AVG AntiVirus

Benutzerhandbuch

Dokumentversion AVG.07 (25.11.2016)

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

Inhalt

1. Einführung **3**

2. Installationsvoraussetzungen für AVG **4**

2.1 Unterstützte Betriebssysteme 4

2.2 Mindestanforderungen und Empfehlungen für Hardware 4

3. Installationsvorgang bei AVG **5**

3.1 Willkommen! 5

3.2 Geben Sie Ihre Lizenznummer ein 6

3.3 Anpassen Ihrer Installation 8

3.4 AVG installieren 9

3.5 Installation abgeschlossen 10

4. Nach der Installation **11**

4.1 Update der Virendatenbank 11

4.2 Produktregistrierung 11

4.3 Zugriff auf die Benutzeroberfläche 11

4.4 Gesamten Computer scannen 11

4.5 Eicar-Test 11

4.6 Standardkonfiguration von AVG 12

5. Benutzeroberfläche von AVG **13**

5.1 Obere Navigationszeile 14

5.2 Informationen zum Sicherheitsstatus 17

5.3 Komponentenübersicht 18

5.4 Meine Apps 19

5.5 Quick Links zum Scannen bzw. Aktualisieren 19

5.6 Infobereichsymbol 20

5.7 AVG Advisor 21

5.8 AVG Accelerator 21

6. Komponenten von AVG **22**

6.1 Computerschutz 22

6.2 Schutz beim Surfen im Web 26

6.3 Software Analyzer 27

6.4 E-Mail-Schutz 29

6.5 PC Analyzer 30

7. Erweiterte Einstellungen von AVG **32**

7.1 Darstellung 32

7.2 Sounds 34

7.3 AVG-Schutz vorübergehend deaktivieren 35

7.4 Computerschutz 36

7.5 E-Mail-Scanner 42

7.6 Schutz beim Surfen im Web 52
7.7 Software Analyzer 55
7.8 Scans 56
7.9 Zeitpläne 62
7.10 Aktualisierung 69
7.11 Ausnahmen 73
7.12 Virenquarantäne 75
7.13 AVG-Selbstschutz 76
7.14 Datenschutzeinstellungen 76
7.15 Fehlerstatus ignorieren 78
7.16 Advisor – Bekannte Netzwerke 79

8. AVG-Scans 80
8.1 Vordefinierte Scans 82
8.2 Scans aus dem Windows Explorer 91
8.3 Befehlszeilen-Scan 91
8.4 Scans planen 95
8.5 Scan-Ergebnisse 103
8.6 Details zu den Scan-Ergebnissen 104

9. AVG File Shredder 105

10. Virenquarantäne 106

11. Verlauf 108
11.1 Scan-Ergebnisse 108
11.2 Residenter Schutz – Ergebnisse 109
11.3 Identitätsschutz – Ergebnisse 112
11.4 E-Mail-Schutz – Ergebnisse 113
11.5 Online Shield – Ergebnisse 114
11.6 Ereignisprotokoll 116

12. AVG Updates 118

13. FAQ und technischer Support 119

1. Einführung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG AntiVirus**.

AVG AntiVirus bietet Echtzeitschutz vor den ausgefeiltesten Bedrohungen von heute. Sie können sicher und sorglos chatten, Dateien austauschen, Spiele spielen und Videos ohne Unterbrechung ansehen, Dateien herunterladen und freigeben, soziale Netzwerke nutzen oder im Internet surfen – alles mit Echtzeitschutz.

Sie können auch andere Informationsquellen verwenden:

- ***Hilfedatei***: Der Abschnitt *Problembehebung* steht direkt in der Hilfedatei von **AVG AntiVirus zur Verfügung** *(die Hilfedatei kann in allen Dialogen der Anwendung mit der F1-Taste geöffnet werden)*. Dieser Abschnitt enthält eine Liste der häufigsten Situationen, in denen ein Benutzer professionelle Hilfe zu einem technischen Problem sucht. Bitte wählen Sie die Situation, die Ihr Problem am besten beschreibt, und klicken Sie darauf, um detaillierte Anweisungen zur Lösung des Problems anzuzeigen.

- ***Support Center auf der Website von AVG***: Alternativ können Sie die Lösung zu Ihrem Problem auch auf der Website von AVG suchen (*http://www.avg.com*). Im Bereich ***Support*** finden Sie eine Übersicht über Themenbereiche sowie zu Vertriebs- als auch zu technischen Problemen, einen gegliederten Bereich mit häufig gestellten Fragen sowie alle verfügbaren Kontakte.

- ***AVG ThreatLabs***: eine spezielle AVG-Website (*http://www.avg.com/about-viruses*), die Fragen zu Viren gewidmet ist und übersichtliche Informationen zu Online-Bedrohungen bietet. Dort finden Sie außerdem Anweisungen zum Entfernen von Viren und Spyware sowie Ratschläge zur Aufrechterhaltung Ihres Schutzes.

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

2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG AntiVirus wurde für den Schutz von Workstations mit den folgenden Betriebssystemen entwickelt:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (alle Editionen)
- Windows 7 (alle Editionen)
- Windows 8 (alle Editionen)
- Windows 10 (alle Editionen)

(sowie ggf. höhere Service Packs für bestimmte Betriebssysteme)

2.2. Mindestanforderungen und Empfehlungen für Hardware

Hardware-Mindestanforderungen für **AVG AntiVirus**:

- Intel Pentium CPU 1,5 GHz oder schneller
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM-Speicher
- 1,3 GB freier Festplattenspeicher *(für Installationszwecke)*

Empfohlene Hardware-Anforderungen für **AVG AntiVirus**:

- Intel Pentium CPU 1,8 GHz oder schneller
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM-Speicher
- 1,6 GB freier Festplattenspeicher *(für Installationszwecke)*

3. Installationsvorgang bei AVG

Für die Installation von **AVG AntiVirus** auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Um sicherzustellen, dass Sie die neueste Version von **AVG AntiVirus** installieren, wird empfohlen, die Installationsdatei von der Website von AVG (http://www.avg.com) herunterzuladen. Der Bereich ***Support*** enthält eine gegliederte Übersicht über die Installationsdateien jeder AVG-Version. Nachdem Sie die Installationsdatei heruntergeladen und auf Ihrer Festplatte gespeichert haben, können Sie den Installationsvorgang starten. Die Installation ist eine Abfolge von einfachen und leicht verständlichen Dialogen. Jeder Dialog beschreibt kurz, was bei jedem Schritt des Installationsvorgangs zu tun ist. Im Folgenden finden Sie eine detaillierte Erläuterung zu jedem Dialogfenster:

3.1. Willkommen!

Der Installationsvorgang beginnt mit dem Dialog ***Willkommen bei AVG Internet Security***:

Sprachauswahl

In diesem Dialog können Sie die Sprache auswählen, die für den Installationsvorgang verwendet wird. Klicken Sie auf die Combo-Box neben der Option ***Sprache***, um das Sprachenmenü aufzuklappen. Wählen Sie die gewünschte Sprache aus. Der Installationsvorgang wird dann in der Sprache Ihrer Wahl fortgesetzt. Die Kommunikation in der Anwendung erfolgt ebenfalls in der ausgewählten Sprache, mit der Option, auf die standardmäßig installierte Sprache Englisch umzuschalten.

Lizenzvereinbarung für Endbenutzer und Datenschutzrichtlinie

Bevor Sie mit dem Installationsvorgang fortfahren, empfehlen wir Ihnen, sich mit der ***Lizenzvereinbarung für Endnutzer*** und der ***Datenschutzrichtlinie*** vertraut zu machen. Auf beide Dokumente kann über die aktiven Links im unteren Teil des Dialogfelds zugegriffen werden. Klicken Sie auf einen der Hyperlinks, um ein neues

Dialogfeld/neues Browserfenster mit dem vollständigen Wortlaut des entsprechenden Dokuments zu öffnen. Lesen Sie diese rechtsverbindlichen Dokumente sorgfältig durch. Indem Sie auf die Schaltfläche ***Fortfahren*** klicken, bestätigen Sie Ihre Zustimmung zu den Dokumenten.

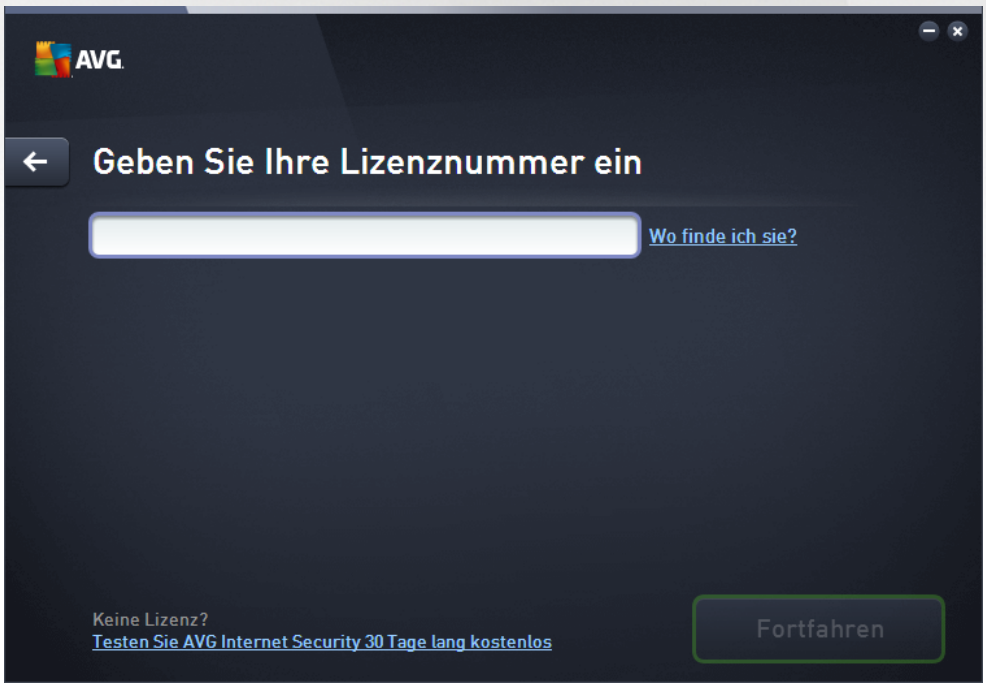
Mit der Installation fortfahren

Klicken Sie zum Fortsetzen des Installationsvorgangs auf die Schaltfläche ***Fortfahren***. Sie werden nach Ihrer Lizenznummer gefragt und der Installationsvorgang läuft dann automatisch. Für die meisten Benutzer wird empfohlen, diese Standardoption für die Installation von **AVG AntiVirus** mit allen vom Programmhersteller vordefinierten Einstellungen zu verwenden. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration in Zukunft geändert werden muss, können Sie diese Änderung immer direkt in der Anwendung vornehmen.

Alternativ besteht die Option der ***Benutzerdefinierten Installation***, die in Form eines Hyperlinks unter der Schaltfläche ***Fortfahren*** zur Verfügung steht. Die benutzerdefinierte Installation sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, die Anwendung nicht mit den Standardeinstellungen zu installieren, beispielsweise um bestimmte Systemanforderungen zu erfüllen. Wenn Sie sich für diesen Weg entscheiden, werden Sie nach dem Eintragen Ihrer Lizenznummer zum Dialogfeld ***Anpassen Ihrer Installation*** umgeleitet, wo Sie Ihre Einstellungen angeben können.

3.2. Geben Sie Ihre Lizenznummer ein

Im Dialog ***Geben Sie Ihre Lizenznummer ein*** werden Sie dazu aufgefordert, Ihre Lizenznummer zu aktivieren, indem Sie sie in das dafür vorgesehene Textfeld eingeben *(bzw. kopieren und einfügen)*:



Wo finde ich meine Lizenznummer?

Die Verkaufsnummer finden Sie auf der CD-Verpackung Ihres **AVG AntiVirus** -Pakets. Die Lizenznummer ist in der Bestätigungs-E-Mail enthalten, die Sie nach dem Online-Kauf von **AVG AntiVirus** erhalten haben. Sie müssen die Nummer exakt wie dargestellt eingeben. Wenn die Lizenznummer in digitaler Form verfügbar ist (*in der E-Mail*), empfehlen wir Ihnen, diese zu kopieren und einzufügen.

So verwenden Sie die Methode „Kopieren und Einfügen“

Verwenden Sie die Methode ***Kopieren und Einfügen***, um Ihre Lizenznummer von **AVG AntiVirus** korrekt einzugeben. Gehen Sie wie folgt vor:

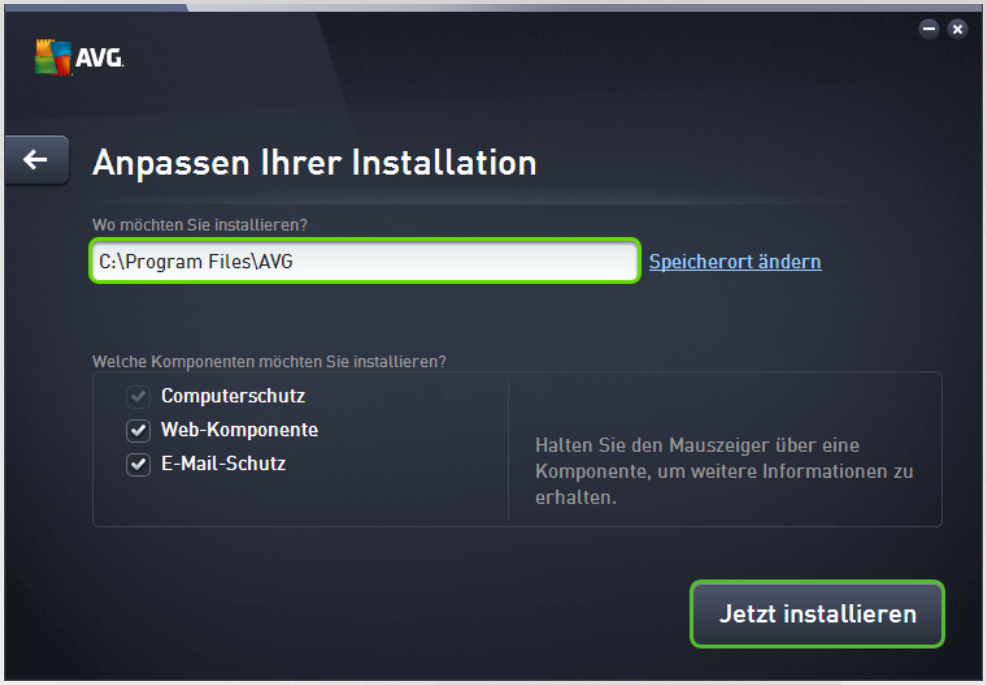
- Öffnen Sie die E-Mail mit Ihrer Lizenznummer.
- Klicken Sie mit der linken Maustaste an den Anfang der Lizenznummer, ziehen Sie die Maus bei gedrückter Maustaste bis zum Ende der Nummer, und lassen Sie die Maustaste los. Die Nummer ist jetzt markiert.
- Halten Sie die ***Strg-Taste*** gedrückt und drücken Sie die ***Taste C***. Damit wird die Nummer in den Zwischenspeicher verschoben.
- Positionieren Sie den Cursor an der Stelle, an der Sie die kopierte Nummer einfügen möchten, z. B. im Textfeld des Dialogfelds ***Geben Sie Ihre Lizenznummer ein***.
- Halten Sie die ***Strg-Taste*** gedrückt und drücken Sie die ***Taste V***. Damit wird die Nummer an der gewünschten Stelle eingefügt.

Mit der Installation fortfahren

Unten im Dialogfeld finden Sie die Schaltfläche ***Jetzt installieren***. Die Schaltfläche wird aktiviert, wenn Sie Ihre Lizenznummer eingeben. Klicken Sie dann einfach auf die aktivierte Schaltfläche, um den Installationsvorgang zu starten. Wenn Sie über keine gültige Lizenznummer verfügen, haben Sie die Möglichkeit, die ***AVG AntiVirus Free Edition*** der Anwendung zu installieren. Leider unterstützt die kostenlose Version nicht alle Funktionen, die in der professionellen Vollversion zur Verfügung stehen. Detaillierte Informationen zum Kauf und zur Aktualisierung von AVG finden Sie auf der Website von AVG (http://www.avg.com).

3.3. Anpassen Ihrer Installation

Im Dialog ***Anpassen Ihrer Installation*** können Sie detailliert Parameter für die Installation festlegen:



Wo möchten Sie installieren?

Hier können Sie festlegen, wo die Anwendung installiert werden soll. Die Adresse im Textfeld zeigt den vorgeschlagenen Ordner in Ihren Programmdateien. Wenn Sie einen anderen Ordner verwenden möchten, klicken Sie auf den Link zum Wechseln des Ordners, um in der Baumstruktur Ihres Laufwerks ein neues Fenster zu öffnen. Navigieren Sie dann zu dem gewünschten Ordner, und bestätigen Sie Ihre Wahl.

Welche Komponenten möchten Sie installieren?

In diesem Abschnitt wird eine Übersicht über alle Komponenten angezeigt, die installiert werden können. Wenn die Standardeinstellungen nicht Ihren Anforderungen entsprechen, können Sie einzelne Komponenten entfernen. Sie können jedoch nur Komponenten auswählen, die in AVG AntiVirus enthalten sind. Die einzige Ausnahme ist die Komponente ***Computerschutz***, sie kann von der Installation nicht ausgeschlossen werden. Durch Markieren eines Eintrags in diesem Bereich wird eine kurze Beschreibung der entsprechenden Komponente auf der rechten Seite dieses Bereichs angezeigt. Weitere Informationen zu den Funktionen der einzelnen Komponenten finden Sie im Kapitel Komponentenübersicht in dieser Dokumentation.

Mit der Installation fortfahren

Klicken Sie zum Fortsetzen des Installationsvorgangs auf die Schaltfläche ***Jetzt installieren***. Sie können aber auch, wenn Sie Ihre Spracheinstellungen ändern oder überprüfen müssen, in das vorherige Dialog zurückgehen, indem Sie im oberen Bereich dieses Dialogs auf die Pfeiltaste ← klicken.

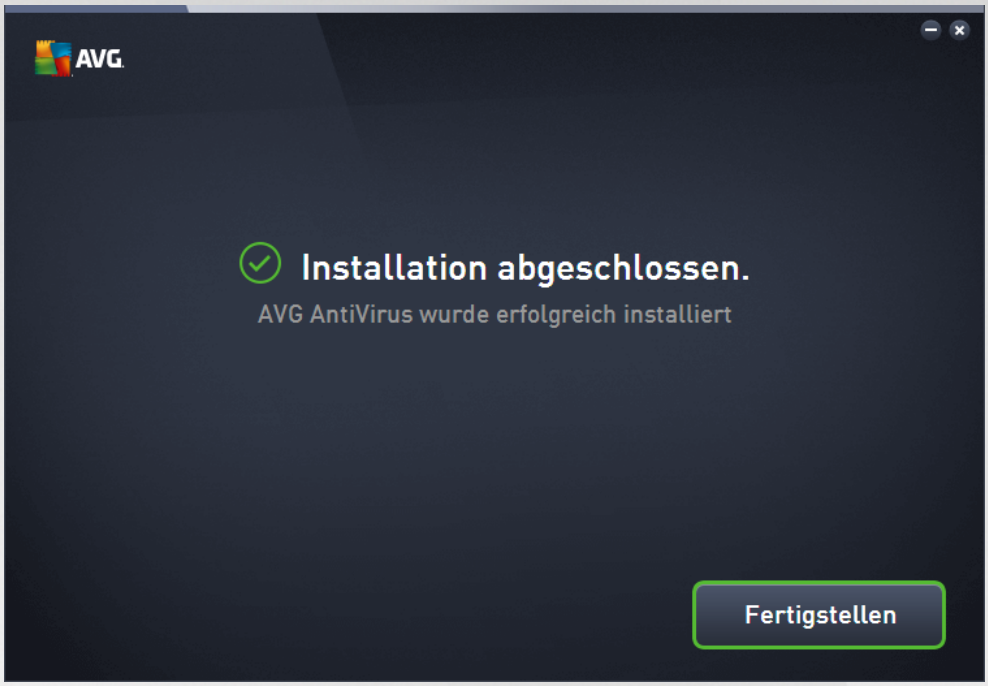
3.4. AVG installieren

Nachdem Sie den Start des Installationsvorgangs im vorherigen Dialogfeld bestätigt haben, wird die Installation vollkommen automatisch ausgeführt und erfordert keinen Eingriff:

Wenn die Installation abgeschlossen ist, wird automatisch das nächste Dialogfeld angezeigt.

3.5. Installation abgeschlossen

Der Dialog ***Installation abgeschlossen*** bestätigt, dass AVG AntiVirus vollständig installiert und konfiguriert wurde:



Klicken Sie auf die Schaltfläche ***Fertig stellen***, um die Installation abzuschließen.

4. Nach der Installation

4.1. Update der Virendatenbank

Beachten Sie, dass nach der Installation *(gegebenenfalls nach einem Neustart des Computers)* **AVG AntiVirus** automatisch seine Virendatenbank und alle Komponenten aktualisiert und funktionstüchtig macht. Dieser Vorgang kann einige Minuten dauern. Während des Aktualisierungsvorgangs werden Sie anhand von Benachrichtigungen im Hauptfenster informiert. Warten Sie eine Zeit lang, bis die Aktualisierung abgeschlossen und **AVG AntiVirus** vollständig eingerichtet ist, um Sie zu schützen.

4.2. Produktregistrierung

Nach Abschluss der Installation von **AVG AntiVirus** registrieren Sie bitte Ihr Produkt online auf der Website von AVG (*http://www.avg.com*). Nach der Registrierung erhalten Sie vollen Zugriff auf Ihr AVG-Benutzerkonto, den AVG Update-Newsletter und andere exklusive Dienste für registrierte Benutzer. Die einfachste Möglichkeit zur Registrierung bietet die Benutzeroberfläche von **AVG AntiVirus**. Wählen Sie die obere Navigationszeile > Optionen > Jetzt registrieren Sie werden auf die ***Registrierungsseite*** der AVG-Website (*http://www.avg.com*) weitergeleitet. Bitte folgen Sie den Anweisungen auf dieser Seite.

4.3. Zugriff auf die Benutzeroberfläche

Der Hauptdialog von AVG kann auf mehrere Arten geöffnet werden:

- durch Doppelklicken auf das AVG AntiVirus Infobereichsymbol
- durch Doppelklicken auf das AVG-Protection-Symbol auf dem Desktop
- über das Menü *Start/Programme/AVG /AVG Protection*

4.4. Gesamten Computer scannen

Es besteht das potentielle Risiko, dass vor der Installation von **AVG AntiVirus** 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. Dieser erste Scan nimmt möglicherweise einige Zeit in Anspruch *(etwa eine Stunde)*. Es wird jedoch empfohlen, den Scan zu starten, um sicherzustellen, dass Ihr Computer keinen Bedrohungen ausgesetzt ist. Eine Anleitung zum Ausführen der Option Gesamten Computer scannen finden Sie im Kapitel AVG-Scans.

4.5. Eicar-Test

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

Der EICAR-Test ist eine standardmäßige und absolut sichere Methode, um die Funktion von Virenschutzsystemen zu überprüfen. Der Eicar-Virus kann ohne Sicherheitsrisiko weitergegeben werden, da es sich dabei nicht um einen wirklichen Virus handelt und er auch keine Fragmente viralen Codes enthält. Die meisten Produkte reagieren jedoch, als würde es sich tatsächlich um ein Virus handeln (*es wird in der Regel mit einem offensichtlichen Namen wie „EICAR-AV-Test“ gemeldet*). Sie können das EICAR-Virus von der EICAR-Website unter www.eicar.com herunterladen und finden dort auch alle wichtigen Informationen zum EICAR-Test.

Laden Sie die Datei *eicar.com* herunter und speichern Sie sie auf Ihrer lokalen Festplatte. Direkt nachdem Sie das Herunterladen der Testdatei bestätigt haben, gibt **AVG AntiVirus** eine Warnmeldung aus. Diese Meldung zeigt, dass AVG korrekt auf dem Computer installiert ist.

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

4.6. Standardkonfiguration von AVG

Die Standardkonfiguration (*Konfiguration der Anwendung unmittelbar nach der Installation*) von **AVG AntiVirus** ist vom Software-Hersteller 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.*** Wenn Sie die Konfiguration von AVG ändern und besser an Ihre Bedürfnisse anpassen möchten, rufen Sie Erweiterte Einstellungen von AVG auf und wählen Sie *Optionen/Erweiterte Einstellungen*. Daraufhin wird der Dialog Erweiterte Einstellungen von AVG angezeigt, in dem Sie die Konfiguration von AVG ändern können.

5. Benutzeroberfläche von AVG

AVG AntiVirus öffnet das Hauptfenster:

Das Hauptfenster ist in mehrere Bereiche gegliedert:

- ***Die obere Navigationszeile*** besteht aus vier aktiven Links, die sich im oberen Bereich des Hauptfensters befinden *(Mehr von AVG, Berichte, Support, Optionen)*. Details >>
- ***Informationen zum Sicherheitsstatus*** gibt Auskunft über den derzeitigen Sicherheitsstatus von **AVG AntiVirus**. Details >>
- ***Die Übersicht installierter Komponenten*** befindet sich in einem Streifen horizontal angeordneter Rechtecke in der Mitte des Hauptfensters. Die Komponenten werden als hellgrüne Rechtecke mit dem entsprechenden Symbol angezeigt und geben Auskunft über den Komponentenstatus. Details >>
- ***Meine Apps*** werden im unteren mittleren Streifen des Hauptfensters abgebildet und geben Ihnen zusätzlich zu **AVG AntiVirus** einen Überblick über die Anwendungen, die bereits auf Ihrem Computer installiert sind oder deren Installation empfohlen wird. Details >>
- ***Quick Links scannen/aktualisieren*** befindet sich im unteren Streifen aus Rechtecken im Hauptfenster. Mithilfe dieser Schaltflächen haben Sie direkten Zugriff auf die wichtigsten und am häufigsten genutzten Funktionen von AVG. Details >>

Außerhalb des Hauptfensters von **AVG AntiVirus** befindet sich ein weiteres Steuerelement, mit dem Sie auf die Anwendung zugreifen können:

- ***Das Infobereichsymbol*** befindet sich unten rechts in der Ecke des Bildschirms *(auf der Taskleiste)* und zeigt den derzeitigen Status von **AVG AntiVirus** an. Details >>

5.1. Obere Navigationszeile

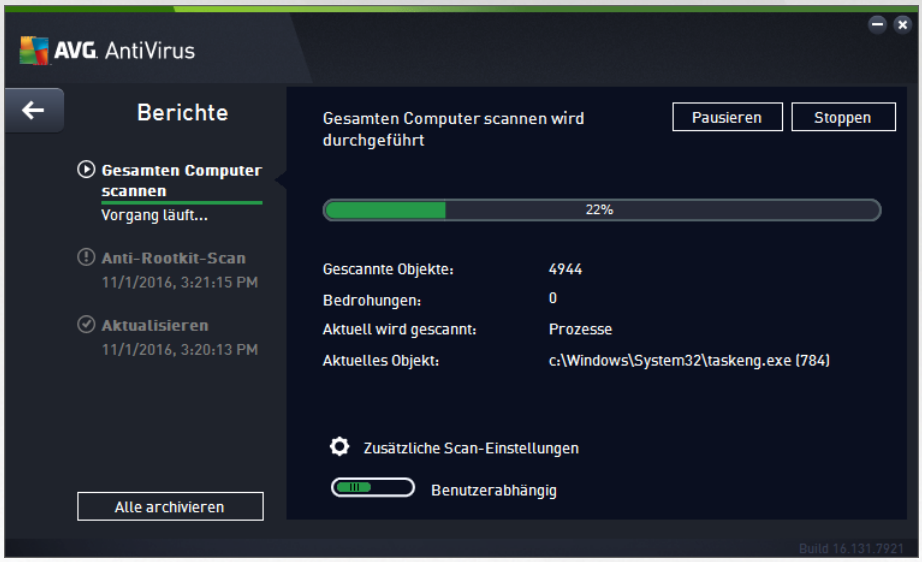
Die ***obere Navigationszeile*** besteht aus mehreren aktiven Links, die sich im oberen Bereich des Hauptfensters befinden. Sie enthält folgende Schaltflächen:

5.1.1. Mehr von AVG

Klicken Sie auf den Link, um die AVG-Website aufzurufen, auf der Sie sämtliche Informationen zum AVG-Schutz für maximale Sicherheit im Internet erhalten.

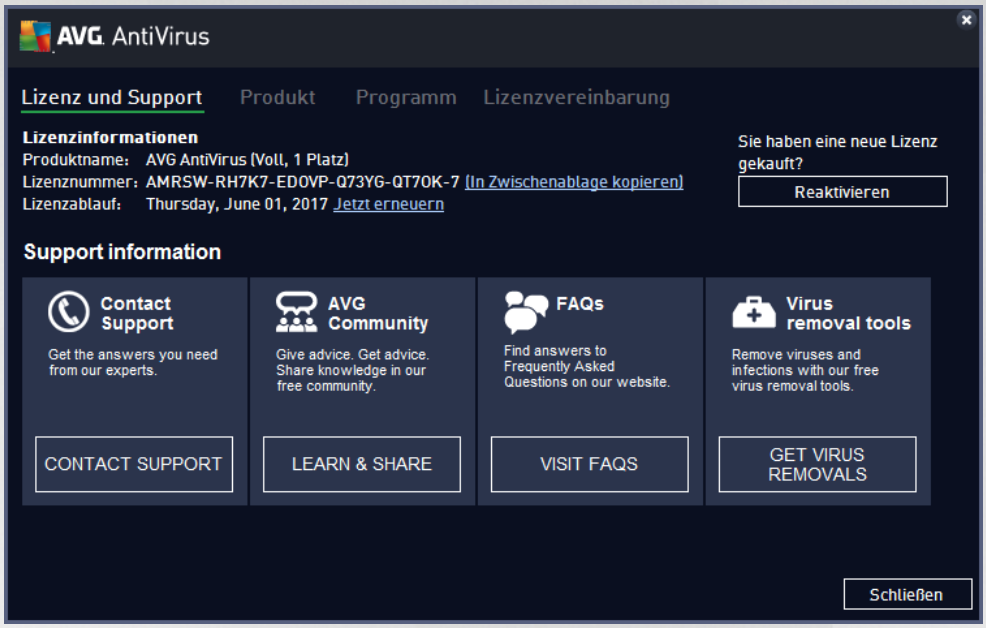
5.1.2. Berichte

Öffnet ein neues Dialogfeld ***Berichte*** mit einer Übersicht über alle relevanten Berichte zu zuvor gestarteten Scans und Updates. Wenn der Scan bzw. das Update derzeit ausgeführt wird, wird ein rotierender Kreis neben dem Wort ***Berichte*** in der oberen Navigationszeile der Hauptbenutzeroberfläche angezeigt. Klicken Sie auf diesen Kreis, um das Dialogfeld mit dem Fortschritt des ausgeführten Prozesses zu öffnen:



5.1.3. Support

Öffnet ein neues Dialogfeld mit vier Registerkarten, die alle relevanten Informationen zu **AVG AntiVirus** enthalten:



- ***Lizenz und Support*** - Auf der Registerkarte finden Sie Informationen zu Produktname, Lizenznummer sowie Ablaufdatum. Im unteren Bereich des Dialogfelds befindet sich außerdem eine klar gegliederte Übersicht mit sämtlichen verfügbaren Kontaktmöglichkeiten zum Kundendienst. Die Registerkarte enthält folgende aktive Links und Schaltflächen:
    - *(Re-)Aktivieren* – Öffnet das neue Dialogfeld zum ***Aktivieren der AVG-Software***. Geben Sie Ihre Lizenznummer in das entsprechende Feld ein, um entweder die Vertriebsnummer *(die Sie während der AVG AntiVirus-Installation verwenden)* zu ersetzen oder Ihre aktuelle Lizenznummer durch eine andere zu ersetzen *(z. B. beim Upgrade auf ein höheres AVG-Produkt)*.
    - *In Zwischenablage kopieren* – Verwenden Sie diesen Link, um die Lizenznummer zu kopieren und an anderer Stelle einzufügen. Auf diese Weise wird Ihre Lizenznummer korrekt eingegeben.
    - *Jetzt verlängern* – Wir empfehlen, die Lizenzverlängerung für **AVG AntiVirus** frühzeitig zu erwerben, mindestens einen Monat vor Ablauf Ihrer aktuellen Lizenz. Sie werden auf das bevorstehende Ablaufdatum hingewiesen. Klicken Sie auf diesen Link, um zur AVG-Website *(http://www.avg.com)* zu gelangen, auf der Sie detaillierte Informationen zu Lizenzstatus, Ablaufdatum und Verlängerungs- bzw. Upgrade-Angeboten finden.
- ***Produkt*** – Diese Registerkarte bietet eine Übersicht über die wichtigsten technischen Daten von **AVG AntiVirus** zu AV-Produktinformationen, installierten Komponenten und installiertem E-Mail-Schutz.
- ***Programm*** – Auf dieser Registerkarte finden Sie detaillierte technische Informationen zu der installierten Version von **AVG AntiVirus** wie zum Beispiel die Versionsnummer des Hauptprodukts und die Liste der Versionsnummern aller entsprechenden Produkte *(z. B. Zen, PC TuneUp, ...)*. Die

Registerkarte gibt auch einen Überblick über alle installierten Komponenten und spezifischen Sicherheitsinformationen *(Versionsnummern von Virendatenbank und LinkScanner)*.

- ***Lizenzvereinbarung*** – Die Registerkarte enthält den vollständigen Text der Lizenzvereinbarung zwischen Ihnen und AVG Technologies.

5.1.4. Optionen

Die Wartung von **AVG AntiVirus** kann über das Element ***Optionen*** aufgerufen werden. Klicken Sie auf den Pfeil, um das Dropdown-Menü zu öffnen.

- ***Computer scannen*** startet einen Scan des gesamten Computers.
- ***Ausgewählten Ordner scannen...*** – wechselt zur Scan-Oberfläche von AVG und ermöglicht es Ihnen, in der Baumstruktur Ihres Computers zu entscheiden, welche Dateien und Ordner gescannt werden sollen.
- ***Datei scannen...*** – ermöglicht es Ihnen, bei Bedarf einen Test für eine bestimmte einzelne Datei auszuführen. Klicken Sie auf diese Option, um in der Baumstruktur Ihres Laufwerks ein neues Fenster zu öffnen. Wählen Sie die gewünschte Datei, und bestätigen Sie den Start des Scans.
- ***Update*** – Startet automatisch den Aktualisierungsvorgang von **AVG AntiVirus**.
- ***Aus Verzeichnis aktualisieren...*** – Führt den Aktualisierungsvorgang über die 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 unterbrochen wurde 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 Updatedatei zuvor gespeichert haben, und starten Sie den Updatevorgang.
- ***Virenquarantäne*** – Öffnet die Benutzeroberfläche der Virenquarantäne. Dorthin verschiebt AVG alle erkannten Infektionen. Innerhalb dieser Quarantäne werden die infizierten Dateien isoliert, sodass die Sicherheit Ihres Computers gewährleistet ist. Gleichzeitig werden die infizierten Dateien für eine mögliche Reparatur gespeichert.
- ***Verlauf*** – Enthält weitere Untermenü-Optionen:
  - *Scan-Ergebnisse* – Öffnet ein Dialogfeld mit einer Übersicht der Scan-Ergebnisse.
  - *Residenter Schutz – Ergebnisse* – Zeigt ein Dialogfenster mit einer Übersicht der Bedrohungen an, die durch den residenten Schutz erkannt wurden.
  - *Software Analyzer – Ergebnisse* – Zeigt ein Dialogfeld mit einer Übersicht der Bedrohungen an, die durch die Komponente Software Analyzer erkannt wurden.
  - *E-Mail-Schutz – Ergebnisse* – Öffnet einen Dialog mit einer Übersicht der E-Mail-Anhänge, die von der Komponente E-Mail-Schutz als gefährlich eingestuft wurden.
  - *Online Shield – Ergebnisse* – Öffnet einen Dialog mit einer Übersicht der Bedrohungen, die von Online Shield erkannt wurden.

