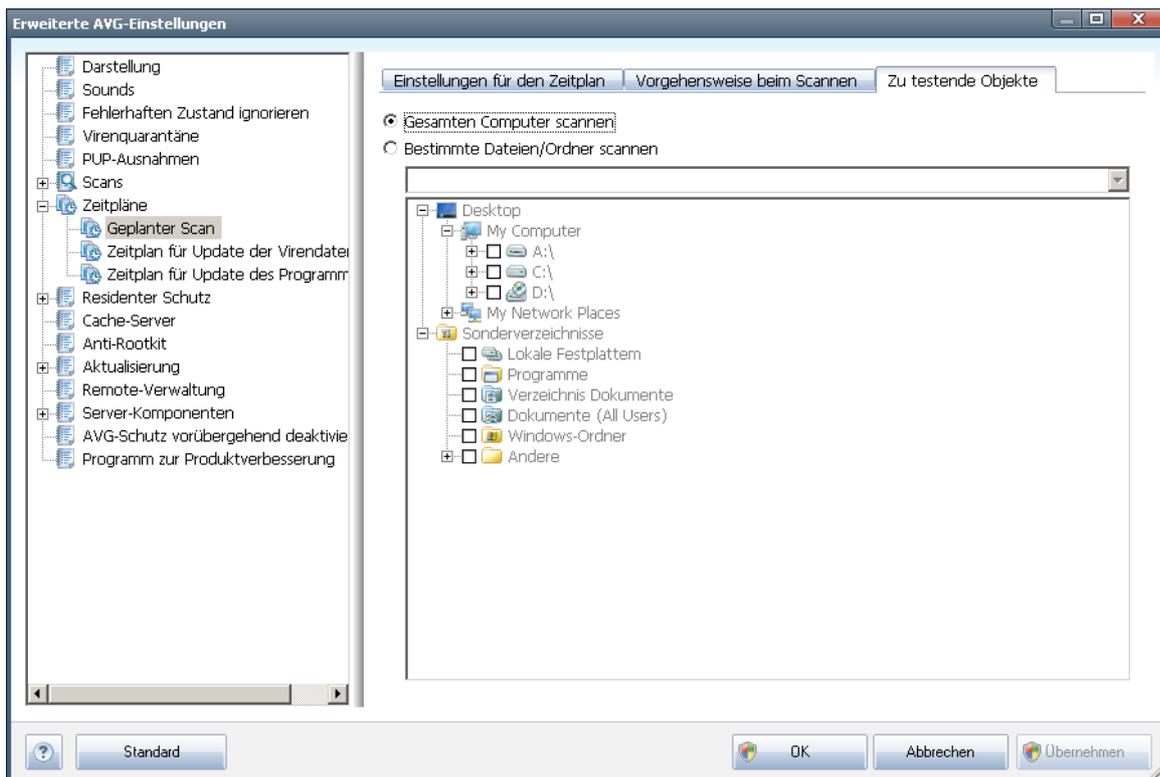
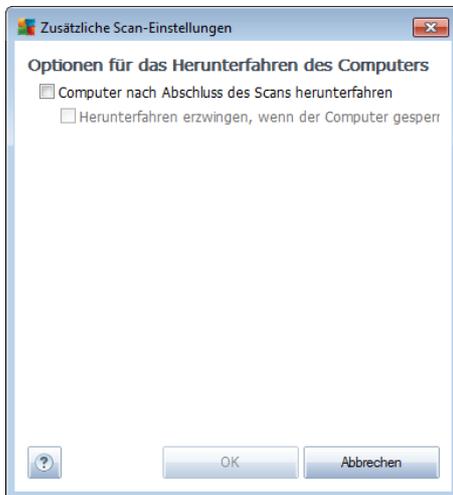
Zusätzliche Scan-Berichte einstellen

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:



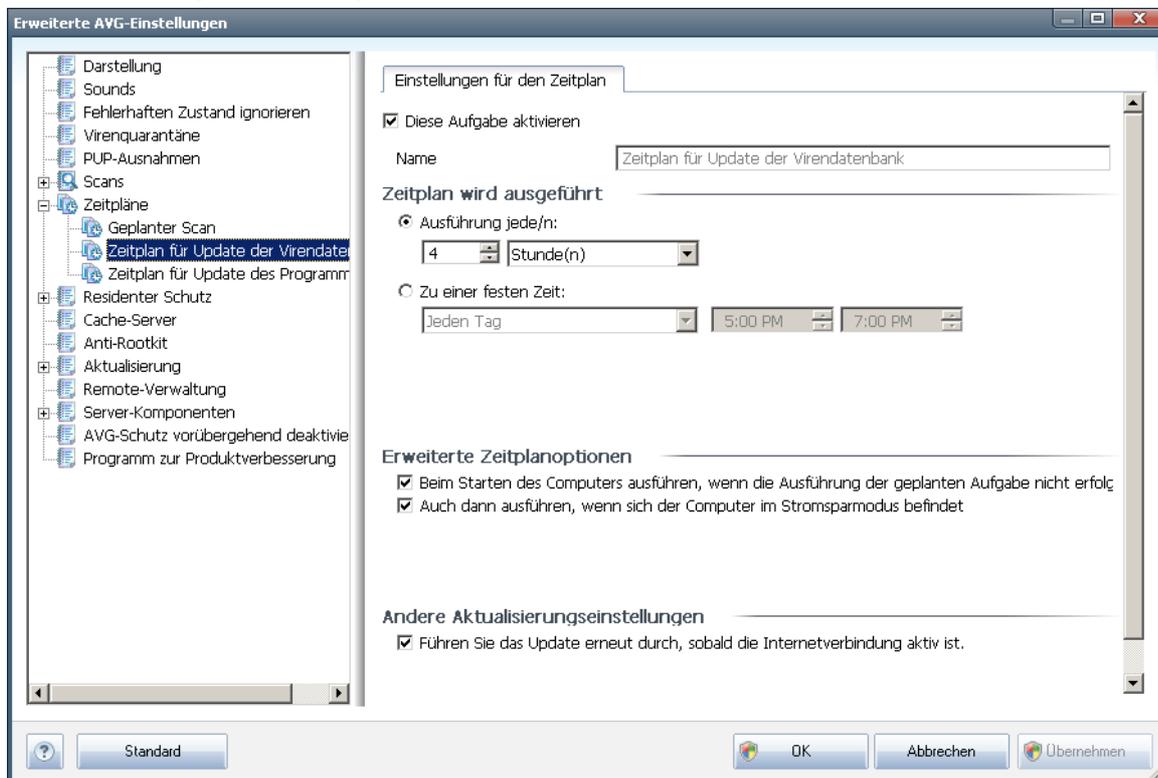
Zusätzliche Scan-Einstellungen

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.

11.7.2. Zeitplan für Update der Virendatenbank



Auf dem Reiter **Einstellungen für den Zeitplan** können Sie den Eintrag **Diese Aufgabe aktivieren** aktivieren oder deaktivieren, um das geplante Update der Virendatenbank vorübergehend zu deaktivieren. Anschließend können Sie den Zeitplan bei Bedarf hier wieder aktivieren. Der grundlegende Aktualisierungszeitplan der Virendatenbank erfolgt über die Komponente **Updatemanager**. In diesem Dialog können Sie verschiedene Parameter des Aktualisierungszeitplans der Virendatenbank im Detail festlegen. Im Textfeld mit dem Titel **Name** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

Zeitplan wird ausgeführt

Legen Sie in diesem Bereich die Zeitintervalle fest, in denen das neu geplante Update der Virendatenbank durchgeführt werden soll. Sie können entweder wiederholte Starts des 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 die



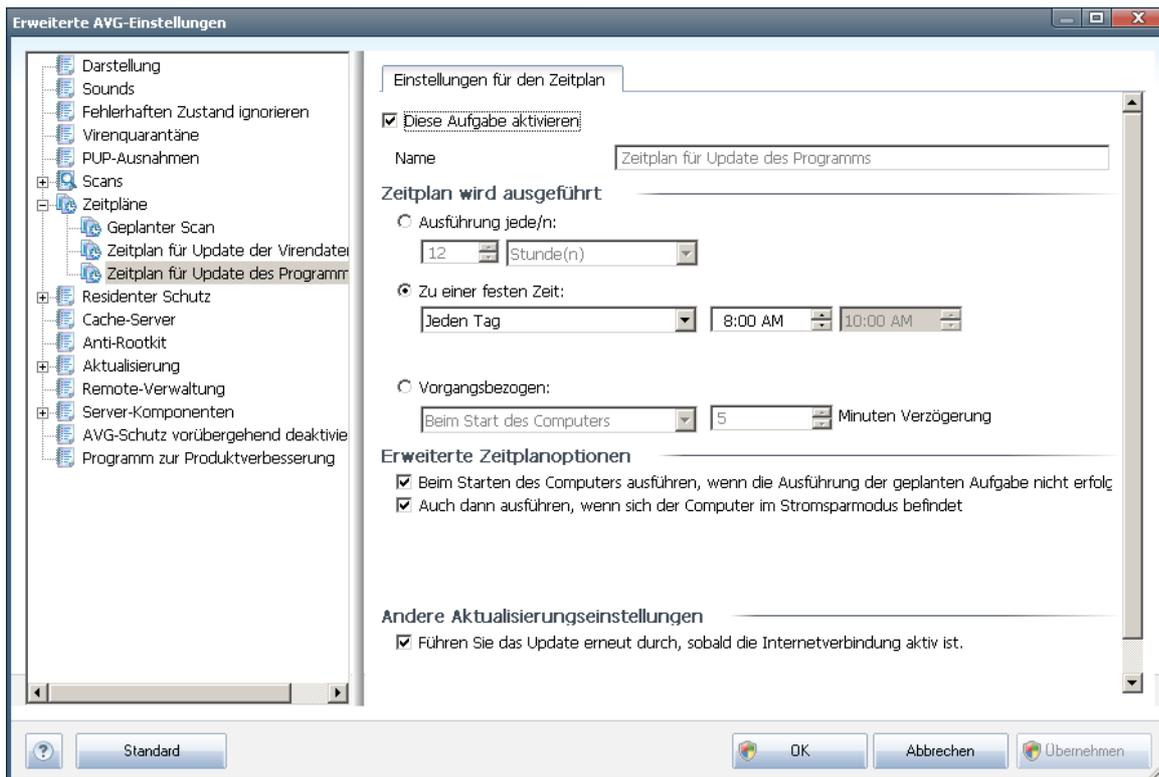
Virendatenbank aktualisiert werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmmodus befindet oder ganz ausgeschaltet ist).

Andere Aktualisierungseinstellungen

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

Sobald das geplante Update zu der von Ihnen festgelegten Zeit startet, werden Sie 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).

11.7.3. Zeitplan für Update des Programms



Auf dem Reiter **Einstellungen für den Zeitplan** können Sie den Eintrag **Diese Aufgabe aktivieren** aktivieren oder deaktivieren, um auf einfache Weise das geplante Programm-Update vorübergehend z.B. zu deaktivieren. Anschließend können Sie den Updatezeitplan bei Bedarf hier wieder aktivieren. Im Textfeld mit dem Titel **Name** (bei allen Standardzeitplänen deaktiviert) 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

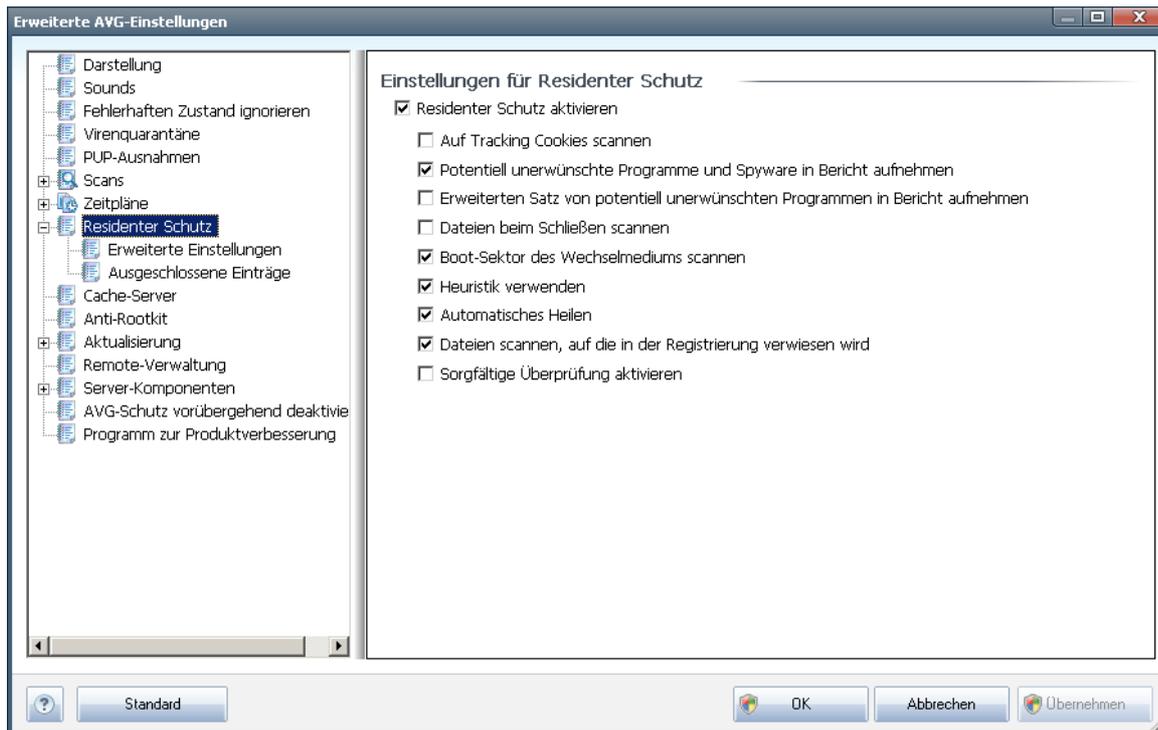
Aktivieren Sie die Option **Update erneut durchführen, sobald die Internetverbindung aktiv ist**, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung erneut gestartet wird.

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.

11.8. Residenter Schutz

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



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

- **Auf Tracking Cookies scannen** (*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

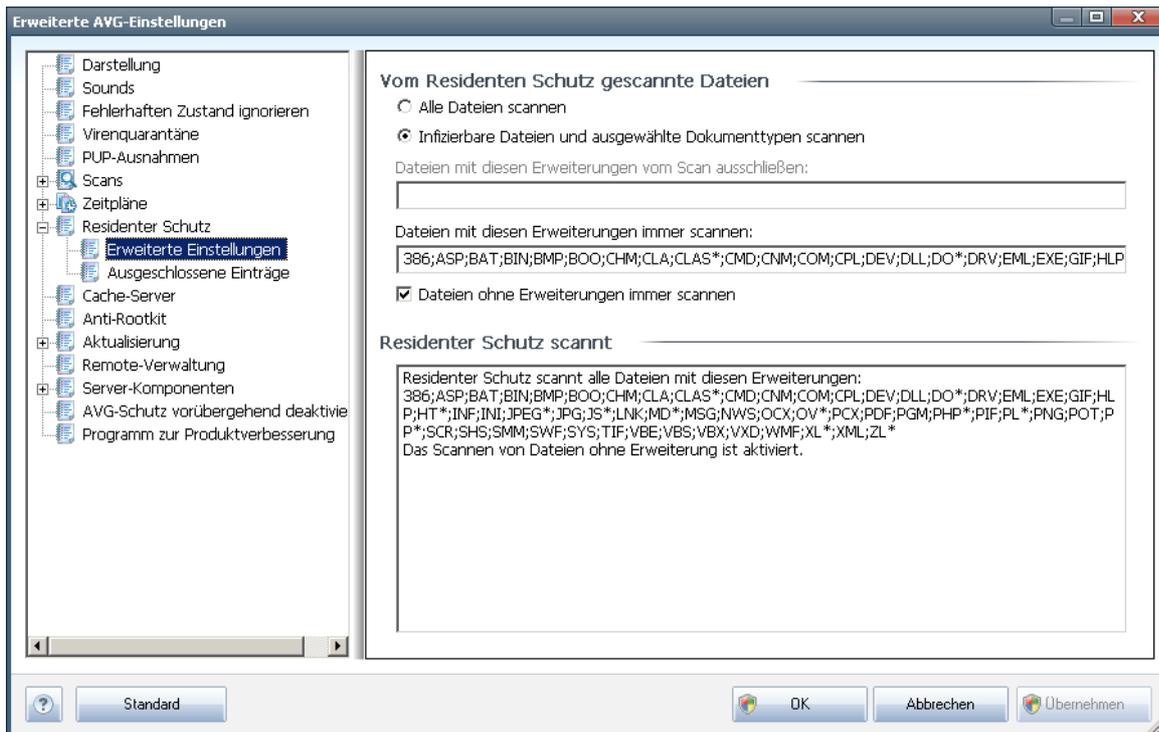


erweitertes Paket von [Spyware](#) zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können 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 Beenden 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*)
- **Automatisches Heilen** (*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.

