

# **AVG 7.5 File Server Edition**

## Benutzerhandbuch

Document revision 75.3 (31.10.2006)

**Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.**

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek <dolecek@ics.muni.cz>

This product uses compression library zlib, Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler  
All other trademarks are property of their respective owners.

## **Inhalt**

<b>1. Einleitung</b> .....	<b>5</b>
1.1. Anti-Virus Erkennungsmethoden und Schutzlevels .....	5
1.2. Schutz vor Spyware.....	6
1.3. Unterstützte Betriebssysteme .....	6
1.4. Gründe zur Installation der AVG 7.5 File Server Edition.....	7
<b>2. Installation</b> .....	<b>8</b>
2.1. Installation aus dem Internet.....	8
<b>3. Installationsprozess</b> .....	<b>9</b>
3.1. Installation – Willkommendialog .....	9
3.2. Installation – Lizenzvertrag.....	9
3.3. Installation – Auswahl des Installationstyps .....	10
3.4. Installation – Zusammenfassung .....	17
3.5. Installation – Beenden der Anwendungen .....	18
3.6. Installation – Installation ist fertig! .....	19
<b>4. AVG Erste-Schritte</b> .....	<b>21</b>
4.1. Erste Schritte-Assistent.....	21
4.2. AVG Programmstart.....	23
<b>5. Nach der Installation</b> .....	<b>24</b>
5.1. Durchführung des kompletten Tests.....	24
5.2. Einstellen der Option "Beim Schliessen kontrollieren" .....	24
5.3. Eicar Test.....	24
5.4. Test und Aktualisierungsplanung .....	25
<b>6. Produkt-Registrierung</b> .....	<b>26</b>
<b>7. AVG Basis Oberfläche</b> .....	<b>27</b>
7.1. Umschalten auf die Advanced Oberfläche.....	28
7.2. Control Center .....	28
7.3. Virenquarantäne .....	28
7.4. Test Ergebnisse .....	28
7.5. Aktualisierungen .....	33
7.6. Programm beenden .....	34
7.7. Testeinstellungen .....	34
7.8. Testplanung .....	35
7.9. Programmeinstellungen.....	35

7.10. Rettungsdiskette .....	37
7.11. Aktualisierungs-Scheduler .....	38
7.12. Ereignisprotokoll .....	39
7.13. Sprachauswahl.....	39
7.14. Potentiell unerwünschte Programme - Ausnahmen .....	40
7.15. Informationen.....	42
<b>8. AVG Advanced Oberfläche.....</b>	<b>46</b>
8.1. Testmanager .....	47
8.2. Geplante Aufgaben .....	47
8.3. Testergebnisse .....	49
8.4. Programmeinstellungen.....	51
8.5. Aktualisierung.....	57
8.6. Rettungsdiskette.....	58
8.7. Virenenzyklopädie .....	59
8.8. Informationen.....	60
8.9. Hilfethemen .....	60
<b>9. Control Center.....</b>	<b>61</b>
9.1. Start des AVG Control Center.....	61
9.2. AVG Control Center linkes Menü .....	62
9.3. AVG Control Center Hauptmenü .....	64
9.4. AVG Komponenten im Control Center .....	65
9.5. Control Center-Symbol in der Systemablage .....	66
9.6. Komponenten, die vom AVG Control Center kontrolliert werden .....	66
9.7. Control Center – Anti-Virus.....	66
9.8. Control Center – Anti-Spyware .....	68
9.9. Control Center - Scheduler .....	68
9.10. Control Center - Residenter Schutz .....	69
9.11. Control Center - Virenquarantäne .....	75
9.12. AVG Control Center - Aktualisierungsmanager .....	77
9.13. Control Center - Shell Erweiterung.....	83
9.14. AVG Control Center - eMail Kontrolle .....	88
<b>10. Control Center Alarm Manager .....</b>	<b>92</b>
10.2. Control Center - Lizenz.....	99
<b>11. Virenquarantäne .....</b>	<b>102</b>
11.1. Verschieben verdächtiger Objekte in die Virenquarantäne .....	102
11.2. Virenquarantäne Umgebung.....	102

11.3. Verwalten der Virenquarantäne .....	103
<b>12. Test Übersicht .....</b>	<b>105</b>
12.1. Kompletter Test .....	105
12.2. Benutzertest .....	120
12.3. Ausgewählte Bereiche Test .....	121
12.4. Ausführliche Tests .....	124
12.5. AVG eMail-Kontrolle .....	124
12.6. Start eines Test von der Kommandozeile .....	125
<b>13. Programm Aktualisierungen .....</b>	<b>127</b>
13.1. Aktualisierungslevels.....	127
13.2. Aktualisierungsarten .....	127
13.3. Aktualisierungsplan.....	128
<b>1. Terminal Services Server Modus .....</b>	<b>133</b>
1.1 Installations-Hinweise.....	133
1.2 Geplante Aufgaben.....	133
<b>14. AVG Alarm Manager .....</b>	<b>134</b>
14.1. Ereignisse und Aktionen .....	134
14.2. Alarm Manager-Regeln .....	134
14.3. Regelkonfiguration.....	135
<b>15. FAQ und technischer Support.....</b>	<b>142</b>
15.1. AVG Diagnoseprogramm.....	143

## 1. Einleitung

Dies ist ein umfassendes Benutzerhandbuch zu **AVG 7.5 File Server Edition**.

### 1.1. Anti-Virus Erkennungsmethoden und Schutzlevels

**Anti-Virus** verwendet die folgenden Methoden, um Computerviren zu erkennen:

- **Scannen** – sucht nach charakteristischen Zeichenfolgen, die charakteristisch für ein bestimmtes Virus sind
- **Heuristische Analyse** – dynamische Emulation für die Anweisungen der durchsuchten Objekte in einer virtuellen Computerumgebung
- **Generische Entdeckung** – Entdeckung von Anweisungen, die charakteristisch für bestimmte Viren/Virengruppen sind

Da eine einzelne Methode eventuell ein Virus übersehen könnte, verbindet AVG verschiedene Methoden um zu gewährleisten, dass Ihr Computer geschützt ist.

AVG kann auch ausführbare Anwendungen oder DLL-Bibliotheken erkennen und analysieren, die innerhalb des Systems potentiell unerwünscht sein könnten. Wir nennen solche Bedrohungen **Potentiell Unerwünschte Programme** (PUP). Solch ein Programm kann z.B. eine Art Spyware, Adware usw. sein. Aufgrund der Anforderungen für die Benutzer kann AVG solche Programme entfernen oder den Zugang dazu sperren.

Außerdem überprüft AVG Ihre System-Registry auf verdächtige Eingänge, temporäre Internet-Dateien und verfolgende Cookies und ermöglicht Ihnen, alle potentiell schädlichen Programme auf die gleiche Weise zu behandeln, wie jede andere Infektion.

Es gibt verschiedene Möglichkeiten, wie ein Virus in Ihren Computer gelangen kann. Zum Beispiel über eine infizierte eingehende eMail, wobei das Virus durch den Empfang der Nachricht aktiviert und auf der Festplatte gespeichert wird und sich nun von dort aus verbreiten kann. Ein Virenschutz-Programm, das sich nur auf einen Entdeckungslevel konzentriert, kann eventuell an der Isolierung des Virus scheitern. AVG ermöglicht Ihnen jedoch, Virentests auf verschiedenen Levels durchzuführen – z.B. beim Empfang von eMails oder beim Arbeiten mit Dateien auf Ihrem Computer. Sie können einen Test auch auf Anforderung (On-Demand) ausführen. Die folgende Liste beschreibt jeden einzelnen Level:

#### a) eMail-Kontrolle

überprüft eingehende und ausgehende eMails über Plugins für die am häufigsten verwendeten eMail Programme. Die **eMail-Kontrolle** ist ein zusätzliches Programm zur Überwachung von eMails; dies kann im automatischen Modus durchgeführt werden oder Sie können sie Ihren Bedürfnissen entsprechend konfigurieren. Die **eMail-Kontrolle** wurde für Programme entwickelt, die das POP3/SMTP Protokoll verwenden. Sobald Viren entdeckt werden, werden diese in die **Virenquarantäne** verschoben (und dort sicher verwahrt). Einige eMail-Clients unterstützen eine Zertifizierungsnachricht, die besagt, dass die versendete bzw. empfangene eMail auf Viren überprüft wurde. Eine weitere Komponente, die den Sicherheitslevel der eMails erhöht, ist der Anhangsfilter, in dem unerwünschte und verdächtige Dateiendungen definiert werden können.

## b) Residenter Schutz

Der **Residente Schutz** überprüft Dateien, während diese kopiert, geöffnet und gespeichert werden. Sobald der **Residente Schutz** ein Virus in einer Datei entdeckt, auf die zugegriffen wird, stoppt er den aktuell gestarteten Arbeitsablauf und verhindert dadurch die Aktivierung des Virus selbst. Der **Residente Schutz** wird während des Computerstarts in den Speicher Ihres Computers geladen und sorgt weiterhin für einen Schutz der Systembereiche Ihres Computers.

## c) Tests

Das Scannen ist der wesentliche Teil der Funktion von AVG. Sie können On-Demand Tests durchführen oder die Tests so planen, dass sie periodisch zu voreingestellten Zeiten durchgeführt werden. Verwenden Sie entweder die voreingestellten Tests oder erstellen Sie Ihre eigenen benutzerdefinierten Tests.

## 1.2. Schutz vor Spyware

Spyware wird normalerweise als eine Art von Malware angesehen; z.B. Software, die Informationen von einem Computer sammelt, ohne dass der Benutzer darüber Bescheid weiß oder sein Einverständnis gibt. Einige Spyware- Anwendungen können auch absichtlich installiert werden und enthalten oftmals Werbungen, Pop-Ups oder verschiedene Arten unangenehmer Software.

Im Idealfall sollten Sie Ihren Computer vor dem Eindringen von Spyware und anderen schädliche Programme schützen. Aktuell ist die am weitesten verbreitete Quelle für Infektionen Webseiten mit potentiell gefährlichem Inhalt. Andere Methoden für die Übertragung, wie z.B. über eMails oder über Würmer und Viren sind auch sehr verbreitet. Der wichtigste Schutz besteht darin, immer einen Scanner im Hintergrund laufen zu haben, wie z.B. Grisoft's Komponente **Anti-Spyware**, die wie ein residenter Schutz arbeitet und Ihre Anwendungen beim Ablauf im Hintergrund scannt.

Außerdem besteht noch das potentielle Risiko, dass bösartige Programme auf Ihren Computer übertragen wurden, bevor Sie AVG installiert haben oder dass Sie versäumt haben, Ihr AVG mit den neuesten Aktualisierungen der Datenbank und der Programme auf dem Laufenden zu halten. Aus diesem Grund ermöglicht Ihnen AVG, mit dem Scanner Ihren Computer vollständig auf schädliche Programme/Spyware überprüfen zu lassen. Der Scanner erkennt auch *schlafende und nicht gefährliche* schädliche Programme, d.h. schädliche Programme, die herunter geladen wurden aber noch nicht aktiviert worden sind.

## 1.3. Unterstützte Betriebssysteme

**AVG 7.5 File Server Edition** ist vorgesehen, Server mit den folgenden Betriebssystemen zu schützen: Windows NT/9x/Me/2000/XP einschließlich der 64-bit-Versionen.

-Windows 2003 Server

-Windows 2000 Server

-Windows NT 4.0 Server

Einschliesslich der 64-bit Versionen

**Anmerkung:** Einige ältere Betriebssysteme, wie Windows 95/98/Me unterstützen nicht das Scannen von geöffneten Dateien durch die Komponenten Anti-Spyware.

## 1.4. Gründe zur Installation der AVG 7.5 File Server Edition

Unter folgenden Bedingungen sollten Sie die AVG 7.5 File Server Edition auf Ihrem Server installieren:

Der Server wird zur Datenspeicherung im Netzwerk verwendet

AVG 7.5 File Server Edition ist in der Lage alle Dateien zu prüfen, sobald sie auf das Laufwerk des Servers gespeichert werden, und Viren oder potentiell schädliche Software zu erkennen, die den gespeicherten Daten schaden könnten. Ebenso werden Dateien beim Zugriff der Clients geprüft, wenn sie diese öffnen oder auf ihre Arbeitsstationen kopieren.

Der Server wird als "Terminal Server" verwendet

Wenn Ihr Server den Anwendern Remotezugriff und das direkte Arbeiten auf dem Server gestattet (wenn er z.B. als Terminal Server genutzt wird) ist Ihr Server ebenfalls möglichen Schädlingen und Virenangriffen ausgesetzt. In diesem Fall sollten Sie definitiv die AVG 7.5 File Server Edition installieren. Der Server benötigt die AVG 7.5 File Server Edition zur weiteren Viren/Malware Überprüfung. Um zum Beispiel einen Microsoft Share Point Portal Server 2003 schützen wollen, müssen Sie zunächst die AVG 7.5 File Server Edition installieren.

## 2. Installation

AVG kann entweder über die Installationsdatei installiert werden, die sich auf der Installations-CD befindet oder Sie können die aktuelle Installationsdatei von der **Grisoft** Webseite – <http://www.grisoft.de> im Abschnitt **DOWNLOADS -> Programme** herunterladen.

*Bevor Sie mit der Installation von AVG starten, empfehlen wir dringend, die Grisoft Produkt Downloadseite aufzusuchen, um zu überprüfen, ob eine neue Installationsdatei verfügbar ist. Auf diese Weise können Sie sicherstellen, dass Sie die aktuellste Version von AVG installieren.*

Während der Installation werden Sie aufgefordert, Ihre Lizenz-/Vertriebsnummer anzugeben. Bitte halten Sie diese Nummer vor dem Start der Installation bereit. Die Lizenz/Vertriebsnummer finden Sie auf einer Registrierungskarte im AVG-Paket. Wenn Sie AVG über das Internet erworben haben, wurde Ihnen die Lizenz/Vertriebsnummer per eMail zugeschickt.