- *Ereignisprotokoll* – Zeigt die Ereignisprotokoll-Oberfläche mit einer Übersicht über alle von **AVG AntiVirus** protokollierten Aktionen an.

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

- ***Inhalt*** – Öffnet die Hilfedateien von AVG.

- ***Support nutzen*** – Öffnet den Support-Dialog, der alle verfügbaren Kontakte und Supportinformationen enthält.

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

- ***Info zu Viren und Bedrohungen*** – Öffnet die Online-Virenenzyklopädie auf der AVG-Website (*http://www.avg.com*), in der Sie genaue Informationen über das ermittelte Virus finden.

- ***(Re-)Aktivieren*** – Öffnet das Dialogfeld zum Aktivieren mit der von Ihnen während des Installationsprozesses angegebenen Lizenznummer. In diesem Dialogfeld können Sie Ihre Lizenznummer bearbeiten, um entweder die Vertriebsnummer (*mit der Sie AVG installiert haben*) oder die alte Lizenznummer (*zum Beispiel beim Upgrade auf ein neues AVG-Produkt*) zu ersetzen. Wenn Sie die Testversion von **AVG AntiVirus** verwenden, werden die letzten zwei Einträge als ***Jetzt kaufen*** und ***Aktivieren*** angezeigt, sodass Sie die Vollversion des Programms direkt kaufen können. Wenn **AVG AntiVirus** mit einer Vertriebsnummer installiert ist, werden die Einträge als ***Registrieren*** und ***Aktivieren*** angezeigt:

- ***Jetzt registrieren/MyAccount*** – Verbindet Sie mit der Registrierungsseite der AVG-Website (*http://www.avg.com*). Bitte geben Sie Ihre Registrierungsdaten ein. Nur Kunden, die ihr AVG-Produkt registrieren, erhalten kostenlosen technischen Support.

- ***Info zu AVG*** – Öffnet einen neuen Dialog mit vier Registerkarten. Diese enthalten Informationen über die von Ihnen erworbene Lizenz und den zur Verfügung stehenden Support, Produkt- und Programminformationen sowie den vollständigen Wortlaut der Lizenzvereinbarung. *(Derselbe Dialog kann über den Support-Link im Haupt-Navigationsmenü geöffnet werden.)*

5.2. Informationen zum Sicherheitsstatus

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

– das grüne Symbol zeigt an, dass Ihr ***AVG AntiVirus vollständig funktionsfähig ist***. Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

– das gelbe Symbol warnt Sie, ***wenn eine oder mehrere Komponenten falsch konfiguriert sind*** und Sie die entsprechenden Eigenschaften/Einstellungen überprüfen sollten. Es besteht kein grundlegendes Problem in **AVG AntiVirus**, und Sie haben sich wahrscheinlich entschieden, eine Komponente aus bestimmten Gründen zu deaktivieren. Sie sind immer noch geschützt. Sie sollten jedoch die Einstellungen der problematischen Komponente überprüfen! Die falsch konfigurierte Komponente wird in der Hauptbenutzeroberfläche mit einer orangefarbigen Warnleiste angezeigt.

Das gelbe Symbol wird auch dann angezeigt, wenn Sie aus einem bestimmten Grund festgelegt haben, den Fehlerstatus einer Komponente zu ignorieren. Die Option ***Fehlerstatus ignorieren*** kann unter Erweiterte Einstellungen > Fehlerstatus ignorieren aufgerufen werden. Sie können hier angeben, dass Ihnen bekannt ist, dass die Komponente einen Fehlerstatus aufweist, aber **AVG AntiVirus** aus einem bestimmten Grund diesen Status beibehalten soll und Sie nicht gewarnt werden möchten. Es kann vorkommen, dass Sie diese Option in bestimmten Situationen verwenden müssen. Es wird jedoch dringend empfohlen, die Option ***Fehlerstatus ignorieren*** so bald wie möglich zu deaktivieren!

Alternativ dazu wirddas gelbe Symbol auch angezeigt, wenn **AVG AntiVirus** einen Neustart Ihres Computers erfordert (***Neustart erforderlich***). Beachten Sie die Warnung und starten Sie Ihren Computer neu.

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

Wenn AVG AntiVirus nicht für optimale Leistung konfiguriert ist, wird neben den Informationen zum Sicherheitsstatus eine neue Schaltfläche „Reparieren“ angezeigt (alternativ auch „Alles reparieren“, wenn das Problem mehrere Komponenten betrifft). Klicken Sie auf die Schaltfläche, um eine automatische Überprüfung und Konfiguration des Programms zu starten. Anhand dieser einfachen Methode können Sie die optimale Leistung von AVG AntiVirus gewährleisten und maximale Sicherheit erzielen.

Es wird dringend empfohlen, die ***Informationen zum Sicherheitsstatus*** zu beachten und angezeigte Probleme umgehend zu lösen. Anderenfalls ist Ihr Computer gefährdet!

Hinweis:*Statusinformationen zu AVG AntiVirus erhalten Sie auch jederzeit über das Infobereichsymbol.*

5.3. Komponentenübersicht

Die ***Übersicht installierter Komponenten*** befindet sich in einem Streifen horizontal angeordneter Rechtecke in der Mitte des Hauptfensters. Die Komponenten werden als hellgrüne Rechtecke mit dem entsprechenden Symbol angezeigt. Jedes Rechteck bietet Informationen zum derzeitigen Sicherheitsstatus. Wenn die Komponente korrekt konfiguriert und voll funktionsfähig ist, wird die Information in grünen Buchstaben angezeigt. Wenn die Komponente angehalten wurde, sie nicht voll funktionsfähig ist oder einen Fehlerstatus aufweist, werden Sie davon in einer Meldung mit einem orangefarbigen Textfeld in Kenntnis gesetzt. ***Es wird dringend empfohlen, die Komponenteneinstellungen zu beachten!***

Wenn Sie den Mauszeiger über die Komponente bewegen, wird ein kurzer Text unten im Hauptfenster eingeblendet. Darin werden die grundlegenden Funktionen der Komponente vorgestellt. Darüber hinaus wird der derzeitige Status der Komponente angezeigt und es wird angegeben, welche Dienste der Komponente nicht korrekt konfiguriert sind.

Liste der installierten Komponenten

In **AVG AntiVirus** enthält der Bereich ***Komponentenübersicht*** Informationen zu folgenden Komponenten:

- ***Computer*** – Diese Komponente deckt zwei Dienste ab: ***AntiVirus Shield*** erkennt Viren, Spyware, Würmer, Trojaner, unerwünschte ausführbare Dateien oder Bibliotheken in Ihrem System und schützt

Sie vor schädlicher Adware. ***Anti-Rootkit*** sucht nach gefährlichen Rootkits, die sich in Anwendungen, Treibern oder Bibliotheken verbergen. Details >>

- ***Surfen im Web*** – schützt Sie beim Surfen im Internet vor webbasierten Angriffen. Details >>
- ***Software*** – Die Komponente führt den Dienst ***Software Analyzer*** aus, der Ihre digitalen Daten dauerhaft vor neuen und unbekannten Bedrohungen aus dem Internet schützt. Details >>
- ***E-Mails*** – Überprüft eingehende E-Mail-Nachrichten auf Spam und blockiert Viren, Phishing-Angriffe und andere Bedrohungen. Details >>

Verfügbare Aktionen

- ***Bewegen Sie Ihre Maus über eines der Komponentensymbole***, um die Komponente in der Übersicht zu markieren. Im unteren Teil der Benutzeroberfläche wird eine kurze Funktionsbeschreibung der ausgewählten Komponente angezeigt.
- ***Klicken Sie auf das Komponentensymbol***, um die Oberfläche der Komponente mit ihren Statusinformationen zu öffnen und Zugriff auf ihre Konfigurations- und Statistikinformationen zu erhalten.

5.4. Meine Apps

Im Bereich ***Meine Apps*** *(die aus grünen Rechtecken bestehende Zeile unter der Komponentensammlung)* finden Sie eine Übersicht der zusätzlichen AVG-Anwendungen, die entweder bereits auf Ihrem Computer installiert sind oder deren Installation empfohlen wird. Die Rechtecke werden nur unter bestimmten Umständen angezeigt und können die folgenden Anwendungen darstellen:

- ***Mobiler Schutz*** ist eine Anwendung, die Ihr Mobiltelefon vor Viren und Malware schützt. Außerdem können Sie Ihr Smartphone mithilfe dieser Anwendung bei einem eventuellen Verlust orten.
- ***PC Tuneup*** ist ein leistungsstarkes Tool zur detaillierten Systemanalyse und Optimierung der Geschwindigkeit und Gesamtleistung Ihres Computers.

Genauere Informationen zu den Anwendungen aus ***Meine Apps*** erhalten Sie durch einen Klick auf das entsprechende Rechteck. Sie gelangen dann auf die entsprechende AVG-Webseite, von der aus Sie die Komponente auch direkt herunterladen können.

5.5. Quick Links zum Scannen bzw. Aktualisieren

Quick Links befinden sich in der unteren Zeile der Schaltflächen der **AVG AntiVirus** Benutzeroberfläche. Über diese Links können Sie direkt auf die wichtigsten und am häufigsten verwendeten Funktionen der Anwendung zugreifen, d. h. Scan und Update. Die Quick Links sind von allen Dialogen der Benutzeroberfläche aus verfügbar:

- ***Jetzt scannen*** – Die Schaltfläche ist in zwei Bereiche unterteilt. Klicken Sie auf den Link ***Jetzt scannen***, um den Scan des gesamten Computers sofort zu starten. Der Fortschritt und die Ergebnisse werden in dem automatisch geöffneten Fenster Berichte angezeigt. Die Schaltfläche ***Optionen*** öffnet das Dialogfeld ***Scan-Optionen***, in dem Sie geplante Scans verwalten und Parameter für Gesamten Computer scannen / Bestimmte Dateien/Ordner scannen bearbeiten können. *(Weitere Informationen finden Sie im Kapitel AVG-Scans.)*

- ***Leistungsprobleme beheben*** – Durch diese Schaltfläche wird der Service ***PC Analyzer*** aufgerufen, ein leistungsstarkes Tool zur detaillierten Systemanalyse und Optimierung der Geschwindigkeit und Gesamtleistung Ihres Computers.

- ***Jetzt aktualisieren*** – Klicken Sie auf die Schaltfläche, um das Produkt-Update sofort zu starten. Über das Popup-Fenster oberhalb des Infobereichsymbols von AVG werden Sie über die Ergebnisse der Updates informiert. *(Weitere Informationen finden Sie im Kapitel AVG Updates.)*

5.6. Infobereichsymbol

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

Anzeige des Infobereichsymbols von AVG

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

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

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

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

Informationen zum Infobereichsymbol von AVG

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

Über das Infobereichsymbol von AVG verfügbare Aktionen

Das ***Infobereichsymbol von AVG*** kann auch als Quick Link verwendet werden, um auf die Benutzeroberfläche von **AVG AntiVirus** zuzugreifen. Doppelklicken Sie dazu einfach auf das Symbol. Wenn Sie mit der rechten Maustaste auf das Kontextmenü klicken, erhalten Sie Zugriff auf die wichtigsten Funktionen:

- ***Öffnen*** – verwenden Sie diese Schaltfläche, um die Benutzeroberfläche zu öffnen.
- ***Jetzt scannen*** – verwenden Sie diese Schaltfläche, um Gesamten Computer scannen sofort zu starten.
- ***Schutz*** (aktiviert /deaktiviert) – verwenden Sie diesen Schalter, um die **AVG AntiVirus**-Komponenten herunterzufahren, die Echtzeitschutz bereitstellen. Anschließend können Sie angeben, wie lange **AVG AntiVirus** deaktiviert bleiben soll. Sie können den **AVG AntiVirus**-Schutz jederzeit erneut aktivieren – klicken Sie einfach wieder auf den Schalter.

5.7. AVG Advisor

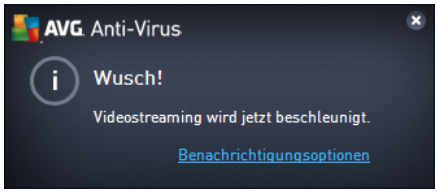
AVG Advisor erkennt Probleme, die Ihren Computer einem Risiko aussetzen, und schlägt Maßnahmen zum Beheben des Problems vor. ***AVG Advisor*** wird in Form eines gleitenden Popup-Fensters im Infobereich angezeigt. Der Dienst hat ein möglicherweise ***unbekanntes Netzwerk mit einem bekannten Namen festgestellt***. Dies trifft normalerweise nur auf Benutzer zu, die eine Verbindung zu mehreren Netzwerken herstellen, üblicherweise über tragbare Computer: Wenn ein neues, unbekanntes Netzwerk denselben Namen wie ein bekanntes, häufig verwendetes Netzwerk hat *(z. B. Home oder Mein WLAN)*, kann es zu Verwirrung kommen und es kann passieren, dass Sie aus Versehen eine Verbindung zu einem völlig unbekannten und möglicherweise nicht gesicherten Netzwerk herstellen. ***AVG Advisor*** kann dies verhindern, indem er Sie darauf hinweist, dass der vermeintlich bekannte Name tatsächlich zu einem neuen Netzwerk gehört. Wenn Sie jedoch entscheiden, dass das unbekannte Netzwerk sicher ist, können Sie es einer ***AVG Advisor***-Liste bekannter Netzwerke hinzufügen, sodass es in Zukunft nicht mehr gemeldet wird.

Unterstützte Webbrowser

Diese Funktion ist in den folgenden Webbrowsern nutzbar: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

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



6. Komponenten von AVG

6.1. Computerschutz

Die Komponente ***Computer*** enthält zwei wichtige Sicherheitsdienste: ***AntiVirus*** und ***Daten-Safe***:

- ***AntiVirus*** besteht aus einer Scan-Engine, die alle Dateien, Systembereiche des Computers und Wechselmedien *(z. B. Flash-Laufwerke)* schützt und auf bekannte Viren untersucht. Alle erkannten Viren werden blockiert, sodass sie keine Aktionen ausführen können, und anschließend bereinigt oder in die Virenquarantäne verschoben. Normalerweise merken Sie von diesem Vorgang nichts, da der Residente Schutz „im Hintergrund“ läuft. AntiVirus verwendet auch den heuristischen Scan, bei dem Dateien auf typische Virenmerkmale hin untersucht werden. Auf diese Weise kann AntiVirus neue, unbekannte Viren erkennen, wenn diese typische Merkmale eines vorhandenen Virus aufweisen. **AVG AntiVirus** ist auch in der Lage, potenziell unerwünschte ausführbare Dateien oder DLL-Bibliotheken *(verschiedene Arten von Spyware, Adware usw.)* zu analysieren und aufzuspüren. Außerdem durchsucht AntiVirus Ihre Systemregistrierung nach verdächtigen Einträgen und temporären Internetdateien und ermöglicht es Ihnen, alle potenziell unerwünschten Elemente wie jede andere Infektion zu behandeln.

- ***Data-Safe*** bietet Ihnen die Möglichkeit, sichere virtuelle Tresore zu erstellen, in denen Sie wertvolle bzw. vertrauliche Daten aufbewahren können. Der Inhalt eines Daten-Safe wird verschlüsselt und durch ein von Ihnen gewähltes Kennwort geschützt, sodass niemand ohne die entsprechende Autorisierung darauf zugreifen kann.

Steuerelemente des Dialogfelds

Um zwischen den beiden Bereichen des Dialogfelds zu wechseln, klicken Sie einfach in den entsprechenden Bereich. Der Bereich wird daraufhin in einem helleren Blau hervorgehoben. In beiden Bereichen des Dialogfelds finden Sie die folgenden Schaltflächen. Die Funktionen sind dieselben, unabhängig davon, zu welchem Sicherheitsdienst sie gehören *(AntiVirus oder Daten-Safe)*:

Aktiviert/Deaktiviert – Die Schaltfläche erinnert Sie möglicherweise an eine Ampel (sowohl das Aussehen als auch die Funktionen). Klicken Sie einmal, um zwischen den beiden Positionen zu wechseln. Grün bedeutet ***Aktiviert***, d. h. der Sicherheitsdienst von AntiVirus ist aktiviert und voll funktionsfähig. Rot bedeutet ***Deaktiviert***, d. h., der Dienst ist deaktiviert. Es wird dringend empfohlen, die Standardeinstellungen für alle Sicherheitskonfigurationen beizubehalten, sofern kein triftiger Grund besteht, den Dienst zu deaktivieren. Die Standardeinstellungen gewährleisten die optimale Leistung der Anwendung und bieten Ihnen optimalen Schutz. Wenn Sie den Dienst dennoch deaktivieren möchten, werden Sie sofort mit einem roten ***Warnzeichen*** vor möglichen Risiken gewarnt und darüber informiert, dass Sie derzeit nicht vollständig geschützt sind. ***Sie sollten den Dienst so bald wie möglich erneut aktivieren!***

Einstellungen – Klicken Sie auf die Schaltfläche, um das Dialogfeld Erweiterte Einstellungen aufzurufen. Das entsprechende Dialogfenster wird geöffnet und Sie können den ausgewählten Dienst konfigurieren, d. h. AntiVirus. Unter „Erweiterte Einstellungen“ können Sie die Konfiguration aller Dienste in **AVG AntiVirus** bearbeiten. Dies wird jedoch nur erfahrenen Benutzern empfohlen!

Pfeil – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Hauptbenutzeroberfläche mit der Komponentenübersicht zurück.

So erstellen Sie einen Daten-Safe

Im Abschnitt ***Daten-Safe*** des Dialogfelds ***Computerschutz*** finden Sie die Schaltfläche ***Safe erstellen***. Klicken Sie auf die Schaltfläche, um ein neues Dialogfeld mit derselben Bezeichnung aufzurufen, in dem Sie die Parameter Ihres geplanten Safes festlegen können. Geben Sie alle erforderlichen Informationen ein und folgen Sie den Anweisungen in der Anwendung:

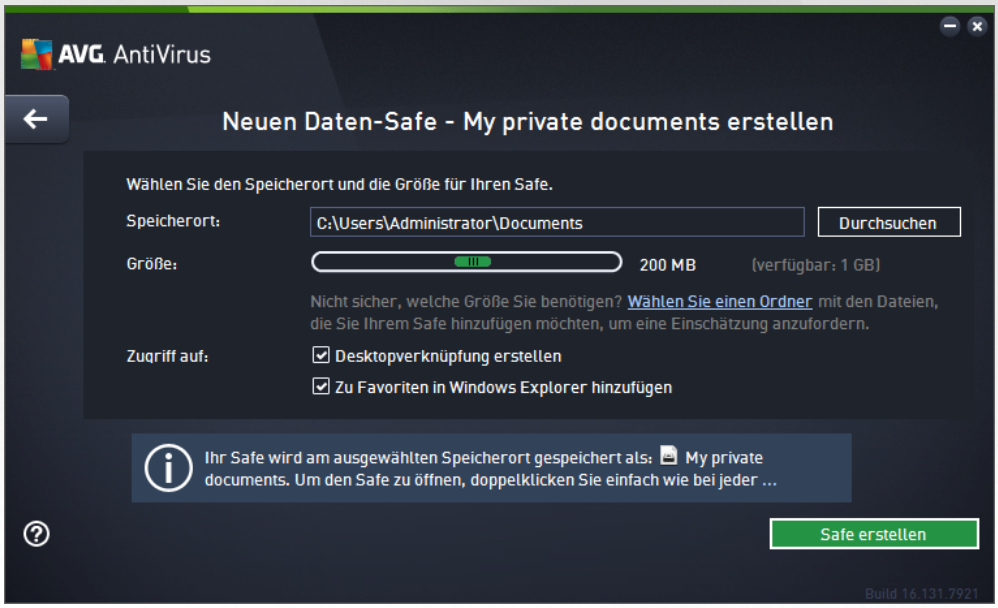
Geben Sie zuerst den Namen des Safes an und erstellen Sie ein sicheres Kennwort:

- ***Safe-Name*** – Um einen neuen Daten-Safe zu erstellen, müssen Sie zuerst einen geeigneten Safe-Namen zur Identifizierung wählen. Wenn Sie den Computer gemeinsam mit anderen Familienmitgliedern nutzen, können Sie beispielsweise Ihren Namen sowie einen Hinweis auf den Safe-Inhalt einfügen, z. B. *Papas E-Mails*.

- ***Kennwort erstellen/Kennwort erneut eingeben*** – Erstellen Sie ein Kennwort für Ihren Daten-Safe und geben Sie es in die entsprechenden Textfelder ein. Die grafische Anzeige auf der rechten Seite zeigt an, ob Ihr Kennwort einen schwachen *(mit speziellen Software-Tools relativ einfach zu knacken)* oder einen starken Schutz bietet. Es wird empfohlen, ein Kennwort zu wählen, das mindestens die Stärke „Mittel“ hat. Sie können die Sicherheit Ihres Kennworts erhöhen, indem Sie Großbuchstaben, Zahlen und andere Zeichen wie Punkte, Bindestriche usw. verwenden. Wenn Sie sich vergewissern möchten, dass Sie das Kennwort wie beabsichtigt eingeben, können Sie dies im Feld ***Kennwort anzeigen*** überprüfen *(währenddessen sollte natürlich niemand außer Ihnen selbst auf Ihren Bildschirm schauen)*.

- ***Kennworthinweis*** – Es wird dringend empfohlen, außerdem einen Kennworthinweis zu erstellen, der Sie bei Bedarf an Ihr Kennwort erinnert. Beachten Sie, dass ein Daten-Safe für die Sicherheit Ihrer Dateien sorgt, indem nur mit dem entsprechenden Kennwort auf diese zugegriffen werden kann. Das Kennwort lässt sich nicht umgehen, d. h. wenn Sie Ihr Kennwort vergessen, können Sie nicht auf Ihren Daten-Safe zugreifen!

Nachdem Sie alle erforderlichen Daten in die Textfelder eingegeben haben, klicken Sie auf die Schaltfläche ***Weiter***, um mit dem nächsten Schritt fortzufahren:



Dieser Dialog enthält die folgenden Konfigurationsoptionen:

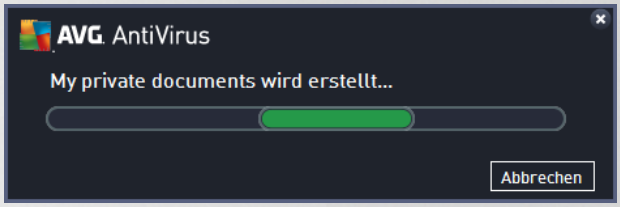
- ***Standort*** – Gibt den physischen Standort des Daten-Safe an. Durchsuchen Sie Ihre Festplatte nach einem geeigneten Ziel. Sie können den voreingestellten Speicherort, Ihren Dokumentenordner, beibehalten. Bitte beachten Sie, dass Sie nach dem Erstellen eines Daten-Safe dessen Speicherort nicht mehr ändern können.

- ***Größe*** – Sie können die Größe Ihres Daten-Safe angeben. Der erforderliche Speicherplatz auf der Festplatte wird dann zugewiesen. Dieser Wert sollte weder zu klein *(nicht ausreichend für Ihre Anforderungen)*, noch zu groß *(unnütze Belegung von Speicherplatz)* sein. Wenn Sie bereits wissen, was Sie in Ihrem Daten-Safe aufbewahren möchten, können Sie alle Dateien in einen Ordner verschieben und über den Link ***Ordner auswählen*** automatisch die Gesamtgröße berechnen. Sie können die Größe später nach Bedarf ändern.

- ***Zugriff*** – Mithilfe der Kontrollkästchen in diesem Abschnitt können Sie bequeme Verknüpfungen zu Ihrem Daten-Safe erstellen.

So verwenden Sie Ihren Daten-Safe

Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf die Schaltfläche ***Safe erstellen***. Es wird ein neues Dialogfeld ***Ihr Daten-Safe ist jetzt bereit*** angezeigt. Sie werden darüber informiert, dass der Safe zum Speichern Ihrer Dateien verfügbar ist. Bei jedem weiteren Versuch, auf den Safe zuzugreifen, müssen Sie den Safe mit dem von Ihnen definierten Kennwort öffnen:



Um den neuen Daten-Safe zu verwenden, müssen Sie ihn zunächst öffnen – klicken Sie auf ***Jetzt öffnen***. Beim Öffnen wird der Daten-Safe auf Ihrem Computer als neuer virtueller Datenträger angezeigt. Weisen Sie ihm einen beliebigen Buchstaben aus dem Dropdown-Menü zu (*Sie können nur derzeit freie Datenträger auswählen*). In der Regel stehen C *(üblicherweise Ihrer Festplatte zugeordnet)*, A *(Diskettenlaufwerk)*oder D *(DVD-Laufwerk)* nicht zur Verfügung. Sie können jedes Mal, wenn Sie einen Daten-Safe entsperren, einen anderen verfügbaren Laufwerksbuchstaben auswählen.

So entsperren Sie Ihren Daten-Safe

Beim nächsten Versuch, auf den Daten-Safe zuzugreifen, müssen Sie den Safe mit dem von Ihnen definierten Kennwort öffnen:

Geben Sie im Textfeld Ihr Kennwort ein, um sich selbst zu autorisieren, und klicken Sie dann auf die Schaltfläche ***Entsperren***. Wenn Sie das Kennwort vergessen haben, klicken Sie auf ***Hinweis***, um den Kennworthinweis anzuzeigen, den Sie beim Erstellen des Daten-Safe angegeben haben. Der neue Daten-Safe wird in der Übersicht Ihrer Daten-Safes als ENTSPERRT angezeigt, und Sie können nach Bedarf Dateien hinzufügen/entfernen.

6.2. Schutz beim Surfen im Web

Der ***Schutz beim Surfen im Web*** besteht aus zwei Diensten: ***LinkScanner Surf-Shield*** und ***Online Shield***:

- ***Link Scanner Surf-Shield*** schützt vor der steigenden Anzahl kurzlebiger Bedrohungen aus dem Internet. Gefahren können sich auf jeder Art von Website verbergen, egal ob es sich um Seiten von Regierungsbehörden, großen und bekannten Markenfirmen oder Kleinbetrieben handelt. Und sie verweilen dort selten länger als 24 Stunden. Link Scanner sorgt für den nötigen Schutz durch Analyse aller sich hinter einem Link verbergenden Webseiten. Das garantiert den gewünschten Schutz im entscheidenden Moment: nämlich kurz bevor Sie auf den Link klicken. ***Link Scanner Surf-Shield ist nicht für den Schutz von Serverplattformen vorgesehen!***

- ***Online Shield*** ist eine Art von Echtzeitschutz. Der Inhalt besuchter Webseiten (und möglicher enthaltener Dateien) wird gescannt, noch bevor diese Inhalte in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen werden. Online Shield erkennt, ob eine Seite, die Sie gerade besuchen, gefährliches Javascript enthält, und verhindert die Anzeige der Seite. Die Komponente erkennt auch die auf einer Seite enthaltene Malware, stoppt automatisch das Herunterladen und sorgt so dafür, dass sie niemals auf Ihren Computer gelangt. Diese leistungsfähige Schutzfunktion sorgt dafür, dass bösartige Inhalte von jeder Webseite, die Sie öffnen möchten, blockiert und nicht auf Ihren Computer heruntergeladen werden. Wenn diese Funktion aktiviert ist und Sie auf einen gefährlichen Link klicken oder die Internetadresse einer gefährlichen Site eingeben, wird die entsprechende Webseite automatisch blockiert, damit sich Ihr Computer nicht infiziert. Denken Sie daran, dass Website-Exploits Ihren Computer bereits infizieren können, wenn Sie einfach nur die entsprechende Website besuchen. ***Online Shield ist nicht für den Schutz von Serverplattformen vorgesehen!***

Steuerelemente des Dialogfelds

Um zwischen den beiden Bereichen des Dialogfelds zu wechseln, klicken Sie einfach in den entsprechenden Bereich. Der Bereich wird daraufhin in einem helleren Blau hervorgehoben. In beiden Bereichen des Dialogfelds finden Sie die folgenden Schaltflächen. Die Funktionen sind dieselben, unabhängig davon, zu welchem Sicherheitsdienst sie gehören *(Link Scanner Surf-Shield oder Online Shield)*:

Aktiviert/Deaktiviert – Die Schaltfläche erinnert Sie möglicherweise an eine Ampel (sowohl das Aussehen als auch die Funktionen). Klicken Sie einmal, um zwischen den beiden Positionen zu wechseln. Grün bedeutet ***Aktiviert***, d. h. Link Scanner Surf-Shield/Online Shield ist aktiviert und voll funktionsfähig. Rot bedeutet ***Deaktiviert***, d. h., der Dienst ist deaktiviert. Es wird dringend empfohlen, die Standardeinstellungen für alle Sicherheitskonfigurationen beizubehalten, sofern kein triftiger Grund besteht, den Dienst zu deaktivieren. Die Standardeinstellungen gewährleisten die optimale Leistung der Anwendung und bieten Ihnen optimalen Schutz. Wenn Sie den Dienst dennoch deaktivieren möchten, werden Sie sofort mit einem roten ***Warnzeichen*** vor möglichen Risiken gewarnt und darüber informiert, dass Sie derzeit nicht vollständig geschützt sind. ***Sie sollten den Dienst so bald wie möglich erneut aktivieren!***

Einstellungen – Klicken Sie auf die Schaltfläche, um das Dialogfeld Erweiterte Einstellungen aufzurufen. Das Dialogfenster wird geöffnet, und Sie können den gewählten Dienst konfigurieren, d. h. Link Scanner Surf-Shield oder Online Shield. Unter „Erweiterte Einstellungen“ können Sie die Konfiguration aller Dienste in **AVG AntiVirus** bearbeiten. Dies wird jedoch nur erfahrenen Benutzern empfohlen!

Pfeil – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Hauptbenutzeroberfläche mit der Komponentenübersicht zurück.

6.3. Software Analyzer

Die Komponente ***Software Analyzer*** schützt Ihre digitalen Daten dauerhaft vor neuen und unbekannten Bedrohungen aus dem Internet:

- ***Software Analyzer*** ist ein Anti-Malware-Dienst, der Sie mithilfe verhaltensbasierter Technologien vor allen Arten von Malware (*Spyware, Bots oder Identitätsdiebstahl*) schützt, und der Zero-Day-Schutz verhindert, dass Ihr Computer mit neuen Viren infiziert wird. Identity Protection ist darauf ausgerichtet, Identitätsdiebe daran zu hindern, Ihre Kennwörter, die Zugangsdaten zu Ihrem Bankkonto, Kreditkartennummern und andere persönliche und vertrauliche Daten mithilfe verschiedener schädlicher Software *(Malware)* von Ihrem PC zu stehlen. Er stellt sicher, dass alle auf Ihrem Computer oder Ihrem freigegebenen Netzwerk ausgeführten Programme ordnungsgemäß funktionieren. Software Analyzer erkennt und blockiert kontinuierlich verdächtiges Verhalten und schützt Ihren Computer vor neuer Malware. Software Analyzer gewährt Ihrem Computer Echtzeitschutz vor neuen und unbekannten Bedrohungen. Die Komponente überwacht alle *(auch versteckte)* Prozesse und mehr als 285 verschiedene Verhaltensmuster. Außerdem kann sie erkennen, wenn auf Ihrem Computer ein schädlicher Vorgang ausgeführt wird. Aus diesem Grund kann die Komponente Bedrohungen erkennen, noch bevor sie in der Virendatenbank beschrieben sind. Jedes Mal, wenn ein unbekannter Code auf Ihrem Computer auftritt, wird er sofort auf schädliches Verhalten überprüft und aufgezeichnet. Falls die Datei als schädlich erachtet wird, verschiebt Software Analyzer den Code in die Virenquarantäne und macht alle Änderungen rückgängig, die am System durchgeführt wurden *(Codeeinschleusungen, Registrierungsänderungen, Öffnen von Ports usw.)*. Sie müssen keinen Scan starten, um geschützt zu sein. Diese Technologie ist sehr proaktiv, muss selten aktualisiert werden und ist immer aktiv.

Steuerelemente des Dialogfelds

In dem Dialogfeld finden Sie die folgenden Schaltflächen:

Aktiviert/Deaktiviert – Die Schaltfläche erinnert Sie möglicherweise an eine Ampel (sowohl das Aussehen als auch die Funktionen). Klicken Sie einmal, um zwischen den beiden Positionen zu wechseln. Grün bedeutet ***Aktiviert***, d. h. der Sicherheitsdienst von Software Analyzer ist aktiviert und voll funktionsfähig. Rot bedeutet ***Deaktiviert***, d. h., der Dienst ist deaktiviert. Es wird dringend empfohlen, die Standardeinstellungen für alle Sicherheitskonfigurationen beizubehalten, sofern kein triftiger Grund besteht, den Dienst zu deaktivieren. Die Standardeinstellungen gewährleisten die optimale Leistung der Anwendung und bieten Ihnen optimalen Schutz. Wenn Sie den Dienst dennoch deaktivieren möchten, werden Sie sofort mit einem roten ***Warnzeichen*** vor möglichen Risiken gewarnt und darüber informiert, dass Sie derzeit nicht vollständig geschützt sind. ***Sie sollten den Dienst so bald wie möglich erneut aktivieren!***

Einstellungen – Klicken Sie auf die Schaltfläche, um das Dialogfeld Erweiterte Einstellungen aufzurufen. Das entsprechende Dialogfenster wird geöffnet und Sie können den ausgewählten Dienst konfigurieren, d. h. Software Analyzer. Unter „Erweiterte Einstellungen“ können Sie die Konfiguration aller Dienste in **AVG AntiVirus** bearbeiten. Dies wird jedoch nur erfahrenen Benutzern empfohlen!

Pfeil – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Hauptbenutzeroberfläche mit der Komponentenübersicht zurück.

Leider ist Identity Alert in **AVG AntiVirus** nicht enthalten. Wenn Sie diese Art des Schutzes wünschen, klicken Sie auf die Schaltfläche ***Zum Aktivieren aktualisieren***, um auf die entsprechende Website weitergeleitet zu werden, auf der Sie die Lizenz für Identity Alert erwerben können.

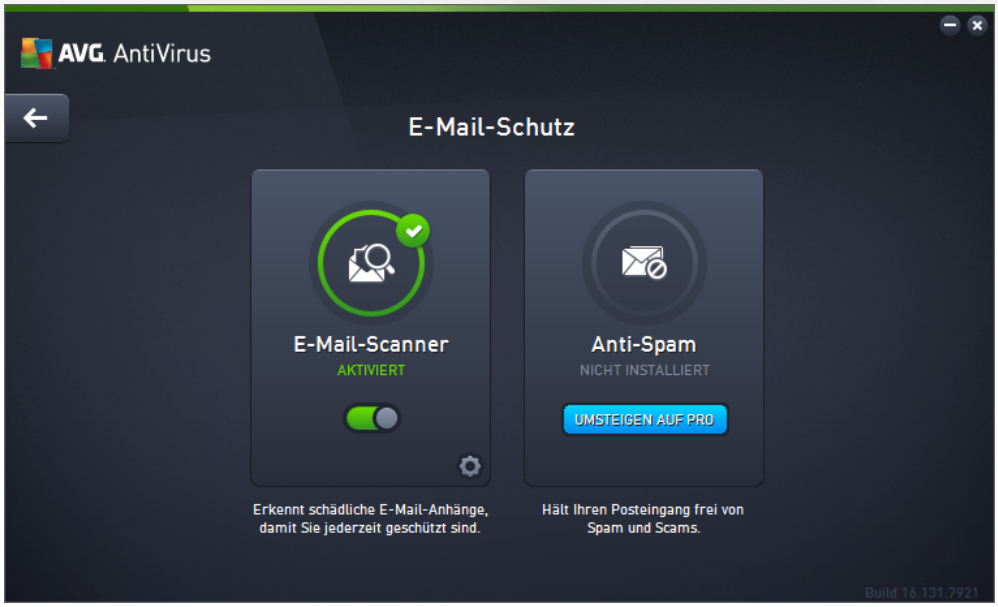
Bitte beachten Sie, dass selbst bei den AVG Premium Security-Editionen der Identity Alert-Dienst derzeit nur in ausgewählten Regionen verfügbar ist: USA, Großbritannien, Kanada und Irland.