11.8.1. Erweiterte Einstellungen

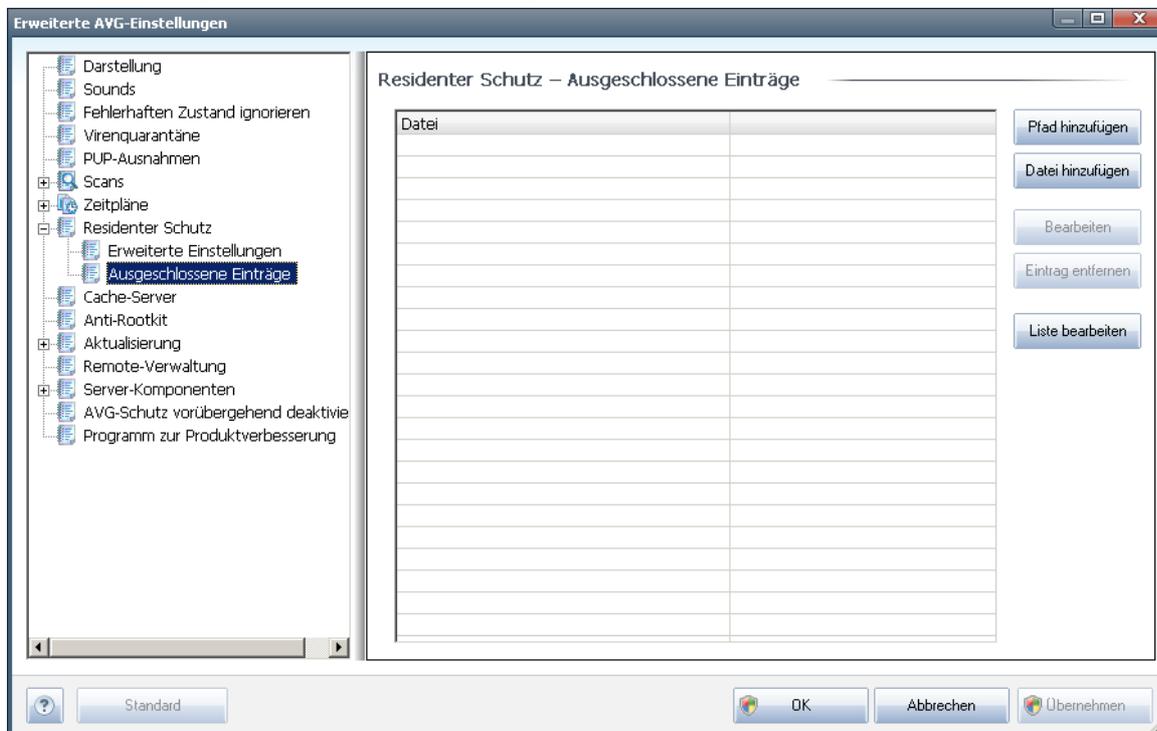
Im Dialog **Vom Residenten Schutz gescannte Dateien** können Sie festlegen, welche Dateien gescannt werden sollen (*durch Angabe der Erweiterungen*):



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

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

11.8.2. Ausgeschlossene Einträge



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

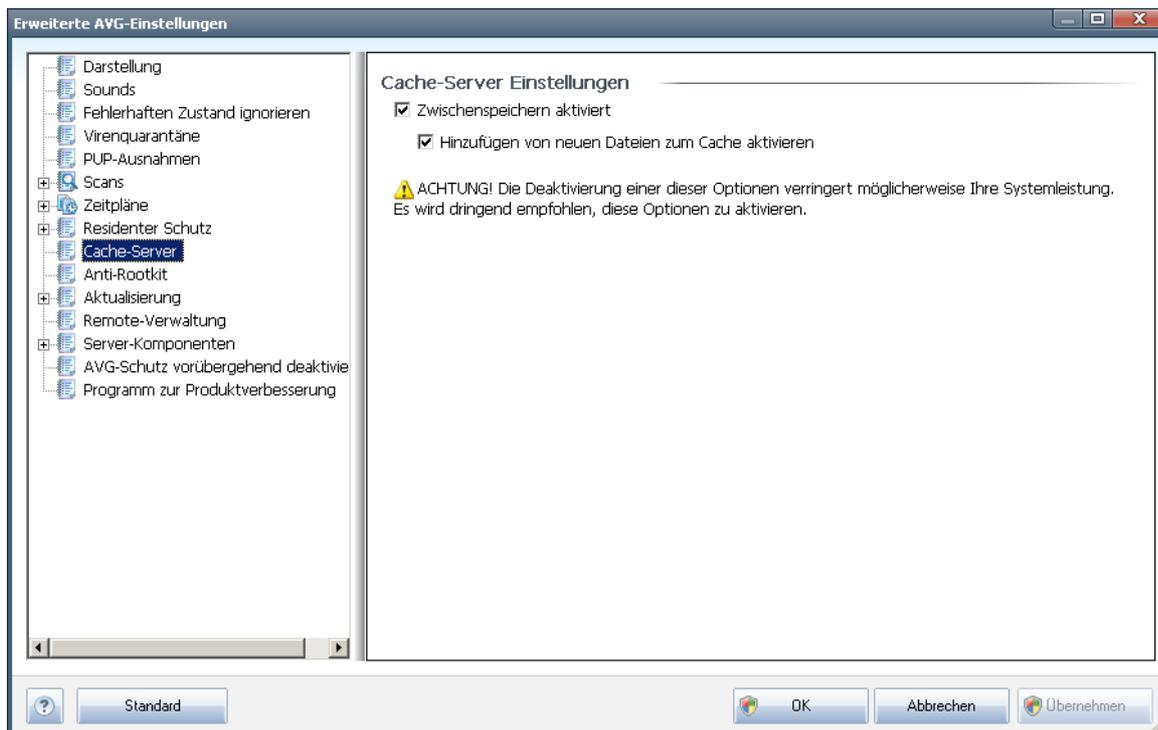
Wenn dies nicht unbedingt notwendig ist, empfehlen wir dringend, keine Einträge auszuschließen!

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

11.9. Cache-Server

Der **Cache-Server** ist ein Prozess, der alle Scans (*On-Demand-Scan, geplanter Scan des gesamten Computers, Scan durch den Residenten Schutz*) beschleunigen soll. Er sammelt und speichert Informationen vertrauenswürdiger Dateien (*Systemdateien mit digitaler Signatur usw.*): Diese Dateien werden als sicher eingestuft und beim Scan übersprungen.

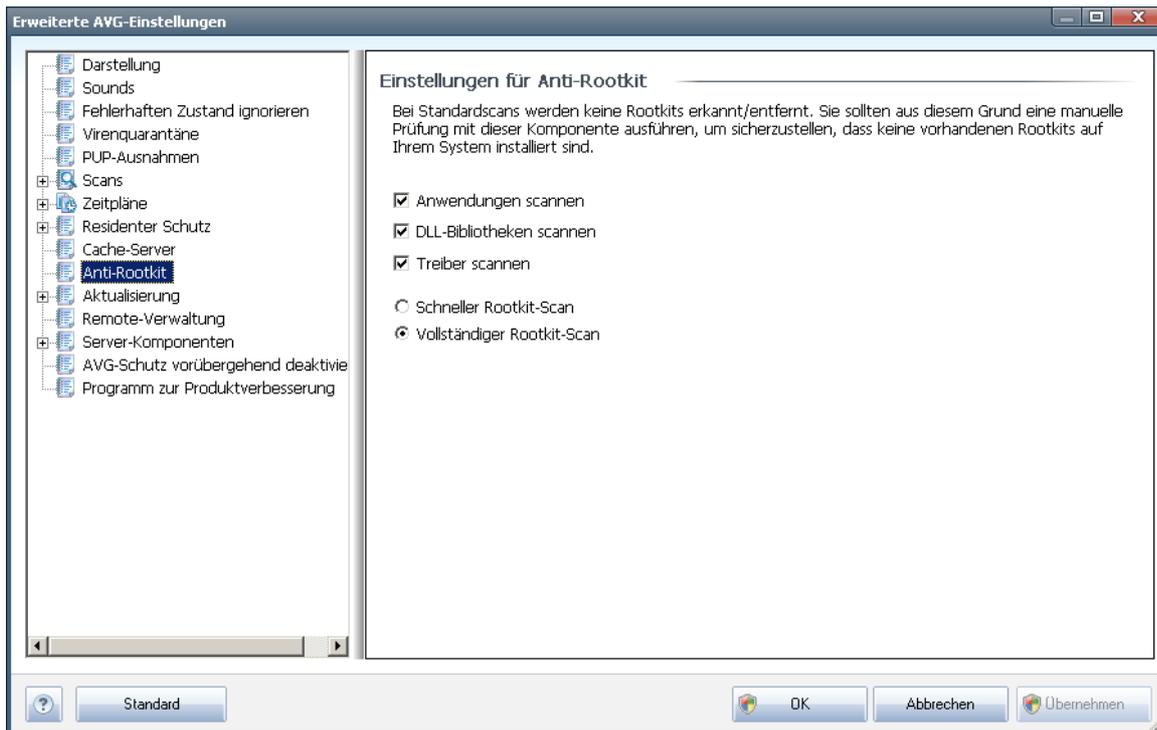


Im Dialog „Einstellungen“ stehen zwei Optionen zur Verfügung:

- **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.

11.10. Anti-Rootkit

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



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

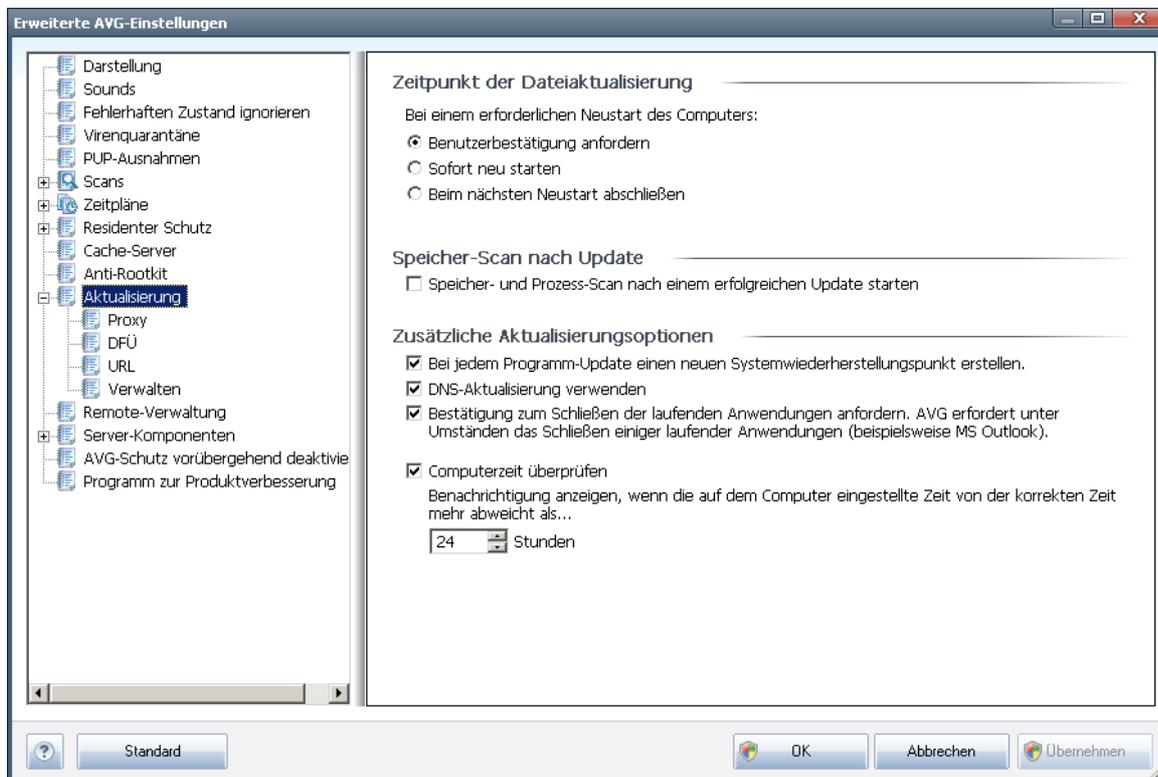
Aktivieren Sie die entsprechenden Kontrollkästchen, um festzulegen, welche Objekte gescannt werden sollen:

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

Wählen Sie anschließend den Rootkit-Scanmodus aus:

- **Schneller Rootkit-Scan** – 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*)

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

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

- **Benutzerbestätigung anfordern** – Sie werden aufgefordert, den Neustart Ihres Computers zu bestätigen, um den [Aktualisierungsprozess abzuschließen](#)
- **Sofort neu starten** – Der Computer wird automatisch neu gestartet, unmittelbar nachdem der [Aktualisierungsprozess](#) abgeschlossen ist. Sie müssen den Neustart nicht bestätigen



- **Beim nächsten Neustart abschließen** – Der Abschluss des [Aktualisierungsprozesses](#) wird bis zum nächsten Neustart des Computers verschoben – Bitte beachten Sie, dass diese Option nur empfohlen wird, wenn Sie sicher sind, dass der Computer regelmäßig, mindestens einmal täglich, neu gestartet wird

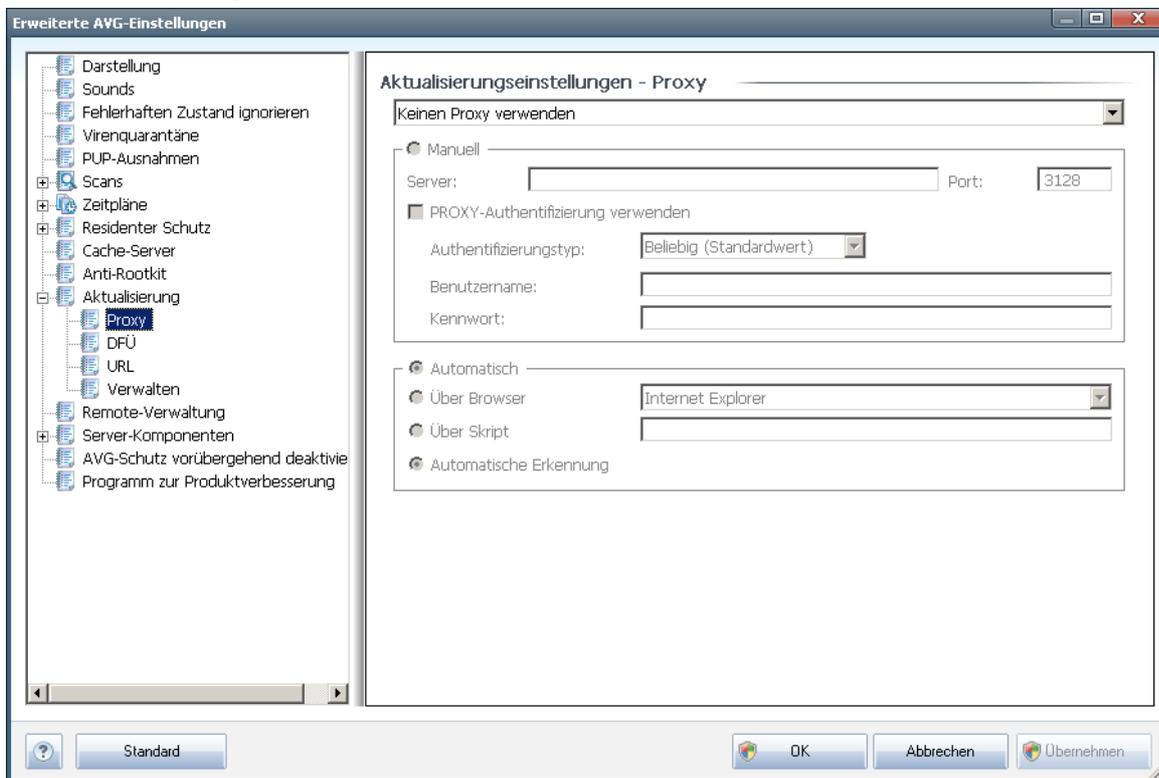
Speicher-Scan nach Update

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

Zusätzliche Aktualisierungsoptionen

- **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-Aktualisierung verwenden** – Aktivieren Sie dieses Kontrollkästchen, um zu bestätigen, dass Sie die Erkennungsmethode für Update-Dateien verwenden möchten, durch welche die zwischen dem Update-Server und dem AVG-Client übertragene Datenmenge verringert wird.
- **Mithilfe der Option „Bestätigung zum Schließen der laufenden Anwendungen anfordern“** (*standardmäßig aktiviert*) können Sie dafür sorgen, dass keine aktuell ausgeführten Anwendungen ohne Ihre Genehmigung geschlossen werden. Dies kann zum Abschluss des Updatevorgangs erforderlich sein;
- **Computerzeit überprüfen** – Aktivieren Sie diese Option, wenn eine Benachrichtigung angezeigt werden soll, falls die Computerzeit um mehr als die angegebene Anzahl an Stunden von der korrekten Zeit abweicht.

