

AVG 7.5 eMail Server Edition

Benutzerhandbuch

Dokumentversion 75.3 (31.10.2006)

Copyright GRISOFT, s.r.o. Alle Rechte vorbehalten.

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

In diesem Produkt wird Code aus der Bibliothek C-SaCzech verwendet, Copyright (c) 1996–2001 Jaromír Dolecek <dolecek@ics.muni.cz>

In diesem Produkt wird die Kompressionsbibliothek zlib verwendet, Copyright (c) 1995–2002 Jean-loup Gailly and Mark Adler.

In diesem Produkt wird die Kompressionsbibliothek libzip2 verwendet, Copyright (c) 1996–2002 Julian R. Seward.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Besitzer.

Inhalt

| | |
|---|-----------|
| 1. Einführung | 3 |
| 1.1. Erkennungstechnologien für Anti-Virus und Anti-Spyware | 3 |
| 1.2. Unterstützte Betriebssysteme | 3 |
| 1.3. Unterstützte Versionen von eMail-Servern | 3 |
| 1.4. Gründe für die Installation von AVG 7.5 eMail Server..... | 4 |
| 2. Installationsschritte | 5 |
| 2.1. Lizenznummer | 5 |
| 2.2. Aktuelle Installationsdateien | 5 |
| 2.3. Installation von CD..... | 5 |
| 2.4. Installation über das Internet..... | 6 |
| 3. AVG für Exchange 5.x Server | 7 |
| 3.1. Installationsvorgang | 7 |
| 3.2. Programmstart | 8 |
| 4. AVG für Exchange 2000/2003 Server | 14 |
| 4.1. Installationsvorgang | 14 |
| 4.2. Programmwartung | 15 |
| 4.3. Überwachung von AVG für Exchange 2000/2003 Server..... | 18 |
| 5. AVG für Lotus Notes/Domino Server | 21 |
| 5.1. Installationsvorgang | 21 |
| 5.2. Programmwartung | 22 |
| 5.3. AVG Virenquarantäne | 26 |
| 5.4. AVG Protokolldatei | 28 |
| 6. AVG für Kerio MailServer | 29 |
| 6.1. Antivirus | 29 |
| 6.2. Filter für Anhänge | 30 |
| 7. Programmaktualisierung | 32 |
| 7.1. Aktualisierungsstufen..... | 32 |
| 7.2. Aktualisierungsarten..... | 33 |
| 7.3. Aktualisierungs-Zeitplan..... | 33 |
| 8. FAQ und technischer Support | 35 |
| 8.1. Dienstprogramm AVG Diagnose..... | 35 |

1. Einführung

Der Schutz vor Computerviren ist heute weltweit eine der wichtigsten Herausforderungen für die Computersicherheit.

In diesem Benutzerhandbuch werden die Installation, Konfiguration und Wartung der Produkte von AVG 7.5 eMail Server beschrieben.

AVG 7.5 eMail Server bietet viele Tools für einen automatischen und zuverlässigen Schutz gegen Viren aller Art, die eine Bedrohung für Ihren eMail-Server darstellen. Die Kernfunktion ist sowohl das Überprüfen eingehender und ausgehender Nachrichten auf dem Server als auch das Überprüfen der internen Ordnerstrukturen oder Datenbanken des Servers (mit Hilfe der integrierten Edition von AVG7.5 File Server).

1.1. Erkennungstechnologien für Anti-Virus und Anti-Spyware

AVG 7.5 eMail Server enthält AVG 7.5 File Server und erkennt über dessen Überprüfungs- und Schutztechnologien Computerviren und Malware. Beide Produkte sollten auf dem E-Mail-Server installiert werden, so dass AVG 7.5 eMail Server die Funktionen der Komponenten von AVG 7.5 File Server nutzen kann.

Dadurch ist der als eMail-Server verwendete Computer vollständig gegen Viren und Malware geschützt. Weitere Informationen zu den Schutzfunktionen von AVG 7.5 File Server finden Sie im Benutzerhandbuch für AVG 7.5 File Server, das auf der Grisoft-Website unter www.grisoft.com im Download-Bereich verfügbar ist.

1.2. Unterstützte Betriebssysteme

AVG 7.5 eMail Server wurde zum Schutz von eMail-Servern konzipiert, die unter folgenden Betriebssystemen ausgeführt werden:

- Windows 2003 Server
- Windows 2000 Server
- Windows NT 4.0 Server
- Windows 9x/Me/2000/XP, Workstation Edition (Lotus Notes/Domino und Kerio-Server)

(einschließlich der 64-Bit-Windows-Versionen)

AVG 7.5 File Server muss auf dem Computer installiert sein, damit bei Verwendung des Virenschanners von AVG ein Schutz der eMails gegen Viren und Spyware gewährleistet ist!

1.3. Unterstützte Versionen von eMail-Servern

- **AVG für Exchange 5.x Server** – Exchange 5.x Server-Versionen
- **AVG für Exchange 2000/2003 Server** – Exchange 2000/2003 Server-Versionen; für Exchange 2000 Server muss zuerst das Service Pack 1 (oder höher) installiert werden, bevor das AVG-Modul verwendet werden kann; AVG 7.5 File Server verwendet die Oberfläche von VSAPI 2.0 (oder 2.5 mit Exchange 2003 Server), die in diesem Service Pack enthalten ist.
- **AVG für Lotus Notes/Domino Server** – Version 4.6 und höher

- **AVG für Kerio MailServer** – Version 5.0.0 und höher (alle Versionen verfügbar)

1.4. Gründe für die Installation von AVG 7.5 eMail Server

AVG 7.5 eMail Server durchsucht das System zuverlässig und umfassend nach Viren in verarbeiteten eMails und den Ordnerstrukturen des internen Postfachs des Servers. AVG 7.5 eMail Server verfügt über die folgenden Hauptfunktionen:

- Zuverlässige Prüfung eingehender eMails und der Postfachordner auf dem Server
- Einfache Konfiguration (durch Verwendung der grafischen Benutzeroberflächen einzelner Server oder der eigenständigen AVG-Anwendung)

2. Installationsschritte

2.1. Lizenznummer

Halten Sie Ihre Lizenz- bzw. Vertriebsnummer bereit, da Sie während der Installation danach gefragt werden. Die Lizenznummer ist auch dann erforderlich, wenn Sie die aktuelle Produktversion herunterladen möchten. Die Lizenz- bzw. Vertriebsnummer haben Sie beim Erwerb des AVG-Produkts erhalten: per eMail oder auf der Registrierungskarte der CD.

Die Installation von AVG für Exchange 5.x Server, AVG für Exchange 2000/2003 Server und AVG für Lotus Notes/Domino Server besteht aus zwei Schritten – zuerst muss AVG 7.5 File Server installiert werden, anschließend können Sie dann das AVG-Plugin für den entsprechenden Server installieren.

2.2. Aktuelle Installationsdateien

Eine Version von AVG 7.5 eMail Server befindet sich auf der CD.

Alternativ können Sie auch auf der Grisoft Website unter www.grisoft.com im Download-Bereich die aktuellen Installationspakete herunterladen. Folgen Sie im Download-Bereich dem jeweiligen Link für AVG 7.5 eMail Server, wählen Sie den entsprechenden Server aus, und laden Sie alle erforderlichen Dateien herunter (*Installationspakete für AVG 7.5 File Server und im Falle von Exchange 5.x Server, Exchange 2000/2003 Server und Lotus Notes/Domino Server auch das Installationspaket des speziellen AVG-Plugins für den entsprechenden Server*).

Hinweis: Wenn Sie vor der Installation der Version 7.5 eine ältere AVG-Version verwendet haben, muss diese zuerst manuell deinstalliert werden. Die folgenden Produkte einer älteren Version von AVG eMail Server müssen manuell deinstalliert werden:

- **AVG für Exchange 5.x Server** – Führen Sie für das Verzeichnis, in dem sich die Dateien der Anwendung AVG für Exchange 5.x Server befinden, den Befehl **setupes.exe /uninstall** aus.
- **AVG für Exchange 2000/2003 Server** – Führen Sie für das Verzeichnis, in dem sich die Dateien der Anwendung AVG für Exchange 2000 Server befinden, den Befehl **setupes.exe /uninstall** aus.
- **AVG für Lotus Notes/Domino Server** – Führen Sie für das Verzeichnis, in dem sich die Dateien der Anwendung AVG für Lotus Notes/Domino befinden, den Befehl **setupln.exe /uninstall** aus.

Nach der Deinstallation der alten Version können Sie mit der Installation von Version 7.5 beginnen.

2.3. Installation von CD

Führen Sie zur Installation bitte die folgenden Schritte aus:

- a) Legen Sie die CD in das CD-ROM-Laufwerk ein. Wenn auf dem Computer die Funktion CD-Autorun aktiviert ist, wird die CD automatisch gestartet; führen Sie anschließend die weiteren Schritte aus. (*Wenn die Installation nicht automatisch gestartet wird, müssen Sie auf der Installations-CD die entsprechenden Dateien manuell starten.*)

- b) Wählen Sie eine Sprache für die Anwendung aus.

Hinweis: In der Standardeinstellung werden für die Anwendung nur zwei Sprachen installiert: die von Ihnen in diesem Dialogfeld ausgewählte Sprache und Englisch (die Standardsprache). Wenn Sie Englisch als Sprache auswählen, wird nur Englisch installiert. Über das Dialogfeld **Komponentenauswahl** können Sie weitere Sprachen installieren (zu einem späteren Zeitpunkt während der Installation).

- c) Wählen Sie die Aktion aus, die ausgeführt werden soll – Klicken Sie auf **AVG Installation**.
- d) Wählen Sie das Produkt aus, das Sie installieren möchten – Klicken Sie auf **AVG für eMail Server**.
- e) Wählen Sie im Menü den gewünschten eMail-Server aus.
- f) Wählen Sie in demselben Dialogfeld die Vollversion des entsprechenden Produkts aus.

Wenn auf dem Computer AVG 7.5 File Server nicht installiert ist, müssen Sie dieses Programm zuerst installieren, bevor Sie ein spezielles Plugin für Exchange 5.x-, Exchange 2000/2003- und Lotus Notes/Domino-Server installieren. Für Kerio MailServer darf nur AVG 7.5 File Server installiert werden, da diese Server die Steuerung des Virenschutzes für eMails mit Hilfe des Virenschanners von AVG intern unterstützen.

2.4. Installation über das Internet

- a) Das aktuelle Installationspaket finden Sie auf der Grisoft Website unter www.grisoft.com im Download-Bereich.
- b) Wählen Sie im Bereich **AVG für 7.5 eMail Server** den entsprechenden Server aus, laden Sie alle erforderlichen Dateien herunter, und speichern Sie diese auf der lokalen Festplatte.
- c) Führen Sie in dem Ordner, in dem Sie das Installationspaket gespeichert haben, die ausführbaren Dateien für die Installation aus.

3. AVG für Exchange 5.x Server

3.1. Installationsvorgang

Der Setup-Prozess überprüft zuerst die Versionen auf alle erforderlichen Systembibliotheken. Wenn die Installation neuer Bibliotheken erforderlich ist, fügt das Installationsprogramm den alten Bibliotheken die Erweiterung **.delete** hinzu. Diese werden beim nächsten Neustart des Systems gelöscht. Nachdem Sie zur Beendigung der erfolgreichen Installation auf **Beenden** geklickt haben, wird das System neu gestartet, wenn Sie im entsprechenden Dialogfeld das Kontrollkästchen **Jetzt neu starten** aktiviert haben.

a) Setup – Willkommen

Nach dem Ausführen des Installationspakets wird der Begrüßungsbildschirm angezeigt. Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

b) Setup – Lizenzbedingungen

Im nächsten Fenster wird der vollständige Wortlaut der Lizenzvereinbarung angezeigt. Lesen Sie diese sorgfältig durch. Wenn Sie mit allen Punkten einverstanden sind, klicken Sie zum Bestätigen auf **Weiter**.

c) Setup – Registrierung

Geben Sie hier die Lizenznummer ein, wenn Sie AVG File Server und AVG eMail Server getrennt erworben haben. Sie werden im späteren Verlauf nicht mehr nach der Nummer gefragt. Bestätigen Sie die eingegebenen Informationen durch Klicken auf **Weiter**.

d) Setup – Zielverzeichnis

Nachdem Sie der Vereinbarung zugestimmt haben, werden Sie aufgefordert, das Installationsverzeichnis auszuwählen. Klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen. Es wird jedoch empfohlen, den Standardspeicherort beizubehalten. Klicken Sie auf **Weiter**, um fortzufahren.

e) Setup – Kopiere Dateien

Setup fordert Sie auf, die Installationsdateien zu kopieren, bevor die Installation beendet ist. Stimmen Sie durch Klicken auf **Weiter** zu.

f) Setup – Serverdienst

Nach der Installation der Anwendungsdateien muss der Server-Dienst für AVG für Exchange 5.x Server installiert werden. Sie müssen als Systemadministrator angemeldet sein, um diese Installation vornehmen zu können. Zur Bestätigung werden Sie nach dem Administratorkennwort gefragt, nachdem sämtliche Installationsdateien kopiert wurden. Geben Sie das Kennwort ein, und klicken Sie auf **Weiter**, um die Installation abzuschließen.

g) Setup – Installation beendet

Nachdem der Installationsassistent alle erforderlichen Dateien auf die Festplatte kopiert hat und der AVG für Exchange Server-Dienst aktiviert wurde, ist die Installation beendet.