6.4. E-Mail-Schutz

Die Komponente ***E-Mail-Schutz*** deckt die beiden folgenden Sicherheitsdienste ab: ***E-Mail-Scanner*** und ***Anti-Spam*** *(Anti-Spam ist nur für Internet Security und Premium Security verfügbar)*.

- ***E-Mail-Scanner***: E-Mails sind eine der häufigsten Quellen von Viren und Trojanern. E-Mail-Nachrichten können jedoch in Form von Phishing und Spam noch weitere Risiken in sich bergen. Kostenlose E-Mail-Konten sind häufiger solchen schädlichen E-Mails ausgesetzt *(da nur selten Technologie für Anti-Spam eingesetzt wird)*; solche Konten werden vor allem von privaten Benutzer verwendet. Durch das Aufsuchen unbekannter Websites sowie das Ausfüllen von Online-Formularen mit persönlichen Daten (*inklusive E-Mail-Adresse*) erhöht sich für private Benutzer das Risiko, Opfer eines Angriffs via E-Mail zu werden. Unternehmen nutzen in der Regel eigene E-Mail-Konten und verwenden Anti-Spam-Filter, um die beschriebenen Risiken zu minimieren. Die E-Mail-Schutz-Komponente scannt jede E-Mail-Nachricht, die Sie senden oder empfangen. Wenn in einer E-Mail ein Virus erkannt wird, wird sie sofort in die Virenquarantäne verschoben. Die Komponente kann auch bestimmte Arten von E-Mail-Anhängen filtern und einen Zertifizierungstext zu nicht infizierten Nachrichten hinzufügen. ***E-Mail-Scanner ist nicht für Serverplattformen vorgesehen!***

- ***Anti-Spam*** überprüft alle eingehenden E-Mails und markiert unerwünschte E-Mails als Spam *(als Spam gelten unerwünschte E-Mails, meistens Werbung für einen Dienst oder ein Produkt, die an zahlreiche E-Mail-Adressen gleichzeitig gesendet werden und den Posteingang füllen. Legitime Werbemails, für die der Verbraucher sein Einverständnis gegeben hat, fallen nicht in diese Kategorie.)* Anti-Spam kann den Betreff einer E-Mail *(die als Spam eingestuft worden ist)* durch das Hinzufügen einer speziellen Zeichenfolge ändern. So können Sie Ihre E-Mails in Ihrem E-Mail-Client bequem filtern. AVG Anti-Spam verwendet verschiedene Analysemethoden, um die einzelnen E-Mails zu verarbeiten und bietet damit optimalen Schutz vor unerwünschten E-Mail-Nachrichten. Anti-Spam nutzt zur Erkennung von Spam eine Datenbank, die in regelmäßigen Abständen aktualisiert wird. Sie können auch RBL-Server verwenden *(öffentliche Datenbanken, in denen „bekannte Spam-Absender" erfasst sind)* und E-Mail-Adressen manuell zu Ihrer Whitelist *(E-Mails von diesen Absendern nie als Spam kennzeichnen)* oder zu Ihrer Blacklist *(immer als Spam kennzeichnen) hinzufügen*.



Steuerelemente des Dialogfelds

Um zwischen den beiden Bereichen des Dialogfelds zu wechseln, klicken Sie einfach in den entsprechenden Bereich. Der Bereich wird daraufhin in einem helleren Blau hervorgehoben. In beiden Bereichen des Dialogfelds finden Sie die folgenden Schaltflächen. Die Funktionen sind dieselben, unabhängig davon, zu welchem Sicherheitsdienst sie gehören *(E-Mail-Scanner oder Anti-Spam)*:

Aktiviert/Deaktiviert – Die Schaltfläche erinnert Sie möglicherweise an eine Ampel (sowohl das Aussehen als auch die Funktionen). Klicken Sie einmal, um zwischen den beiden Positionen zu wechseln. Grün bedeutet ***Aktiviert***, d. h., der Sicherheitsdienst ist aktiviert und voll funktionsfähig. Rot bedeutet ***Deaktiviert***, d. h., der Dienst ist deaktiviert. Es wird dringend empfohlen, die Standardeinstellungen für alle Sicherheitskonfigurationen beizubehalten, sofern kein triftiger Grund besteht, den Dienst zu deaktivieren. Die Standardeinstellungen gewährleisten die optimale Leistung der Anwendung und bieten Ihnen optimalen Schutz. Wenn Sie den Dienst dennoch deaktivieren möchten, werden Sie sofort mit einem roten ***Warnzeichen*** vor möglichen Risiken gewarnt und darüber informiert, dass Sie derzeit nicht vollständig geschützt sind. ***Sie sollten den Dienst so bald wie möglich erneut aktivieren!***

Einstellungen – Klicken Sie auf die Schaltfläche, um das Dialogfeld Erweiterte Einstellungen aufzurufen. Das entsprechende Dialogfenster wird geöffnet und Sie können den ausgewählten Dienst konfigurieren, d. h. E-Mail-Scanner oder Anti-Spam. Unter „Erweiterte Einstellungen“ können Sie die Konfiguration aller Dienste in **AVG AntiVirus** bearbeiten. Dies wird jedoch nur erfahrenen Benutzern empfohlen!

Pfeil – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Hauptbenutzeroberfläche mit der Komponentenübersicht zurück.

6.5. PC Analyzer

Die Komponente ***PC Analyzer*** ist ein leistungsstarkes Tool zur detaillierten Systemanalyse und Optimierung der Geschwindigkeit und Gesamtleistung Ihres Computers. Sie kann über die Schaltfläche ***Leistungsprobleme beheben*** in der Hauptbenutzeroberfläche oder über die gleiche Option im Kontextmenü des AVG-Symbols im Infobereich geöffnet werden. Sie können den Analysefortschritt nachvollziehen und die Ergebnisse der Analyse direkt im Diagramm sehen:

Die folgenden Kategorien können analysiert werden: Registrierungsfehler, Junk-Dateien, Fragmentierung und beschädigte Verknüpfungen:

- ***Registrierungsfehler*** gibt die Anzahl der Fehler in der Windows-Registrierung an, die Ihren Computer möglicherweise verlangsamen oder zur Anzeige von Fehlermeldungen führen.
- ***Junk-Dateien*** gibt die Anzahl der Dateien an, die Ihren Festplattenspeicher aufbrauchen und wahrscheinlich unnötig sind. Dazu gehören typischerweise temporäre Dateien und Dateien, die sich im Papierkorb befinden.
- ***Fragmentierung*** berechnet die Fragmentierung Ihrer Festplatte in Prozent, d. h. Daten, die schon lange verwendet werden und über verschiedene Teile der physischen Festplatte verteilt sind.
- ***Beschädigte Verknüpfungen*** sucht Verknüpfungen, die beispielsweise nicht mehr funktionieren oder auf nicht vorhandene Speicherorte verweisen.

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

Schaltflächen

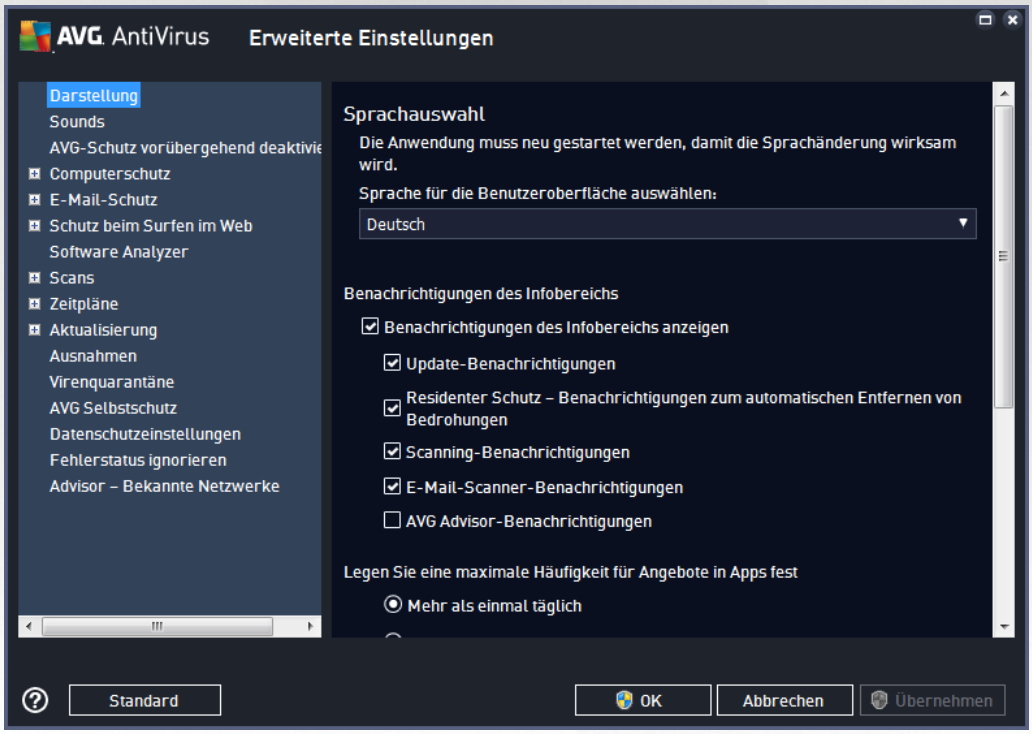
- ***Analyse stoppen*** (*wird während der Analyse angezeigt*) – Klicken Sie auf diese Schaltfläche, um die Analyse Ihres Computers zu unterbrechen.
- ***Fehler jetzt beheben*** *(wird nach Abschluss der Analyse angezeigt*) – Leider ist die Funktion von PC Analyzer in **AVG AntiVirus** auf die Analyse des aktuellen PC-Status beschränkt. AVG bietet jedoch ein leistungsstarkes Tool zur detaillierten Systemanalyse und Optimierung der Geschwindigkeit und Gesamtleistung Ihres Computers. Klicken Sie auf die Schaltfläche, um weitere Informationen auf der zugehörigen Website anzuzeigen.

7. Erweiterte Einstellungen von AVG

Der Dialog zur erweiterten Konfiguration von **AVG AntiVirus** 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 aus, deren Konfiguration Sie ändern möchten (*oder einen bestimmten Teil*), damit das Dialogfeld zum Bearbeiten rechts im Fenster geöffnet wird.

7.1. Darstellung

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



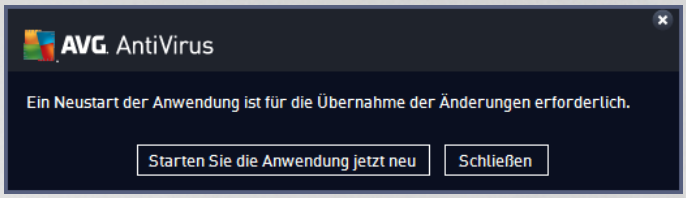
Sprachauswahl

Im Abschnitt ***Sprachauswahl*** können Sie Ihre gewünschte Sprache aus dem Dropdown-Menü auswählen. Die ausgewählte Sprache wird dann für die gesamte **AVG AntiVirus**-Benutzeroberfläche verwendet. Im Dropdown-Menü werden nur die Sprachen angeboten, die Sie während des Installationsprozesses ausgewählt haben, sowie Englisch (*Englisch wird standardmäßig automatisch installiert*). Um die Umstellung von **AVG AntiVirus** auf eine andere Sprache abzuschließen, müssen Sie die Anwendung neu starten. Gehen Sie wie folgt vor:

- Wählen Sie im Dropdown-Menü die gewünschte Sprache der Anwendung aus.
- Bestätigen Sie Ihre Auswahl durch Klicken auf die Schaltfläche ***Übernehmen*** *(untere rechte Ecke des Dialogfelds).*
- Klicken Sie zum Bestätigen auf die Schaltfläche ***OK***.

- Ein neuer Dialog wird angezeigt, der Sie darüber informiert, dass Sie **AVG AntiVirus** νευ σταρτεν μ]σσεν, υμ διε Σπραχηε δερ Ανωενδυνγ ζυ ™νδερν.

- Klicken Sie auf die Schaltfläche ***Starten Sie AVG jetzt neu***, um den Programmneustart zu bestätigen, und warten Sie eine Sekunde, damit die Sprache übernommen wird:



Benachrichtigungen des Infobereichs

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

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

- ***Benachrichtigungen des Infobereichs anzeigen*** *(standardmäßig aktiviert)* – Standardmäßig werden alle Benachrichtigungen angezeigt. Heben Sie die Markierung dieses Eintrags auf, um die Anzeige aller Systembenachrichtigungen zu deaktivieren. Wenn diese Funktion aktiviert ist, können Sie auswählen, welche Benachrichtigungen angezeigt werden sollen:

    - ***Update-Benachrichtigungen*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zum Start, Fortschritt und Abschluss des Updatevorgangs von **AVG AntiVirus** angezeigt werden sollen.

    - ***Residenter Schutz – Benachrichtigungen zum automatischen Entfernen von Bedrohungen*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zum Speichern, Kopieren und Öffnen von Dateien angezeigt werden sollen (*diese Konfiguration wird nur angezeigt, wenn die Option zum automatischen Heilen des Residenten Schutzes aktiviert ist*).

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

    - ***E-Mail-Scanner-Benachrichtigungen*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zur Überprüfung aller eingehenden und ausgehenden E-Mails angezeigt werden sollen.

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

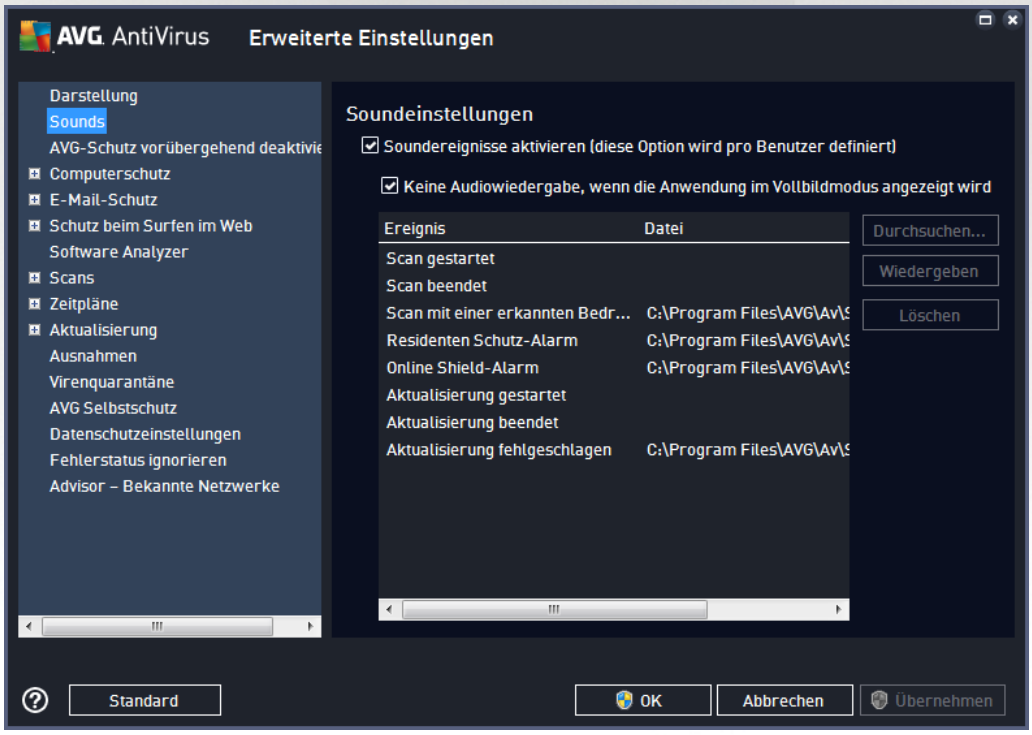
- ***AVG Advisor-Benachrichtigungen*** *(standardmäßig aktiviert)* – Legen Sie fest, ob Informationen zu den Aktivitäten von AVG Advisor im Popup-Fenster in der Taskleiste angezeigt werden sollen.

Spielemodus

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 ***Spielemodus bei Ausführung einer Anwendung im Vollbildmodus aktivieren*** aktiviert lassen (*Standardeinstellung*).

7.2. Sounds

Im Dialogfeld ***Soundeinstellungen*** können Sie festlegen, ob Sie bei bestimmten Aktionen von **AVG AntiVirus** per Soundbenachrichtigung informiert werden möchten:



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

Schaltflächen

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

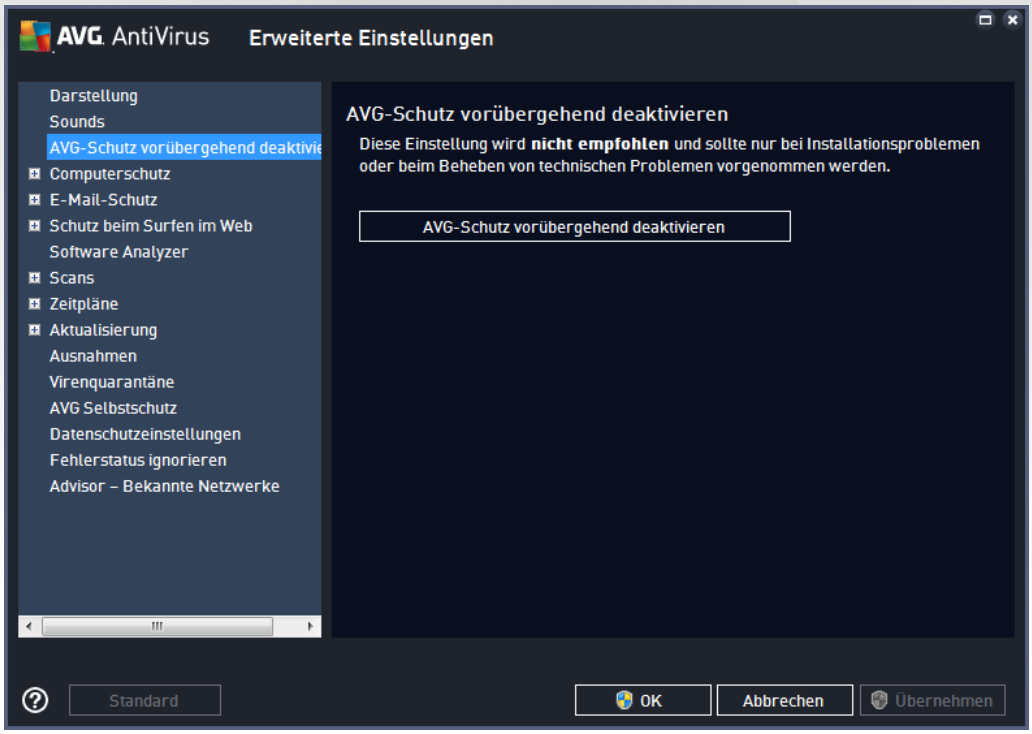
- ***Wiedergeben*** – Um den ausgewählten Sound anzuhören, markieren Sie das Ereignis in der Liste und klicken Sie auf die Schaltfläche ***Wiedergeben***.

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

7.3. AVG-Schutz vorübergehend deaktivieren

Im Dialogfeld ***AVG-Schutz vorübergehend deaktivieren*** können Sie alle Schutzfunktionen von **AVG AntiVirus** gleichzeitig deaktivieren.

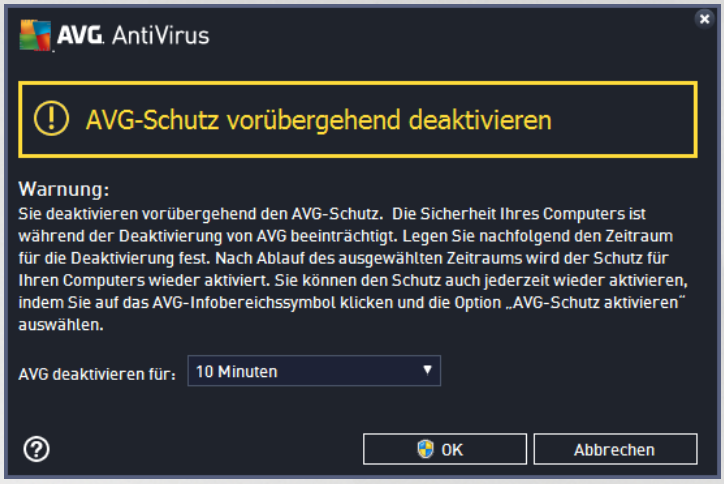
Verwenden Sie diese Option nur, wenn es unbedingt erforderlich ist.



In der Regel ***müssen*** Sie **AVG AntiVirus** nicht deaktivieren, bevor Sie neue Software oder Treiber installieren, auch wenn das Installationsprogramm oder der Software-Assistent darauf hinweist, dass laufende Programme und Anwendungen beendet werden sollten, um den Installationsvorgang ohne Unterbrechungen abzuschließen. Falls während der Installation tatsächlich Probleme auftreten, deaktivieren Sie den Residenten Schutz *(deaktivieren Sie zunächst im verknüpften Dialogfenster das Element **Residenten Schutz aktivieren**)*. Wenn Sie **AVG AntiVirus** vorübergehend deaktivieren müssen, sollten Sie es so bald wie möglich wieder aktivieren. Ihr Computer ist Bedrohungen ausgesetzt, wenn Sie bei deaktiviertem Virenschutz mit dem Internet oder einem Netzwerk verbunden sind.

So deaktivieren Sie den AVG-Schutz

Aktivieren Sie das Kontrollkästchen ***AVG-Schutz vorübergehend deaktivieren*** und bestätigen Sie Ihre Auswahl über die Schaltfläche ***Übernehmen***. Legen Sie im neu geöffneten Dialog ***AVG-Schutz vorübergehend deaktivieren*** fest, wie lange Sie **AVG AntiVirus** deaktivieren möchten. Der Schutz wird standardmäßig für 10 Minuten deaktiviert, was für allgemeine Aufgaben wie die Installation neuer Software usw. ausreichend sein sollte. Sie können auch einen längeren Zeitraum wählen, doch diese Option wird nicht empfohlen, wenn dies nicht unbedingt erforderlich ist. Anschließend werden alle deaktivierten Komponenten automatisch wieder aktiviert. Sie können den AVG-Schutz maximal bis zum nächsten Computerneustart deaktivieren.



7.4. Computerschutz

7.4.1. AntiVirus

AntiVirus und ***Residenter Schutz*** schützen Ihren Computer dauerhaft vor allen bekannten Virentypen, Spyware und Malware im Allgemeinen *(z. B. sogenannte ruhende und nicht aktive Malware. Dabei handelt es sich um Malware, die heruntergeladen, jedoch noch nicht aktiviert wurde)*.

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

- ***Vor dem Entfernen von Bedrohungen Bestätigung anfordern*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, um sicherzugehen, dass Residenter Schutz nicht automatisch eine Aktion ausführt. Stattdessen wird ein Dialogfeld mit einer Beschreibung der erkannten Bedrohung angezeigt, sodass Sie sich für eine geeignete Maßnahme entscheiden können. Sofern Sie das Feld deaktiviert lassen, werden Infektionen von **AVG AntiVirus** automatisch entfernt. Wenn dies nicht möglich ist, wird das Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

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

- ***Dateien beim Schließen scannen*** (*standardmäßig deaktiviert*) – Diese Option sorgt dafür, dass AVG aktive Objekte (z. B. Anwendungen oder Dokumente) sowohl beim Öffnen als auch beim Schließen scannt. Durch diese Funktion ist Ihr Computer auch vor besonders hinterlistigen Virenarten geschützt.

- ***Boot-Sektor des Wechselmediums scannen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um den Boot-Sektor von verbundenen USB-Flashlaufwerken, externen Festplatten und anderen Wechseldatenträgern auf Bedrohungen zu scannen.

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

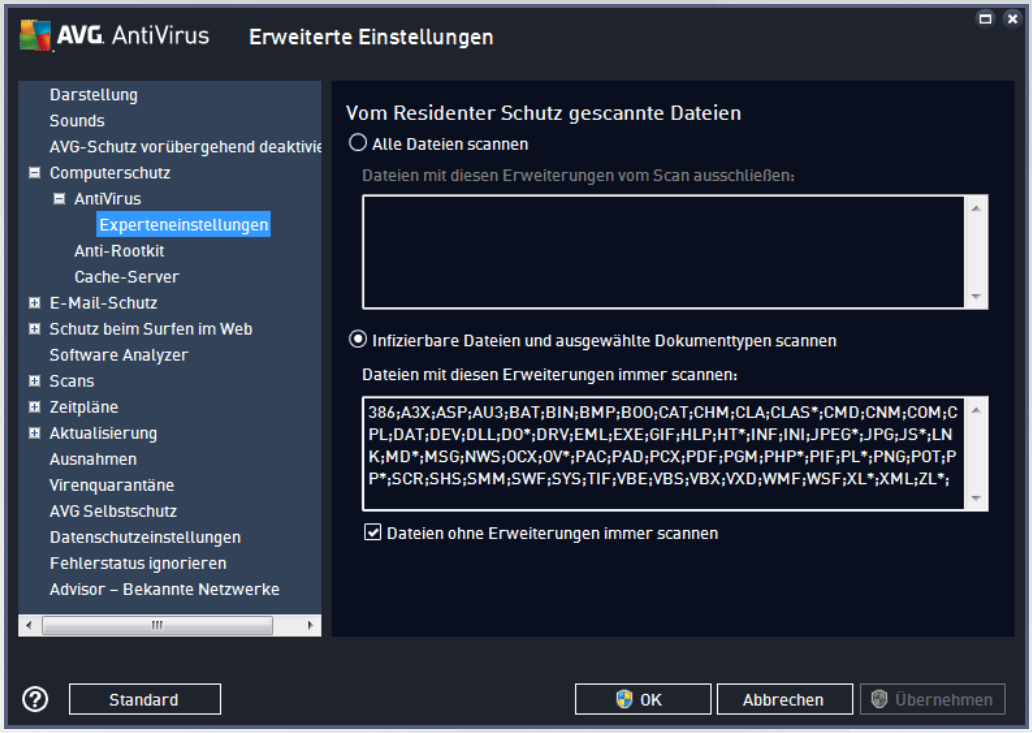
- ***Dateien scannen, auf die in der Registrierung verwiesen wird*** (*standardmäßig aktiviert*) – Mit diesem Parameter wird festgelegt, dass AVG alle ausführbaren Dateien der Startup-Registrierung scannt, um zu verhindern, dass eine bekannte Infektion beim nächsten Computerstart ausgeführt wird.

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

- ***Instant Messaging-Schutz und P2P-Downloadschutz aktivieren*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option zum Überprüfen der Virenfreiheit von Kommunikation über Instant Messaging (*AIM, Yahoo!, MSN Messenger, ICQ, Skype usw.*) und von Daten, die über Peer-to-Peer-Netzwerke heruntergeladen wurden. (*P2P-Netzwerke stellen eine direkte Verbindung zwischen Clients her, ohne einen Server zu verwenden, was gefährlich sein kann. Sie werden häufig zur Freigabe von Musikdateien genutzt.*)

Hinweis: *Wenn AVG unter Windows 10 installiert wird, ist eine weitere Option* ***Windows Antimalware Scan Interface (AMSI) für ausführlichere Software-Scans aktivieren*** *in der Liste vorhanden. Durch diese Funktion wird der Virenschutz verbessert, da durch die engere Zusammenarbeit zwischen Windows und AVG schädlicher Code festgestellt werden kann, wodurch der Schutz zuverlässiger und die Anzahl der Fehlalarme verringert wird.*

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

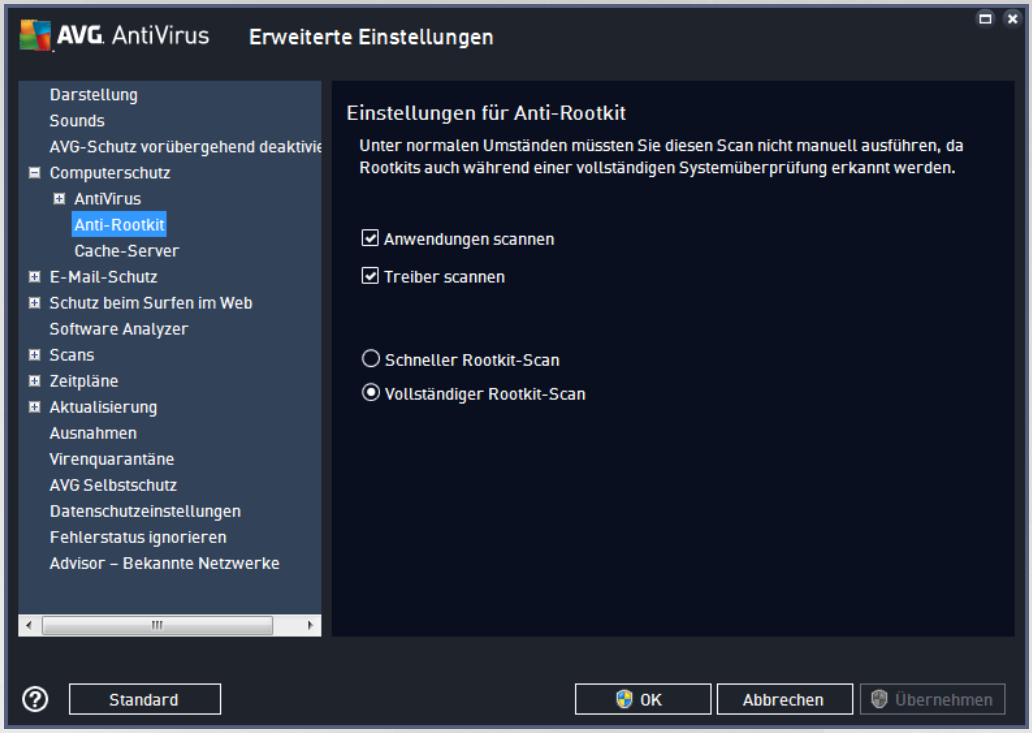


Aktivieren Sie das entsprechende Kontrollkästchen, um festzulegen, ob Sie ***Alle Dateien scannen*** oder nur ***Infizierbare Dateien und ausgewählte Dokumenttypen scannen*** möchten. Um den Scan-Vorgang zu beschleunigen und gleichzeitig den höchstmöglichen Schutz zu gewährleisten, empfehlen wir Ihnen, die Standardeinstellungen beizubehalten. So werden nur potenziell infizierte Dateien gescannt. Im entsprechenden Bereich des Dialogfeldes finden Sie eine bearbeitbare Liste mit Erweiterungen und den dazugehörigen Dateien, die im Scan enthalten sind.

Aktivieren Sie ***Dateien ohne Erweiterungen immer scannen*** (*standardmäßig aktiviert*) und sorgen Sie so dafür, dass alle Dateien ohne Erweiterung oder mit unbekanntem Format vom Residenten Schutz gescannt werden. Wir empfehlen, diese Funktion aktiviert zu lassen, da Dateien ohne Erweiterung verdächtig sind.

7.4.2. Anti-Rootkit

Im Dialogfeld ***Einstellungen für Anti-Rootkit*** können Sie die Konfiguration der ***Anti-Rootkit***-Komponente und spezifische Parameter für Anti-Rootkit-Scans bearbeiten. Der Anti-Rootkit-Scan ist ein Standardprozess beim Scan des gesamten Computers:

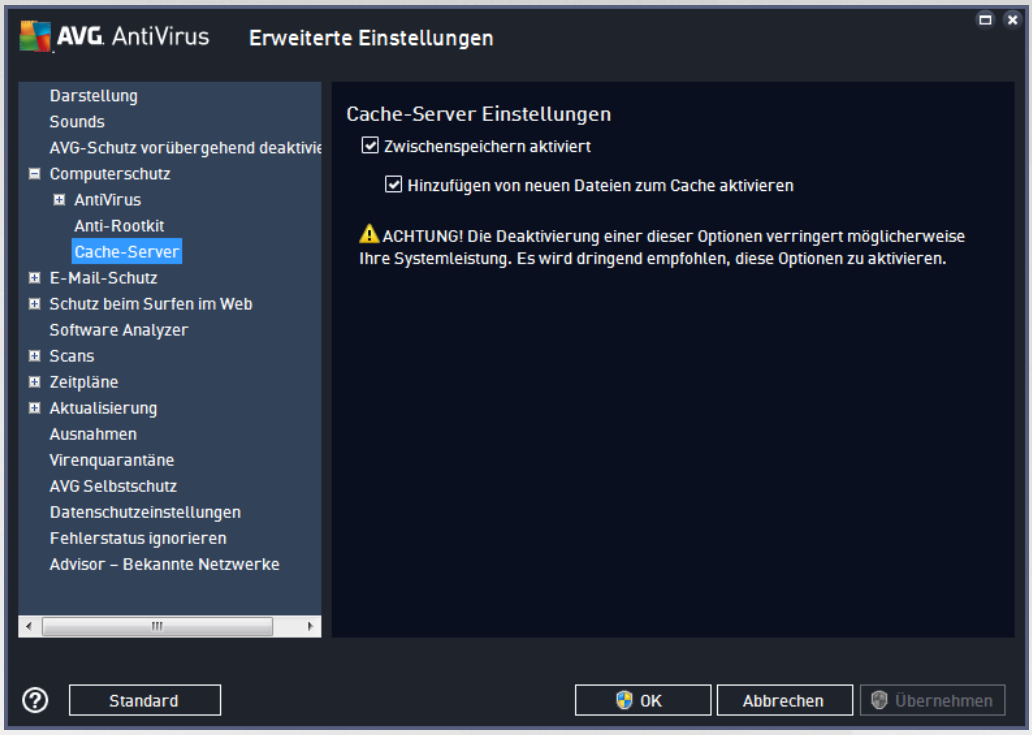


Mit ***Anwendungen scannen*** und ***Treiber scannen*** können Sie detailliert angeben, was im Anti-Rootkit-Scan enthalten sein soll. Diese Konfigurationsmöglichkeiten sind für erfahrene Benutzer gedacht. Es wird empfohlen, keine der Optionen zu deaktivieren. Sie können auch den Rootkit-Scanmodus auswählen:

- ***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*).

7.4.3. Cache-Server

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



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

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

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

- ***Hinzufügen von neuen Dateien zum Cache aktivieren*** (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, damit dem Zwischenspeicher keine weiteren Dateien hinzugefügt werden. Dateien, die sich bereits im Zwischenspeicher befinden, bleiben darin enthalten und werden bis zum nächsten Update der Virendatenbank oder bis zum vollständigen Ausschalten des Zwischenspeichers weiter verwendet.

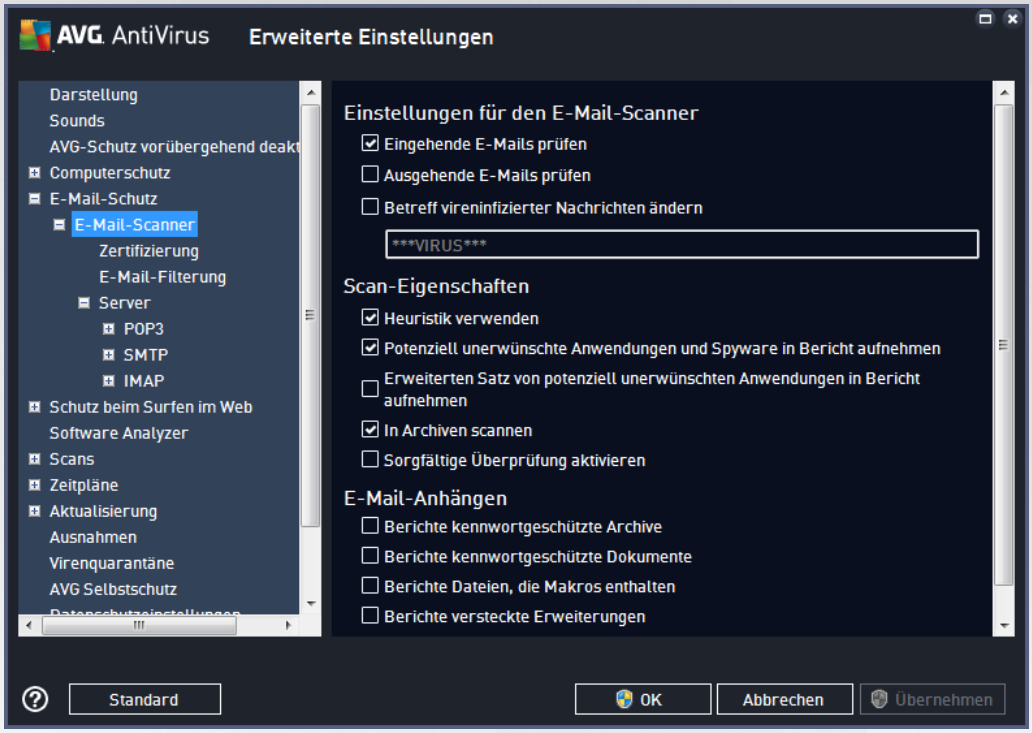
Wir empfehlen dringend, die Standardeinstellungen beizubehalten und beide Optionen aktiviert zu lassen, es sei denn, es besteht ein triftiger Grund, den Cache-Server zu deaktivieren. Andernfalls können Leistung und Geschwindigkeit Ihres Systems deutlich abnehmen.