11.11.1. Proxy



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

- **Proxy verwenden**
- **Keinen Proxy verwenden** – Standardeinstellungen
- **Stellen Sie eine direkte Verbindung her, wenn eine Proxy-Verbindung fehlschlägt**

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*)

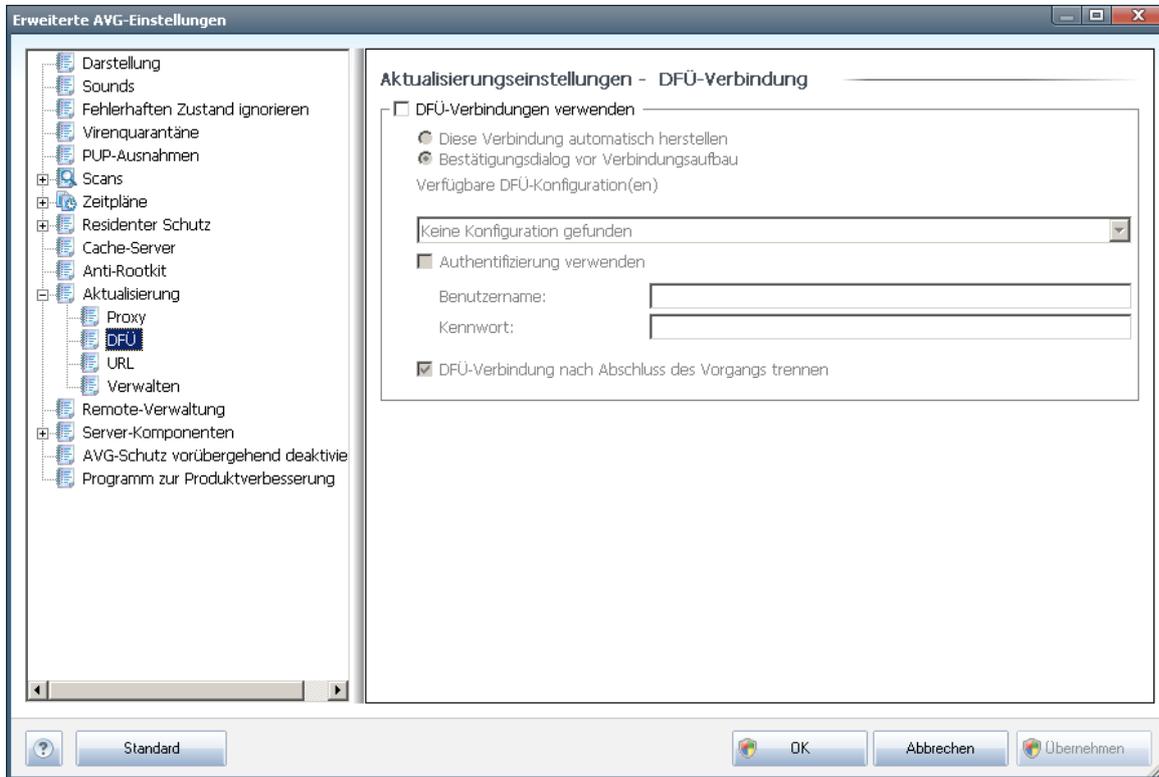
Auf dem Proxy-Server können auch besondere Regeln für jeden Benutzer festgelegt sein. Aktivieren Sie in diesem Fall das Kontrollkästchen **PROXY-Authentifizierung verwenden**, um zu bestätigen, dass Ihr Benutzername und Ihr Kennwort für die Verbindung mit dem Internet über den Proxy-Server gültig sind.

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

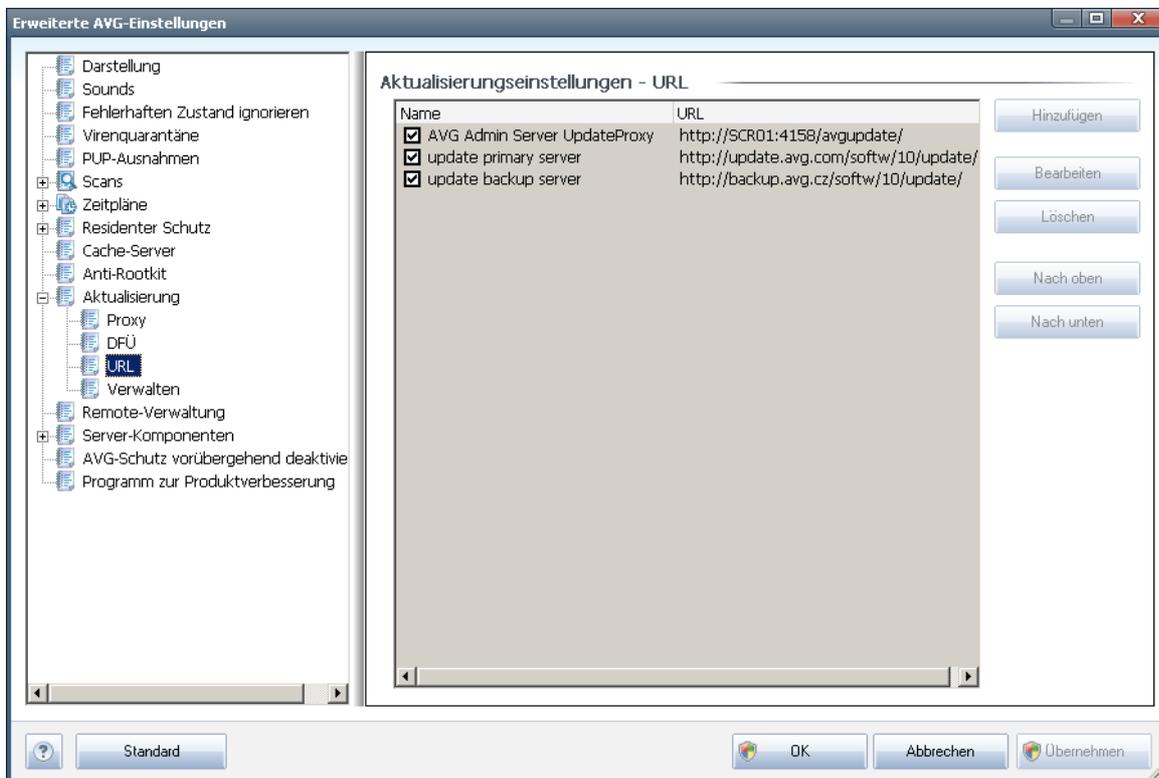
11.11.2. DFÜ



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**).

11.11.3. URL

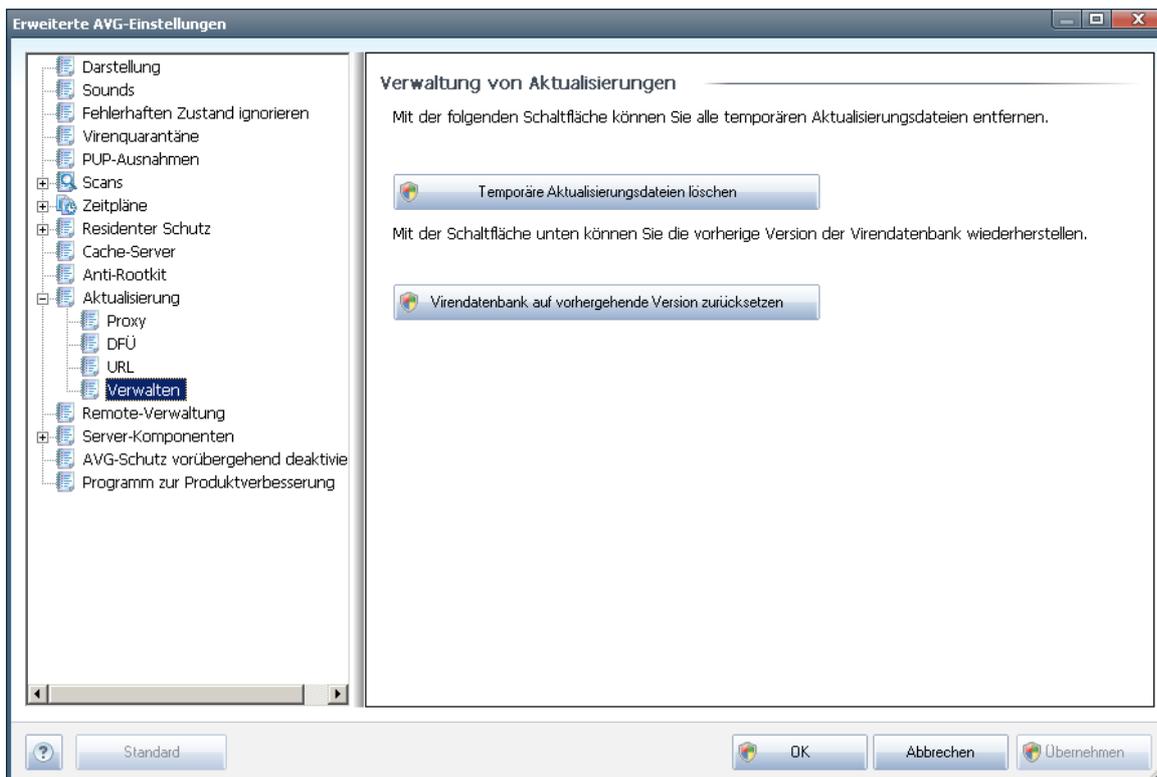


Der Dialog **URL** zeigt eine Liste von Internetadressen an, von denen Updates heruntergeladen werden können. Die Liste kann über die folgenden Schaltflächen geändert werden:

- **Hinzufügen** – Ein Dialog wird geöffnet, in dem Sie der Liste eine neue URL hinzufügen können
- **Bearbeiten** – Ein Dialog wird geöffnet, in dem Sie die Parameter der ausgewählten URL bearbeiten können
- **Löschen** – Die ausgewählte URL wird aus der Liste gelöscht
- **Nach oben** – Die ausgewählte URL wird in der Liste eine Position nach oben verschoben
- **Nach unten** – Die ausgewählte URL-Adresse wird in der Liste eine Position nach unten verschoben

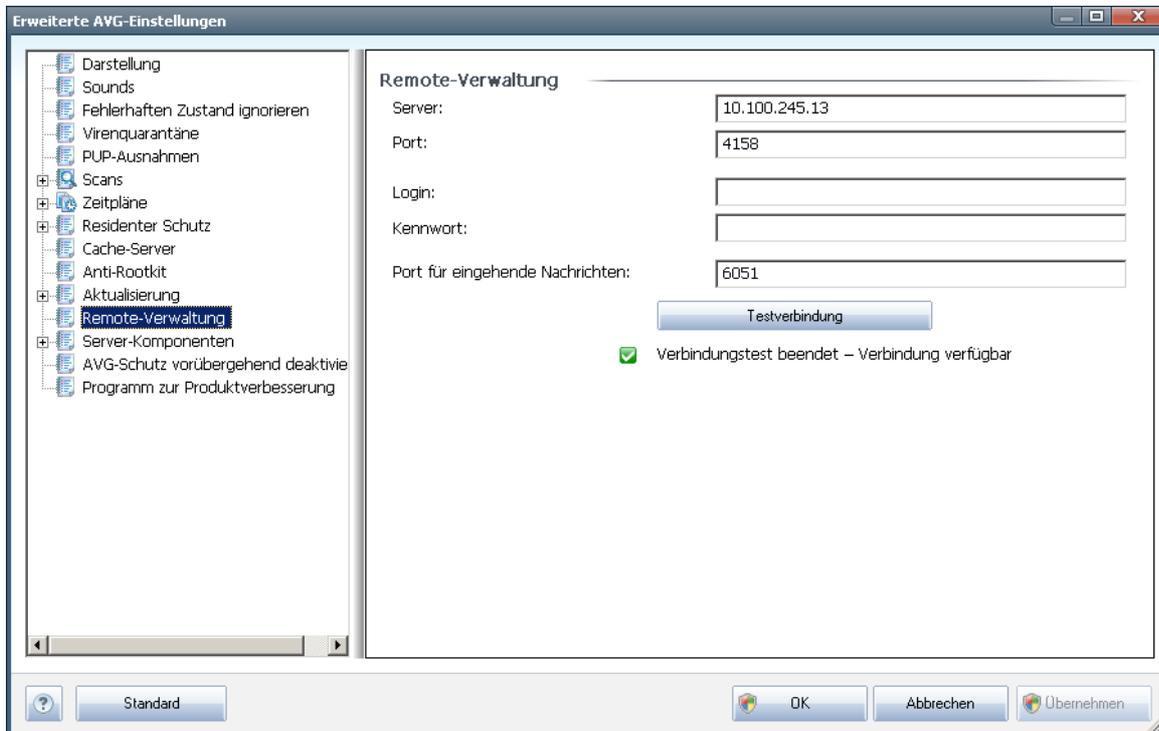
11.11.4. Verwalten

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



- **Temporäre Aktualisierungsdateien löschen** – Klicken Sie auf diese Schaltfläche, wenn Sie alle redundanten Update-Dateien von Ihrer Festplatte löschen möchten (*standardmäßig werden diese Dateien 30 Tage gespeichert*)
- **Virendatenbank auf vorhergehende Version zurücksetzen** – Klicken Sie auf diese Schaltfläche, um die letzte Version der Virendatenbank auf Ihrer Festplatte zu löschen und zur vor diesem Update gespeicherten Version zurückzukehren (*Die neue Version der Virendatenbank ist Teil des nächsten Update*)

11.12. Remote-Verwaltung



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

- **Server** – Name oder IP-Adresse des Servers, auf dem der AVG Admin-Server installiert ist
- **Port** – Geben Sie die Nummer des Ports an, über den der AVG-Client mit dem AVG Admin-Server kommuniziert (*Standard-Port ist 4158. Wenn Sie diesen Port verwenden, müssen Sie ihn gesondert angeben*)
- **Login** – Wenn die Kommunikation zwischen dem AVG-Client und dem AVG Admin-Server gesichert ist, geben Sie bitte Ihren Benutzernamen ...
- **Kennwort** – ... und Ihr Kennwort an
- **Port für eingehende Nachrichten** – Nummer des Ports, auf dem der AVG-Client vom AVG Admin-Server eingehende Nachrichten empfängt