Klicken Sie im Fenster **Installation beendet** auf **OK**, um das Setup-Dialogfeld zu schließen. Wenn Sie das Kontrollkästchen **Start Konfiguration des AVG für Exchange Server** aktiviert haben, wird das Konfigurationsfenster **AVG für Exchange 5.x Server** direkt nach der Installation geöffnet.

3.2. Programmstart


Nach der Installation von AVG für Exchange 5.x Server verfügt der Computer über den umfangreichsten und zuverlässigsten Schutz gegen Computerviren.

Es gibt verschiedene Möglichkeiten, das Hauptkonfigurationsfenster für das Plugin zu starten:

- Doppelklicken Sie auf dem Desktop auf das Symbol **AVG für Exchange 5.x Server**.
- Wählen Sie im Ordner, in dem AVG für Exchange 5.x Server installiert wurde, die Anwendungsdatei AVG4ESMAN.EXE.
- Klicken Sie in der Komponente **AVG Control Center/eMail Scanner** von AVG File Server auf die Schaltfläche **Optionen**, wählen Sie das Plugin **AVG für MS Exchange Server** aus, und klicken Sie im entsprechenden Fenster **AVG Control Center/eMail-Kontrolle** auf **Optionen des Plugins**.

Nachdem AVG für Exchange 5.x Server gestartet wurde, wird ein neues Fenster angezeigt.

Im Hauptmenü des Fensters können Sie die bearbeiteten Einstellungen über den Eintrag **Server** speichern. Sie können das Layout der Anwendung über den Eintrag **Ansicht** anpassen. Zusätzlich erhalten Sie über die Menüoption **Hilfe** einen Überblick über die Hilfe- und Programminformationen. In der Standardeinstellung wird unter dem Hauptmenü eine Symbolleiste mit Verknüpfungen angezeigt. Darunter werden in der Standardeinstellung weitere Schaltflächen angezeigt. Mit Hilfe dieser Schaltflächen kann der Dienst **AVG für Exchange 5.x Server** ausgeführt und angehalten werden.

Über die Schaltfläche  aus der eben genannten Schaltflächengruppe können Sie den Dienst **AVG für Exchange 5.x Server** neu starten. Die Schaltfläche bleibt deaktiviert, bis der Dienst ausgeführt wird.

Hinweis: Die Anwendung prüft den Dienststatus (auch die Statusänderung der Schaltflächen) alle 10–15 Sekunden, sodass Sie möglicherweise warten müssen, bis die Schaltfläche wieder aktiviert ist.

Die Konfiguration von AVG für Exchange 5.x Server besteht aus zwei grundlegenden Teilen. Im linken Bereich des Anwendungsfensters befindet sich eine Baumstruktur. Im rechten Bereich werden die für den ausgewählten Zweig relevanten Elemente angezeigt.

In der Baumstruktur befinden sich die folgenden Hauptzweige:

a) Informationszweig

Der Informationszweig enthält drei Unterzweige:

o **Statistik**

Enthält statistische Informationen über den Dienststatus von AVG für Exchange 5.x Server und die Anzahl der überprüften Postfächer, öffentlichen Ordner und Nachrichten.

Hier erhalten Sie einen Überblick über verschiedene statistische Daten:

- *Status* – Programmstatus
- *Version* – Ausführliche Angaben zur Version von AVG für Exchange 5.x Server
- *Betriebszeit* – Vergangene Zeit seit dem letzten Neustart von AVG für Exchange 5.x Server
- *Abgefangene Nachrichten* – Anzahl der abgefangenen Nachrichten
- *Nachrichten in Warteschlange* – Anzahl der Nachrichten, die sich in der Warteschlange für die Überprüfung befinden
- *Nachrichten in Bearbeitung* – Anzahl der derzeit verarbeiteten Nachrichten
- *Bearbeitete Nachrichten* – Anzahl der bereits verarbeiteten Nachrichten
- *Überprüfte Postfächer* – Anzahl der überprüften Postfächer
- *Postfächer in Warteschlange* – Anzahl der Postfächer, die sich in der Warteschlange für die Überprüfung befinden
- *Überwachte Postfächer* – Anzahl der überwachten Postfächer
- *Überprüfte Verzeichnisse* – Anzahl der überprüften Verzeichnisse
- *Ordner in Warteschlange* – Anzahl der Ordner, die sich in der Warteschlange für die Überprüfung befinden
- *Überwachte Ordner* – Anzahl der überwachten Ordner

o **Geladene Aktionen**

Enthält interne Informationen über die Datei, die für die Aktionen ausführt.

Die Informationen beschreiben die Aktion (Plugin **AVG für Exchange 5.x Server**), die entsprechende Version und den Pfad zur entsprechenden Bibliotheksdatei.

o **Geladene Einschränkungen**

Enthält interne Informationen über Bedingungen und Einschränkungen.

Hier erhalten Sie interne Informationen über die Datei, die Einschränkungen für die eMail-Verarbeitung bereitstellt. Die Informationen beschreiben die Aktion, die entsprechende Programmversion und den Pfad zur entsprechenden Bibliotheksdatei.

b) AVG Einstellungen

Der Zweig **AVG-Einstellungen** enthält Elemente, die sich auf die Konfiguration von überprüften Benutzerpostfächern und öffentlichen Ordnern beziehen.

In diesem Zweig gibt es zwei Unterzweige. Beide verfügen über ähnliche Funktionen. Der Zweig **Mailboxes** bezieht sich auf die Überprüfung der Postfächer auf mögliche Virusinfektionen, der Zweig **Öffentliche Ordner** bietet die gleichen Informationen für öffentliche Ordner.

Hinweis: Die Überprüfung wird über das AVG Control Center mit Hilfe der Einstellungen des Plugins **AVG für MS Exchange Server** gesteuert.

Wenn Sie das Überprüfen von eingehenden eMails im AVG Control Center deaktivieren, wird die Überprüfung auch nicht von AVG für Exchange 5.x Server ausgeführt. Nachdem Sie im Fenster **AVG Control Center – eMail-Kontrolle** auf **Testkonfiguration** geklickt haben, können Sie das Filtern der Anhänge nach Dateierweiterungen und das Filtern verschlüsselter Archive und weitere Funktionen konfigurieren.

Außerdem kann der Text der eMail-Zertifizierung mit Hilfe von AVG Control Center / eMail-Kontrolle erst dann geändert werden, nachdem Sie auf **Testkonfiguration** geklickt haben.

Anschließend müssen Sie im Fenster **Control Center – eMail-Kontrolle** auf **Konfigurieren** klicken und dort den Zertifikatstext ändern.

Weitere Informationen über das Control Center finden Sie im Benutzerhandbuch für AVG eMail Server. Das Benutzerhandbuch kann auf der Grisoft-Website unter www.grisoft.com heruntergeladen werden.

o Postfachliste

Im Zweig **Postfachliste** können Sie Postfächer auswählen, die überprüft werden sollen, indem Sie im Dialogfeld (siehe nachfolgender Screenshot) unter **Art der Auswahl** das entsprechende Element auswählen. Es können drei Elemente ausgewählt werden:

- *Alle Postfächer* – Keine weitere Auswahl möglich, alle Postfächer werden überprüft.
- *Alle Postfächer mit Ausnahme ausgewählter Postfächer* – Nur die nicht markierten Postfächer werden überprüft.
- *Nur ausgewählte Postfächer* – Nur die markierten Postfächer werden überprüft.

Sie können auch das Verhalten des Programms für den Fall festlegen, dass eine infizierte Nachricht entdeckt wird. Wählen Sie dazu den Zweig **AVG für Exchange 5.x Server** aus.

In diesem Fenster können Sie die Funktion zum Verschieben der infizierten Dateien in den Exchange 5.x Server-Ordner aktivieren und deaktivieren (siehe unten). Mit diesem Vorgang können Sie einen allgemeinen Speicherort festlegen, an dem die vom Virens Scanner verarbeiteten Nachrichten gespeichert und weiter behandelt werden:

- Sie können das Kontrollkästchen **Verschieben infizierter Nachrichten in ein spezielles Verzeichnis** aktivieren oder deaktivieren.

Wenn das Verschieben der infizierten Nachrichten deaktiviert ist, verbleiben alle als infiziert erkannten Nachrichten am ursprünglichen Ort (sie werden jedoch in die AVG Virenquarantäne kopiert). Wenn die Option aktiviert ist, werden infizierte Anhänge in die AVG Virenquarantäne verschoben und Informationen über den infizierten Anhang und das entdeckte Virus im Nachrichtentext der eMail angezeigt.
- In der Schaltflächengruppe **Virenverzeichnis** können Sie die Struktur des speziellen Verzeichnisses festlegen. Sie können auswählen, ob sich für jeden Benutzer ein spezieller Virenordner in *jedem Postfach*, in *öffentlichen Ordnern* oder in den *einzelnen Unterordnern der öffentlichen Ordner* befinden soll.
- Im Feld **Postfach/Öffentlicher Ordner** können Sie den Speicherort des speziellen Virenquarantäneordners ändern. Es wird jedoch empfohlen, den aktuellen Speicherort beizubehalten.

Hinweis: Der Quarantäne-Ordner wird als öffentlicher Ordner erstellt. Deshalb werden in der Standardeinstellung für jeden Benutzer entsprechende Bearbeitungsrechte festgelegt. Der Ordner wird automatisch erstellt, wenn die erste infizierte Nachricht entdeckt und die entsprechende Quarantäneregeln angewendet wird. Es wird empfohlen, die Zugriffsrechte für den Ordner (mit Hilfe des AVG Exchange Administrator) wie folgt zu ändern:

- (i) Wählen Sie in der Baumstruktur **MS Exchange Administrator** die Option **Ordner/Öffentliche Ordner** aus.
 - (ii) Wählen Sie einen der Öffentlichen Ordner aus.
 - (iii) Wählen Sie im Hauptmenü **Datei** die Option **Optionen** aus.
 - (iv) Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Client-Berechtigungen**.
 - (v) Wählen Sie als Standardnamen die Rolle **Keine** aus.
 - (vi) Deaktivieren Sie das Standardrecht **Ordner sichtbar**.
 - (vii) Jetzt können nur Benutzer, denen Zugriff über MS Exchange 5.x Server Administrator gewährt wurde, den Inhalt dieses Ordners anzeigen und ändern.
- o **Öffentliche Ordner**
Im Zweig **Ordner** können Sie Ordner auswählen, die überprüft werden sollen, indem Sie im Dialogfeld (siehe nachfolgender Screenshot) unter **Art der Auswahl** das entsprechende Element auswählen. Es können drei Elemente ausgewählt werden:
 - *Alle Ordner* – Keine weitere Auswahl möglich, alle Ordner werden überprüft.

AVG 7.5 eMail Server

- *Alle Ordner, mit Ausnahme der ausgewählten Ordner* – Nur die nicht ausgewählten Ordner werden überprüft.
- *Nur ausgewählte Ordner* – Nur die ausgewählten Ordner werden überprüft.

Sie können auch das Verhalten von **AVG für Exchange 5.x Server** für den Fall festlegen, dass eine infizierte Nachricht entdeckt wird. Wählen Sie dazu den Zweig **AVG für Exchange 5.x Server** aus.