### 2.1. Installation aus dem Internet

Um AVG aus dem Internet zu installieren, folgen Sie bitte diesen Schritten:

- a) Gehen Sie auf die **Grisoft** Webseite und laden Sie sich die aktuelle Version des Installationspaketes zu **AVG 7.5 File Server Edition** unter <http://www.grisoft.de> im Abschnitt **DOWNLOADS -> Programme**, herunter.
- b) Laden Sie die Datei herunter und speichern Sie diese auf Ihrer Festplatte.
- c) Starten Sie die herunter geladene Installationsdatei aus dem Verzeichnis, in das Sie sie beim Herunterladen gespeichert haben.

## 3. Installationsprozess

### 3.1. Installation – Willkommendialog

Im Installationsdialog Willkommen werden Sie aufgefordert, die Sprache für die Anwendung auszuwählen.

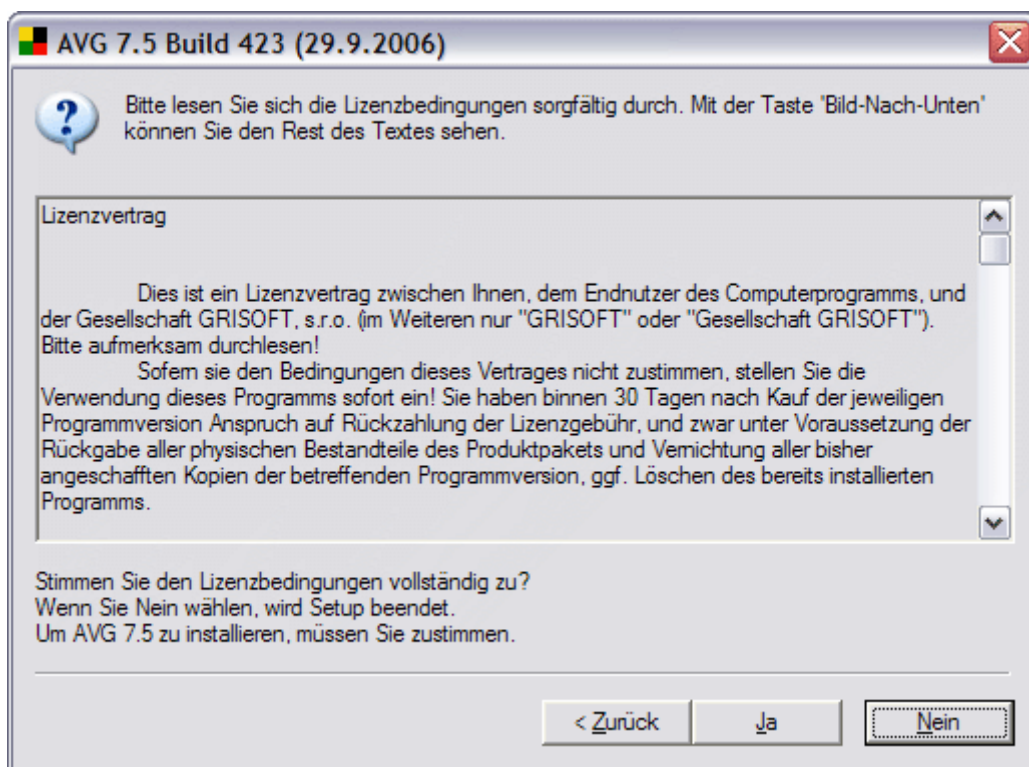
**Anmerkung:** Standardmäßig werden nur zwei Sprachen für die Anwendung installiert; die Sprache, die Sie wählen und die englische Sprache (Standardeinstellung). Wenn Sie die englische Sprache wählen, so wird nur Englisch installiert, Sie können im Dialog **Komponentenauswahl** wählen, dass zusätzliche Sprachen installiert werden (später während der Installation).

Drücken Sie bitte die Schaltfläche **Weiter**, um Ihre Auswahl zu bestätigen:



### 3.2. Installation – Lizenzvertrag

Der folgende Dialog zeigt den vollständigen Wortlaut der Lizenzbedingungen an. Lesen Sie diese sorgfältig durch und wenn Sie diesen zustimmen, klicken Sie auf die Schaltfläche **Ja**. Andernfalls wird der Installationsprozess an dieser Stelle abgebrochen.



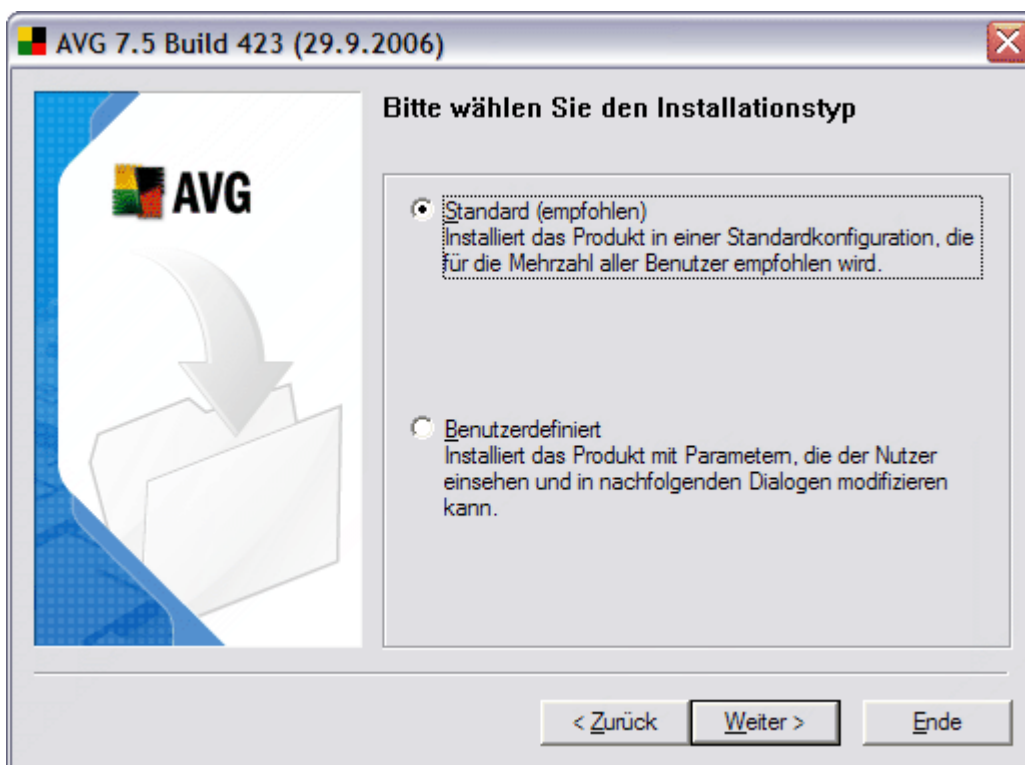
### 3.3. Installation – Auswahl des Installationstyps

In diesem Dialogfenster müssen Sie sich zwischen zwei Installationstypen entscheiden: **Standard** und **Benutzerdefiniert**.

#### a) Standard-Installation

Die Standard-Installation installiert AVG automatisch mit der voreingestellten Konfiguration aller Komponenten. Wenn Sie keine besonderen Anforderungen an die Konfiguration einiger AVG-Komponenten haben, empfehlen wir Ihnen dringend die Auswahl dieser Option (Sie können alle AVG-Komponenteneinstellungen auch nach Beendigung der Standard-Installation konfigurieren).

## AVG 7.5 File Server



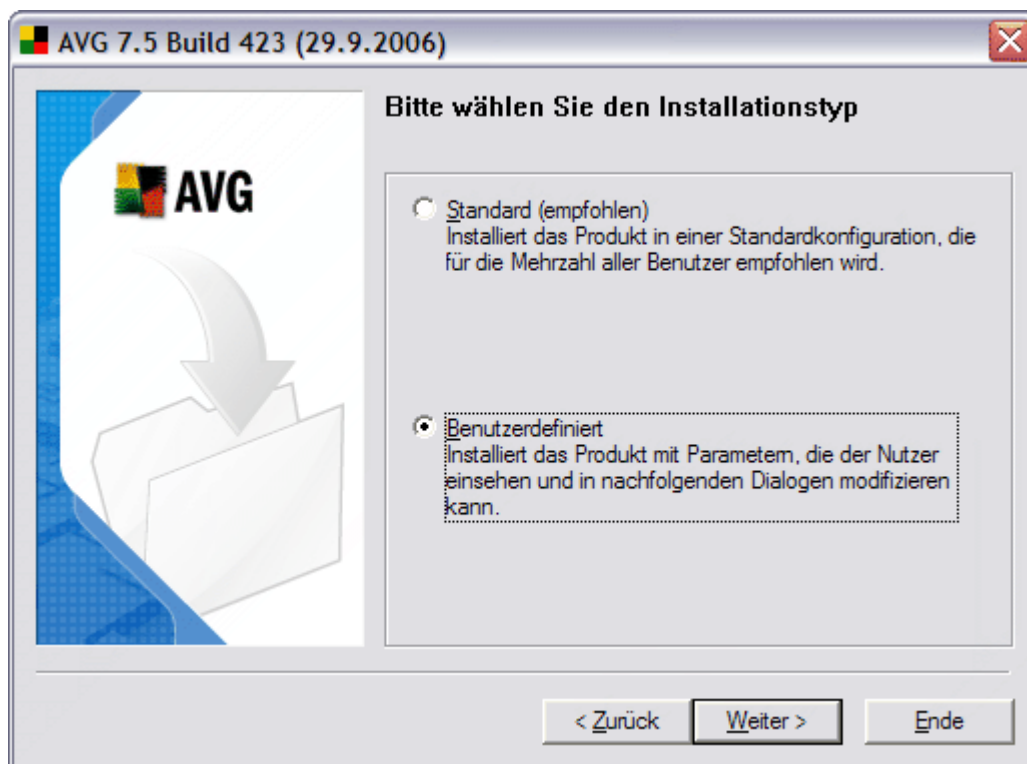
Bestätigen Sie die Option **Standard** durch Drücken der Schaltfläche **Weiter**; Sie gelangen nun zum Dialog **AVG 7.5 personalisieren**, in dem Sie Ihren Namen/Firmennamen und Ihre Lizenznummer angeben müssen:



Bestätigen Sie die eingegebenen Lizenzdaten wieder durch Drücken der Schaltfläche **Weiter**. Danach gelangen Sie zum Dialog [Installationszusammenfassung](#).

#### b) Benutzerdefinierte Installation

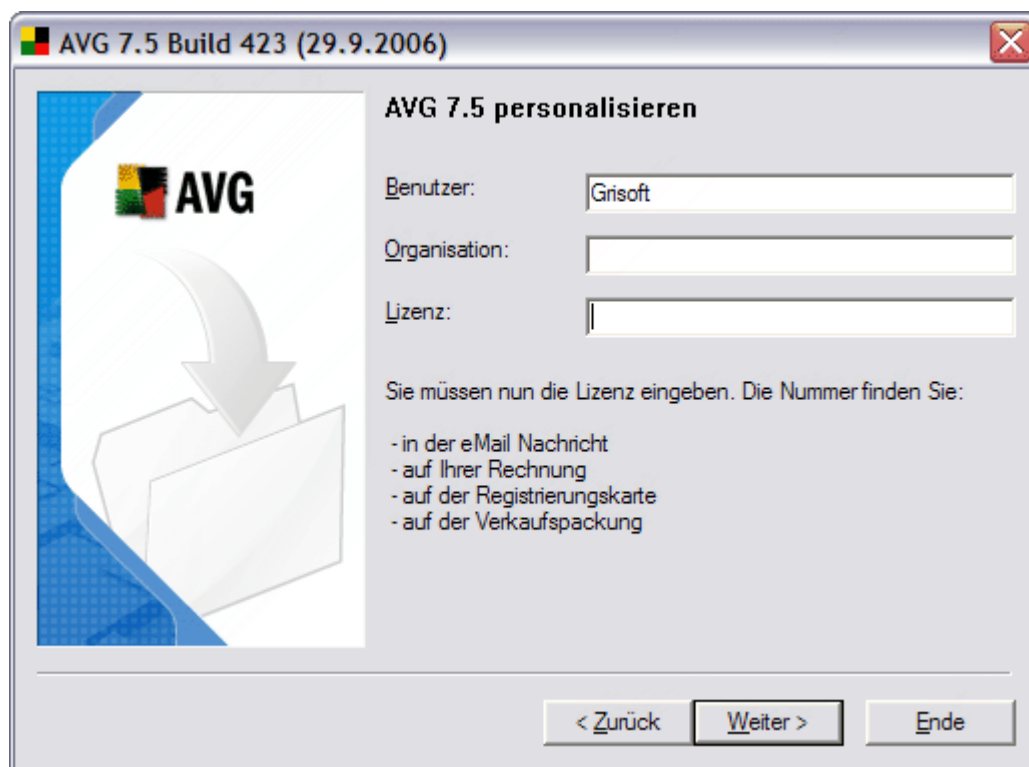
Die benutzerdefinierte Installation wird nur erfahrenen Benutzern empfohlen, die besondere Anforderungen an die Konfiguration der AVG-Komponenten haben und die die Einstellungen bereits während des Installationsprozesses vornehmen möchten. Sie haben jedoch auch die Möglichkeit, alle AVG-Komponenten nach Beendigung der Installation zu konfigurieren.



Bestätigen Sie Ihre Auswahl durch Betätigen der Schaltfläche **Weiter**; nun gelangen Sie zum nächsten Dialog der benutzerdefinierten Installation:

#### o **AVG 7.5 personalisieren**

Im Dialog **AVG 7.5 personalisieren** müssen Sie Ihren Namen/Firmennamen und Ihre gültige Lizenznummer angeben:



○ **Zielverzeichnis**

Im Dialog Zielverzeichnis können Sie den Pfad zu dem Verzeichnis angeben, in das Sie AVG installieren möchten. Falls nicht anders angegeben, wird das Programm im vordefinierten Verzeichnis (siehe Bild) installiert. Sie können den Verzeichnispfad entweder manuell eingeben oder Sie können den Installationsort mit Hilfe der Schaltfläche **Durchsuchen** auswählen.