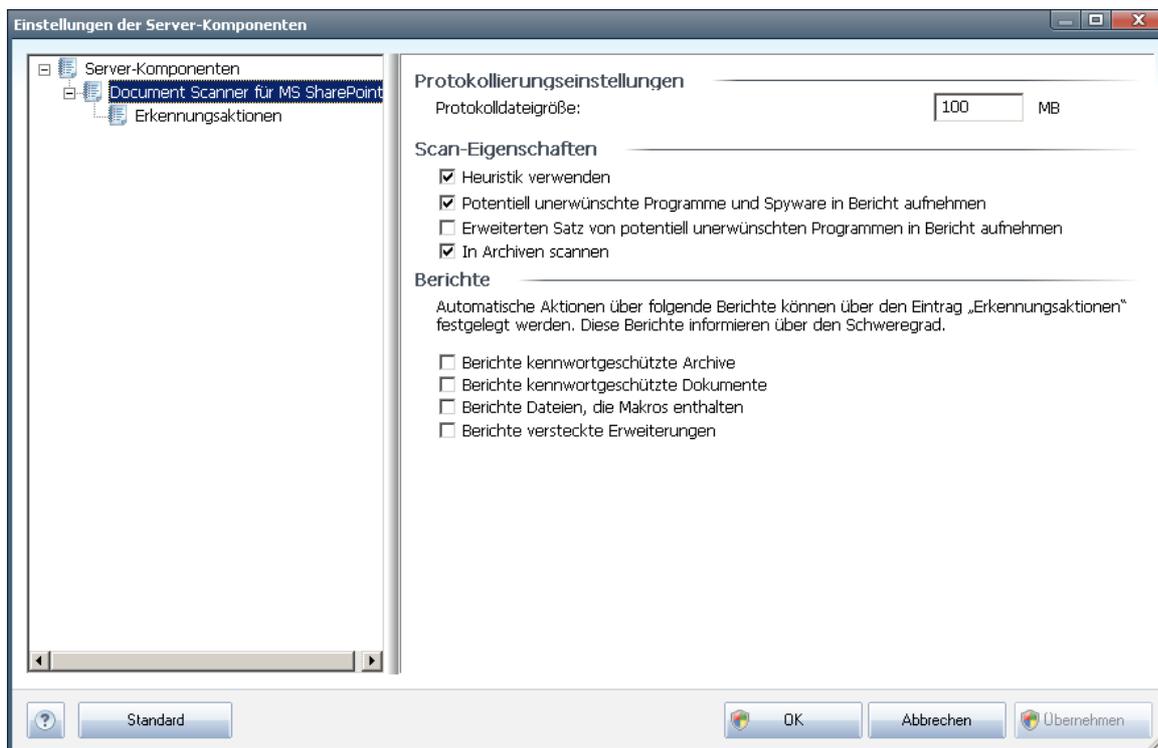
Über die Schaltfläche **Testverbindung** können Sie überprüfen, ob alle oben genannten Daten gültig sind und für eine erfolgreiche Verbindung zum DataCenter genutzt werden können.

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

11.13. Server-Komponenten

11.13.1. Document Scanner für MS SharePoint

In diesem Dialog befinden sich mehrere voreingestellte Optionen, die sich auf die Leistung von [Document Scanner für MS SharePoint](#) beziehen. Dieser Dialog ist in mehrere Bereiche gegliedert.



Protokollierungseinstellungen

Feld **Logdateigröße** – Die Logdatei protokolliert verschiedene Ereignisse, die sich auf **Document Scanner für MS SharePoint** beziehen, wie das Laden von Programmbibliotheken, Ereignisse zu gefundenen Viren, Warnungen zur Fehlerbehandlung usw. Geben Sie die maximale Größe für diese Datei in das Textfeld ein.

Scan-Eigenschaften

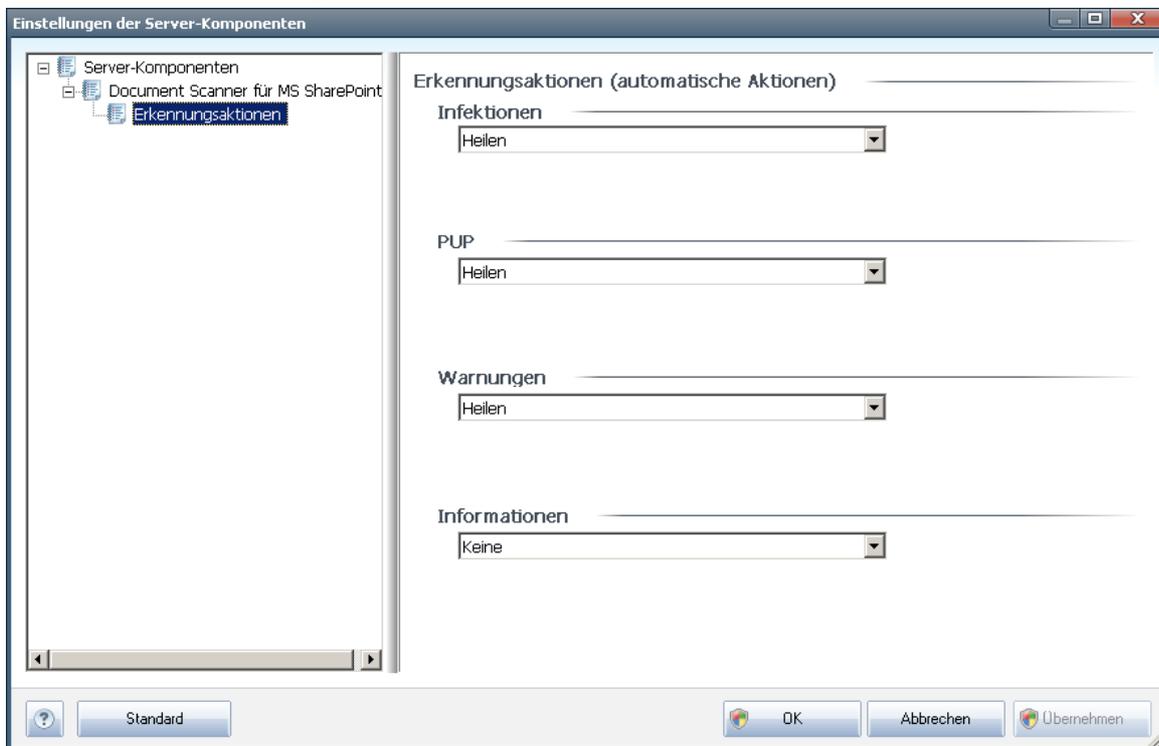
- **Heuristik verwenden** – Wenn Sie diese Option aktivieren, wird als Erkennungsmethode beim Scannen der Dokumente die Heuristik verwendet. Wenn diese Option aktiviert ist, werden Dokumente nicht nur anhand ihrer Dateierweiterungen gefiltert. Der eigentliche Inhalt des Dokuments wird ebenfalls betrachtet.

- **Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen**
– Wenn Sie diese Option aktivieren, wird die Anti-Spyware-Engine verwendet, d. h. beim Scannen der Dokumente wird nach verdächtigen und potentiell unerwünschten Programmen gesucht.
- **Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen** – Aktivieren Sie dieses Kontrollkästchen, 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, oder Programme, die in jedem Fall harmlos, jedoch nicht erwünscht sind (verschiedene Symbolleisten usw.). Dies stellt eine zusätzliche Maßnahme für mehr Komfort und eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist. Hinweise: Diese Erkennungsfunktion stellt eine Ergänzung der vorangehenden Option dar. Lassen Sie daher die vorangehende Option immer aktiviert, um einen grundlegenden Schutz vor Spyware zu gewährleisten.
- **In Archiven scannen** – Wenn Sie diese Option aktivieren, werden die Inhalte von Archiven gescannt.

Berichte

- **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.

11.13.2. Erkennungsaktionen



In diesem Dialog können Sie das Verhalten der Komponente **Document Scanner für MS SharePoint** bei der Erkennung einer Bedrohung konfigurieren. Die Bedrohungen werden in unterschiedliche Kategorien unterteilt:

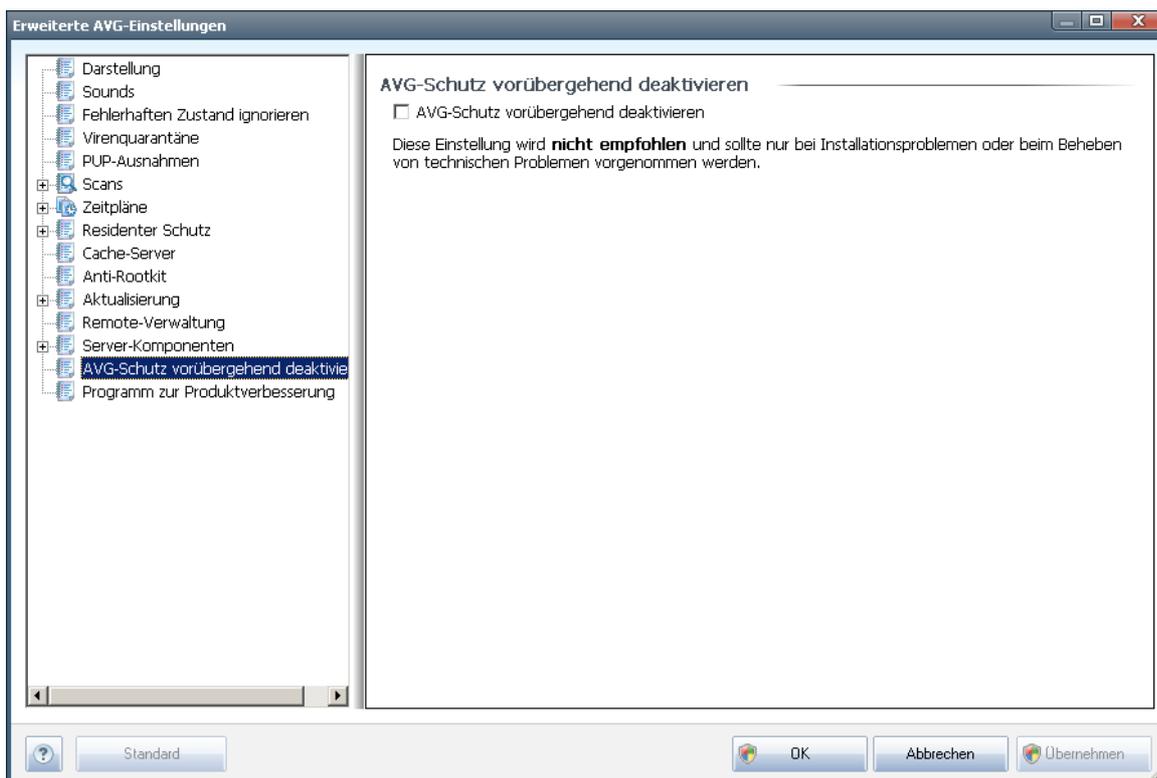
- **Infektionen** – bösartige Codes, die sich selbst kopieren und verbreiten. Sie werden oft erst bemerkt, wenn sie bereits Schaden angerichtet haben.
- **PUP (Potentiell unerwünschte Programme)** – Diese Programme variieren im Allgemeinen von tatsächlich ernsthaft bedrohlich bis nur potentiell bedrohlich für Ihre Privatsphäre.
- **Warnungen** – erkannte Objekte können nicht gescannt werden.
- **Information** – enthält alle erkannten potentiellen Bedrohungen, die keiner der oben genannten Kategorie zugeteilt werden können.

Über die Dropdown-Menüs können Sie automatische Aktionen für jede Bedrohung auswählen:

- **Keine** – Dokumente, die diese Bedrohung enthalten, bleiben unberührt.
- **Heilen** – Versucht die infizierten Dateien/Dokumente zu heilen.

- **In Quarantäne verschieben***** – Alle infizierten Dokumente werden in die Virenquarantäne verschoben.
- **Entfernen** – Mit Viren infizierte Dokumente werden gelöscht.

11.14. AVG-Schutz vorübergehend deaktivieren



Im Dialog **AVG-Schutz vorübergehend deaktivieren** können Sie alle Schutzfunktionen von **AVG File Server 2011** gleichzeitig deaktivieren.

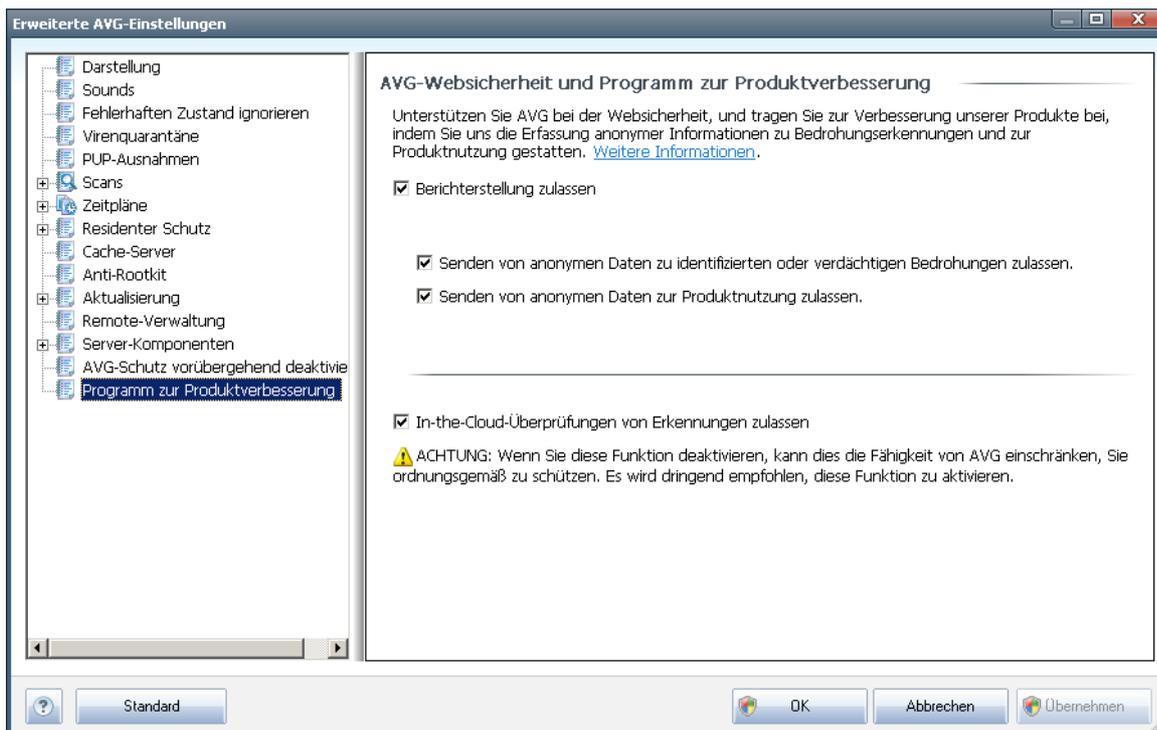
Verwenden Sie diese Option nur, wenn es unbedingt erforderlich ist.

In der Regel **müssen Sie AVG 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 müssen, um den Installationsvorgang ohne Unterbrechungen abzuschließen. Wenn Sie während der Installation jedoch ein Problem feststellen, deaktivieren Sie zunächst die Komponente **Residenter Schutz**. Wenn Sie AVG vorübergehend deaktivieren müssen, denken Sie daran, es so bald wie möglich wieder zu aktivieren. Ihr Computer ist Bedrohungen ausgesetzt, wenn Sie bei deaktivierter Virenschutz-Software mit dem Internet oder einem Netzwerk verbunden sind.