In diesem Fenster können Sie die Funktion zum Verschieben der infizierten Dateien in den unten beschriebenen Exchange 5.x Server-Ordner aktivieren und deaktivieren. Mit diesem Vorgang können Sie einen allgemeinen Speicherort festlegen, an dem die vom Virenschanner verarbeiteten Nachrichten gespeichert und weiter behandelt werden:

- Sie können das Kontrollkästchen **Verschieben infizierter Nachrichten in einen speziellen Ordner** aktivieren oder deaktivieren. Wenn das Verschieben der infizierten Nachrichten deaktiviert ist, verbleiben alle als infiziert erkannten Nachrichten am ursprünglichen Ort (sie werden jedoch in die AVG Virenquarantäne kopiert). Wenn die Option aktiviert ist, werden infizierte Anhänge in die AVG Virenquarantäne verschoben und Informationen über den infizierten Anhang und den entdeckten Virus im Nachrichtentext der eMail angezeigt.
- In der Schaltflächengruppe **Virenordner** können Sie die Struktur des speziellen Ordners festlegen. Sie können auswählen, ob sich für jeden Benutzer ein spezieller Virenordner in den *Öffentlichen Ordnern* oder in den *einzelnen Unterordnern der Öffentlichen Ordner* befinden soll.
- Im Feld **Postfach/Öffentlicher Ordner** können Sie den Speicherort des speziellen Virenquarantäneordners angeben.

Hinweis: Der Quarantäneordner wird als öffentlicher Ordner erstellt. Deshalb werden in der Standardeinstellung für jeden Benutzer entsprechende Bearbeitungsrechte festgelegt. Der Ordner wird automatisch erstellt, wenn die erste infizierte Nachricht entdeckt und die entsprechende Quarantäneregeln angewendet wird. Es wird empfohlen, die Zugriffsrechte für den Ordner (mit Hilfe von AVG Exchange Administrator) wie folgt zu ändern:

- (viii) Wählen Sie in der Baumstruktur **MS Exchange Administrator** die Option **Ordner/Öffentliche Ordner** aus.
- (ix) Wählen Sie einen der öffentlichen Ordner aus.
- (x) Wählen Sie im Hauptmenü **Datei** die Option **Eigenschaften** aus.
- (xi) Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Client-Berechtigungen**.
- (xii) Wählen Sie als Standardnamen die Rolle **Keine** aus.
- (xiii) Deaktivieren Sie das Standardrecht **Ordner sichtbar**.

(xiv) Jetzt können nur Benutzer, denen Zugriff über MS Exchange 5.x ServerAdministrator gewährt wurde, den Inhalt dieses Ordners anzeigen und ändern.

c) Zweig Optionen

Der Zweig Optionen enthält Einstellungen des Elements zu Diagnoseinformationen. Der Zweig **Optionen** verfügt nur über einen Unterzweig: **Diagnoseprotokolle**.

Hier können Sie verschiedene Protokolleigenschaften von AVG für Exchange 5.x Server bearbeiten.

- In der Schaltflächengruppe **Protokollmodus** können Sie mit Hilfe der folgenden Optionen die Detailstufe für das Protokoll festlegen:
 - *Fehlersuche* – Detaillierte Diagnoseberichte werden protokolliert.
 - *Maximal* – Alle Ereignisse (auch Informationsmeldungen) werden protokolliert.
 - *Mittel* – Folgeschwere Ereignisse und Warnungen werden protokolliert.
 - *Minimal* – Nur folgeschwere Ereignisse werden protokolliert.
 - *Keine* – Es werden keine Ereignisse protokolliert.
- In der Schaltflächengruppe **Neuer Protokollzeitraum** können Sie auswählen, wie häufig eine neue Protokolldatei erstellt werden soll:
 - *Stündlich* – Jede Stunde wird ein neues Protokoll erstellt.
 - *Täglich* – Jeden Tag wird ein neues Protokoll erstellt.
 - *Wöchentlich* – Jede Woche wird ein neues Protokoll erstellt.
 - *Monatlich* – Jeden Monat wird ein neues Protokoll erstellt.
 - *Jährlich* – Jedes Jahr wird ein neues Protokoll erstellt.
 - *Unbegrenzte Dateigröße* – Es wird nur eine und in der Größe unbegrenzte Protokolldatei verwendet.
 - *Bei Dateigröße von* – Im darunter liegenden Feld können Sie die maximale Größe der Protokolldatei angeben. Bei Erreichen dieser Größe wird eine neue Protokolldatei angelegt.
- Unter **Verzeichnis für Protokolldatei** können Sie den Pfad zum Speicherort der Protokolldatei angeben.
- Im Feld **Name der Protokolldatei** wird die allgemeine Maske für einen Protokolldateinamen angezeigt.

Sie können die Konfiguration in diesem Fenster durch Klicken auf **OK** bestätigen. Durch Klicken auf **Abbrechen** werden die Änderungen verworfen. Die Änderungen werden übernommen, wenn Sie auf **Übernehmen** klicken.

4. AVG für Exchange 2000/2003 Server

4.1. Installationsvorgang

Da AVG für Exchange 2000/2003 Server die Virensan-Schnittstelle VSAPI 2.0/2.5 verwendet, muss das Service Pack 1 (oder höher) für Exchange 2000 auf dem Computer installiert sein. Unter dem nachfolgenden Link finden Sie das Service Pack 1 für Exchange 2000 Server:

SP 1 für Exchange 2000 Server:

<http://www.microsoft.com/exchange/downloads/2000/sp1.asp>

Für Exchange 2003 Server 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.

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.

a) Setup – Willkommen

Nach dem Ausführen der Installationsdatei wird ein Begrüßungsdialog angezeigt. Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

b) Setup – Lizenzbedingungen

Im nächsten Fenster wird der vollständige Wortlaut der Lizenzbedingungen angezeigt. Lesen Sie diese sorgfältig durch. Wenn Sie mit allen Punkten einverstanden sind, klicken Sie zum Bestätigen auf **Ja**.

c) Setup – Registrierung

Geben Sie hier Ihre Lizenz- bzw. Vertriebsnummer ein.

Dieser Bildschirm wird nur angezeigt, wenn Sie AVG File Server und AVG für Exchange 2000/2003 Server getrennt erworben haben. Andernfalls haben Sie Ihre Lizenz- bzw. Vertriebsnummer bereits während der Installation von AVG File Server eingegeben und müssen diese nicht erneut eingeben.

Bestätigen Sie die eingegebenen Informationen durch Klicken auf Weiter.

d) Setup –Zielverzeichnis

Im nächsten Fenster werden Sie aufgefordert, den Installationsordner auszuwählen. Klicken Sie auf **Durchsuchen**, um einen anderen Speicherort als den Standardspeicherort auszuwählen. Wenn kein triftiger Grund vorliegt, die Standardeinstellungen zu ändern, wird empfohlen, den aktuellen Speicherort beizubehalten. Klicken Sie auf **Weiter**, um fortzufahren.

e) Setup – Kopiere Dateien

Setup fordert Sie auf, die Installationsdateien zu kopieren, bevor die Installation beendet ist. Stimmen Sie durch Klicken auf **Weiter** zu.

f) Setup – Installation beendet

Nachdem der Installationsassistent alle erforderlichen Dateien auf die Festplatte kopiert hat, ist die Installation beendet.

Sie können die Protokolldatei der Installation anzeigen, indem Sie auf **Protokoll** klicken.

Sie können sich das Setup-Protokoll auch später in der Datei **setup.log** im temporären Verzeichnis des Systems ansehen.

Klicken Sie im Fenster **Installation beendet** auf **OK**, um das Setup-Dialogfeld zu schließen.

g) Setup – Speicherdienst neu starten

Nachdem Sie das Setup-Dialogfeld geschlossen haben, werden Sie aufgefordert, den Speicherdienst für den Exchange 2000/2003 Server neu zu starten.

Klicken Sie auf **Ja**, um den Speicherdienst inklusive aller enthaltenen Komponenten von AVG für Exchange 2000/2003 neu zu starten. Danach können Sie das Produkt verwenden.

***Hinweis:** Durch den Neustart des Speicherservice ist der Server für einige Zeit nicht erreichbar! Warnen Sie die Benutzer vor einem Neustart, da für alle Benutzer, die während des Neustarts online sind, die Verbindung automatisch getrennt wird.*

4.2. Programmwartung

Wenn der Speicherdienst für Exchange 2000/2003 nach der Installation von AVG für Exchange 2000/2003 Server neu gestartet wird, sind für den Start keine weiteren Aktionen erforderlich.

Den Status für AVG für Exchange 2000/2003 Server können Sie im Exchange-System-Manager anzeigen. Wählen Sie im Zweig **Server** der Baumstruktur (links im Hauptfenster) den entsprechenden Server aus. Im Unterzweig des Servers befindet sich der Zweig **AVG für Exchange**. Wenn Sie diesen Zweig auswählen, wird das Informationsfenster geöffnet, das einen Überblick über verschiedene Daten enthält.

In diesem Fenster werden unter anderem der Servername, die Anwendungsversion, die Datenbankversion und die gesamte Laufzeit seit dem letzten Neustart. Zusätzlich werden hier Elemente mit Informationen zur Virenschutzleistung angezeigt (*Zähler zur Leistungsüberwachung*).

AVG für Exchange 2000/2003 Server prüft alle Nachrichten in den Datenbanken der privaten und öffentlichen Ordner. Wenn ein Virus gefunden wird, vermerkt AVG für Exchange 2000/2003 Server dieses in der AVG-Protokolldatei und im Ereignisprotokoll.

(Weitere Details finden Sie in diesem Kapitel unter [4.3 – Überwachung von AVG für Exchange 2000/2003 Server](#).)

In der Virenschnittstelle API 2.0 (VSAPI 2.0 wie in Exchange 2000 Server) können infizierte eMail-Dateien nicht gelöscht werden. Da der infizierte Anhang der eMail nicht gelöscht werden kann, wird der Dateiname des Anhangs geändert: AVG für Exchange 2000/2003 Server fügt dem ursprünglichen Dateinamen die Erweiterung **.virusinfo.txt** hinzu. Der Dateiinhalt wird mit einer Nachricht zum bekannten Virus überschrieben. Wenn sich direkt in der Nachricht ein Virus befindet, wird der gesamte eMail-Text mit dem Hinweis überschrieben, dass in der Nachricht ein Virus gefunden wurde.

In der Virenschnittstelle API 2.5 (VSAPI 2.5 wie in Exchange 2003 Server) können außerdem Nachrichten mit infizierten Dateien gelöscht werden. Diese Funktion kann im Konfigurationsdialogfeld **AVG für Exchange 2000/2003 Server** eingerichtet werden.

Das Konfigurationsfenster **AVG für Exchange 2000/2003 Server** kann geöffnet werden, indem Sie mit der rechten Maustaste auf den Zweig **AVG für Exchange** klicken und **Eigenschaften** auswählen. Alternativ können Sie das Fenster auch über die Schaltfläche **Aktion** öffnen, die sich direkt unter dem Hauptmenü des Exchange-System-Managers befindet.

Das Konfigurationsfenster **AVG für Exchange Eigenschaften** enthält zwei Reiter. Hier können Sie die Einstellungen für den eMail-Virenschutz und das Protokollverhalten ändern.

a) Reiter „Allgemein“

Auf der Registerkarte **Allgemein** befinden sich mehrere voreingestellte Optionen, die sich auf die Leistung des eMail-Virenschutzes von AVG für Exchange 2000/2003 Server beziehen:

- Kontrollkästchen **Aktivieren** – Sie können das Scannen der E-Mails aktivieren und deaktivieren.
- Kontrollkästchen **Hintergrundprüfung** – Sie können 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. Wenn ein Objekt vor dem Speichern in den Ordnern der Benutzerpostfächer nicht überprüft wurde, wird es zum Überprüfen an AVG für Exchange 2000/2003 Server weitergeleitet. Die Suche nach nicht geprüften Objekten und der Virentest werden parallel ausgeführt.
- Kontrollkästchen **Vorausschauendes Scannen** – Sie können die Funktion zum vorausschauenden Scannen der VSAPI 2.0/2.5 hier aktivieren und deaktivieren. Beim vorausschauenden Scannen wird ein dynamisches Prioritätsmanagement der Objekte in der Prüfungswarteschlange genutzt. Objekte mit niedrigerer Priorität werden erst überprüft, wenn die Überprüfung für alle Objekte höherer Priorität abgeschlossen ist (meist werden diese auf Anforderung in die Warteschlange gestellt). Wenn ein Objekt durch Clientzugriff eine höhere Priorität erhält, wird der Vorrang des Objekts entsprechend der Benutzeraktivität geändert.
- Kontrollkästchen **RTF scannen** – Sie können hier festlegen, ob RTF-Dateien geprüft werden sollen.