7.5. E-Mail-Scanner

In diesem Bereich können Sie die detaillierte Konfiguration von E-Mail-Scanner und Anti-Spam bearbeiten:

7.5.1. E-Mail-Scanner

Der Dialog ***E-Mail-Scanner*** ist in drei Bereiche unterteilt:



E-Mail-Scan

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

- ***Eingehende E-Mails prüfen*** (*standardmäßig aktiviert*) – Aktivieren/deaktivieren Sie diese Option, um alle an Ihren E-Mail-Client gesendeten Nachrichten zu scannen bzw. nicht zu scannen.
- ***Ausgehende E-Mails prüfen*** (*standardmäßig deaktiviert*) – Aktivieren/deaktivieren Sie diese Option, um alle von Ihrem Konto gesendeten E-Mails zu scannen bzw. nicht zu scannen.
- ***Betreff vireninfizierter Nachrichten ändern*** *(standardmäßig deaktiviert*) – Wenn Sie gewarnt werden möchten, dass beim Scannen eine infizierte E-Mail erkannt wurde, aktivieren Sie diesen Eintrag, und geben Sie im Textfeld den gewünschten Text ein. Dieser Text wird dem Betreff jeder infizierten E-Mail-Nachricht hinzugefügt , um die Identifikation und Filterung zu erleichtern. Der Standardtext lautet ***VIRUS***. Wir empfehlen, diesen beizubehalten.

Scan-Eigenschaften

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

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

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

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

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

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

Berichte über E-Mail-Anhänge

In diesem Bereich können Sie zusätzliche Berichte über Dateien einrichten, die potenziell gefährlich oder verdächtig sind. Bitte beachten Sie, dass keine Warnmeldung angezeigt, sondern nur ein Bestätigungstext an das Ende der E-Mail-Nachricht angehängt wird. Alle derartigen Berichte werden im Dialog E-Mail-Schutz aufgelistet:

- ***Berichte kennwortgeschützte Archive*** – Archive (*ZIP, RAR usw.*), die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Archive als potenziell gefährlich anzuzeigen.

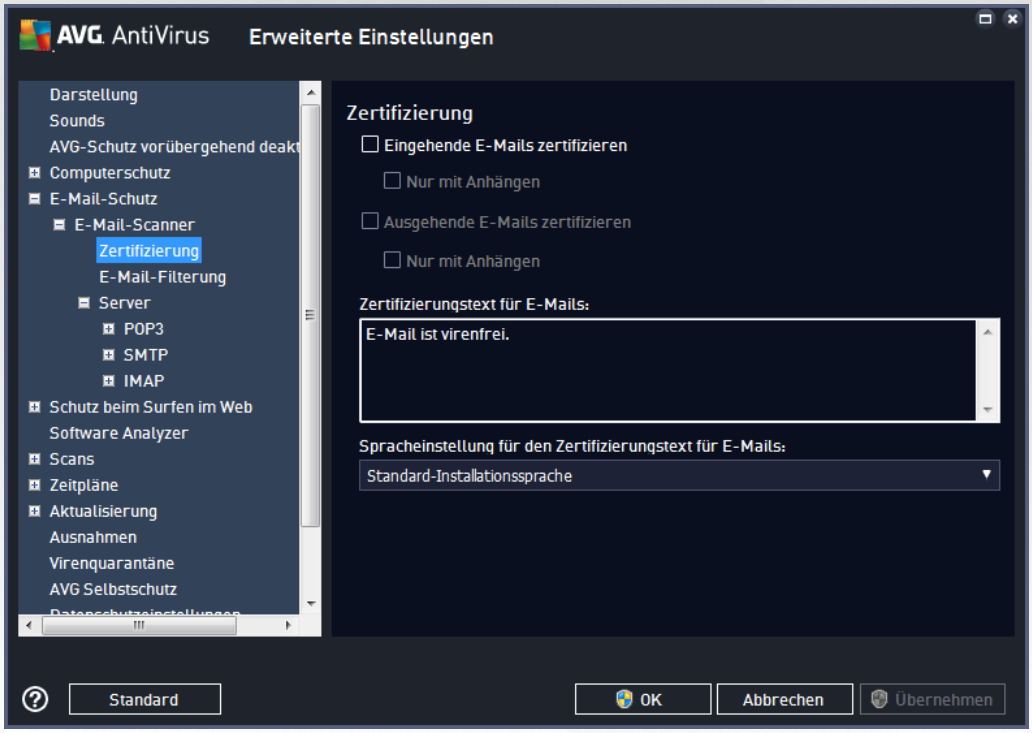
- ***Berichte kennwortgeschützte Dokumente*** – Dokumente, die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Dokumente als potenziell gefährlich anzuzeigen.

- ***Berichte 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 potenziell gefährliche Anweisungen enthalten. Aktivieren Sie das Kontrollkästchen, um sicherzustellen, dass Makros als verdächtig gemeldet werden.

- ***Dateien mit versteckten Erweiterungen in Bericht aufnehmen*** – Durch versteckte Erweiterungen kann beispielsweise eine verdächtige ausführbare Datei wie „abcdef.txt.exe“ als harmlose Textdatei „abcdef.txt“ angezeigt werden. Aktivieren Sie das Kontrollkästchen, um diese Dateien als potenziell gefährlich anzuzeigen.

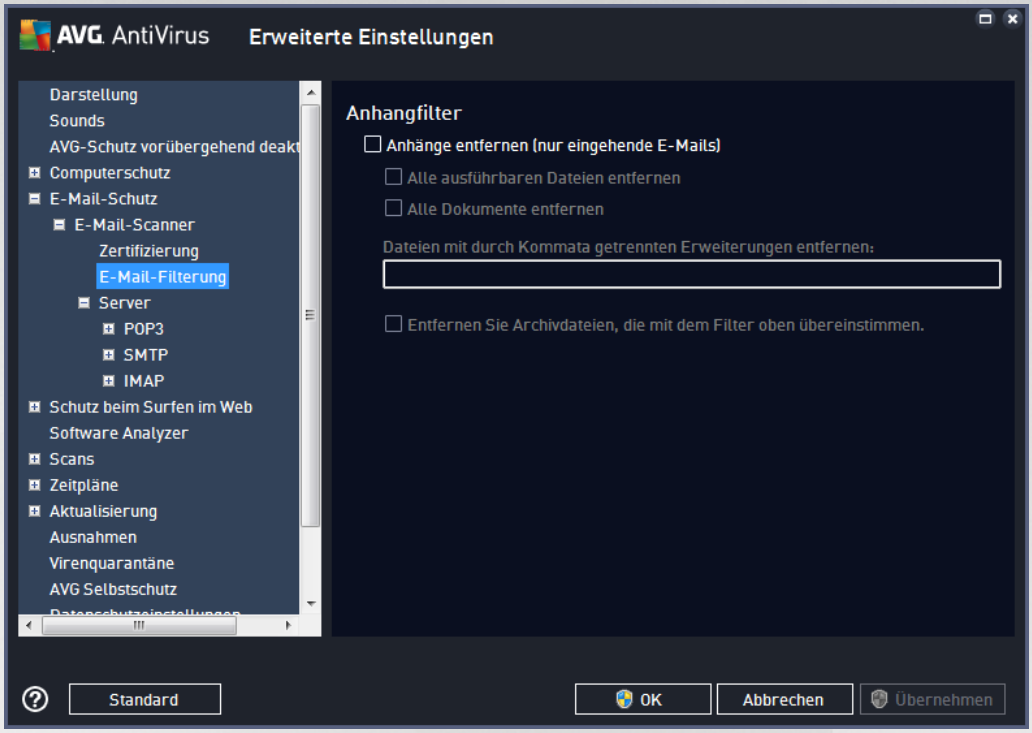
- ***Erkannte Anhänge in Virenquarantäne verschieben*** – Geben Sie an, ob Sie per E-Mail über kennwortgeschützte Archive, kennwortgeschützte Dokumente, Dateien mit Makros und/oder Dateien mit versteckter Erweiterung benachrichtigt werden möchten, die als Anhang der gescannten E-Mail-Nachricht erkannt wurden. Legen Sie fest, ob eine solche, während des Scans erkannte Nachricht, als infiziertes Objekt in die Virenquarantäne verschoben werden soll.

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



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

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



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

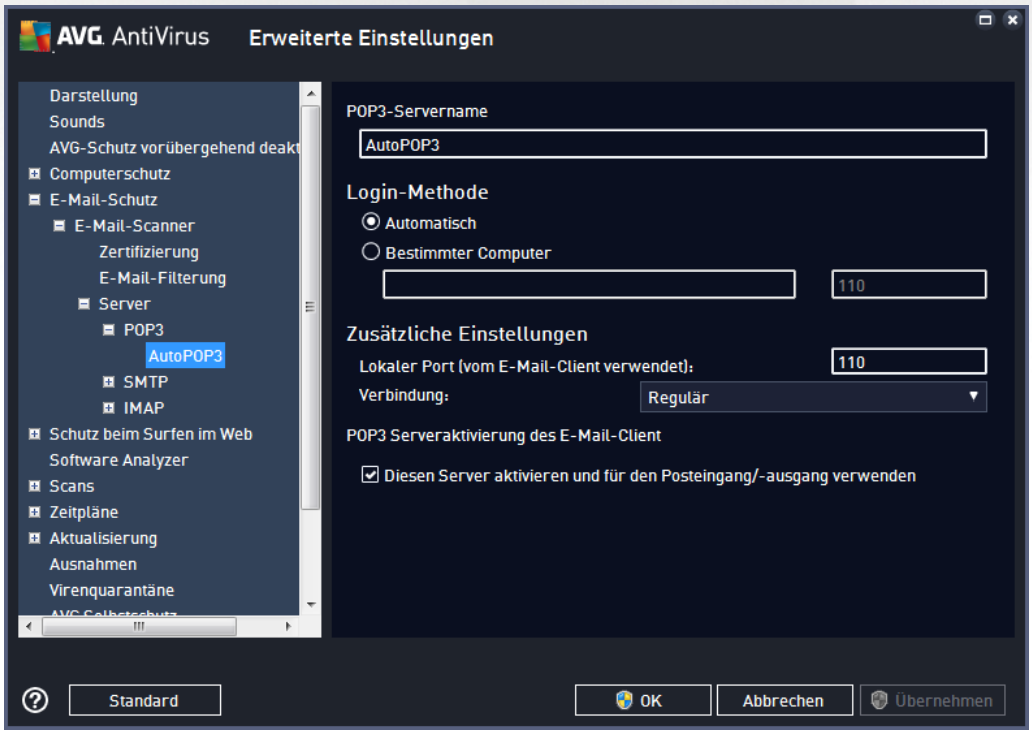
- ***Alle ausführbaren Dateien entfernen*** – Alle Dateien des Typs *.exe werden gelöscht.
- ***Alle Dokumente entfernen*** – Alle Dateien mit folgenden Erweiterungen werden entfernt: *.doc, *.docx, *.xls, *.xlsx.
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Alle Dateien mit den definierten Erweiterungen werden entfernt.

Im Bereich ***Server*** können Sie die Parameter für die E-Mail-Scanner-Server bearbeiten:

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

Sie können außerdem neue Server für eingehende oder ausgehende E-Mails über die Schaltfläche ***Neuen Server hinzufügen*** festlegen.

In diesem Dialog können Sie einen neuen E-Mail-Scanner-Server einrichten, der das POP3-Protokoll für eingehende E-Mails verwendet:



- ***POP3-Servername*** – In diesem Feld können Sie den Namen neu hinzugefügter Server angeben (*klicken Sie zum Hinzufügen eines POP3-Servers mit der rechten Maustaste auf den POP3-Eintrag im linken Navigationsmenü*).

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

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

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

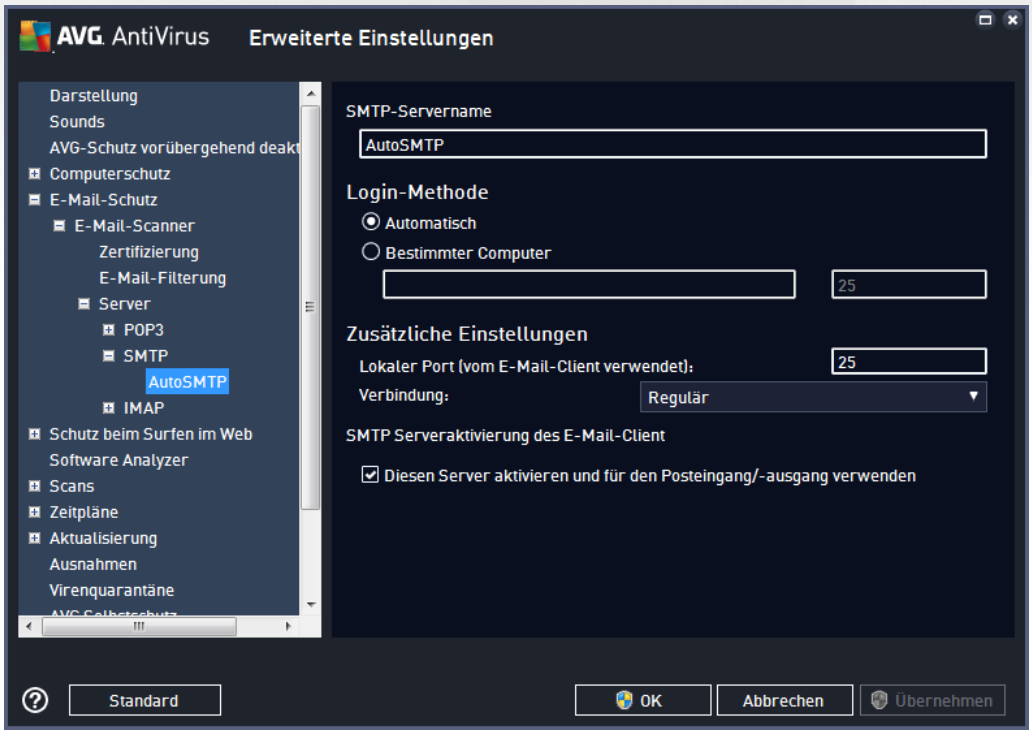
- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:

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

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

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

In diesem Dialog können Sie einen neuen E-Mail-Scanner -Server einrichten, der das SMTP-Protokoll für ausgehende E-Mails verwendet:



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

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der für ausgehende E-Mails verwendete E-Mail-Server bestimmt werden soll:

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

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

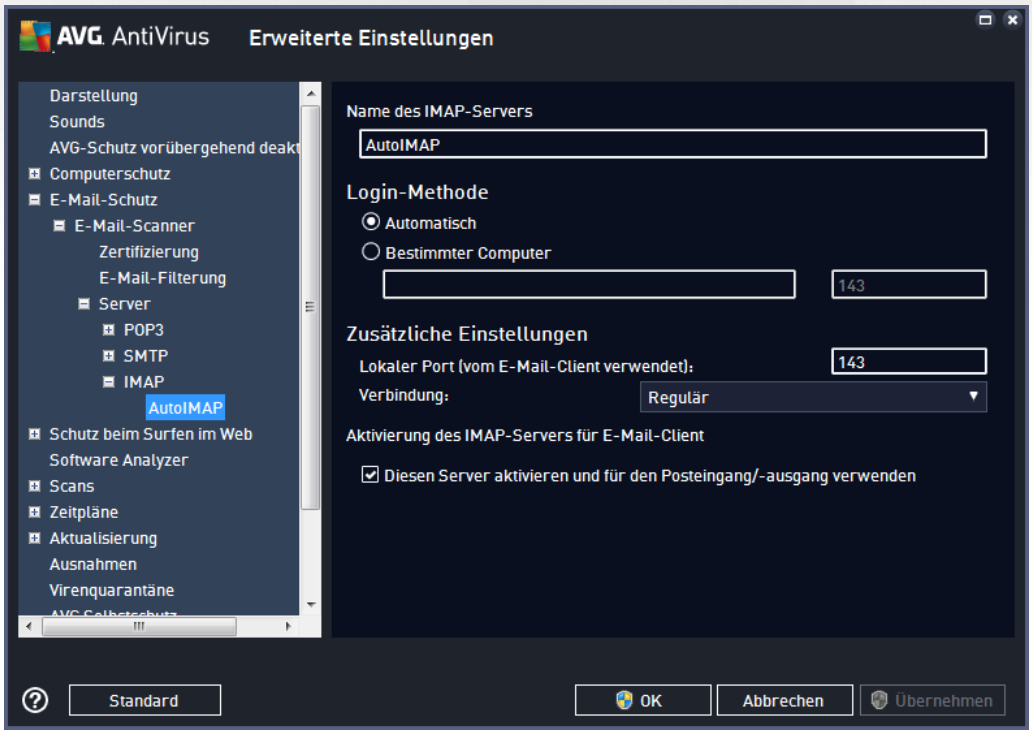
- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:

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

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

- ***IMAP-Serveraktivierung des E-Mail-Client*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten IMAP-Server zu aktivieren/deaktivieren.

In diesem Dialog können Sie einen neuen E-Mail-Scanner-Server einrichten, der das IMAP-Protokoll für ausgehende E-Mails verwendet:



- ***IMAP-Servername*** – In diesem Feld können Sie den Namen des neu hinzugefügten Servers angeben (*klicken Sie zum Hinzufügen eines IMAP-Servers mit der rechten Maustaste auf den IMAP-Eintrag im linken Navigationsmenü*).

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der für ausgehende E-Mails verwendete E-Mail-Server bestimmt werden soll:

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

    - ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres Mailservers an. Als Namen können Sie einen Domainnamen (*z. B. imap.acme.com*) oder eine IP-Adresse (*z. B. 123.45.67.89*) verwenden. Wenn der E-Mail-Server keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen verwendet wird (*z. B. imap.acme.com:8200*). Der Standardport für die IMAP-Kommunikation ist 143.

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

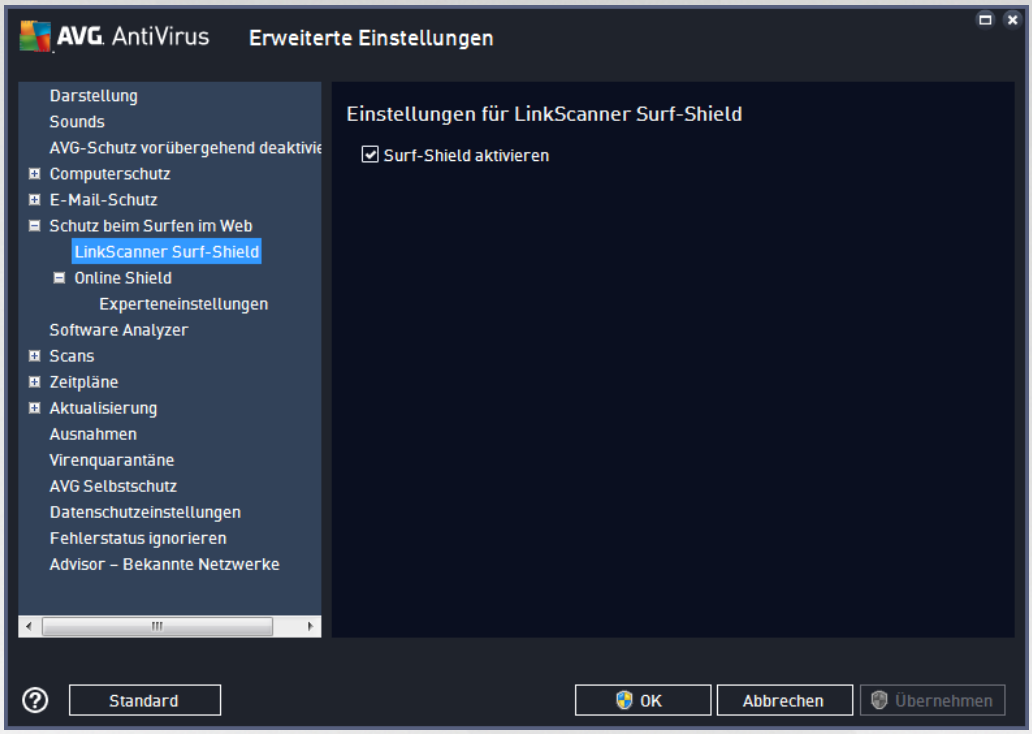
    - ***Lokaler Port verwendet in*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer E-Mail-Anwendung ankommen soll. In Ihrem E-Mail-Programm müssen Sie diesen Port als Port für die IMAP-Kommunikation angeben.

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

- ***IMAP-Serveraktivierung des E-Mail-Client*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten IMAP-Server zu aktivieren/deaktivieren.

7.6. Schutz beim Surfen im Web

Im Dialogfenster ***Einstellungen des Link Scanner*** können Sie die folgenden Funktionen aktivieren bzw. deaktivieren:



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

7.6.1. Online Shield

Das Dialogfeld ***Online Shield*** enthält die folgenden Optionen:

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

Benachrichtigungsmodus für Bedrohungen

Im unteren Bereich des Dialogfelds können Sie die Methode zur Benachrichtigung über potenzielle Bedrohungen auswählen: mit einem Standard-Popup-Fenster, mit einer Benachrichtigung über Sprechblasen oder durch ein Symbol im Infobereich.

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

- ***Archive überprüfen*** – (*standardmäßig deaktiviert*): Archivinhalte, die möglicherweise auf einer anzuzeigenden Webseite enthalten sind, werden ebenfalls gescannt.
- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** – (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, doch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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.
- ***Heuristik verwenden*** – (*standardmäßig aktiviert*): Der Inhalt der angezeigten Webseite wird mithilfe der heuristischen Analyse gescannt (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*).
- ***Sorgfältige Überprüfung aktivieren*** – (*standardmäßig deaktiviert*): Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres

Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.

- ***Verschlüsselten Netzwerkverkehr (TLS und SSL) scannen*** – (*standardmäßig aktiviert*): Lassen Sie diese Option aktiviert, damit AVG auch den gesamten verschlüsselten Netzwerkverkehr scannt, d. h. Verbindungen über Sicherheitsprotokolle (SSL und dessen neuere Version TLS). Dies trifft auf Websites, die HTTPS verwenden, und auf E-Mail-Client-Verbindungen über TLS/SSL zu. Der gesicherte Datenverkehr wird entschlüsselt, auf Malware gescannt und wieder verschlüsselt, um sicher auf Ihren Computer zu gelangen. Hier können Sie die Option ***Beinhaltet Datenverkehr von Servern, die EV-Zertifikate (Extended Validation) besitzen*** aktivieren und festlegen, ob auch der verschlüsselte Netzwerkverkehr von Servern gescannt werden soll, die mit einem EV-Zertifikat versehen sind. Das Ausstellen eines EV-Zertifikats erfordert eine umfangreiche Überprüfung durch die Zertifizierungsstelle, und mit diesem Zertifikat versehene Websites sind daher wesentlich vertrauenswürdiger (*es besteht ein geringeres Risiko, dass sie Malware enthalten*). Aus diesem Grund können Sie Datenverkehr von EV-zertifizierten Servern aus dem Scan ausschließen, wodurch die verschlüsselte Kommunikation etwas beschleunigt wird.

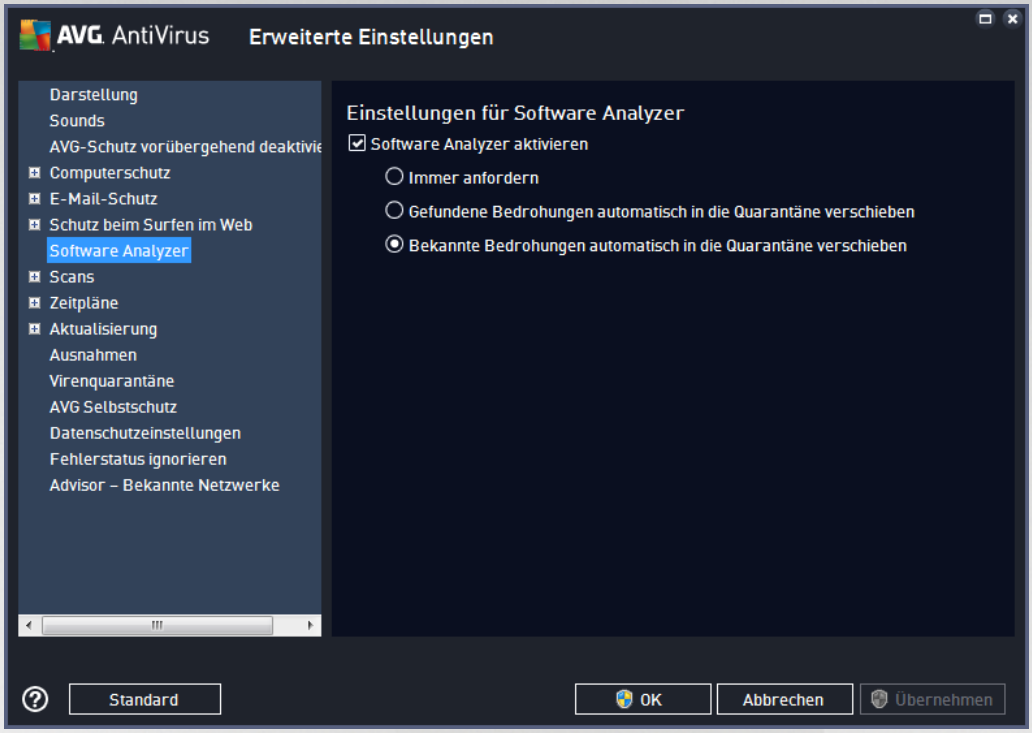
- ***Scan hat ausführbare Dateien mit Residentem Schutz heruntergeladen*** – (*standardmäßig aktiviert*): Scannt ausführbare Dateien *(übliche Dateiendungen: exe, bat, com)* nach dem Download. Der Residente Schutz scannt Dateien vor dem Download, um sicherzustellen, dass keine schädlichen Codes auf Ihren Computer heruntergeladen werden. Diese Scans sind jedoch durch ***Maximale Teilgröße zu scannender Dateien begrenzt*** – siehe nächstes Element in diesem Dialogfeld. Daher werden große Dateien in einzelnen Teilen gescannt. Dies ist für die meisten ausführbaren Dateien der Fall. Ausführbare Dateien können verschiedene Aufgaben auf Ihrem Computer durchführen, daher ist es wichtig, dass sie 100 % sicher sind. Dies wird durch einen Scan der Teile vor dem Download und direkt nach Abschluss des Downloads gewährleistet. Es wird empfohlen, diese Option zu aktivieren. Wenn Sie diese Option deaktivieren, findet AVG trotzdem weiterhin potenziell gefährlichen Code. Allerdings werden ausführbare Dateien üblicherweise nicht als vollständige Datei erkannt, sodass einige Fehlalarme auftreten können.

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

7.7. Software Analyzer

Software Analyzer ist eine Anti-Malware-Komponente, die Sie mithilfe verhaltensbasierter Technologien vor allen Arten von Malware schützt (*Spyware, Bots, Identitätsdiebstahl usw.*), und der Zero-Day-Schutz verhindert, dass Ihr Computer mit neuen Viren infiziert wird *(eine detaillierte Beschreibung der Funktionsweise dieser Komponente finden Sie im Kapitel Software Analyzer*).

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



Software Analyzer aktivieren (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, um die Komponente Identität zu deaktivieren. ***Es wird dringend empfohlen, dies nur in Ausnahmesituationen zu tun!*** Wenn Software Analyzer aktiviert ist, können Sie festlegen, was im Falle einer erkannten Bedrohung geschehen soll:

- ***Immer anfordern*** – Sie werden bei Erkennung einer Bedrohung gefragt, ob diese in die Virenquarantäne verschoben werden soll. Damit wird sichergestellt, dass keine Anwendungen entfernt werden, die Sie ausführen möchten.
- ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** – Aktivieren Sie dieses Kontrollkästchen, um alle potenziell gefährlichen Bedrohungen umgehend in die sichere Virenquarantäne zu verschieben. Wenn Sie die Standardeinstellungen beibehalten, werden Sie bei der Erkennung einer Bedrohung gefragt, ob diese in die Virenquarantäne verschoben werden soll. Damit wird sichergestellt, dass keine Anwendungen entfernt werden, die Sie ausführen möchten.
- ***Bekannte Bedrohungen automatisch in die Quarantäne verschieben*** (*standardmäßig aktiviert*) – Behalten Sie die Aktivierung dieses Eintrags bei, wenn Sie möchten, dass alle Anwendungen mit Verdacht auf Malware automatisch und sofort in die Virenquarantäne. ϖερσχηοβεν ωερδεν.

7.8. Scans

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

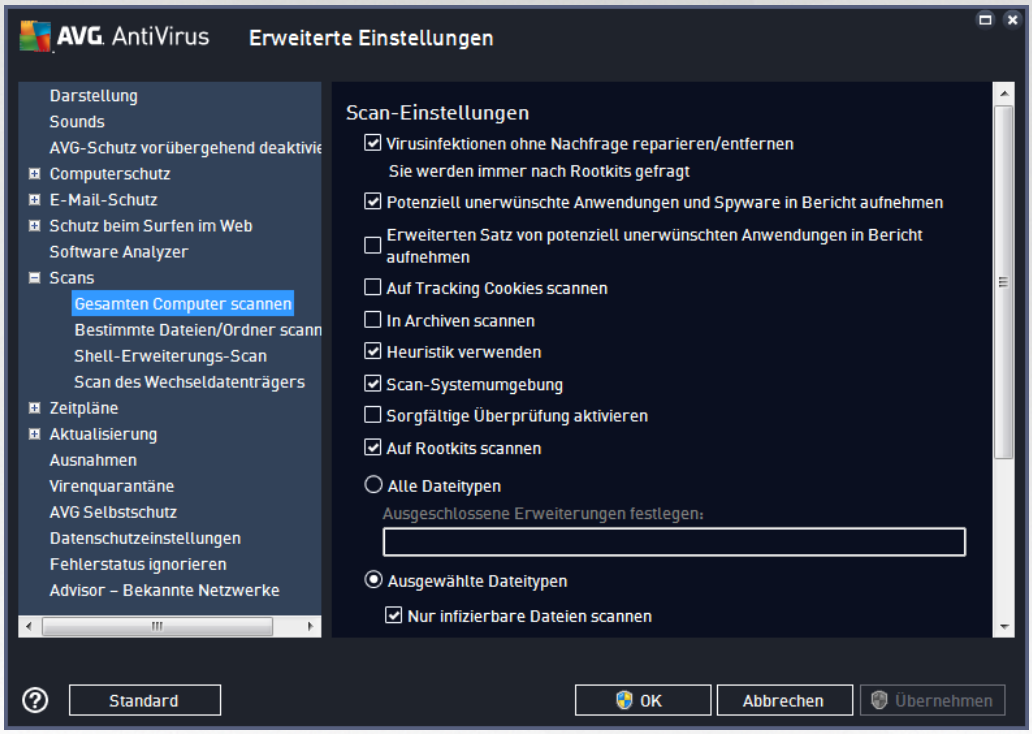
- Scan des gesamten Computers – Vordefinierter Standard-Scan des gesamten Computers
- Scan bestimmter Dateien oder Ordner – vordefinierter Standard-Scan ausgewählter Bereiche Ihres Computers

- Shell-Erweiterungs-Scan – Bestimmter Scan eines ausgewählten Objekts direkt von der Umgebung des Windows Explorers aus

- Scan des Wechseldatenträgers – spezifischer Scan der Wechseldatenträger, die an Ihren Computer angeschlossen sind

7.8.1. Scan des gesamten Computers

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



Scan-Einstellungen

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

- ***Virusinfektionen ohne Nachfrage reparieren/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 repariert werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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 legt fest, dass 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 umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.

- ***Auf Rootkits scannen*** (*standardmäßig aktiviert*) – Anti-Rootkit-Scan überprüft Ihren Computer auf mögliche Rootkits, d. h. auf 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.

Sie sollten bestimmen, welche Dateien überprüft werden:

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommas getrennten Dateierweiterungen erstellen (*nach dem Speichern ändern sich die Kommas in Semikolons*), die nicht gescannt werden sollen.

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potenziell infizierte 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 dieses Kontrollkästchen deaktiviert bleibt, ist die Scan-Zeit 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

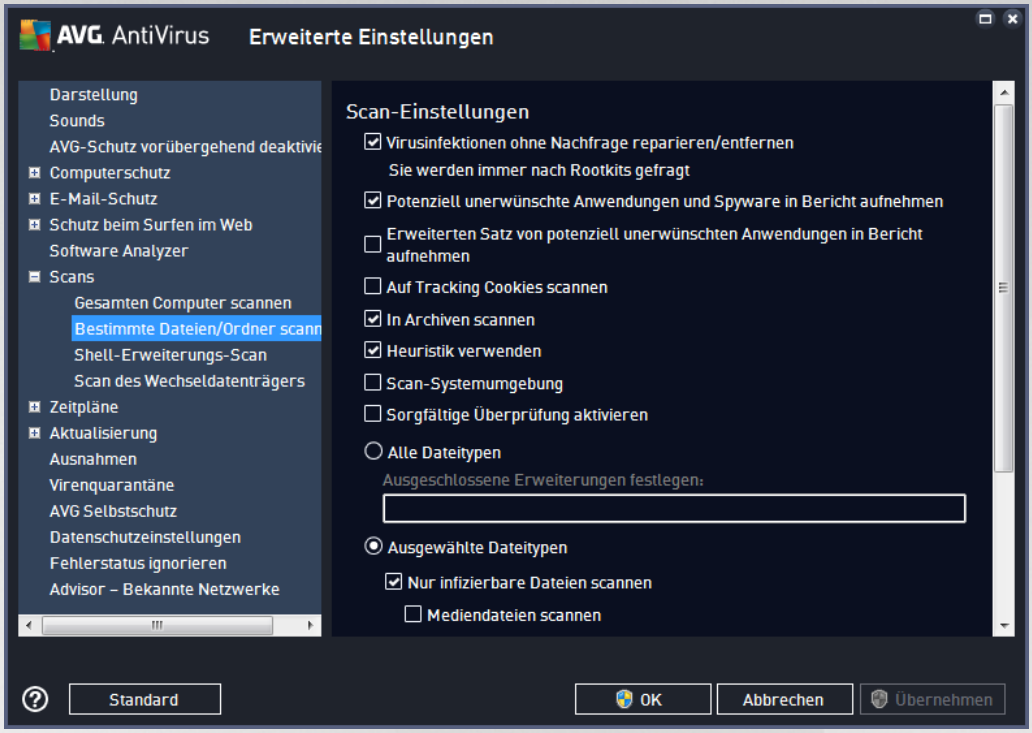
Im Bereich ***Dauer des Scans anpassen*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Wenn der Scan schneller ausgeführt werden soll, nimmt er zwar weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan ist aber deutlich höher, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*Diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber gerade nicht verwendet wird*). Andererseits 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 das separate Dialogfeld ***Scan-Berichte*** zu öffnen, in dem Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:

7.8.2. Bestimmte Dateien/Ordner scannen

Die Bearbeitungsoberfläche für die Option ***Bestimmte Dateien/Ordner scannen*** ist dem Bearbeitungsdialogfeld Gesamten Computer scannen sehr ähnlich. Die Standardeinstellungen für die Option Gesamten Computer scannen sind jedoch strenger:

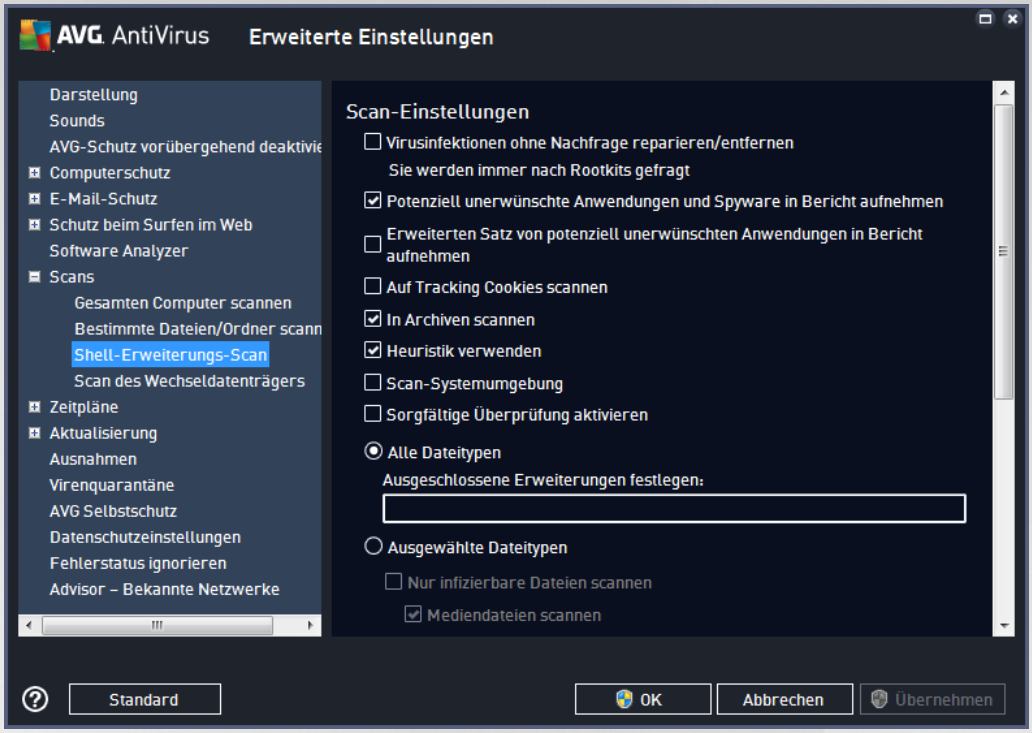


Alle Parameter, die in diesem Konfigurationsdialogfeld festgelegt werden, gelten nur für die Scan-Bereiche, die unter der Option Bestimmte Dateien/Ordner scannen ausgewählt wurden!