- **Komponentenauswahl**

In dem Dialog **Komponentenauswahl** definieren Sie, welche AVG-Komponenten installiert werden sollen. Standardmäßig werden alle vorhandenen Komponenten ausgewählt und installiert. Wir empfehlen, dass Sie diese Einstellung beibehalten, solange Sie keinen wichtigen Grund für eine Änderung haben. Wenn keine Komponente ausgewählt ist, wird das Programm deinstalliert.

Achten Sie auf die Option **Weitere installierbare Sprachen**, in der Sie ein oder mehrere weitere Sprachen auswählen können. Standardmäßig werden nur Englisch und die zu Beginn der Installation festgelegte Sprache installiert.

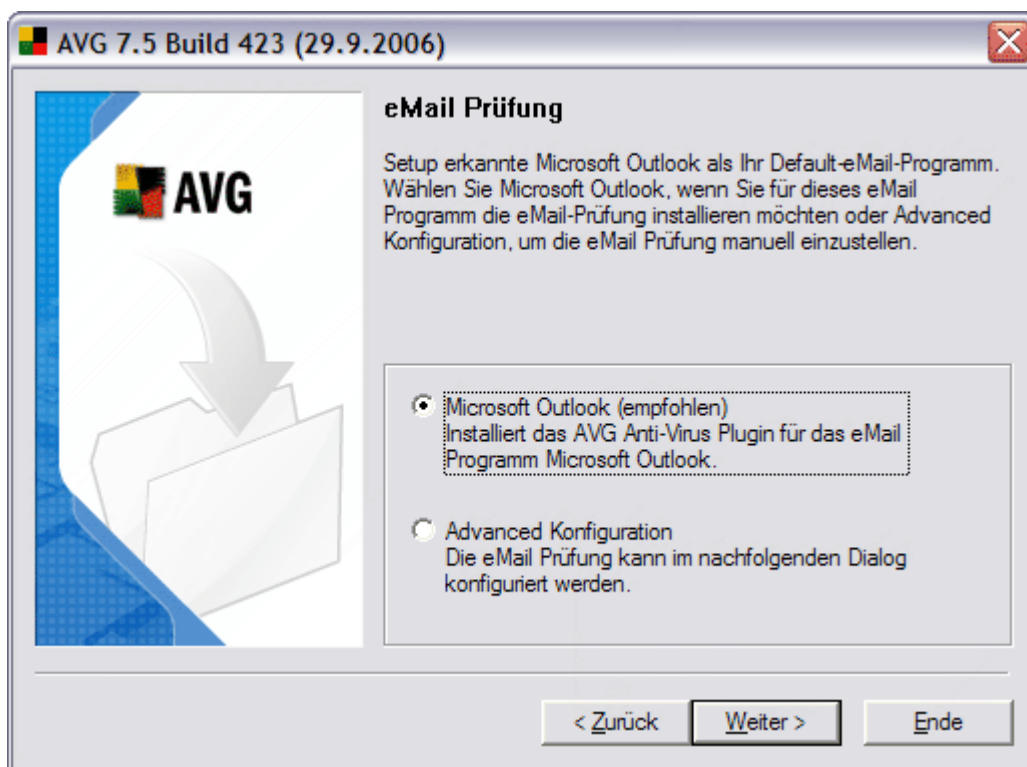


- **eMail Prüfung**
- **Die eMail-Prüfung der AVG 7.5 File Server Edition eignet sich nur zum Schutz des eMail-Clients auf dem Fileserver. Da es nicht üblich ist, einen eMail-Client auf einem Fileserver zu installieren, wird die eMail-Prüfung standarmässig nicht installiert. Wenn Sie im vorhergehenden Dialog die Installation der eMail-Prüfung ausgewählt haben, führen Sie bitte die folgenden Schritte durch, um die Überprüfung Ihrer eMail einzurichten.**

**Hinweis: die eMail-Prüfung eignet sich nicht, um die gesamten Mails auf einem Mailserver zu prüfen. Zur Prüfung der gesamten Mails auf einem Mailserver verwenden Sie bitte die AVG 7.5 eMail Server Edition.**

**- Empfohlene Konfiguration**

AVG ermöglicht Ihnen die Überprüfung Ihrer Mails unter Verwendung der Programm-Plugins für die am häufigsten verbreiteten eMail Programme: MS Outlook, MS Exchange, The BAT!, Qualcomm Eudora. Wenn Sie eines dieser Programme verwenden, erkennt das Setup-Programm dies automatisch und empfiehlt Ihnen die Installation eines direkten Plugins für Ihr eMail-Programm (siehe Bild).



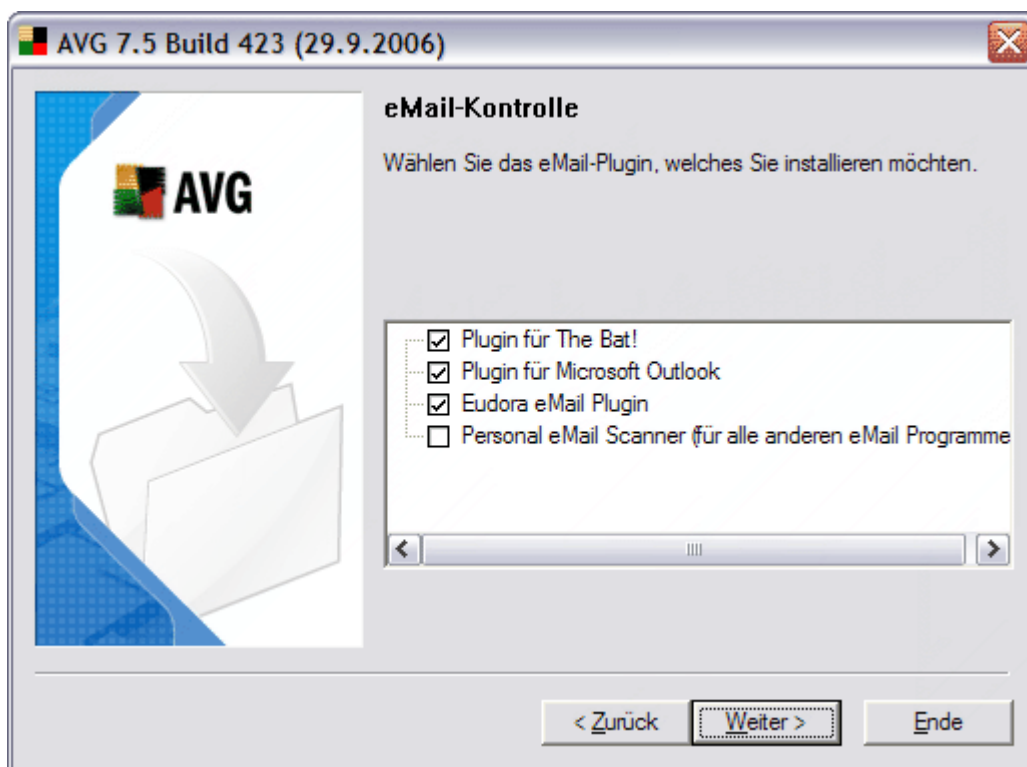
Für andere eMail-Programme stellt Ihnen AVG einen umfassenden eMail-Schutz unter Verwendung der Komponente **eMail-Kontrolle** zur Verfügung. Für diesen Fall bietet der Setup Dialog die empfohlene Option **Personal eMail Scanner**.

Bestätigen Sie die Konfiguration durch Betätigen der Schaltfläche **Weiter**. Sie gelangen nun zum Dialog [Installationszusammenfassung](#).

- **Advanced Konfiguration**

Wenn Sie die eMail-Überprüfung manuell konfigurieren möchten, wählen Sie bitte die Option **Advanced Konfiguration** aus. Diese Option wird nur erfahrenen Benutzern empfohlen!

Die Konfiguration wird in dem folgenden Dialog durchgeführt:



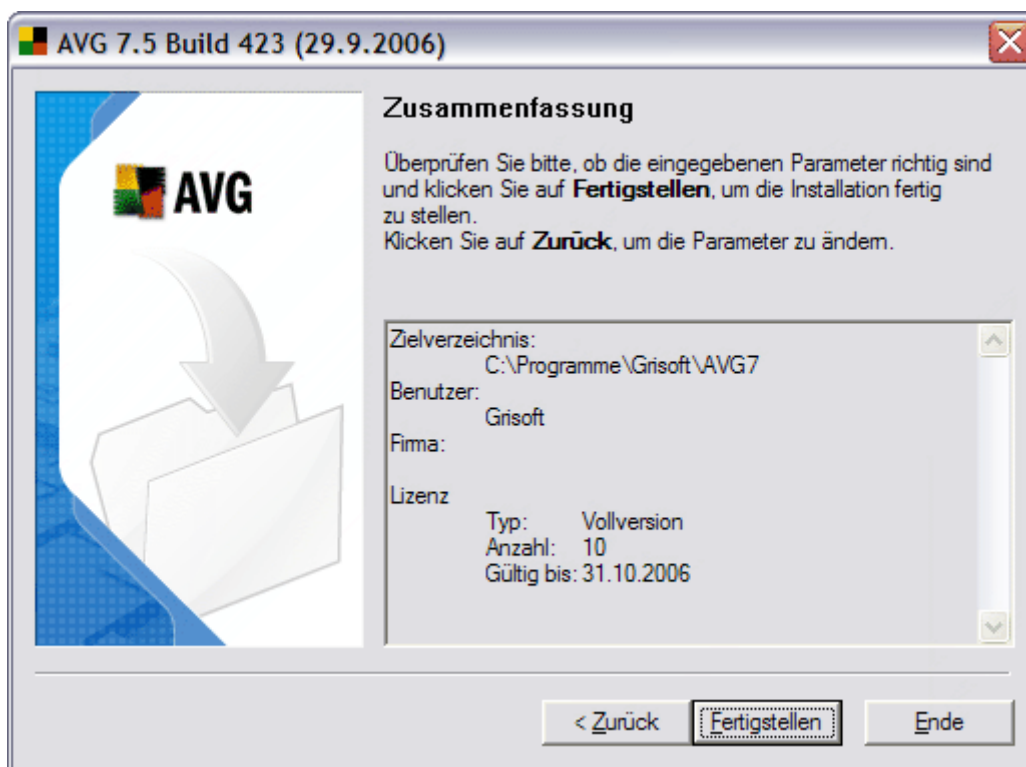
Sie können ein Plugin für das eMail-Programm auswählen, das Sie verwenden. Wenn Ihr eMail-Programm nicht direkt unterstützt wird, wählen Sie bitte die Option **Personal eMail Scanner** aus.

**Anmerkung:** Der *Personal eMail-Scanner* wird vollständig automatisch installiert und ausgeführt. Die Konfiguration hierfür kann auch manuell eingestellt werden – für weitere Details besuchen Sie bitte den Bereich <http://www.grisoft.de> -> FAQ -> Technische FAQs.

Drücken Sie die Schaltfläche **Weiter**, um Ihre Auswahl zu bestätigen und um mit dem Dialog [Zusammenfassung](#) fortzufahren.

### 3.4. Installation – Zusammenfassung

Der Dialog **Zusammenfassung** bietet Ihnen einen Überblick über alle installierten Parameter.



### 3.5. Installation – Beenden der Anwendungen

Einige der Programme, die auf Ihrem PC gerade ausgeführt werden, können Probleme während des Installationsprozesses verursachen. In diesem Fall öffnet sich das Dialogfenster **Beenden der Anwendungen**, das eine Liste aller Programme anzeigt, die zum Fertigstellen des Installationsprozesses geschlossen werden müssen. Sie können die aufgelisteten Programme manuell schließen oder die Programme werden automatisch vom Setup geschlossen, nachdem Sie auf die Schaltfläche **Weiter** geklickt haben:



### 3.6. Installation – Installation ist fertig!

Der Installationsprozess ist beendet, sobald das Dialogfenster **Installation ist fertig!** erscheint. „**Computer jetzt neu starten**“ ist standardmäßig markiert und wir empfehlen Ihnen dringend, dies beizubehalten. Bestätigen Sie dies durch Drücken der Schaltfläche **OK**.



**Anmerkung:** Sollte der Installationsprozess aus irgendeinem Grund fehlschlagen, wird im letzten Dialogfenster zusätzlich die Schaltfläche *Details* angezeigt. Drücken Sie diese Schaltfläche, um eine Übersicht über alle diagnostischen Daten zu erhalten. Die diagnostischen Daten und die *AVG7INST.LOG* Installations-Logdatei (die im *TEMP* Verzeichnis des Systems gespeichert ist) enthalten alle Informationen, die Sie für die Lösung des Problems benötigen.

Ist die Installation abgeschlossen, öffnet sich automatisch der **Firewall-Konfigurationsassistent** und bietet Ihnen die Möglichkeit, auf einfache Art und Weise die Standardkonfiguration der Firewall einzurichten. Sie können diesen Schritt auch auslassen, aber es wird Ihnen dringend empfohlen, diese Möglichkeit zu nutzen. Eine detaillierte Beschreibung finden Sie im Kapitel [10.6 Firewall-Konfigurationsassistent](#).

## 4. AVG Erste-Schritte

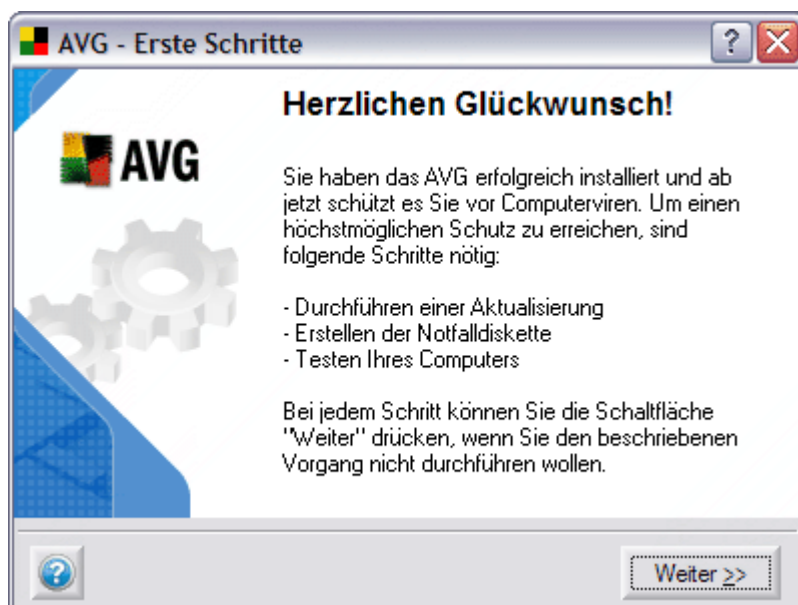
### 4.1. Erste Schritte-Assistent

Wenn Sie zum ersten Mal AVG auf Ihrem Computer installieren, öffnet sich der **AVG Erste-Schritte-Assistent**, der Ihnen bei der Ersteinstellung behilflich ist. Obwohl Sie alle vorgeschlagenen Werte auch noch später einstellen können, empfehlen wir, dass Sie den Assistenten ausführen, um Ihren Computer auf einfache Weise gegen Viren zu schützen.