- Feld **Scan-Threads** – Der Prozess der Virenprüfung ist in der Standardeinstellung in verschiedene Threads aufgeteilt, um die Testleistung auf einem hohen Niveau zu halten. Sie können hier die Anzahl der Threads ändern. Die Standardanzahl wird nach der Formel $2 \times (\text{Anzahl der Prozessoren}) + 1$ berechnet.
- Feld **Scan-Timeout** – Die maximale Wartezeit (in Sekunden) eines Threads für den Zugriff auf eine zu scannende Nachricht.
- **Infizierte Dateien in die Virenquarantäne verschieben** – Wenn dieses Kontrollkästchen aktiviert ist, wird jede infizierte eMail in die AVG Virenquarantäne verschoben.
- **Nachrichten mit infizierten Dateien löschen (nur ES 2003)** – Wenn dieses Kontrollkästchen aktiviert ist, werden infizierte eMails gelöscht. Wenn dieses Kontrollkästchen deaktiviert ist, wird die infizierte Nachricht an den Empfänger übertragen, und der infizierte Anhang wird durch einen Text über den gefundenen Virus ersetzt. Diese Option ist nur bei VSAPI 2.5 in Exchange 2003 Server verfügbar.

Alle Funktionen auf diesem Reiter 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:80/support/kb/articles/Q285/6/67.ASP> – Allgemeine Informationen über die VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> – Informationen über die Zusammenarbeit von Exchange und Virenschutz-Software
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> – Informationen über die erweiterten Eigenschaften der VSAPI2.5 in Exchange2003 Server

Hinweis: Das Scannen wird über das AVG Control Center mit Hilfe der Einstellungen des Plugins **AVG für MS Exchange Server** gesteuert.

Wenn Sie das Scannen der eingehenden eMail-Nachrichten im AVG Control Center deaktivieren, wird diese Überprüfung auch nicht von AVG für Exchange 2000/2003 Server ausgeführt. Hier können Sie außerdem das Filtern der Anhänge nach Dateierweiterungen und das Filtern verschlüsselter Archive und weitere Funktionen konfigurieren:

Weitere Informationen über das AVG Control Center finden Sie im Benutzerhandbuch für AVG File Server, das auf der Grisoft-Website unter www.grisoft.com im Download-Bereich verfügbar ist.

b) Reiter „Diagnoseprotokoll“

Auf dieser Registerkarte können Sie die Häufigkeit der Protokollierung für die Virenprüfung und das allgemeine Verhalten definieren. Auf dem Reiter **Diagnoseprotokolle** wurden bestimmte Voreinstellungen vorgenommen:

- Optionsfeldgruppe **Protokollmodus** – Hier können Sie die Menge der protokollierten Informationen festlegen.

- Optionsfeldgruppe **Neuer Protokollzeitraum** – Hier können Sie definieren, wann eine neue Protokolldatei angelegt werden soll und wie groß diese werden darf.
- Feld **Protokolldateiverzeichnis** – Hier können Sie den Standardspeicherort der Protokolldatei ändern.
- Feld **Protokolldateiname** – Hier wird der Standardname der Protokolldatei angezeigt.
- Feld **Aktualisieren** – Hier können Sie festlegen, wie oft der Bildschirm im Monitor (zu sehen im Informationsfenster **AVG für Exchange 2000/2003 Server**) aktualisiert werden soll.

4.3. Überwachung von AVG für Exchange 2000/2003 Server

a) Online-Überwachung

Im Informationsfenster **AVG für Exchange 2000/2003 Server** (siehe hierzu den [Anfang](#) dieses Abschnitts) werden mehrere Felder angezeigt:

Die ersten vier Elemente bieten allgemeine Informationen über den Status des Servers und von AVG für Exchange 2000/2003 Server:

- **Server** – Servername
- **Version** – Version von AVG für Exchange 2000/2003 Server
- **Kernel-Version** – Version des Virenschutz-Kernels und dessen interner Virendatenbank
- **Betriebszeit** – Gesamtzeit seit dem letzten Neustart des Exchange 5.x-Servers

Die anderen Einträge stellen bestimmte Zähler der Leistungsüberwachung der VSAPI 2.0/2.5 mit Bezug auf die Virenprüfung von Exchange 2000/2003 Server dar. Die Zähler haben folgende Bedeutung:

- **Gescannte Bytes** – Gesamtanzahl der Bytes in allen vom Virenschanner geprüften Dateien
- **Gesäuberte Dateien** – Gesamtanzahl der einzelnen vom Virenschanner gesäuberten Dateien
- **Gesäuberte Dateien/Sek.** – Rate, mit der einzelne Dateien durch den Virenschanner gesäubert werden
- **Unter Quarantäne gestellte Dateien** – Gesamtanzahl der einzelnen vom Virenschanner in die Quarantäne verschobenen Dateien
- **Unter Quarantäne gestellte Dateien/Sek.** – Rate, mit der einzelne Dateien durch den Virenschanner in die Quarantäne verschoben werden
- **Im Hintergrund überprüfte Ordner** – Gesamtanzahl der Ordner, die durch die Hintergrundprüfung bearbeitet werden
- **Gesäuberte Nachrichten** – Gesamtanzahl der vom Virenschanner gesäuberten Nachrichten oberster Priorität.
- **Gesäuberte Nachrichten/Sek.** – Rate, mit der Nachrichten oberster Priorität durch den Virenschanner gesäubert werden

- **Unter Quarantäne gestellte Nachrichten** – Gesamtanzahl der vom Virens Scanner in die Quarantäne verschobenen Nachrichten oberster Priorität
- **Unter Quarantäne gestellte Nachrichten/Sek.** – Rate, mit der Nachrichten oberster Priorität durch den Virens Scanner in die Quarantäne verschoben werden
- **Verarbeitete Nachrichten** – Kumulierte Anzahl der Nachrichten oberster Priorität, die vom Virens Scanner verarbeitet wurden
- **Verarbeitete Nachrichten/Sek.** – Rate, mit der Nachrichten oberster Priorität durch den Virens Scanner verarbeitet werden
- **Im Hintergrund gescannte Nachrichten** – Gesamtanzahl der Nachrichten, die durch die Hintergrundprüfung verarbeitet werden
- **Warteschlangenlänge** – Aktuelle Anzahl ausstehender Anforderungen zur Virenprüfung in der Warteschlange
- **Wartende Dateien** – Anzahl der Dateien, die auf eine Virenprüfung warten
- **Gelöschte Nachrichten** – Gesamtanzahl aller verdächtigen Nachrichten, die vom Virens Scanner gelöscht wurden (nur in VSAPI 2.5 verfügbar)
- **Gelöschte Nachrichten/Sek.** – Rate, mit der verdächtige Nachrichten vom Virens Scanner gelöscht werden (nur in VSAPI 2.5 verfügbar)

b) Ereignisanzeige des Betriebssystems

Neben der Online-Überwachung von AVG für Exchange 2000/2003 Server können Sie auch eine Protokollierung von Ereignissen des Virens Scanners im Ereignisprotokoll konfigurieren. Mit den verfügbaren Ereignissen können viele Aspekte erfasst werden, z. B. Ladehinweise zu den Programmbibliotheken, Ereignisse zu gefundenen Viren, Warnungen zur Fehlerbehandlung usw.

Das Protokollverhalten des Exchange VSAPI 2.0/2.5 konfigurieren Sie im Hauptfenster des Exchange-System-Managers (*siehe [Anfang dieses Kapitels](#)*).

- Doppelklicken Sie in der Baumstruktur auf den Zweig **Server**.
- Wählen Sie den entsprechenden Server aus (*im Beispiel unten ist der Servername hervorgehoben*)
- Klicken Sie mit der rechten Maustaste auf den Servernamen, und wählen Sie im Kontextmenü die Option **Eigenschaften** aus.
- Das Fenster **Eigenschaften** wird angezeigt.
- Wechseln Sie zur Registerkarte **Diagnoseprotokolle**.
- Wählen Sie im Zweig **Dienste** den Ordner **MExchangeIS / System** aus.
- Markieren Sie in der Liste **Kategorien** den Eintrag **Virenschutz**, und wählen Sie die Protokollierungsebene für das Ereignisprotokoll des Betriebssystems aus. Folgende Ebenen stehen zur Verfügung:
 - Keine
 - Minimal

AVG 7.5 eMail Server

- Mittel
- Maximal

Hinweis: Eine vollständige Beschreibung der VSAPI2.0/2.5-Ereignisse finden Sie unter folgender Adresse:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336>

5. AVG für Lotus Notes/Domino Server

5.1. Installationsvorgang

Stellen Sie sicher, dass vor Beginn der Installation von AVG für Lotus Notes/Domino Server keine eMail-Server-Anwendung ausgeführt werden. Nachdem alle Serverprozesse und -dienste beendet wurden, können Sie die nachfolgenden Installationsschritte ausführen.

Der Setup-Prozess überprüft zuerst die Versionen auf alle erforderlichen Systembibliotheken. Wenn die Installation neuer Bibliotheken erforderlich ist, fügt das Installationsprogramm den alten Bibliotheken die Erweiterung **.delete** hinzu. Diese werden beim nächsten Neustart des Systems gelöscht. Nachdem Sie zur Beendigung der erfolgreichen Installation auf **Fertigstellen** geklickt haben, wird das System neu gestartet, wenn Sie im entsprechenden Dialogfeld das Kontrollkästchen **Jetzt neu starten** aktiviert haben.

a) Setup – Willkommen

Nach Ausführung des Installationspakets wird ein Begrüßungsdialog angezeigt. Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

b) Setup – Lizenzbedingungen

Im nächsten Fenster wird der vollständige Wortlaut der Lizenzbedingungen angezeigt. Lesen Sie diese sorgfältig durch. Wenn Sie mit allen Punkten einverstanden sind, klicken Sie zum Bestätigen auf **Ja**.

c) Setup –Registrierung

Geben Sie in diesem Bildschirm die Lizenznummer für AVG für Lotus Notes/Domino Server ein.

Sie werden nur dann nach der Lizenznummer gefragt, wenn Sie AVG File Server (oder AVG Anti-Virus) und AVG für Lotus Notes/Domino Server getrennt erworben haben. Andernfalls haben Sie die Lizenznummer bereits während der Installation von AVG File Server oder AVG Anti-Virus angegeben und werden nicht danach gefragt.

Bestätigen Sie die Informationen durch Klicken auf **Weiter**.

d) Setup – Installationsverzeichnis

Sobald Sie den Lizenzbedingungen zugestimmt haben, werden Sie aufgefordert, das Installationsverzeichnis auszuwählen. Die Daten und Programmdateien von AVG für Lotus Notes/Domino Server werden direkt im Ordner **Lotus Notes/Domino** installiert. Klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen. Es wird jedoch empfohlen, den Standardspeicherort beizubehalten. Klicken Sie auf **Weiter**, um fortzufahren.

e) Setup – NOTES.INI

Für eine ordnungsgemäße Installation von AVG für Lotus Notes/Domino Server müssen Sie den Speicherort der entsprechenden Konfigurationsdatei NOTES.INI angeben. Wenn NOTES.INI nicht automatisch gefunden wird,

werden Sie aufgefordert, den Pfad manuell einzugeben (klicken Sie dazu auf **Durchsuchen**, oder geben Sie den vollständigen Pfad direkt ein). Klicken Sie auf **Weiter**, um fortzufahren.

f) Setup – Installation beendet

Nachdem der Installationsassistent alle erforderlichen Dateien auf die Festplatte kopiert hat, ist die Installation beendet.

5.2. Programmwartung

Der Computer wird jetzt mit einem umfangreichen und zuverlässigen Schutz gegen Computerviren ausgestattet.