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

7.8.3. Shell-Erweiterungs-Scan

Ähnlich der vorhergehenden Option Gesamten Computer scannen 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 Explorers aus gestartet wird (*Shell-Erweiterung*). Siehe Kapitel Scans aus dem Windows Explorer:



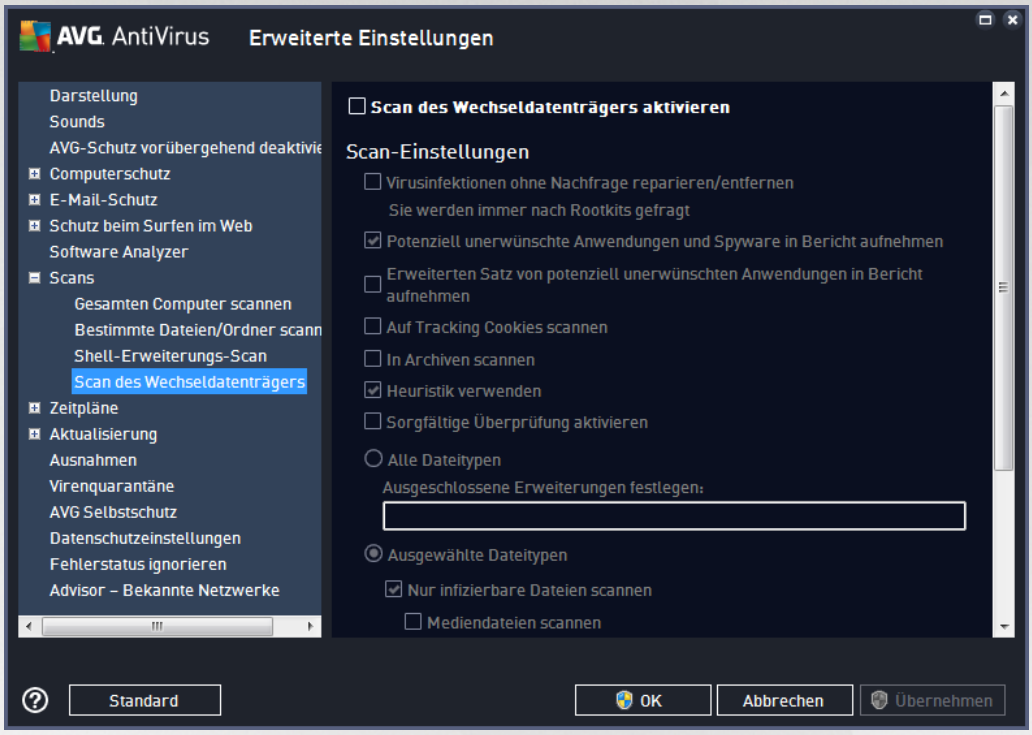
Die Bearbeitungsoptionen sind nahezu identisch mit denen für die Option Gesamten Computer scannen, die Standardeinstellungen unterscheiden sich jedoch (*während beim Scan des gesamten Computers standardmäßig keine Archive, aber die Systemumgebung gescannt wird, verhält es sich beim Shell-Erweiterungs-Scan umgekehrt*).

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

Im Vergleich zum Dialogfeld Gesamten Computer scannen enthält das Dialogfeld ***Shell-Erweiterungs-Scan*** auch den Bereich ***Anzeigen von Scan-Fortschritt und -Ergebnissen***, in dem Sie festlegen können, dass der Scan-Fortschritt und die Scan-Ergebnisse auch über die Benutzeroberfläche von AVG aufgerufen werden können. Sie können außerdem festlegen, dass Scan-Ergebnisse nur bei einer beim Scan erkannten Infektion angezeigt werden sollen.

7.8.4. Scan des Wechseldatenträgers

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



Der ***Scan des Wechseldatenträgers*** wird automatisch gestartet, sobald Sie einen Wechseldatenträger an Ihren Computer anschließen. Standardmäßig ist dieser 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 / Gesamten Computer scannen.*

7.9. Zeitpläne

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

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

7.9.1. Geplanter Scan

Auf drei Registerkarten können die Parameter für den geplanten Scan bearbeitet (*oder ein neuer Zeitplan erstellt*) werden. Sie können den Eintrag ***Diese Aufgabe aktivieren*** auf jeder Registerkarte aktivieren bzw.

deaktivieren, um den geplanten Test vorübergehend zu deaktivieren. Anschließend können Sie den Eintrag 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. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag* ***Geplanter Scan*** *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 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 dagegen „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 nur um den Scan ausgewählter Ordner oder Dateien. Ihre eigenen Scans sind immer bestimmte Versionen eines Scans ausgewählter Dateien oder Ordner.*

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

Zeitplan wird ausgeführt

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

Erweiterte Zeitplanoptionen

- ***Nach Systemstart ausführen, wenn die geplante Aufgabe nicht ausgeführt wurde*** – Falls die Ausführung einer Aufgabe zu einer bestimmten Zeit festgelegt wurde, der Computer jedoch zu dieser Zeit ausgeschaltet war, sorgt diese Option dafür, dass die Aufgabe nachträglich ausgeführt wird.

- ***Auch dann ausführen, wenn sich der Computer im Stromsparmodus befindet*** – Die Aufgabe wird ausgeführt, auch wenn der Computer zur geplanten Zeit über Batteriestrom betrieben wird.

Auf der Registerkarte ***Einstellungen*** finden Sie 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 kein triftiger Grund besteht, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten***:

- ***Virusinfektionen ohne Nachfrage reparieren/entfernen*** *(standardmäßig aktiviert):* Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, wenn eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch repariert werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert):* Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu

erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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 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 umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.

- ***Auf Rootkits scannen*** *(standardmäßig aktiviert):* Anti-Rootkit-Scan überprüft Ihren Computer auf mögliche Rootkits, d. h. 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.

Sie sollten bestimmen, welche Dateien überprüft werden:

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommas getrennten Dateierweiterungen erstellen (*nach dem Speichern ändern sich die Kommas in Semikolons*), die nicht gescannt werden sollen.

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potenziell infizierte 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 dieses Kontrollkästchen deaktiviert bleibt, ist die Scan-Zeit 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.

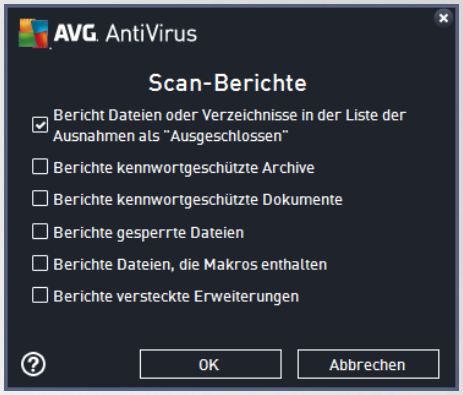
- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt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

Dauer des Scans anpassen

In diesem Bereich 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 er zwar weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan ist aber deutlich höher, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber derzeit nicht verwendet wird*). Andererseits können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

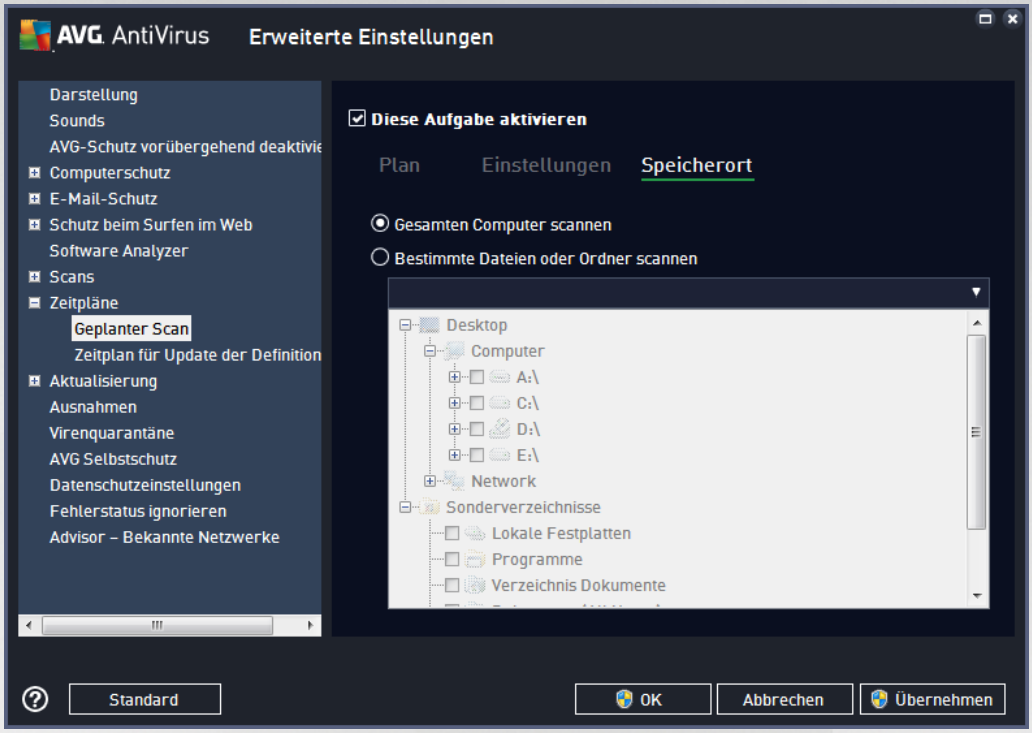
Zusätzliche Scan-Berichte einstellen

Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen...***, um das separate Dialogfeld ***Scan-Berichte*** zu öffnen, in dem Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



Optionen für das Herunterfahren des Computers

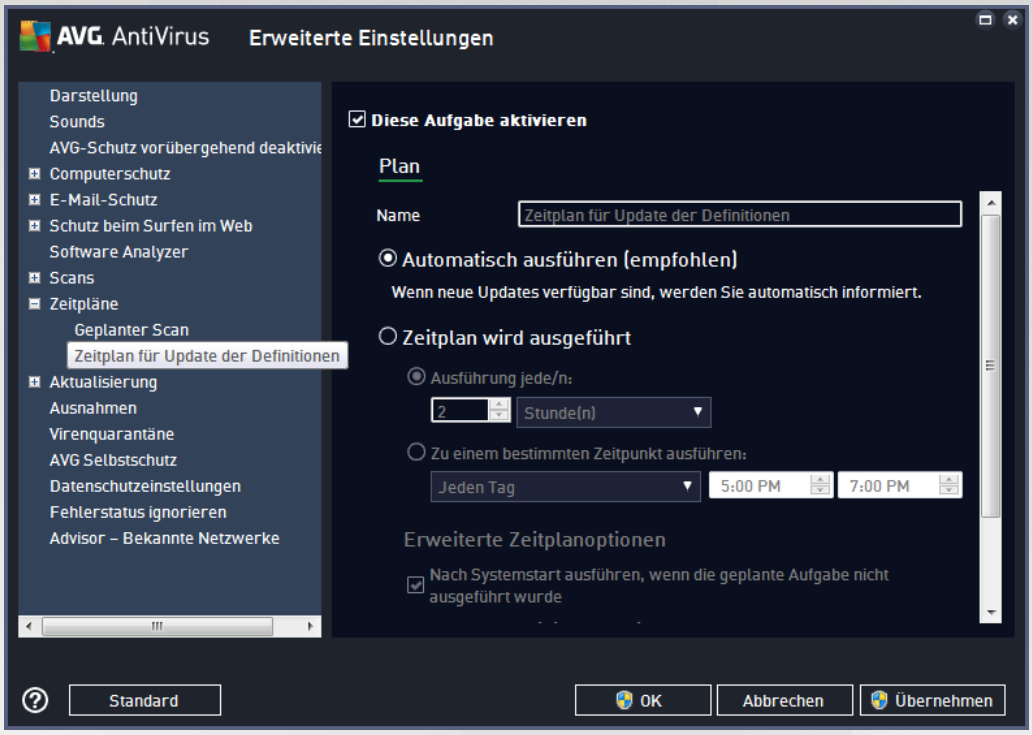
Im Bereich ***Optionen für das Herunterfahren des Computers*** können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert,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



Auf der Registerkarte ***Speicherort*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien/Ordner scannen wählen 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.

7.9.2. Zeitplan für Update der Definitionen

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



In diesem Dialogfeld können Sie genauere Parameter für den Zeitplan für Definitionsaktualisierungen 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

Standardmäßig wird diese Aufgabe automatisch gestartet (***Automatisch ausführen***), sobald eine aktualisierte Virendefinition verfügbar ist. Wir empfehlen Ihnen, diese Konfiguration beizubehalten, es sei denn, es gibt einen speziellen Grund, dies nicht zu tun. In diesem Fall können Sie den manuellen Start der Aufgabe festlegen und die Zeitintervalle angeben, in denen das neu geplante Update der Definitionen durchgeführt werden soll. Sie können entweder wiederholte Starts des Updates nach einem bestimmten Zeitraum (***Ausführung jede/n...***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) festlegen.

Erweiterte Zeitplanoptionen

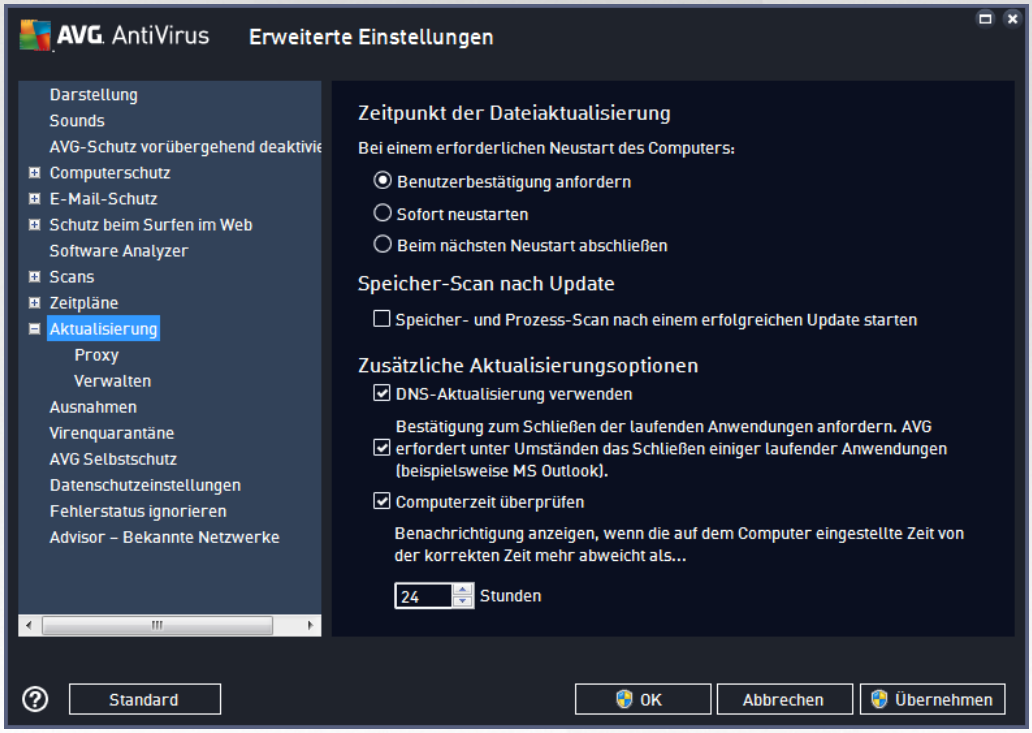
In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen die Definitionsaktualisierung gestartet werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder komplett ausgeschaltet ist).

Andere Aktualisierungseinstellungen

Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung neu gestartet wird. Sobald das geplante Update zu dem von Ihnen festgelegten Zeitpunkt startet, werden Sie darüber in einem Popup-Fenster informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialogfeld Erweiterte Einstellungen/Darstellung beibehalten).*

7.10. Aktualisierung

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



Zeitpunkt der Dateiaktualisierung

In diesem Bereich können Sie zwischen drei alternativen Optionen wählen, wenn der Update-Vorgang einen Neustart des Computers erfordert. Der Abschluss des Updates kann für den nächsten Neustart des Computers geplant werden, oder Sie können den Neustart sofort durchführen:

- ***Benutzerbestätigung anfordern*** *(standardmäßig aktiviert)* – Sie werden aufgefordert, den Neustart Ihres Computers zu bestätigen, um das Update abzuschließen.
- ***Sofort neu starten*** – Der Computer wird automatisch neu gestartet, sobald das Update abgeschlossen ist. Sie müssen den Neustart nicht bestätigen.
- ***Beim nächsten Neustart abschließen*** – der Abschluss des Updates wird bis zum nächsten Neustart des Computers verschoben. Diese Option wird nur empfohlen, 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 Scan umgehend angewendet werden.

Zusätzliche Aktualisierungsoptionen

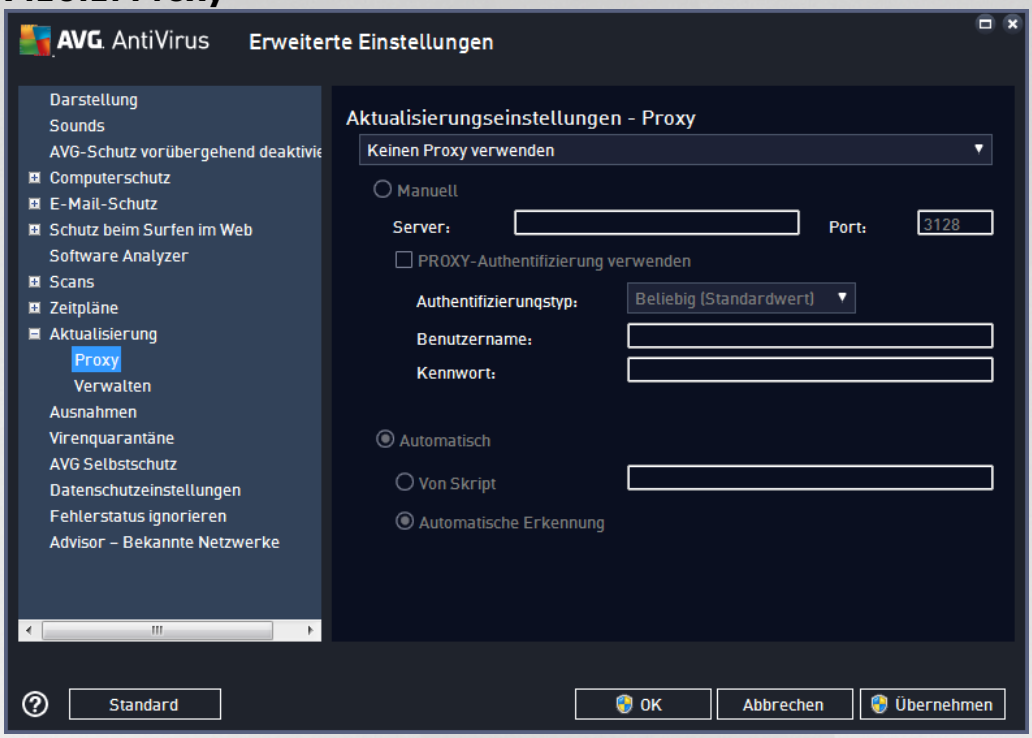
- ***Bei jedem Programmupdate einen neuen Systemwiederherstellungspunkt erstellen*** (*standardmäßig aktiviert*) – Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem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

- ***DNS-Update verwenden*** (*standardmäßig aktiviert*) – Wenn diese Option aktiviert ist, sucht **AVG AntiVirus** nach Informationen zur neuesten Version der Virendatenbank sowie der neuesten Programmversion auf dem DNS-Server, sobald das Update gestartet wird. Dann werden nur die kleinsten unabdingbar erforderlichen Aktualisierungsdateien heruntergeladen und ausgeführt. Auf diese Weise wird die heruntergeladene Datenmenge auf einem Minimum gehalten, und der Aktualisierungsprozess ist schneller.

- ***Bestätigung zum Schließen der laufenden Anwendungen anfordern*** (*standardmäßig aktiviert*) – Hiermit können Sie sicherstellen, dass derzeit ausgeführte Anwendungen nicht ohne Ihre Genehmigung geschlossen werden. Dies kann zum Abschluss des Updatevorgangs erforderlich sein.

- ***Computerzeit überprüfen*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, wenn Benachrichtigungen angezeigt werden sollen, falls die Computerzeit um mehr als die angegebene Anzahl an Stunden von der korrekten Zeit abweicht.

7.10.1. 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:

- ***Keinen Proxy verwenden*** – Standardeinstellung
- ***Proxy verwenden***
- ***Direkte Verbindung herstellen, wenn eine Proxy-Verbindung fehlschlägt***

Wenn Sie eine Option mit einem 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 bestimmte 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.

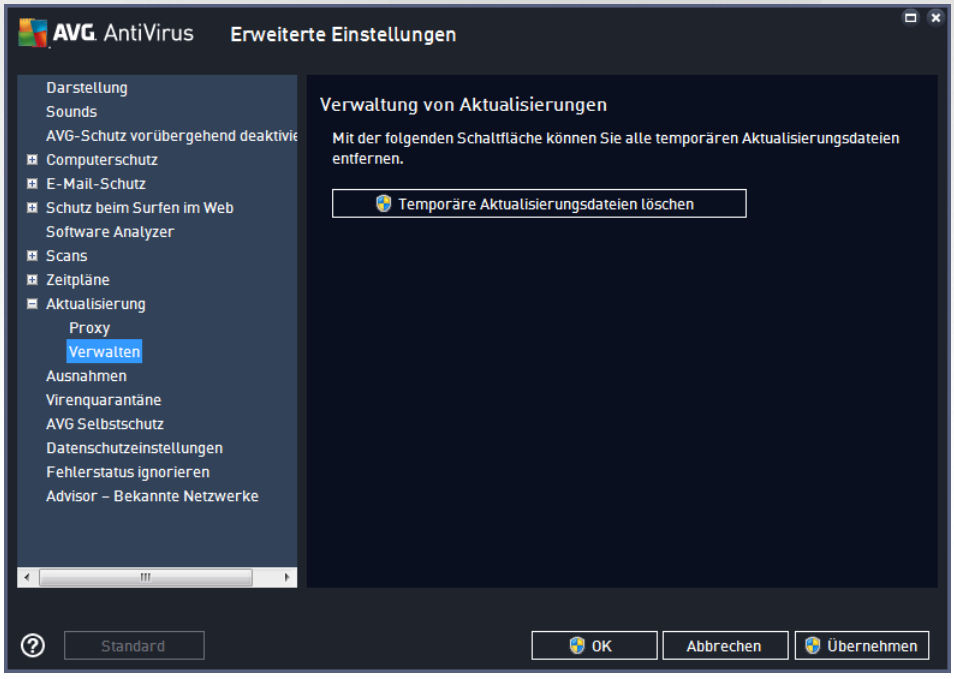
Automatische Konfiguration

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-Internetbrowser 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.

7.10.2. Verwalten

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

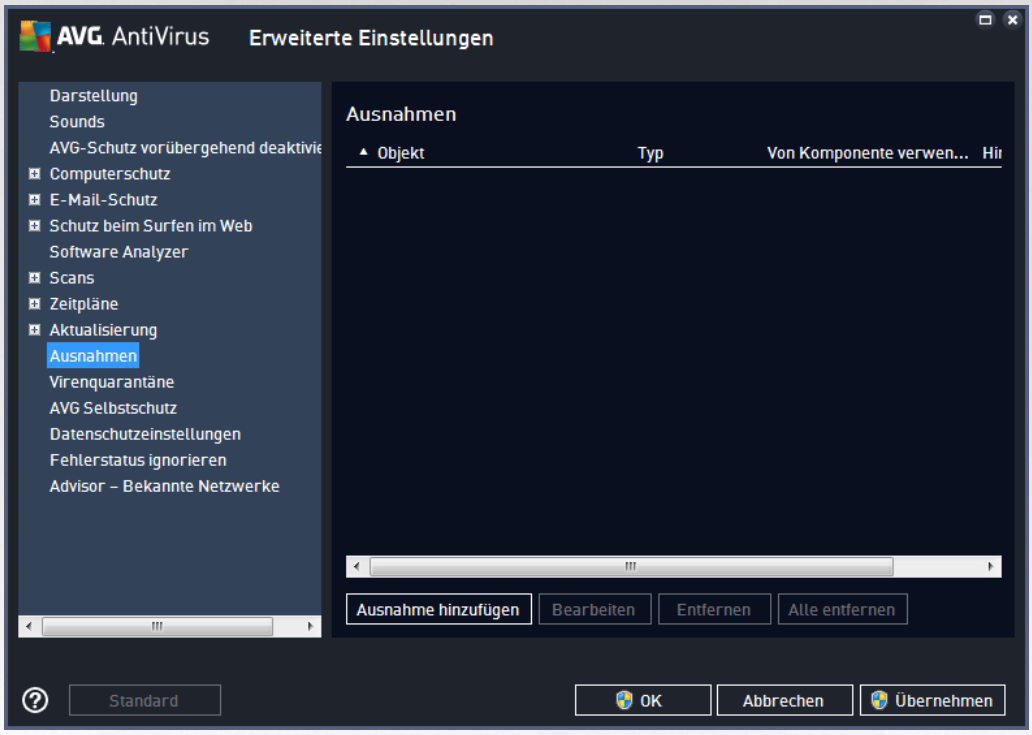


- ***Temporäre Aktualisierungsdateien löschen*** – Klicken Sie auf diese Schaltfläche, wenn Sie alle redundanten Update-Dateien von Ihrer Festplatte löschen möchten (*standardmäßig werden diese Dateien 30 Tage gespeichert*).
- ***Virendatenbank auf vorhergehende Version zurücksetzen*** – Klicken Sie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

7.11. Ausnahmen

Im Dialogfeld ***Ausnahmen*** können Sie Ausnahmen definieren, also Elemente, die von **AVG AntiVirus** ignoriert werden sollen. Wenn AVG ein Programm oder eine Datei häufig als Bedrohung erkennt oder eine sichere Website als gefährlich einstuft und blockiert, sollten Sie eine Ausnahme definieren. Fügen Sie die Datei oder Website zu dieser Ausnahmeliste hinzu, damit sie von AVG nicht mehr gemeldet oder blockiert wird.

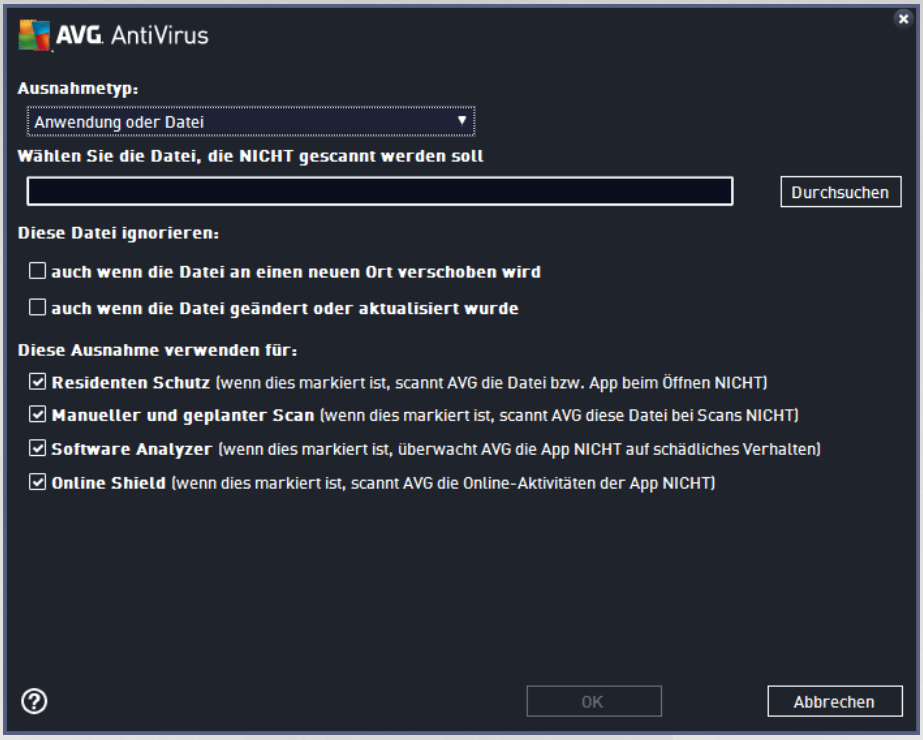
Stellen Sie jedoch stets sicher, dass die betroffene Datei, das Programm oder die Website auch wirklich absolut sicher sind.



Im Diagramm des Dialogfeldes befindet sich eine Liste der Ausnahmen, sofern bereits Ausnahmen definiert wurden. Neben jedem Element befindet sich ein Kontrollkästchen. Wenn das Kontrollkästchen markiert ist, ist die Ausnahme aktiv. Liegt keine Markierung vor, wurde die Ausnahme zwar definiert, sie wird aber derzeit nicht verwendet. Wenn Sie auf die Kopfzeile einer Spalte klicken, werden die zugelassenen Elemente nach den entsprechenden Kriterien sortiert.

Schaltflächen

- ***Ausnahme hinzufügen*** – Klicken Sie auf diese Schaltfläche, um ein neues Dialogfeld zu öffnen, in dem Sie angeben können, welches Element vom AVG-Scan ausgeschlossen werden soll:



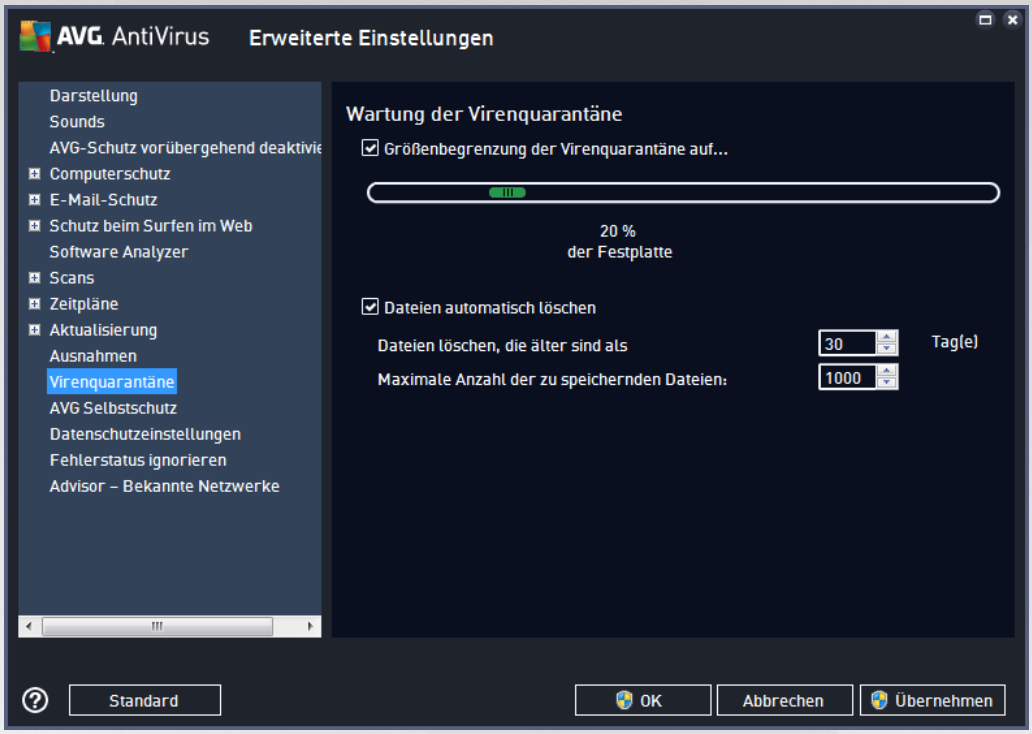
Zuerst werden Sie dazu aufgefordert, den Objekttyp zu definieren, d. h., ob es sich beispielsweise um eine Anwendung, eine Datei, einen Ordner, eine URL oder ein Zertifikat handelt. Anschließend müssen Sie den Pfad zu dem entsprechenden Objekt auf Ihrer Festplatte angeben oder die URL eingeben. Zum Schluss können Sie auswählen, welche AVG-Funktionen *(Residenter Schutz, manueller und geplanter Scan, Software Analyzer, Online Shield und Windows Antimalware Scan Interface)* das ausgewählte Objekt ignorieren sollen.

- ***Bearbeiten*** – Diese Schaltfläche ist nur dann aktiv, wenn bereits einige Ausnahmen definiert wurden und im Diagramm aufgeführt sind. Mit dieser Schaltfläche können Sie dann das Dialogfeld zum Bearbeiten einer ausgewählten Ausnahme öffnen und deren Parameter konfigurieren.

- ***Entfernen*** – Verwenden Sie diese Schaltfläche, um eine vorher definierte Ausnahme zu entfernen. Sie können sie entweder einzeln entfernen oder auch einen ganzen Satz Ausnahmen aus der Liste markieren und diesen entfernen. Nachdem Sie die entsprechende Datei, den Ordner oder die URL entfernt haben, überprüft AVG sie nochmals. Beachten Sie, dass nur die Ausnahme entfernt wird, nicht die Datei oder der Ordner selbst.

- ***Alle entfernen*** – Verwenden Sie diese Schaltfläche, um alle in der Liste festgelegten Ausnahmen zu löschen.