**Folgen Sie bitte den Schritten in jedem einzelnen Fenster des Assistenten:**

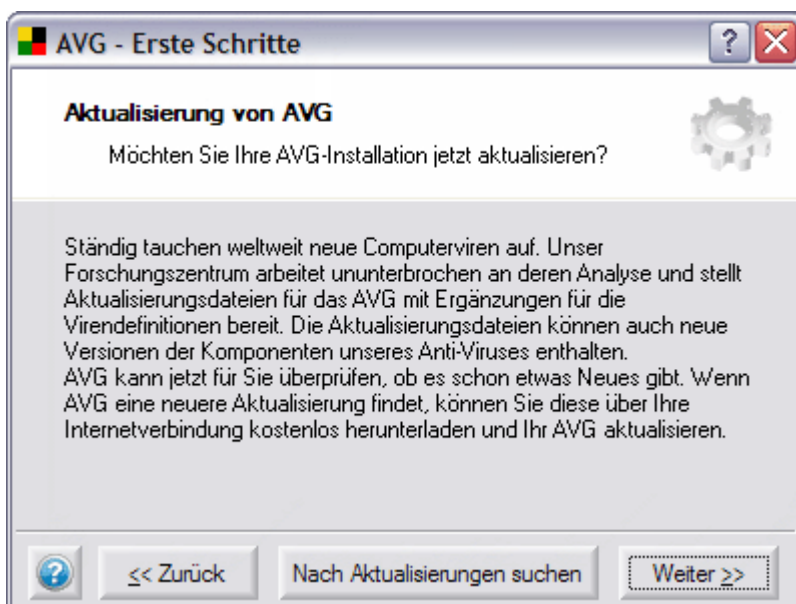
#### 4.1.1. Erste Schritte-Assistent – Herzlichen Glückwunsch!

Der Willkommensbildschirm des **AVG Erste Schritte-Assistenten** zeigt kurz den aktuellen Status von AVG auf Ihrem Computer an und schlägt Ihnen daraufhin Schritte zur Vervollständigung Ihres Schutzes vor. Klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren:



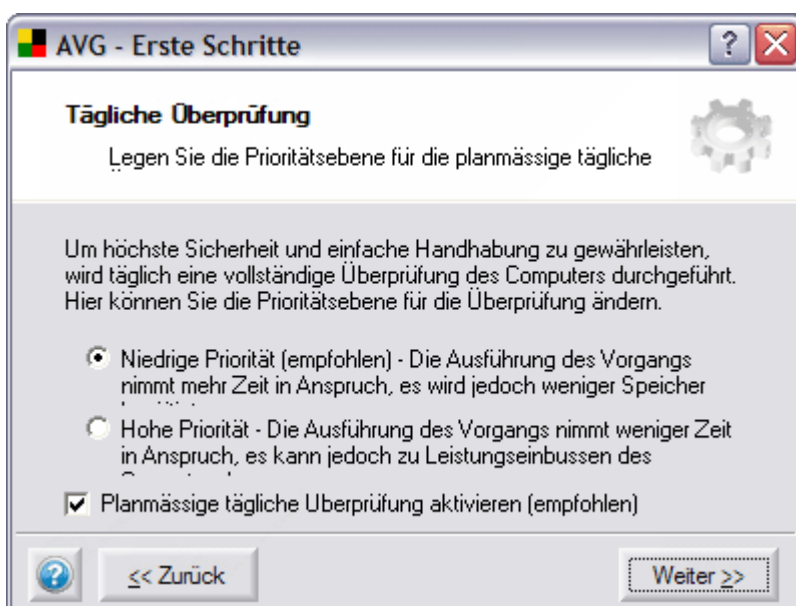
#### 4.1.2. Erste Schritte-Assistent - Aktualisierung von AVG Anti-Virus

Das Fenster **Aktualisierung von AVG** bietet Ihnen die Möglichkeit, automatisch nach neuen AVG-Aktualisierungen zu suchen und diese herunterzuladen. Klicken Sie auf die Schaltfläche **Nach Aktualisierungen suchen**, um die aktuellen Aktualisierungsdateien herunterzuladen und die Aktualisierung durchzuführen:



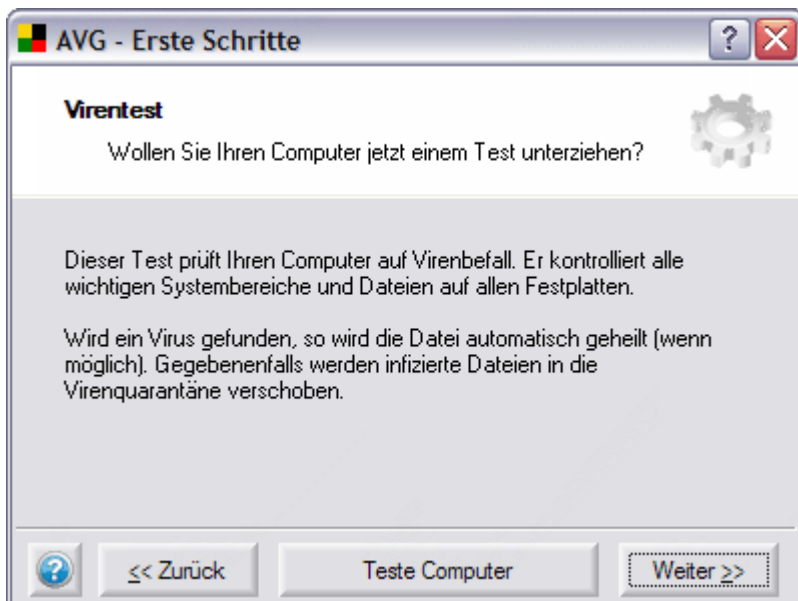
#### 4.1.3. Erste Schritte-Assistent – Tägliche Überprüfung

Das Fenster **Tägliche Überprüfung** fragt Sie nach einer Entscheidung, welches Prioritätslevel für die für täglich geplanten Tests Ihres Computers angewendet werden soll. Es wird empfohlen, die Voreinstellungen beizubehalten. Bestätigen Sie Ihre Auswahl, indem Sie einfach auf die Schaltfläche **Weiter** klicken.



#### 4.1.4. Erste Schritte-Assistent - Virentest

Das Fenster **Virentest** startet einen kompletten Test und behandelt eventuell vorhandene Viren. Zum Starten der Überprüfung klicken Sie bitte auf die Schaltfläche **Teste Computer**.



#### 4.1.5. Erste Schritte-Assistent – Sie sind geschützt!

Jetzt ist Ihr Computer überprüft und Ihr AVG wurde vollständig konfiguriert. Klicken Sie auf die Schaltfläche **Weiter**, um die Arbeit mit AVG zu starten:



#### 4.2. AVG Programmstart

Wenn Sie das nächste Mal das Programm starten wollen, können Sie dies folgendermaßen durchführen:

- Doppelklick auf das auf Ihrem Desktop erstellte AVG-Symbol
- aus dem Start Menü: **Start/Programme/AVG 7.5/AVG Control Center**  
aus dem Kontext Menü der AVG Control Center Systemleiste.

## 5. Nach der Installation

Damit eine maximale Effizienz Ihres Virenschutzlevels gewährleistet werden kann, empfehlen wir, die folgenden Schritte nach Ihrer Installation von AVG durchzuführen:

### 5.1. Durchführung des kompletten Tests

Da die Möglichkeit besteht, dass bereits vor der Installation von AVG Viren auf Ihren Computer gelangt sind, sollten Sie den **kompletten Test** durchführen, um alle Bereiche Ihres Computers auf mögliche Viren zu überprüfen. Wenn Sie alle vorgeschlagenen Schritte im Erste Schritte-Assistenten befolgt haben, wurde Ihr Computer bereits automatisch auf mögliche Viren überprüft und Sie können diesen Schritt überspringen.

Für weitere Informationen zum kompletten Test lesen Sie bitte Kapitel [13.1 - Kompletter Test](#).

### 5.2. Einstellen der Option "Beim Schliessen kontrollieren"

Es wird empfohlen, die Option **Dateien beim Schliessen kontrollieren** im **Residenten Schutz** zu aktivieren. Die Einstellung "Dateien beim Schliessen kontrollieren" garantiert Ihnen, dass AVG alle aktiven Objekte (z.B. Anwendungen, Dokumente ...) nicht nur wenn sie geöffnet werden, sondern auch wenn sie geschlossen werden, schützt. Dies bewahrt Ihren Computer vor jeglicher Art komplexer Viren.

Sie können die Einstellung "Dateien beim Schliessen kontrollieren" über den **Residenten Schutz** im **Control Center** aktivieren.

Für weitere Informationen zu den Einstellungen der Option "Beim Schliessen kontrollieren" sehen Sie bitte im Kapitel [9.12 – Komponenten, die vom Control Center kontrolliert werden/Residenter Schutz](#) nach.

### 5.3. Eicar Test

Um zu überprüfen, ob AVG fehlerfrei installiert wurde, können Sie den **Eicar Test** durchführen.

Der **Eicar Test** ist eine standardisierte und absolut sichere Methode, um die Leistungsfähigkeit von Virenschutzprogrammen zu überprüfen. Er basiert auf einer virusartigen Testdatei, die sicher genug ist, um weitergegeben zu werden, da es kein wirkliches Virus ist und keinerlei Fragmente eines Viren-Codes enthält. Die meisten Virenschutz-Programme reagieren auf diese Test-Datei, als wenn es ein echter Virus wäre (daher steht er mit einem auffälligen Namen in den Berichten, z.B. "EICAR-AV-Test"). Sie können sich die "Eicar Testdatei" von der Webseite [www.eicar.com](http://www.eicar.com) herunterladen. Dort finden Sie auch alle notwendigen Informationen bezüglich des "Eicar Test".

Versuchen Sie, die "**eicar.com**"- Datei herunter zu laden und speichern Sie diese auf Ihrer lokalen Festplatte. Gleich, nachdem Sie das Herunterladen der Testdatei bestätigen, wird der **Residente Schutz** darauf mit einer Warnung reagieren. Diese Warnung bestätigt, dass Ihr AVG fehlerfrei auf Ihrem Computer installiert wurde.

Sollte AVG die Eicar-Testdatei nicht als Virus identifizieren, müssen Sie dringend noch einmal die Konfiguration des Programms überprüfen.

#### 5.4. Test und Aktualisierungsplanung

Um sicherzustellen, dass Ihr Computer virenfrei ist, ist es notwendig, dass Sie regelmäßige AVG Tests/Aktualisierungen planen.

- **Test** - ein Kompletter Test sollte auf einer Workstation mindestens einmal wöchentlich geplant sein; weitere Informationen zum Planen von Tests lesen Sie bitte im Kapitel [13. Test Übersicht](#)
- **Aktualisierung** – für eine Workstation empfehlen wir eine tägliche Überprüfung auf neue Aktualisierungsdaten; weitere Informationen zu Aktualisierungsarten und -planung lesen Sie bitte im Kapitel [14. Programm Aktualisierungen](#)
- Hinweis: für AVG 7.5 File Server Editionen, die auf einem Terminal Server installiert sind empfehlen wir dringend, alle wesentlichen geplanten Tests und Aktualisierungen mit der Option "für alle Benutzer" einzurichten (im Scheduler unter geplante Aufgaben/Reiter Aufgabe/Option "für alle Benutzer") Dadurch stellen Sie sicher, dass die geplanten Aufgaben auch gestartet werden, wenn niemand angemeldet ist. Ebenfalls kann dadurch garantiert werden, dass kein Plan gleichzeitig in mehreren Instanzen ausgeführt wird (beispielsweise wenn ein Anwender mehrere Sessions gleichzeitig geöffnet hat), was die Verwendung von Systemressourcen minimiert.

## 6. Produkt-Registrierung

Wenn Sie die Installation von AVG beendet haben, sollten Sie Ihr Produkt registrieren, um den vollständigen Technischen Support von AVG, das AVG-Newsletter Aktualisierungen und anderen Service zu erhalten, den Grisoft exklusiv für registrierte Nutzer bereitstellt.

**Anmerkung:** Kunden, die ihr AVG im Online-Shop der Firma Grisoft gekauft haben wurden automatisch registriert und müssen sich daher nicht noch einmal registrieren lassen.

