AVG eMail Server Edition 2013

Benutzerhandbuch

Dokumentversion 2013.01 (20.11.2012)

Inhalt

1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG eMail Server Edition 2013**.

Herzlichen Glückwunsch zum Kauf von AVG eMail Server Edition 2013!

AVG eMail Server Edition 2013 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 2013** 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 enthält die Beschreibung spezifischer Funktionen der E-Mail-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 2013 wurde für den Schutz von E-Mail-Servern mit den folgenden Betriebssystemen entwickelt:

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

2.2. Unterstützte eMail-Server

Folgende Mailserver 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 2013**:

- 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 2013**:

- 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 E-Mail Server installiert haben, müssen Sie diese vor der Installation von **AVG eMail Server Edition 2013** 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/en-us/download/details.aspx?id=9664

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

Service Pack für MS Exchange 2010 Server (optional):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. Installationsvorgang bei AVG

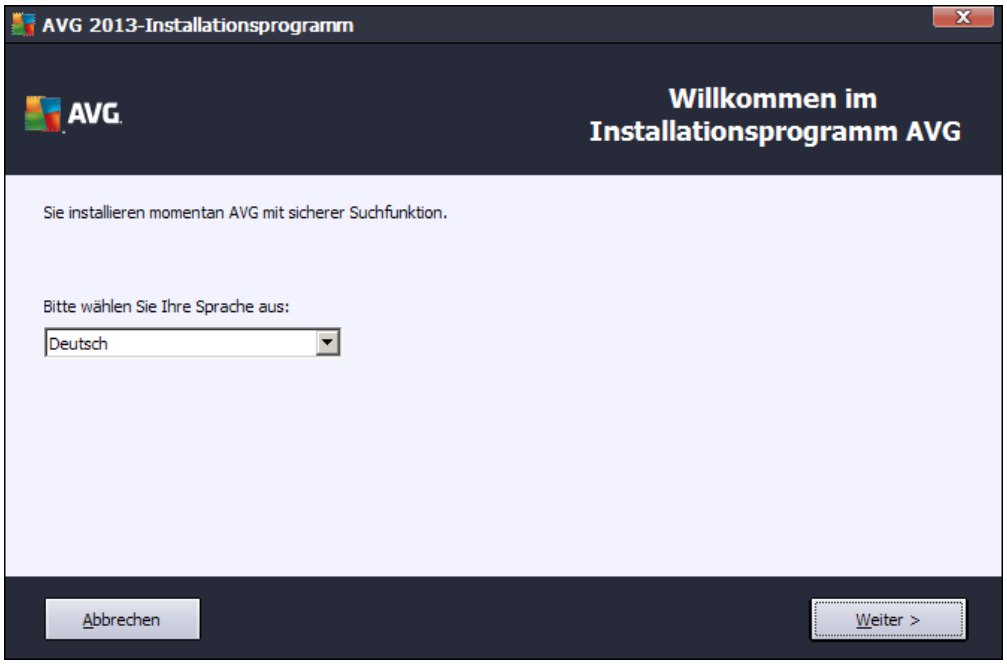
Für die Installation von AVG auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei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

Für Ihr Produkt sind zwei Installationspakete verfügbar: für 32-Bit-Betriebssysteme (gekennzeichnet mit x86) und für 64-Bit-Betriebssysteme (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 E-Mail 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:

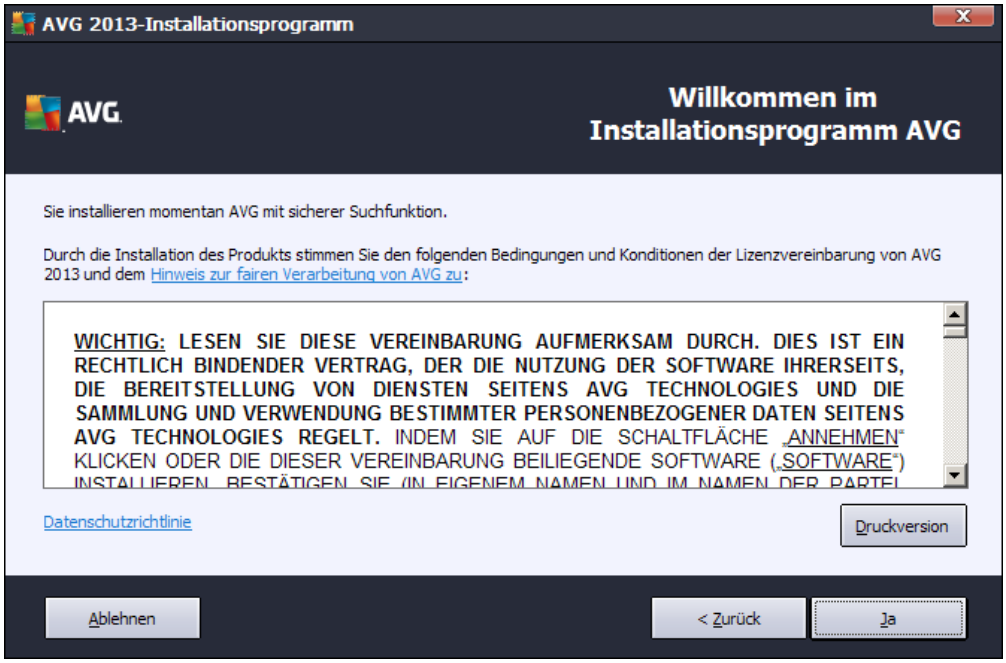
3.1. Beginn der Installation



Der Installationsvorgang beginnt mit dem Fenster ***Willkommen***. Hier wählen Sie die Sprache für die Installation. Klicken Sie anschließend auf ***Weiter***.

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

3.2. Lizenzvereinbarung

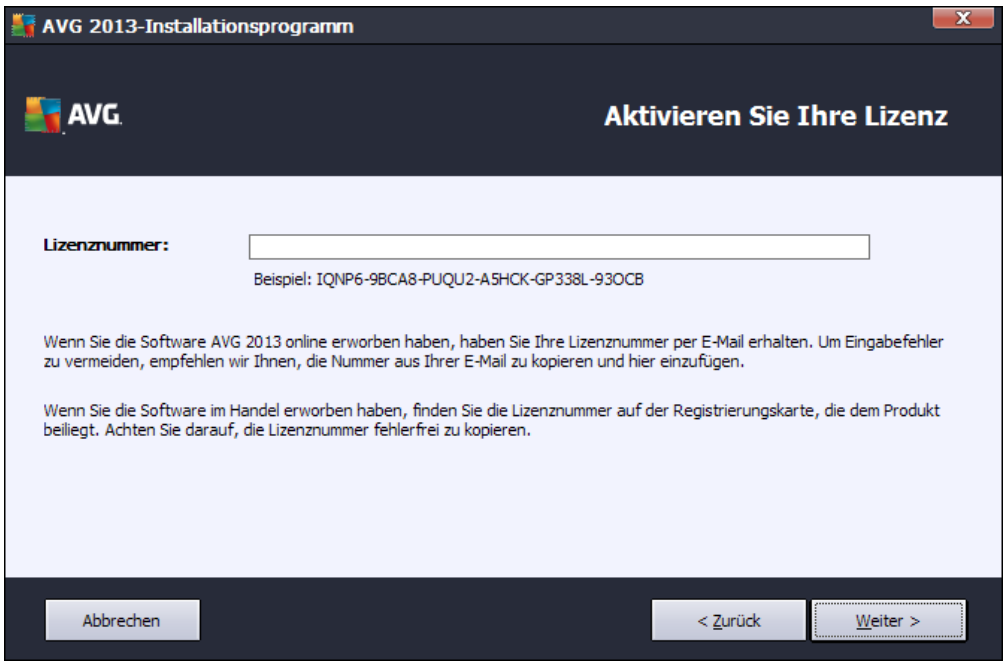


In diesem Dialog können Sie die Lizenzbedingungen anzeigen. Klicken Sie auf die Schaltfläche ***Druckversion***, um den Text der Lizenzvereinbarung in einem neuen Fenster zu öffnen. Klicken Sie anschließend auf die Schaltfläche ***Akzeptieren***, um mit dem nächsten Dialog fortzufahren.

