AVG eMail Server Edition 2012

Benutzerhandbuch

Dokumentversion 2012.06 (2/28/2012)

Inhalt

1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG eMail Server Edition 2012**.

Herzlichen Glückwunsch zum Kauf von AVG eMail Server Edition 2012!

AVG eMail Server Edition 2012 zählt zu einer Reihe von preisgekrönten AVG-Produkten, die vollständige Sicherheit für Ihren Server bieten, damit Sie in Ruhe arbeiten können. Wie alle Produkte von AVG wurde **AVG eMail Server Edition 2012** von Grund auf vollkommen neu gestaltet, um den anerkannten Schutz von AVG noch benutzerfreundlicher und effizienter bereitzustellen.

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

Hinweis: *Diese Dokumentation die Beschreibung verschiedener Funktionen der eMail Server Edition. Wenn Sie Informationen zu anderen Funktionen von AVG benötigen, finden Sie diese im Benutzerhandbuch der Internet Security Edition. Sie können das Handbuch von der http://www.avg.com/de herunterladen.*

2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG eMail Server Edition 2012 wurde für den Schutz von eMail-Servern entwickelt, auf denen die folgenden Betriebssysteme ausgeführt werden:

- Windows 2008 Server Edition (x86 und x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Unterstützte eMail-Server

Folgende eMail-Server werden unterstützt:

- MS Exchange 2003 Server-Version
- MS Exchange 2007 Server-Version
- MS Exchange 2010 Server-Version
- Kerio MailServer – Version 6.7.2 und höher

2.3. Hardware-Anforderungen

Minimale Hardware-Anforderungen für **AVG eMail Server Edition 2012**:

- Intel Pentium CPU 1.5 GHz
- 500 MB an freiem Festplattenplatz (für die Installation)
- 512 MB RAM-Speicher

Empfohlene Hardware-Anforderungen für **AVG eMail Server Edition 2012**:

- Intel Pentium CPU 1.8 GHz
- 600 MB an freiem Festplattenplatz (für die Installation)
- 512 MB RAM-Speicher

2.4. Deinstallieren vorheriger Versionen

Wenn Sie eine ältere Version von AVG eMail Server installiert haben, müssen Sie diese vor der Installation von **AVG eMail Server Edition 2012** zunächst manuell deinstallieren. Sie müssen die frühere Version mit Hilfe der Windows-Standardfunktion manuell deinstallieren.

- Wählen Sie über ***Start/Einstellungen/Systemsteuerung/Software*** das richtige Programm

aus der Liste installierter Software. (Alternativ können Sie auch über ***Start/Programme/AVG/AVG deinstallieren*** die ältere Version deinstallieren.)

- Wenn Sie bereits AVG 8.x oder eine ältere Version verwendet haben, müssen Sie auch die individuellen Server-Plugins deinstallieren.

  Hinweis: *Der Speicherdienst muss während der Deinstallation neu gestartet werden.*

  Exchange-Plugin – Die Datei „setupes.exe“ wird mit dem Parameter „/uninstall“ aus dem Ordner ausgeführt, in dem das Plugin installiert war.

  z. B. C:\AVG4ES2K\setupes.exe /uninstall

  Lotus Domino/Notes-Plugin – Die Datei „setupln.exe“ wird mit dem Parameter „/uninstall“ aus dem Ordner ausgeführt, in dem das Plugin installiert war:

  z. B. C:\AVG4LN\setupln.exe /uninstall

2.5. Service Packs für MS Exchange

Für MS Exchange Server 2003 ist kein zusätzliches Service Pack erforderlich. Es wird dennoch empfohlen, das System über die neuesten Service Packs und Hotfixes auf dem aktuellen Stand zu halten, damit eine maximale Sicherheit gewährleistet ist.

Service Pack für MS Exchange 2003 Server (optional):

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

Zu Beginn des Setups werden alle Versionen der Systembibliotheken geprüft. Wenn die Installation neuer Bibliotheken erforderlich ist, fügt das Installationsprogramm den alten Bibliotheken die Erweiterung .delete hinzu. Diese werden bei einem Neustart des Systems gelöscht.

Service Pack für MS Exchange 2007 Server (optional):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=de

3. Installationsvorgang bei AVG

Für die Installation von AVG auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei online herunterzuladen. Sie können die Datei von der AVG-Website (unter http://www.avg.com/de/download?prd=msw) herunterladen.

Hinweis: *Für Ihr Produkt sind zwei Installationspakete verfügbar: für 32-Bit-Betriebssysteme (gekennzeichnet mit x86) und für 64-Bit-Betriebssystem (gekennzeichnet mit x64). Stellen Sie sicher, dass Sie das korrekte Installationspaket für Ihr Betriebssystem verwenden.*

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

Nachdem Sie die Installationsdatei heruntergeladen und auf Ihrer Festplatte gespeichert haben, können Sie den Installationsvorgang starten. Der Installationsvorgang besteht aus einer Abfolge von Dialogen, die jeweils eine kurze Beschreibung der erforderlichen Schritte enthalten. Im Folgenden werden die einzelnen Dialoge erläutert:

3.1. Beginn der Installation

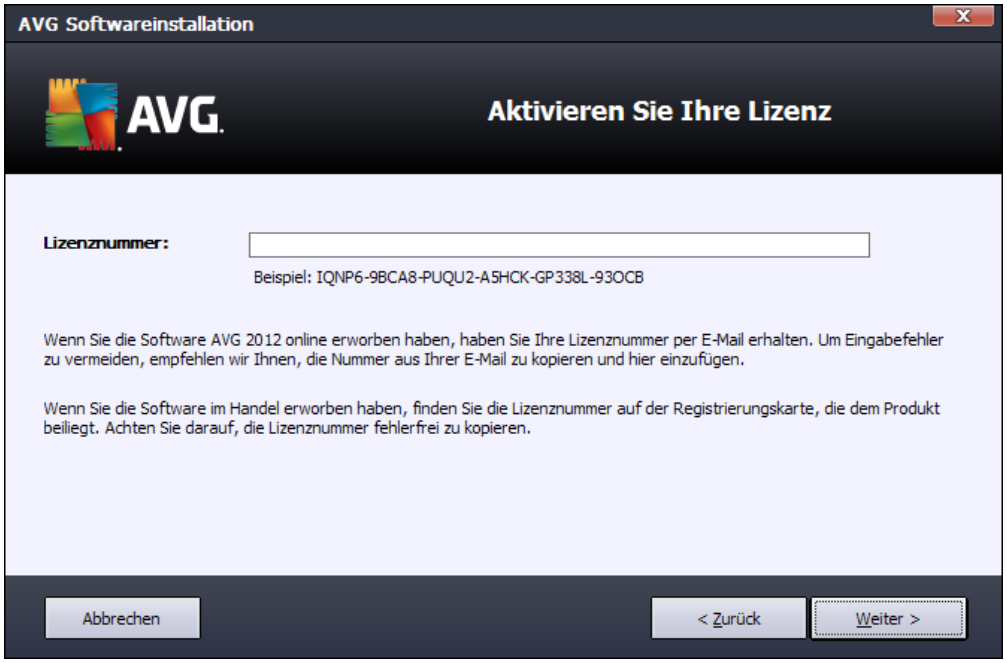
Der Installationsvorgang beginnt mit dem Fenster ***Willkommen***. Hier können Sie die Sprache für den Installationsvorgang auswählen und die Lizenzbedingungen lesen. Klicken Sie auf die Schaltfläche ***Druckversion***, um den Text der Lizenzvereinbarung in einem neuen Fenster zu öffnen. Klicken Sie anschließend auf die Schaltfläche ***Akzeptieren***, um mit dem nächsten Dialog fortzufahren.

Achtung: *Sie können zu einem späteren Zeitpunkt während des Installationsvorgangs zusätzliche Sprachen für die Benutzeroberfläche auswählen.*

3.2. Aktivieren Sie Ihre Lizenz

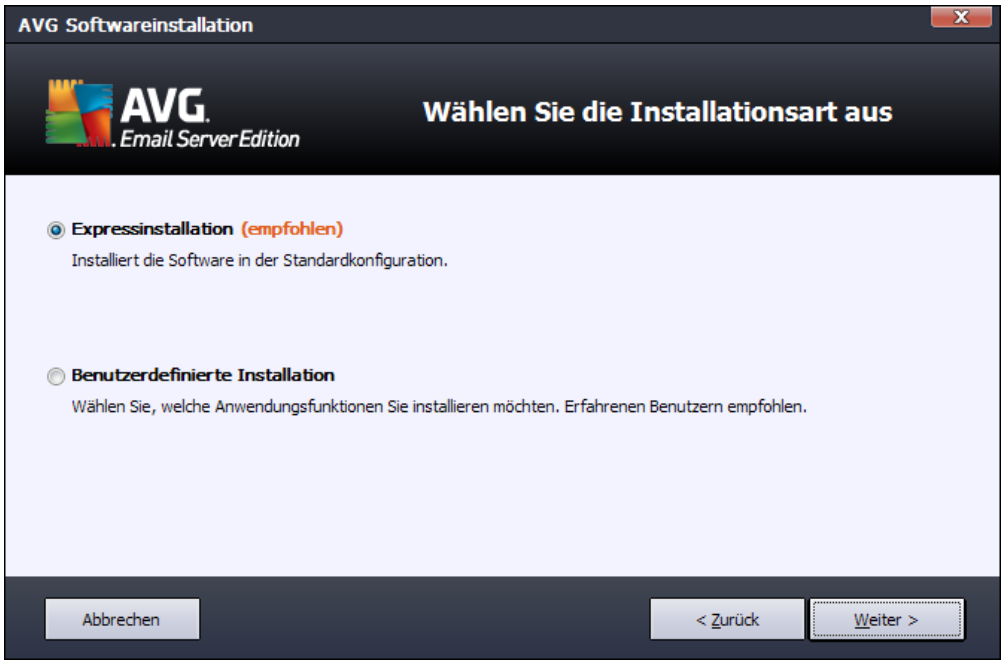
Im Dialog ***AVG-Lizenz aktivieren*** müssen Sie Ihre Lizenznummer eingeben.

Geben Sie Ihre Lizenznummer in das Textfeld ***Lizenznummer*** ein. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von AVG erhalten haben. Sie müssen die Nummer exakt wie dargestellt eingeben. Wenn die Lizenznummer in digitaler Form verfügbar ist (in der eMail), wird empfohlen, sie zu kopieren und einzufügen.



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

3.3. Bitte wählen Sie den Installationstyp



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

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

Die ***Benutzerdefinierte Installation*** sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, AVG nicht mit den Standardeinstellungen zu installieren, beispielsweise um bestimmte Systemanforderungen zu erfüllen.

3.4. Benutzerdefinierte Installation – Benutzerdefinierte Optionen

Im Dialog ***Zielverzeichnis*** können Sie den Speicherort für die Installation von AVG angeben. Standardmäßig wird AVG im Ordner C:/Programme installiert. Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf ***Durchsuchen***, um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus.

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

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

- ***AVG Remote-Verwaltungsclient*** – Wählen Sie diese Option aus, wenn Sie AVG mit einem AVG DataCenter (AVG Netzwerk Editionen) verbinden möchten.

- ***Einstellungsmanager*** – Ein besonders für Netzwerkadministratoren geeignetes Tool, mit dem Sie die Konfiguration von AVG kopieren, bearbeiten und bereitstellen können. Die Konfiguration kann auf einem Wechseldatenträger (USB-Flash-Laufwerk usw.) gespeichert und dann manuell oder auf einem anderen Weg auf die gewählten Stationen angewendet werden.

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

Grundlegende Übersicht über die einzelnen Serverkomponenten (***Server-Add-Ins***):

- ***Anti-Spam-Server für MS Exchange***

  Überprüft alle eingehenden eMail-Nachrichten und markiert unerwünschte eMails als SPAM. Die Komponente verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit den größtmöglichen Schutz gegen unerwünschte eMail-Nachrichten.

- ***eMail-Scanner für MS Exchange (Routing-Transport-Agent)***

  Prüft alle eingehenden, ausgehenden und internen eMail-Nachrichten, die über die HUB-Rolle von MS Exchange laufen.

  Für MS Exchange 2007/2010 verfügbar und kann nur für die HUB-Rolle installiert werden.

- ***eMail-Scanner für MS Exchange (SMTP-Transport-Agent)***

  Prüft alle eMail-Nachrichten, die über die SMTP-Schnittstelle von MS Exchange eingehen.

  Nur für MS Exchange 2007/2010 verfügbar und kann sowohl für EDGE- als auch HUB-Rollen installiert werden.

- ***eMail-Scanner für MS Exchange (VSAPI)***

  Überprüft alle eMail-Nachrichten, die in den Postfächern der Benutzer gespeichert sind. Erkannte Viren werden in die Virenquarantäne verschoben oder vollständig entfernt.

Hinweis: *Für die verschiedenen Versionen von MS Exchange sind verschiedene Optionen verfügbar.*

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

3.5. Abschluss der Installation

Wenn Sie bei der Modulauswahl das Modul ***Komponente „Remote-Verwaltung“*** ausgewählt haben, können Sie in der letzten Ansicht die Verbindungszeichenkette für die Verbindung zum AVG DataCenter festlegen.

AVG ist nun auf Ihrem Computer installiert und voll funktionsfähig. Das Programm wird im Hintergrund vollständig automatisch ausgeführt.

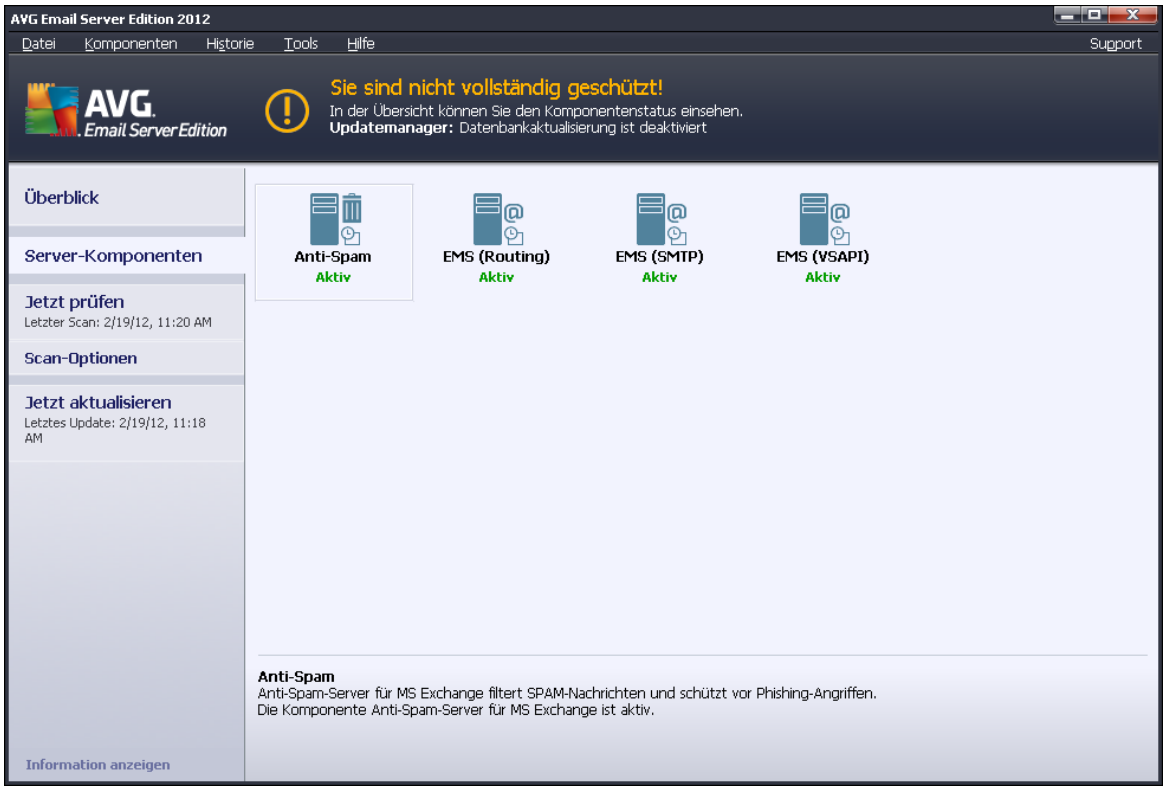
Um individuellen Schutz für Ihren eMail-Server einzurichten, folgen Sie den Anweisungen im entsprechenden Kapitel:

- ***eMail-Scanner für MS Exchange Server 2007/2010***
- ***eMail-Scanner für MS Exchange Server 2003***
- ***AVG für Kerio MailServer***

4. eMail-Scanner für MS Exchange Server 2007/2010

4.1. Übersicht

Die Konfigurationsoptionen von AVG für MS Exchange Server 2007/2010 sind vollständig in AVG eMail Server Edition 2012 als Server-Komponenten integriert.