11.15. 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. Aktivieren Sie die Option **Berichterstattung zulassen**, um die Berichterstattung über erkannte Bedrohungen an AVG 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. Wir möchten Sie jedoch bitten, diese Funktion ebenfalls zu aktivieren, da sie uns hilft, 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 einflussreich, 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 anrichtet.
- **Αυξη 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.
- **Μιτ 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.

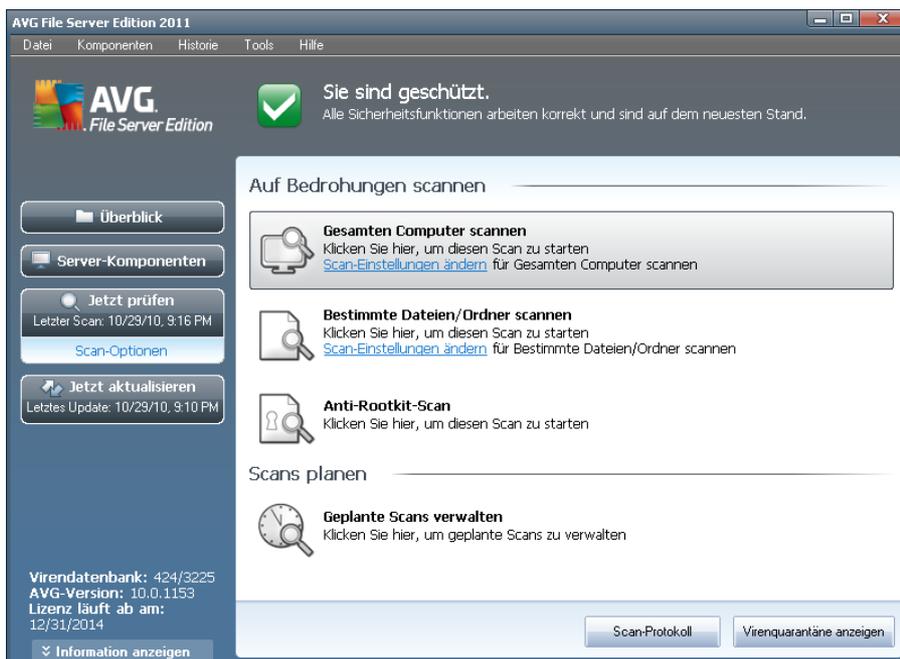
Um Sie vor diesen verschiedenen Bedrohungen zu schützen, bietet AVG folgende besonderen Komponenten:

- **Anti-Virus**, um Ihren Computer vor Viren zu schützen,
- **Anti-Spyware**, um Ihren Computer vor Spyware zu schützen.

12. AVG-Scans

Die Durchführung von Scans ist eine der wichtigsten Funktionen von **AVG File Server 2011**. Sie können Scans nach Bedarf (on-Demand) ausführen oder geplant regelmäßig [nach einem festgelegten Zeitplan](#), der Ihren Anforderungen entspricht.

12.1. Benutzeroberfläche für Scans



Auf die Benutzeroberfläche für Scans von AVG kann über den Quick Link **Computer-Scanner** [zugegriffen werden](#). Klicken Sie auf den Link, um zum Dialog **Auf Bedrohungen scannen** zu wechseln. Im Dialog finden Sie Folgendes:

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

12.2. Vordefinierte Scans

Eine der Hauptfunktionen von **AVG File Server 2011** 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.

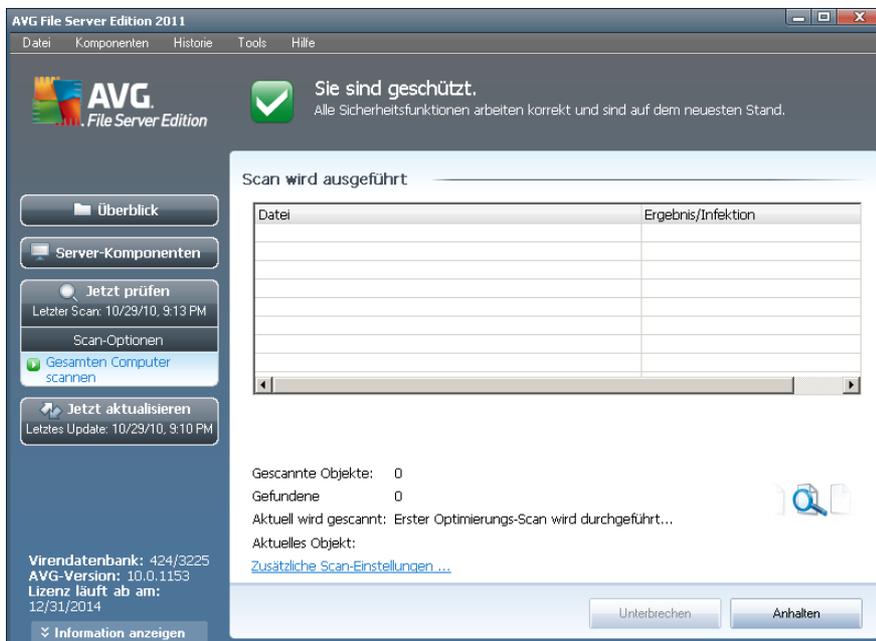
In **AVG File Server 2011** stehen die folgenden vom Software-Hersteller vordefinierten Arten von Scans zur Verfügung:

12.2.1. 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.

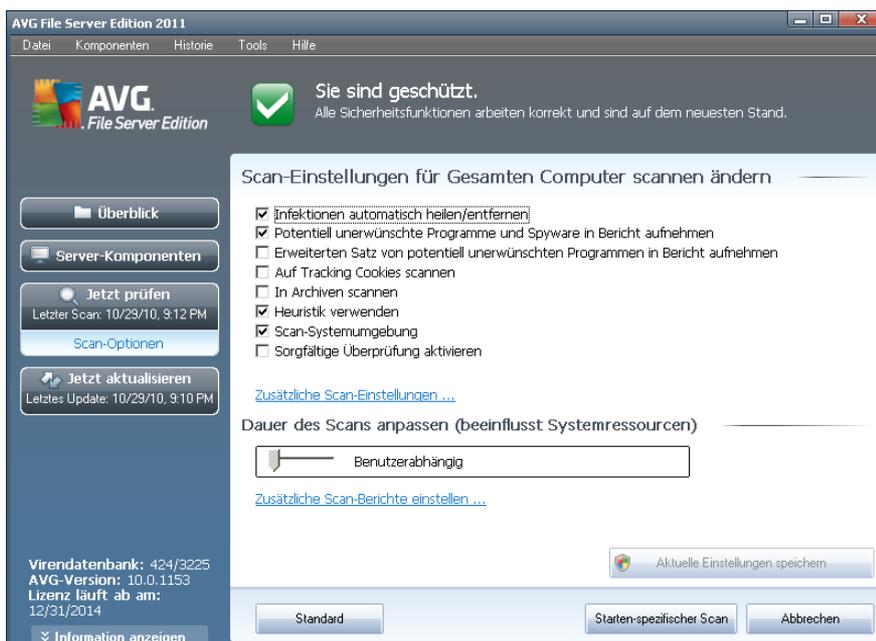
Start von Scans

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

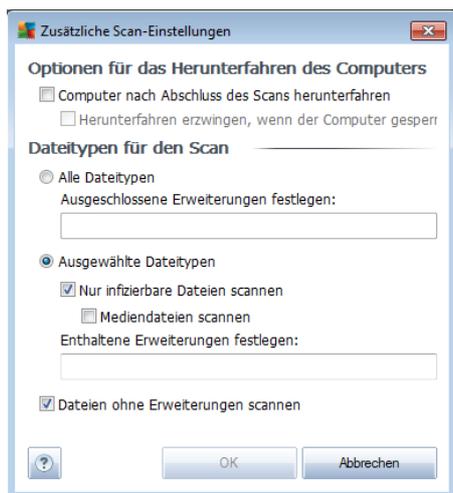
Sie können die vordefinierten Standardeinstellungen der Option **Scan des gesamten Computers** bearbeiten. Klicken Sie auf den Link **Scan-Einstellungen ändern**, um den Dialog **Scan-Einstellungen für Scan des gesamten Computers ändern** zu öffnen (Zugriff über [Benutzeroberfläche für Scans](#) über 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 festlegen** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:
 - **Alle Dateitypen** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;
 - **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 die Priorität auf *Benutzerabhängig* eingestellt, wodurch die Geschwindigkeit des Scan-Vorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).
- **Zusätzliche Scan-Berichte einstellen** – Dieser Link öffnet den Dialog **Scan-Berichte**, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:



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

12.2.2. Bestimmte Dateien/Ordner scannen

Bestimmte Dateien oder Ordner scannen – Scant 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

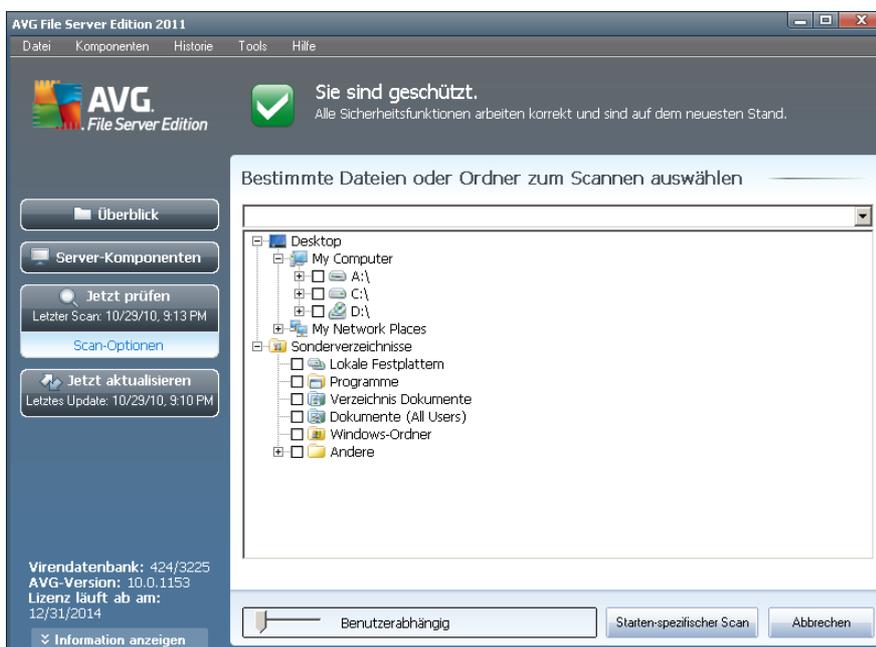
Die Option **Bestimmte Dateien/Ordner scannen** kann direkt von der [Benutzeroberfläche für Scans](#) durch Klicken auf das Symbol des Scans gestartet werden. Es öffnet sich der Dialog **Bestimmte Dateien oder Ordner zum Scannen auswählen**. Wählen Sie in der Baumstruktur Ihres Computers den zu scannenden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



Textfeld im oberen Bereich dieses Dialogs angezeigt.

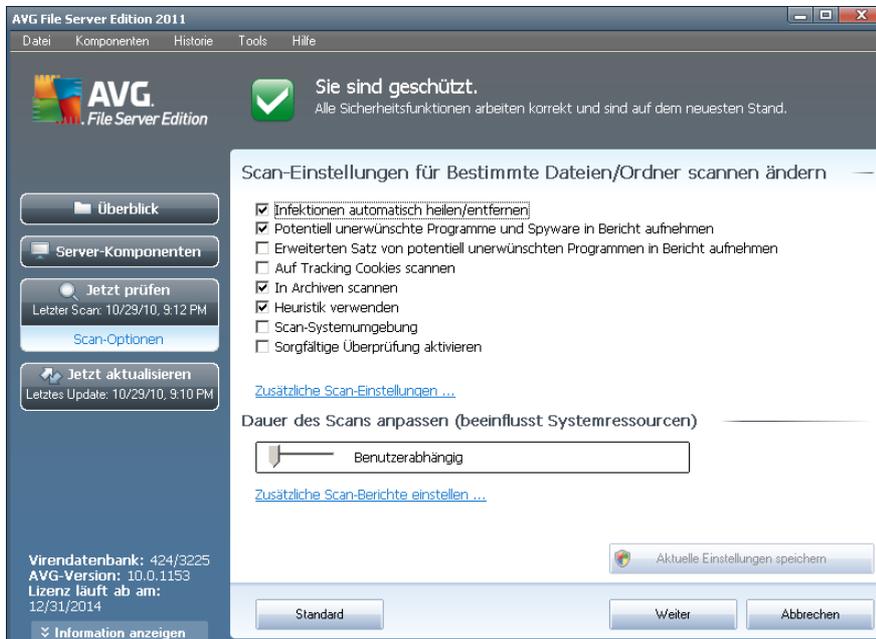
Es ist möglich, einen bestimmten Ordner zu scannen, jedoch seine Unterordner vom Scan auszuschließen. Setzen Sie dafür ein Minuszeichen „-“ vor den automatisch generierten Pfad (*siehe Screenshot*). Um den gesamten Ordner vom Scan auszuschließen, verwenden Sie das Ausrufezeichen „!“ parameter.

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

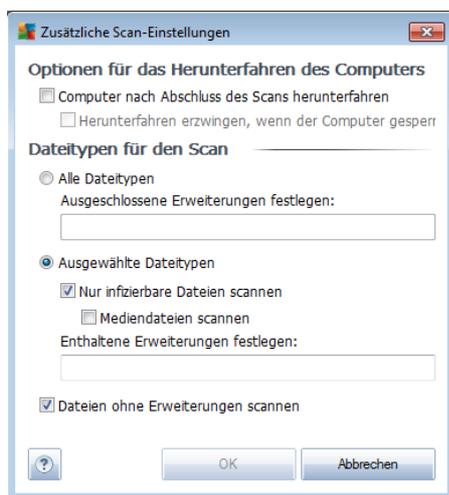
Sie können die vordefinierten Standardeinstellungen der Option **Bestimmte Dateien oder Ordner scannen** bearbeiten. Klicken Sie auf den Link **Scan-Einstellungen ändern**, um den Dialog **Scan-Einstellungen für Bestimmte Dateien/Ordner scannen ändern** zu öffnen. **Es empfiehlt sich, die Standardeinstellungen 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 festlegen** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:
 - **Alle Dateitypen** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;
 - **Ausgewählte Dateitypen** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.
 - Auf Wunsch können Sie auch **Dateien ohne Erweiterungen scannen** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.
- **Priorität des Scan-Vorgangs** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die Stufe *Benutzerabhängig* eingestellt, wodurch die Geschwindigkeit des Scan-Vorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).
- **Zusätzliche Scan-Berichte einstellen** – Dieser Link öffnet den Dialog **Scan-Berichte**, wo Sie wählen können, welche Scan-Ergebnisse berichtet werden sollen:



Warnung: Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel [AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen](#) beschrieben. Wenn Sie die Standardkonfiguration der Option **Bestimmte Dateien oder Ordner scannen** ändern, können Sie Ihre neuen Einstellungen als Standardkonfiguration speichern, die für alle



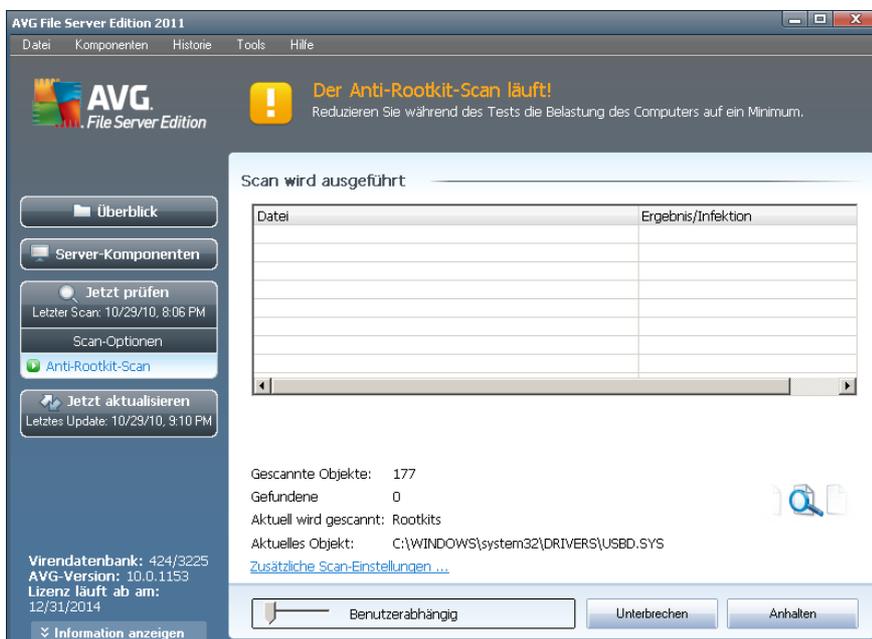
weiteren Scans bestimmter Dateien oder Ordner verwendet wird. Diese Konfiguration wird auch als Vorlage für alle Ihre neuen geplanten Scans verwendet ([alle benutzerdefinierten Scans basieren auf der aktuellen Konfiguration des Scans bestimmter Dateien oder Ordner](#)).