### Um Ihr AVG zu registrieren:

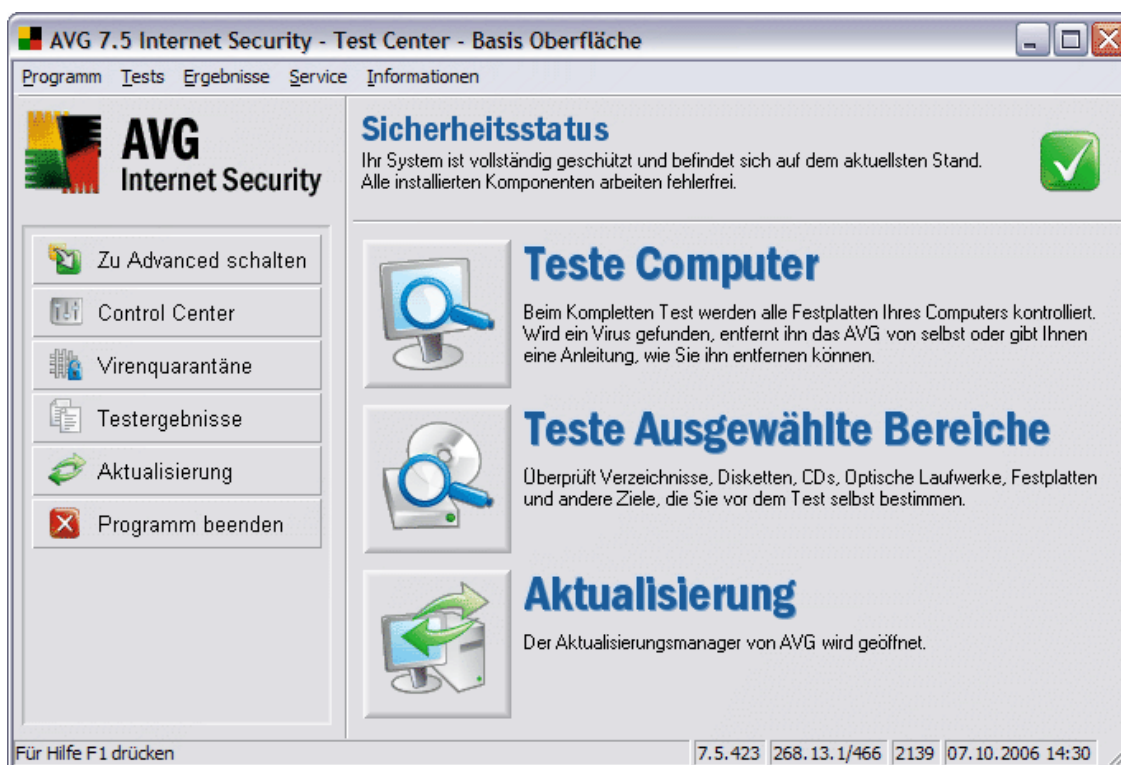
- Können Sie direkt zur Grisoft Webseite unter <http://www.grisoft.de> gehen und folgen dem Link **Registrierung**  
oder
- In Ihrer AVG Benutzer-Oberfläche wählen Sie aus dem Hauptmenü:  
**Informationen -> Registrieren im Internet**, um zur Grisoft Registrierungs-Webseite zu gelangen
- Geben Sie Ihre Vertriebs-/Lizenznummer in das leere Feld ein. Vergewissern Sie sich, dass Sie die Lizenznummer fehlerfrei eingeben (Groß/Kleinschreibung, Leerstellen usw.)!
- Drücken Sie die Schaltfläche **Senden**, um Ihre Registrierung zu bestätigen.

## 7. AVG Basis Oberfläche



Nachdem Sie AVG erfolgreich auf Ihrem Computer installiert haben, erscheint das AVG-Symbol auf Ihrem Windows Desktop. Doppelklicken Sie auf dieses Symbol, um das **Test Center** zu starten. AVG bietet Ihnen zwei unterschiedliche Oberflächen des Test-Centers – **Basis** und **Advanced**.

Die **Basis Oberfläche** ermöglicht den Zugriff auf die meisten AVG-Schutzfunktionen: Aktualisierungen, Tests, Aufgabenplanung und grundlegende Programm Konfiguration. Die Funktionen der beiden Oberflächen sind sich sehr ähnlich, wobei der größte Unterschied in der Anzahl der verfügbaren Einstellungen und der Auswahl der Advanced Funktionen, wie z.B. der Erstellung von Tests und Aktualisierungsplänen, zu sehen ist. Wenn Sie eine einfache Bedienoberfläche wünschen, wählen Sie die **Basis Oberfläche**.

**Die Basis Oberfläche wird für weniger geübte Anwender empfohlen, die die Vorteile des maximalen Virenschutzes bei möglichst wenigen Anwender-Interaktionen nutzen möchten.**



Zusätzlich können Sie den **Sicherheitsstatus** von AVG im Hauptbereich des Test Centers überprüfen. Es gibt drei mögliche Zeichen:

-  Ihr Computer ist vollständig geschützt, aktualisiert und alle installierten Komponenten arbeiten fehlerfrei
-  Eine oder mehrere Komponenten sind falsch konfiguriert und Sie sollten ihre Eigenschaften/Einstellungen überprüfen. Die Problemkomponenten werden in der Fehlerbenachrichtigung aufgelistet.



- Zeigt an, dass Sie sich dafür entschieden haben, den fehlerhaften Status einer der Komponenten zu ignorieren.

**Anmerkung:** Um das Control Center schnell zu öffnen, doppelklicken Sie einfach in den Bereich Sicherheitsstatus.

Für das Umschalten auf die Advanced Oberfläche können Sie die Schaltfläche Zu Advanced schalten im linken Menü nutzen. Oder Sie wählen aus dem Hauptmenü Programm/Zur Advanced Oberfläche umschalten.

Standardmäßig finden Sie in der Basis-Oberfläche die folgenden Einträge (linkes Menü) – siehe ihre Beschreibungen in den folgenden Kapiteln.

**Anmerkung:** Die Liste der Menüeinträge kann jedoch modifiziert werden; dafür lesen Sie bitte Kapitel [8.4 Programmeinstellungen/Anpassen](#).

### 7.1. Umschalten auf die Advanced Oberfläche

Der Menüeintrag **Zu Advanced schalten** ermöglicht das Umschalten zwischen der **Basis/Advanced**- Oberfläche von AVG.

Für weitere Details zur **Advanced Oberfläche** sehen Sie bitte im Kapitel [8. AVG Advanced Oberfläche](#) nach

### 7.2. Control Center

Der Menüeintrag **Control Center** ruft das **Control Center** auf – die zentrale Kontrollanwendung für AVG; im **Control Center** können Sie sich einen Überblick verschaffen, konfigurieren und das gesamte AVG-Programm verwalten.

Für weitere Details zum **Control Center** lesen Sie bitte Kapitel [9. AVG Control Center](#)

### 7.3. Virenquarantäne

Der Menüeintrag **Virenquarantäne** öffnet die **Virenquarantäne** - eine sichere Umgebung zum Speichern von infizierten Objekten und für deren weitere Behandlung.

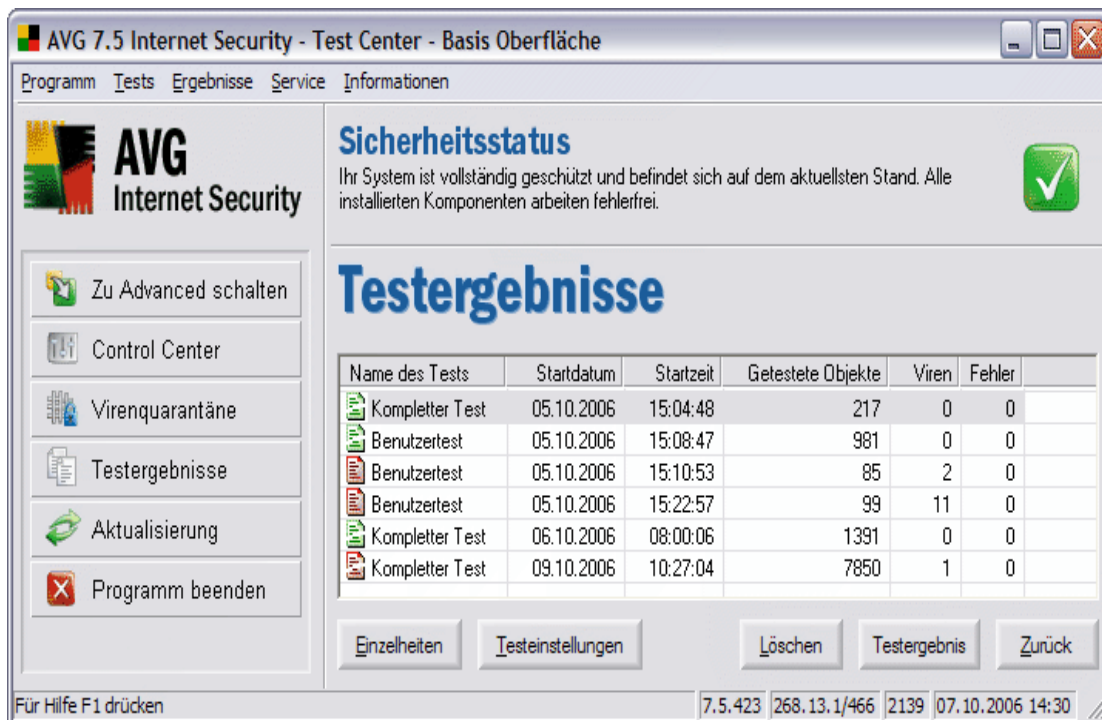
Für weitere Details zur **Virenquarantäne** lesen Sie bitte Kapitel [12. Virenquarantäne](#) nach

### 7.4. Test Ergebnisse

Der Shortcut **Testergebnisse** bietet einen Überblick über die kürzlich durchgeführten Tests und deren Ergebnisse:

- Name des Tests – vollständiger Name des durchgeführten Tests
- Startdatum – Datum des Teststarts
- Startzeit – genaue Zeitangabe des Teststarts
- Getestete Objekte – Anzahl der getesteten Objekte
- Viren – Anzahl der gefundenen Viren

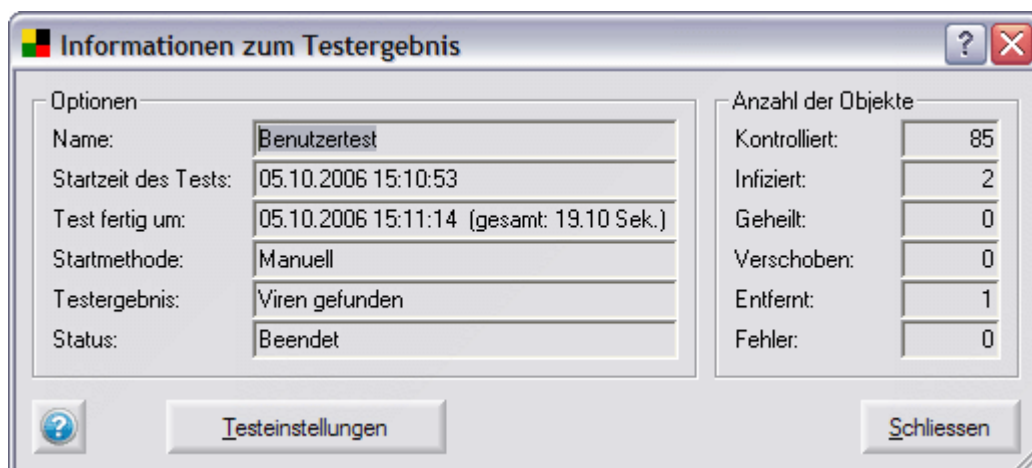
- Fehler – Anzahl der aufgetretenen Fehler



Sie können zusätzlich weitere detaillierte Informationen über die aufgelisteten Tests mit Hilfe der Schaltflächen im unteren Bereich des Dialogfensters **Testergebnisse** erhalten:

**a) Einzelheiten**

Die Schaltfläche **Einzelheiten** öffnet ein neues Dialogfenster, das Ihnen weitergehende Informationen über die durchgeführten Tests und deren Ergebnisse zeigt. Die Daten sind in zwei Gruppen unterteilt: **Optionen** (Testparameter und Testergebnisse) und **Anzahl der Objekte** (kontrollierte Objekte und Teststatistiken):

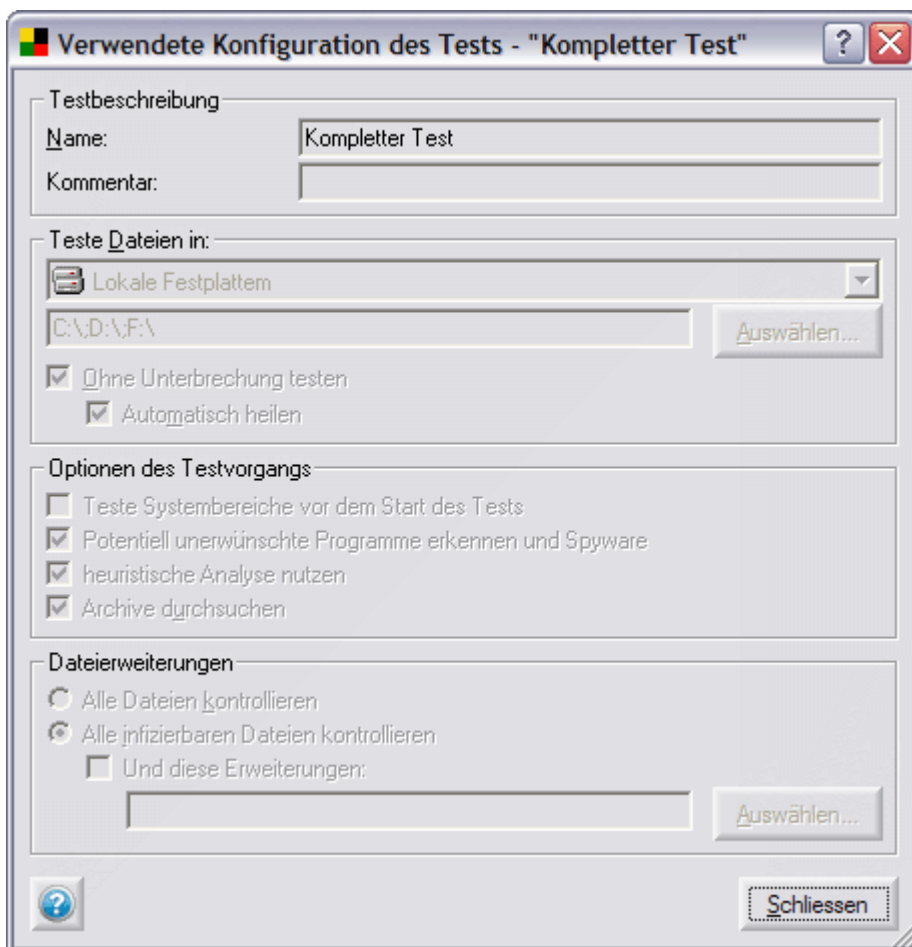


In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- **Testeinstellungen** – öffnet ein neues Dialogfenster mit einem Überblick über die Testeinstellungen (Für detaillierte Informationen zu den einzelnen Testeinstellungen lesen Sie bitte das Kapitel [11. Test-Übersicht](#))
- **Schliessen** – schließt das Fenster **Informationen zum Testergebnis**