3.3. Aktivieren Sie Ihre Lizenz

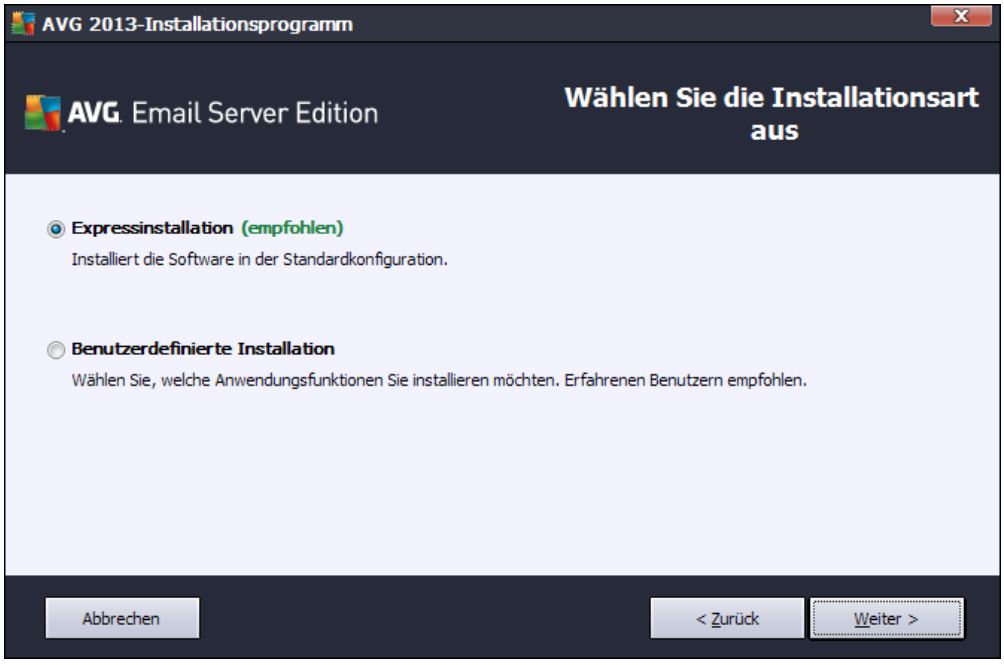
Im Dialog ***AVG-Lizenz aktivieren*** müssen Sie Ihre Lizenznummer eingeben.

Geben Sie Ihre Lizenznummer in das Textfeld ***Lizenznummer*** ein. Die Lizenznummer ist in der Bestätigungs-E-Mail 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 E-Mail), wird empfohlen, sie zu kopieren und einzufügen.



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

3.4. Bitte wählen Sie den Installationstyp



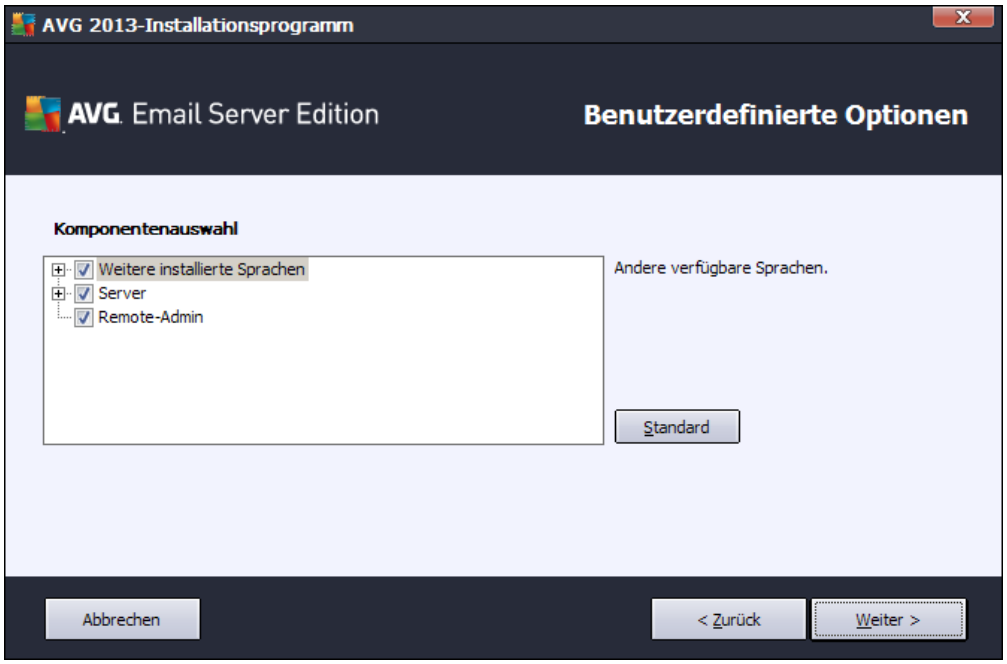
Im Dialog ***Wählen Sie die Installationsart aus*** stehen zwei Installationsoptionen zur Verfügung: ***Expressinstallation*** und ***Benutzerdefinierte Installation***.

Den meisten Benutzern wird empfohlen, die ***Expressinstallation*** 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.

Wenn Sie die benutzerdefinierte Installation wählen, wird der Bereich ***Zielverzeichnis*** im unteren Teil des Dialogs geöffnet. Hier können Sie den Speicherort angeben, unter dem AVG installiert werden soll. 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.

3.5. Benutzerdefinierte Installation – Benutzerdefinierte Optionen



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!

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

- ***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 gewünschten Sprachen aus dem Menü.

Grundlegender Überblick über die einzelnen Serverkomponenten (unter dem Zweig ***Server***):

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

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

- ***E-Mail-Scanner für MS Exchange (Routing-Transport Agent)***

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

- ***E-Mail-Scanner für MS Exchange (SMTP-Transport Agent)***

  Prüft alle E-Mail-Nachrichten, die über die MS Exchange-SMTP-Oberfläche laufen (kann sowohl für die EDGE- als auch für die HUB-Rolle installiert werden).

- ***E-Mail-Scanner für MS Exchange (VSAPI)***

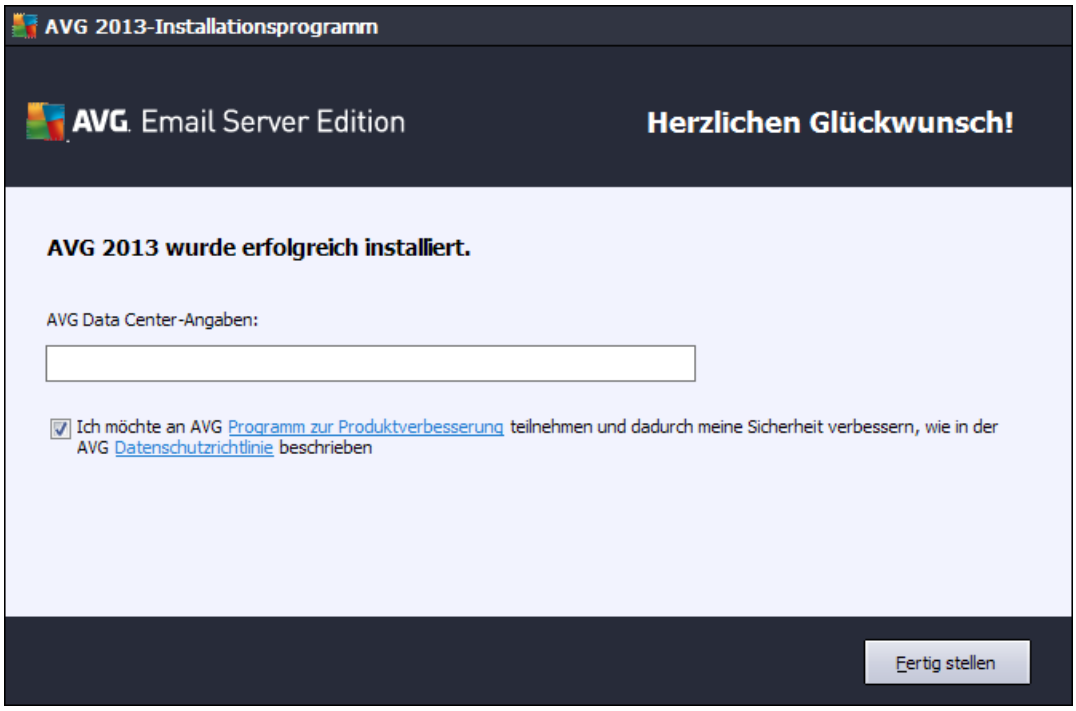
  Überprüft alle E-Mail-Nachrichten, die in den Postfächern der Benutzer gespeichert sind. Erkannte Viren werden in die Virenquarantäne verschoben oder vollständig entfernt.