12.2.3. 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

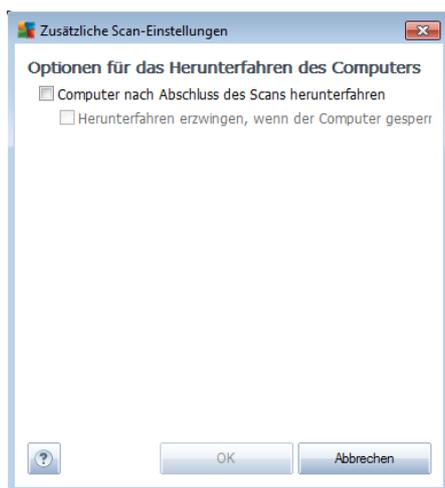
Anti-Rootkit-Scan können Sie direkt über die [Benutzeroberfläche für Scans](#) starten, indem Sie auf das Scan-Symbol klicken. Für diesen Scan-Typ müssen keine weiteren Einstellungen vorgenommen werden. Der Scan startet sofort im Dialog **Scan wird ausgeführt** (siehe Screenshot). Der Scanvorgang kann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



Bearbeitung der Scan-Konfiguration

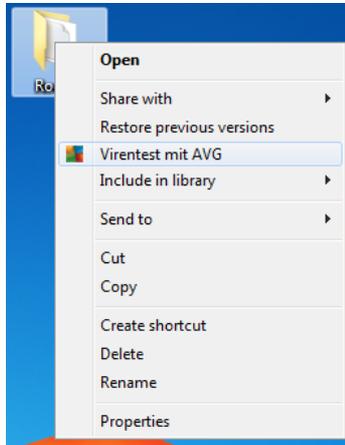
Anti-Rootkit-Scan wird stets mit den Standardeinstellungen gestartet; die Scanparameter können nur im Dialog [Erweiterte Einstellungen von AVG/Anti-Rootkit](#) bearbeitet werden. Auf der Scan-Oberfläche steht während der Ausführung eines Scans die folgende Konfiguration zur Verfügung:

- **Automatischer Scan** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist die Priorität auf die mittlere Stufe eingestellt (*Automatischer Scan*), wodurch die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert werden. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).
- **Zusätzliche Scan-Einstellungen** – Mit diesem Link lässt sich der Dialog **Zusätzliche Scan-Einstellungen** öffnen, in dem Sie mögliche Bedingungen für ein Herunterfahren des Computers im Hinblick auf den **Anti-Rootkit-Scan** festlegen können (**Computer nach Abschluss des Scans herunterfahren, möglicherweise Herunterfahren erzwingen, wenn der Computer gesperrt ist**):



12.3. Scans aus dem Windows Explorer

Neben den vordefinierten Scans, die für den gesamten Computer oder ausgewählte Bereiche gestartet werden, umfasst **AVG File Server 2011** auch eine Option für die Schnellprüfung eines bestimmten Objekts direkt in Windows Explorer. Wenn Sie eine unbekannte Datei öffnen und ihren Inhalt nicht genau kennen, möchten Sie sie möglicherweise On-Demand überprüfen. Gehen Sie dazu wie folgt vor:



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

12.4. Scannen von Befehlszeilen

Mit **AVG File Server 2011** 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.

12.4.1. 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** aufnehmen „[Potentiell unerwünschte Programme](#)“ in Bericht
- **/REG** Registry scannen
- **/COO** Cookies scannen
- **/?** Hilfe zu diesem Thema anzeigen
- **/HELP** Hilfe zu diesem Thema anzeigen
- **/PRIORITY** Scan-Priorität einstellen /Niedrig, Auto, 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

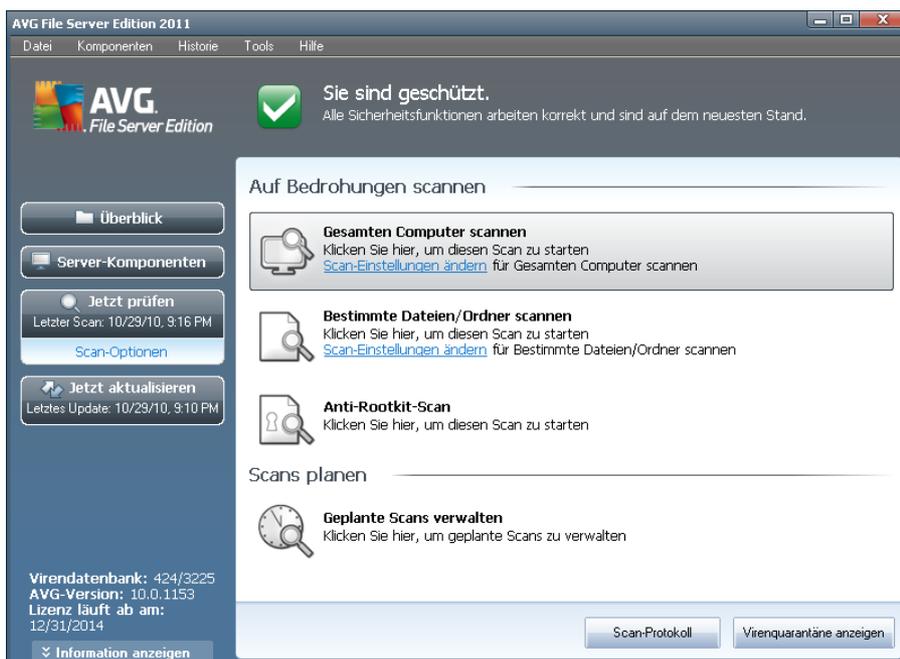


12.5. Scans planen

Mit **AVG File Server 2011** 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.

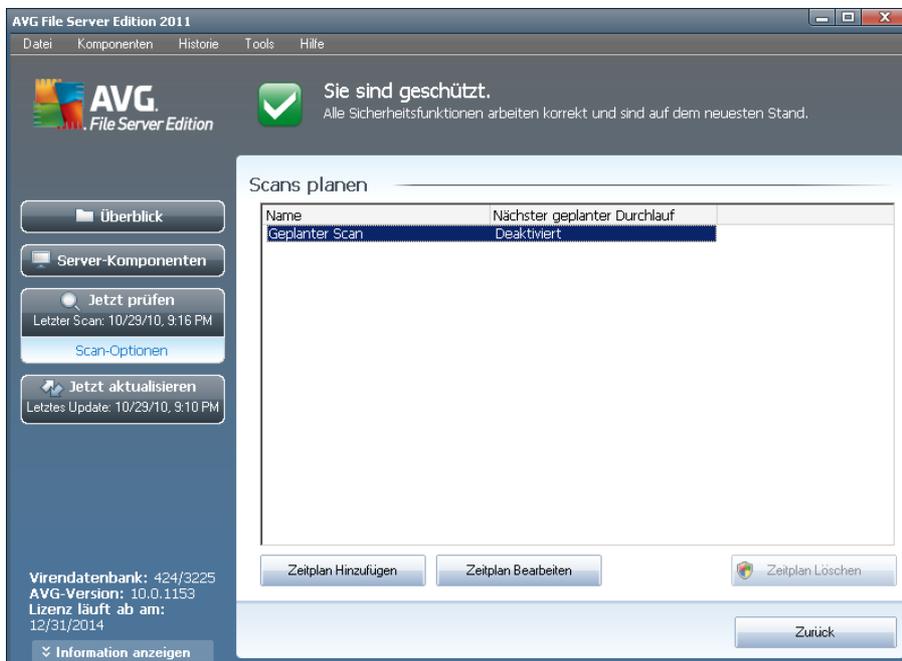
Sie sollten die Funktion [Scan des gesamten Computers](#) regelmäßig, mindestens einmal pro Woche, starten. Wenn möglich, sollten Sie Ihren gesamten Computer täglich scannen. Dies ist auch die Standardkonfiguration für geplante Scans. Wenn der Computer immer eingeschaltet ist, können Sie die Scans für 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 Scan-Pläne zu erstellen, gehen Sie auf der [Scan-Oberfläche von AVG](#) unten zum Abschnitt **Scans planen**:



Scans planen

Klicken Sie im Bereich **Scans planen** auf das grafische Symbol, um den Dialog **Scans planen** zu öffnen, in dem eine Liste aller gegenwärtig geplanten Scans angezeigt wird:



Sie können Scans mithilfe der folgenden Schaltflächen bearbeiten oder hinzufügen:

- **Zeitplan Hinzufügen** – Mit dieser Schaltfläche wird der Dialog **Einstellungen für geplanten Scan** auf dem Reiter **Einstellungen für den Zeitplan** geöffnet. In diesem Dialog können Sie die Parameter für den neu definierten Scan festlegen.
- **Zeitplan Bearbeiten** – Diese Schaltfläche steht nur zur Verfügung, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. In diesem Fall ist die Schaltfläche aktiv, und Sie können darauf klicken, um zum Dialog **Einstellungen für geplanten Scan** auf dem Reiter **Einstellungen für den Zeitplan** zu wechseln. Hier sind bereits Parameter des ausgewählten Scans festgelegt und können bearbeitet werden.
- **Zeitplan Löschen** – Diese Schaltfläche ist ebenfalls nur aktiv, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. Dieser Scan wird durch Klicken auf die Schaltfläche aus der Liste gelöscht. Sie können jedoch nur Ihre eigenen Scans entfernen. Der **Zeitplan für Scans des gesamten Computers**, der in den Standardeinstellungen vordefiniert ist, kann nicht gelöscht werden.
- **Zurück** – Zurück zur [Scan-Oberfläche von AVG](#)

12.5.1. 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



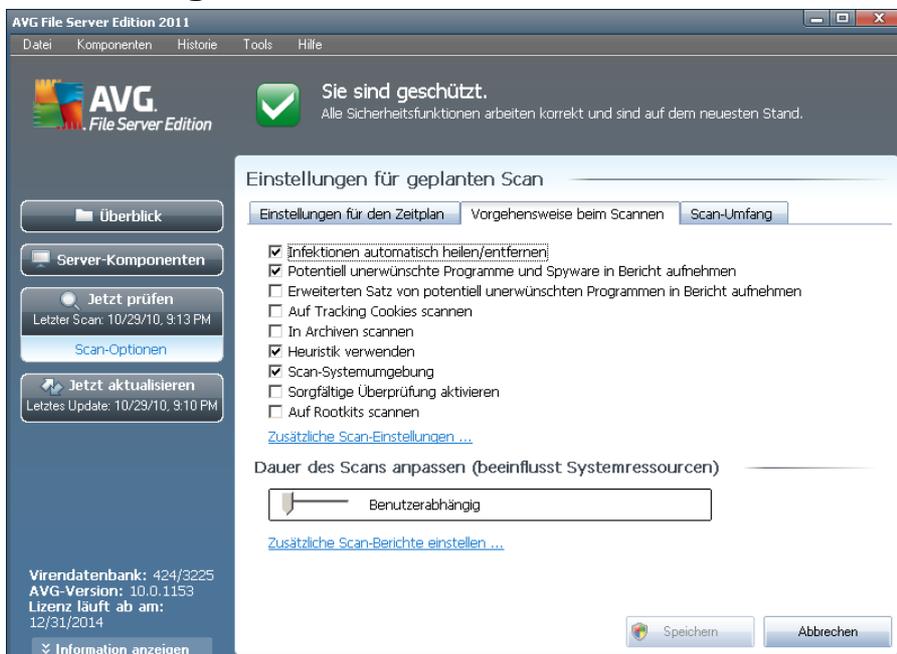
welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmmodus befindet oder vollständig ausgeschaltet ist.

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 dieselbe Funktion haben:

- **Übernehmen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#). Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.
- **Abbrechen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#).

12.5.2. Vorgehensweise beim Scannen

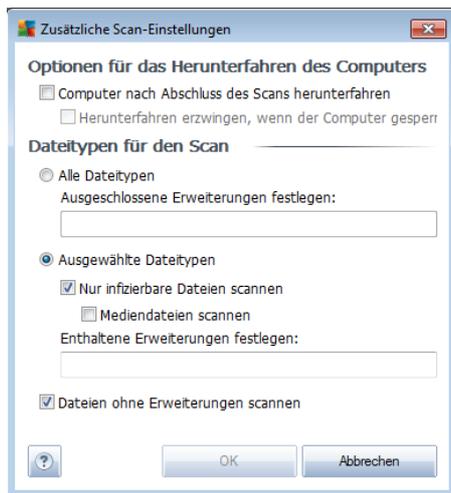


Der Reiter **Vorgehensweise beim Scannen** enthält eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. Standardmäßig sind die meisten Parameter aktiviert und ihre Funktionen werden während des Scans angewandt. Wenn Sie keinen wichtigen Grund haben, diese Einstellungen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

Anschließend können Sie die Scan-Konfiguration wie folgt ändern:

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



- **Optionen für das Herunterfahren des Computers** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (**Computer nach Abschluss des Scans herunterfahren**) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (**Herunterfahren erzwingen, wenn der Computer gesperrt ist**).
- **Dateitypen für den Scan festlegen** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:
 - **Alle Dateitypen** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Komma 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. Auf der mittleren Stufe wird die Geschwindigkeit des Scanvorgangs und die Systemressourcenbelastung optimiert. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (z. B. *wenn am Computer zeitweise nicht gearbeitet wird*).
- **Zusätzliche Scan-Berichte einstellen** – Dieser Link öffnet den Dialog **Scan-Berichte**, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:



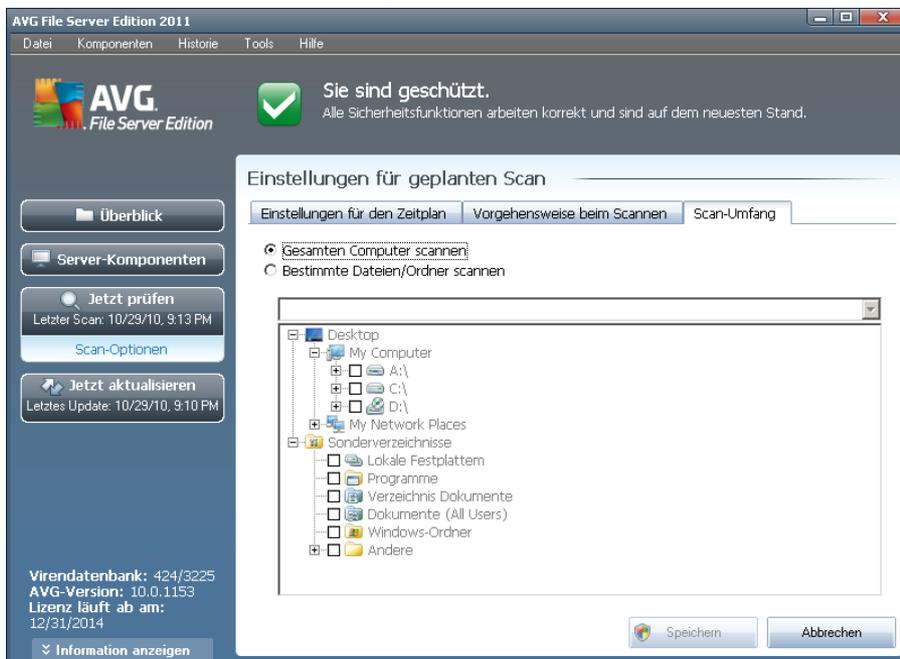
Hinweis: Standardmäßig ist die Scan-Konfiguration so eingestellt, dass eine optimale Leistung erzielt wird. Wenn Sie keinen wichtigen Grund haben, die Scan-Einstellungen zu ändern, wird dringend empfohlen, die vordefinierte Konfiguration beizubehalten. Änderungen an der Konfiguration sollten nur von erfahrenen Benutzern durchgeführt werden. Weitere Optionen für die Scan-Konfiguration finden Sie im Dialog **Erweiterte Einstellungen**, den Sie über das Systemmenü mit **Tools/ Erweiterte Einstellungen** aufrufen können.