## b) Testeinstellungen

Die Schaltfläche **Testeinstellungen** zeigt Ihnen ein neues Dialogfenster mit Informationen zur verwendeten Testkonfiguration an: Name, Kommentar, Teste Dateien in: Optionen des Testvorgangs und Dateierweiterungen:

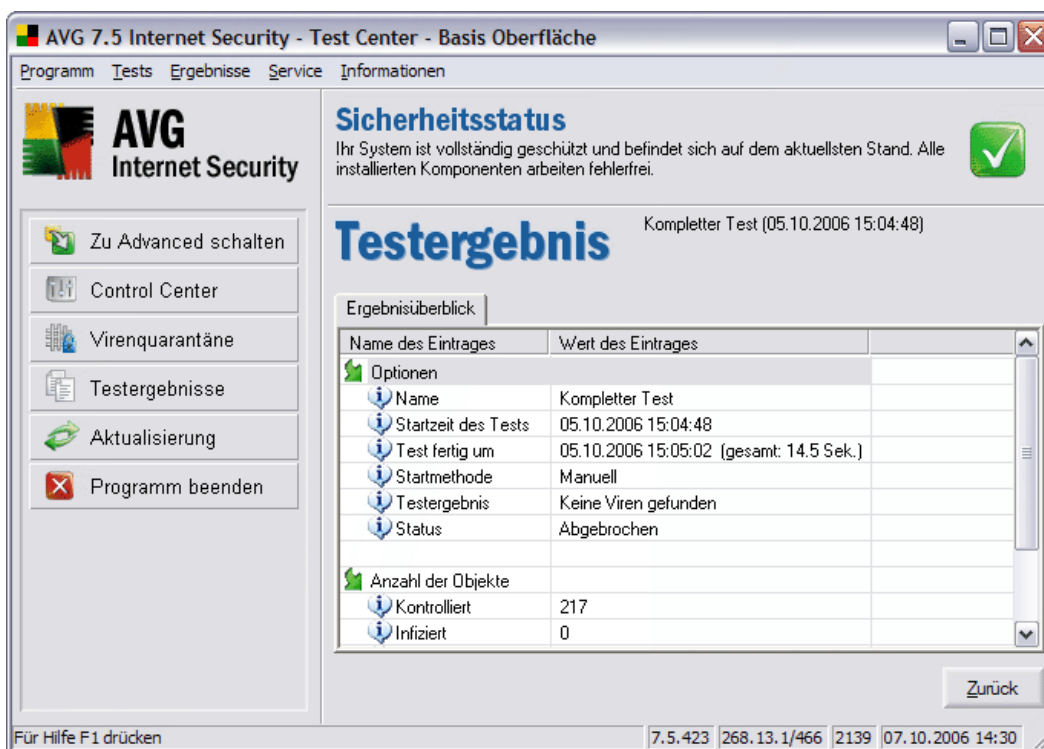


## c) Löschen

Die Schaltfläche **Löschen** entfernt die markierten Testergebnisse aus der Liste.

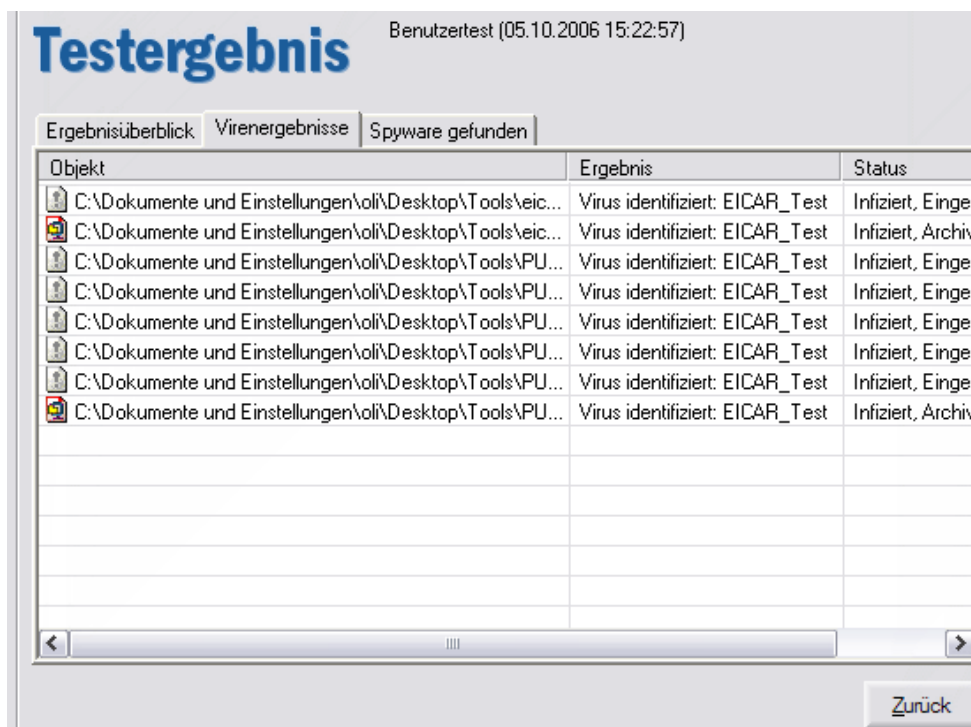
## d) Inhalt

Die Schaltfläche **Inhalt** öffnet einen Überblick über detaillierte Informationen zu den Testergebnissen für den ausgewählten Test: Ort der infizierten Datei, Ergebnis (Suchspezifikation) und Status der infizierten Datei.



Dieser Dialog ist in verschiedene Reiter unterteilt:

- **Ereignisüberblick**  
Unter diesem Reiter finden Sie detaillierte Statistiken und Zusammenfassungen zu den Tests.
- **Virenergebnisse**  
Dieser Reiter wird nur angezeigt, wenn ein Virus während des Testvorgangs erkannt wurde. Der Reiter listet alle erkannten Viren auf.



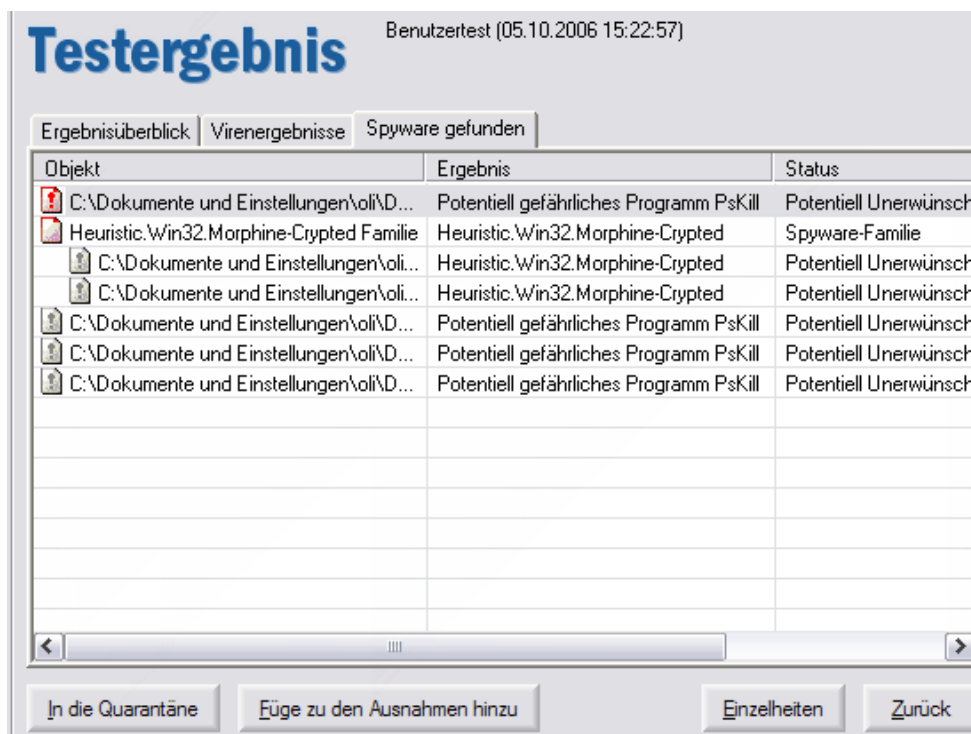
In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- **Heilen** – ermöglicht Ihnen, das infizierte Objekt zu heilen, wenn ein Mittel zum Heilen für diese Art Infektion verfügbar ist.
- **In die Quarantäne** – verschiebt das gewählte infizierte Objekt in die Quarantäne.
- **Einzelheiten** – öffnet die Virenenzyklopädie, die weitere Informationen über das gefundene Virus liefert
- **Zurück** – schließt den Dialog **Testergebnisse**

**Anmerkung:** Schaltflächen werden nur für Maßnahmen angezeigt, die für das in der Liste gewählte Virus auch durchgeführt werden können. Wenn z.B. das ausgewählte Virus bereits während der Überprüfung automatisch entfernt wurde (sh. oben), kann es nicht geheilt oder verschoben werden.

- o **Spyware gefunden**

Dieser Reiter wird nur angezeigt, wenn eine Infektion durch Spyware/Malware oder durch ein Internet- Cookie während des Tests erkannt wurde. Unter diesem Reiter werden all solche Funde aufgelistet.



Die Schaltflächen für diesen Dialog sind folgende:

- **In die Quarantäne** – verschiebt das gewählte, infizierte Objekt in die Virenquarantäne.
- **Füge zu den Ausnahmen hinzu** – fügt das **Potentiell Unerwünschte Programm** (oder die Spyware/Malware) der Liste der Ausnahmen hinzu. Anschließend arbeitet das gewählte Programm wieder fehlerfrei und AVG ignoriert es bei zukünftigen Tests. Weitere Informationen zu diesem Thema erhalten Sie im Bereich [Potentiell Unerwünschte Programme-Ausnahmen \(Kapitel 7.14\)](#).
- **Einzelheiten** – öffnet die Virenenzyklopädie, die Ihnen Informationen zur erkannten Infektion bietet.

**Anmerkung:** Die Schaltflächen werden nur für Maßnahmen angezeigt, die mit der in der Liste gewählten Malware auch durchführbar sind.

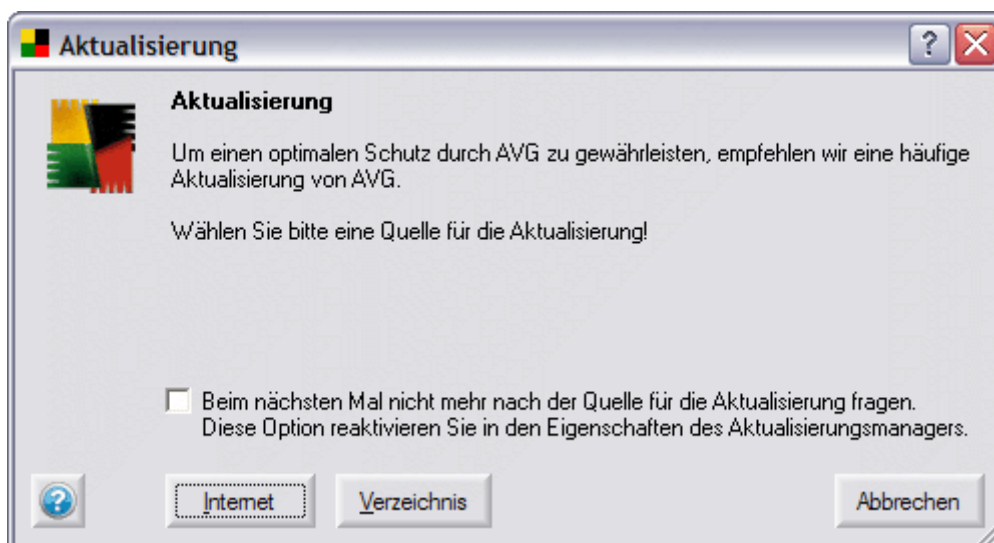
#### e) Zurück

Die Schaltfläche **Zurück** schliesst das Fenster **Testergebnis**.

### 7.5. Aktualisierungen

Der Menüeintrag **Aktualisierung** öffnet ein Fenster, das eine sofortige Aktualisierung von AVG anbietet.

Für weitere Informationen zu den Aktualisierungsmöglichkeiten sehen Sie bitte unter [14. Programm-Aktualisierungen](#) nach.



In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- **Internet** – startet die Aktualisierung von AVG aus dem Internet
- **Verzeichnis** – öffnet ein Dialogfenster, in dem Sie das Aktualisierungs-Quellverzeichnis (entweder lokal oder im Netzwerk) angeben müssen; drücken Sie die Schaltfläche **OK**, um die Auswahl zu bestätigen und um die Aktualisierung von AVG zu starten
- **Abbrechen** – schliesst das Dialogfenster **Aktualisierung**

Wenn Sie immer dieselbe Quelle für die Aktualisierungsdateien nutzen möchten, aktivieren Sie bitte die Option **Beim nächsten Mal nicht mehr nach der Quelle für die Aktualisierung fragen**. Bei der nächsten Aktualisierung werden Sie daraufhin nicht mehr nach der Aktualisierungsquelle gefragt und die Aktualisierung wird automatisch von der angegebenen Quelle aus durchgeführt.

Wenn Sie die Aktualisierungsquellen-Abfrage in Zukunft wieder im Dialog **Aktualisierung** angezeigt bekommen möchten, können Sie die in der Komponente **Aktualisierungsmanager** im Control Center einstellen – für eine detaillierte Beschreibung der Einstellungen lesen Sie bitte auch im Kapitel [9.14 –Control Center – Aktualisierungsmanager](#) den Abschnitt **Optionen**.