Grundlegende Übersicht über die einzelnen Serverkomponenten:

- ***Anti-Spam – Anti-Spam-Server für MS Exchange***

  Überprüft alle eingehenden eMail-Nachrichten und markiert unerwünschte eMails als SPAM. Die Komponente verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit den größtmöglichen Schutz gegen unerwünschte eMail-Nachrichten.

- ***EMS (Routing) – eMail-Scanner für MS Exchange (Routing-Transport-Agent)***

  Prüft alle eingehenden, ausgehenden und internen eMail-Nachrichten, die über die HUB-Rolle von MS Exchange laufen.

  Für MS Exchange 2007/2010 verfügbar und kann nur für die HUB-Rolle installiert werden.

- ***EMS (SMTP) – eMail-Scanner für MS Exchange (SMTP-Transport-Agent)***

Prüft alle eMail-Nachrichten, die über die SMTP-Schnittstelle von MS Exchange eingehen.

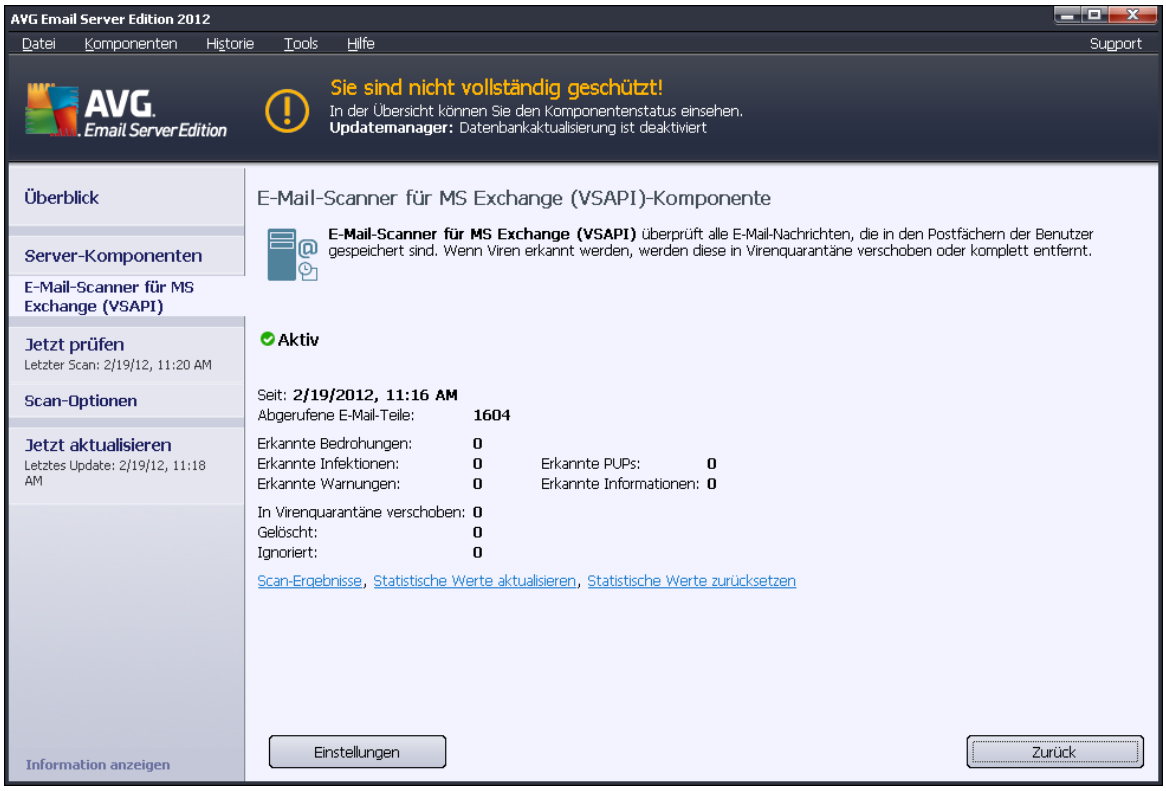
Nur für MS Exchange 2007/2010 verfügbar und kann sowohl für EDGE- als auch HUB-Rollen installiert werden.

- ***EMS (VSAPI) – eMail-Scanner für MS Exchange (VSAPI)***

  Überprüft alle eMail-Nachrichten, die in den Postfächern der Benutzer gespeichert sind. Erkannte Viren werden in die Virenquarantäne verschoben oder vollständig entfernt.

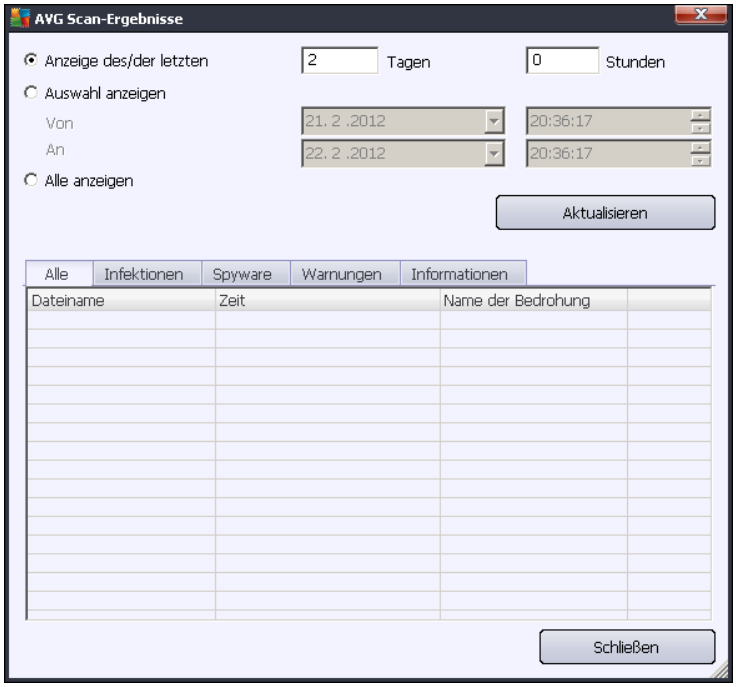
Wichtiger Hinweis: *Wenn Sie VSAPI installiert haben und es in Kombination mit einem Routing-Transport-Agenten auf einer Hub Exchange-Rolle verwenden, werden Ihre eMails zweimal gescannt. Um dies zu verhindern, aktivieren Sie in den VSAPI-Einstellungen das Kontrollkästchen* ***Ausgehende Nachrichten nicht scannen (MS Exchange 2007/2010)****. (Weitere Informationen finden Sie hier.)*

Klicken Sie auf das Symbol der gewünschten Komponente, um die Benutzeroberfläche zu öffnen. Mit Ausnahme von Anti-Spam verfügen alle Komponenten über folgende Schaltflächen und Links:



- ***Scan-Ergebnisse***

  Öffnet einen neuen Dialog, in dem Sie die Scan-Ergebnisse überprüfen können:



Hier können Sie Nachrichten prüfen, die je nach Schweregrad in verschiedene Reiter unterteilt wurden. Einstellungen für Schweregrad und Berichte können Sie in der Konfiguration der einzelnen Komponenten vornehmen.

Standardmäßig werden nur die Ergebnisse der letzten zwei Tage angezeigt. Sie können den Anzeigezeitraum ändern, indem Sie die folgenden Optionen anpassen:

- ***Letzte anzeigen*** – Geben Sie die gewünschten Tage und Stunden ein.
- ***Auswahl anzeigen*** – Geben Sie ein benutzerdefiniertes Zeitintervall an.
- ***Alle anzeigen*** – Zeigt die Ergebnisse für den gesamten Zeitraum an.

Verwenden Sie die Schaltfläche ***Aktualisieren***, um die Ergebnisse neu zu laden.

- ***Statistikwerte aktualisieren*** – Aktualisiert die oben angezeigten Statistiken.
- ***Statistikwerte zurücksetzen*** – Setzt die gesamte Statistik auf null zurück.

Folgende Schaltflächen stehen zur Verfügung:

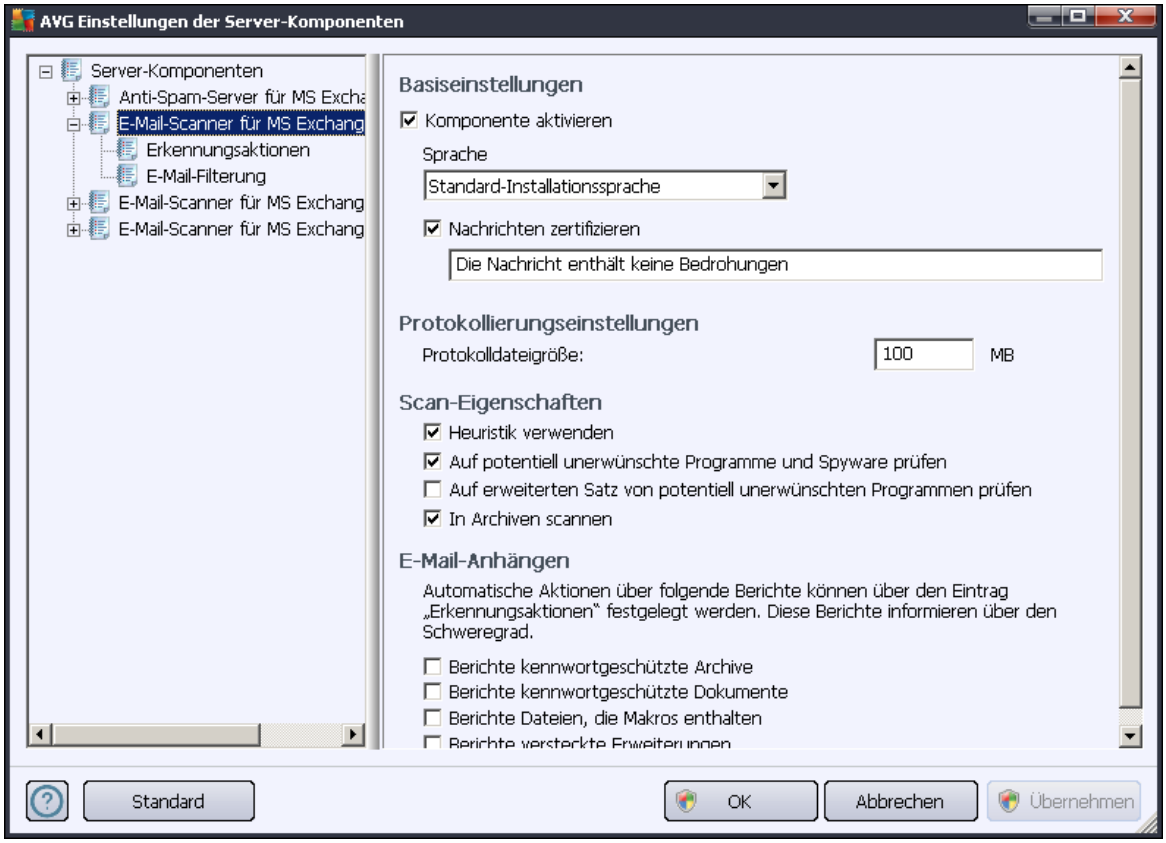
- ***Einstellungen*** – Verwenden Sie diese Schaltfläche, um die Einstellungen der Komponente zu öffnen.
- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um zur Übersicht über die Server-Komponenten zurückzukehren.

Mehr Informationen zu den individuellen Einstellungen der Komponenten finden Sie in den folgenden Kapiteln.

4.2. eMail-Scanner für MS Exchange (Routing-TA)

Um die Einstellungen von ***eMail-Scanner für MS Exchange (Routing-Transport-Agent)*** zu öffnen, wählen Sie auf der Oberfläche der Komponente die Schaltfläche ***Einstellungen*** aus.

Wählen Sie in der Liste ***Server-Komponenten*** das Element ***eMail-Scanner für MS Exchange (Routing-TA)*** aus:



Der Abschnitt ***Grundeinstellungen*** enthält die folgenden Optionen:

- ***Komponente aktivieren*** – Deaktivieren Sie diese Option, um die gesamte Komponente zu deaktivieren.
- ***Sprache*** – Wählen Sie die bevorzugte Komponentensprache aus.
- ***Nachrichten zertifizieren*** – Aktivieren Sie diese Option, wenn Sie allen überprüften Nachrichten einen Zertifizierungshinweis hinzufügen möchten. Die Nachricht kann im nächsten Feld angepasst werden.

Der Abschnitt ***Protokollierungseinstellungen***:

- ***Protokolldateigröße*** – Legen Sie die gewünschte Größe für die Protokolldatei fest. Standardwert: 100 MB.

Der Abschnitt ***Scan-Eigenschaften***:

- ***Heuristik verwenden*** – Aktivieren Sie dieses Kontrollkästchen, um die heuristische Analyse bei der Überprüfung zu aktivieren.
- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – Aktivieren Sie diese Option, wenn potentiell unerwünschte Programme und Spyware gemeldet werden sollen.
- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** – Aktivieren Sie dieses Kontrollkästchen, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können, oder Programme, die in jedem Fall harmlos, jedoch nicht erwünscht sind (verschiedene Symbolleisten usw.). Dies stellt eine zusätzliche Maßnahme für mehr Komfort und eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist. Hinweise: Diese Erkennungsfunktion stellt eine Ergänzung der vorangehenden Option dar. Lassen Sie daher die vorangehende Option immer aktiviert, um einen grundlegenden Schutz vor Spyware zu gewährleisten.
- ***In Archiven scannen*** – Aktivieren Sie diese Option, wenn der Scanner auch Archiv-Dateien (ZIP, RAR usw.) durchsuchen soll.

Im Abschnitt ***Berichte über eMail-Anhänge*** können Sie festlegen, welche Einträge bei der Überprüfung gemeldet werden sollen. Ist diese Option aktiviert, erhalten alle eMails mit einem solchen Element das Kennzeichen [INFORMATION] im Betreff der Nachricht. Dies ist die Standardeinstellung, sie kann jedoch leicht im Bereich ***Erkennungsaktionen*** im Teil ***Informationen*** (siehe unten) angepasst werden.

Folgende Optionen sind verfügbar:

- ***Kennwortgeschützte Archive berichten***
- ***Kennwortgeschützte Dokumente berichten***
- ***Dateien berichten, die Makros enthalten***
- ***Versteckte Erweiterungen berichten***

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***eMail-Filterung***

4.3. eMail-Scanner für MS Exchange (SMTP-TA)

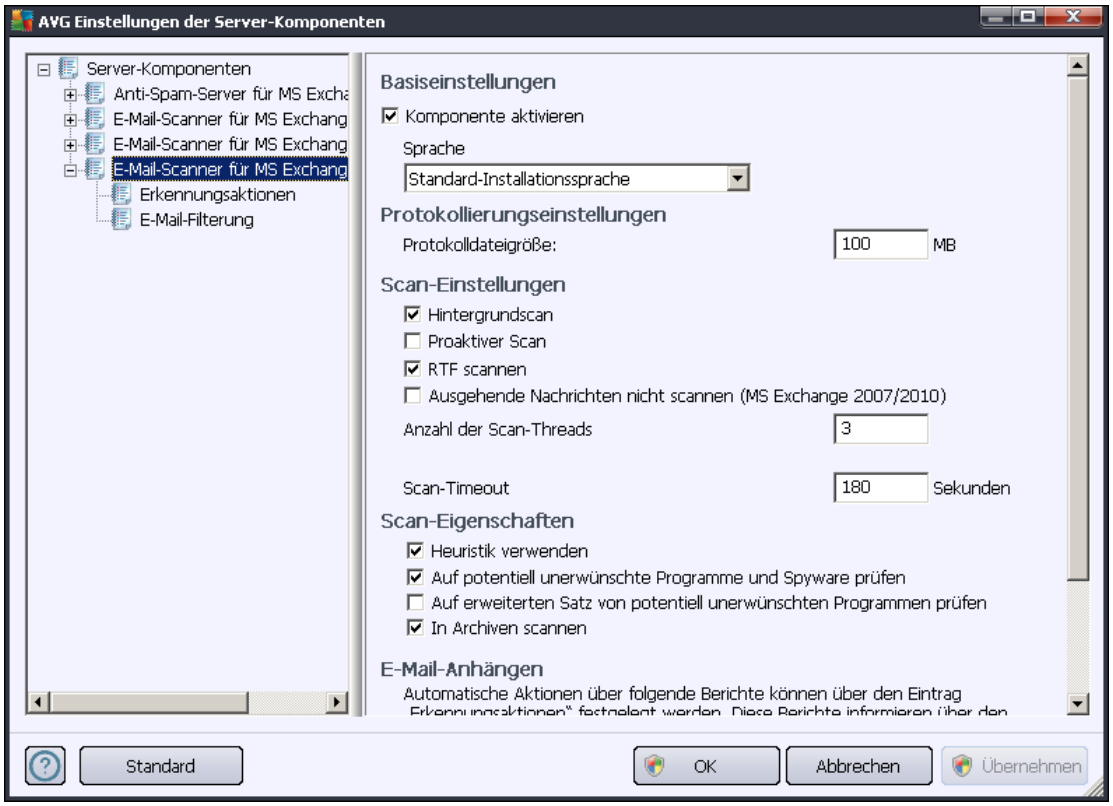
Die Konfiguration für den ***eMail-Scanner für MS Exchange (SMTP-Transport-Agent)*** ist exakt die gleiche wie für den Routing-Transport-Agent. Weitere Informationen finden Sie im Kapitel ***eMail-Scanner für MS Exchange (Routing-TA)*** weiter oben.