Die folgenden Dateien wurden installiert:

- **Lotus Notes/Domino-Programmverzeichnis:**
 - navgscan.exe – Serveranwendung zum Prüfen von Datenbanken
 - navgmail.exe – Virenschutz des Servers für eMails
 - navghook.dll – Bibliothek zum Aufbewahren von eMails aus der MAIL.BOX-Datenbank, bis diese auf Viren geprüft wurden
- **Lotus Notes/Domino-Datenverzeichnis:**
 - avgsetup.ntf – Vorlage für die Konfigurationsdatenbank
 - avglog.ntf – Vorlage für die Protokolldatenbank
 - avgvirus.ntf – Vorlage für die Virenquarantäne
 - avgsetup.nsf – Konfigurationsdatenbank
 - avglog.nsf – Protokolldatenbank
 - avgvirus.nsf – Datenbank für Virenquarantäne

Zum Abschließen der Installation muss der Lotus Notes/Domino-Server neu gestartet werden. Hiermit wird AVG für Lotus Notes/Domino Server automatisch gestartet (Serverdienste AvgScan und AvgMail). Außerdem werden die AVG-Datenbanken (Konfiguration, Protokoll und Quarantäne) erstellt. Diese können bei Bedarf später über die entsprechenden Konfigurationsbereiche gesperrt werden.

Nach der fehlerfreien Installation von AVG für Lotus Notes/Domino Server und dem Neustart des Lotus Domino-Servers sind keine weiteren Schritte für einen effizienten eMail-Schutz erforderlich. Die Standardeinstellungen von AVG für Lotus Notes/Domino Server sind nachfolgend aufgeführt:

- Scannen aller eMails mit Anhängen.
- An jede virenfreie eMail wird eine Bestätigung angehängt, die keine Signatur enthält und nicht verschlüsselt wird.
- Eingehende Dateien, die als infiziert angesehen werden, werden an den Empfänger mit einer Benachrichtigung gesendet, die Details zur Datei und zum Virus enthalten.
- Ausgehende eMails mit infizierten Anhängen werden an den Absender mit einer Information über die infizierten Objekte und die entsprechenden Viren zurückgesendet. Die infizierte eMail wird nicht an den Empfänger gesendet.

Sie können die Standardkonfiguration von AVG für Lotus Notes/Domino Server sehr leicht mit dem Dienstprogramm Domino Administrator ändern. Wenn Sie im ersten Fenster die Registerkarte **Dateien** auswählen, werden drei Dateien bezüglich AVG (Lotus-Datenbanken) neben den anderen zu verwaltenden Dateien angezeigt:

- **AVG-Protokoll** (siehe Abschnitt [5.4 AVG Protokolldatei](#))
- **AVG für Lotus Notes** (siehe Abschnitt [5.2 Programmwartung](#))
- **AVG Virenquarantäne** (siehe Abschnitt [5.3 AVG Virenquarantäne](#))

Doppelklicken Sie im Hauptfenster von Lotus Administrator auf **AVG für Lotus Notes** und anschließend auf die Registerkarte **Datei**, um das Fenster **AVG für Lotus Notes – Konfiguration** zu öffnen.

Wählen Sie in diesem Fenster den Server aus, auf dem die AVG-Konfigurationsdatenbank gespeichert werden soll. Doppelklicken Sie auf das Serverfeld aus, oder klicken Sie auf die Schaltfläche **Bearbeiten**, die sich direkt über der Serverliste befindet. Im Dienstprogramm Lotus Administrator wird dann ein neues Fenster ohne Titel geöffnet.

Sie können das Scannen und Verwalten infizierter eMails über AVG für Lotus Notes/Domino Server vollständig kontrollieren. Außerdem können Sie mehrere Überprüfungen der Lotus-Datenbank planen. Um die durchgeführten Konfigurationsänderungen zu speichern, klicken Sie auf die Schaltfläche **Speichern und schliessen** im oberen Bereich des Fensters.

Die Felder, die in den oben genannten Screenshots dargestellt werden, können folgendermaßen konfiguriert werden:

a) Allgemeine Einstellungen

- **Servername** – Die aktuelle Serverspezifikation.
- **eMail mit Zertifikat versehen** – Wählen Sie aus, ob AVG für Lotus Notes/Domino eMails zertifizieren soll.
- **Text mit Zertifikat versehen** – Sie können den Bestätigungstext (z.B. „Die Nachricht ist virenfrei“) bearbeiten.

b) Überprüfen der eMails

- **eMails scannen** – Aktiviert/deaktiviert das automatische Scannen der eMails.

c) Einstellungen für eingehende eMails

- **Anhänge** – Über diese Option können Dateinamenerweiterungen von eMail-Anhängen definiert werden, die automatisch aus der eMail entfernt werden sollen. Anhänge mit benutzerdefinierten Erweiterungen werden aus einer eingehenden eMail unabhängig davon automatisch entfernt, ob die erkannte Datei mit einem Virus infiziert ist. Die folgenden Aktionen stehen zur Verfügung:
 - **Keine Aktion** – Eingehende Anhänge werden nicht gefiltert oder entfernt.
 - **Entfernen** – Benutzerdefinierte Anhänge werden aus einer virenfizierten eMail entfernt und anschließend gelöscht.

AVG 7.5 eMail Server

- *Entfernen und in Virenquarantäne speichern* – Benutzerdefinierte Anhänge werden aus der vireninfizierten eMail gelöscht und in die Virenquarantäne verschoben.

Sie können Erweiterungen der Dateianhänge aus der Stichwortliste im Feld **Erweiterungen** auswählen (oder auch eine neue Erweiterung eingeben, wenn die gewünschte Erweiterung nicht aufgelistet ist), wenn die Aktionen *Entfernen* oder *Entfernen und speichern* ausgewählt sind.

- **Aktion bei gefundenem Virus** – Sie können festlegen, welche Aktion durchgeführt werden soll, wenn ein Virus in einer eingehenden eMail entdeckt wird:
 - *eMail an Empfänger senden* – Die infizierte eMail wird an den Empfänger mit einer Warnung über den Virus und den infizierten Dateianhang gesendet. Zusätzliche Einstellungen können definiert werden, ob die infizierten Anhänge aus der eMail entfernt werden und/oder in die AVG Virenquarantäne verschoben werden sollen. Im Feld **Infizierte Dateien** können Sie festlegen, welche Aktion mit vireninfizierten Dateien durchgeführt werden soll. Folgende Aktionen können durchgeführt werden:
 - Entfernen* – Die infizierten Dateien werden aus der eMail entfernt.
 - Entfernen und in Virenquarantäne speichern* – Die infizierten Dateien werden aus der eMail entfernt und in der Virenquarantäne gespeichert.
 - In Virenquarantäne speichern und an Empfänger senden* – Die infizierten Dateien bleiben in der eMail enthalten und Kopien werden in der lokalen Virenquarantäne gespeichert.
 - An Empfänger senden* – Die infizierten Dateien bleiben in der eMail enthalten und werden an den Empfänger gesendet.
 - *eMail an Absender zurücksenden* – Die infizierte eMail wird an den Absender als unzustellbar zurückgesendet, mit der Option, eine Warnung über das gefundene Virus anzufügen.
 - **Warnung an Empfänger/Absender senden** – Sie sollten dieses Optionsfeld aktivieren, wenn Sie den Empfänger/Absender vor der vireninfizierten eMail warnen möchten (je nachdem, ob Sie *eMail an Empfänger senden* oder *eMail an Absender zurücksenden* aktiviert haben).
 - **Text der Warnung** – Hier können Sie den Standardtext der Nachricht bearbeiten, der in der vireninfizierten eMail enthalten ist (wenn vorher das Optionsfeld *Warnung an Empfänger/Absender senden* aktiviert wurde).
 - **Warnung an Administrator senden** – Wenn dieses Optionsfeld aktiviert ist, wird eine Warnung bei einer eingehenden infizierten eMail an die Administratoren gesendet, die im Feld *Administratoren* angegeben sind. Sie können den Text dieser Warnung im entsprechenden Feld **Text der Warnung** bearbeiten.

d) Einstellungen für ausgehende eMails

AVG 7.5 eMail Server

- **Aktion bei gefundenem Virus** – Sie können festlegen, welche Aktion durchgeführt werden soll, wenn ein Virus in einer ausgehenden eMail entdeckt wird:
 - E-Mail an Empfänger senden – Die infizierte eMail wird an den Empfänger mit einer Warnung über das Virus und den infizierten Dateianhang gesendet. Zusätzliche Einstellungen können definiert werden, ob die infizierten Anhänge aus der eMail entfernt werden und/oder in die AVG Virenquarantäne verschoben werden sollen. Im Feld **Infizierte Dateien** können Sie festlegen, welche Aktion mit vireninfizierten Dateien durchgeführt werden soll. Folgende Aktionen können durchgeführt werden:
 - Entfernen – Die infizierten Dateien werden aus der eMail entfernt.
 - Entfernen und in Virenquarantäne speichern* – Die infizierten Dateien werden aus der eMail entfernt und in der Virenquarantäne gespeichert.
 - In Virenquarantäne speichern und an Empfänger senden* – Die infizierten Dateien bleiben in der eMail enthalten und Kopien werden in der lokalen Virenquarantäne gespeichert.
 - An Empfänger senden* – Die infizierten Dateien bleiben in der eMail enthalten und werden an den Empfänger gesendet.
- **eMail an Absender zurücksenden** – Die infizierte eMail wird an den Absender als unzustellbar zurückgesendet, mit der Option, eine Warnung über den gefundenen Virus anzufügen.
- **Warnung an Empfänger/Absender senden** – Sie sollten dieses Optionsfeld aktivieren, wenn Sie den Empfänger/Absender vor der vireninfizierten eMail warnen möchten (je nachdem, ob Sie *eMail an Empfänger senden* oder *eMail an Absender zurücksenden* aktiviert haben).
- **Text der Warnung** – Hier können Sie den Standardtext der Nachricht bearbeiten, der in der vireninfizierten eMail enthalten ist (wenn vorher das Optionsfeld *Warnung an Empfänger/Absender senden* aktiviert wurde).
- **Warnung an Administrator senden** – Wenn dieses Optionsfeld aktiviert ist, wird eine Warnung bei einer ausgehenden infizierten eMail an die Administratoren gesendet, die im Feld *Administratoren* angegeben sind. Sie können den Text dieser Warnung im entsprechenden Feld **Text der Warnung** bearbeiten.

e) Geplante Datenbanktests

Sie können die Überprüfung von Server-Datenbanken in diesem Bereich des Konfigurationsformulars von AVG für Lotus Notes/Domino Server planen. Es stehen verschiedene Felder zur Verfügung:

- **Überprüfungszeit** – Legen Sie ein Zeitintervall und/oder den genauen Zeitpunkt fest, wann AVG für Lotus Notes/Domino Server die Datenbanken überprüfen soll.

- **Wiederholen nach** – Legen Sie einen Zeitraum (in Minuten) für die Häufigkeit der Tests entsprechend der Angabe im Feld *Überprüfungszeit* fest.
- **Wochentage** – Sie können die Tage auswählen, an denen Datenbanken überprüft werden sollen.
- **Scannen** (Anhänge) – Hier können Sie definieren, ob alle Anhänge überprüft werden sollen oder nur die Anhänge, deren Erweiterungen im Feld **Erweiterungen** angegeben sind.
- **Infizierte Dateien** – Hier können Sie angeben, welche Aktion mit vireninfizierten Dateien durchgeführt werden soll. Folgende Aktionen können durchgeführt werden:
 - *Entfernen* – Die infizierten Dateien werden aus dem Dokument entfernt.
 - *Entfernen und in Virenquarantäne speichern* – Die infizierten Dateien werden aus dem Dokument entfernt und in der Virenquarantäne gespeichert.
 - *Im Dokument belassen* – Die infizierten Dateien werden im Dokument belassen.
- **Scannen** (Datenbanken) – Hier können Sie definieren, ob alle Server-Datenbanken überprüft werden sollen oder nur jene, die im Feld *Liste der Datenbanken* (zu scannende Dateien) angegeben sind.
- **Warnung an Administratoren senden** – Wenn dieses Optionsfeld aktiviert ist und beim Scannen der Datenbank ein Virus gefunden wird, wird eine Warnung an die Administratoren gesendet, die im Feld *Administratoren* angegeben sind. Sie können den Text dieser Warnung im entsprechenden Feld *Text der Warnung* bearbeiten. Außerdem können Sie die Betreffzeile der Nachricht definieren. Die Nachricht selbst enthält eine Liste der infizierten Dateien (mit Links) und erkannten Viren.