Schaltflächen

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

- **Übernehmen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#). Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.
- **Abbrechen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#).

12.5.3. 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**

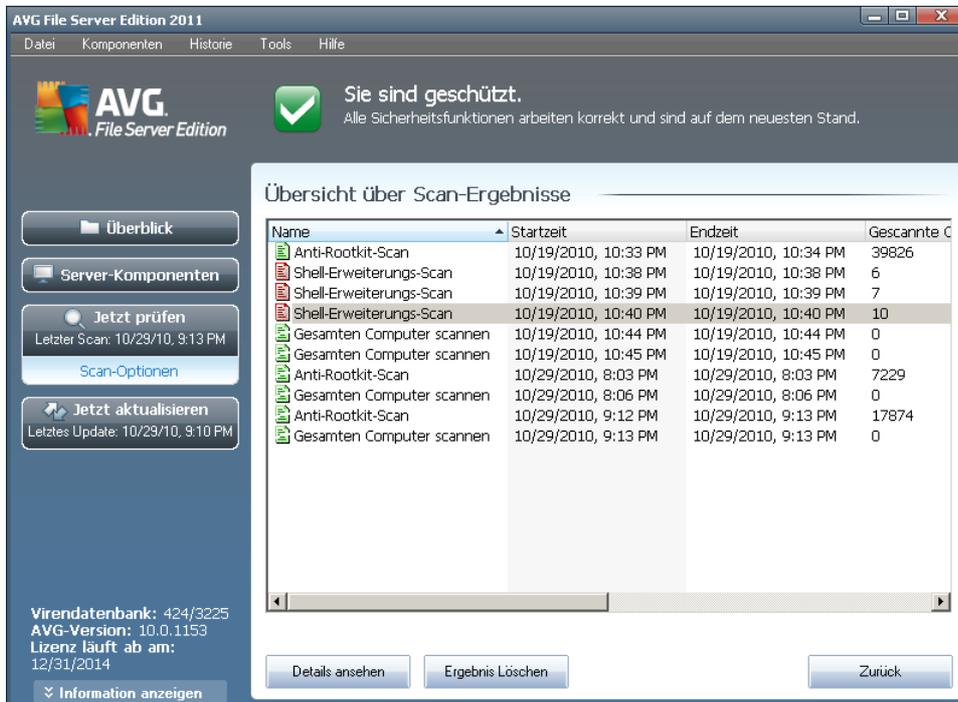
- *Systemlaufwerk* – die Festplatte, auf der das Betriebssystem installiert ist (normalerweise C:)
- *Systemordner* – C:\Windows\System32\
- *Ordner „Temporäre Dateien“* – C:\Dokumente und Einstellungen\Benutzer\Lokal (*Windows XP* oder C:\Benutzer\"Benutzername"\AppData\Local\Temp *Windows Vista/7*)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

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 dieselbe Funktion haben:

- **Übernehmen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#). Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.
- **Abbrechen** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum [Standarddialog der Scan-Oberfläche von AVG](#).

12.6. Übersicht über Scan-Ergebnisse



AVG File Server Edition 2011

Sie sind geschützt.
Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

Übersicht über Scan-Ergebnisse

Name	Startzeit	Endzeit	Gescannte C
 Anti-Rootkit-Scan	10/19/2010, 10:33 PM	10/19/2010, 10:34 PM	39826
 Shell-Erweiterungs-Scan	10/19/2010, 10:38 PM	10/19/2010, 10:38 PM	6
 Shell-Erweiterungs-Scan	10/19/2010, 10:39 PM	10/19/2010, 10:39 PM	7
 Shell-Erweiterungs-Scan	10/19/2010, 10:40 PM	10/19/2010, 10:40 PM	10
 Gesamt Computer scannen	10/19/2010, 10:44 PM	10/19/2010, 10:44 PM	0
 Gesamt Computer scannen	10/19/2010, 10:45 PM	10/19/2010, 10:45 PM	0
 Anti-Rootkit-Scan	10/29/2010, 8:03 PM	10/29/2010, 8:03 PM	7229
 Gesamt Computer scannen	10/29/2010, 8:06 PM	10/29/2010, 8:06 PM	0
 Anti-Rootkit-Scan	10/29/2010, 9:12 PM	10/29/2010, 9:13 PM	17874
 Gesamt Computer scannen	10/29/2010, 9:13 PM	10/29/2010, 9:13 PM	0

Details ansehen Ergebnis Löschen Zurück

Virendatenbank: 424/3225
AVG-Version: 10.0.1153
Lizenz läuft ab am:
12/31/2014

Der Dialog **Übersicht über Scan-Ergebnisse** ist über die [Scan-Oberfläche von AVG](#) über die Schaltfläche **Scan-Ergebnisse** verfügbar. Im Dialog wird eine Liste aller vorher gestarteten Scans und Informationen zu deren Ergebnissen angezeigt:

- **Name** – Scan-Ziel. Dabei kann es sich entweder um den Namen eines [vordefinierten Scans](#) oder um einen Namen handeln, den Sie Ihrem [eigenen geplanten Scan](#) gegeben haben. Jeder Name enthält ein Symbol, das das Scan-Ergebnis anzeigt:

 – Ein grünes Symbol zeigt an, dass beim Scan keine Infektion gefunden wurde

 – Ein blaues Symbol zeigt an, dass beim Scan eine Infektion gefunden, das infizierte Objekt jedoch automatisch entfernt wurde

 – Ein rotes Symbol zeigt an, dass beim Scan eine Infektion gefunden wurde, die nicht entfernt werden konnte!

Jedes Symbol kann entweder ganz oder halb angezeigt werden. Ein vollständig angezeigtes Symbol zeigt an, dass ein Scan vollständig abgeschlossen und korrekt beendet wurde. Ein unvollständig angezeigtes Symbol zeigt an, dass der Scan unterbrochen oder abgebrochen wurde.

Hinweis: Genauere Informationen zu jedem Scan finden Sie im Dialog [Scan-Ergebnisse](#), auf den Sie über die Schaltfläche **Details ansehen**

(im unteren Teil des Dialogs) zugreifen können.

- **Startzeit** – Datum und Uhrzeit des gestarteten Scans
- **Endzeit** – Datum und Uhrzeit des Scan-Endes
- **Gescannte Objekte** – Anzahl der gescannten Objekte
- **Infektionen** – Anzahl der erkannten/entfernten Vireninfectionen
- **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

12.7. 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 Vireninfection 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).

12.7.1. Reiter „Ergebnisübersicht“

AVG File Server Edition 2011

AVG File Server Edition

Sie sind geschützt.
Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

Scan-Ergebnisse

Ergebnisübersicht | Infektionen | Spyware

Scan "Shell-Erweiterungs-Scan" wurde beendet.

	Gefunden	Entfernt und bereinigt	Nicht entfernt oder geheilt
Infektionen	3	0	3
Spyware	2	0	2

Für den Scanvorgang ausgewählte C:\Documents and Settings\Administrator\Desktop\Adware;C:\

Start des Scans: Tuesday, October 19, 2010, 10:40:56 PM
Scan beendet: Tuesday, October 19, 2010, 10:40:58 PM (1 Sekunde(n))
Gesamtanzahl gescannter 10
Benutzer, der den Scan gestartet Administrator
[Übersicht in Datei exportieren ...](#)

Virendatenbank: 424/3225
AVG-Version: 10.0.1153
Lizenz läuft ab am: 12/31/2014

Information anzeigen

Der Scan ist abgeschlossen.

Alle nicht geheilt entfernen

Zurück

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

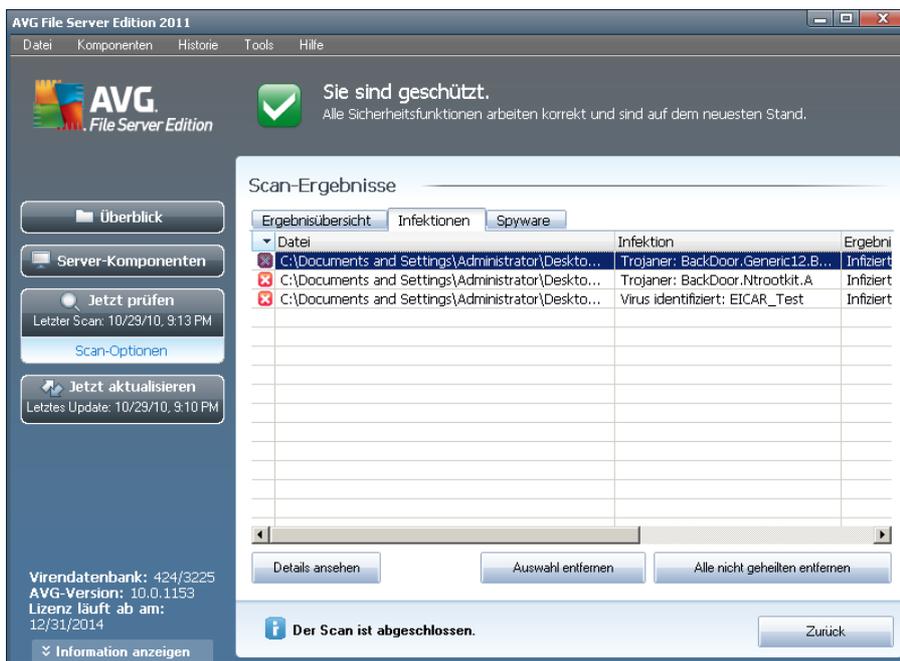
- Erkannte [Vireninfectionen](#) / [Spyware](#)
- Entfernte [Vireninfectionen](#) / [Spyware](#)
- Anzahl der [Vireninfectionen](#) / [Spyware](#), die nicht entfernt oder geheilt werden konnte

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.

12.7.2. 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:

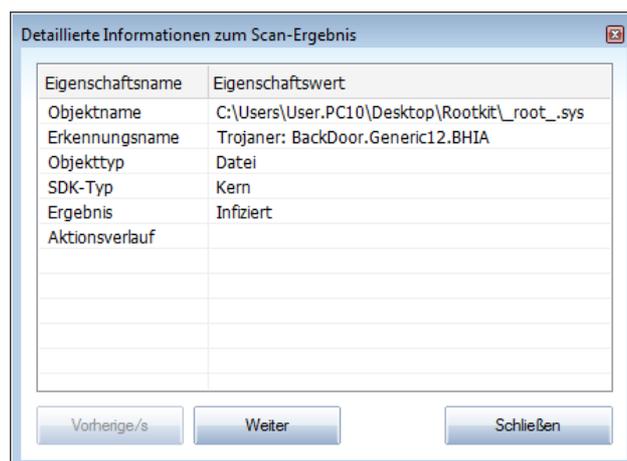
- **Datei** – Der vollständige Pfad zum ursprünglichen Standort des infizierten Objekts
- **Infektion** – Name des erkannten [Virus](#) (*genauere Informationen zu bestimmten Viren finden Sie online in der [Virenenzyklopädie](#)*)
- **Ergebnis** – Hier wird der aktuelle Status des beim Scan erkannten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

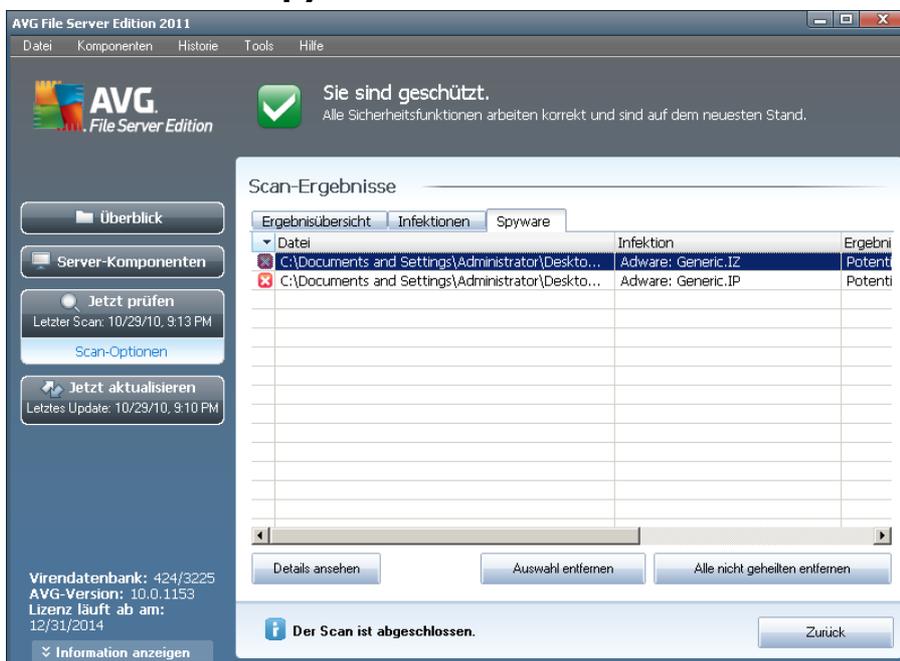
- **Details ansehen** – Diese Schaltfläche öffnet einen neuen Dialog **Detaillierte Objektinformationen**:



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](#)

12.7.3. Reiter „Spyware“



AVG File Server Edition 2011

AVG File Server Edition

Sie sind geschützt.
Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

Scan-Ergebnisse

Ergebnisübersicht | Infektionen | **Spyware**

Datei	Infektion	Ergebnis
C:\Documents and Settings\Administrator\Desktop\...	Adware: Generic.IZ	Potenti
C:\Documents and Settings\Administrator\Desktop\...	Adware: Generic.IP	Potenti

Details ansehen | Auswahl entfernen | Alle nicht geheilten entfernen

Der Scan ist abgeschlossen. Zurück

Virendatenbank: 424/3225
AVG-Version: 10.0.1153
Lizenz läuft ab am: 12/31/2014

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 [Virenzyklopädie](#) 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

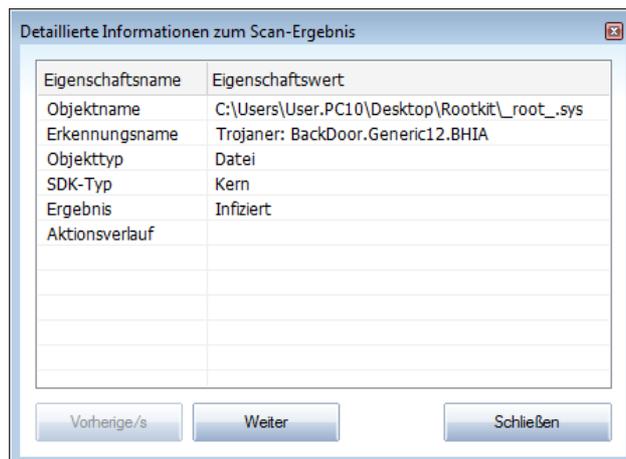
ursprünglichen Ort belassen

- **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](#)

12.7.4. Reiter „Warnungen“

Auf dem Reiter **Warnungen** werden Informationen zu „verdächtigen“ Objekten (*normalerweise Dateien*) angezeigt, die beim Scan erkannt wurden. Wenn diese Dateien von [Residenter Schutz](#) erkannt werden, wird der Zugriff auf diese Dateien blockiert. Typische Funde dieser Art sind beispielsweise folgende: Versteckte Dateien, Cookies, verdächtige Registrierungsschlüssel, kennwortgeschützte Dokumente oder Archive usw. Diese Dateien stellen keine direkte Bedrohung für Ihren Computer oder Sicherheit dar. Informationen zu diesen Dateien können bei der Erkennung von Adware oder Spyware auf Ihrem Computer nützlich sein. Wenn diese Warnungen nur nach einem AVG-Scan ausgegeben werden, ist keine Aktion nötig.