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***eMail-Filterung***

4.4. eMail-Scanner für MS Exchange (VSAPI)

Dieses Element enthält Einstellungen für den ***eMail-Scanner für MS Exchange (VSAPI)***.



Der Abschnitt ***Grundeinstellungen*** enthält die folgenden Optionen:

- ***Komponente aktivieren*** – Deaktivieren Sie diese Option, um die gesamte Komponente zu deaktivieren.
- ***Sprache*** – Wählen Sie die bevorzugte Komponentensprache aus.

Der Abschnitt ***Protokollierungseinstellungen***:

- ***Protokolldateigröße*** – Legen Sie die gewünschte Größe für die Protokolldatei fest. Standardwert: 100 MB.

Der Abschnitt ***Scan-Einstellungen***:

- ***Hintergrundscan*** – Hier können Sie den Prozess der Hintergrundprüfung aktivieren und

deaktivieren. Die Hintergrundprüfung ist eine der Eigenschaften der VSAPI 2.0/2.5-Anwendungsschnittstelle. Es handelt sich um das Scannen der Exchange Messaging Datenbanken in eigenen Threads. Wird ein Objekt in den Ordnern der Benutzerpostfächer gefunden, das noch nicht mit dem neuesten Update der Virendatenbank von AVG gescannt wurde, wird es zum Scannen an AVG für Exchange Server weitergeleitet. Die Suche nach nicht geprüften Objekten und der Virentest werden parallel ausgeführt.

Für jede Datenbank wird ein bestimmter Thread niedriger Priorität verwendet, um sicherzustellen, dass andere Aufgaben (z. B. das Speichern von eMail-Nachrichten in der Microsoft Exchange-Datenbank) vorrangig ausgeführt werden.

- ***Proaktiver Scan (eingehende Nachrichten)***

  Hier können Sie die Funktion zum proaktiven Scannen von VSAPI 2.0/2.5 aktivieren und deaktivieren. Diese Scans werden ausgeführt, wenn ein Element an einen Ordner geliefert wird, aber keine Anforderung vom Client vorliegt.

  Sobald die Nachrichten an den Exchange-Speicher übermittelt wurden, werden sie mit niedriger Priorität in die globale Scan-Warteschlange eingereiht (maximal 30 Elemente). Sie werden in der Reihenfolge ihres Eintreffens gescannt. Sollte ein Zugriff auf ein Element in der Warteschlange registriert werden, wird dieses auf hohe Priorität gesetzt.

  Hinweis: *Sollten zu viele Nachrichten vorliegen, werden diese ohne Scan in den Speicher verschoben.*

Hinweis: *Auch wenn Sie die beiden Optionen* ***Hintergrundscan*** *und* ***Proaktiver Scan*** *deaktivieren, bleibt der On-Access-Scanner weiterhin aktiv, wenn ein Benutzer versucht, eine Nachricht mit MS Outlook herunterzuladen.*

- ***Scan RTF*** – Sie können hier festlegen, ob RTF-Dateien geprüft werden sollen.
- ***Ausgehende Nachrichten nicht scannen (MS Exchange 2007/2010)*** – Wenn sowohl VSAPI als auch der Routing-Transport-Agent (Routing-TA) installiert sind (unabhängig davon, ob auf demselben oder zwei verschiedenen Servern), werden ausgehende eMails möglicherweise zweimal gescannt. Der erste Scan wird vom Bei-Zugriff-Scanner von VSAPI ausgeführt und der zweite vom Routing-Transport-Agent. Dies kann zu Leistungsbeeinträchtigungen der Server und Verzögerungen beim Senden von eMails führen. Wenn Sie sicher sind, dass beide Server-Komponenten installiert und aktiviert sind, können Sie den doppelten Scan ausgehender eMails verhindern, indem Sie dieses Kontrollkästchen aktivieren und den Bei-Zugriff-Scanner von VSAPI deaktivieren.
- ***Anzahl der Scan-Threads*** – Der Prozess der Virenprüfung ist in der Standardeinstellung in verschiedene Threads aufgeteilt, um die Scanleistung auf einem hohen Niveau zu halten. Sie können hier die Anzahl der Threads ändern.

  Die Standardanzahl wird nach der Formel „2 × 'Anzahl der Prozessoren' + 1“ berechnet.

  Die minimale Anzahl der Threads wird nach der Formel (Anzahl der Prozessoren + 1) / 2 berechnet.

  Die maximale Anzahl der Threads wird nach der Formel Anzahl der Prozessoren × 5 + 1 berechnet.

Wenn der Wert der minimale (oder kleiner) oder maximale (oder größer) Wert ist, wird der Standardwert verwendet.

- ***Scan-Timeout*** – Die maximale Wartezeit (in Sekunden) eines Threads für den Zugriff auf eine zu scannende Nachricht (Standardwert: 180 Sekunden).

Der Abschnitt ***Scan-Eigenschaften***:

- ***Heuristik verwenden*** – Aktivieren Sie dieses Kontrollkästchen, um die heuristische Analyse bei der Überprüfung zu aktivieren.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – Aktivieren Sie diese Option, wenn potentiell unerwünschte Programme und Spyware gemeldet werden sollen.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** – Aktivieren Sie dieses Kontrollkästchen, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können, oder Programme, die in jedem Fall harmlos, jedoch nicht erwünscht sind (verschiedene Symbolleisten usw.). Dies stellt eine zusätzliche Maßnahme für mehr Komfort und eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist. Hinweise: Diese Erkennungsfunktion stellt eine Ergänzung der vorangehenden Option dar. Lassen Sie daher die vorangehende Option immer aktiviert, um einen grundlegenden Schutz vor Spyware zu gewährleisten.

- ***In Archiven scannen*** – Aktivieren Sie diese Option, wenn der Scanner auch Archiv-Dateien (ZIP, RAR usw.) durchsuchen soll.

Im Abschnitt ***Berichte über eMail-Anhänge*** können Sie festlegen, welche Einträge bei der Überprüfung gemeldet werden sollen. Die Standardeinstellungen können einfach im ***Abschnitt Erkennungsaktionen***, Unterabschnitt ***Informationen*** angepasst werden (siehe unten).

Folgende Optionen sind verfügbar:

- ***Kennwortgeschützte Archive berichten***

- ***Kennwortgeschützte Dokumente berichten***

- ***Dateien berichten, die Makros enthalten***

- ***Versteckte Erweiterungen berichten***

Einige dieser Funktionen sind benutzerspezifische Erweiterungen der Dienste der Microsoft VSAPI 2.0/2.5-Benutzerschnittstelle. Ausführliche Informationen über die VSAPI 2.0/2.5 finden Sie unter folgenden Adressen und über die dortigen Links:

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – Für Informationen über die Interaktion zwischen Exchange- und Antiviren-Software

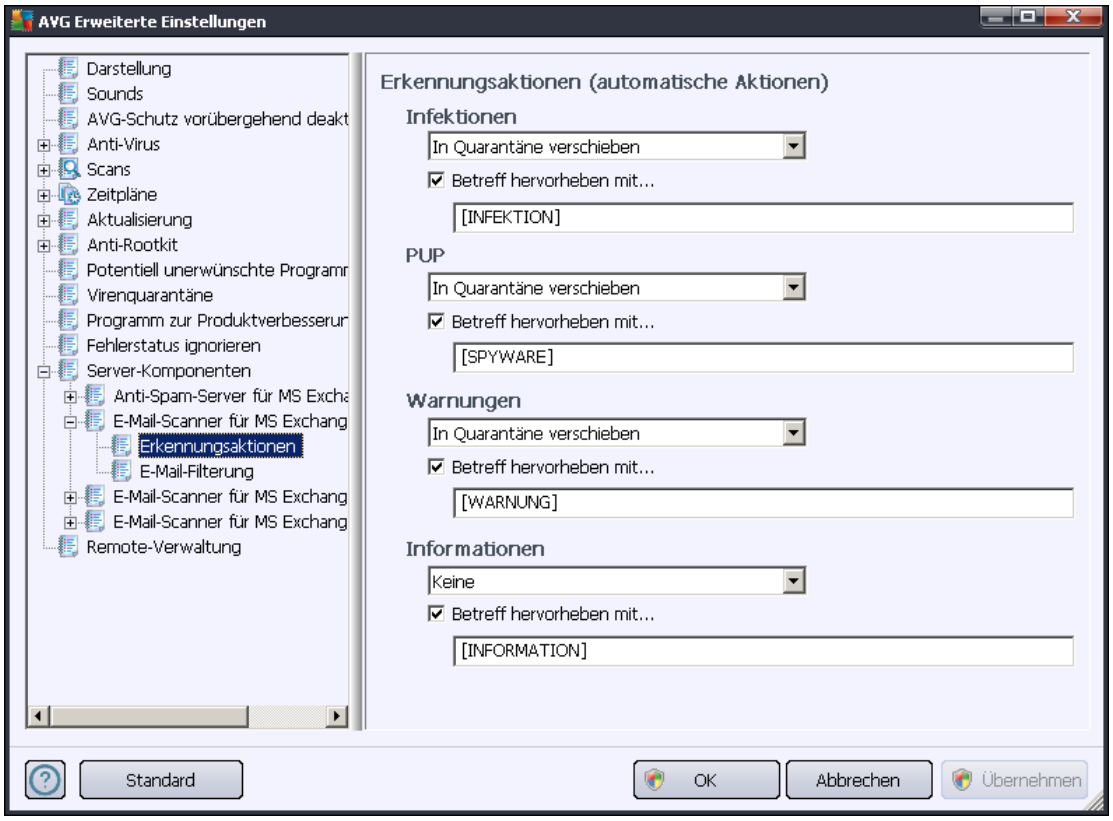
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 für Informationen über

zusätzliche Features von VSAPI 2.5 in der Anwendung Exchange 2003 Server.

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***eMail-Filterung***

4.5. Erkennungsaktionen



Im Untereintrag ***Erkennungsaktionen*** können Sie automatische Aktionen wählen, die während der Überprüfung ausgeführt werden sollen.

Die Aktionen sind für die folgenden Einträge verfügbar:

- ***Infektionen***
- ***PUP (Potentiell unerwünschte Programme)***
- ***Warnungen***
- ***Information***

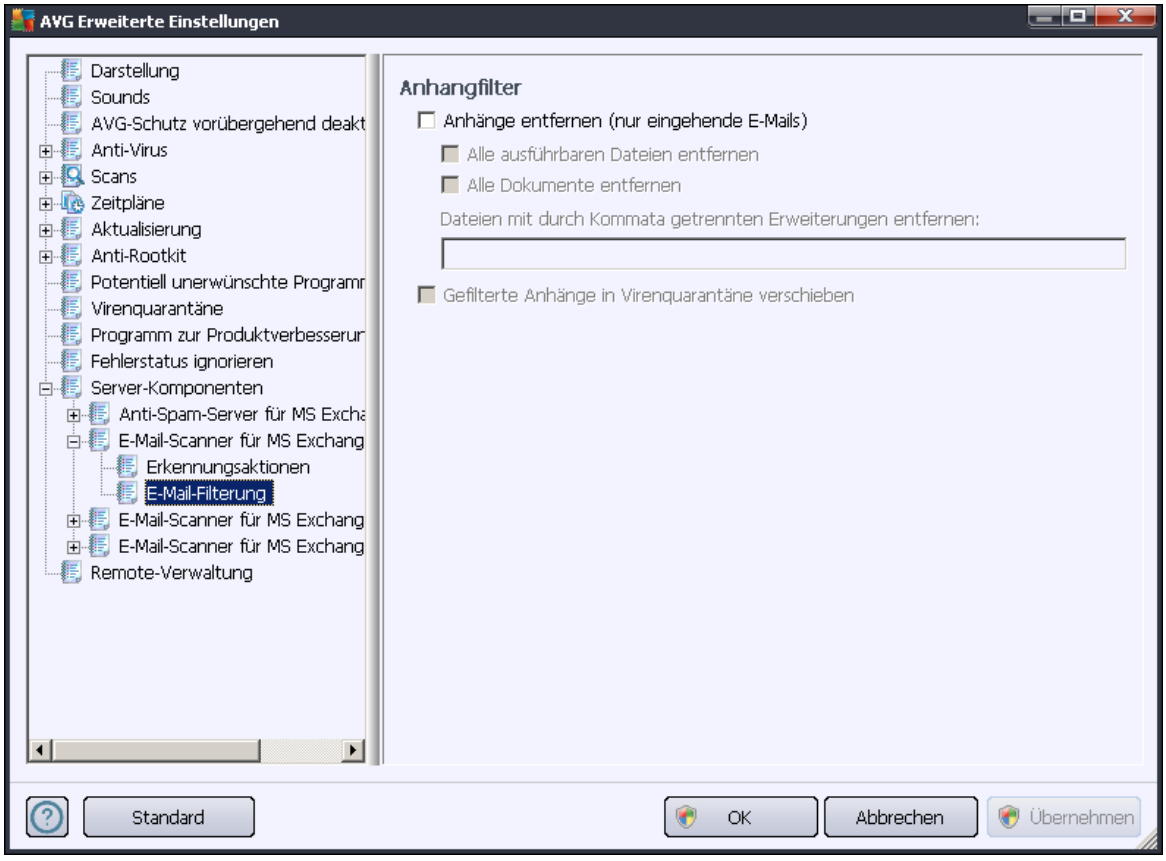
Wählen Sie im Dropdown-Menü für jeden Eintrag eine Aktion aus:

- ***Keine*** – Es wird keine Aktion ausgeführt.
- ***In Quarantäne verschieben*** – Die vorhandene Bedrohung wird in die Virenquarantäne verschoben.
- ***Entfernen*** – Die vorhandene Bedrohung wird entfernt.

Um einen benutzerdefinierten Betrefftext für Nachrichten einzugeben, die den betreffenden Eintrag/ die betreffende Bedrohung enthalten, aktivieren Sie das Kontrollkästchen ***Betreff hervorheben mit...*** , und geben Sie den gewünschten Wert ein.

Hinweis: *Die zuletzt genannte Funktion ist nicht für den eMail-Scanner für MS Exchange (VSAPI) verfügbar.*

4.6. eMail-Filterung



Im Untereintrag ***eMail-Filterung*** können Sie wählen, welche Anhänge automatisch entfernt werden sollen, sofern gewünscht. Folgende Optionen sind verfügbar:

- ***Anhänge entfernen*** – Aktivieren Sie dieses Kontrollkästchen, um die Funktion einzuschalten.
- ***Alle ausführbaren Dateien entfernen*** – Entfernt alle ausführbaren Dateien.

- ***Alle Dokumente entfernen*** – Entfernt alle Dokumentdateien.