Für Benutzer von Exchange 2003 stehen nur die Komponenten Anti-Spam und E-Mail-Scanner (VSAPI) zur Verfügung.

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

3.6. Abschluss der Installation

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



In diesem Dialog können Sie außerdem festlegen, ob Sie am Programm zur Produktverbesserung teilnehmen möchten. Dabei sammeln wir anonyme Informationen zu erkannten Bedrohungen, um die Internetsicherheit insgesamt zu verbessern. Wenn Sie dieser Aussage zustimmen, lassen Sie die Option ***Ich möchte an AVG Programm zur Produktverbesserung teilnehmen und dadurch meine Sicherheit verbessern, wie in der AVG Datenschutzrichtlinie beschrieben*** aktiviert. *(Diese Option ist standardmäßig aktiviert.)*

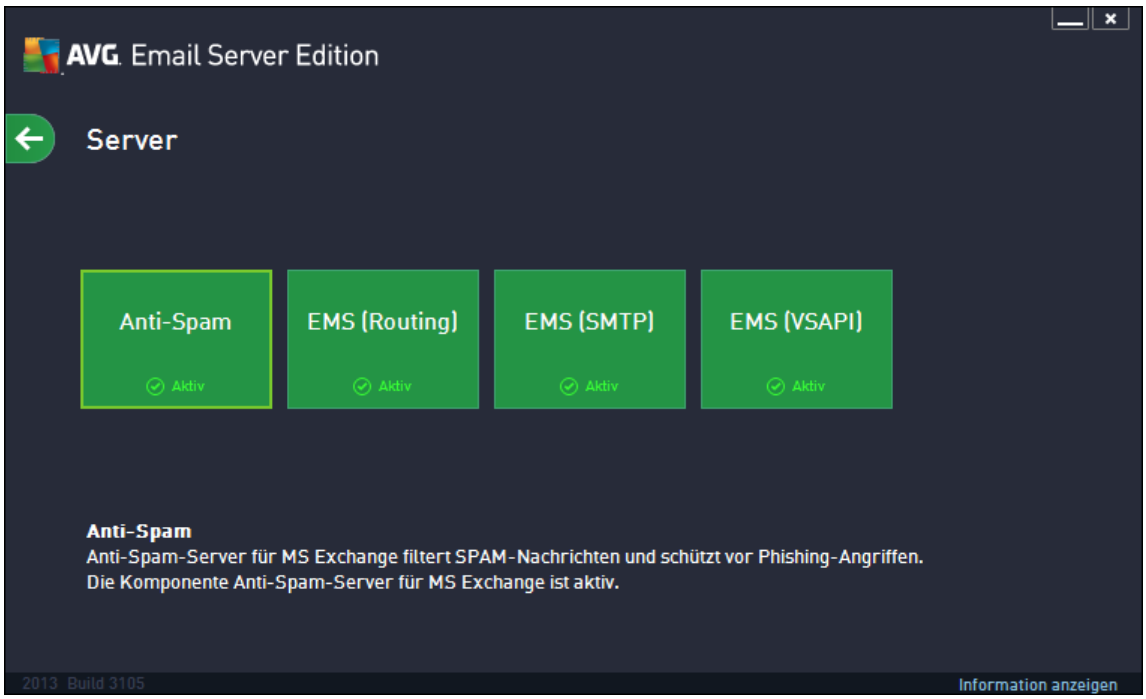
Klicken Sie zur Bestätigung auf die Schaltfläche **Fertig stellen**.

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

4. Nach der Installation

Unmittelbar nach der Installation wird die Hauptseite von ***AVG eMail Server Edition 2013*** angezeigt:

In diesem Handbuch werden nur die speziellen Funktionen von ***AVG eMail Server Edition 2013*** beschrieben. Informationen zu allen anderen Komponenten und Funktionen finden Sie im Handbuch zu AVG Desktop. Um den Dialog zu den Hauptserverkomponenten zu öffnen, klicken Sie auf ***Server***. Folgender Dialog wird angezeigt:



Bitte beachten Sie, dass nur dann alle Serverkomponenten verfügbar sind (es sei denn, Sie haben bei der Installation einige Komponenten ausgeschlossen), wenn Sie MS Exchange 2007 oder höher verwenden. MS Exchange 2003 unterstützt lediglich Anti-Spam und E-Mail-Scanner (VSAPI).

Spezifische Informationen zum Einrichten des Schutzes für Ihren Mailserver finden Sie im jeweils relevanten Kapitel:

- ***E-Mail-Scanner für MS Exchange***
- ***Anti-Spam-Server für MS Exchange***
- ***AVG für Kerio MailServer***

5. eMail-Scanner für MS Exchange

5.1. Überblick

Grundlegende Übersicht über die einzelnen E-Mail-Scanner-Serverkomponenten:

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

  Prüft alle eingehenden, ausgehenden und internen E-Mail-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) – E-Mail-Scanner für MS Exchange (SMTP-Transport-Agent)***

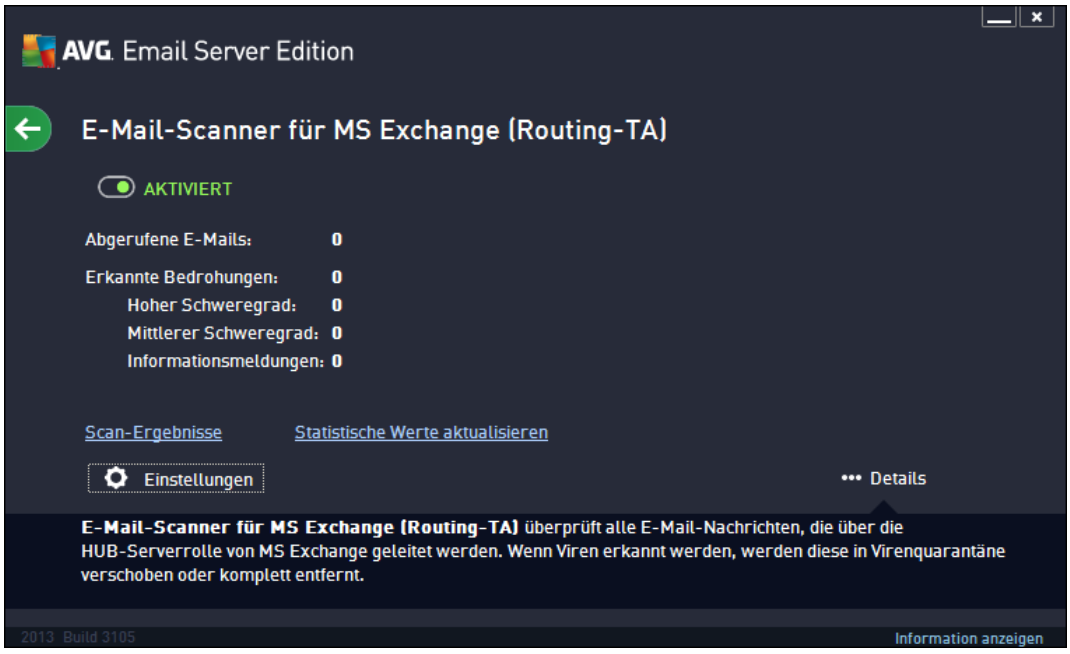
  Prüft alle E-Mail-Nachrichten, die über die SMTP-Schnittstelle von MS Exchange eingehen.