7.12. Virenquarantäne

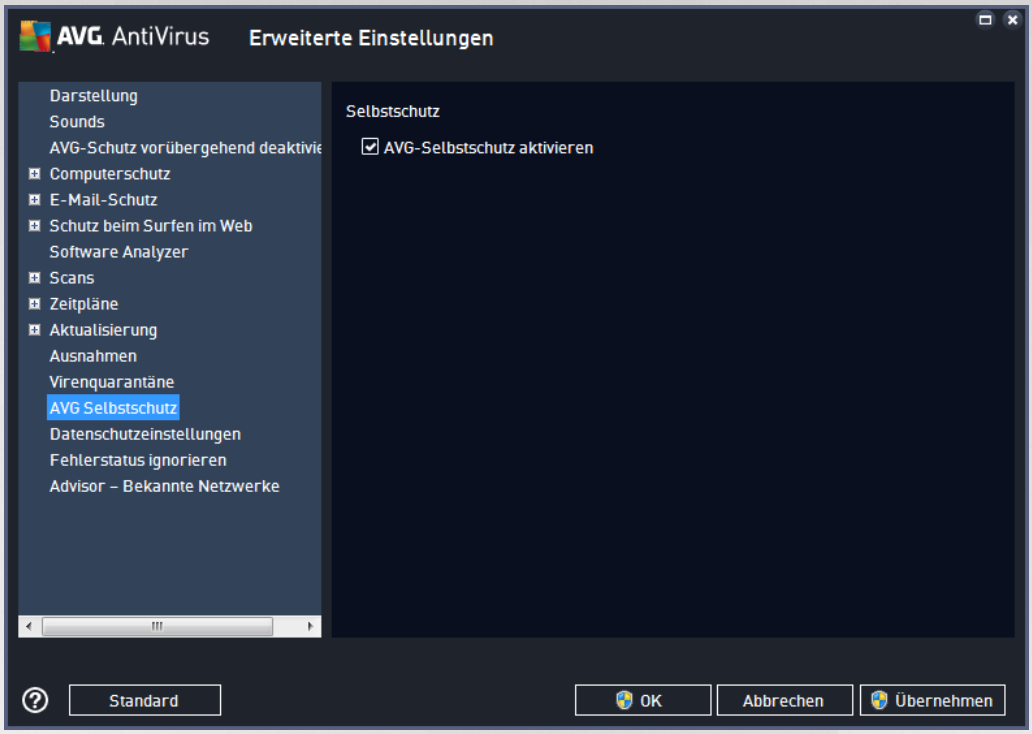


Im Dialog ***Wartung der Virenquarantäne*** können Sie mehrere Parameter hinsichtlich der Verwaltung der in der Virenquarantäne gespeicherten Objekte festlegen:

- ***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, für 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.

7.13. AVG-Selbstschutz

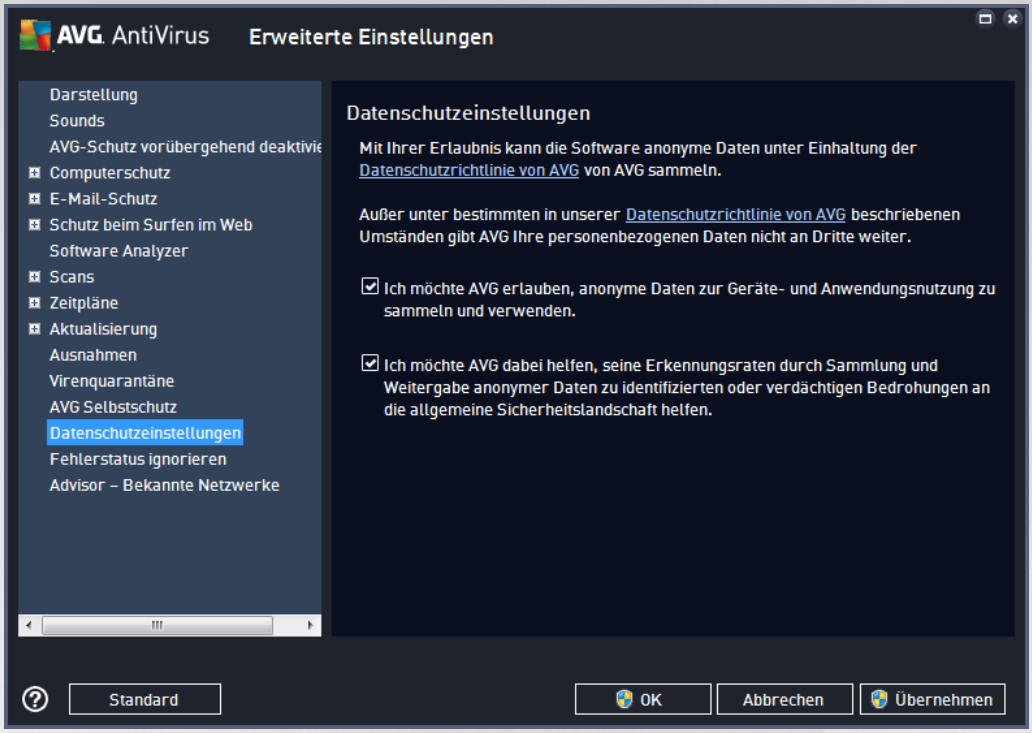


Der ***AVG-Selbstschutz*** ermöglicht es **AVG AntiVirus**, die eigenen Prozesse, Dateien, Registrierungsschlüssel und Treiber vor Änderungen oder Deaktivierung zu schützen. Der Hauptgrund für diesen Schutz ist, dass einige besonders tückische Bedrohungen den Virenschutz deaktivieren und dann ungehindert Schaden auf Ihrem Computer anrichten können.

Wir empfehlen, diese Funktion aktiviert zu lassen!

7.14. Datenschutzeinstellungen

Im Dialogfeld ***Datenschutzeinstellungen*** werden Sie dazu eingeladen, an der AVG-Produktverbesserung teilzunehmen und uns bei der Verbesserung der allgemeinen Internetsicherheit zu unterstützen. Mithilfe Ihrer Berichte erhalten wir von allen Teilnehmern auf der ganzen Welt aktuelle Informationen über die neuesten Bedrohungen und können im Gegenzug unseren Schutz für alle noch weiter verbessern. Die Berichterstattung erfolgt automatisch und bereitet Ihnen somit keine Umstände. In diesen Berichten sind keine persönlichen Daten enthalten. Die Berichterstattung über erkannte Bedrohungen ist optional; dennoch bitten wir Sie, die Aktivierung dieser Option beizubehalten. Sie hilft uns, den Schutz für Sie und andere Benutzer von AVG weiter zu verbessern.



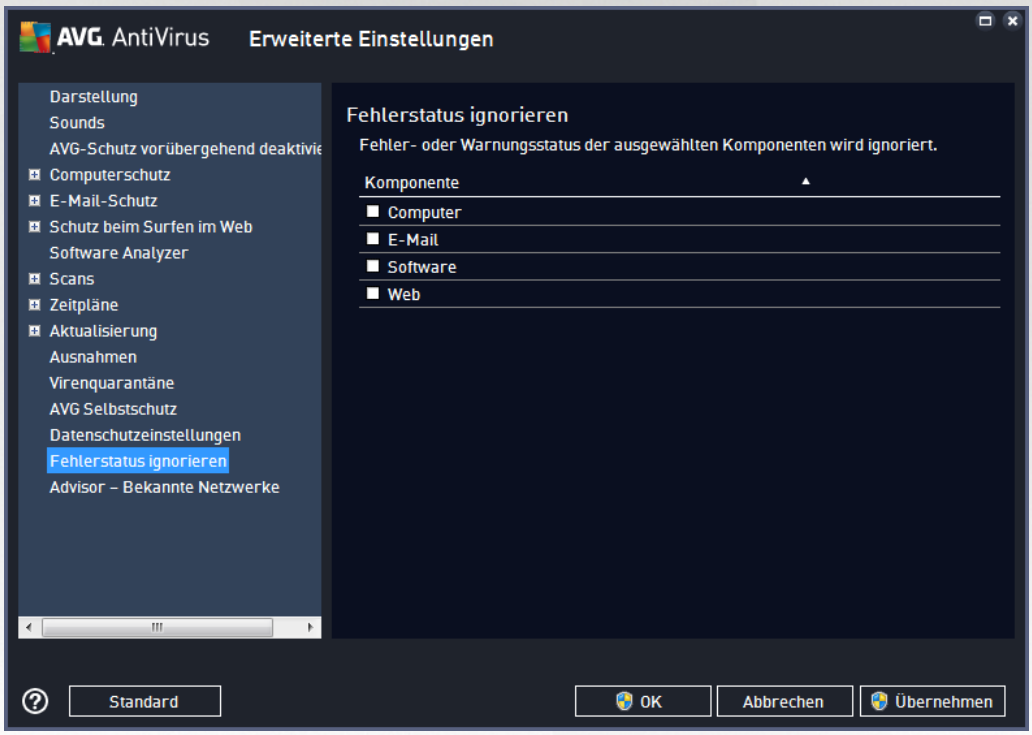
Im Dialog sind folgende Einstellungsoptionen verfügbar:

- ***Ich möchte AVG durch die Teilnahme am AVG-Programm zur Produktverbesserung dabei helfen, die Produkte zu verbessern*** *(standardmäßig aktiviert)* – Wenn Sie uns helfen möchten, **AVG AntiVirus** auch weiterhin zu verbessern, lassen Sie dieses Kontrollkästchen aktiviert. Dadurch wird die Berichterstattung über aufgetretene Bedrohungen an AVG aktiviert, sodass wir von allen Benutzern weltweit aktuelle Informationen über Malware sammeln und als Gegenleistung zuverlässigen Schutz bieten können. Die Berichterstattung erfolgt automatisch und ohne Beeinträchtigungen. In den Berichten sind keine persönlichen Daten enthalten.
    - ***Senden von Daten zu falsch identifizierten E-Mails nach Bestätigung durch den Benutzer zulassen*** *(standardmäßig aktiviert)* – Sendet Informationen zu fälschlicherweise als Spam eingestuften Nachrichten bzw. zu Spam-Nachrichten, die von der Anti-Spam-Komponente nicht erkannt wurden. Vor dem Versand dieser Informationen werden Sie um eine Bestätigung gebeten.
    - ***Senden von anonymen Daten zu identifizierten oder verdächtigen Bedrohungen zulassen*** *(standardmäßig aktiviert)* – Sendet Informationen zu allen auf Ihrem Computer ermittelten verdächtigen oder tatsächlich gefährlichen Codes oder Verhaltensmustern *(dabei kann es sich um Viren, Spyware oder bösartige Websites handeln, auf die Sie zugreifen möchten)* .
    - ***Senden von anonymen Daten zur Produktnutzung zulassen*** *(standardmäßig aktiviert)* – Sendet grundlegende Statistiken über die Nutzung von Anwendungen, wie etwa die Zahl der Erkennungen, der ausgeführten Scans, der erfolgreichen/fehlgeschlagenen Updates usw.
- ***In-the-Cloud-Überprüfungen von Erkennungen zulassen*** *(standardmäßig aktiviert)* – Erkannte Bedrohungen werden daraufhin überprüft, ob es sich tatsächlich um Infektionen handelt, damit falsche Positivmeldungen vermieden werden können.

- ***Ich möchte, dass AVG meine Benutzererfahrung durch Aktivieren von AVG-Anpassung individuell gestaltet*** *(standardmäßig deaktiviert)* – Diese Funktion führt eine anonyme Analyse des Verhaltens von Programmen und Anwendungen auf Ihrem Computer durch. Anhand dieser Analyse kann AVG Ihnen gezielt auf Ihre Anforderungen zugeschnittene Dienste anbieten und maximale Sicherheit gewährleisten.

7.15. Fehlerstatus ignorieren

Im Dialogfeld ***Fehlerstatus ignorieren*** können Sie die Komponenten markieren, über die Sie nicht informiert werden möchten:



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

- Infobereichsymbol – 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 im Bereich Informationen zum Sicherheitsstatus im Hauptfenster von AVG erscheint eine Beschreibung des bestehenden Problems.

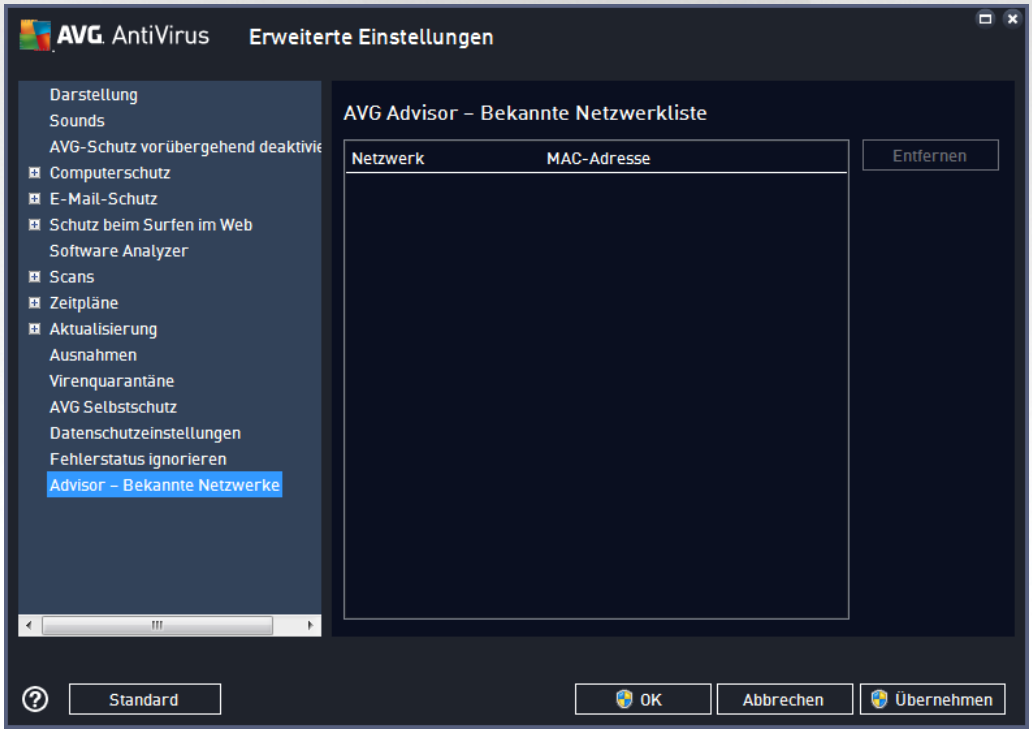
Es kann vorkommen, dass Sie aus einem bestimmten Grund eine Komponente vorübergehend deaktivieren müssen. ***Dies wird nicht empfohlen. Sie sollten versuchen, alle Komponenten permanent aktiviert zu lassen und die Standardeinstellungen beizubehalten.*** Eine solche Situation kann jedoch auftreten.
In diesem Fall zeigt das Infobereichsymbol 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 Dialogfenster ***Fehlerstatus ignorieren*** Komponenten auswählen, die eventuell einen fehlerhaften Status aufweisen (*oder deaktiviert sind*) oder über die Sie keine Informationen erhalten möchten. Klicken Sie auf ***OK, um die Änderungen zu bestätigen.***

7.16. Advisor – Bekannte Netzwerke

AVG Advisor beinhaltet eine Funktion, die Netzwerke überwacht, zu denen Sie eine Verbindung herstellen. Sobald ein neues Netzwerk gefunden wird *(mit einem bereits verwendeten Netzwerknamen, was zu Verwirrung führen kann)*, werden Sie benachrichtigt, und es wird empfohlen, die Sicherheit des Netzwerks zu überprüfen. Wenn Sie beschließen, dass dieses Netzwerk sicher ist, können Sie es in dieser Liste speichern *(Über den Link in der AVG Advisor-Taskleistenbenachrichtigung, die über der Taskleiste angezeigt wird, sobald ein unbekanntes Netzwerk erkannt wird. Weitere Informationen erhalten Sie im Kapitel AVG Advisor)*. AVG Advisor merkt sich dann die Eigenschaften des Netzwerks *(insbesondere die MAC-Adresse)* und zeigt die Benachrichtigung beim nächsten Mal nicht an. Jedes Netzwerk, zu dem Sie eine Verbindung herstellen, wird automatisch als bekannt gewertet und der Liste hinzugefügt. Sie können individuelle Einträge löschen, indem Sie auf die Schaltfläche ***Entfernen*** klicken. Das entsprechende Netzwerk wird dann wieder als unbekannt und möglicherweise nicht sicher betrachtet.

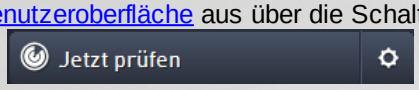
In diesem Dialogfenster können Sie überprüfen, welche Netzwerke als „bekannt“ gespeichert wurden:



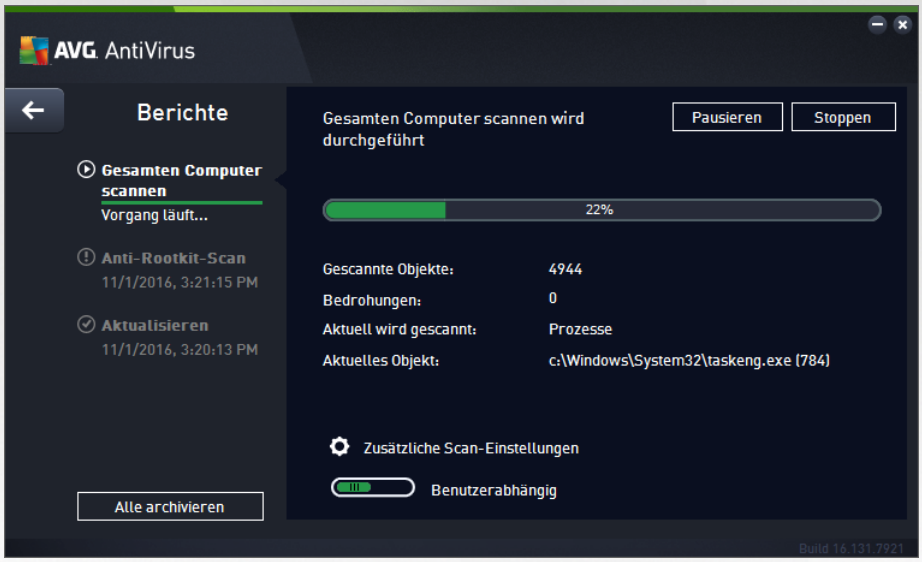
Hinweis: *Die Funktion „Bekannte Netzwerke“ von AVG Advisor wird unter Windows XP 64-Bit nicht unterstützt.*

8. AVG-Scans

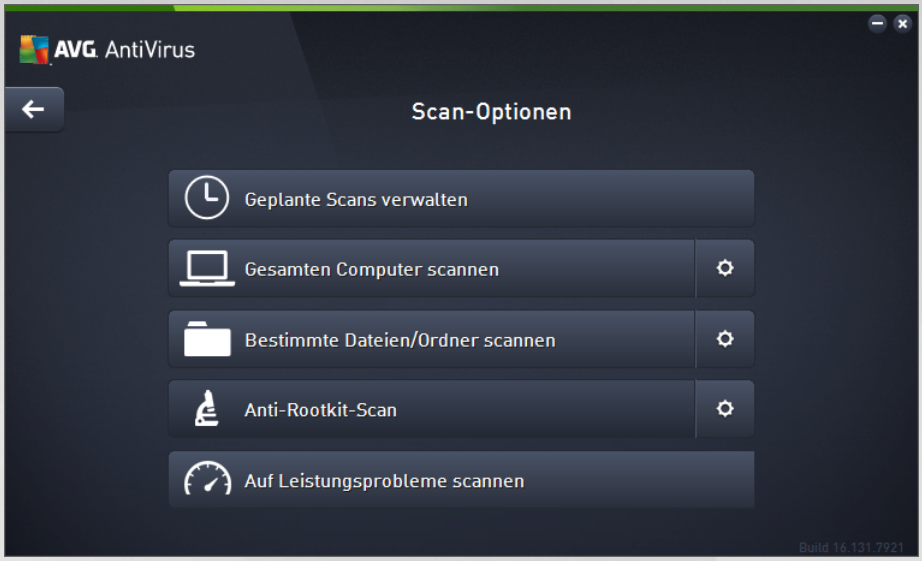
Standardmäßig führt **AVG AntiVirus** keine Scans aus, da Sie nach dem ersten Scan *(zu dessen Start Sie aufgefordert werden)* durch die residenten Komponenten von **AVG AntiVirus** optimal geschützt sein sollten, denn diese überwachen Ihren Computer zuverlässig und lassen keinen schädlichen Code durch. Selbstverständlich können Sie einen Scan planen, der in regelmäßigen Abständen ausgeführt wird, oder auch jederzeit ganz nach Ihrem Bedarf einen Scan starten.

Die Scan-Oberfläche von AVG kann von der Hauptbenutzeroberfläche aus über die Schaltfläche aufgerufen werden, die grafisch in zwei Abschnitte unterteilt ist: 

- ***Jetzt scannen*** – Klicken Sie auf diese Schaltfläche, um den Vorgang Gesamten Computer scannen sofort zu starten. Den Fortschritt und die Ergebnisse können Sie in dem automatisch angezeigten Fenster Berichte ablesen:



- ***Optionen*** – Wählen Sie diese Schaltfläche *(dargestellt als drei horizontale Linien in einem grünen Feld)*, um das Dialogfeld ***Scan-Optionen*** zu öffnen, in dem Sie geplante Scans verwalten und Parameter für Gesamten Computer scannen / Bestimmte Dateien/Ordner scannen festlegen können.



Im Dialogfeld ***Scan-Optionen*** werden drei Hauptabschnitte der Scan-Konfigurationen angezeigt:

- ***Geplante Scans verwalten*** – Klicken Sie auf diese Option, um ein neues Dialogfeld mit einer Übersicht aller geplanten Scans anzuzeigen. Bevor Sie Ihre eigenen Scans definieren, wird nur ein geplanter Scan angezeigt, der von dem in der Grafik aufgeführten Software-Hersteller voreingestellt wurde. Der Scan ist standardmäßig deaktiviert. Um ihn zu aktivieren, klicken Sie mit der rechten Maustaste darauf und wählen Sie im Kontextmenü die Option *Aufgabe aktivieren*. Sobald der geplante Scan aktiviert ist, können Sie die Konfiguration bearbeiten, indem Sie auf die Schaltfläche *Bearbeiten* klicken. Sie können auch auf die Schaltfläche *Hinzufügen* klicken, um einen neuen eigenen Zeitplan zu erstellen.

- ***Gesamten Computer scannen/Einstellungen*** – Diese Schaltfläche ist in zwei Abschnitte aufgeteilt. Klicken Sie auf die Option *Gesamten Computer scannen*, um den Scan für Ihren gesamten Computer sofort zu starten *(genauere Informationen zum Scan des gesamten Computers können Sie dem entsprechenden Kapitel Vordefinierte Scans/Gesamten Computer scannen entnehmen)*. Wenn Sie auf den Abschnitt *Einstellungen* klicken, wird das Dialogfeld für die Konfiguration des Scans für den gesamten Computer aufgerufen.

- ***Bestimmte Dateien/Ordner scannen/Einstellungen*** – Auch diese Schaltfläche ist in zwei Abschnitte aufgeteilt. Klicken Sie auf die Option *Bestimmte Dateien/Ordner scannen*, um den Scan für ausgewählte Bereiche Ihres Computers sofort zu starten *(genauere Informationen zum Scan des gesamten Computers können Sie dem entsprechenden Kapitel Vordefinierte Scans/Bestimmte Dateien/Ordner scannen* entnehmen). Wenn Sie auf den Abschnitt *Einstellungen* klicken, wird das Dialogfeld für die Konfiguration des Scans bestimmter Dateien oder Ordner aufgerufen.

- ***Computer auf Rootkits scannen/Einstellungen*** – Der linke Bereich der Schaltfläche mit der Bezeichnung *Computer auf Rootkits scannen* startet umgehend Anti-Rootkit-Scans *(weitere Details zum Rootkit-Scan finden Sie im entsprechenden Kapitel Vordefinierte Scans/Computer auf Rootkits scannen).* Wenn Sie auf den Abschnitt *Einstellungen* klicken, wird das Dialogfeld für die Konfiguration des Rootkit-Scans aufgerufen.

8.1. Vordefinierte Scans

Eine der Hauptfunktionen von **AVG AntiVirus** ist ein bedarfsorientierter Scan. Tests bei Bedarf 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.

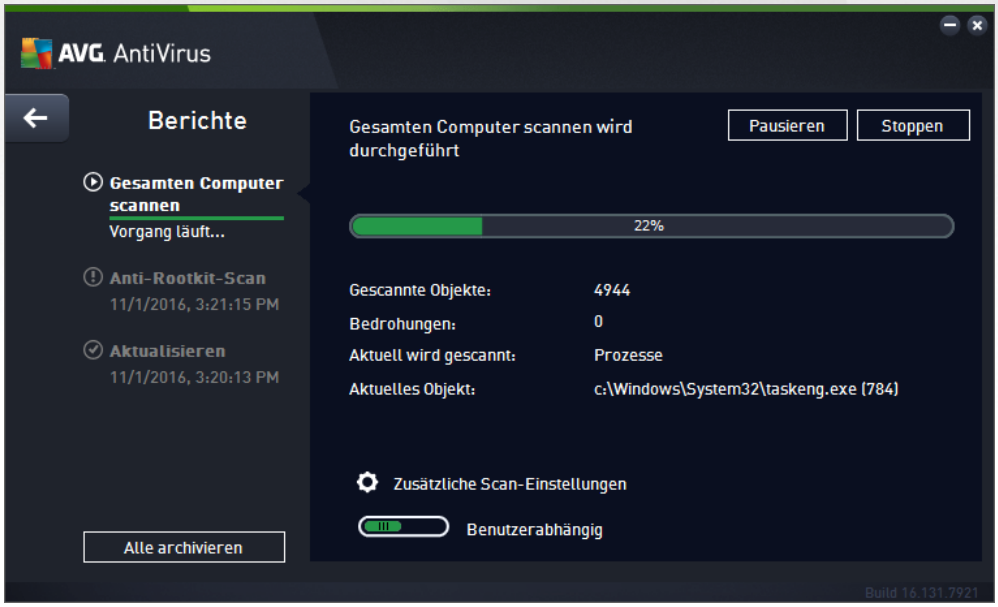
In **AVG AntiVirus** gibt es folgende vom Software-Hersteller vordefinierte Arten von Scans:

8.1.1. Gesamten Computer scannen

Gesamten Computer scannen untersucht Ihren gesamten Computer auf mögliche Infektionen und/oder potenziell unerwünschte Anwendungen. 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 mindestens einmal pro Woche auf Ihrem Computer geplant werden.

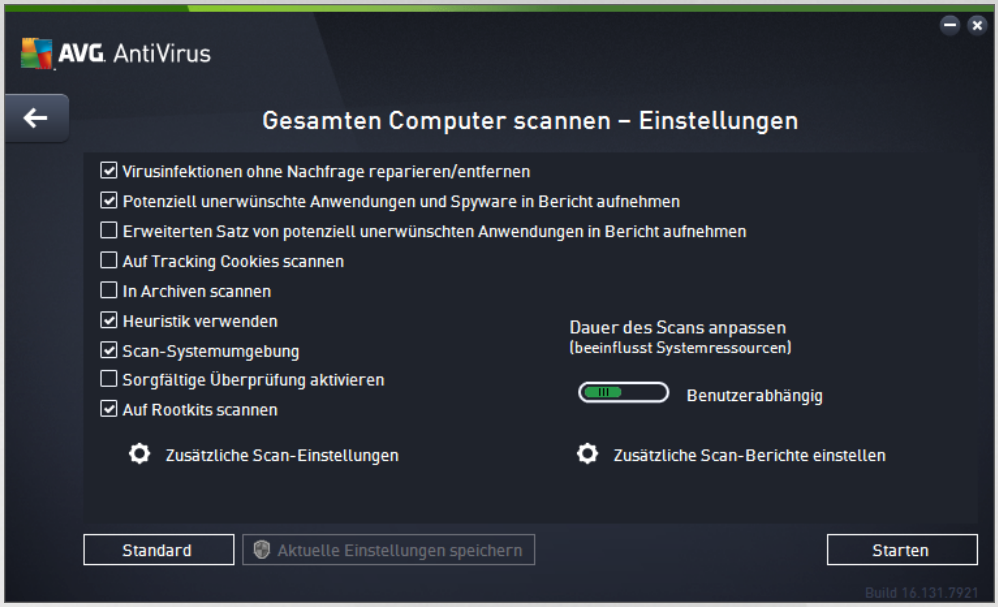
Start von Scans

Die Option ***Gesamten Computer scannen*** kann direkt von der Hauptbenutzeroberfläche aus durch Klicken auf die Schaltfläche ***Jetzt scannen*** gestartet werden. Für diesen Scan müssen keine weiteren spezifischen Einstellungen konfiguriert werden. Der Scan wird sofort gestartet. Im Dialogfeld ***Gesamten Computer scannen – Vorgang läuft*** (*siehe Screenshot*) können Sie den Fortschritt und die Ergebnisse des Scans anzeigen. Der Scanvorgang kann bei Bedarf unterbrochen (***Unterbrechen***) oder abgebrochen (***Anhalten***) werden.



Bearbeitung der Scan-Konfiguration

Sie können die Konfiguration der Option ***Gesamten Computer scannen*** im Dialogfeld ***Gesamten Computer scannen – Einstellungen*** bearbeiten *(Klicken Sie dazu im Dialogfeld Scan-Optionen auf den Link „Einstellungen“ unter „Gesamten Computer scannen“).* ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, es besteht ein triftiger Grund, sie zu ändern!***



In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter ein- bzw. ausschalten:

- ***Virusinfektionen ohne Nachfrage reparieren/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 repariert werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert)* – Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** *(standardmäßig deaktiviert)* – Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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 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, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

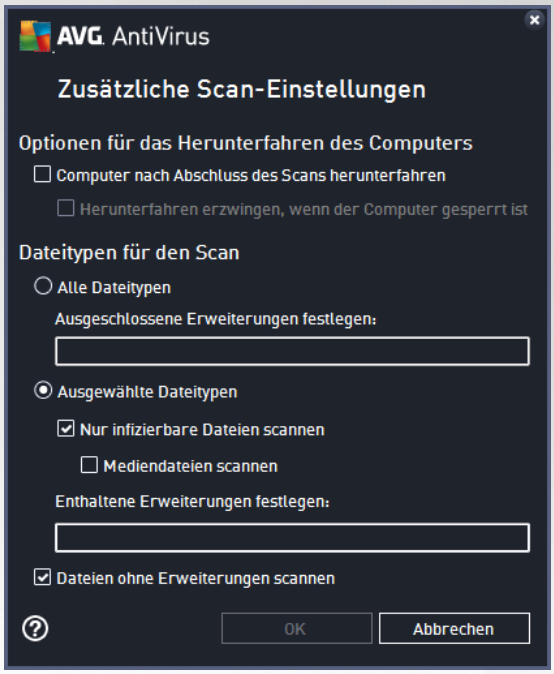
- ***Heuristik verwenden*** *(standardmäßig aktiviert)* – Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse *(dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung)* verwendet.

- ***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 umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.

- ***Auf Rootkits scannen*** *(standardmäßig aktiviert)* – Bietet Anti-Rootkit-Scans beim Scannen des gesamten Computers. Der Anti-Rootkit-Scan kann auch getrennt ausgeführt werden.

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird das Dialogfeld „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*** – Sie sollten außerdem bestimmen, welche Elemente überprüft werden:

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

    - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potenziell infizierte 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 dieses Kontrollkästchen deaktiviert bleibt,*

ist die Scan-Zeit 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.

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

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

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet das Dialogfeld ***Scan-Berichte***, in dem Sie auswählen können, welche Scan-Ergebnisse gemeldet werden:

Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein (wie im Kapitel AVG-Scans/Scans planen/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.*

8.1.2. Bestimmte Dateien/Ordner scannen

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

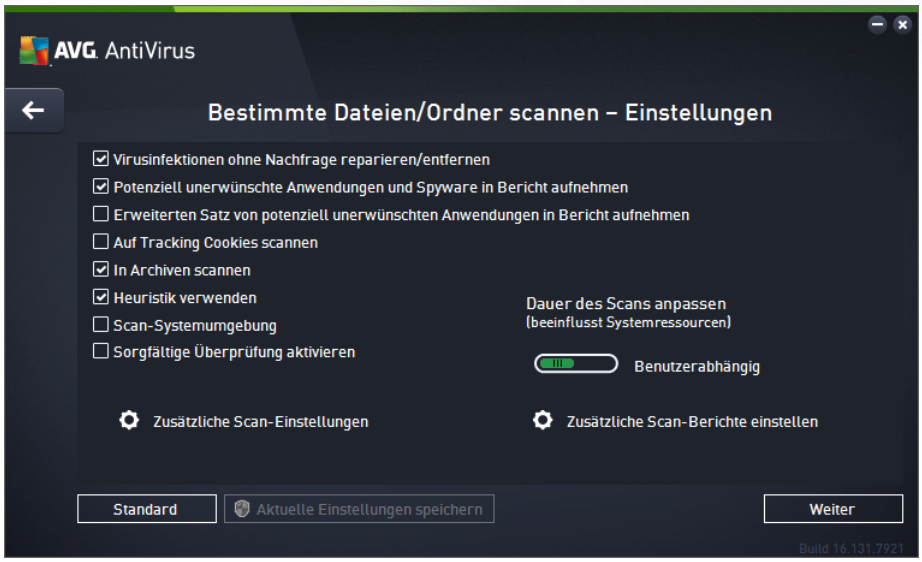
Start von Scans

Der ***Scan bestimmter Dateien oder Ordner*** kann direkt im Dialogfeld Scan-Optionen gestartet werden, indem Sie auf die Schaltfläche **Bestimmte Dateien/Ordner scannen** klicken. Das Dialogfeld ***Bestimmte Dateien***

oder Ordner zum Scannen auswählen wird geöffnet. Wählen Sie in der Baumstruktur Ihres Computers den zu scannenden Ordner aus. Der Pfad zu jedem Ordner wird automatisch generiert und im Textfeld im oberen Bereich dieses Dialogfelds angezeigt. Sie können außerdem einen bestimmten Ordner scannen, seine Unterordner jedoch vom Scan ausschließen. Setzen Sie dazu ein Minuszeichen „**-**“ vor den automatisch generierten Pfad (*siehe Screenshot*). Um den gesamten Ordner vom Scan auszuschließen, verwenden Sie das Ausrufezeichen (!). Klicken Sie zum Starten des Scans auf die Schaltfläche ***Scan starten***. Der Scanvorgang entspricht im Grunde genommen dem Scan des gesamten Computers.

Bearbeitung der Scan-Konfiguration

Sie können die Konfiguration der Option ***Bestimmte Dateien/Ordner scannen*** im Dialogfeld ***Bestimmte Dateien/Ordner scannen – Einstellungen*** bearbeiten *(Klicken Sie dazu im Dialogfeld Scan-Optionen auf den Link „Einstellungen“ unter „Bestimmte Dateien/Ordner scannen“).* ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, es besteht ein triftiger Grund, sie zu ändern!***



In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter ein- bzw. ausschalten:

- ***Virusinfektionen ohne Nachfrage reparieren/entfernen*** *(standardmäßig aktiviert)*: Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, wenn eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch repariert werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert)*: Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** *(standardmäßig deaktiviert)*: Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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 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*).

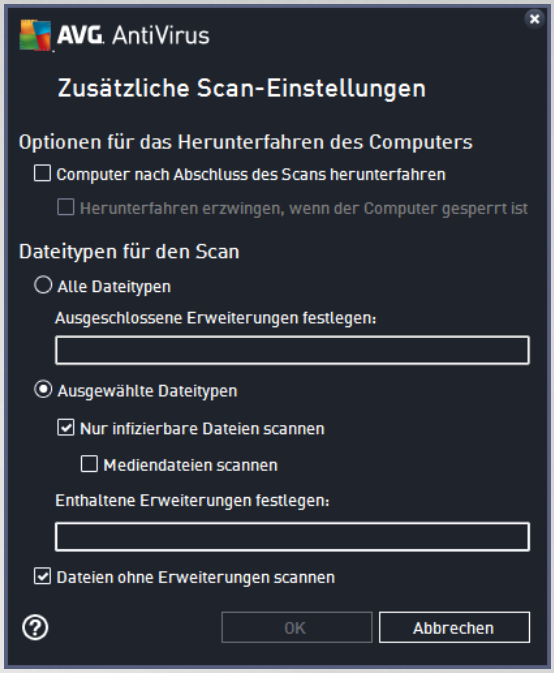
- ***In Archiven scannen*** *(standardmäßig aktiviert)*: Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, auch solche, die in Archiven (ZIP, RAR usw.) gespeichert sind.