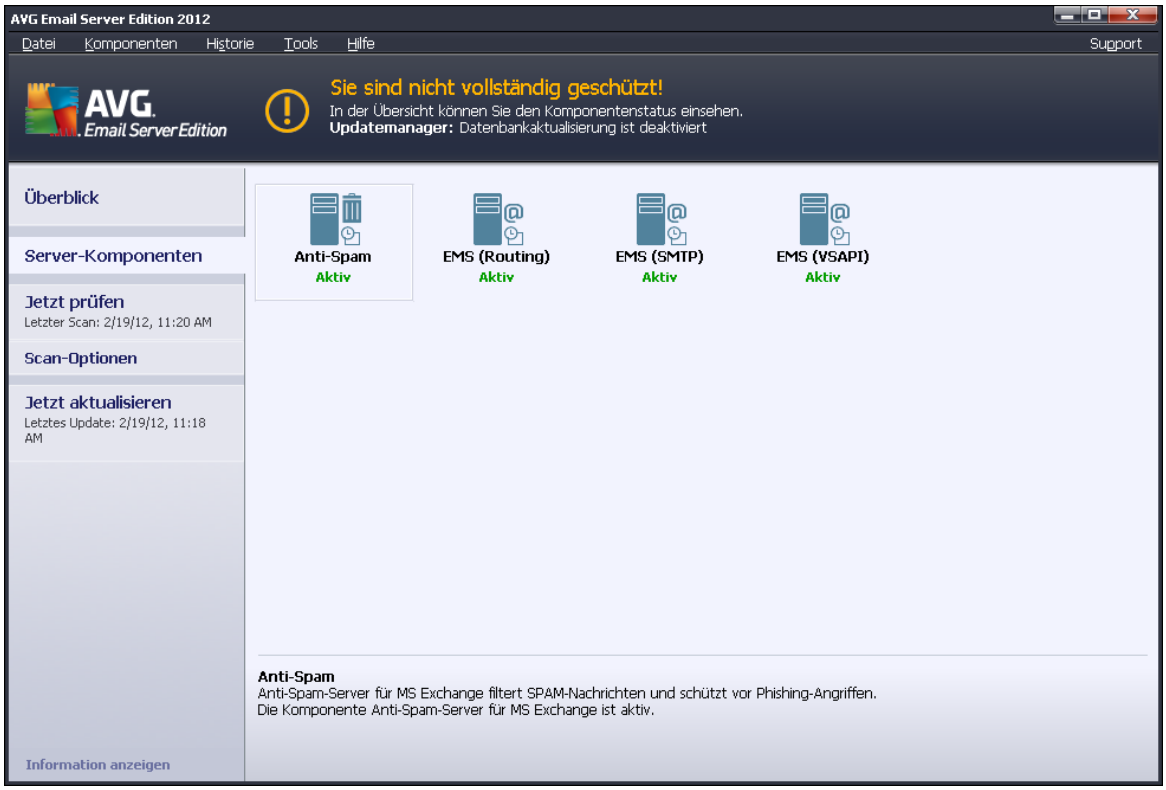
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Tragen Sie in diesem Feld die Dateierweiterungen ein, die Sie automatisch entfernen möchten. Setzen Sie dabei zwischen den einzelnen Erweiterungen Kommata.

- ***Gefilterte Anhänge in Virenquarantäne verschieben*** – aktivieren Sie dieses Kontrollkästchen, wenn die gefilterten Anhänge nicht vollständig entfernt werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, werden alle in diesem Dialog ausgewählten Anhänge automatisch in die Virenquarantäne verschoben. Dies ist ein sicherer Ort, um möglicherweise schädliche Dateien aufzubewahren – Sie können diese Dateien dort ansehen und untersuchen, ohne Ihr System zu gefährden. Sie können über das obere Menü auf Ihrer **AVG eMail Server Edition 2012** Hauptoberfläche auf die Virenquarantäne zugreifen. Klicken Sie einfach mit der linken Maustaste auf das Element ***Verlauf*** und wählen Sie die Option ***Virenquarantäne*** aus dem Kontextmenü aus.

5. eMail-Scanner für MS Exchange Server 2003

5.1. Überblick

Die Konfigurationsoptionen von eMail-Scanner für MS Exchange Server 2003 sind vollständig in AVG eMail Server Edition 2012 als Server-Komponenten integriert.



Zu den Server-Komponenten gehören:

Grundlegende Übersicht über die einzelnen Serverkomponenten:

- ***Anti-Spam – Anti-Spam-Server für MS Exchange***

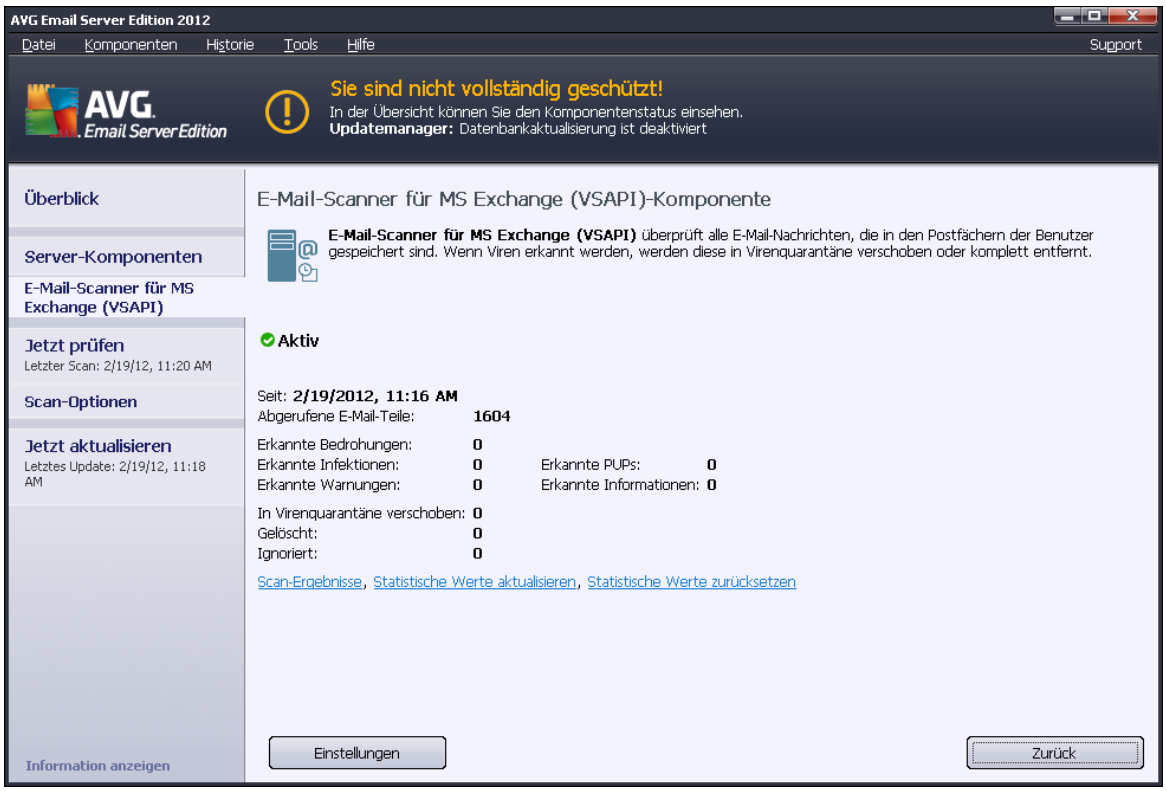
  Überprüft alle eingehenden eMail-Nachrichten und markiert unerwünschte eMails als SPAM. Die Komponente verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit den größtmöglichen Schutz gegen unerwünschte eMail-Nachrichten.

- ***EMS (VSAPI) – eMail-Scanner für MS Exchange (VSAPI)***

  Überprüft alle eMail-Nachrichten, die in den Postfächern der Benutzer gespeichert sind. Erkannte Viren werden in die Virenquarantäne verschoben oder vollständig entfernt.

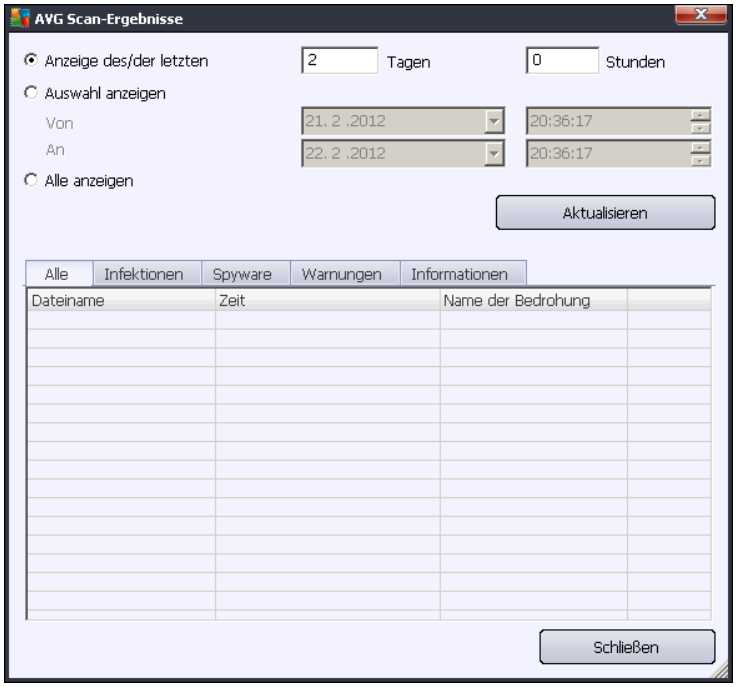
Klicken Sie auf das Symbol der gewünschten Komponente, um die Benutzeroberfläche zu öffnen.

Die ***Anti-Spam-Komponente*** besitzt ein eigenes Fenster, das in einem separaten Kapitel beschrieben wird. Die Oberfläche des ***eMail-Scanner für MS Exchange (VSAPI)*** beinhaltet die folgenden Steuerschaltflächen und Links:



- ***Scan-Ergebnisse***

  Öffnet einen neuen Dialog, in dem Sie die Scan-Ergebnisse überprüfen können:



Hier können Sie Nachrichten prüfen, die je nach Schweregrad in verschiedene Reiter unterteilt wurden. Einstellungen für Schweregrad und Berichte können Sie in der Konfiguration der einzelnen Komponenten vornehmen.

Standardmäßig werden nur die Ergebnisse der letzten zwei Tage angezeigt. Sie können den Anzeigezeitraum ändern, indem Sie die folgenden Optionen anpassen:

- ***Letzte anzeigen*** – Geben Sie die gewünschten Tage und Stunden ein.
- ***Auswahl anzeigen*** – Geben Sie ein benutzerdefiniertes Zeitintervall an.
- ***Alle anzeigen*** – Zeigt die Ergebnisse für den gesamten Zeitraum an.

Verwenden Sie die Schaltfläche ***Aktualisieren***, um die Ergebnisse neu zu laden.

- ***Statistikwerte aktualisieren*** – Aktualisiert die oben angezeigten Statistiken.
- ***Statistikwerte zurücksetzen*** – Setzt die gesamte Statistik auf null zurück.

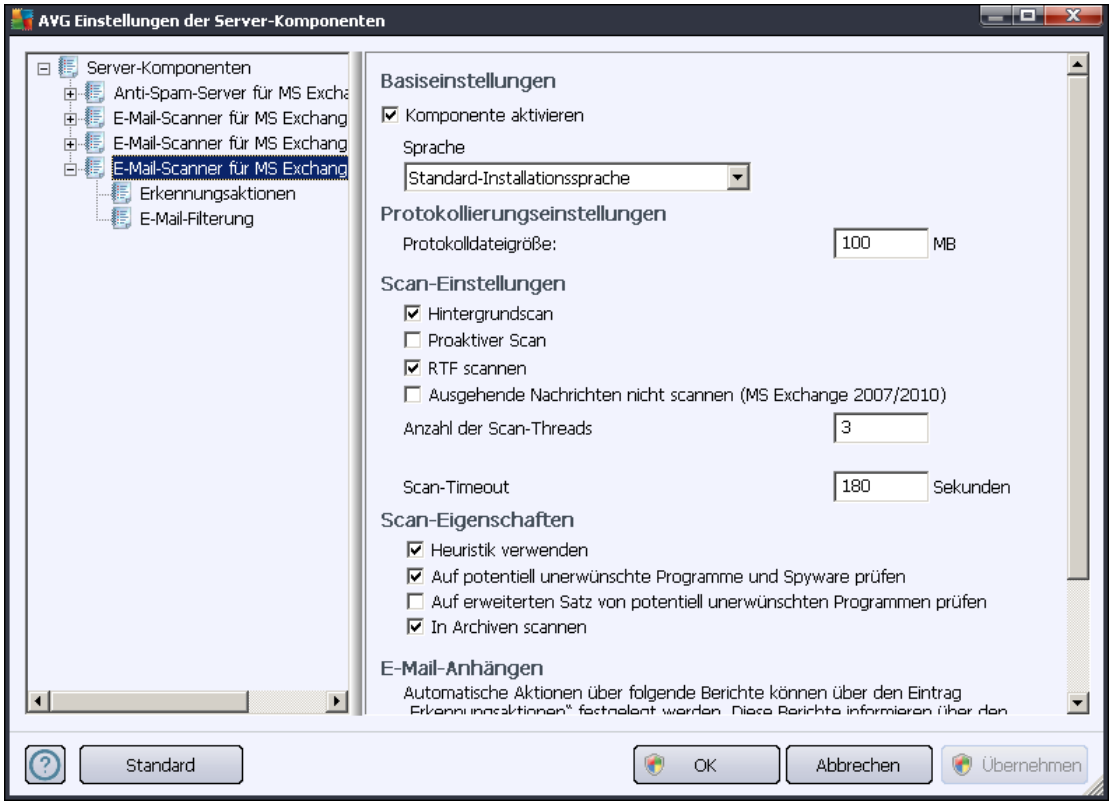
Folgende Schaltflächen stehen zur Verfügung:

- ***Einstellungen*** – Verwenden Sie diese Schaltfläche, um die Einstellungen der Komponente zu öffnen.
- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um zur Übersicht über die Server-Komponenten zurückzukehren.

Mehr Informationen zu den individuellen Einstellungen der Komponenten finden Sie in den folgenden Kapiteln.

5.2. eMail-Scanner für MS Exchange (VSAPI)

Dieses Element enthält Einstellungen für den ***eMail-Scanner für MS Exchange (VSAPI)***.



Der Abschnitt ***Grundeinstellungen*** enthält die folgenden Optionen:

- ***Komponente aktivieren*** – Deaktivieren Sie diese Option, um die gesamte Komponente zu deaktivieren.
- ***Sprache*** – Wählen Sie die bevorzugte Komponentensprache aus.

Der Abschnitt ***Protokollierungseinstellungen***:

- ***Protokolldateigröße*** – Legen Sie die gewünschte Größe für die Protokolldatei fest. Standardwert: 100 MB.

Der Abschnitt ***Scan-Einstellungen***:

- ***Hintergrundscan*** – Hier können Sie den Prozess der Hintergrundprüfung aktivieren und deaktivieren. Die Hintergrundprüfung ist eine der Eigenschaften der VSAPI 2.0/2.5-Anwendungsschnittstelle. Es handelt sich um das Scannen der Exchange Messaging Datenbanken in eigenen Threads. Wird ein Objekt in den Ordnern der Benutzerpostfächer gefunden, das noch nicht mit dem neuesten Update der Virendatenbank von AVG gescannt wurde, wird es zum Scannen an AVG für Exchange Server weitergeleitet. Die Suche nach nicht geprüften Objekten und der Virentest werden parallel ausgeführt.

Für jede Datenbank wird ein bestimmter Thread niedriger Priorität verwendet, um sicherzustellen, dass andere Aufgaben (z. B. das Speichern von eMail-Nachrichten in der Microsoft Exchange-Datenbank) vorrangig ausgeführt werden.

- ***Proaktiver Scan (eingehende Nachrichten)***

  Hier können Sie die Funktion zum proaktiven Scannen von VSAPI 2.0/2.5 aktivieren und deaktivieren. Diese Scans werden ausgeführt, wenn ein Element an einen Ordner geliefert wird, aber keine Anforderung vom Client vorliegt.

  Sobald die Nachrichten an den Exchange-Speicher übermittelt wurden, werden sie mit niedriger Priorität in die globale Scan-Warteschlange eingereiht (maximal 30 Elemente). Sie werden in der Reihenfolge ihres Eintreffens gescannt. Sollte ein Zugriff auf ein Element in der Warteschlange registriert werden, wird dieses auf hohe Priorität gesetzt.

  Hinweis: *Sollten zu viele Nachrichten vorliegen, werden diese ohne Scan in den Speicher verschoben.*

Hinweis: *Auch wenn Sie die beiden Optionen* ***Hintergrundscan*** *und* ***Proaktiver Scan*** *deaktivieren, bleibt der On-Access-Scanner weiterhin aktiv, wenn ein Benutzer versucht, eine Nachricht mit MS Outlook herunterzuladen.*

- ***Scan RTF*** – Sie können hier festlegen, ob RTF-Dateien geprüft werden sollen.
- ***Anzahl der Scan-Threads*** – *Der Prozess der Virenprüfung ist in der Standardeinstellung in verschiedene Threads aufgeteilt, um die Scanleistung auf einem hohen Niveau zu halten.* Sie können hier die Anzahl der Threads ändern.

  Die Standardanzahl wird nach der Formel „2 × 'Anzahl der Prozessoren' + 1“ berechnet.

  Die minimale Anzahl der Threads wird nach der Formel (Anzahl der Prozessoren + 1) / 2 berechnet.

  Die maximale Anzahl der Threads wird nach der Formel Anzahl der Prozessoren × 5 + 1 berechnet.

  Wenn der Wert der minimale (oder kleiner) oder maximale (oder größer) Wert ist, wird der Standardwert verwendet.