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

- ***EMS (VSAPI) – E-Mail-Scanner für MS Exchange (VSAPI)***

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

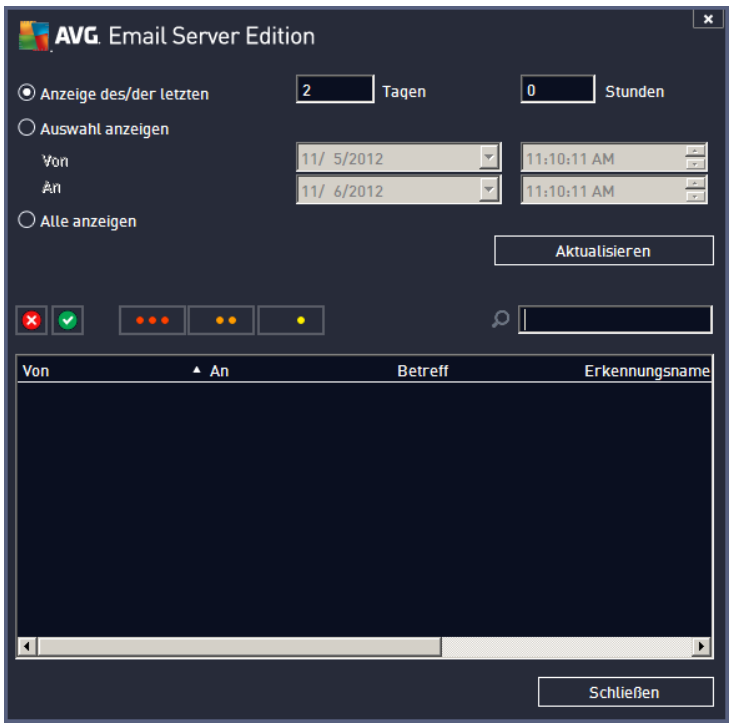
Klicken Sie auf das Symbol der gewünschten Komponente, um die Benutzeroberfläche zu öffnen. Die folgenden Schaltflächen und Links stehen in allen Komponenten zur Verfügung:



- ***AKTIVIERT/DEAKTIVIERT***: Durch Klicken auf diese Schaltfläche aktivieren oder deaktivieren Sie die ausgewählte Komponente. Wenn sie aktiviert ist, sind die Schaltfläche und der Text grün, andernfalls rot.

- ***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:

  - ***Anzeige des/der letzten*** – 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.

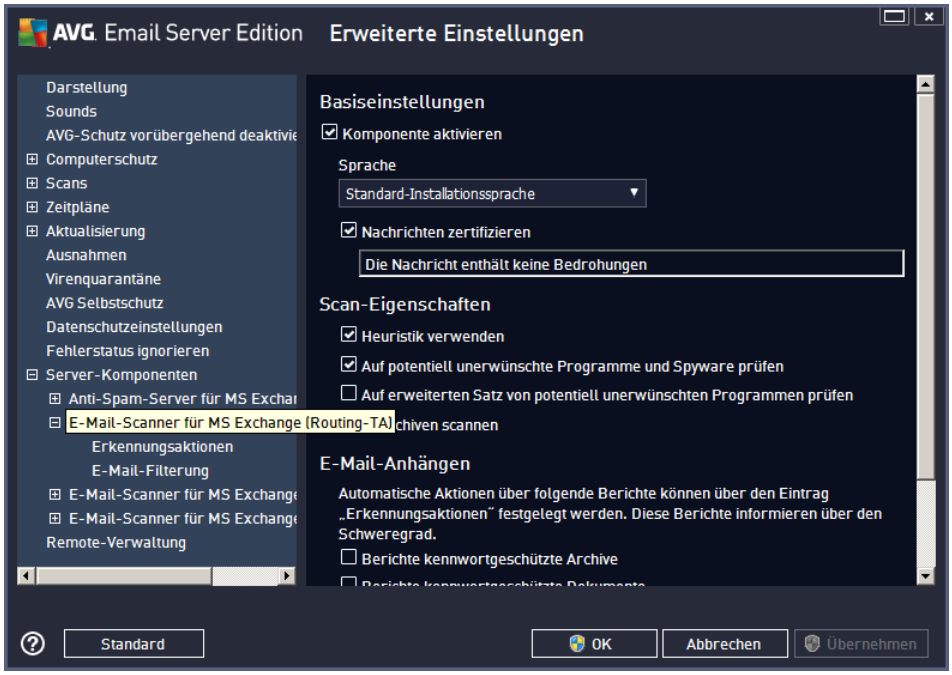
- ***Statistische Werte aktualisieren***: Aktualisiert die oben angezeigten Statistiken.

Durch Klicken auf die Schaltfläche ***Einstellungen*** öffnen Sie erweiterte Einstellungen für die ausgewählte Komponente. (Weitere Informationen zu den einzelnen Einstellungen für alle Komponenten finden Sie in den nachfolgenden Kapiteln.)

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

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

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



Der Abschnitt ***Basiseinstellungen*** 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 ***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 ***E-Mail-Anhängen*** können Sie wählen, über welche Elemente Sie während des Scans informiert werden möchten. Ist diese Option aktiviert, erhalten alle E-Mails 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:

- ***Berichte kennwortgeschützte Archive***
- ***Berichte kennwortgeschützte Dokumente***
- ***Berichte Dateien, die Makros enthalten***
- ***Berichte versteckte Erweiterungen***

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***E-Mail-Filterung***

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

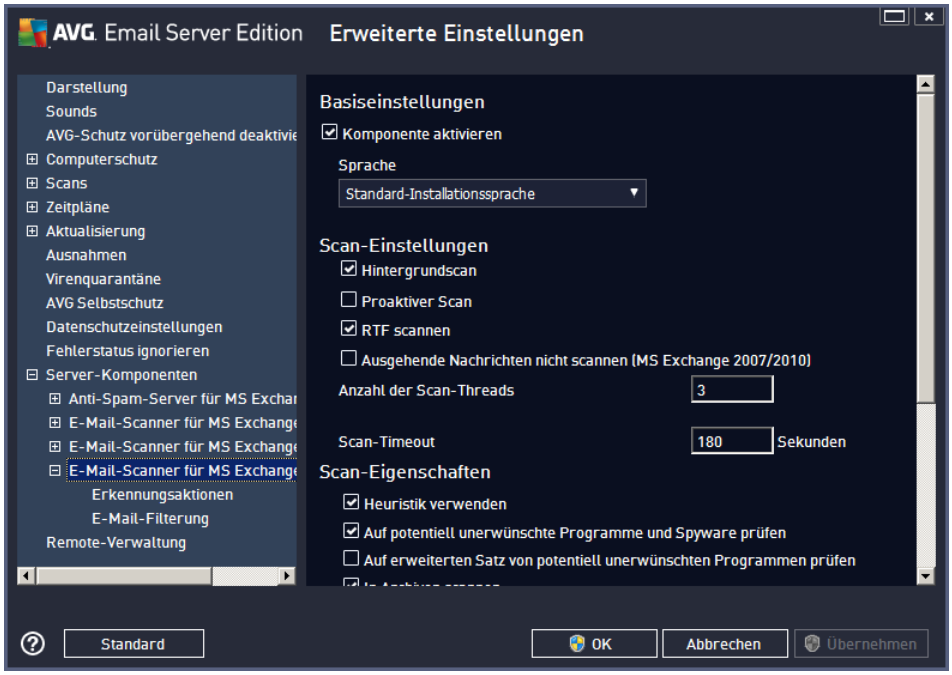
Die Konfiguration für den ***E-Mail-Scanner für MS Exchange (SMTP-Transport Agent)*** ist exakt die gleiche wie für den Routing-Transport-Agent. Weitere Informationen finden Sie im Kapitel ***E-Mail-Scanner für MS Exchange (Routing-TA)*** weiter oben.