- ***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 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 umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die nur selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird das Dialogfeld ***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*** – Sie sollten außerdem bestimmen, welche Elemente überprüft werden:

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

  - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potenziell infizierte 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 dieses Kontrollkästchen deaktiviert bleibt, ist die Scan-Zeit 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.

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

- ***Dauer des Scans anpassen*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen,

wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet das Dialogfeld ***Scan-Berichte***, in dem Sie auswählen können, welche Scan-Ergebnisse gemeldet werden sollen:

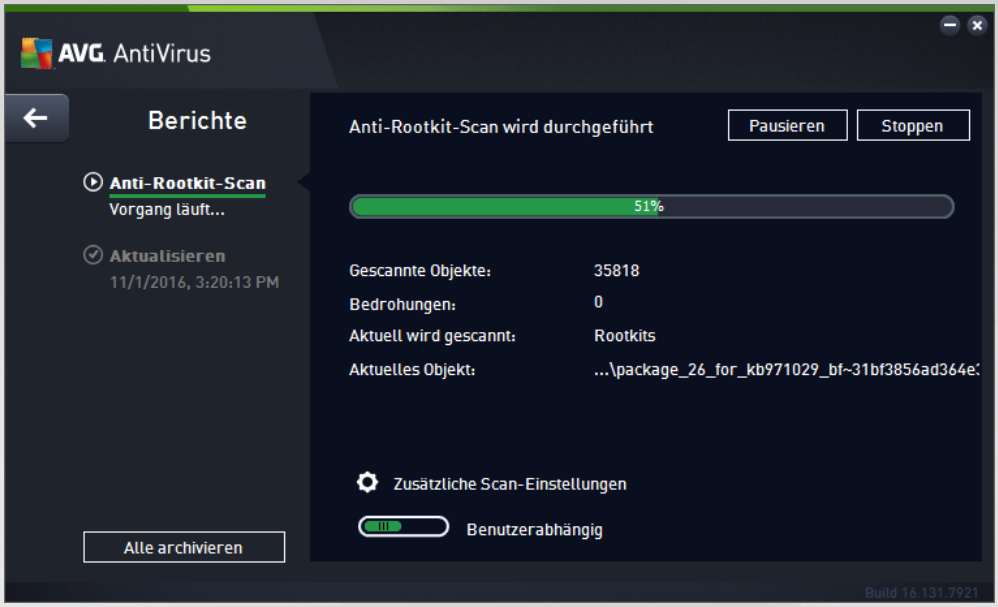
Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein (wie im Kapitel AVG-Scans/Scans planen/Vorgehensweise beim Scannen beschrieben). Wenn Sie die Standardkonfiguration der Option* ***Bestimmte Dateien/Ordner scannen*** *ändern, können Sie Ihre neuen Einstellungen 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).*

8.1.3. Computer auf Rootkits scannen

Computer auf Rootkits scannen erkennt und entfernt effektiv gefährliche Rootkits wie z. B. Programme und Technologien, die das Vorhandensein von schädlicher Software auf Ihrem Computer verschleiern können. Ein Rootkit wurde dafür entwickelt, ohne Genehmigung der Systembesitzer oder berechtigten Manager die Kontrolle über ein Computersystem zu übernehmen. Der Scan erkennt Rootkits auf Basis eines vordefinierten Regelsatzes. Wird ein Rootkit gefunden, bedeutet das nicht unbedingt, dass Ihr Computer infiziert ist. Manchmal werden Rootkits als Treiber eingesetzt oder sie gehören zu ordnungsgemäßen Anwendungen.

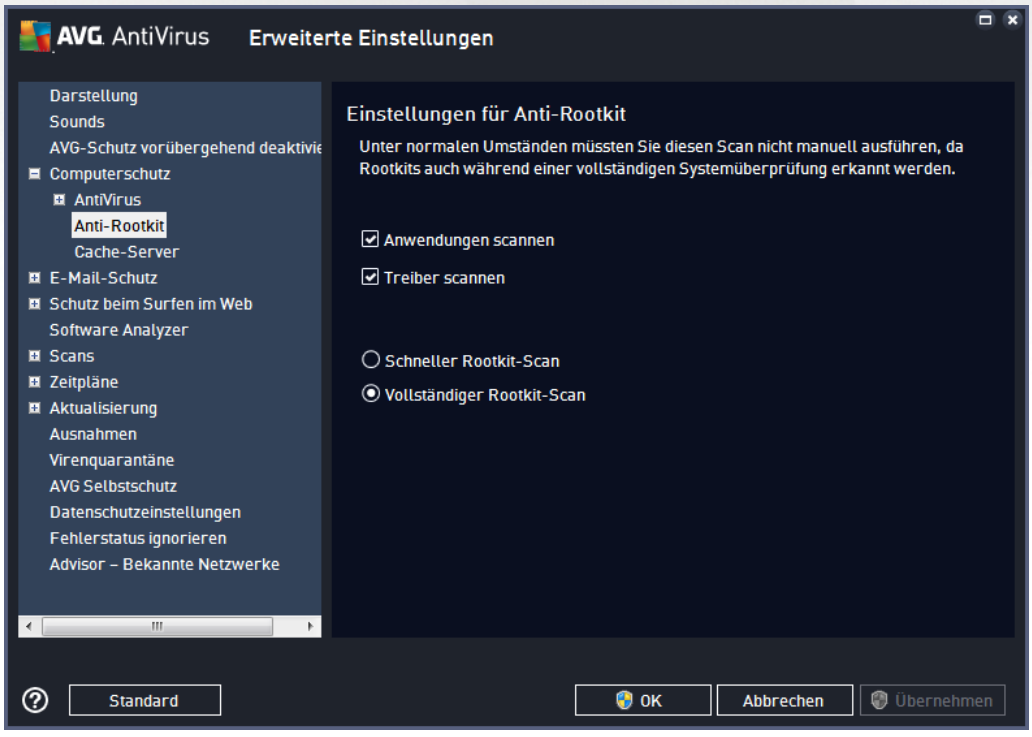
Start von Scans

Computer auf Rootkits scannen kann direkt aus dem Dialogfeld Scan-Optionen durch Klicken auf die Schaltfläche ***Computer auf Rootkits scannen*** gestartet werden. Der neue Dialog ***Anti-Rootkit-Scan wird ausgeführt*** wird mit dem Status des gestarteten Scans geöffnet:



Bearbeitung der Scan-Konfiguration

Sie können die Konfiguration für den Anti-Rootkit-Scan im Dialogfeld ***Einstellungen für Anti-Rootkit*** bearbeiten *(klicken Sie dazu im Dialogfeld Scan-Optionen auf den Link „Einstellungen“ für „Computer auf Rootkits scannen“).* ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, es besteht ein triftiger Grund, sie zu ändern!***

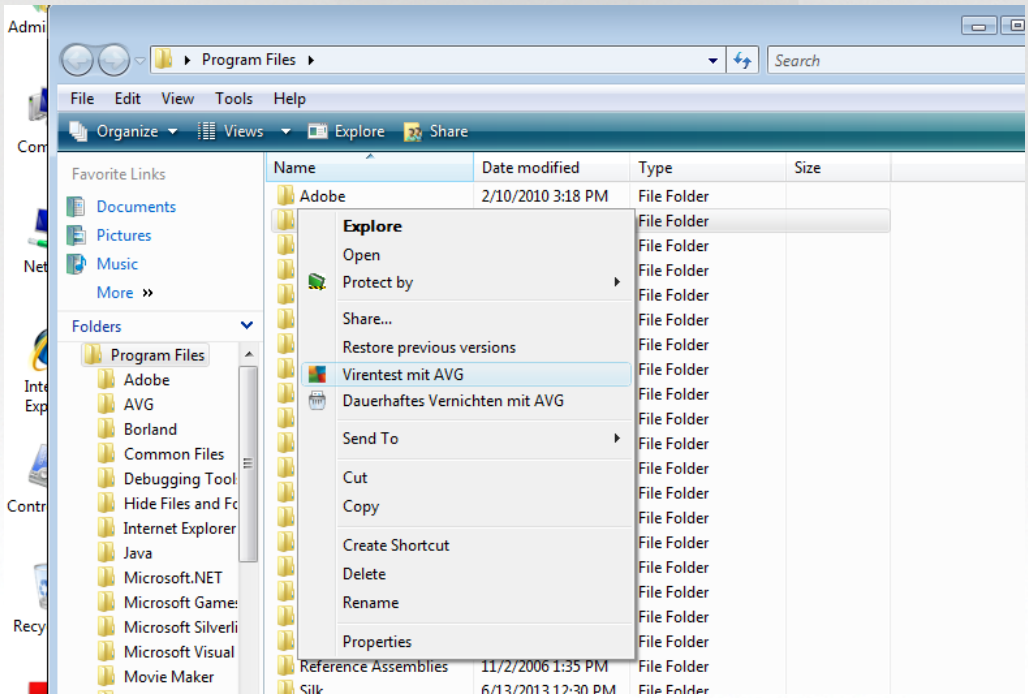


Mit ***Anwendungen scannen*** und ***Treiber scannen*** können Sie detailliert angeben, was im Anti-Rootkit-Scan enthalten sein soll. Diese Konfigurationsmöglichkeiten sind für erfahrene Benutzer gedacht. Es wird empfohlen, keine der Optionen zu deaktivieren. Sie können auch den Rootkit-Scanmodus auswählen:

- ***Schneller Rootkit-Scan*** – Prüft alle laufenden Prozesse, alle geladenen Treiber und den Systemordner (*typischerweise c:\Windows*).
- ***Vollständiger Rootkit-Scan*** – Prüft alle laufenden Prozesse, alle geladenen Treiber, den Systemordner (*typischerweise c:\Windows*) und zusätzlich alle lokalen Festplatten (*einschließlich Flash-Disks, aber keine Disketten-/CD-Laufwerke*).

8.2. Scans aus dem Windows Explorer

Neben den vordefinierten Scans, die für den gesamten Computer oder ausgewählte Bereiche gestartet werden, umfasst **AVG AntiVirus** 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 AntiVirus***, um die Datei mit AVG zu scannen **AVG AntiVirus**

8.3. Befehlszeilen-Scan

Mit **AVG AntiVirus** 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

8.3.1. 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 eine Reihe geschrieben und durch ein Leerzeichen und einen Schrägstrich getrennt sein.
- Wenn ein Parameter einen bestimmten Wert erfordert (der Parameter ***/scan*** erfordert z. B. Informationen über die Bereiche Ihres Computers, die gescannt werden sollen, und die genaue Pfadangabe zum ausgewählten Bereich), werden die einzelnen Werte durch Semikolons getrennt, z. B.: ***avgscanx /scan=C:\;D:***

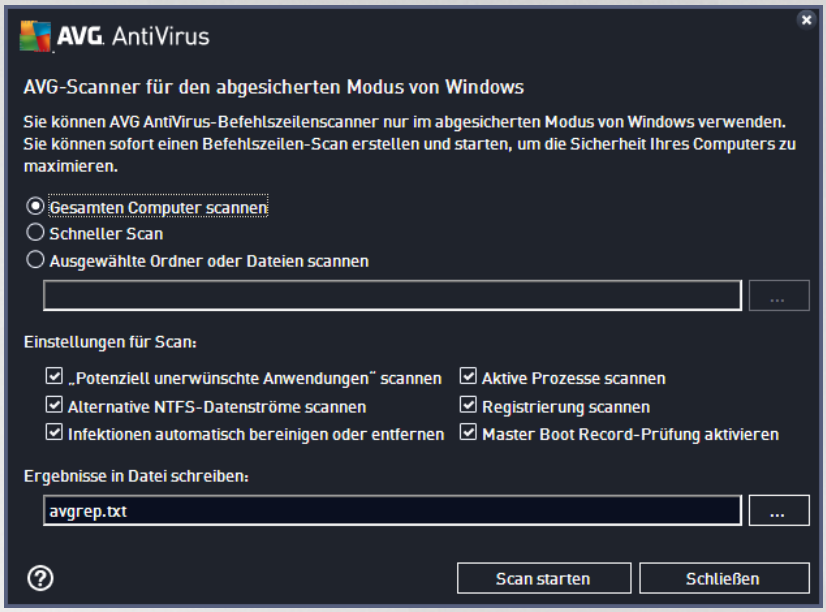
8.3.2. Scan-Parameter

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.

8.3.3. CMD-Scan über die Benutzeroberfläche starten

Wenn Ihr Computer im abgesicherten Modus ausgeführt wird, können Sie den Befehlszeilen-Scan auch über die grafische Benutzeroberfläche starten:



Im abgesicherten Modus wird der Scan von der Befehlszeile aus durchgeführt. In diesem Dialog können Sie nur die Scan-Parameter auf der komfortablen grafischen Benutzeroberfläche festlegen.

Wählen Sie zunächst die Bereiche des Computers, die gescannt werden sollen. Sie können entweder die vordefinierte Option ***Gesamten Computer scannen*** oder die Option ***Ausgewählte Ordner oder Dateien scannen*** wählen. Mit der dritten Option ***QuickScan*** wird ein spezieller Scan gestartet, der für den abgesicherten Modus vorgesehen ist und alle kritischen Bereiche des Computers überprüft, die zum Booten erforderlich sind.

Über die Scan-Einstellungen im nächsten Abschnitt können Sie detaillierte Scan-Parameter festlegen. Es wird empfohlen, die Standardeinstellung zu übernehmen und einen Parameter nur dann zu deaktivieren, wenn es einen konkreten Grund dafür gibt:

- ***Auf „Potenziell unerwünschte Anwendungen" prüfen*** – Beim Scannen wird (neben gängigen Viren) auch nach Spyware gesucht.
- ***Alternative Datenströme scannen (nur NTFS)*** – Alternative NTFS-Datenströme sind eine Windows-Funktion, die von Angreifern (meist Hackern) missbraucht werden kann, um Daten, wie beispielsweise schädlichen Code, zu verbergen.
- ***Virusinfektionen automatisch reparieren/entfernen*** – Alle erkannten Infektionen werden behandelt und automatisch repariert bzw. vom Computer entfernt.
- ***Aktive Prozesse scannen*** – Prozesse und Anwendungen, die in den Speicher des Computers geladen sind, werden gescannt.
- ***Registrierung scannen*** – Die Windows-Registrierung wird gescannt.
- ***Master Boot Record-Prüfung aktivieren*** – Partitionstabelle und Boot-Sektor werden gescannt.

Im unteren Teil des Dialogs können Sie den Dateinamen und Typ des Scan-Berichts festlegen.

8.3.4. Parameter für CMD-Scan

Es folgt eine Liste aller für den Scan von Befehlszeilen verfügbaren Parameter:

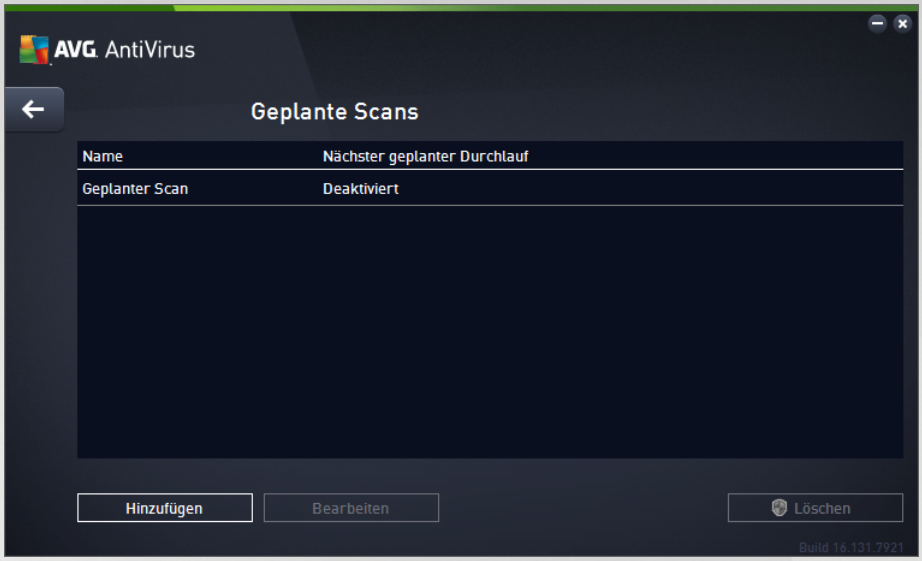
- /? Hilfe zu diesem Thema anzeigen
- /@ Befehlsdatei /Dateiname/
- /ADS Alternative Datenströme scannen *(nur NTFS)*
- /ARC Archive scannen
- /ARCBOMBSW Erneut komprimierte Archivdateien melden
- /ARCBOMBSW Archivbomben *(mehrfach komprim. Archive) in Bericht aufnehmen*
- /BOOT MBR/BOOT-Test aktivieren
- /BOOTPATH QuickScan starten
- /CLEAN Automatisch bereinigen
- /CLOUDCHECK Auf Fehlalarme prüfen
- /COMP Gesamten Computer scannen
- /COO Cookies scannen
- /EXCLUDE Pfad oder Datei(en) vom Scan ausschließen
- /EXT Diese Erweiterungen scannen *(z. B. EXT=EXE,DLL)*
- /FORCESHUTDOWN Herunterfahren erzwingen, wenn der Scan abgeschlossen ist
- /HELP Hilfe zu diesem Thema anzeigen
- /HEUR Heuristische Analyse verwenden
- /HIDDEN Dateien mit versteckten Erweiterungen in Bericht aufnehmen
- /IGNLOCKED Gesperrte Dateien ignorieren
- /INFECTABLEONLY Nur Dateien mit infizierbaren Erweiterungen prüfen
- /LOG Datei mit Scan-Ergebnissen erstellen
- /MACROW Makros in Bericht aufnehmen
- /NOBREAK Kein Abbrechen mit STRG-PAUSE
- /NOEXT Diese Erweiterungen nicht scannen *(z. B. NOEXT=JPG)*

- /PRIORITY Scan-Priorität einstellen *(niedrig, automatisch, hoch - siehe Erweiterte Einstellungen/Scans)*
- /PROC Aktive Prozesse scannen
- /PUP Auf potenziell unerwünschte Anwendungen prüfen
- /PUPEXT Erweiterten Satz potenziell unerwünschter Anwendungen in Bericht aufnehmen
- /PWDW Kennwortgeschützte Dateien in Bericht aufnehmen
- /QT Schnelltest
- /REG Registrierung scannen
- /REPAPPEND An die Berichtsdatei anhängen
- /REPOK Nicht infizierte Dateien als OK in Bericht aufnehmen
- /REPORT Bericht in Datei *(Dateiname)*
- /SCAN Bestimme Dateien oder Ordner scannen *(SCAN=path;path - z. B. /SCAN=C:\;D:\)*
- /SHUTDOWN Computer nach Abschluss des Scans herunterfahren
- /THOROUGHSCAN Sorgfältige Überprüfung aktivieren
- /TRASH Infizierte Dateien in Virenquarantäne ϖερσχηιεβεν

8.4. Scans planen

Mit **AVG AntiVirus** können Sie On-Demand-Scans *(z. B. wenn Sie befürchten, dass Ihr Computer infiziert wurde)* oder geplante Scans ausführen. Es wird dringend empfohlen, geplante Scans auszuführen. Auf diese Weise sorgen Sie dafür, dass Ihr Computer gegen Infektionen geschützt ist, und Sie müssen sich nicht darum kümmern, ob und wann ein Scan gestartet werden soll. Sie sollten die Funktion Gesamten Computer scannen regelmäßig, mindestens einmal pro Woche, verwenden. 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 zum Zeitpunkt eines geplanten Scans ausgeschaltet ist, wird dieser beim nächsten Start des Computers ausgeführt, wenn eine Aufgabe verpasst wurde.

Der Scan-Zeitplan kann im Dialogfeld ***Geplante Scans*** erstellt und bearbeitet werden. Klicken Sie dazu auf die Schaltfläche ***Geplante Scans verwalten*** im Dialogfeld Scan-Optionen. Im neuen Dialogfeld ***Geplanter Scan*** können Sie eine vollständige Übersicht über alle derzeit geplanten Scans anzeigen:

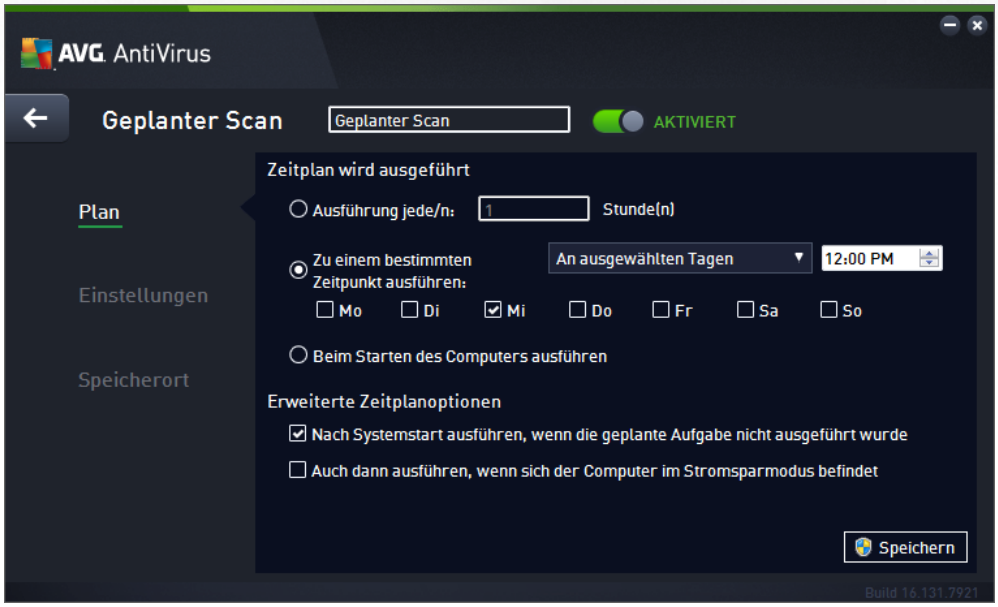


In dem Dialog können Sie Ihre eigenen Scans definieren. Klicken Sie auf die Schaltfläche ***Scan-Zeitplan hinzufügen***, um einen neuen eigenen Zeitplan zu erstellen. Auf den folgenden drei Registerkarten können die Parameter für den geplanten Scan bearbeitet (oder ein neuer Zeitplan erstellt) werden:

- Zeitplan
- Einstellungen
- Speicherort

Sie können den geplanten Test auf jeder Registerkarte über die „Ampel“-Schaltfläche vorübergehend deaktivieren und bei Bedarf hier wieder aktivieren.

8.4.1. Planen



Im oberen Teil der Registerkarte ***Plan*** befindet sich ein Textfeld, in dem Sie den Namen des aktuell definierten Scan-Zeitplans bestimmen können. 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 dagegen „Scan von Systembereichen“ usw.

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

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

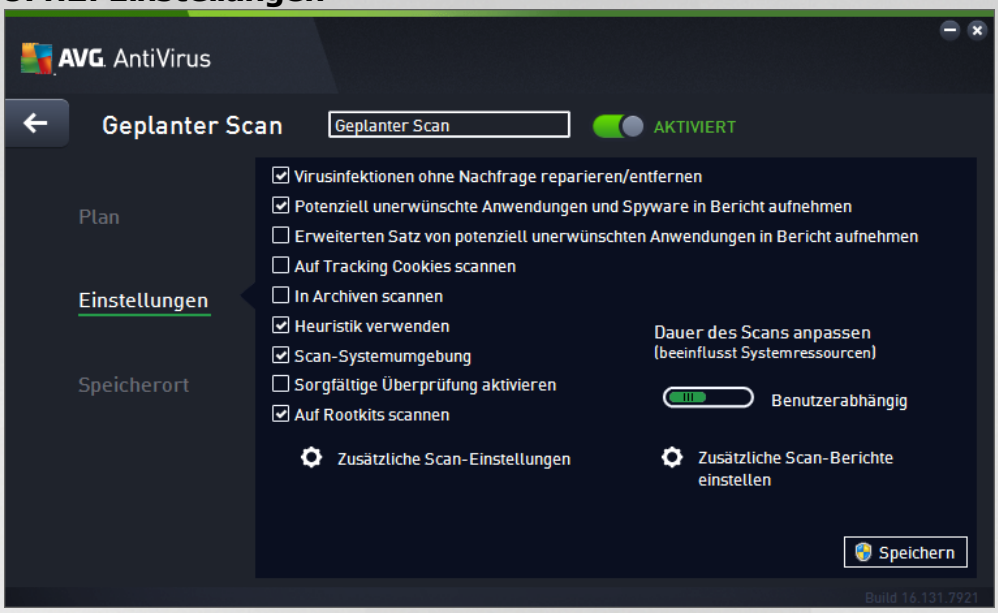
- ***Erweiterte Zeitplanoptionen*** – In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist. Sobald der geplante Scan zu der von Ihnen festgelegten Zeit startet, werden Sie über ein Popup-Fenster darüber informiert, das über dem Infobereichsymbol von AVG geöffnet wird. Daraufhin wird ein neues Infobereichsymbol von AVG angezeigt (in Vollfarbe und mit einer Ampel), das Sie darauf hinweist, dass derzeit 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 sowie die Priorität des momentan ausgeführten Scans ändern können.

Optionen im Dialogfeld

- ***Speichern*** – Speichert alle Änderungen, die Sie auf dieser Registerkarte oder einer anderen Registerkarte dieses Dialogfelds vorgenommen haben, und wechselt zurück zur Übersicht Geplante Scans. Wenn Sie die Parameter des Scans auf allen Registerkarten konfigurieren möchten, klicken Sie daher erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ← – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Übersicht Geplante Scans zurück.

8.4.2. Einstellungen



Im oberen Teil der Registerkarte ***Einstellungen*** befindet sich ein Textfeld, in dem Sie den Namen des derzeit definierten Scan-Zeitplans bestimmen können. 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 dagegen „Scan von Systembereichen“ usw.

Auf der Registerkarte ***Einstellungen*** finden Sie eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. ***Wenn kein triftiger Grund besteht, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten***:

- ***Virusinfektionen ohne Nachfrage reparieren/entfernen*** *(standardmäßig aktiviert):* Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, wenn eine Gegenmaßnahme vorhanden ist. Wenn die infizierte Datei nicht automatisch repariert werden kann, wird das infizierte Objekt in die Virenquarantäne verschoben.

- ***Potenziell unerwünschte Anwendungen und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert):* Aktivieren Sie dieses Kontrollkästchen, um den Scan auf Spyware sowie Viren zu starten. Spyware stellt eine problematische Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko darstellt, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potenziell unerwünschten Anwendungen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um erweiterte Pakete von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu böswilligen Zwecken 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.

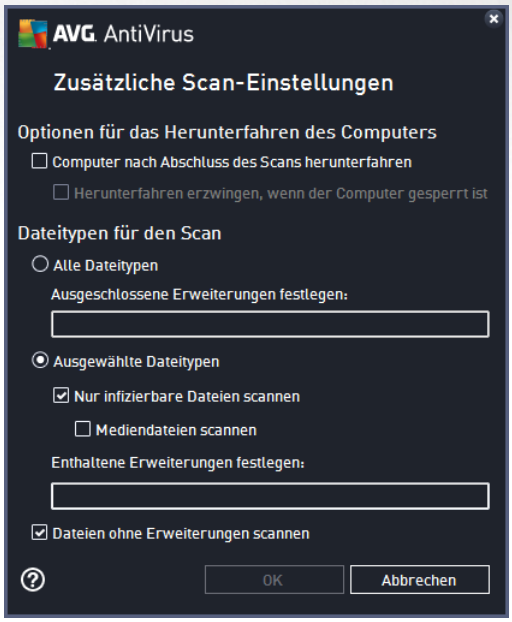
- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*): Dieser Parameter legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen*

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 umfassenden Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan zeitaufwendig ist.
- ***Auf Rootkits scannen*** *(standardmäßig aktiviert):* Anti-Rootkit-Scan überprüft Ihren Computer auf mögliche Rootkits, d. h. 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.

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*** – Sie sollten außerdem bestimmen, welche Elemente überprüft werden:
    - ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommas getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen.
    - ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potenziell infizierte 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 dieses Kontrollkästchen deaktiviert bleibt, ist die Scan-Zeit 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

In diesem Bereich 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 er zwar weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan ist aber deutlich höher, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber derzeit nicht verwendet wird*). Andererseits können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

Zusätzliche Scan-Berichte einstellen

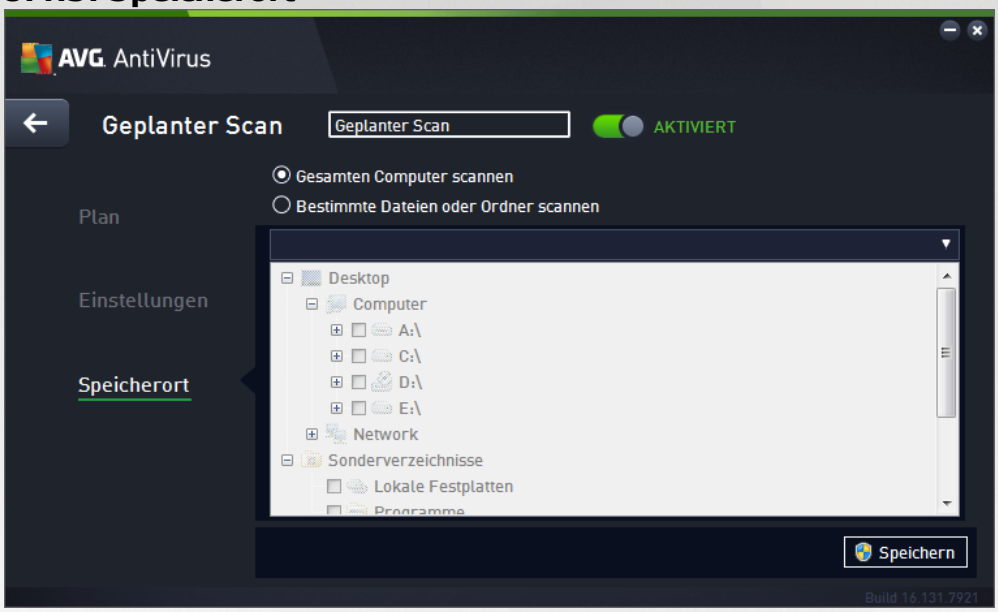
Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen...***, um das separate Dialogfeld ***Scan-Berichte*** zu öffnen, in dem Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:

Optionen im Dialogfeld

- ***Speichern*** – Speichert alle Änderungen, die Sie auf dieser Registerkarte oder einer anderen Registerkarte dieses Dialogfelds vorgenommen haben, und wechselt zurück zur Übersicht Geplante Scans. Wenn Sie die Parameter des Scans auf allen Registerkarten konfigurieren möchten, klicken Sie daher erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ← – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Übersicht Geplante Scans zurück.

8.4.3. Speicherort



Auf der Registerkarte ***Speicherort*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien/Ordner scannen wählen 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 werden im Textfeld im oberen Bereich des Dialogfelds angezeigt. Im Dropdown-Menü wird Ihr Scan-Verlauf für eine spätere Verwendung festgehalten. Alternativ können Sie den vollständigen Pfad zum entsprechenden Ordner manuell eingeben (*bei mehreren Pfaden müssen diese mit einem Semikolon ohne Leerzeichen voneinander getrennt werden*).

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

- ***Lokale Festplatten*** – alle Festplatten Ihres Computers

- ***Programmdateien***

    - C:\Programme\

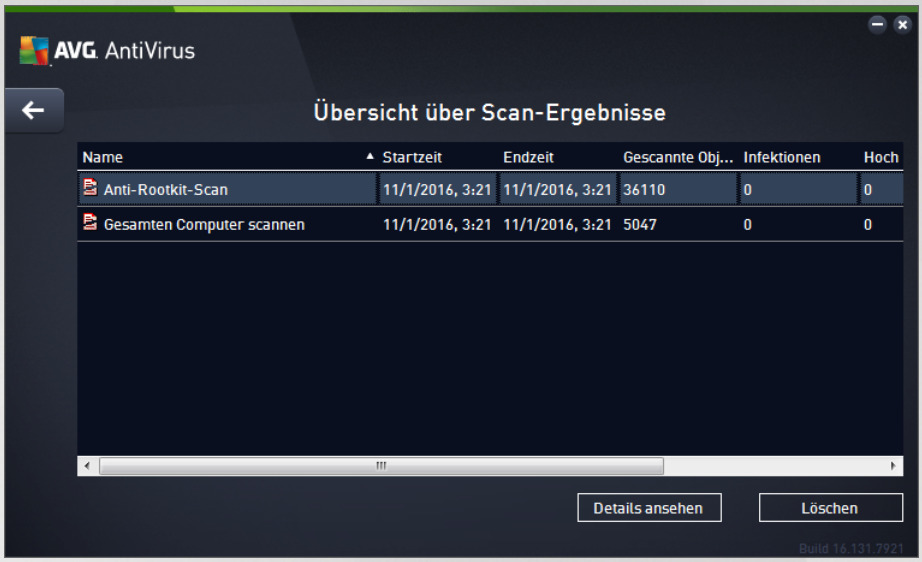
    - *in 64-Bit-Versionen* C:\Programme (x86)

- ***Eigene Dokumente***
    - *unter Windows XP:* C:\Dokumente und Einstellungen\Standardbenutzer\Eigene Dateien\
    - *unter Windows Vista/7*: C:\Benutzer\Benutzername\Eigene Dokumente\
- ***Gemeinsame Dokumente***
    - *unter Win XP*: C:\Dokumente und Einstellungen\Alle Benutzer\Dokumente\
    - *unter Windows Vista/7*: C:\Benutzer\Öffentlich\Öffentliche Dokumente\
- ***Windows-Ordner*** - C:\Windows\
- ***Andere***
    - *Systemlaufwerk* – die Festplatte, auf der das Betriebssystem installiert ist (normalerweise C:)
    - *Systemordner* – C:\Windows\System32\
    - *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*)

Optionen im Dialogfeld

- ***Speichern*** – Speichert alle Änderungen, die Sie auf dieser Registerkarte oder einer anderen Registerkarte dieses Dialogfelds vorgenommen haben, und wechselt zurück zur Übersicht Geplante Scans. Wenn Sie die Parameter des Scans auf allen Registerkarten konfigurieren möchten, klicken Sie daher erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.
- ← – Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Übersicht Geplante Scans zurück.

8.5. Scan-Ergebnisse



Das Dialogfeld ***Übersicht über Scan-Ergebnisse*** enthält eine Liste von Ergebnissen aller bisher ausgeführten Scans. Die Liste enthält die folgenden Informationen zu jedem Scan-Ergebnis:

- ***Symbol*** – Die erste Spalte zeigt ein Informationssymbol an, das den Status des Scans angibt:
  - Keine Infektionen erkannt, Scan abgeschlossen
  - Keine Infektionen erkannt, Scan vorzeitig unterbrochen
  - Infektionen erkannt, aber nicht geheilt, Scan abgeschlossen
  - Infektionen erkannt, aber nicht geheilt, Scan vorzeitig unterbrochen
  - Infektionen erkannt und geheilt oder entfernt, Scan abgeschlossen
  - Infektionen erkannt und geheilt oder entfernt, Scan vorzeitig unterbrochen
- ***Name*** – Die Spalte enthält den Namen des entsprechenden Scans. Dabei handelt es sich entweder um die zwei vordefinierten Scans oder Ihren geplanten Scan.
- ***Startzeit*** – Zeigt Datum und Uhrzeit des Scan-Starts an.
- ***Endzeit*** – Zeigt Datum und Uhrzeit an, zu der der Scan beendet, angehalten oder unterbrochen wurde.
- ***Gescannte Objekte*** – Gibt die Gesamtzahl der gescannten Objekte an.
- ***Infektionen*** – Gibt die Anzahl der entfernten/insgesamt erkannten Infektionen an.
- ***Hoch/Mittel/Niedrig*** – Die folgenden drei Spalten geben die Anzahl der erkannten Infektionen mit einem hohen, mittleren oder niedrigen Schweregrad an.