- ***Scan-Timeout*** – Die maximale Wartezeit (in Sekunden) eines Threads für den Zugriff auf eine zu scannende Nachricht (Standardwert: 180 Sekunden).

Der Abschnitt ***Scan-Eigenschaften***:

- ***Heuristik verwenden*** – Aktivieren Sie dieses Kontrollkästchen, um die heuristische Analyse bei der Überprüfung zu aktivieren.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – Aktivieren Sie diese Option, wenn potentiell unerwünschte Programme und Spyware gemeldet werden sollen.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** – Aktivieren Sie dieses Kontrollkästchen, um ein erweitertes Paket von Spyware zu erkennen:

Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können, oder Programme, die in jedem Fall harmlos, jedoch nicht erwünscht sind (verschiedene Symbolleisten usw.). Dies stellt eine zusätzliche Maßnahme für mehr Komfort und eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist. Hinweise: Diese Erkennungsfunktion stellt eine Ergänzung der vorangehenden Option dar. Lassen Sie daher die vorangehende Option immer aktiviert, um einen grundlegenden Schutz vor Spyware zu gewährleisten.

- ***In Archiven scannen*** – Aktivieren Sie diese Option, wenn der Scanner auch Archiv-Dateien (ZIP, RAR usw.) durchsuchen soll.

Im Abschnitt ***Berichte über eMail-Anhänge*** können Sie festlegen, welche Einträge bei der Überprüfung gemeldet werden sollen. Die Standardeinstellungen können einfach im ***Abschnitt Erkennungsaktionen***, Unterabschnitt ***Informationen*** angepasst werden (siehe unten).

Folgende Optionen sind verfügbar:

- ***Kennwortgeschützte Archive berichten***
- ***Kennwortgeschützte Dokumente berichten***
- ***Dateien berichten, die Makros enthalten***
- ***Versteckte Erweiterungen berichten***

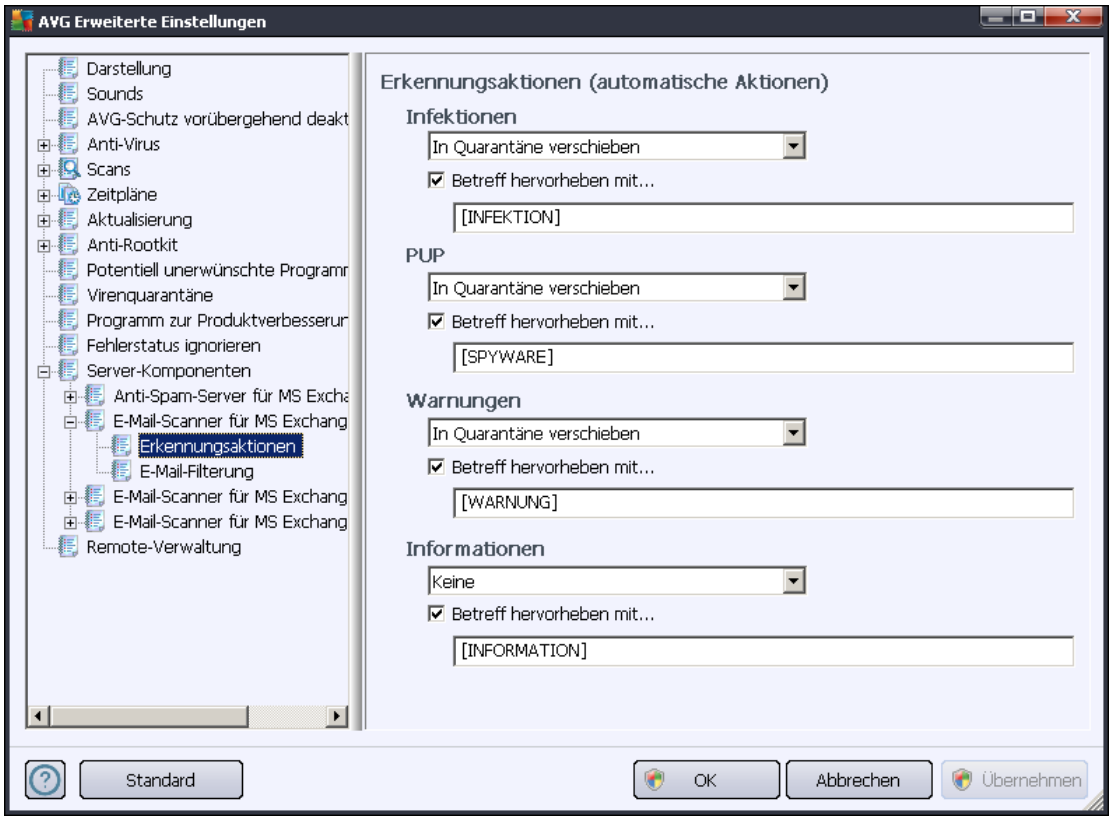
Diese Funktionen sind benutzerspezifische Erweiterungen der Dienste der Microsoft VSAPI 2.0/2.5-Benutzerschnittstelle. Ausführliche Informationen über die VSAPI 2.0/2.5 finden Sie unter folgenden Adressen und über die dortigen Links:

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k – Für Informationen über die Interaktion zwischen Exchange- und Antiviren-Software
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 für Informationen über zusätzliche Features von VSAPI 2.5 in der Anwendung Exchange 2003 Server.

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***eMail-Filterung***

5.3. Erkennungsaktionen



Im Untereintrag ***Erkennungsaktionen*** können Sie automatische Aktionen wählen, die während der Überprüfung ausgeführt werden sollen.

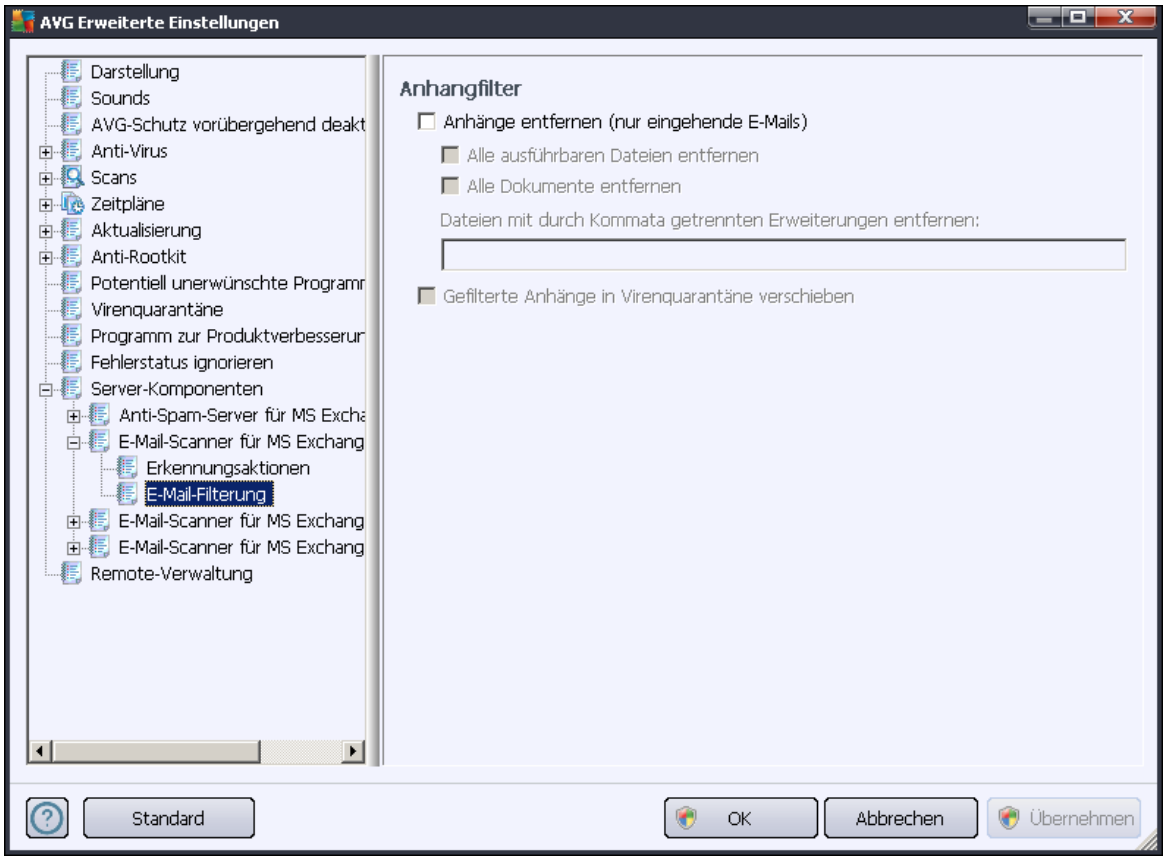
Die Aktionen sind für die folgenden Einträge verfügbar:

- ***Infektionen***
- ***PUP (Potentiell unerwünschte Programme)***
- ***Warnungen***
- ***Information***

Wählen Sie im Dropdown-Menü für jeden Eintrag eine Aktion aus:

- ***Keine*** – Es wird keine Aktion ausgeführt.
- ***In Quarantäne verschieben*** – Die vorhandene Bedrohung wird in die Virenquarantäne verschoben.
- ***Entfernen*** – Die vorhandene Bedrohung wird entfernt.

5.4. eMail-Filterung



Im Untereintrag ***eMail-Filterung*** können Sie wählen, welche Anhänge automatisch entfernt werden sollen, sofern gewünscht. Folgende Optionen sind verfügbar:

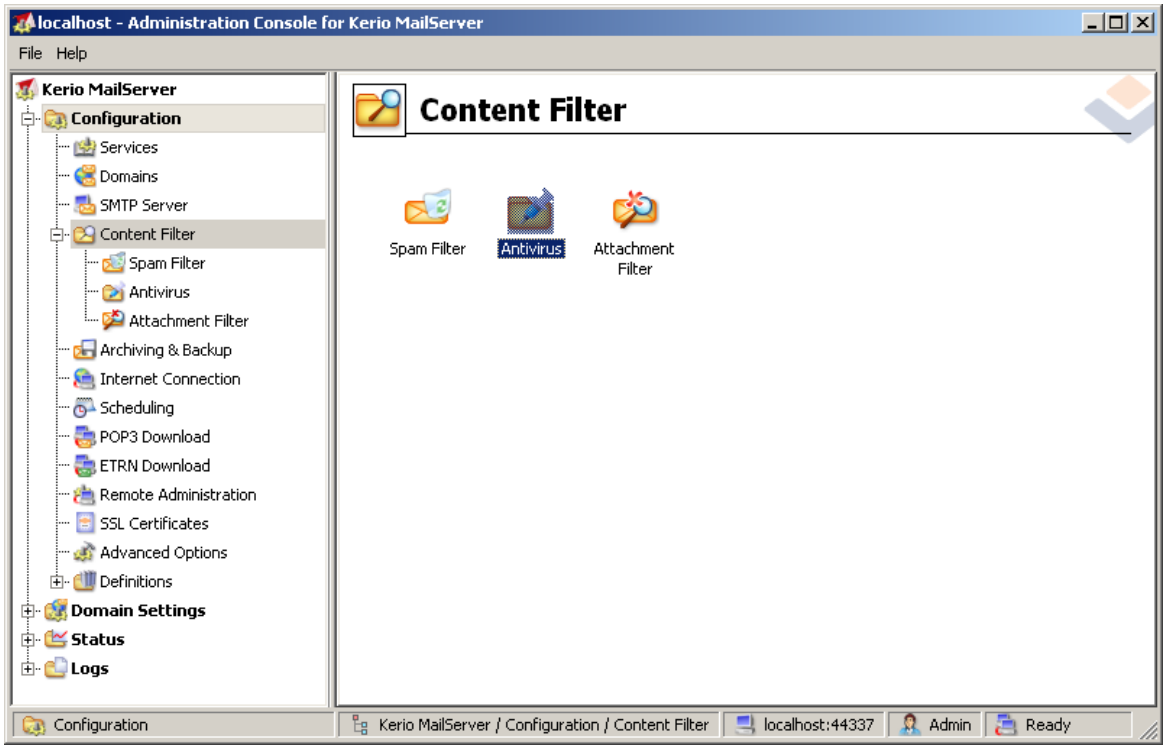
- ***Anhänge entfernen*** – Aktivieren Sie dieses Kontrollkästchen, um die Funktion einzuschalten.
- ***Alle ausführbaren Dateien entfernen*** – Entfernt alle ausführbaren Dateien.
- ***Alle Dokumente entfernen*** – Entfernt alle Dokumentdateien.
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Tragen Sie in diesem Feld die Dateierweiterungen ein, die Sie automatisch entfernen möchten. Setzen Sie dabei zwischen den einzelnen Erweiterungen Kommata.
- ***Gefilterte Anhänge in Virenquarantäne verschieben*** – aktivieren Sie dieses Kontrollkästchen, wenn die gefilterten Anhänge nicht vollständig entfernt werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, werden alle in diesem Dialog ausgewählten Anhänge automatisch in die Virenquarantäne verschoben. Dies ist ein sicherer Ort, um möglicherweise schädliche Dateien aufzubewahren – Sie können diese Dateien dort ansehen und untersuchen, ohne Ihr System zu gefährden. Sie können über das obere Menü auf Ihrer **AVG eMail Server Edition 2012** Hauptoberfläche auf die Virenquarantäne zugreifen. Klicken Sie

einfach mit der linken Maustaste auf das Element ***Verlauf*** und wählen Sie die Option ***Virenquarantäne*** aus dem Kontextmenü aus.

6. AVG für Kerio MailServer

6.1. Konfiguration

In Kerio MailServer ist der Virenschutz direkt integriert. Starten Sie die Kerio-Verwaltungskonsole, um den eMail-Schutz von Kerio MailServer über die Scan-Engine von AVG zu aktivieren. Wählen Sie in der Baumstruktur auf der linken Seite des Anwendungsfensters im Zweig Konfiguration den Unterzweig Inhaltsfilter aus:

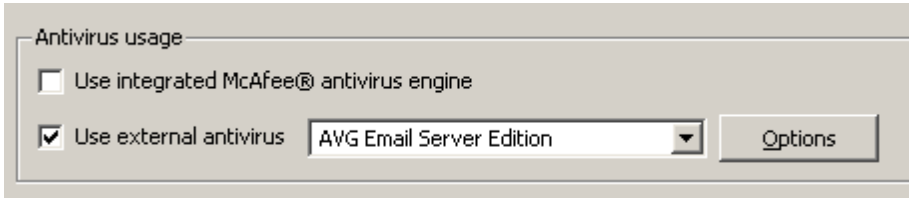


Wenn Sie auf den Eintrag „Inhaltsfilter“ klicken, wird ein Dialog mit drei Einträgen angezeigt:

- ***Spamfilter***
- ***Antivirus*** (siehe Abschnitt ***Antivirus***)
- ***Mailanhänge*** (siehe Abschnitt ***Mailanhänge***)

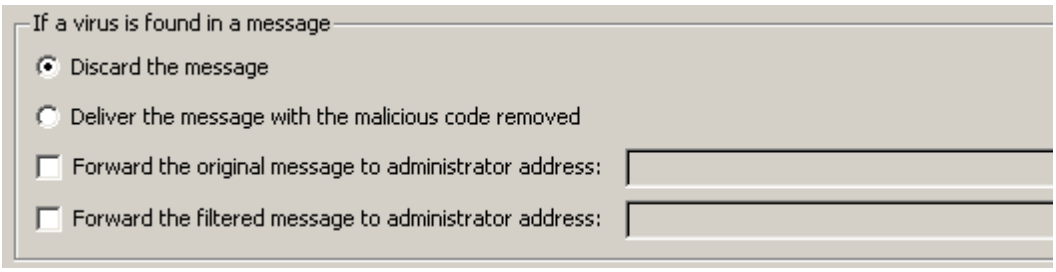
6.1.1. Anti-Virus

Zum Aktivieren von AVG für Kerio MailServer aktivieren Sie das Kontrollkästchen „Externes Antivirusprogramm verwenden“ und wählen Sie im Menü für die externe Antivirus-Software im Konfigurationsfenster im Bereich Antivirusbenutzung die Option „AVG eMail Server Edition“ aus:



Im folgenden Abschnitt können Sie festlegen, was mit einer infizierten oder gefilterten Datei geschehen soll:

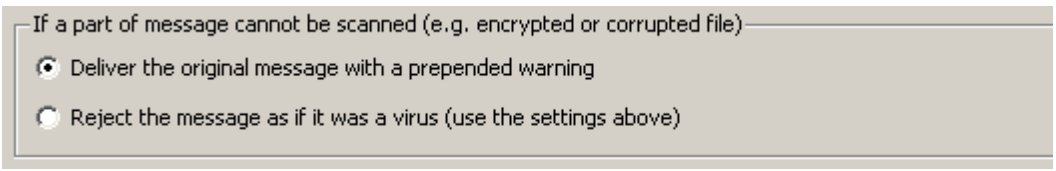
- ***In einer eMail wird ein Virus entdeckt***



Hier wird festgelegt, welche Aktion durchgeführt werden soll, wenn ein Virus in einer Nachricht entdeckt wird oder wenn eine Nachricht mit einem Filter für Anhänge überprüft wird:

  - ***Nachricht verwerfen*** – Wenn dieses Optionsfeld aktiviert ist, wird die infizierte oder gefilterte Nachricht gelöscht.
  - ***Nachricht mit entferntem schädlichem Code senden*** – Wenn dieses Optionsfeld aktiviert ist, wird die Nachricht an den Empfänger gesendet, jedoch ohne den möglicherweise schädlichen Anhang.
  - ***Ursprüngliche Nachricht an Administratoradresse weiterleiten*** – Wenn dieses Optionsfeld aktiviert ist, wird die vireninfizierte Nachricht an die im entsprechenden Textfeld angegebene Adresse gesendet.
  - ***Gefilterte Nachricht an Administratoradresse weiterleiten*** – Wenn dieses Optionsfeld aktiviert ist, wird die gefilterte Nachricht an die im entsprechenden Textfeld angegebene Adresse weitergeleitet.