### 7.6. Programm beenden

Der Menüeintrag **Programm beenden** schliesst das Programm **Test Center**.

Neben der Shortcut Leiste auf der linken Seite bietet das Hauptmenü (oben) die folgenden Optionen:

### 7.7. Testeinstellungen

**Tests/Testeinstellungen von Systembereiche** (alternativ auch andere Testeinstellungen)

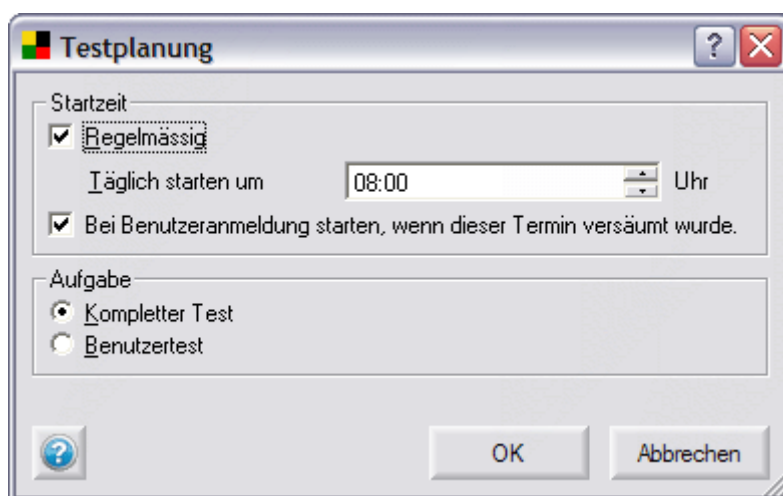
In diesem Abschnitt können Sie Ihre eigenen Parameter anstelle der Standardparameter des Herstellers für die AVG-Tests einstellen.

Für eine detaillierte Beschreibung der Testeinstellungen lesen Sie bitte auch Kapitel [13. Test Übersicht](#).

## 7.8. Testplanung

### Tests/Testplanung

In der **Basis Oberfläche** sind die Optionen für die Testplanung stark eingeschränkt. Sie können einen Test (kompletter Test oder Benutzertest) nur mit dem Intervall täglich planen. Sie können den genauen Startzeitpunkt planen und festlegen, ob der Test nach der Benutzeranmeldung starten soll, falls der geplante Zeitpunkt verpasst wird:



Wir empfehlen für die Testplanung die Verwendung der **Advanced Oberfläche**.

Für detaillierte Informationen zu den Testplanungsoptionen der Advanced Oberfläche lesen Sie bitte auch das Kapitel [8.2 Geplante Aufgaben](#)

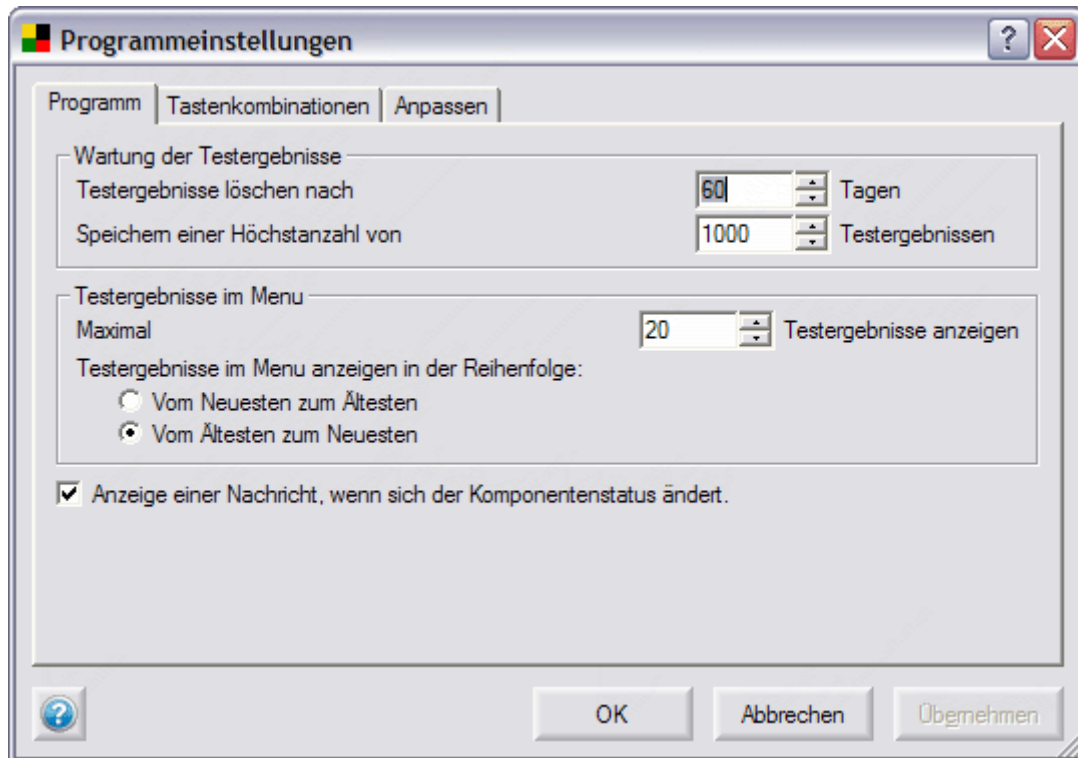
## 7.9. Programmeinstellungen

### Service/Programmeinstellungen

Im Bereich **Programmeinstellungen** können Sie einige generelle AVG-Programmooptionen unter gesonderten Reitern spezifizieren. Die Möglichkeiten sind jedoch in der Basis-Oberfläche sehr begrenzt:

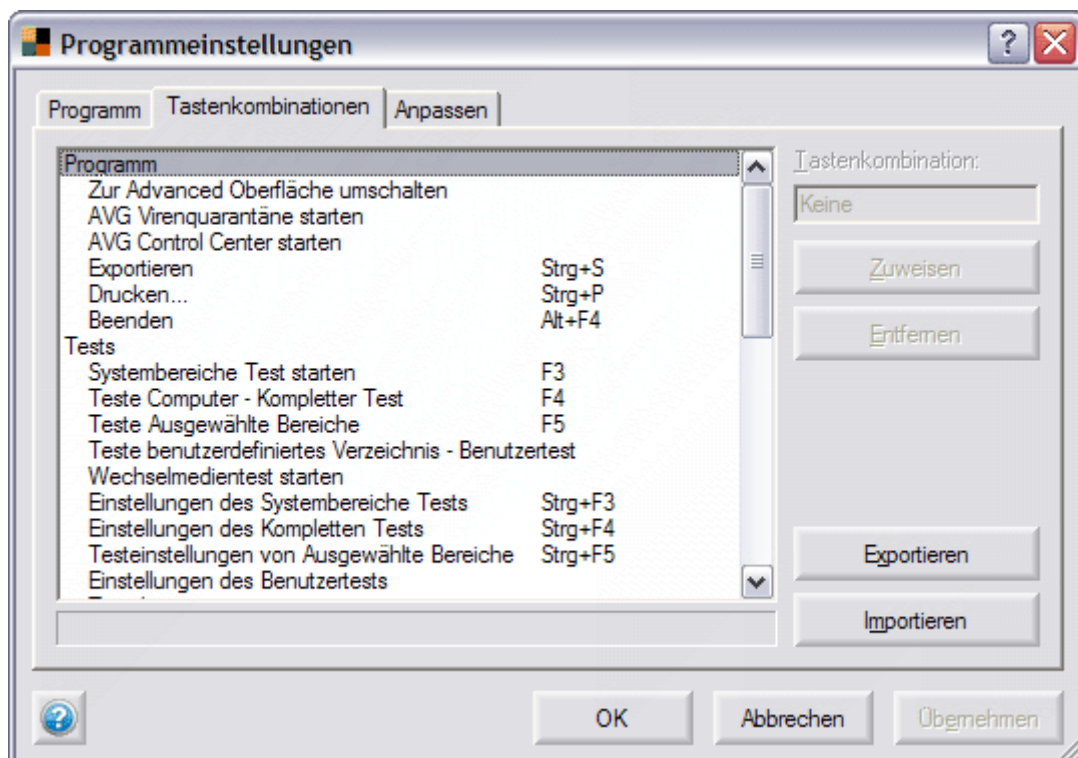
#### a) Programm

- Wie lange und wie viele Testergebnisse wollen Sie speichern
- Wie viele der aktuellen Testergebnisse sollen im Menü der **Basis Oberfläche** angezeigt werden
- Welche zeitabhängige Sortierung der Testergebnisse bevorzugen Sie



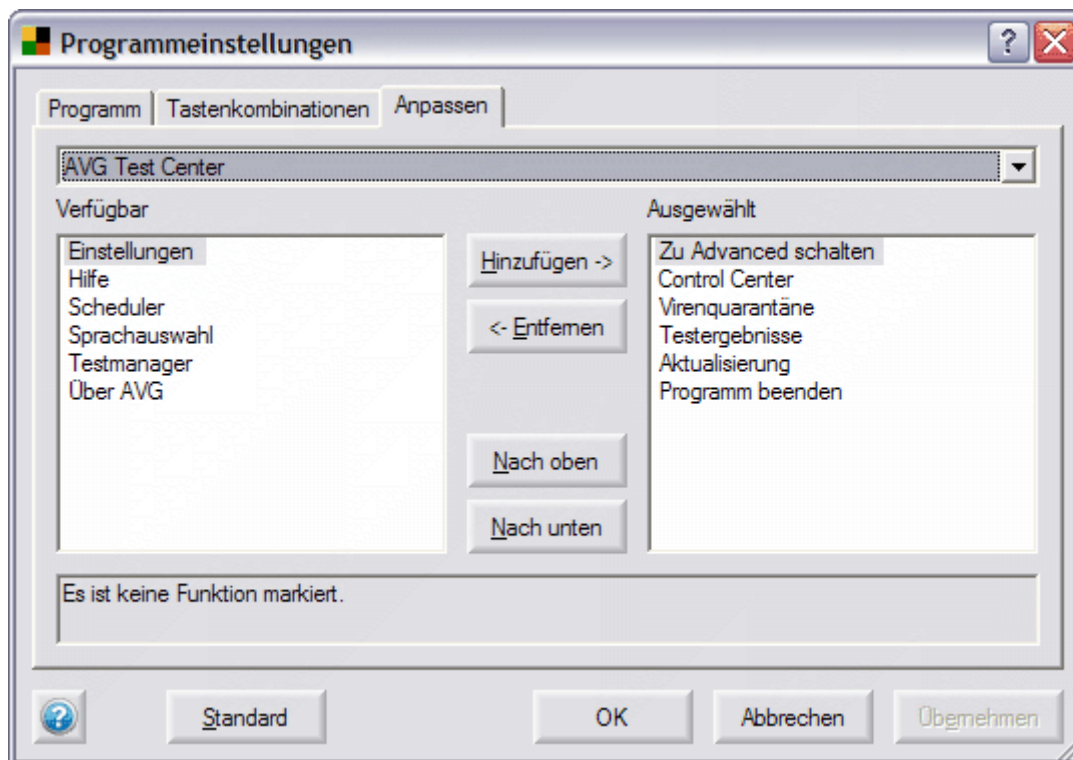
## b) Tastenkombinationen

Der Reiter **Tastenkombinationen** ermöglicht Ihnen das Definieren eigener Tastenkombinationen für die AVG-Umgebung:



### c) Anpassen

Der Reiter **Anpassen** gestattet Ihnen die Auswahl der AVG Funktionen, die im **Test Center/Control Center** über die Shortcut-Links angezeigt werden sollen:



Für weitergehende Programmkonfigurationen empfehlen wir die Verwendung der **Advanced Oberfläche**.

Weitere Details zu der Option Programmkonfiguration in der Advanced Oberfläche erhalten Sie auch in Kapitel [8.4 Programm-Einstellungen](#).

## 7.10. Rettungsdiskette

### Service/Rettungsdiskette

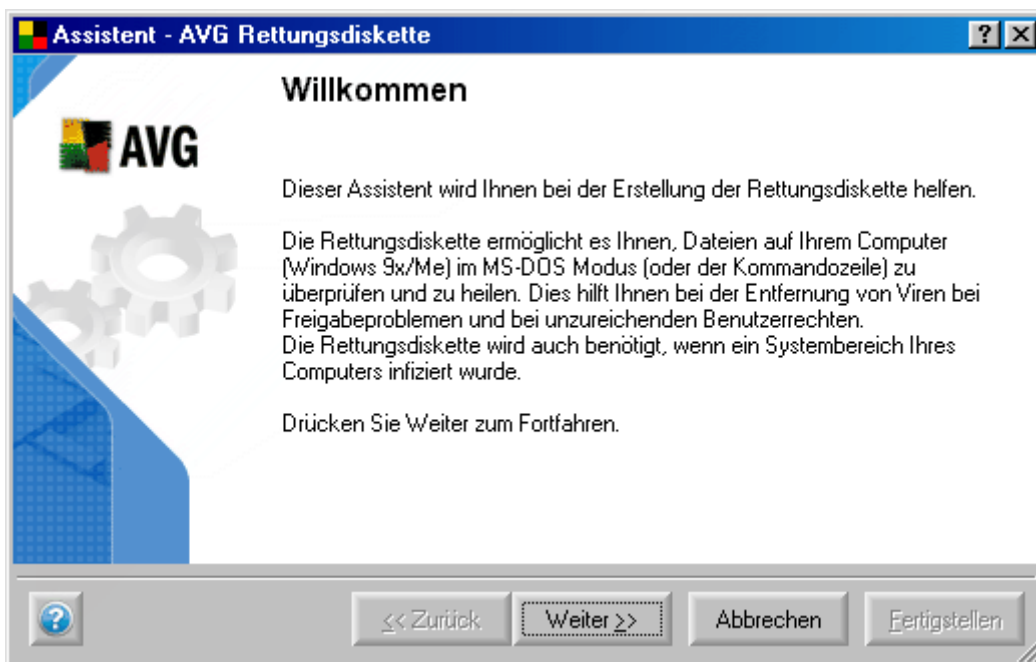
**Ab Windows XP aufwärts wird dieses Feature nicht mehr unterstützt.**

Die **Rettungsdiskette** hilft Ihnen dabei, alle Dateien auf Ihrem Computer im MS-DOS Modus zu testen und zu bereinigen und Systembereiche wieder herzustellen (mit Hilfe der Kommandozeile); sie ist hauptsächlich für die Betriebssysteme Windows9x/Me vorgesehen.