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***E-Mail-Filterung***

5.4. eMail-Scanner für MS Exchange (VSAPI)

Dieser Eintrag enthält Einstellungen für den ***E-Mail-Scanner für MS Exchange (VSAPI)***.



Der Abschnitt ***Basiseinstellungen*** 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 ***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 E-Mail-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.

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

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.

- ***RTF scannen*** – 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 E-Mails möglicherweise zweimal gescannt. Der erste Scan wird vom On-Access-Scanner von VSAPI ausgeführt und der zweite vom Routing-Transport-Agent. Dies kann zu Leistungsbeeinträchtigungen der Server und Verzögerungen beim Senden von E-Mails führen. Wenn Sie sicher sind, dass beide Server-Komponenten installiert und aktiviert sind, können Sie den doppelten Scan ausgehender E-Mails verhindern, indem Sie dieses Kontrollkästchen aktivieren und den On-Access-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.
- ***Auf potentiell unerwünschte Programme und Spyware prüfen*** – Aktivieren Sie diese Option, wenn potentiell unerwünschte Programme und Spyware gemeldet werden sollen.
- ***Auf erweiterten Satz von potentiell unerwünschten Programmen prüfen*** – 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 ***E-Mail-Anhängen*** können Sie wählen, über welche Elemente Sie während des Scans informiert werden möchten. Die Standardeinstellungen können einfach im ***Abschnitt Erkennungsaktionen***, Unterabschnitt ***Informationen*** angepasst werden (siehe unten).

Folgende Optionen sind verfügbar:

- ***Berichte kennwortgeschützte Archive***
- ***Berichte kennwortgeschützte Dokumente***
- ***Berichte Dateien, die Makros enthalten***
- ***Berichte versteckte Erweiterungen***

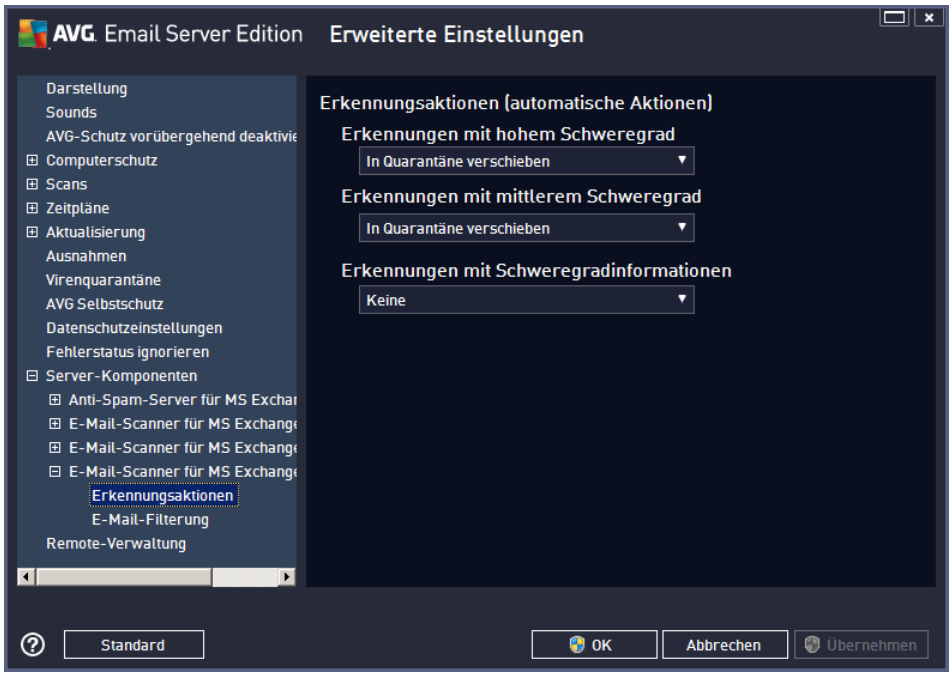
Einige dieser Funktionen sind benutzerspezifische Erweiterungen der Dienste der Microsoft VSAPI 2.0/2.5-Benutzerschnittstelle. Ausführliche Informationen über die VSAPI 2.0/2.5 finden Sie unter folgenden Adressen und über die dortigen Links:

- 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 – Informationen zu zusätzlichen Funktionen von VSAPI 2.5 in Exchange 2003 Server.

In der folgenden Baumstruktur sind auch die folgenden Untereinträge verfügbar:

- ***Erkennungsaktionen***
- ***E-Mail-Filterung***

5.5. Erkennungsaktionen



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

Die Aktionen sind für die folgenden Einträge verfügbar:

- ***Erkennungen mit hohem Schweregrad*** – Bösartige Codes, die sich selbst kopieren und verbreiten. Sie werden oft erst bemerkt, wenn sie bereits Schaden angerichtet haben.
- ***Erkennungen mit mittlerem Schweregrad*** – Diese Programme variieren im Allgemeinen von tatsächlich ernsthaft bedrohlich bis nur potentiell bedrohlich für Ihre Privatsphäre.
- ***Information*** – Enthält alle erkannten potentiellen Bedrohungen, die keiner der oben genannten Kategorie zugeteilt werden können.

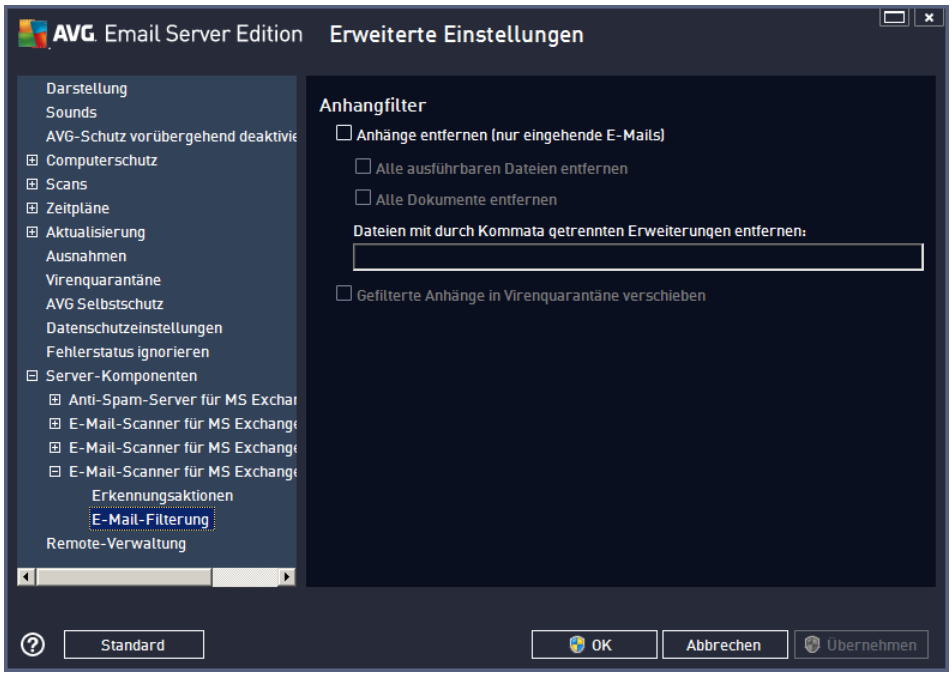
Wählen Sie im Dropdown-Menü für jeden Eintrag eine Aktion aus:

- ***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.