- ***Ein Teil einer Nachricht kann nicht gescannt werden (z. B. bei einer verschlüsselten oder beschädigten Datei)***



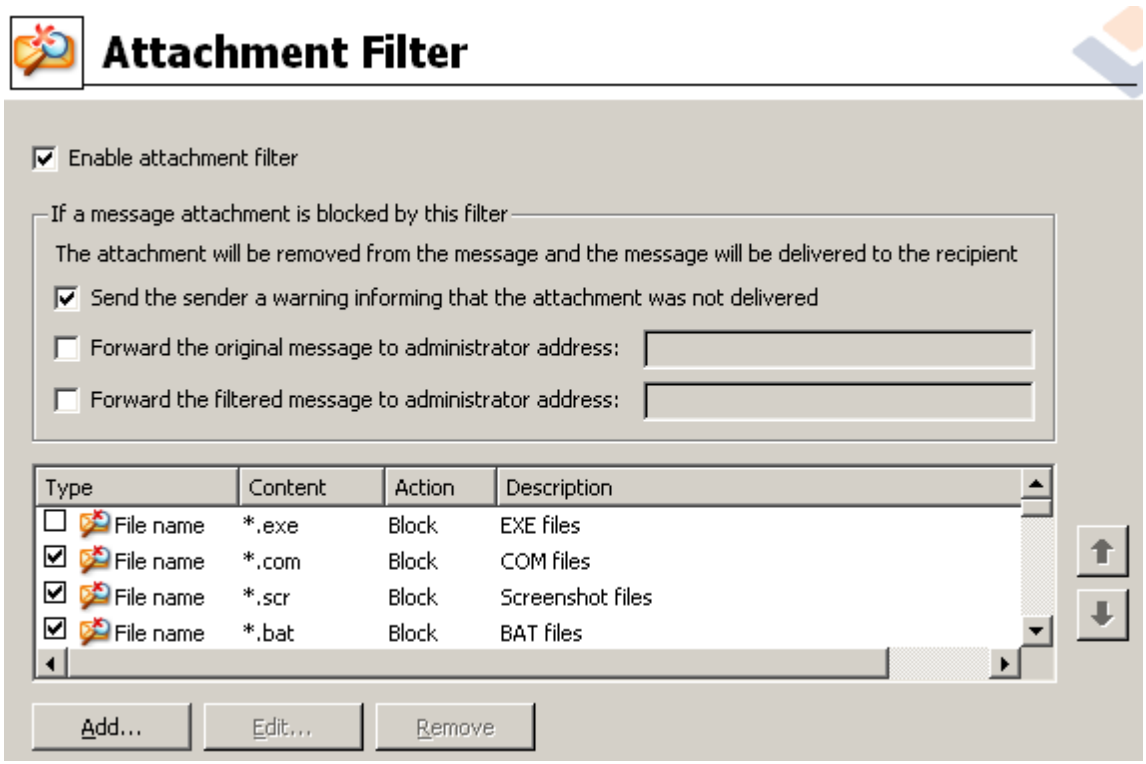
Hier wird festgelegt, welche Aktion durchgeführt werden soll, wenn ein Teil der Nachricht oder des Anhangs nicht gescannt werden kann:

- ***Senden der ursprünglichen Nachricht mit einer vorbereiteten Warnung*** – Die Nachricht (oder der Anhang) wird ungeprüft übermittelt. Der Benutzer wird gewarnt, dass die Nachricht möglicherweise immer noch Viren enthält.

- ***Nachricht als infiziert behandeln und zurückweisen*** – Das System reagiert so, als wäre ein Virus erkannt worden (z. B. wird die Nachricht ohne Anhang ausgeliefert oder der Anhang wird entfernt). Diese Option ist zwar sicher, jedoch ist das Senden von kennwortgeschützten Archiven nicht mehr möglich.

6.1.2. Filter für Anhänge

Im Menü Filter für Anhänge befindet sich eine Liste verschiedener Anhangsdefinitionen:



Über das Kontrollkästchen Filter für Anhang aktivieren können Sie den Filter für eMail-Anhänge aktivieren/deaktivieren. Optional können Sie die folgenden Einstellungen ändern:

- ***Warnung an den Absender schicken, dass der Anhang nicht übertragen wurde***

  Der Absender erhält eine Warnung von Kerio MailServer, dass eine Nachricht mit einem Virus oder einem blockierten Anhang versendet wurde.

- ***Ursprüngliche Nachricht an Administratoradresse weiterleiten***

  Die Nachricht wird (so wie sie ist – mit dem infizierten oder blockierten Anhang) an eine festgelegte eMail-Adresse gesendet – unabhängig davon, ob es sich bei der Adresse um eine lokale oder externe Adresse handelt.

- ***Gefilterte Nachricht an Administratoradresse weiterleiten***

  Die Nachricht wird ohne den infizierten oder blockierten Anhang (ausgenommen der unten ausgewählten Aktionen) an die angegebene eMail-Adresse weitergeleitet. Mit dieser Option kann überprüft werden, ob AVG Anti-Virus und/oder der Filter für Anhänge fehlerfrei funktionieren.

Jedes Element der Erweiterungsliste verfügt über vier Felder:

- ***Typ*** – Angabe zu der Art des Anhangs, der über die Erweiterung im Feld „Inhalt“ festgelegt wurde. Mögliche Werte sind Dateiname oder MIME-Typ. Sie können das entsprechende Kontrollkästchen in diesem Feld aktivieren, um das Filtern des Anhangs für dieses Element zu aktivieren.
- ***Inhalt*** – Hier kann eine zu filternde Erweiterung eingegeben werden. Hierfür können Sie Platzhalter des Betriebssystems nutzen (zum Beispiel steht die Zeichenfolge '*.doc.*' für alle Dateien mit der Erweiterung „.doc“ usw.).
- ***Aktion*** – Definiert die Aktion, die mit dem entsprechenden Anhang durchgeführt werden soll. Mögliche Aktionen lauten „Akzeptieren“ (akzeptiert den Anhang) und „Blockieren“ (eine Aktion wird wie über der Liste deaktivierter Anhänge angegeben ausgeführt).
- ***Beschreibung*** – In diesem Feld wird die Beschreibung des Anhangs festgelegt.

Durch Klicken auf Entfernen können Sie einen Eintrag aus der Liste entfernen. Der Liste können weitere Einträge hinzugefügt werden, indem Sie auf ***Hinzufügen*** klicken. Sie können auch einen bestehenden Eintrag ändern, indem Sie auf ***Bearbeiten*** klicken. Dann wird folgendes Fenster angezeigt:

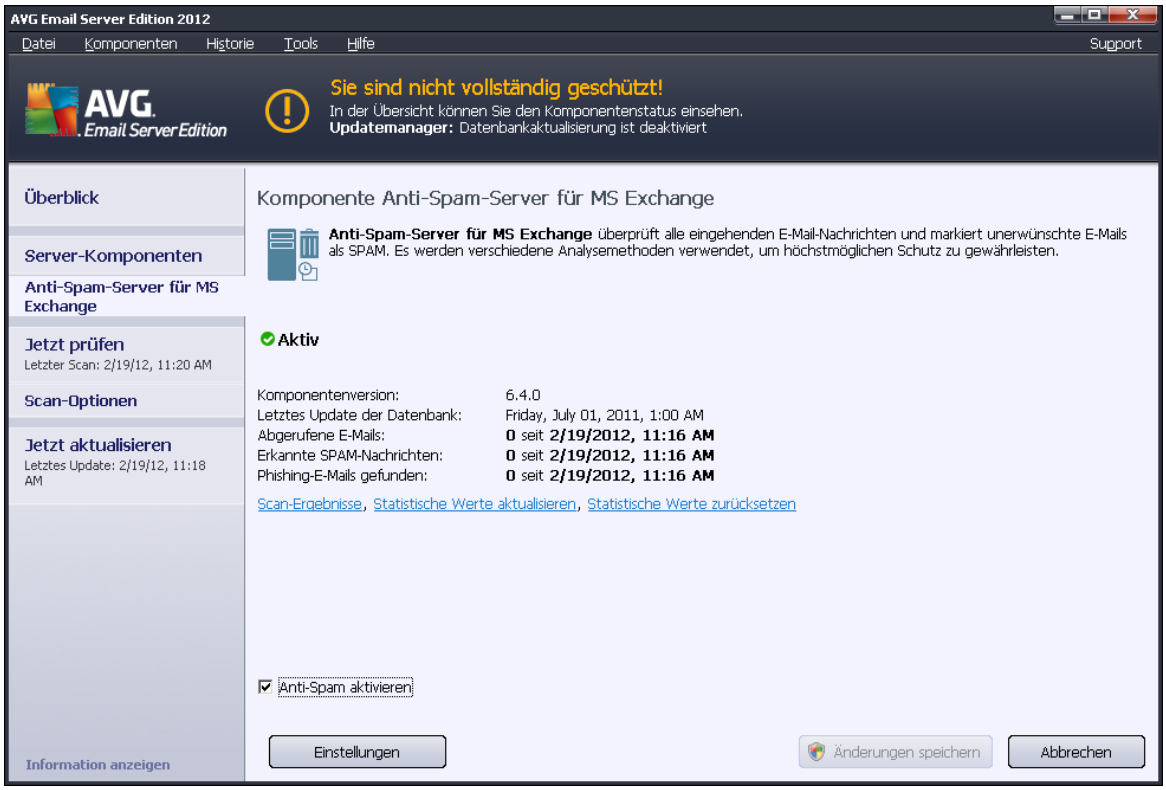
- Im Feld Beschreibung können Sie eine kurze Beschreibung des zu filternden Anhangs eingeben.
- Im Feld Wenn eine eMail den folgenden Anhang enthält können Sie die Art des Anhangs auswählen (Dateiname oder MIME-Typ). Sie können auch eine bestimmte Erweiterung aus

der angebotenen Liste der Erweiterungen auswählen oder den Platzhalter für die Erweiterung direkt eingeben.

Im Feld Auszuführende Aktion können Sie festlegen, ob der definierte Anhang blockiert oder akzeptiert werden soll.

7. Anti-Spam-Konfiguration

7.1. Benutzeroberfläche des Anti-Spam

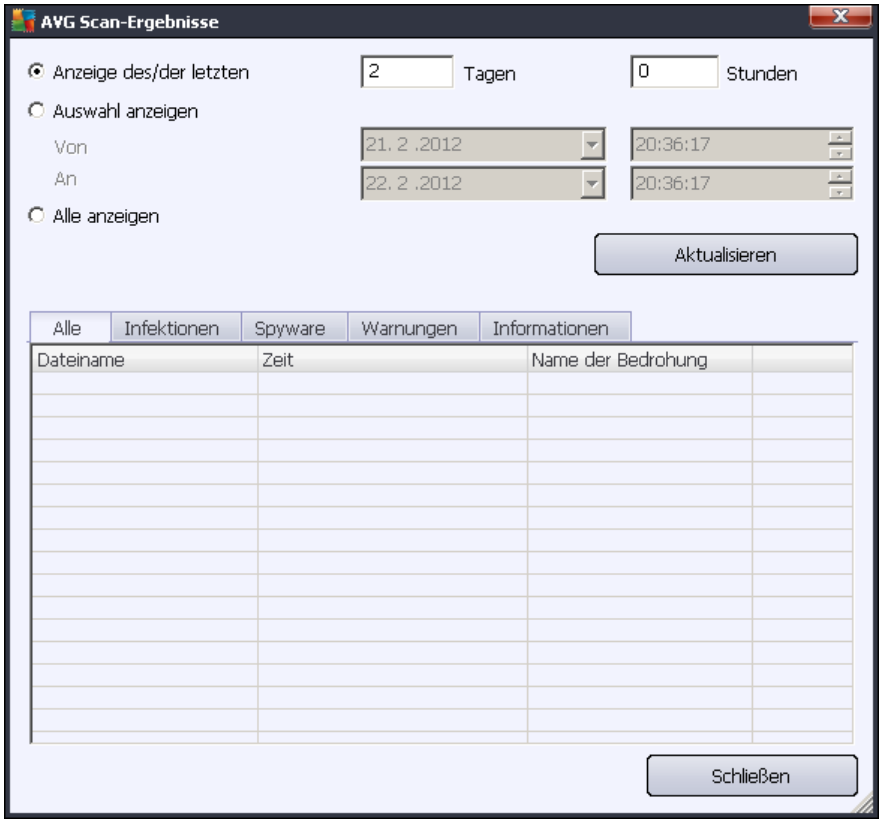


Der Dialog der Server-Komponente ***Anti-Spam*** befindet sich im Abschnitt ***Server-Komponenten*** (Menü links). Dieser Dialog enthält Informationen zur Funktionsweise der Server-Komponente, zum aktuellen Status (*Anti-Spam-Server für MS Exchange ist aktiv*) sowie statistische Daten.

Verfügbare Links:

- ***Scan-Ergebnisse***

  Öffnet einen neuen Dialog, in dem Sie die Scan-Ergebnisse von Anti-Spam überprüfen können:



Hier können Sie Nachrichten prüfen, die entweder als SPAM (unerwünschte Nachricht) oder als Phishing-Versuch (ein Versuch, private Daten, Kontoinformationen, Identitäten usw. zu stehlen) erkannt wurden. Standardmäßig werden nur die Ergebnisse der letzten zwei Tage angezeigt. Sie können den Anzeigezeitraum ändern, indem Sie die folgenden Optionen anpassen:

- ***Letzte anzeigen*** – Geben Sie die gewünschten Tage und Stunden ein.
- ***Auswahl anzeigen*** – Geben Sie ein benutzerdefiniertes Zeitintervall an.
- ***Alle anzeigen*** – Zeigt die Ergebnisse für den gesamten Zeitraum an.

Verwenden Sie die Schaltfläche ***Aktualisieren***, um die Ergebnisse neu zu laden.

- ***Statistikwerte aktualisieren*** – Aktualisiert die oben angezeigten Statistiken.
- ***Statistikwerte zurücksetzen*** – Setzt die gesamte Statistik auf null zurück.

Der Abschnitt **Anti-Spam-Einstellungen** des Dialogs enthält das Kontrollkästchen ***Anti-Spam aktivieren***. Deaktivieren Sie es, um den Anti-Spam-Schutz aufzuheben (d.h. die gesamte Komponente zu deaktivieren). Der Anti-Spam-Schutz kann über dasselbe Kontrollkästchen oder durch Aktivierung eines ähnlichen Kontrollkästchens in Anti-Spam-Einstellungen wieder aktiviert werden.