Dies ist eine kurze Beschreibung der bekanntesten Beispiele solcher Objekte:

- **Versteckte Dateien** – Versteckte Dateien sind in Windows standardmäßig nicht sichtbar, und bestimmte Viren oder andere Bedrohungen können versuchen, der Erkennung durch das Speichern ihrer Dateien mit diesem Attribut zu umgehen. Wenn Ihr AVG eine versteckte Datei meldet, die verseucht sein könnte, können Sie diese in die [AVG Virenquarantäne](#) verschieben.
- **Cookies** – Cookies sind reine Textdateien, die von Webseiten dazu verwendet werden, benutzerbezogene Informationen zu speichern. Diese Informationen werden später verwendet, um benutzerdefinierte Layouts von Websites zu laden, Benutzernamen einzutragen usw.
- **Verdächtige Registrierungsschlüssel** – Manche Malware speichert Informationen in der Windows-Registrierung, um sicherzustellen, dass sie beim Hochfahren geladen wird oder um ihre Auswirkung auf das Betriebssystem zu erweitern.

12.7.5. 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](#).

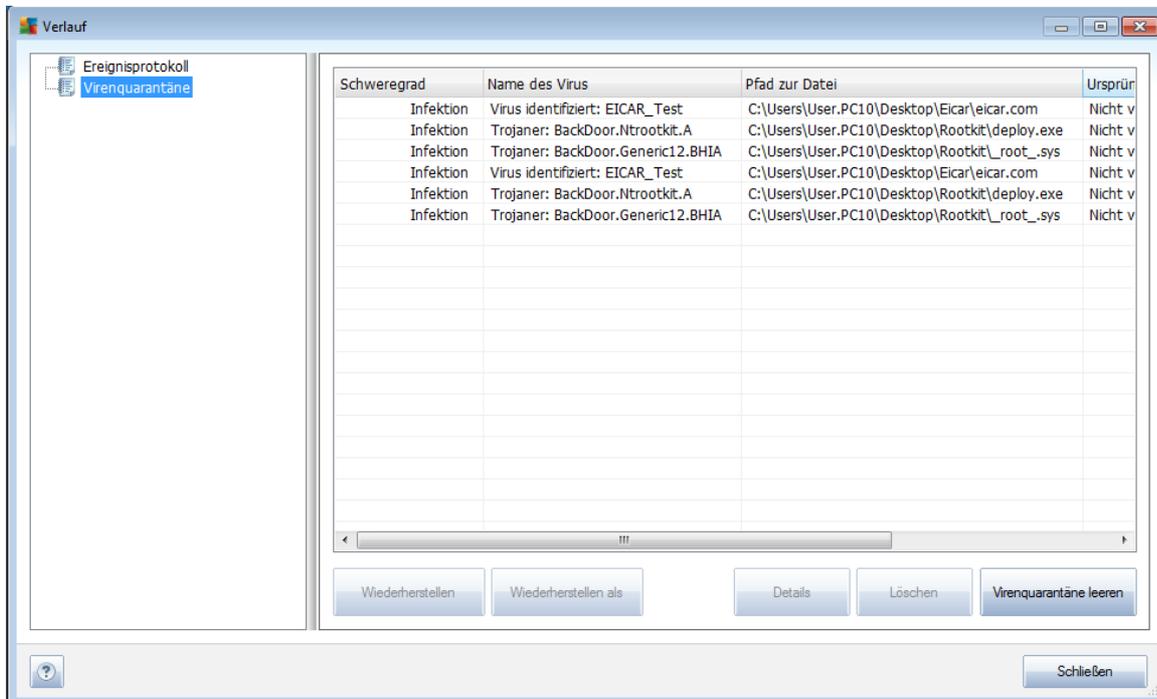
12.7.6. Reiter „Informationen“

Der Reiter **Informationen** enthält Daten über „Funde“, die nicht als Infektionen, Spyware usw. eingestuft werden können. Sie können nicht eindeutig als gefährlich klassifiziert werden, müssen jedoch trotzdem beachtet werden. AVG-Scan kann Dateien erkennen, die möglicherweise nicht infiziert, aber verdächtig sind. Diese Dateien werden entweder als [Warnung](#) oder als **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 eingeschickt werden.
- **Kennwortgeschützte Dokumente oder Archive** – Kennwortgeschützte Dateien können von AVG (*bzw. anderen Anti-Malware-Programmen*) nicht gescannt werden.
- **Dokument mit Makros** – Das gemeldete Dokument enthält Makros, die möglicherweise schädlich sind.
- **Versteckte Erweiterung** – Dateien mit versteckten Erweiterungen können beispielsweise wie Bilder aussehen, sind jedoch in Wahrheit ausführbare Dateien (*z. B. bild.jpg.exe*). Die zweite Erweiterung ist standardmäßig in Windows nicht sichtbar. AVG berichtet solche Dateien, um ein versehentliches Öffnen dieser Dateien zu verhindern.
- **Falscher Dateipfad** – Wenn eine wichtige Systemdatei nicht vom Standardpfad ausgeführt wird (*winlogon.exe wird z. B. nicht aus dem Windows-Ordner ausgeführt*), meldet AVG diese Unstimmigkeit. In einigen Fällen verwenden Viren die Namen von Standardsystemprozessen, damit ihr Vorhandensein im System weniger auffällt.
- **Gesperrte Datei** – Die gemeldete Datei ist gesperrt und kann von AVG nicht gescannt werden. Das bedeutet üblicherweise, dass diese Datei dauerhaft vom System verwendet wird (*z. B. Auslagerungsdateien*).

12.8. Virenquarantäne



Schweregrad	Name des Virus	Pfad zur Datei	Ursprünglicher Objektname
Infektion	Virus identifiziert: EICAR_Test	C:\Users\User.PC10\Desktop\Eicar\eicar.com	Nicht v
Infektion	Trojaner: BackDoor.Ntrootkit.A	C:\Users\User.PC10\Desktop\Rootkit\deploy.exe	Nicht v
Infektion	Trojaner: BackDoor.Generic12.BHIA	C:\Users\User.PC10\Desktop\Rootkit_root_sys	Nicht v
Infektion	Virus identifiziert: EICAR_Test	C:\Users\User.PC10\Desktop\Eicar\eicar.com	Nicht v
Infektion	Trojaner: BackDoor.Ntrootkit.A	C:\Users\User.PC10\Desktop\Rootkit\deploy.exe	Nicht v
Infektion	Trojaner: BackDoor.Generic12.BHIA	C:\Users\User.PC10\Desktop\Rootkit_root_sys	Nicht v

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** – Legt die Infektionsart fest (*basierend auf ihrer Infektionsstufe – alle aufgeführten Objekte können tatsächlich oder potentiell infiziert sein*).
- **Name des Virus** – Der Name der erkannten Infektion wird entsprechend der [Virenzyklopädie](#) (online) angegeben
- **Pfad zur Datei** – Der vollständige Pfad zum ursprünglichen Standort der infizierten Datei
- **Ursprünglicher Objektname** – Alle hier aufgelisteten Objekte wurden von AVG während des Scanvorgangs mit dem Standardnamen gekennzeichnet. Wenn das Objekt einen bekannten ursprünglichen Namen hat (z. B. *der Name eines*



eMail-Anhangs, der nicht mit dem eigentlichen Inhalt des Anhangs übereinstimmt), wird der Name in dieser Spalte angegeben.

- **Speicherdatum** – Datum und Uhrzeit, zu dem die verdächtige Datei erkannt und in die **Virenquarantäne verschoben wurde**

Schaltflächen

Auf der Oberfläche der **Virenquarantäne** stehen folgende Schaltflächen zur Verfügung:

- **Wiederherstellen** – Die infizierte Datei wird zurück zu ihrem ursprünglichen Standort auf Ihrer Festplatte verschoben
- **Wiederherstellen als** – Wenn Sie das erkannte infizierte Objekt aus der **Virenquarantäne** in einen ausgewählten Ordner verschieben möchten, klicken Sie auf diese Schaltfläche, und das verdächtige und erkannte Objekt wird mit seinem ursprünglichen Namen gespeichert. Wenn der ursprüngliche Name nicht bekannt ist, wird stattdessen der Standardname verwendet.
- **Löschen** – Die infizierte Datei wird vollständig 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*).



13. AVG Updates

Die regelmäßige Aktualisierung von AVG ist entscheidend, damit alle neu entdeckten Viren so früh wie möglich erkannt werden.

Da AVG-Updates nicht nach einem festen Zeitplan, sondern entsprechend der Anzahl und des Schweregrads neuer Bedrohungen zur Verfügung gestellt werden, wird empfohlen, mindestens einmal täglich (oder bei Bedarf sogar öfter) eine Prüfung auf neue Updates durchzuführen. Dadurch können Sie sicherstellen, dass Ihr **AVG File Server 2011** auch tagsüber auf dem aktuellsten Stand ist.

13.1. Updatestufen

Sie können in AVG eine von zwei Updatestufen auswählen:

- **Update der Definitionen** enthält die erforderlichen Änderungen für einen zuverlässigen Virenschutz. In der Regel umfasst sie keine Änderungen am Code und es wird nur die Virendatenbank aktualisiert. Dieses Update sollte durchgeführt werden, sobald es verfügbar ist.
- **Das Programmupdate** enthält verschiedene Programmänderungen, -ausbesserungen und -verbesserungen.

Beim [Planen von Updates](#) können Sie auswählen, welche Prioritätsstufe heruntergeladen und angewendet werden soll.

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

13.2. Updatetypen

Sie können zwischen zwei Aktualisierungstypen wählen:

- **Eine Aktualisierung On-Demand** ist ein sofortiges Update von AVG, das bei Bedarf jederzeit durchgeführt werden kann.
- **Geplante Aktualisierung – Innerhalb von AVG können Sie auch einen Aktualisierungsplan voreinstellen.** Die geplante Aktualisierung wird dann regelmäßig zu den festgelegten Zeiten ausgeführt. Immer wenn neue Aktualisierungsdateien an dem angegebenen Speicherort verfügbar sind, werden sie entweder direkt über das Internet oder das Netzwerkverzeichnis heruntergeladen. Wenn keine neuen Aktualisierungen verfügbar sind, passiert nichts.

13.3. Updatevorgang

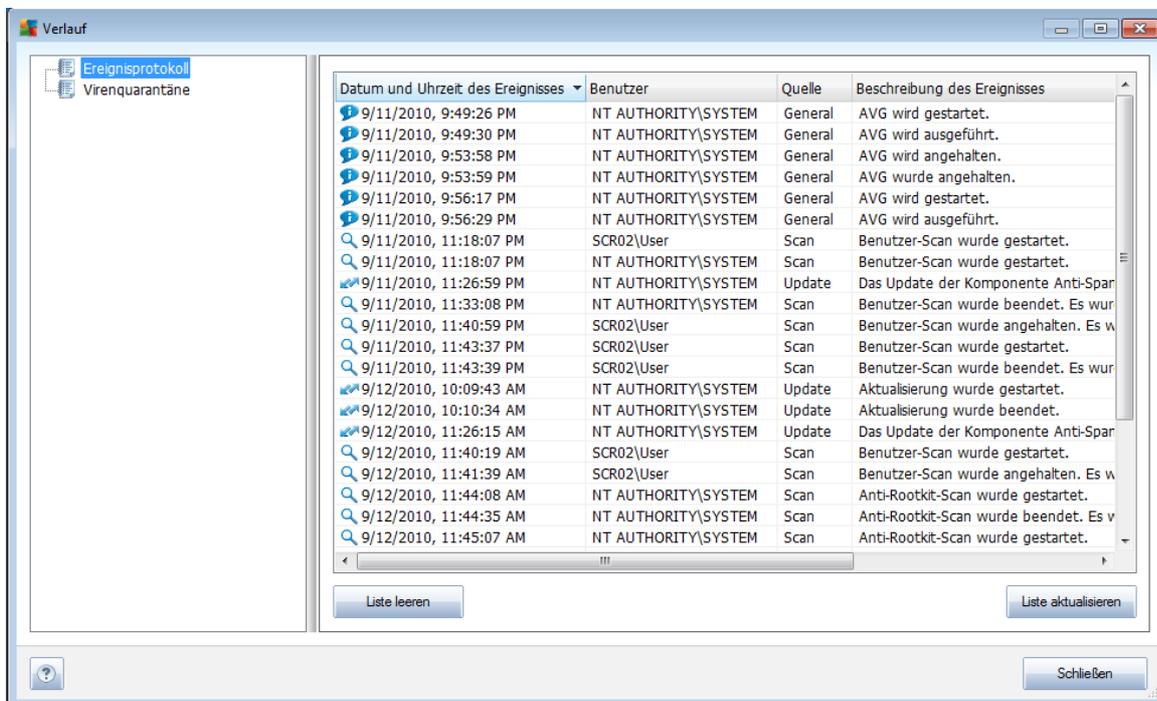
Der Updateprozess kann bei Bedarf unmittelbar gestartet werden, indem Sie auf den Quick LinkJetzt aktualisieren*** klicken. Dieser Link steht Ihnen jederzeit in allen Dialogen der [Benutzeroberfläche von AVG](#) zur Verfügung. Es empfiehlt sich jedoch, Updates regelmäßig entsprechend dem Updatezeitplan durchzuführen, der in der Komponente [Updatemanager](#) bearbeitet werden kann.



Wenn Sie das Update starten, überprüft AVG zunächst, ob neue Updatedateien zur Verfügung stehen. Wenn dies der Fall ist, lädt AVG diese eigenständig herunter und startet den Updateprozess. Während des Updateprozesses werden Sie zur Benutzeroberfläche **Update** weitergeleitet, wo der Fortschritt des Updates grafisch dargestellt und wie eine Übersicht über die statistischen Parameter (*Größe der Updatedatei, empfangene Daten, Download-Geschwindigkeit, verstrichene Zeit usw.*) angezeigt wird.

Hinweis: Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen Konfiguration wiederherstellen. Diese Option kann über *Start/Programme/Zubehör/Systemprogramme/Systemwiederherstellung* aufgerufen werden. Änderungen sollten jedoch nur von erfahrenen Benutzern vorgenommen werden!

14. 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 File Server 2011** aufgetreten sind. In der **Historie** werden folgende Ereignistypen aufgezeichnet:

- Informationen über Updates der AVG-Anwendung
- Start, Ende oder Unterbrechung des Scans (*einschließlich automatisch ausgeführter Tests*)
- Ereignisse in Verbindung mit der Virenerkennung (*durch [Residenten Schutz](#) oder 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 exakte Datum und die exakte Uhrzeit des Ereignisses an.
- **Benutzer** gibt an, von wem das Ereignis initialisiert wurde.
- **Quelle** gibt die Quellkomponente oder den 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** – Alle Einträge der Ereignisliste werden gelöscht
- **Liste aktualisieren** – Alle Einträge der Ereignisliste werden aktualisiert



15. FAQ und technischer Support

Bei Problemen mit AVG, egal ob diese geschäftlicher oder technischer Art sind, konsultieren Sie bitte den Abschnitt **FAQ** auf der Website von AVG (<http://www.avg.com/de>).

Falls Sie auf diese Weise keine Lösung für Ihr Problem finden, wenden Sie sich bitte per eMail an den technischen Support. Verwenden Sie bitte das Kontaktformular, das im Systemmenü unter **Hilfe / Onlinehilfe** zur Verfügung steht.