Die letztgenannte Funktion steht nicht für E-Mail-Scanner für MS Exchange VSAPI zur Verfügung.

5.6. E-Mail-Filterung



Im Untereintrag ***E-Mail-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 2013** Hauptoberfläche auf die Virenquarantäne zugreifen. Klicken Sie einfach mit der linken Maustaste auf das Element ***Optionen*** und wählen Sie im Kontextmenü die Option ***Virenquarantäne***.

6. Anti-Spam-Server für MS Exchange

6.1. Grundlagen zu Anti-Spam

Unter Spam versteht man unerwünschte E-Mails, die meist für ein Produkt oder eine Dienstleistung werben. Sie werden mittels Massenversand an eine riesige Anzahl von E-Mail-Adressen verschickt und füllen so die Mailboxen der Empfänger. Legitime Werbemails, für die der Verbraucher sein Einverständnis gegeben hat, fallen nicht in diese Kategorie. Spam ist nicht nur störend, sondern auch oft eine Quelle für Betrugsversuche, Viren und anstößige Inhalte.

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

6.2. Benutzeroberfläche von Anti-Spam

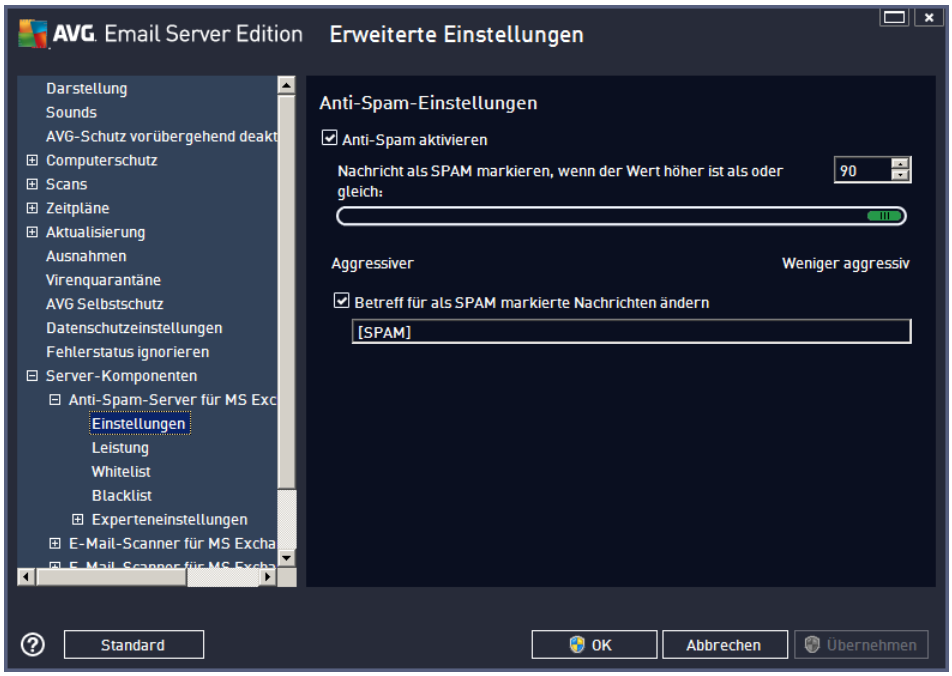
In diesem Dialog werden in Kurzform Informationen zur Funktion der Serverkomponente, zu ihrem aktuellen Status (*aktiviert/deaktiviert*) sowie einige statistische Werte angezeigt.

Verfügbare Schaltflächen und Links:

- ***AKTIVIERT/DEAKTIVIERT***: Durch Klicken auf diese Schaltfläche aktivieren oder deaktivieren Sie die ausgewählte Komponente. Wenn sie aktiviert ist, sind die Schaltfläche und der Text grün, andernfalls rot.
- ***Statistische Werte aktualisieren***: Aktualisiert die oben angezeigten Statistiken.
- ***Einstellungen***: Über diese Schaltfläche öffnen Sie erweiterte Anti-Spam-Einstellungen.

6.3. Anti-Spam-Einstellungen

6.3.1. Einstellungen



In diesem Dialog können Sie über das Kontrollkästchen ***Anti-Spam aktivieren*** festlegen, ob Sie die Prüfung Ihrer E-Mail-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 E-Mails werden normal in den Posteingang geleitet (ohne als Spam gekennzeichnet zu werden). Die am leichtesten als Spam identifizierbaren E-Mails werden ausgefiltert, aber es kann immer noch ein großer Anteil an Spam auf Ihren Computer gelangen.

- ***Wert 80–89*** – E-Mail-Nachrichten, die mit einiger Wahrscheinlichkeit Spam sind, werden ausgefiltert. Auch einige nicht als Spam zu klassifizierende Nachrichten werden eventuell fälschlicherweise ausgefiltert.

- ***Wert 60–79*** – Als relativ aggressive Konfiguration einzuordnen. E-Mails, bei denen es sich möglicherweise um Spam handelt, werden ausgefiltert, aber auch E-Mails, die keine Spam-Nachrichten sind, können als solche eingestuft werden.

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

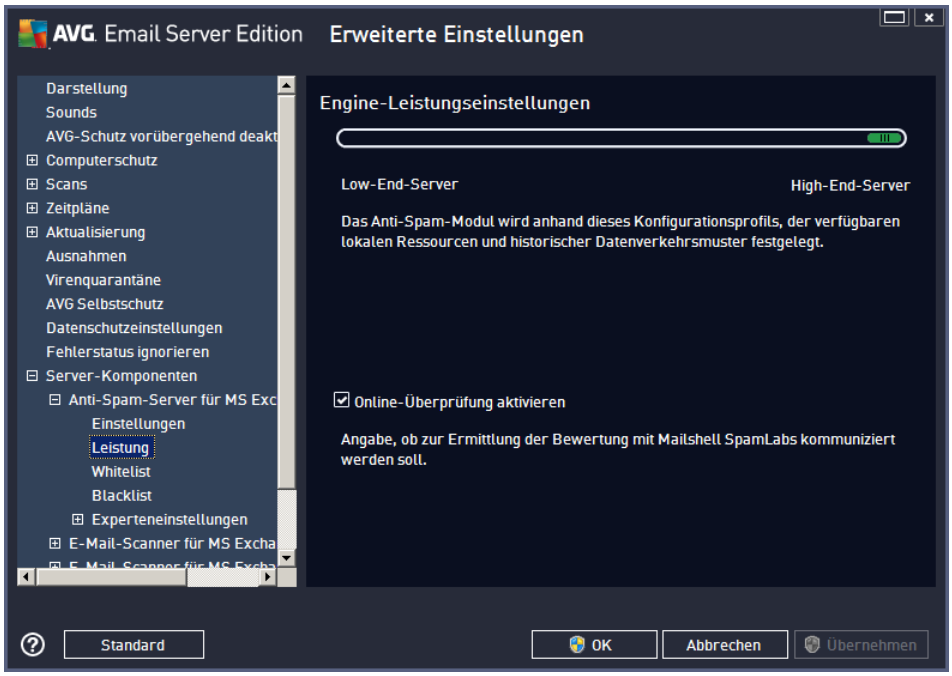
Gebrauch nicht empfohlen.

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.