Hinweis: Die Leistung und des Scanners und der Anhangfilter werden über das AVG Control Center gesteuert. Im Allgemeinen können im AVG Control Center die Einstellungen des Plugins nicht konfiguriert werden. Funktionen wie das Aktivieren/Deaktivieren der eMail-Überprüfung und eMail-Bestätigungen können nur in den Datenbanken von AVG für Lotus Notes/Domino Server konfiguriert werden.

5.3. AVG Virenquarantäne

Die Virenquarantäne von AVG für Lotus Notes/Domino Server ist eine spezielle Serverdatenbank, in die Sie vireninfilzierte Dateien für eine sichere Weiterbehandlung (Entfernung oder Wiederherstellung) ohne Risiko für die Systemressourcen speichern können.

In der Verwaltungsoberfläche von Lotus Notes/Domino Server können Sie über die Datenbank der AVG Virenquarantäne auf die Virenquarantäne von AVG für Lotus Notes/Domino Server zugreifen. Diese Datenbank ist vollständig unabhängig von der Anwendung AVG Virenquarantäne! Es handelt sich vielmehr um eine spezielle Lotus Notes/Domino Server-Datenbank. Doppelklicken Sie im Hauptfenster von Lotus Administrator oder auf der Registerkarte **Datei** auf das entsprechende Feld. Anschließend wird ein neues Fenster geöffnet.

Sie können die in der Virenquarantäne gespeicherten Viren gemäß den folgenden Gruppierungsparametern untersuchen:

a) Gliederung nach virenfizierten Datenbankdateien, die während der Datenbanküberprüfung entdeckt wurden:

In der Standardeinstellung werden vier Felder angezeigt:

- *Erstellt* – Zeitstempel der Datenbankerstellung
- *Geändert* – Zeitstempel der Datenbankänderung
- *Dateien* – Die infizierten Dateien
- *Viren* – Die Kennung der gefundenen Viren

b) Gliederung nach Viren, die in Datenbanken während der Datenbanküberprüfung entdeckt wurden:

In der Standardeinstellung werden vier Felder angezeigt:

- *Erstellt* – Zeitstempel der Datenbankerstellung
- *Geändert* – Zeitstempel der Datenbankänderung
- *Dateien* – Die infizierten Dateien
- *Viren* – Die Kennung der gefundenen Viren

c) Gliederung nach dem Datum der infizierten Nachricht, die während der eMail-Überprüfung entdeckt wurde:

In der Standardeinstellung werden fünf Felder angezeigt:

- *Zeit* – Empfangszeit der infizierten eMail
- *An* – Informationen zum Empfänger
- *Von* – Informationen zum Absender
- *Dateien* – Die Kennung der infizierten Dateien
- *Viren* – Die Kennung der gefundenen Viren

d) Gliederung nach dem Empfänger der infizierten Nachricht, die während der eMail-Überprüfung entdeckt wurde:

In der Standardeinstellung werden fünf Felder angezeigt:

- *Zeit* – Empfangszeit der infizierten e-Mail
- *An* – Informationen zum Empfänger
- *Von* – Informationen zum Absender
- *Dateien* – Die Kennung der infizierten Dateien
- *Viren* – Die Kennung der gefundenen Viren

e) Gliederung nach dem Virus der infizierten Nachricht, die während der eMail-Überprüfung entdeckt wurde:

In der Standardeinstellung werden fünf Felder angezeigt:

- *Zeit* – Empfangszeit der infizierten eMail
- *An* – Informationen zum Empfänger

- *Von* – Informationen zum Absender
- *Dateien* – Die Kennung der infizierten Dateien
- *Viren* – Die Kennung der gefundenen Viren

5.4. AVG Protokolldatei

Informationen über aufgetretene Ereignisse bei AVG für Lotus Notes/Domino Server während der Ausführung des Servers werden in der AVG Protokolldatei gespeichert. Hier können Sie die Ereignisse überprüfen und weiter untersuchen, z.B. Initialisierungsfortschritt, gefundene Viren usw.

In der Verwaltungsoberfläche von Lotus Notes/Domino Server können Sie über die AVG Protokolldatenbank auf die AVG Protokolldatei zugreifen. Doppelklicken Sie im Hauptfenster von Lotus Administrator oder auf der Registerkarte **Datei** auf das entsprechende Feld. Anschließend wird ein neues Fenster geöffnet.

Es werden zwei Felder angezeigt, eines für die Datenbanken und eines für die eMail-Ordner:

- *Datum* – Zeitstempel des protokollierten Datensatzes
- *Text* – Text der Protokollierungsinformationen

6. AVG für Kerio MailServer

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

Klicken Sie zum Öffnen des Fensters auf **Inhaltsfilter**. Im Fenster befinden sich drei Reiter:

- **Spamfilter**
- **Antivirus** (siehe Abschnitt [6.1 – Antivirus](#))
- **Filter für Anhänge** (siehe Abschnitt [6.2 – Filter für Anhänge](#))

Alle vorgenommenen Änderungen können durch Klicken auf **Übernehmen** im unteren Bereich des Konfigurationsfensters gespeichert werden. Über die Schaltfläche **Zurücksetzen** kehren Sie zum zuletzt gespeicherten Zustand zurück.

6.1. Antivirus

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** aus.

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

a) 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 vireninferierte 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.

b) Ein Teil einer Nachricht kann nicht überprüft 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 überprüft 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 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 entfernt). Diese Option ist zwar sicher, jedoch ist das Senden von kennwortgeschützten Archiven nicht mehr möglich.

Hinweis: Die Leistung und das Verhalten des Scanners wird über das AVG Control Center gesteuert. Wenn Sie das Überprüfen der eingehenden eMail-Nachrichten im AVG Control Center deaktivieren, wird das Scannen auch nicht von AVG für Kerio MailServer ausgeführt. Weitere Informationen über das AVG Control Center finden Sie im Benutzerhandbuch zu AVG File Server (oder AVG Anti-Virus), das auf der Grisoft-Website unter www.grisoft.com im Download-Bereich verfügbar ist.

6.2. 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 sind *Akzeptieren* (akzeptiert den

AVG 7.5 eMail Server

Anhang) und *Blockieren* (blockiert den Anhang, wie auf dem Reiter **Aktion** festgelegt).

- **Beschreibung** – In diesem Feld wird die Beschreibung des Anhangs angegeben.

Durch Klicken auf **Entfernen** können Sie einen Eintrag aus der Liste entfernen. Weitere Einträge können der Liste hinzugefügt werden, indem Sie auf **Hinzufügen** klicken. Sie können auch einen bestehenden Eintrag ändern, indem Sie auf **Bearbeiten** klicken. Anschließend wird ein Fenster mit den folgenden Einträgen 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. Programmaktualisierung

Virenschutz-Programme können nur bei regelmäßiger Aktualisierung einen zuverlässigen Schutz garantieren. AVG 7.5 eMail Server bietet einen zuverlässigen und schnellen Aktualisierungsdienst mit kurzen Reaktionszeiten. Moderne Viren breiten sich sehr schnell aus und infizieren in kürzester Zeit sehr viele Computer. Daher muss der Virenschutz besonders auf Servern so schnell wie möglich aktualisiert werden, damit die Gefahr gebannt wird, bevor die Computer von Endbenutzern infiziert werden.

7.1. Aktualisierungsstufen

AVG bietet drei Aktualisierungsstufen:

- **Vorrangige Aktualisierung**

Eine vorrangige Aktualisierung enthält die erforderlichen Änderungen für einen zuverlässigen Virenschutz. In der Regel wird der Code nicht geändert, sondern nur die Virendefinitionsdatenbank wird aktualisiert. Aktualisierungen dieser Art sollten unmittelbar nach deren Veröffentlichung angewendet werden.

- **Empfohlene Aktualisierung**

Eine empfohlene Aktualisierung umfasst verschiedene Änderungen, Fehlerbehebungen und Verbesserungen des Programms.

Für besonders wichtige Systeme wird empfohlen, dass diese Aktualisierungen nicht automatisch nach deren Veröffentlichung installiert werden, sondern vorher in einer Testumgebung getestet werden.

***Hinweis:** Wenn gemäß den Systemrichtlinien Patches und Aktualisierungen für das Betriebssystem erst dann auf Produktionsservern angewendet werden dürfen, nachdem sie einem ausführlichen Test in einer Testumgebung unterzogen wurden, sollten Sie auch die empfohlenen Aktualisierungen von AVG nicht auf diesen Servern installieren. Wenn Sie Patches für das Betriebssystem ohne vorherige Tests direkt auf den Servern installieren, können Sie auch empfohlene Aktualisierungen direkt installieren.*

- **Optionale Aktualisierung**

Bei optionalen Aktualisierungen werden Änderungen vorgenommen, die sich nicht auf die Programmfunktionen auswirken – z.B. Texte, Aktualisierungen der Installationskomponente usw. Optionale Aktualisierungen können heruntergeladen und zusammen mit empfohlenen Aktualisierungen übernommen werden, sie sind jedoch nicht besonders wichtig.

Beim Planen von Aktualisierungen können Sie auswählen, welche Prioritätsstufe heruntergeladen und angewendet werden soll. Höhere Aktualisierungsstufen enthalten automatisch auch die wichtigen Aktualisierungen.

Für eMail-Server werden folgende Aktualisierungszeiten werden empfohlen:

- Vorrangige Aktualisierung – alle zwei Stunden
- Empfohlene Aktualisierung – bei Bedarf oder einmal täglich

7.2. Aktualisierungsarten

Sie können zwischen zwei Aktualisierungsarten auswählen:

- **Aktualisierung bei Bedarf**

Eine Aktualisierung bei Bedarf ist eine Aktualisierung, die jederzeit ausgeführt werden kann, wenn entsprechender Bedarf besteht.

- **Geplante Aktualisierung**

Für AVG File Server oder AVG Anti-Virus kann auch ein Aktualisierungszeitplan vorgegeben werden. Die geplante Aktualisierung wird dann regelmäßig zu den festgelegten Zeiten ausgeführt. Wenn neue Aktualisierungsdateien verfügbar sind, werden diese heruntergeladen.

7.3. Aktualisierungs-Zeitplan

Die Aktualisierungsdateien können direkt aus dem Internet heruntergeladen werden. Damit Sie stets die neuesten Versionen der Aktualisierungsdateien erhalten, wird empfohlen, einen Aktualisierungsplan anzulegen, nach dem in regelmäßigen Abständen im Internet nach neuen Aktualisierungen gesucht wird.

Führen Sie folgende Schritte aus, um einen Aktualisierungszeitplan einzurichten:

a) **Aktualisierung – Control Center**

Wählen Sie im AVG Control Center mit der rechten Maus die Komponente Scheduler aus und wählen das Kontextmenü **Geplante Aufgaben**.

b) **Aktualisierung – Geplante Aufgaben**

Klicken Sie im neuen Dialogfeld **Geplante Aufgaben** auf **Neu**.

c) **Aktualisierung –Aufgabe / Reiter Aufgabe**

Nehmen Sie im neuen Dialogfeld **Aufgaben** auf der Registerkarte **Aufgabe** in der Liste der verfügbaren Möglichkeiten für den Punkt **Aktualisierung** eine Auswahl vor.

***Hinweis:** Es wird empfohlen, den Zeitplan für AVG 7.5 eMail Server für alle Benutzer nicht nur für den aktuellen Benutzer zu planen!*

d) **Aktualisierung – Aufgabe / Reiter Ausführen**

Sie können dann für beide Aktualisierungsarten auf der Registerkarte **Ausführen** die reguläre Aktualisierungszeit festlegen.

Sie können die Einstellungen für den Startzeitpunkt unter **Startzeitpunkt** aus einer Liste auswählen. Je nach Internetverbindung empfiehlt sich ein Intervall von 2 bis 6 Stunden für diese Aufgabe auf einem eMail-Server. Sie können den Startzeitpunkt jedoch auch nach eigenen Wünschen und Bedürfnissen festlegen und dann auch andere Zeitabstände entsprechend konfigurieren.

e) **Aktualisierung – Aufgabe / Verhalten und Fehler**

Auf den Registerkarten **Verhalten** und **Fehler** können Sie angeben, was geschehen soll, wenn beim Ausführen einer Aktualisierung die Server nicht reagieren oder wenn aus irgendeinem Grund der Zeitpunkt für die regelmäßige Aktualisierung ausgelassen wurde.