Folgende Schaltflächen stehen zur Verfügung:

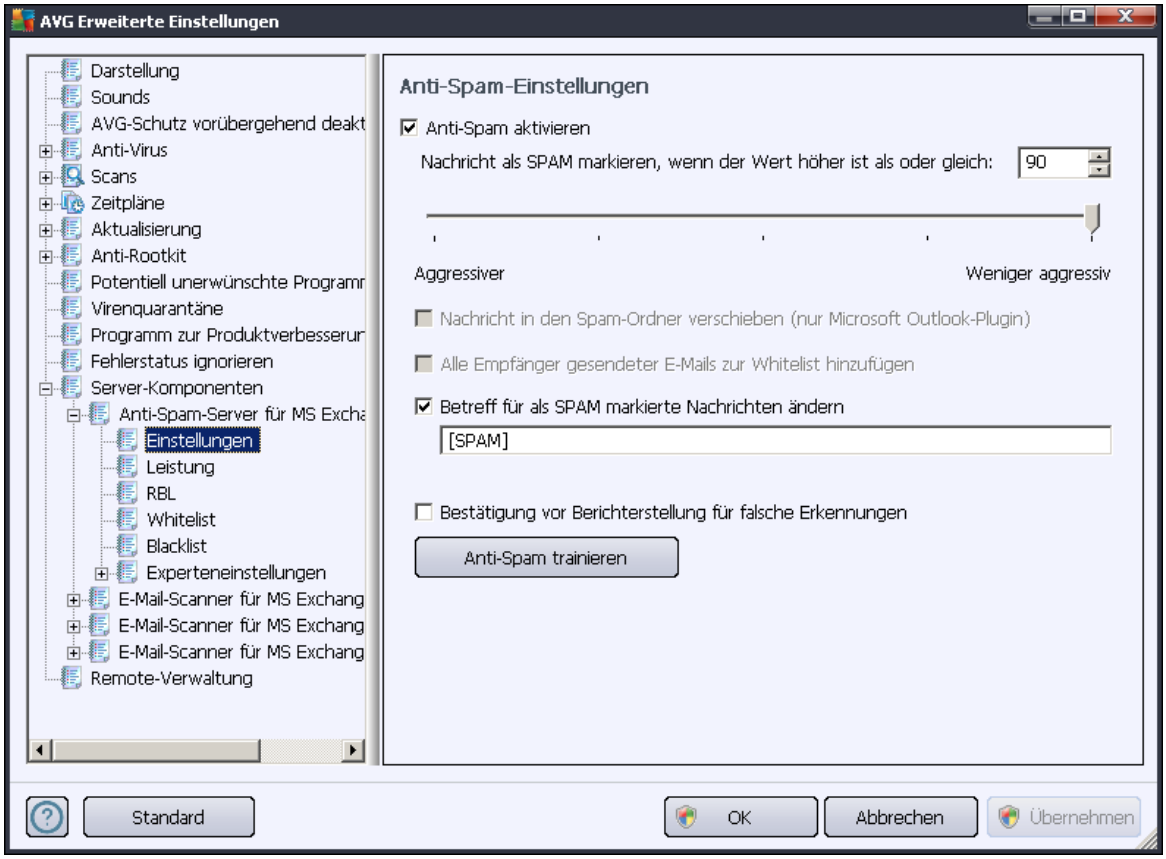
- ***Einstellungen*** – Klicken Sie auf diese Schaltfläche, um die Anti-Spam-Einstellungen zu öffnen.
- ***Zurück*** – Klicken Sie auf diese Schaltfläche, um zur Übersicht über die Server-Komponenten zurückzukehren.

7.2. Grundlagen zu Anti-Spam

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

Anti-Spam überprüft alle eingehenden eMails und markiert unerwünschte eMails als SPAM. Die Komponente verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit den größtmöglichen Schutz gegen unerwünschte eMail-Nachrichten.

7.3. Anti-Spam-Einstellungen



Im Dialog ***Grundeinstellungen für Anti-Spam*** können Sie über die Option ***Anti-Spam aktivieren*** festlegen, ob Sie die Überprüfung Ihrer eMail-Kommunikation auf Spam zulassen oder verweigern möchten.

In diesem Dialog können Sie zudem mehr oder weniger aggressive Bewertungen auswählen. Der ***Anti-Spam***-Filter weist jeder Nachricht eine Bewertung zu (*z. B. wie sehr der Nachrichteninhalt SPAM ähnelt*), die auf verschiedenen dynamischen Prüftechniken basiert. Sie können die Einstellung ***Nachricht als Spam markieren, wenn der Wert höher ist als oder gleich*** anpassen, indem Sie entweder den Wert (*50 bis 90*) eingeben oder den Schieberegler nach links oder rechts verschieben.

Im Folgenden finden Sie eine kurze Erläuterung der Schwellenwerte:

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

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

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

- ***Wert 50–59*** – Sehr aggressive Konfiguration. Es ist sehr wahrscheinlich, dass auch Nachrichten abgefangen werden, die nicht wirklich Spam sind. Dieser Wertebereich wird für den normalen Gebrauch nicht empfohlen.

Sie können außerdem festlegen, wie die erkannten Spam-Nachrichten behandelt werden sollen:

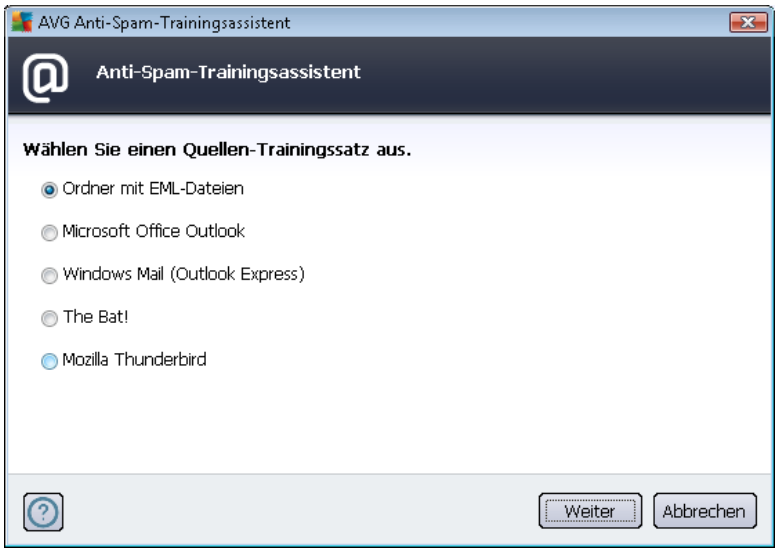
- ***Betreff für als SPAM markierte Nachrichten ändern*** – Aktivieren Sie dieses Kontrollkästchen, wenn alle als Spam erkannten Nachrichten mit einem bestimmten Wort oder Zeichen im Betrefffeld markiert werden sollen (geben Sie den gewünschten Text in das aktivierte Textfeld ein)

- ***Bestätigung vor Berichterstellung für falsche Erkennungen*** – (Setzt voraus, dass Sie während des Installationsvorgangs der Teilnahme am Programm zur Produktverbesserung zugestimmt haben.) Mithilfe dieses Programms erhalten wir von Benutzern auf der ganzen Welt aktuelle Informationen über Bedrohungen und können im Gegenzug unseren Online-Schutz für alle noch weiter verbessern, d. h. wenn Sie es zulassen, erkannte Bedrohungen an AVG zu senden. Die Berichterstellung erfolgt automatisch. Sie können jedoch das Kontrollkästchen aktivieren, wenn Sie benachrichtigt werden möchten, bevor ein Bericht über erkannten Spam an AVG gesendet wird. So können Sie sich vergewissern, dass es sich bei der Nachricht wirklich um Spam handelt.

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

7.3.1. Anti-Spam-Trainingsassistent

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



Folgende Optionen stehen zur Auswahl:

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

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

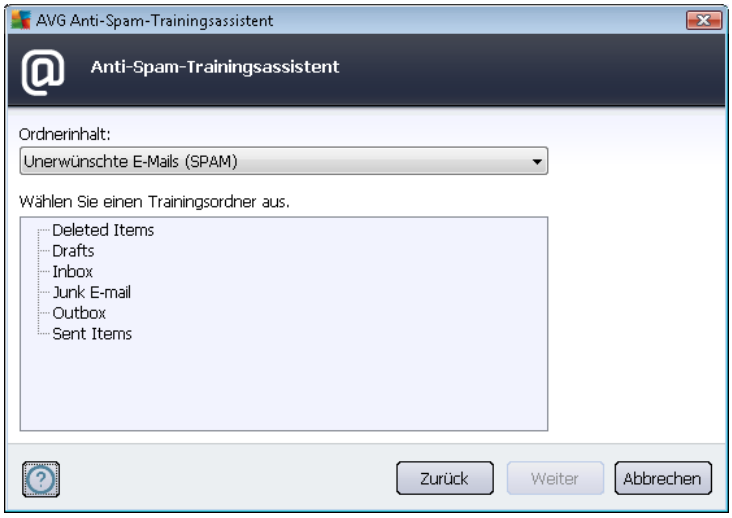
Um das Training zu erleichtern und zu beschleunigen, empfiehlt sich eine entsprechende Vorsortierung, so dass·der Ordner nur noch die (erwünschten bzw.·unerwünschten) eMails für das Training enthält. Dieser Schritt ist jedoch nicht zwingend erforderlich, da Sie die eMails auch später filtern können.

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

7.3.2. Ordner mit Nachrichten auswählen

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

Ordner mit EML-Dateien



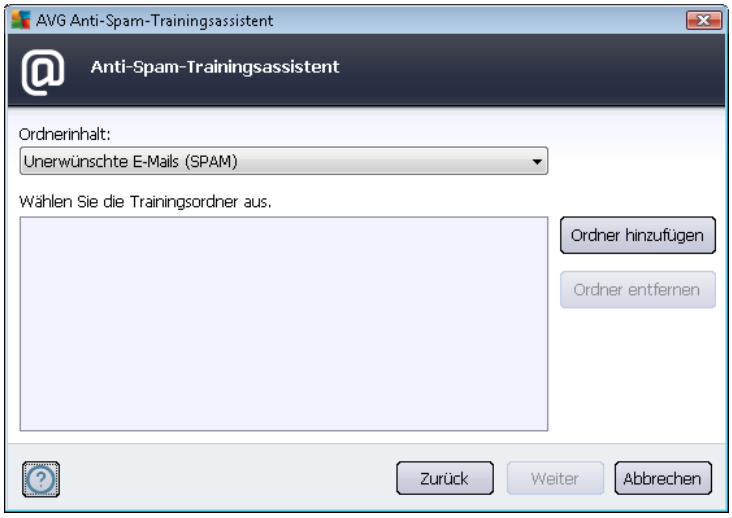
Wählen Sie in diesem Dialog bitte den Ordner mit den Nachrichten aus, den Sie für Trainingszwecke verwenden möchten. Klicken Sie auf die Schaltfläche ***Ordner hinzufügen***, um den Ordner mit den EML-Dateien zu suchen (*gespeicherte eMail-Nachrichten*). Der ausgewählte Ordner wird anschließend im Dialog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

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

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

Ein bestimmter eMail-Client

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

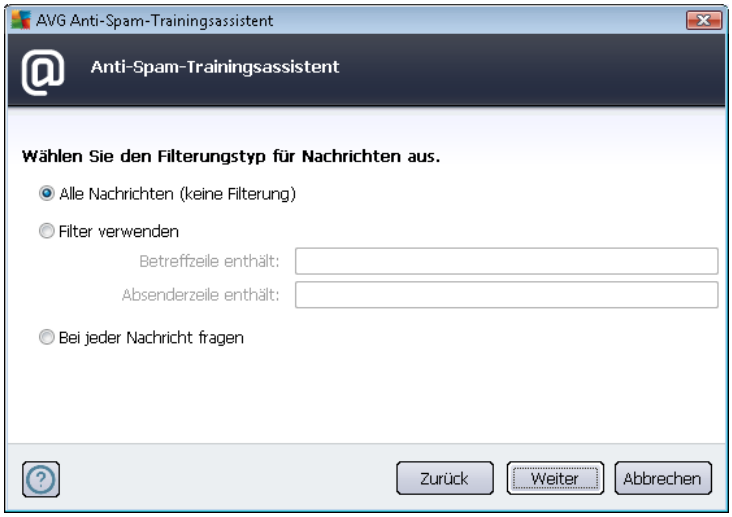


Hinweis: *Wenn Sie Microsoft Office Outlook verwenden, werden Sie zunächst dazu aufgefordert, ein Profil in „MS Office Outlook" auszuwählen.*

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

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

7.3.3. Optionen für Nachrichtenfilterung



In diesem Dialog können Sie Filter für eMail-Nachrichten konfigurieren.

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

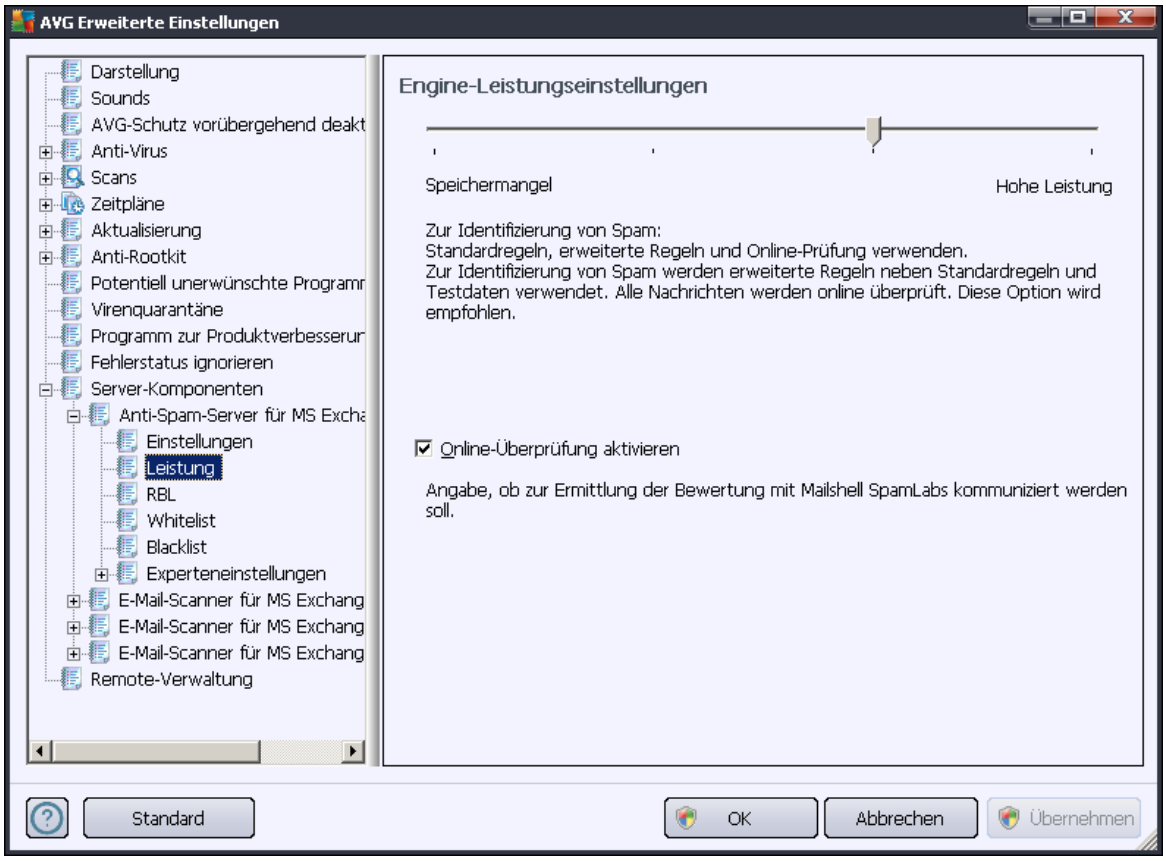
ausschließlich Nachrichten enthält, die Sie für das Training verwenden möchten, wählen Sie die Option ***Alle Nachrichten (keine Filterung)*** .

- ***Filter verwenden*** – Um eine erweiterte Filterung anzuwenden, wählen Sie die Option ***Filter verwenden*** aus. Sie können ein Wort (*Name*), ein Teil eines Wortes oder eine Phrase eingeben, um im Betreff bzw. im Absenderfeld der eMail danach zu suchen. Alle Nachrichten, die exakt mit den Suchkriterien übereinstimmen, werden unmittelbar·für das Training verwendet. Wenn Sie beide Textfelder ausfüllen, werden auch Adressen verwendet, für die nur eines der beiden Suchkriterien zutrifft!

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

Nachdem Sie die gewünschte Option ausgewählt haben, klicken Sie auf ***Weiter***. Im folgenden Dialog wird Ihnen lediglich mitgeteilt, dass der Assistent zur Bearbeitung der Nachrichten bereit ist. Um das Training zu starten, klicken Sie erneut auf die Schaltfläche ***Weiter***. Das Training wird nun den zuvor ausgewählten Bedingungen entsprechend gestartet.

7.4. Leistung



Der Dialog ***Engine-Leistungseinstellungen*** (*zu öffnen über das Element* ***Leistung*** *im linken*

Navigationsbereich) enthält Leistungseinstellungen für die Komponente ***Anti-Spam***. Bewegen Sie den Schieberegler nach links oder rechts, um die Scan-Leistung zwischen den Modi ***Speichermangel*** / ***Hohe Leistung*** einzustellen.