6.3.2. Leistung



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

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

- ***Hohe Leistung*** – Für diesen Modus ist sehr viel Speicher erforderlich. Während des Scanvorgangs werden zur Identifizierung von Spam folgende Funktionen verwendet:

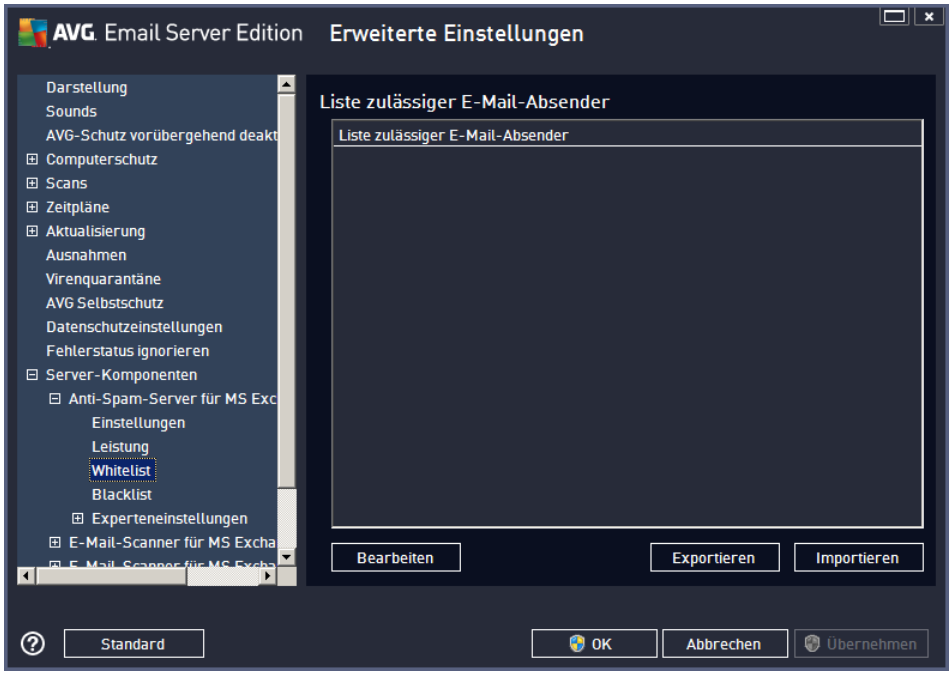
Regeln und Spam-Datenbank-Cache, einfache und erweiterte Regeln, IP-Adressen von Spammern und Spammer-Datenbanken.

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

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

6.3.3. Whitelist

Wenn Sie den Eintrag ***Whitelist*** wählen, wird ein Dialog mit einer allgemeinen Liste genehmigter E-Mail-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:

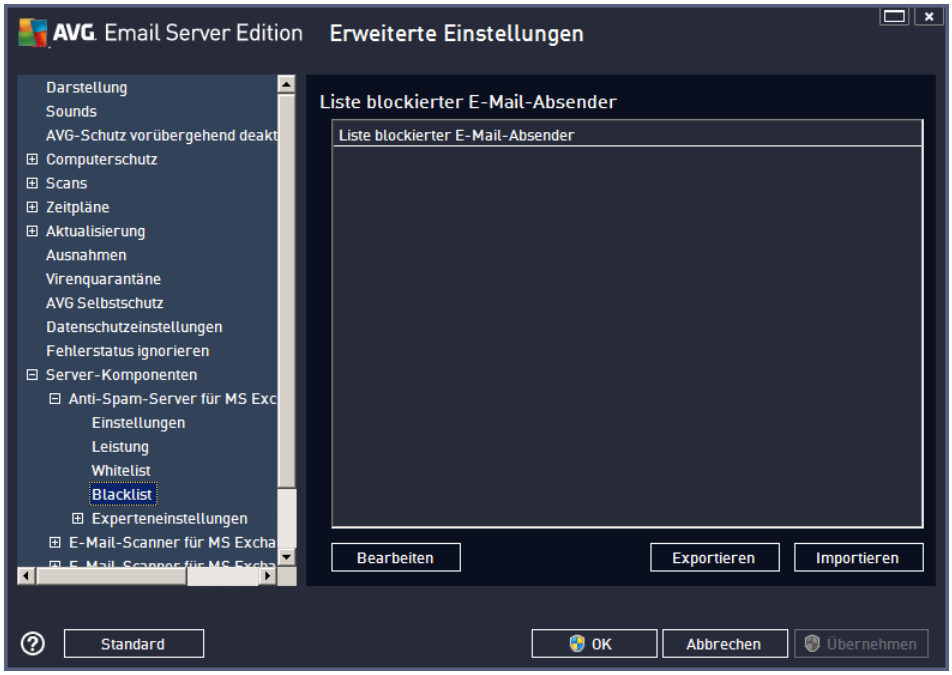
- ***Bearbeiten*** – Klicken Sie auf diese Schaltfläche, um einen Dialog zu öffnen, in dem Sie manuell eine Liste von Adressen eingeben können (Sie können die Adressen auch mittels *Kopieren und Einfügen* eingeben). Tragen Sie jeweils ein Element (Absender, Domainname) pro Zeile ein.

- ***Importieren*** – Durch Klicken auf diese Schaltfläche können Sie Ihre vorhandenen E-Mail-Adressen importieren. Die Eingabedatei 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 aus Microsoft Office Outlook erfolgen.

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

6.3.4. Blacklist

Wenn Sie den Eintrag ***Blacklist*** wählen, wird ein Dialog mit einer allgemeinen Liste blockierter E-Mail-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 E-Mail-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 E-Mail-Adressen importieren. Die Eingabedatei 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 aus Microsoft Office Outlook erfolgen.

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

6.3.5. Experteneinstellungen

Dieser Bereich enthält eine große Auswahl an Einstellungen für die Anti-Spam-Komponente. Diese Einstellungen sind ausschließlich für erfahrene Benutzer vorgesehen; normalerweise sind dies Netzwerkadministratoren, die die Anti-Spam-Funktionen sehr präzise festlegen müssen, um den optimalen Schutz für die Mailserver zu erzielen. Daher steht für die einzelnen Dialoge keine weitere Hilfe zur Verfügung. Auf der Benutzeroberfläche finden Sie jedoch eine kurze Beschreibung der jeweiligen Option.

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

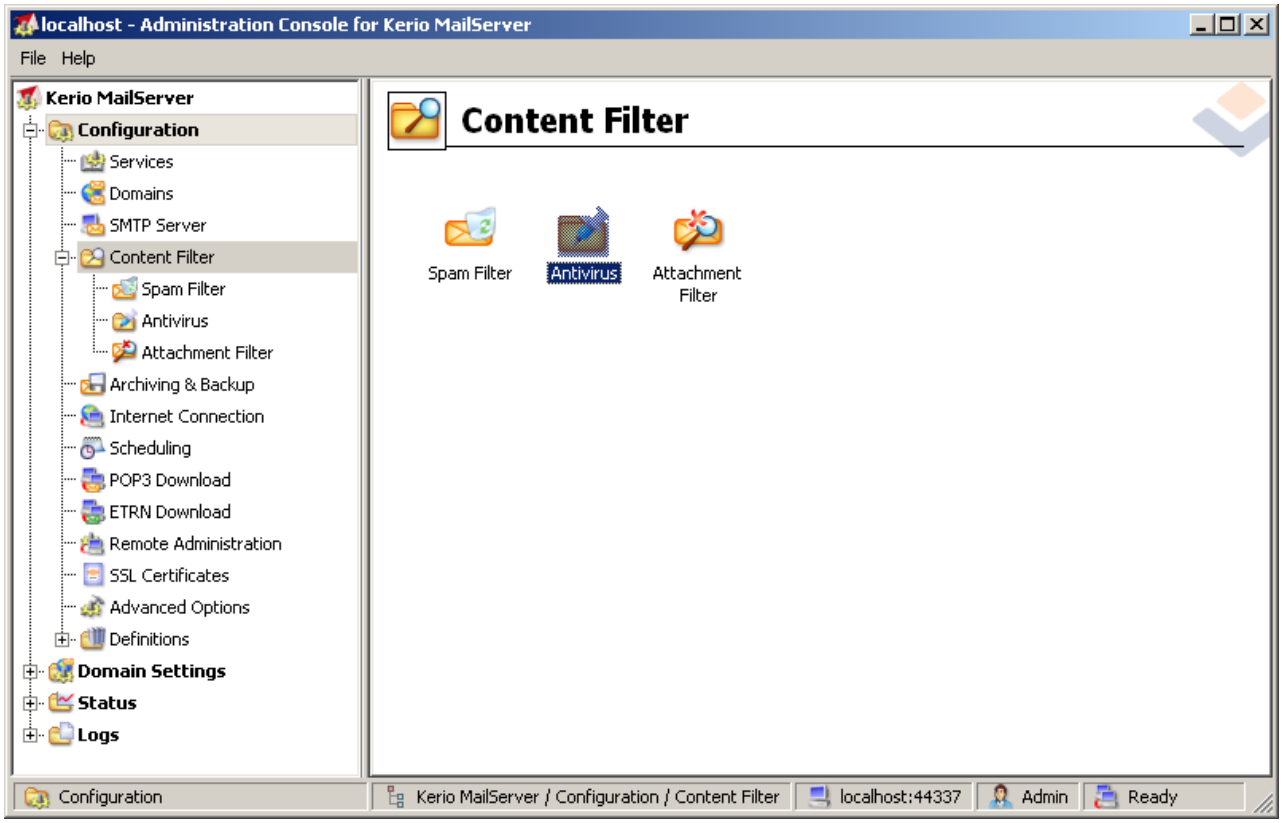
Wenn Sie dennoch der Meinung sind, dass Sie die Konfiguration von Anti-Spam im Detail ändern müssen, folgen Sie den Anweisungen direkt auf der Benutzeroberfläche. Im Allgemeinen finden Sie in jedem Dialog eine bestimmte Funktion, die Sie bearbeiten können, sowie die zugehörige Beschreibung:

- ***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

7. AVG für Kerio MailServer

7.1. Konfiguration

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

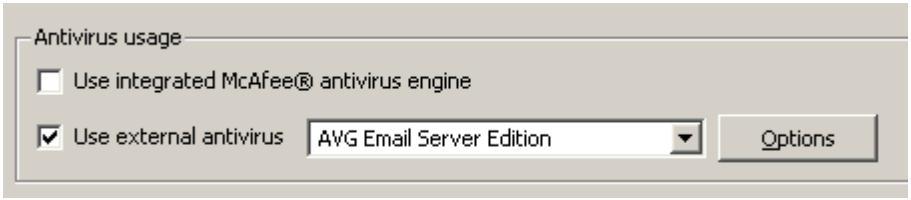


Wenn Sie auf den Eintrag „Inhaltsfilter“ klicken, wird ein Dialog mit drei Einträgen angezeigt:

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

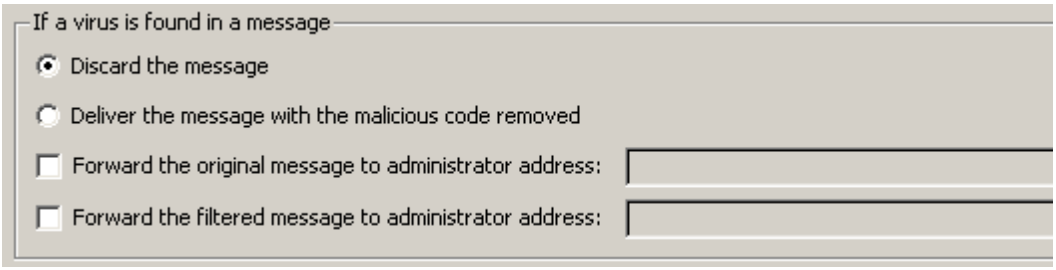
7.1.1. Anti-Virus

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 E-Mail Server Edition“ aus:



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

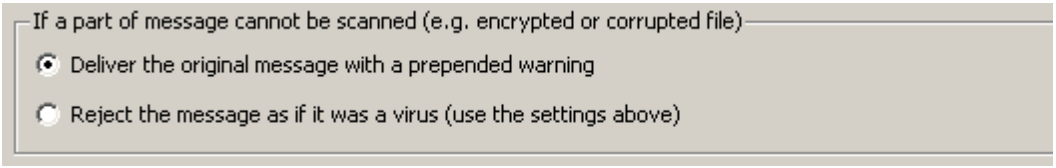
- ***In einer E-Mail wird ein Virus entdeckt***



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:

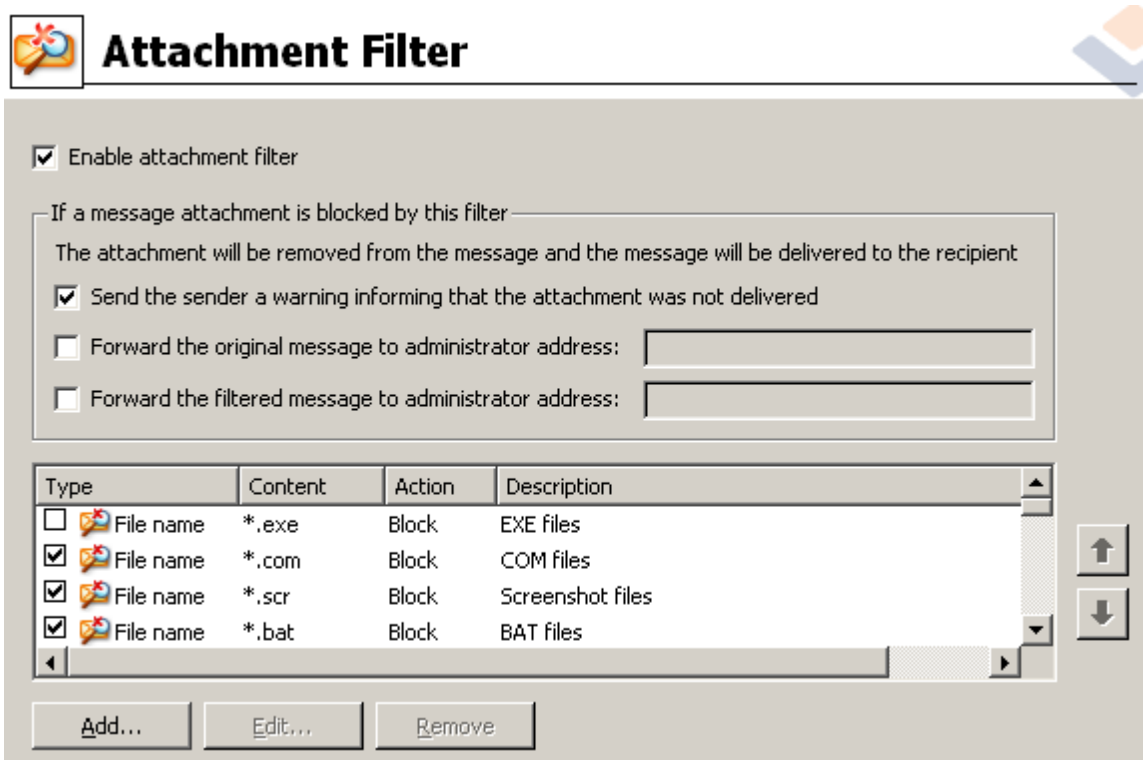
  - ***Senden der ursprünglichen Nachricht mit einer vorbereiteten Warnung*** – Die Nachricht (oder der Anhang) wird ungeprüft übermittelt. Der Benutzer wird gewarnt, dass die Nachricht

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.

7.1.2. 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 E-Mail-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 E-Mail-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 die unten ausgewählten

Aktionen) an die angegebene E-Mail-Adresse weitergeleitet. Mit dieser Option kann überprüft werden, ob AVG AntiVirus 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 E-Mail 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.

8. 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 E-Mail an den technischen Support. Verwenden Sie bitte das Kontaktformular, das im Systemmenü unter ***Hilfe / Onlinehilfe*** zur Verfügung steht.