8. FAQ und technischer Support

Wenn bei der Installation von AVG 7.5 eMail Server Edition betriebliche oder technische Probleme auftreten, finden Sie auf der Grisoft-Website unter www.grisoft.com weitere Informationen im Bereich **FAQ**.

Wenn Sie dort keine Lösung finden, wenden Sie sich an den technischen Support unter technicalsupport@grisoft.com. Achten Sie darauf, dass Ihre AVG-Lizenznummer in der eMail enthalten ist.

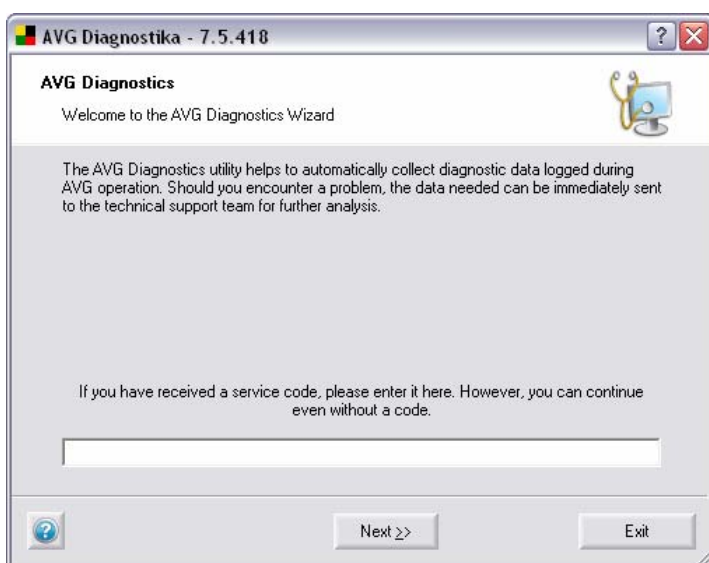
Es wird jedoch empfohlen, dass Sie sich über das Dialogfeld, auf das Sie in allen AVG-Anwendungen zugreifen können (z.B. AVG Test Center, AVG Control Center usw.), an den technischen Support von Grisoft wenden. Wählen Sie zum Öffnen des Dialogfelds im Hauptmenü der Anwendung im Ordner **Information** die Option **Technischer Support per eMail** aus. Fahren Sie anschließend mit Kapitel [8.1 Dienstprogramm AVG Diagnose](#) fort, in dem Sie weitere Informationen zu Anfragen an den technischen Support erhalten.

8.1. Dienstprogramm AVG Diagnose

AVG Diagnose ist ein unterstützendes Dienstprogramm, das der technische Support von AVG zur Verfügung stellt. Es dient in erster Linie dem Beziehen von Informationen vom Host-Computer. Anhand dieser Informationen kann der technische Support Ihre Probleme mit AVG leichter lösen. Dies erfolgt durch die Analyse von gesammelten Protokollen, Fehlerberichten, Systeminformationen, verdächtigen Dateien, Ihren Kommentaren und anderen Daten.

Hinweis: *AVG Diagnose versendet ohne Ihr ausdrückliches Einverständnis unter keinen Umständen private oder andere vertrauliche Daten, die sich auf Ihrem Computer befinden. Sie können den Inhalt aller gesammelten Dateien überprüfen und das Senden dieser Dateien an den technischen Support von AVG verhindern.*

- a) Nach dem Öffnen von AVG Diagnose werden Sie im folgenden Dialogfeld zur Eingabe eines Servicecodes aufgefordert:



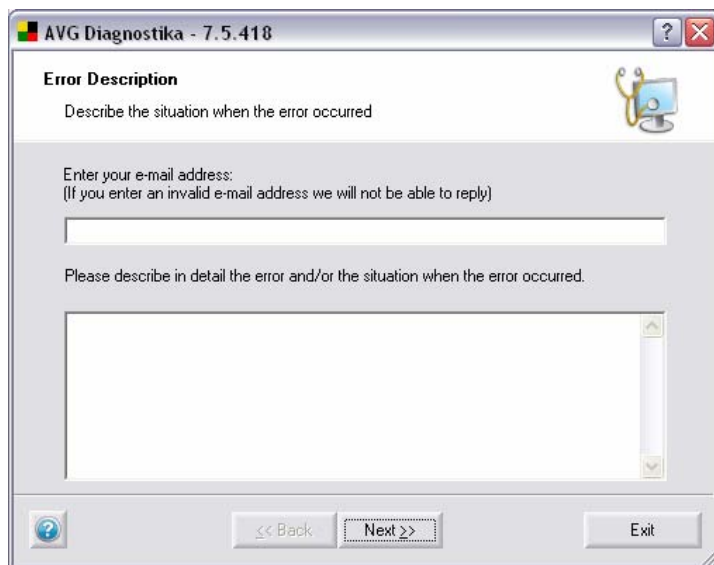
Wenn Sie einen Servicecode erhalten haben, geben Sie diesen direkt oder durch Kopieren und Einfügen im Textfeld ein. Der Code richtet automatisch den korrekten AVG Diagnose-Modus ein. Dieser stellt sicher, dass ausschließlich erforderliche (und keine redundanten) Daten während der AVG Diagnose-Sitzung gesammelt werden.

Wenn Sie nicht über einen Servicecode verfügen, können Sie aus den folgenden Optionen auswählen:

- Wenden Sie sich an den [technischen Support von AVG](#), und lassen Sie sich einen Servicecode für AVG Diagnose bereitstellen. Diese Option wird unerfahrenen Benutzern ausdrücklich empfohlen.
- Klicken Sie auf **Weiter**, und führen Sie AVG Diagnose im vollständigen Modus (Standardmodus) aus. Fahren Sie in diesem Fall mit Schritt [b – Fehlerbeschreibung](#) fort.
- Erfahrene Benutzer können AVG Diagnose schließen und den Anweisungen in Schritt [d\) Erweiterte Einstellungen – AVG Diagnose-Modi](#) folgen.

b) Fehlerbeschreibung

Über dieses Dialogfeld können den Daten eigene Kommentare und Ihre Kontaktinformationen hinzugefügt werden, die an den technischen Support von Grisoft gesendet werden.



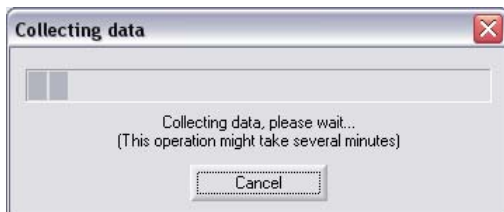
Beschreiben Sie das Problem bei der AVG Installation möglichst detailliert und geben Sie an, unter welchen Umständen das Problem auftritt. Der technische Support ist für die Bereitstellung jeglicher für die Problemlösung relevanten Informationen dankbar.

Geben Sie im Feld oben Ihre eMail-Kontaktadresse für den technischen Support ein.

Hinweis: In diesem Dialogfeld ist die Schaltfläche **Zurück** deaktiviert. Wenn Sie einen anderen Servicecode für AVG Diagnose eingeben möchten, müssen

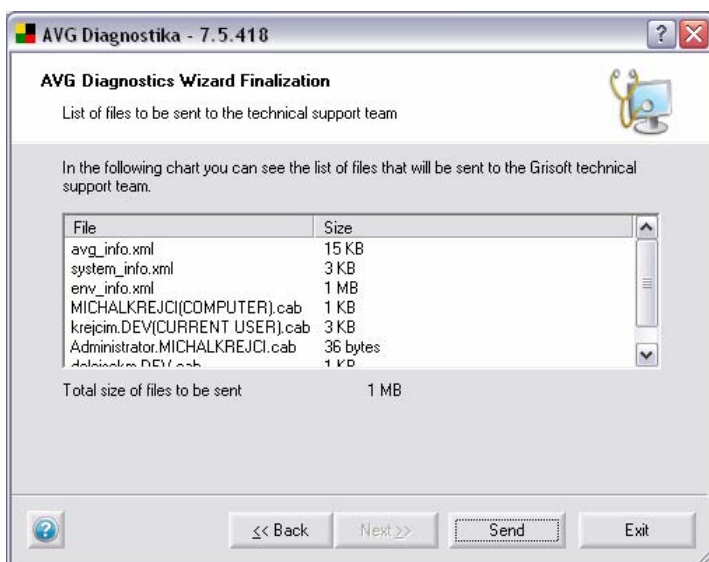
Sie die aktuelle Sitzung beenden und AVG Diagnose anschließend erneut starten.

Klicken Sie zum Fortfahren auf **Weiter**. AVG Diagnose beginnt mit dem Sammeln der Daten. Dieser Vorgang kann einige Zeit in Anspruch nehmen.



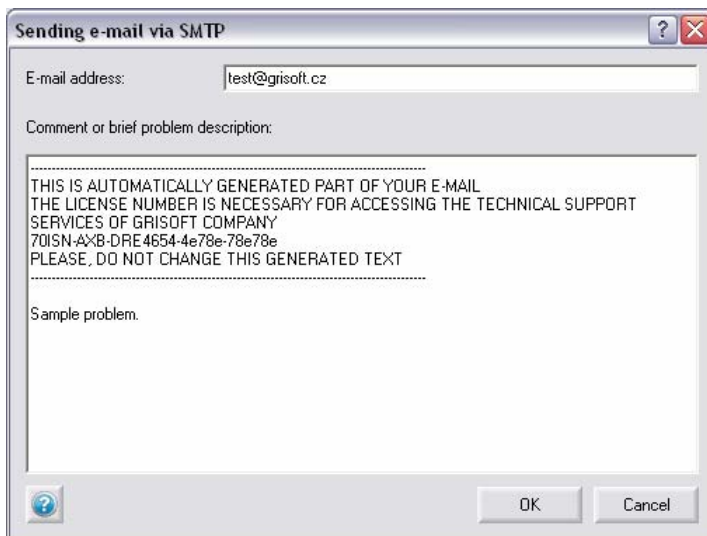
c) **AVG Diagnose-Assistenten fertig stellen**

Dieses Dialogfeld enthält eine Übersicht der Daten (Dateiname und -größe), die an den technischen Support von Grisoft gesendet werden. Außerdem wird die Gesamtgröße der Daten angezeigt.



Bestätigen Sie den Vorgang durch Klicken auf **Senden**. Es wird ein Dialogfeld mit den vorher eingegebenen Daten und Ihrer Lizenznummer angezeigt.

Hinweis: Wenn Sie den automatisch generierten Text der eMail ändern, der Ihre Lizenznummer enthält, erhalten Sie möglicherweise keine Antwort vom technischen Support von Grisoft!



Klicken Sie auf **OK**, um die Daten an den technischen Support von Grisoft zu senden. AVG Diagnose versendet die gesammelten Daten anschließend automatisch.

Hinweis: Wenn das Versenden des Berichts nicht möglich ist, überprüfen Sie, ob die Übertragung durch die Firewall blockiert wird.

d) **Erweiterte Einstellungen – AVG Diagnose-Modi**

Hinweis: Befolgen Sie diese Anweisungen nur dann, wenn Sie umfassend mit den erweiterten Funktionen von AVG Diagnose vertraut sind.

Wenn AVG Diagnose bereits ausgeführt wird, schließen Sie das Programm, und starten Sie es erneut über die Befehlszeile mit den entsprechenden Parametern für den jeweiligen AVG Diagnose-Modus.

Die AVG Diagnose-Modi dienen dem Sammeln der erforderlichen Diagnosedaten (redundante Daten werden ausgeschlossen). Jeder Modus legt ein bestimmtes Verhalten für das Dienstprogramm fest. Entsprechend dem Modus werden nur die Aktionen ausgeführt bzw. Dialogfelder angezeigt, die für den Benutzer erforderlich sind. Auf diese Weise wird der Gesamtprozess wesentlich beschleunigt.