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

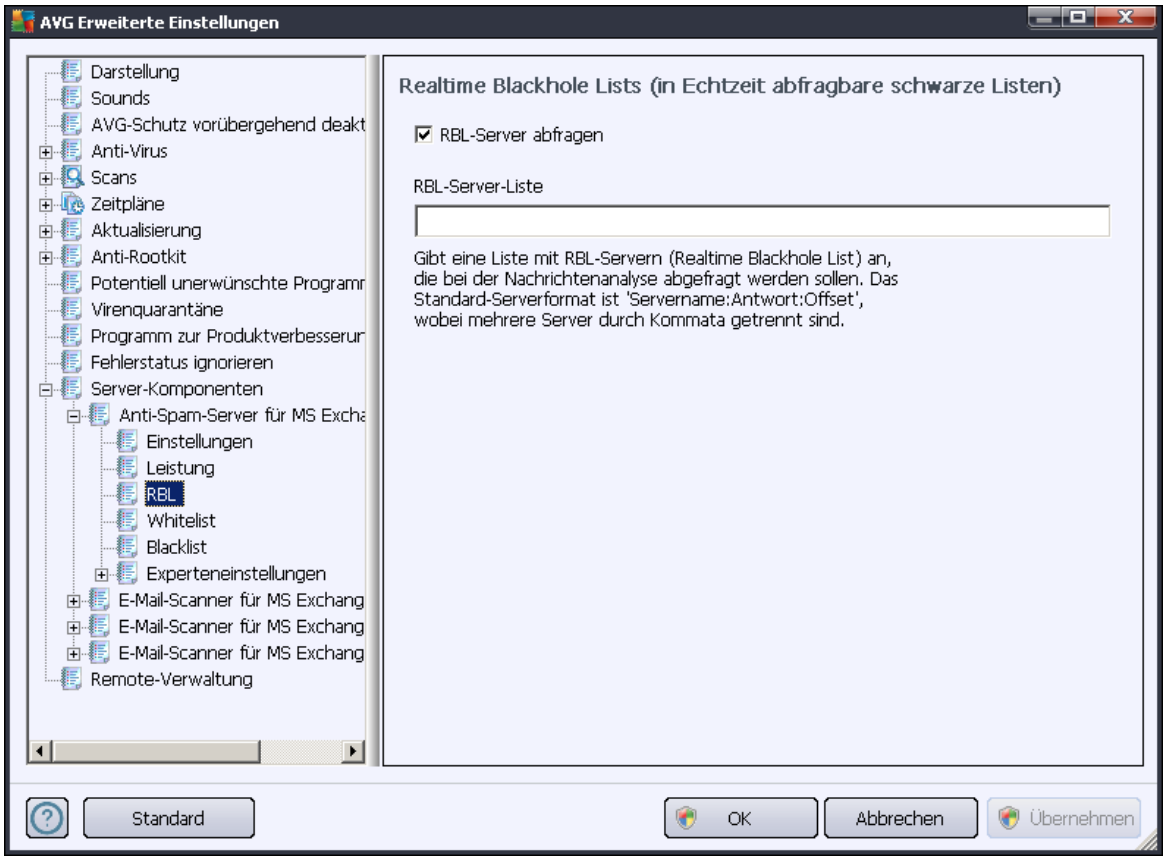
- ***Hohe Leistung*** – Für diesen Modus ist sehr viel Speicher erforderlich. Während des Scanvorgangs werden zur Identifizierung von Spam folgende Funktionen verwendet: Regeln und Spam-Datenbank-Cache, einfache und erweiterte Regeln, IP-Adressen von Spammern und Spammer-Datenbanken.

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

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

7.5. RBL

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



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

Der RBL-Server (*Realtime Blackhole Lists (in Echtzeit abfragbare schwarze Listen)*) ist ein DNS-Server mit einer umfangreichen Datenbank bekannter Spam-Sender. Bei Aktivierung dieser Funktion werden alle eMails mit den Adressen der RBL-Serverdatenbank verglichen und als Spam markiert, wenn Sie einem Datenbankeintrag entsprechen.

Die RBL-Serverdatenbanken enthalten die allerneuesten Spam-Fingerabdrücke und ermöglichen so die beste und exakteste Spam-Erkennung. Diese Funktion ist besonders nützlich für Benutzer, die sehr viel Spam empfangen, der normalerweise nicht von der Anti-Spam-Engine erkannt wird.

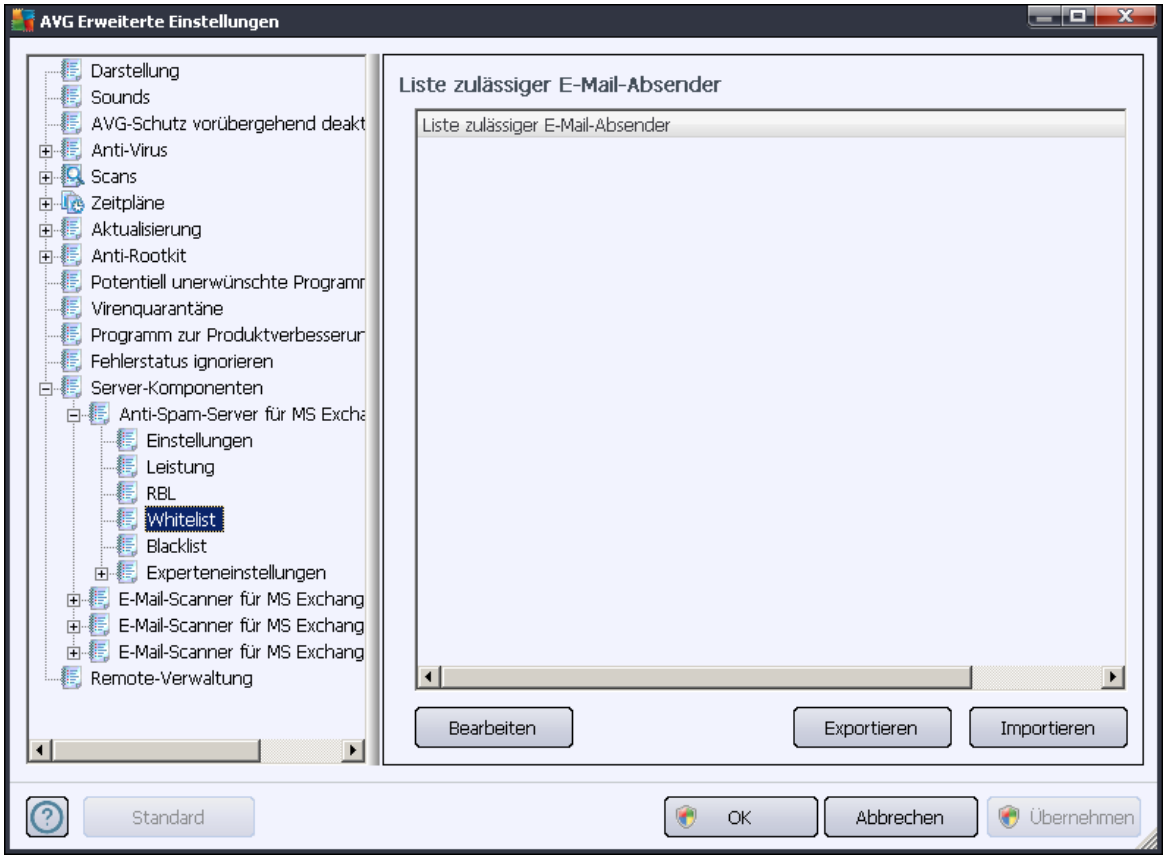
Über die ***RBL-Server-Liste*** können Sie spezielle RBL-Serverstandorte festlegen. Standardmäßig sind zwei RBL-Serveradressen festgelegt. Wir empfehlen, die Standardeinstellungen beizubehalten, sofern Sie kein erfahrener Benutzer sind und diese Einstellungen wirklich ändern müssen!

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

Es werden keine persönlichen Daten an den Server gesendet!

7.6. Whitelist

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



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

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

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

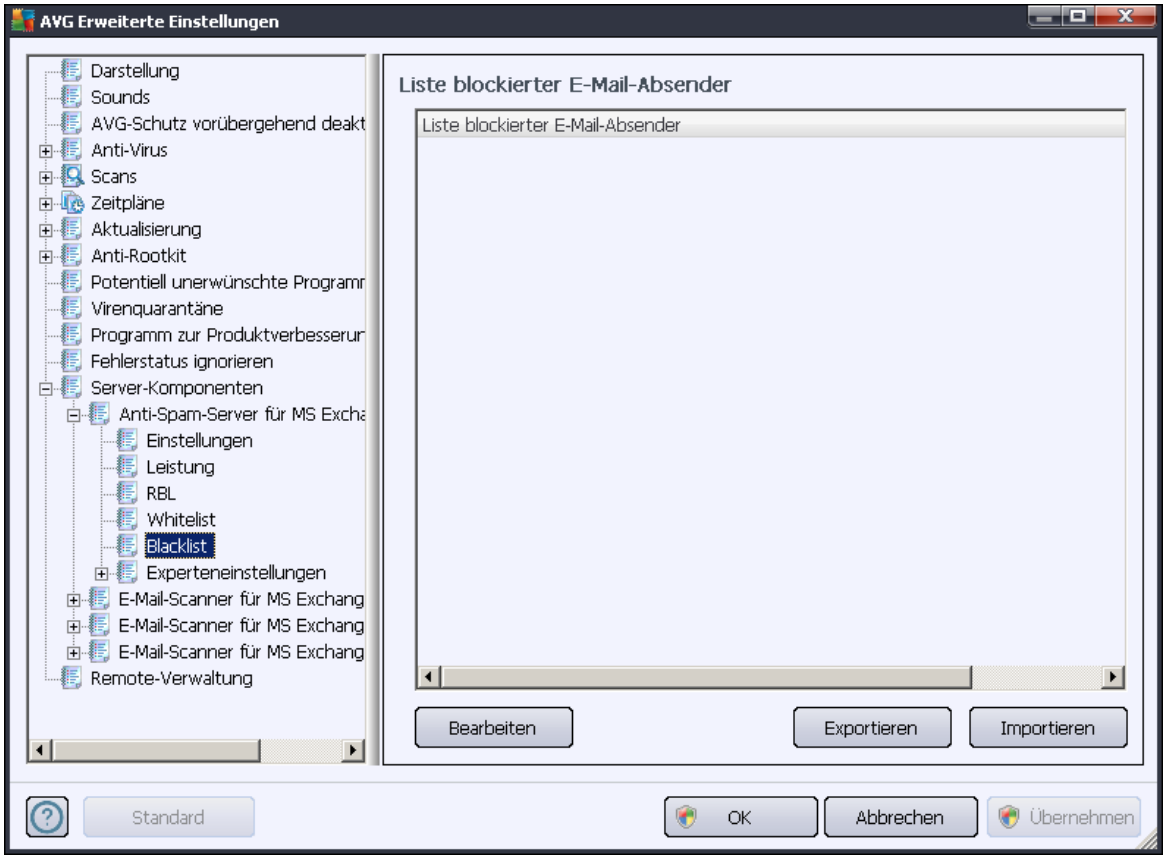
- ***Importieren*** – Durch Klicken auf diese Schaltfläche können Sie Ihre vorhandenen eMail-

Adressen importieren. Die Importdatei kann eine Textdatei (reines Textformat, pro Zeile nur ein Element – Adresse, Domainname) oder eine WAB-Datei sein, oder der Import kann aus dem Windows-Adressbuch oder Microsoft Office Outlook erfolgen.

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

7.7. Blacklist

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



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

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

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

- ***Importieren*** – Durch Klicken auf diese Schaltfläche können Sie Ihre vorhandenen eMail-Adressen importieren. Die Importdatei kann eine Textdatei (reines Textformat, pro Zeile nur ein Element – Adresse, Domainname) oder eine WAB-Datei sein, oder der Import kann aus dem Windows-Adressbuch oder Microsoft Office Outlook erfolgen.

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

7.8. Experteneinstellungen

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

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

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

- ***Training*** – maximale Worteinträge, Schwellenwert für Autotraining, Gewicht

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

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

- ***Internetverbindung*** – Timeout, Proxyserver, Proxyauthentifizierung

8. AVG Einstellungsmanager

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

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

Alle Programme/AVG 2012/AVG Einstellungsmanager

- **AVG Einstellungen**
    - ***AVG-Einstellungen bearbeiten*** – benutzen Sie diesen Link, um einen Dialog mit den erweiterten Einstellungen Ihres lokalen AVG zu öffnen. Alle hier vorgenommenen Änderungen zeigen sich auch in der lokalen Installation von AVG.
    - ***AVG-Einstellungen laden und bearbeiten*** – wenn Sie bereits eine AVG-Konfigurationsdatei (.pck) besitzen, können Sie sie durch Klicken auf diese Schaltfläche öffnen, um sie zu bearbeiten. Wenn Sie Ihre Änderungen durch Klicken auf ***OK*** oder ***Übernehmen*** bestätigen, wird die Datei durch die neuen Einstellungen ersetzt!
- **AVG Firewall-Einstellungen**

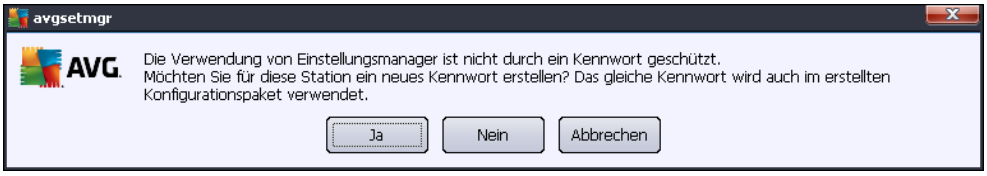
    In diesem Bereich können Sie Änderungen an den Firewall-Einstellungen Ihrer lokalen AVG-Installation vornehmen oder die Firewall-Einstellungen in einer bereits vorbereiteten AVG-Konfigurationsdatei (.pck) bearbeiten. Da Ihr AVG eMail Server Edition 2012 die Firewall-Komponente aber nicht enthält, sind beide Links ausgegraut und funktionieren nicht.

- **Optionen laden**

  - ***Gespeicherte Einstellungen in AVG laden*** – benutzen Sie diesen Link, um eine AVG-Konfigurationsdatei (.pck) zu öffnen und auf die lokale AVG-Installation anzuwenden.

- **Optionen speichern**

  - ***Lokale AVG-Einstellungen in einer Datei speichern*** – benutzen Sie diesen Link, um die AVG-Konfigurationsdatei (.pck) der lokalen AVG-Installation zu speichern. Wenn Sie kein Kennwort für die Zugelassenen Aktionen angeben, wird möglicherweise folgender Dialog angezeigt:



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

- **Optionen klonen**

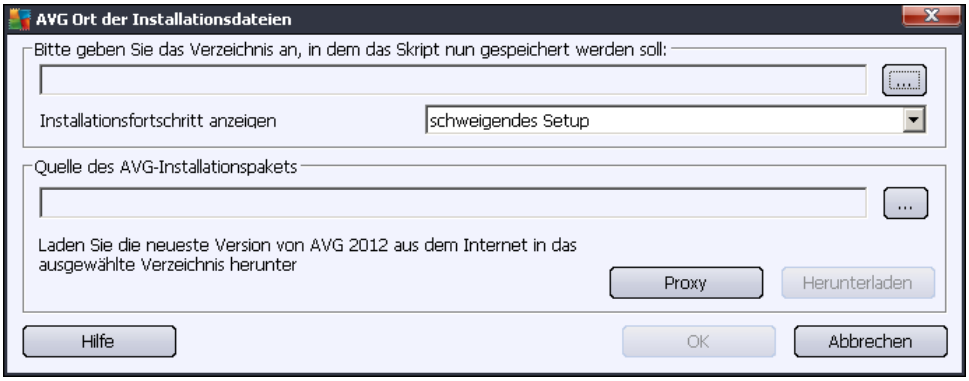
  - ***Identische Einstellungen auf gesamtes Netzwerk anwenden*** – durch Klicken auf diesen Link können Sie eine Kopie der lokalen AVG-Installation erstellen, indem Sie ein Installationspaket mit benutzerdefinierten Optionen anlegen. Die Kopie umfasst den Großteil der AVG-Einstellungen mit folgenden Ausnahmen:

    ✓ *Spracheinstellungen*

    ✓ *Soundeinstellungen*

    ✓ *Liste „Zugelassen“ und Ausnahmen der potentiell unerwünschten Programme der Komponente „Identitätsschutz“.*

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



Wählen Sie anschließend aus dem Dropdownmenü eine der folgenden Optionen:

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

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

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

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

9. FAQ und technischer Support

Wenn bei der Installation oder Verwendung von AVG betriebliche oder technische Probleme auftreten, finden Sie im Bereich ***FAQ*** der AVG-Website unter http://www.avg.com/de hilfreiche Informationen.

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