- ***Rootkits*** – Zeigt die Gesamtzahl der beim Scan erkannten Rootkits an.

Steuerelemente des Dialogfelds

Details ansehen – Klicken Sie auf die Schaltfläche, um detaillierte Informationen zu einem ausgewählten Scan *(in der Liste oben markiert)* anzuzeigen.

Ergebnisse löschen – Klicken Sie auf die Schaltfläche, um ausgewählte Scan-Ergebnisse aus der Liste zu entfernen.

– Über den grünen Pfeil links oben im Dialogfeld kehren Sie zur Hauptbenutzeroberfläche mit der Komponentenübersicht zurück.

8.6. Details zu den Scan-Ergebnissen

Klicken Sie zum Öffnen einer Übersicht mit detaillierten Informationen zu einem ausgewählten Scan-Ergebnis auf ***Details ansehen*** im Dialogfeld Übersicht über Scan-Ergebnisse. Sie werden zum gleichen Dialogfenster weitergeleitet, das detaillierte Informationen zu einem bestimmten Scan-Ergebnis anzeigt. Die Informationen sind auf drei verschiedene Registerkarten aufgeteilt:

- ***Zusammenfassung*** – Diese Registerkarte stellt grundlegende Informationen zum Scan bereit: Sie gibt an, ob der Scan erfolgreich durchgeführt wurde, ob Bedrohungen gefunden wurden und welche Maßnahmen ergriffen wurden.

- ***Details*** – Diese Registerkarte zeigt sämtliche Informationen zum Scan an, einschließlich Details zu erkannten Bedrohungen. Mit „Übersicht in Datei exportieren“ können Sie sie als CSV-Datei speichern.

- ***Erkennungen*** – Diese Registerkarte wird nur angezeigt, wenn während des Scans Bedrohungen erkannt wurden, und enthält detaillierte Informationen zu den Bedrohungen:

  Schweregrad Information: Informationen oder Warnungen, keine echte Bedrohungen. Üblicherweise handelt es sich um Makros, Dokumente oder Archive, die durch ein Kennwort geschützt sind, gesperrte Dateien usw.

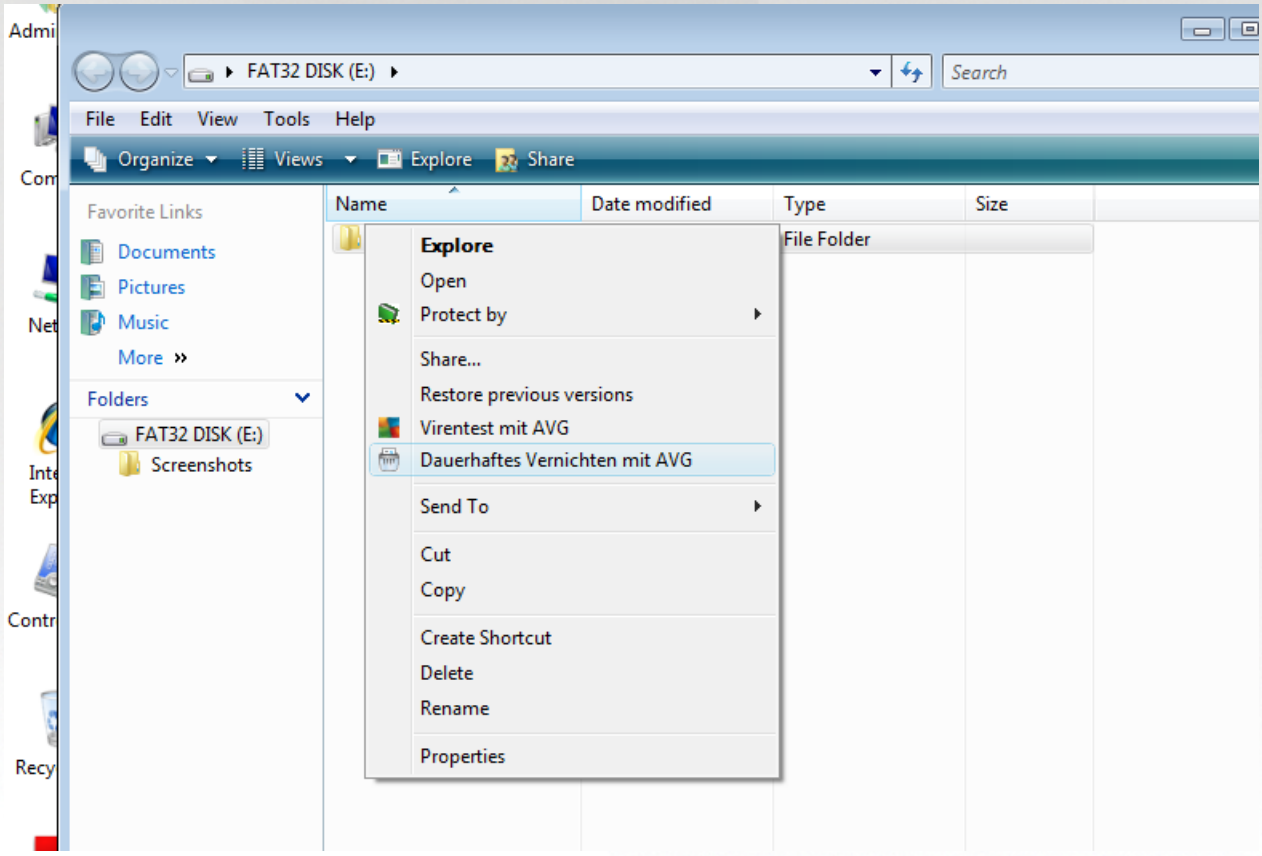
  Mittlerer Schweregrad: Normalerweise potenziell unerwünschte Anwendungen *(wie etwa Adware)* oder Tracking Cookies.

  Hoher Schweregrad: Gravierende Bedrohungen, wie z. B. Viren, Trojaner, Exploits usw. Auch von der Erkennungsmethode Heuristik erkannte Objekte, d. h. Bedrohungen, die noch keine Beschreibung in der Virendatenbank besitzen.

9. AVG File Shredder

Mit ***AVG File Shredder*** lassen sich Dateien absolut sicher löschen. D. h. es gibt keine Möglichkeit, einmal gelöschte Dateien wiederherzustellen, auch nicht mit leistungsstarken Software-Tools für diesen Zweck.

Um eine Datei oder einen Ordner zu vernichten, klicken Sie in einem Dateimanager *(Windows Explorer, Total Commander)* mit der rechten Maustaste auf die Datei bzw. den Ordner und wählen Sie im Kontextmenü ***Dauerhaft mit AVG vernichten***. Auch im Papierkorb befindliche Dateien können vernichtet werden. Wenn eine bestimmte Datei an einem bestimmten Speicherort*(z. B. CD-ROM)* nicht zuverlässig vernichtet werden kann, erhalten Sie eine entsprechende Benachrichtigung oder die Option ist im Kontextmenü von vornherein nicht verfügbar.



Beachten Sie dabei immer Folgendes: Wenn Sie eine Datei vernichten, kann diese unter keinen Umständen wiederhergestellt werden.

10. Virenquarantäne

Virenquarantäne ist eine sichere Umgebung zur Verwaltung von verdächtigen und infizierten Objekten, die von AVG beim Scan erkannt wurden. Sobald beim Scan ein infiziertes Objekt erkannt wird und AVG dieses nicht automatisch heilen kann, werden Sie gefragt, wie dieses verdächtige Objekt behandelt werden soll. Es wird empfohlen, das Objekt zur weiteren Behandlung in die ***Virenquarantäne*** zu verschieben. Die ***Virenquarantäne*** ist in erster Linie dazu da, entfernte Dateien so lange zu speichern, bis sie an ihrem ursprünglichen Speicherort nicht mehr benötigt werden. Wenn das Fehlen der Datei zu Problemen führt, können Sie die betroffene Datei zur Analyse senden oder sie an ihrem ursprünglichen Speicherort wiederherstellen.

Die Oberfläche der ***Virenquarantäne*** wird in einem eigenen Fenster geöffnet und enthält Informationen zu infizierten Objekten, die sich in der Quarantäne befinden:

- ***Hinzugefügt am*** – Gibt Datum und Uhrzeit an, an dem/zu der die verdächtige Datei erkannt und in die Virenquarantäne verschoben wurde.
- ***Bedrohung*** – Falls Sie sich entschieden haben, die Komponente Software Analyzer (Identitätsschutz) innerhalb von **AVG AntiVirus** zu installieren, wird in diesem Bereich eine grafische Identifizierung des Schweregrads dargestellt: von unbedenklich *(drei grüne Punkte)* bis sehr gefährlich *(drei rote Punkte)*. Außerdem finden Sie Informationen zur Infektionsart und ihrem ursprünglichen Speicherort. Über den Link *Weitere Informationen* gelangen Sie zu einer Seite mit detaillierten Informationen zu der erkannten Bedrohung aus der Online-Virenenzyklopädie.
- ***Quelle*** – Gibt an, welche Komponente von **AVG AntiVirus** die jeweilige Bedrohung erkannt hat.
- ***Benachrichtigungen*** – In sehr seltenen Fällen werden in dieser Spalte detaillierte Kommentare zur jeweils erkannten Bedrohung angezeigt.

Schaltflächen

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

- ***Wiederherstellen*** – Die infizierte Datei wird zurück an ihren ursprünglichen Speicherort auf Ihrer Festplatte verschoben.
- ***Wiederherstellen als*** – Die infizierte Datei wird in den gewählten Ordner verschoben.
- ***Zur Analyse senden*** – Diese Schaltfläche ist nur aktiv, wenn Sie ein Objekt in der Liste von Erkennungen oben markieren. In einem solchen Fall haben Sie die Möglichkeit, die ausgewählte Erkennung zur detaillierten Analyse an das Virenlabor von AVG zu senden. Beachten Sie, dass diese Funktion vorrangig zum Senden von Dateien mit Fehlalarmen dient, das heißt Dateien, die von AVG als infiziert oder verdächtig eingestuft wurden, von denen Sie aber glauben, dass sie harmlos sind.
- ***Details*** – Um detaillierte Informationen zu einer bestimmten Bedrohung anzuzeigen, die sich in der ***Virenquarantäne*** befindet, markieren Sie das ausgewählte Element in der Liste, und klicken Sie auf ***Details***. Ein neues Dialogfeld mit einer Beschreibung der erkannten Bedrohung wird geöffnet.
- ***Löschen*** – Die infizierte Datei wird vollständig und unwiderruflich aus der ***Virenquarantäne*** gelöscht.

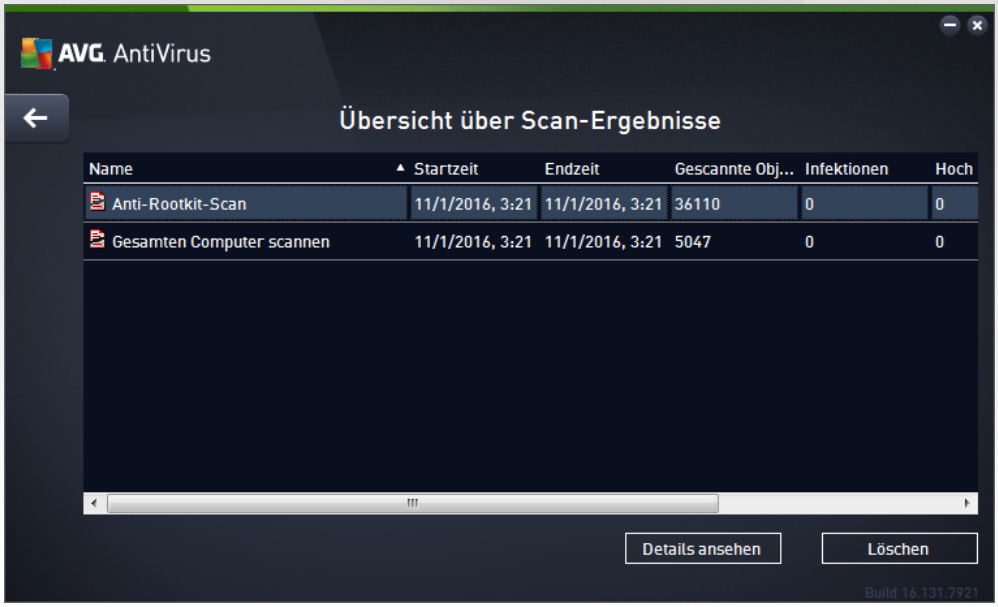
- ***Virenquarantäne leeren*** – Alle Objekte werden vollständig aus der ***Virenquarantäne*** entfernt. Durch Entfernen der Dateien aus der ***Virenquarantäne*** werden die Dateien unwiderruflich von der Festplatte entfernt (*nicht in den Papierkorb verschoben*).

11. Verlauf

Der Bereich ***Historie*** enthält Informationen zu allen vergangenen Ereignissen *(Updates, Scans, Erkennungen usw.)* und Berichte zu diesen Ereignissen. Dieser Bereich ist von der Hauptbenutzeroberfläche aus über ***Optionen > Historie*** erreichbar. Zudem ist die Historie aller gespeicherten Ereignisse in folgende Kategorien unterteilt:

- Scan-Ergebnisse
- Residenter Schutz – Ergebnisse
- E-Mail-Schutz – Ergebnisse
- Online Shield – Ergebnisse
- Ereignisprotokoll

11.1. Scan-Ergebnisse



Das Dialogfeld ***Übersicht über Scan-Ergebnisse*** kann über ***Optionen > Historie > Scan-Ergebnisse*** in der oberen Navigationszeile des Hauptfensters von **AVG AntiVirus** aufgerufen werden. Im Dialogfeld wird eine Liste aller zuvor gestarteten Scans sowie 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: *Hinweis: Genauere Informationen zu jedem Scan finden Sie im Dialogfeld Scan-Ergebnisse, auf das Sie über die Schaltfläche „Details ansehen" (im unteren Teil des Dialogfelds) zugreifen können.*

- ***Startzeit*** – Datum und Uhrzeit des gestarteten Scans
- ***Endzeit*** – Datum und Uhrzeit des Scan-Endes
- ***Gescannte Objekte*** – Anzahl der gescannten Objekte
- ***Infektionen*** – Anzahl der erkannten/entfernten Vireninfektionen
- ***Hoch/Mittel*** – Die Anzahl der entfernten/insgesamt erkannten Infektionen mit einem hohen oder mittleren Schweregrad
- ***Info*** – Informationen zum Ablauf und Ergebnis des Scans *(normalerweise nach dessen Abschluss oder bei Unterbrechung)*
- ***Rootkits*** – Anzahl der erkannten Rootkits

Schaltflächen

Im Dialogfeld ***Übersicht über Scan-Ergebnisse*** stehen folgende Schaltflächen zur Verfügung:

- ***Details ansehen*** – Klicken Sie auf diese Schaltfläche, um in das Dialogfeld Scan-Ergebnisse zu wechseln und detaillierte Daten zu einem ausgewählten Scan anzuzeigen.
- ***Ergebnis löschen*** – Klicken Sie auf diese Schaltfläche, um den gewählten Eintrag aus der Übersicht der Scan-Ergebnisse zu löschen.
- – Über den grünen Pfeil links oben im Dialogfeld können Sie zum standardmäßigen AVG-Hauptfenster *(Komponentenübersicht)* zurückkehren.

11.2. Residenter Schutz – Ergebnisse

Der Dienst ***Residenter Schutz*** ist Teil der Komponente ***Computer*** und scannt Dateien, wenn sie kopiert, geöffnet oder gespeichert werden. Wenn ein Virus oder eine andere Bedrohung erkannt wird, werden Sie unmittelbar mit folgendem Dialog gewarnt:

In dieser Warnmeldung werden Informationen zu dem erkannten und als infiziert eingestuften Objekt (*Bedrohung*) und eine Beschreibung der erkannten Infektion (*Beschreibung*) angezeigt. Über den Link *Weitere Informationen* gelangen Sie zu einer Seite mit detaillierten Informationen zur erkannten Bedrohung aus der Online-Virenenzyklopädie, sofern diese bekannt sind. Im Dialogfeld wird auch eine Übersicht mit vorhandenen Lösungen für die erkannte Bedrohung angezeigt. Einer der Vorschläge wird als empfohlen angezeigt: ***Schützen (empfohlen). Wenn möglich, sollten Sie immer diese Option wählen!***

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

Unten im Dialogfeld finden Sie den Link ***Details anzeigen***. Klicken Sie darauf, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess anzuzeigen, der beim Erkennen der Infektion ausgeführt wurde.

Eine Liste aller Erkennungen des Residenten Schutzes kann im Dialogfeld ***Residenter Schutz*** abgerufen werden. Das Dialogfeld kann über ***Optionen > Historie > Residenter Schutz*** in der oberen Navigationszeile des Hauptfensters von **AVG AntiVirus** aufgerufen werden. Das Dialogfenster enthält eine Übersicht über Objekte, die durch den Residenten Schutz erkannt, als gefährlich bewertet und entweder repariert oder in die Virenquarantäne verschoben wurden.

Zu jedem erkannten Objekt werden folgende Informationen angegeben:

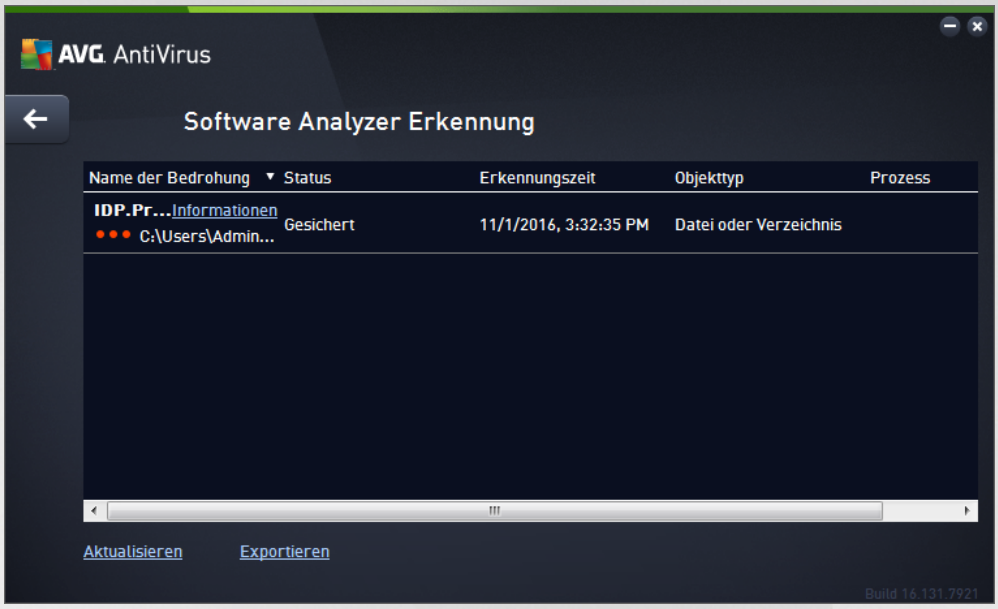
- ***Bedrohungsname*** – Beschreibung (*nach Möglichkeit auch Name*) des erkannten Objekts und seines Speicherorts. Über den Link *Weitere Informationen* gelangen Sie zu einer Seite mit detaillierten Informationen zu der erkannten Bedrohung aus der Online-Virenenzyklopädie.
- ***Status*** – Aktion, die mit dem erkannten Objekt ausgeführt wurde.
- ***Erkennungszeit*** – Zeitpunkt (Datum und Uhrzeit), zu dem die Bedrohung entdeckt und blockiert wurde.
- ***Objekttyp*** – Typ des erkannten Objekts.
- ***Vorgang*** – Ausgeführte Aktion, mit der das potenziell gefährliche Objekt aufgerufen wurde, sodass es erkannt werden konnte.

Schaltflächen

- ***Aktualisieren*** – Aktualisiert die Liste der von ***Online Shield erkannten Funde.***
- ***Exportieren*** – Exportiert die gesamte Liste erkannter Objekte in eine Datei.
- ***Auswahl entfernen*** – Sie können in der Liste bestimmte Berichte markieren und anschließend mit dieser Schaltfläche entfernen.
- ***Alle Bedrohungen entfernen*** – Mit dieser Schaltfläche können Sie alle in diesem Dialogfeld aufgelisteten Berichte entfernen.
- ← – Über den grünen Pfeil links oben im Dialogfeld können Sie zum standardmäßigen AVG-Hauptfenster *(Komponentenübersicht) zurückkehren.*

11.3. Identitätsschutz – Ergebnisse

Das Dialogfeld ***Software Analyzer – Ergebnisse*** kann über die ***Optionen > Historie > Software Analyzer – Ergebnisse*** in der oberen Navigationszeile des **AVG AntiVirus** -Hauptfensters aufgerufen werden.



Im Dialogfeld werden alle von der Komponente E-Mail-Scanner erkannten Funde angezeigt. Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Bedrohungsname*** – Beschreibung *(nach Möglichkeit auch Name)* des erkannten Objekts und seines Standorts. Über den Link *Weitere Informationen* gelangen Sie zu einer Seite mit detaillierten Informationen zu der erkannten Bedrohung aus der Online-Virenenzyklopädie.
- ***Status*** – Aktion, die mit dem erkannten Objekt ausgeführt wurde.
- ***Erkennungszeit*** – Zeitpunkt (Datum und Uhrzeit), zu dem die Bedrohung entdeckt und blockiert wurde.
- ***Objekttyp*** – Typ des erkannten Objekts.
- ***Vorgang*** – Ausgeführte Aktion, mit der das potenziell gefährliche Objekt aufgerufen wurde, sodass es erkannt werden konnte.

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

Schaltflächen

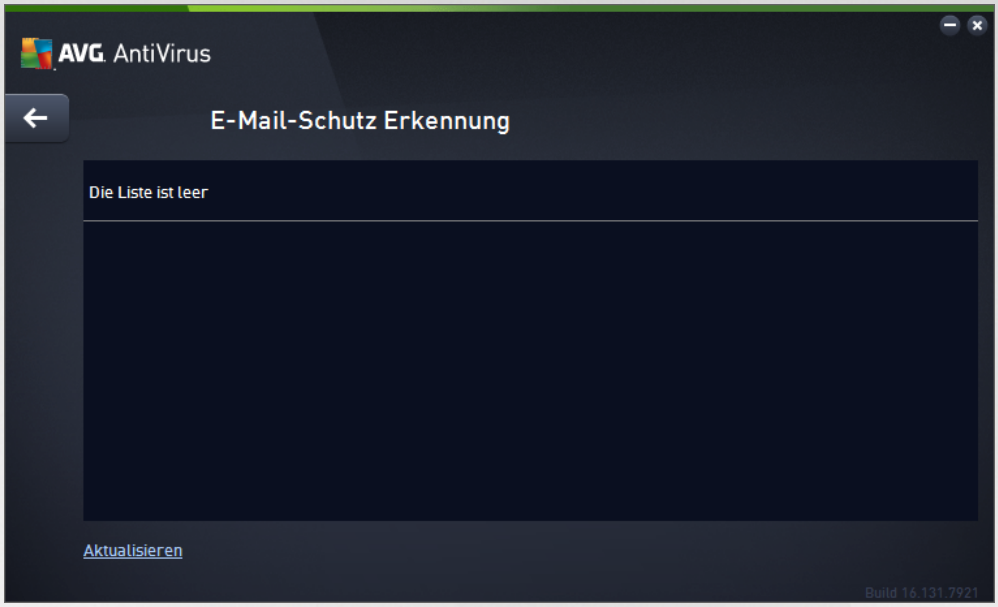
Auf der Oberfläche von ***Software Analyzer – Ergebnisse*** stehen folgende Schaltflächen zur Verfügung:

- ***Liste aktualisieren*** – Aktualisiert die Liste der erkannten Bedrohungen.

- ← – Über den grünen Pfeil links oben im Dialogfeld können Sie zum standardmäßigen AVG-Hauptfenster *(Komponentenübersicht)* zurückkehren.

11.4. E-Mail-Schutz – Ergebnisse

Das Dialogfeld ***E-Mail-Schutz – Ergebnisse*** kann über ***Optionen > Historie > E-Mail-Schutz – Ergebnisse*** in der oberen Navigationszeile des **AVG AntiVirus**-Hauptfensters aufgerufen werden.



Im Dialogfeld werden alle von der Komponente E-Mail-Scanner erkannten Funde angezeigt. Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Erkennungsname*** – Beschreibung *(nach Möglichkeit auch Name)* des erkannten Objekts und seiner Quelle.
- ***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 potenziell gefährliche Objekt aufgerufen wurde, sodass es erkannt werden konnte.

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

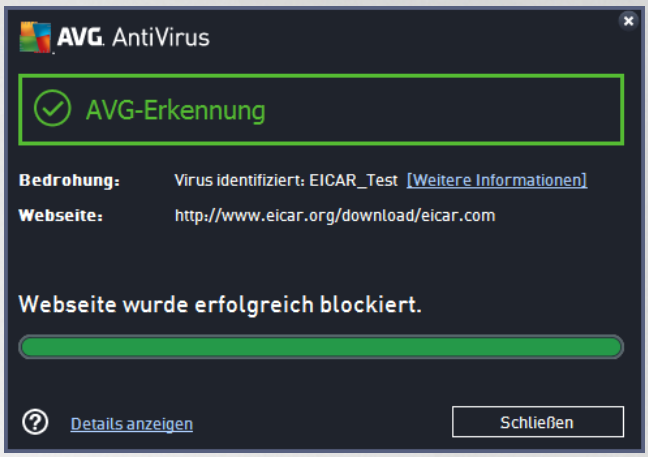
Schaltflächen

Auf der Oberfläche von ***E-Mail-Scanner*** stehen folgende Schaltflächen zur Verfügung:

- ***Liste aktualisieren*** – Aktualisiert die Liste der erkannten Bedrohungen.
- ← – Über den grünen Pfeil links oben im Dialogfeld können Sie zum standardmäßigen AVG-Hauptfenster *(Komponentenübersicht) zurückkehren.*

11.5. Online Shield – Ergebnisse

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



In dieser Warnmeldung werden Informationen zu dem erkannten und als infiziert eingestuften Objekt (*Bedrohung*) und eine Beschreibung der erkannten Infektion (*Objektname*) angezeigt. Über den Link *Weitere Informationen* gelangen Sie zur Online-Virenenzyklopädie, wo Sie genauere Informationen über die erkannte Infektion erhalten können, wenn diese bekannt sind. Der Dialog enthält folgende Schaltflächen:

- ***Details anzeigen*** – Klicken Sie auf diesen Link, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess anzuzeigen, der beim Erkennen der Infektion ausgeführt wurde.
- ***Schließen*** – Klicken Sie auf diese Schaltfläche, um die Warnmeldung zu schließen.

Die verdächtige Website wird nicht geöffnet, und die Bedrohungserkennung wird in der Liste der ***Ergebnisse des Online-Shield*** protokolliert. Die Übersicht der erkannten Bedrohungen kann über ***Optionen > Historie > Ergebnisse des Online Shield*** in der oberen Navigationszeile des Hauptfensters von **AVG AntiVirus** aufgerufen werden.

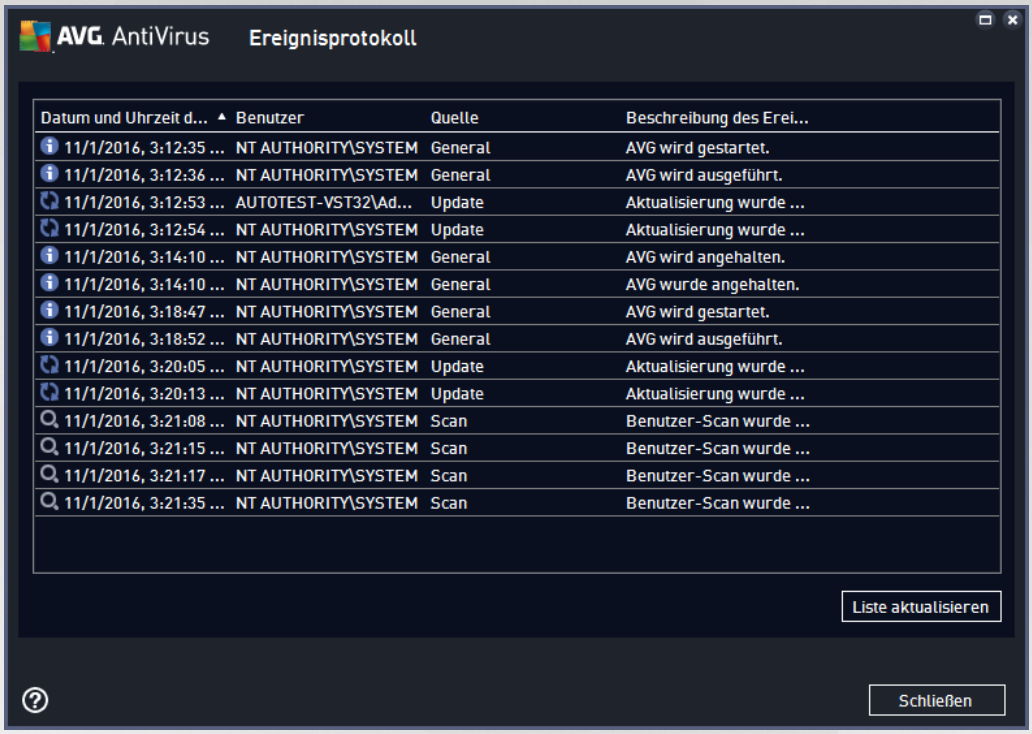
Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Name der Bedrohung*** – Beschreibung (*nach Möglichkeit auch Name*) des erkannten Objekts, sowie seine Quelle (*Webseite*); über den Link *Weitere Informationen* gelangen Sie zu einer Seite mit detaillierten Informationen zu der erkannten Bedrohung aus der Online-Virenenzyklopädie.
- ***Status*** – Aktion, die mit dem erkannten Objekt ausgeführt wurde.
- ***Erkennungszeit*** – Zeitpunkt (Datum und Uhrzeit), zu dem die Bedrohung entdeckt und blockiert wurde.
- ***Objekttyp*** – Typ des erkannten Objekts.

Schaltflächen

- ***Aktualisieren*** – Aktualisiert die Liste der von ***Online Shield erkannten Funde.***
- ***Exportieren*** – Exportiert die gesamte Liste erkannter Objekte in eine Datei.
- ← – Über den grünen Pfeil links oben im Dialogfeld können Sie zum standardmäßigen AVG-Hauptfenster *(Komponentenübersicht) zurückkehren.*

11.6. Ereignisprotokoll



Das Dialogfeld ***Ereignisprotokoll*** kann über das Menüelement ***Optionen / Historie > Ereignisprotokoll*** in der oberen Navigationszeile des Hauptfensters von **AVG AntiVirus** aufgerufen werden. In diesem Dialog finden Sie eine Zusammenfassung aller wichtigen Ereignisse, die während der Ausführung von **AVG AntiVirus** aufgetreten sind. In dem Dialogfenster werden Berichte über die folgenden Ereignistypen angezeigt: Informationen zu Updates der AVG-Anwendungen, Informationen zum Starten, Beenden oder Anhalten des Scanvorgangs (*einschließlich automatisch ausgeführter Tests*), Informationen zu Ereignissen, die mit der Virenerkennung (*entweder durch Residenten Schutz oder Scannen*) zusammenhängen, einschließlich dem Ort des Auftretens, und andere wichtige Ereignisse.

Für jedes Ereignis werden die folgenden Informationen aufgelistet:

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

Schaltflächen

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

- ***Schließen*** – Klicken Sie auf diese Schaltfläche, um zum Hauptfenster von **AVG AntiVirus** zurückzukehren.

12. AVG Updates

Keine Sicherheitssoftware kann einen wirksamen Schutz gegen verschiedene Bedrohungen bieten, wenn sie nicht regelmäßig aktualisiert wird! Verfasser von Viren suchen stets nach neuen Lücken in Software und Betriebssystemen, die sie ausnutzen können. Jeden Tage gibt es neue Viren, neue Malware und neue Hacker-Angriffe. Software-Hersteller geben daher ständig neue Updates und Sicherheits-Patches heraus, mit denen entdeckte Sicherheitslücken geschlossen werden sollen. Angesichts der vielen neuen Computerbedrohungen und der Geschwindigkeit, mit der sie sich verbreiten, ist es besonders wichtig, dass Sie **AVG AntiVirus** regelmäßig aktualisieren. Am besten ist es, die Standardeinstellungen des Programms beizubehalten, in denen das automatische Update konfiguriert ist. Bitte beachten Sie, dass das Programm die neuesten Bedrohungen nicht erkennen kann, wenn die Virendatenbank von **AVG AntiVirus** nicht auf dem neuesten Stand ist!

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

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

Wenn Sie die neuen Update-Dateien sofort überprüfen möchten, verwenden Sie den Quick Link Jetzt aktualisieren auf der Hauptbenutzeroberfläche. Dieser Link steht Ihnen jederzeit in allen Dialogfeldern der Benutzeroberfläche zur Verfügung. Wenn Sie das Update starten, überprüft AVG zunächst, ob neue Update-Dateien zur Verfügung stehen. Ist dies der Fall, startet **AVG AntiVirus** den Download dieser Dateien und ruft auch selbst den Update-Vorgang auf. Über das Popup-Fenster oberhalb des AVG-Symbols im Infobereich werden Sie über die Ergebnisse der Updates informiert.

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

- Zeitplan für Update der Definitionen

13. FAQ und technischer Support

Wenn Probleme mit dem Vertrieb oder technische Probleme mit Ihrer Anwendung **AVG AntiVirus** auftreten, haben Sie verschiedene Möglichkeiten, Hilfe in Anspruch zu nehmen. Bitte wählen Sie eine der folgenden Optionen:

- ***Support nutzen***: In der AVG-Anwendung selbst können Sie eine dedizierte Kundendienstseite der AVG-Website (*http://www.avg.com*) aufrufen. Wählen Sie aus dem Hauptmenü die Option ***Hilfe/Support nutzen***, um auf die Website von AVG mit weiteren Support-Hinweisen zu gelangen. Folgen Sie zum Fortfahren den Anweisungen auf der Webseite.

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

- ***Problembehandlung in der Hilfedatei***: Ein neuer Abschnitt ***Problembehandlung*** steht direkt in der Hilfedatei von **AVG AntiVirus** *zur Verfügung (die Hilfedatei kann von allen Dialogen aus mit der F1-Taste geöffnet werden)*. Dieser Abschnitt enthält eine Liste der häufigsten Situationen, in denen ein Benutzer professionelle Hilfe zu einem technischen Problem sucht. Bitte wählen Sie die Situation aus, die Ihr Problem am besten beschreibt, und klicken Sie darauf, um detaillierte Anweisungen zur Lösung des Problems zu anzuzeigen.

- ***Support Center auf der Website von AVG***: Alternativ können Sie die Lösung zu Ihrem Problem auch auf der Website von AVG suchen (*http://www.avg.com*). Im Bereich ***Support*** finden Sie eine Übersicht über Themenbereiche sowie zu Vertriebs- als auch zu technischen Problemen, einen gegliederten Bereich mit häufig gestellten Fragen sowie alle verfügbaren Kontakte.

- ***AVG ThreatLabs***: eine spezielle AVG-Website (*http://www.avg.com/about-viruses*), die Fragen zu Viren gewidmet ist und übersichtliche Informationen zu Online-Bedrohungen bietet. Dort finden Sie außerdem Anweisungen zum Entfernen von Viren und Spyware sowie Ratschläge zur Aufrechterhaltung Ihres Schutzes.

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