Die AVG Diagnose-Modi können folgendermaßen festgelegt werden:

- automatisch durch einen Servicecode für AVG Diagnose (vom technischen Support von AVG in AVG Diagnose bereitgestellt)
- durch Ausführen von AVG Diagnose an der Befehlszeile mit den entsprechenden Parametern

Informationen zum Ausführen von AVG Diagnose an der Befehlszeile finden Sie auch in Schritt [e\) AVG Diagnose – Vollständige Übersicht über die Parameter](#).

Erforderliche Parameter und weitere Informationen zu den einzelnen AVG Diagnose-Modi können Sie dem entsprechenden Thema entnehmen:

- **Vollständige Diagnose**

Bei diesem Modus handelt es sich um den grundlegenden Modus von AVG Diagnose.

Im vollständigen Modus von AVG Diagnose werden umfassende Informationen über einen Computer zusammengestellt: Darin enthalten sind Protokolle und Systeminformationen sowie Informationen zur Konfiguration, zur Lizenz, zur Netzwerkumgebung und zu weiteren für die Problemlösung relevanten Bereichen.

Parameter: /MODE=FULL oder kein Parameter

o **Verdächtige Datei zur Analyse versenden**

In diesem Modus von AVG Diagnose können verdächtige Dateien zur Analyse an den technischen Support von Grisoft gesendet werden.

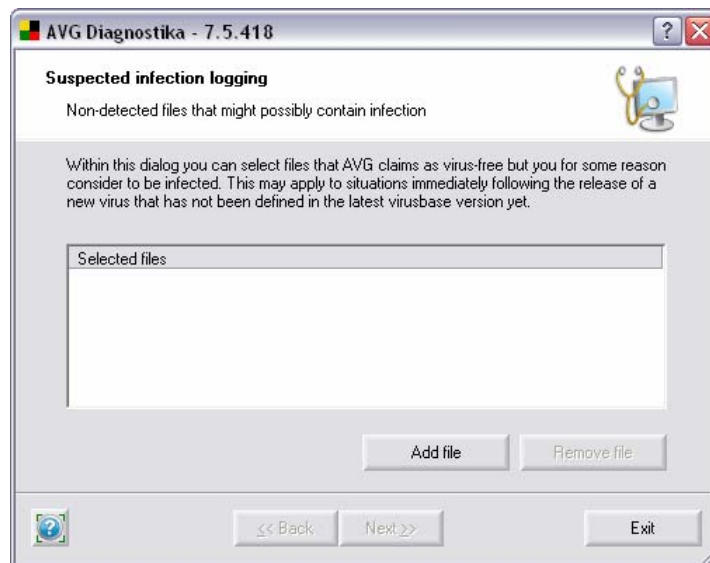
Bei *verdächtigen* Dateien handelt es sich um nicht von AVG erkannte Dateien, die infiziert oder unerwünschte Programme sein könnten.

Parameter: /MODE=VIRUS

So suchen Sie nach einer bestimmten verdächtigen Datei:

/FILE=<Datei>

Das Dialogfeld **Mögliche Infektionen protokollieren** wird angezeigt:



Über dieses Dialogfeld können Sie dem Bericht, der an den technischen Support von Grisoft gesendet wird, eine Datei hinzufügen.

Sie können auch eine Datei hinzufügen, die nicht von AVG erkannt wurde, von der Sie aber vermuten, dass sie infiziert ist.

Klicken Sie auf **Datei hinzufügen**, um die anzuhängende Datei auszuwählen. Sie können diesen Schritt beliebig oft wiederholen.

Klicken Sie auf **Datei entfernen**, um die markierte Datei aus der Liste zu löschen.

Klicken Sie zum Fortfahren auf **Weiter**.

- **Durch Fehlalarm erkannte Datei zur Analyse versenden**

In diesem Modus von AVG Diagnose können durch *Fehlalarm* erkannte Dateien zur Analyse an den technischen Support von Grisoft gesendet werden.

Ein Fehlalarm liegt vor, wenn eine Datei von AVG erkannt wurde, die Ihrer Meinung nach virenfrei ist.

Parameter: /MODE=FALSE

So suchen Sie direkt nach einer durch Fehlalarm erkannten Datei:

/FILE=<Datei>

- **Kunden-Feedback**

In diesem Modus von AVG Diagnose können Sie eigene Kommentare an den technischen Support von Grisoft senden.

An Ihre Nachricht werden AVG-Einstellungen und Systeminformationen angehängt.

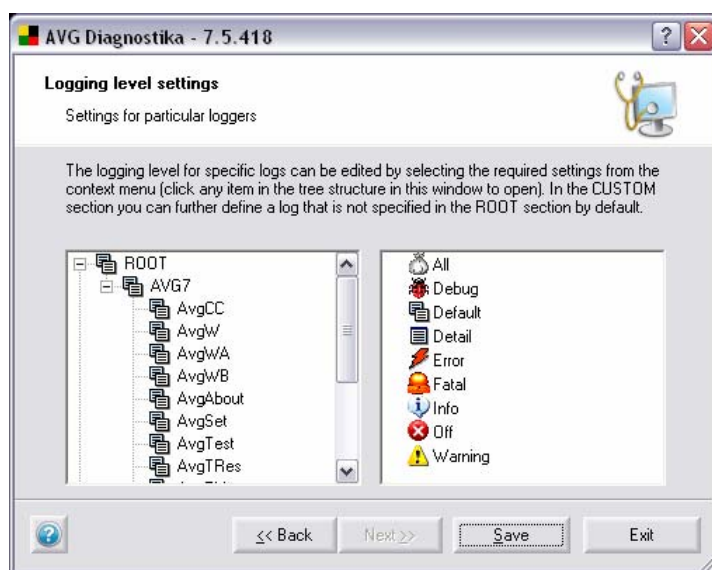
Parameter: /MODE=FEEDBACK

- **Protokollebenen-Einstellung**

In diesem Modus von AVG Diagnose können Sie eine Protokollebene für die AVG-Software festlegen. Auf diese Weise werden während der Verwendung von AVG nur die erforderlichen Informationen protokolliert, und der technische Support von Grisoft kann diese effizient verarbeiten.

Parameter: /MODE=LOGLEVEL

Eine Änderung dieser Einstellungen wird nur erfahrenen Benutzern empfohlen!



Im linken Bereich wird ein erweiterter Protokoll-Baum angezeigt. Der Zweig AVG7 enthält alle AVG-Protokolle. Im Zweig BENUTZERDEFINIERT kann ein neues Protokoll definiert werden (durch Doppelklicken auf <Neues Element>). Trennen Sie beim Angeben eines Pfads für den Logger die einzelnen Elemente durch einen Punkt, z. B. „AVG7.AvgWB.MeinProtokoll“.

Klicken Sie zum Entfernen eines benutzerdefinierten Protokolls mit der rechten Maustaste darauf, und wählen Sie **Protokoll entfernen** aus.

Sie können für jedes Baumelement eine spezifische Protokollebene festlegen. Die verfügbaren Ebenen werden rechts im Dialogfeld angezeigt. Klicken Sie mit der rechten Maustaste auf ein Element, und wählen Sie die gewünschte Protokollebene aus dem Kontextmenü aus. Wenn Sie die Auswahl für alle untergeordneten Protokolle übernehmen möchten, klicken Sie zunächst auf **Für alle übernehmen**.

Klicken Sie anschließend auf **Speichern**, um die Einstellungen zu übernehmen und zu speichern. (Die Schaltfläche **Weiter** ist in diesem Dialogfeld deaktiviert.)

Klicken Sie auf **Beenden**, um AVG Diagnose zu beenden.

- o **AVG Fehlererkennung**

In diesem Modus von AVG Diagnose können Sie ERR- und DMP-Dateien (nur nach einem Absturz des AVG-Programms vorhanden) erkennen und versenden. Das Fehlen dieser Dateitypen zeigt an, dass kein AVG-Fehler auftrat.

Wenn ein AVG-Fehler erkannt wird, wird ein Bestätigungsdialogfeld mit einer Übersicht der Fehlerdateien angezeigt, und Sie werden gefragt, ob Sie die Dateien zur Analyse versenden möchten.

Bei der nächsten Ausführung von AVG Diagnose im Modus **Fehlererkennung** werden nur neu erkannte Fehlerdateien berichtet.

Parameter: /MODE=ERRDUMP

e) **AVG Diagnose – Vollständige Übersicht über die Parameter**

Die nachfolgende Liste enthält eine Übersicht über alle Parameter von AVG Diagnose.

| Parameter | Beschreibung |
|---------------------------|---|
| <i>Kein Parameter</i> | Startet AVG Diagnose im vollständigen Modus (Standard). |
| <i>/CODE=<Code></i> | Ermöglicht die Eingabe des Servicecodes für AVG Diagnose, den Sie vom technischen Support von AVG erhalten haben. Der Code legt automatisch den erforderlichen Modus für AVG Diagnose fest. |

AVG 7.5 eMail Server

| | | | | | | | | | | | | | | | |
|-------------------------------------|---|-------------------------------------|-----------|-----------|-----------|--|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| <code>/MODE=FULL</code> | Startet AVG Diagnose im vollständigen Modus (Standard). | | | | | | | | | | | | | | |
| <code>/MODE=VIRUS</code> | Startet AVG Diagnose im Modus Verdächtige Datei zur Analyse versenden . | | | | | | | | | | | | | | |
| <code>/MODE=FALSE</code> | Startet AVG Diagnose im Modus Durch Fehlalarm erkannte Datei zur Analyse versenden . | | | | | | | | | | | | | | |
| <code>/MODE=FEEDBACK</code> | Startet AVG Diagnose im Modus Kunden-Feedback . | | | | | | | | | | | | | | |
| <code>/MODE=LOGLEVEL</code> | Startet AVG Diagnose im Modus Protokollebenen-Einstellung . | | | | | | | | | | | | | | |
| <code>/MODE=ERRDUMP</code> | Startet AVG Diagnose im Modus AVG Fehlererkennung . | | | | | | | | | | | | | | |
| <code>/LOGROOT=<Ebene></code> | Legt automatisch den Modus Protokollebenen-Einstellung fest und ermöglicht die direkte Auswahl einer Protokollebene. | | | | | | | | | | | | | | |
| <code>/FILE=<Datei></code> | Ermöglicht in den Modi Verdächtige Datei zur Analyse versenden und Durch Fehlalarm erkannte Datei zur Analyse versenden die Direktsuche nach den entsprechenden Dateien. Ermöglicht im vollständigen Modus (Standard) das Anhängen einer zusätzlichen Datei an den Bericht. | | | | | | | | | | | | | | |
| <code>/CLEARUPD</code> | Löscht veraltete Aktualisierungs- sowie temporäre Dateien. | | | | | | | | | | | | | | |
| <code>/NOUI</code> | Minimiert die Anzahl der angezeigten Dialogfelder. | | | | | | | | | | | | | | |
| <code>/LNG=<Sprache></code> | Ermöglicht das Ändern der Spracheinstellungen für die Benutzeroberfläche von AVG Diagnose. <table border="1" data-bbox="630 1438 1295 1839"> <tr> <td rowspan="4">Verfügbare Sprachen und ihre Codes:</td> <td>DE=0x0407</td> <td>PB=0x0416</td> </tr> <tr> <td>CZ=0x0405</td> <td></td> </tr> <tr> <td>SK=0x041b</td> <td>FR=0x040c</td> <td>PL=0x0415</td> </tr> <tr> <td>US=0x0409</td> <td>ES=0x040a</td> <td>SC=0x081a</td> </tr> <tr> <td>IT=0x0410</td> <td>HU=0x040e</td> <td>NL=0x0413</td> </tr> </table> | Verfügbare Sprachen und ihre Codes: | DE=0x0407 | PB=0x0416 | CZ=0x0405 | | SK=0x041b | FR=0x040c | PL=0x0415 | US=0x0409 | ES=0x040a | SC=0x081a | IT=0x0410 | HU=0x040e | NL=0x0413 |
| Verfügbare Sprachen und ihre Codes: | DE=0x0407 | | PB=0x0416 | | | | | | | | | | | | |
| | CZ=0x0405 | | | | | | | | | | | | | | |
| | SK=0x041b | | FR=0x040c | PL=0x0415 | | | | | | | | | | | |
| | US=0x0409 | ES=0x040a | SC=0x081a | | | | | | | | | | | | |
| IT=0x0410 | HU=0x040e | NL=0x0413 | | | | | | | | | | | | | |