Diese Funktion ist hilfreich, wenn Sie Viren von einem Computer entfernen wollen:

- der ein Problem mit Freigaben hat
- zu dem Sie nicht entsprechende Zugriffsrechte haben
- bei dem die Systembereiche infiziert sind

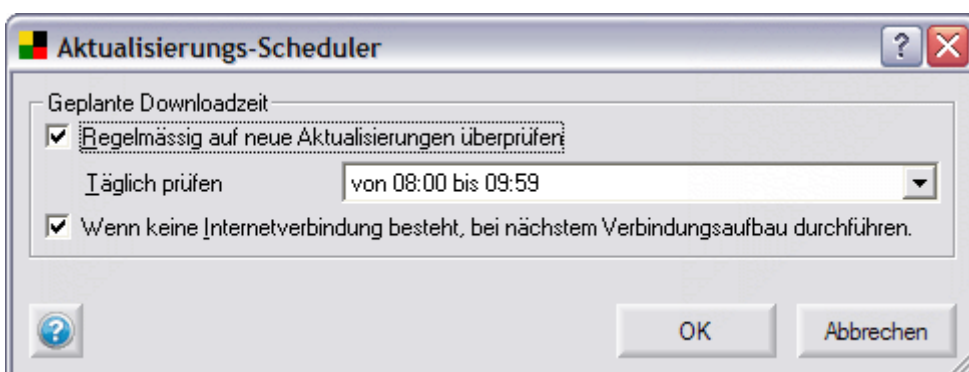
Der Menüeintrag **Rettungsdiskette** ruft einen Assistenten auf, der Sie durch den Erstellungsprozess einer Rettungsdiskette führen wird. Um die Rettungsdiskette zu erstellen, folgen Sie den Anweisungen des Assistenten:



### 7.11. Aktualisierungs-Scheduler

#### Service/Aktualisierungs- Scheduler

In der **Basis Oberfläche** sind die Optionen zum Planen von Aktualisierungen sehr begrenzt. Sie können nur eine tägliche Aktualisierung planen. Sie können die exakte Aktualisierungszeit festlegen und bestimmen, ob die Aktualisierung beim nächsten Verbindungsaufbau gestartet werden soll (falls der geplante Zeitpunkt verpasst wurde):



Für eine weitergehende Konfiguration empfehlen wir die Verwendung der **Advanced Oberfläche**.

Sie finden weiterführende Informationen zur Planung von Aktualisierungen mit Hilfe der Advanced Oberfläche im Kapitel [8.2 Geplante Aufgaben](#)

## 7.12. Ereignisprotokoll

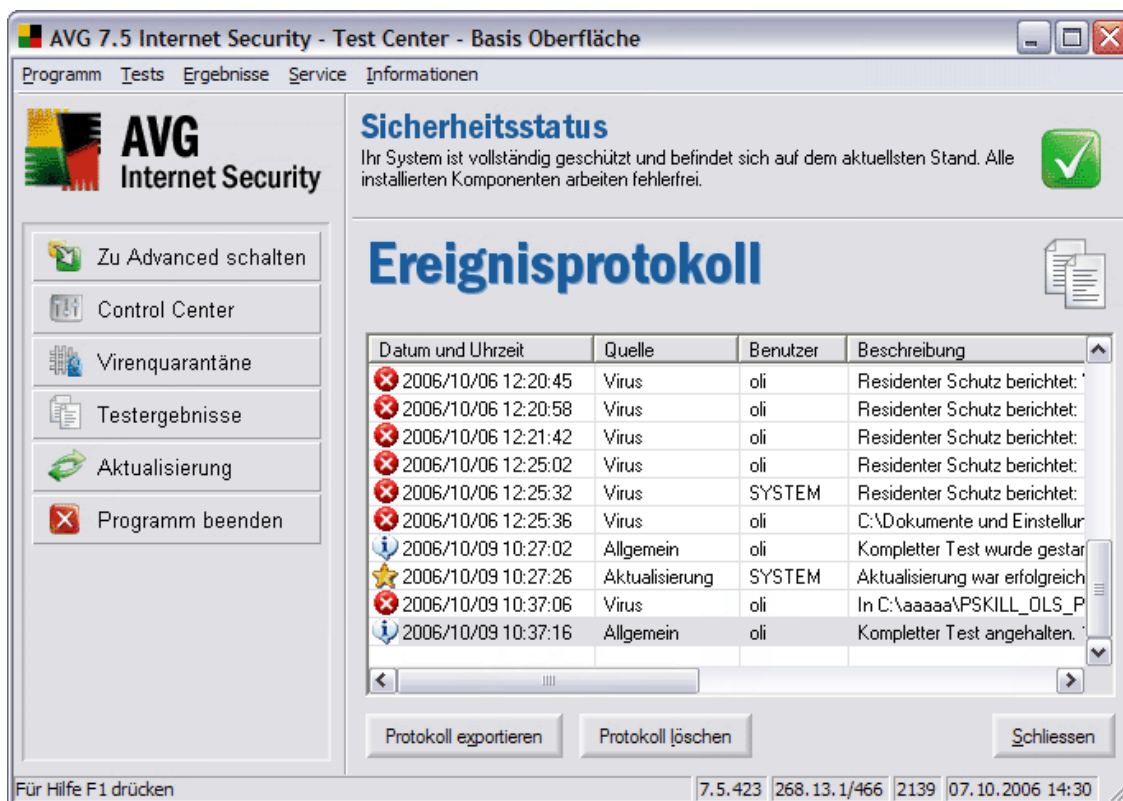
### Service/Ereignisprotokoll

In diesem Bereich finden Sie eine Zusammenfassung wichtiger Ereignisse, die während des Betriebs von AVG auftraten.

Das **Ereignisprotokoll** speichert die folgenden verschiedenen Ereignisse:

- Informationen zu den Aktualisierungen der AVG-Anwendung
- Start, Ende oder Unterbrechung von Tests (einschließlich der automatisch durchgeführten Tests)
- Ereignisse in Verbindung mit Virenfunden (durch den Residenten Schutz oder Testläufe) einschließlich des Fundortes
- Andere wichtige Ereignisse

Mittels der Schaltfläche „Protokoll exportieren“ können Sie das Protokoll im XML Format speichern. Alle Einträge können über die Schaltfläche „Protokoll löschen“ entfernt werden.



**AVG 7.5 Internet Security - Test Center - Basis Oberfläche**

Programm Tests Ergebnisse Service Informationen

**Sicherheitsstatus**  
Ihr System ist vollständig geschützt und befindet sich auf dem aktuellsten Stand. Alle installierten Komponenten arbeiten fehlerfrei.

**Ereignisprotokoll**

Datum und Uhrzeit	Quelle	Benutzer	Beschreibung
2006/10/06 12:20:45	Virus	oli	Residenter Schutz berichtet:
2006/10/06 12:20:58	Virus	oli	Residenter Schutz berichtet:
2006/10/06 12:21:42	Virus	oli	Residenter Schutz berichtet:
2006/10/06 12:25:02	Virus	oli	Residenter Schutz berichtet:
2006/10/06 12:25:32	Virus	SYSTEM	Residenter Schutz berichtet:
2006/10/06 12:25:36	Virus	oli	C:\Dokumente und Einstellu
2006/10/09 10:27:02	Allgemein	oli	Kompletter Test wurde gestar
2006/10/09 10:27:26	Aktualisierung	SYSTEM	Aktualisierung war erfolgreich
2006/10/09 10:37:06	Virus	oli	In C:\aaaaa\PSKILL_OLS_P
2006/10/09 10:37:16	Allgemein	oli	Kompletter Test angehalten.

Protokoll exportieren Protokoll löschen Schliessen

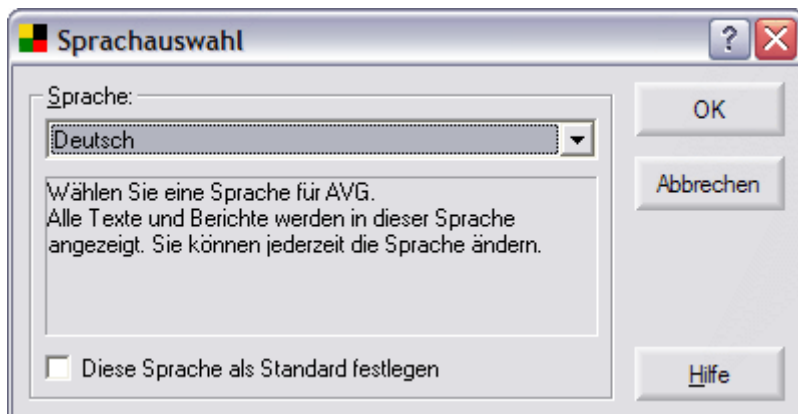
Für Hilfe F1 drücken 7.5.423 268.13.1/466 2139 07.10.2006 14:30

## 7.13. Sprachauswahl

### Service/Sprachauswahl

Diese Option ermöglicht Ihnen die Auswahl der Sprache, die Sie verwenden möchten; falls gewünscht, wird die ausgewählte Sprache auch als Standard für die gesamte Anwendung verwendet:

**Anmerkung:** Standardmäßig ist nur die englische Sprache und die Sprache, die Sie während der Installation gewählt haben, installiert. Sie können den [Installationsprozess \(Kapitel 3\)](#) jederzeit neu starten und zusätzliche Sprachen im Auswahldialog der Komponenten wählen.

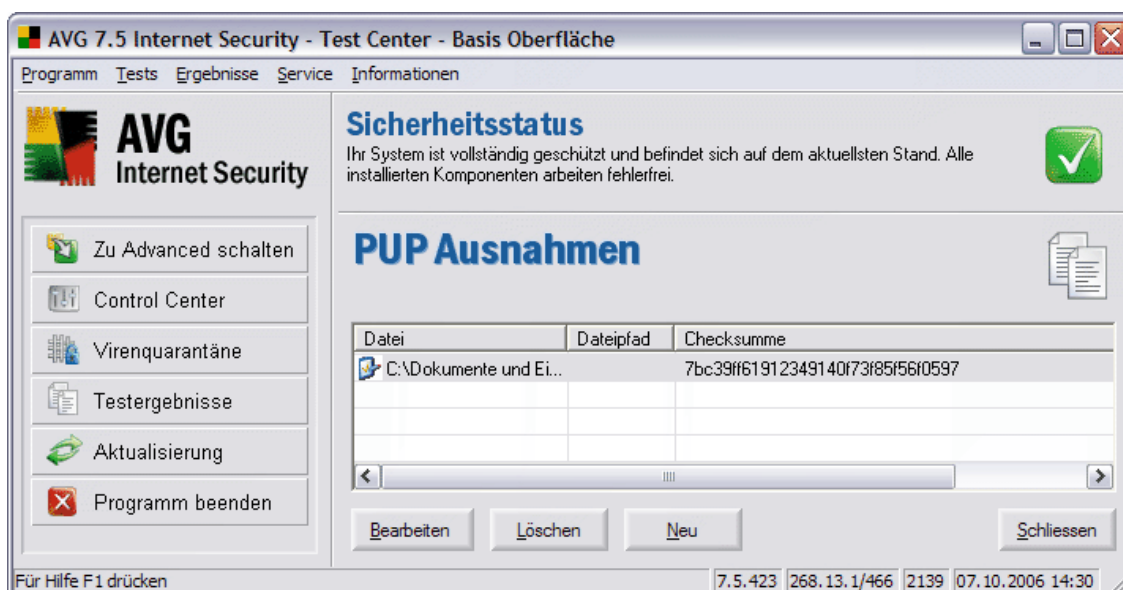


## 7.14. Potentiell unerwünschte Programme - Ausnahmen

### Service/Potentiell unerwünschte Programme - Ausnahmen

Dieser Menüeintrag aktiviert das Dialogfenster zum Bestimmen der Ausnahmen zu **potentiell unerwünschten Programmen (PUP)**.

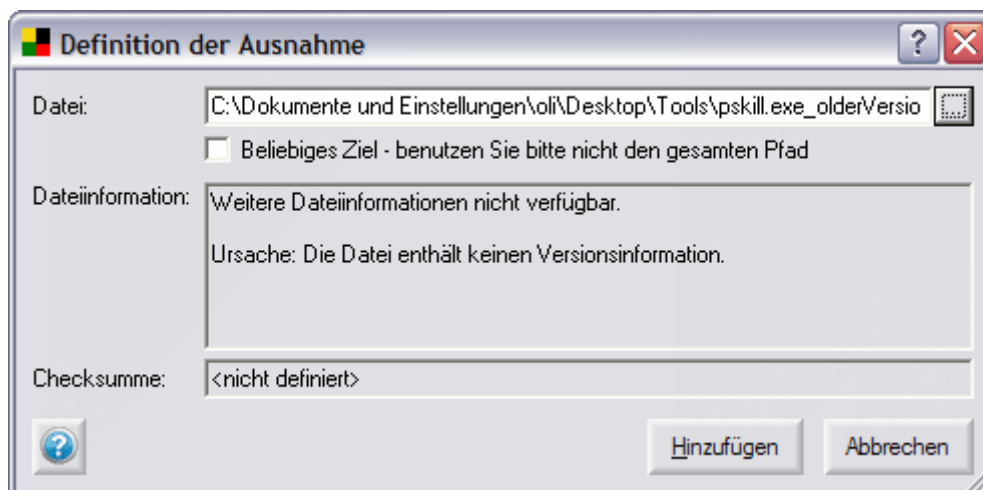
AVG kann ausführbare Anwendungen oder DLL-Bibliotheken, die innerhalb des Systems als potentiell unerwünscht angesehen werden, erkennen und analysieren. In einigen Fällen kann es vorkommen, dass der Benutzer bestimmte unerwünschte Programme auf dem Computer behalten möchte (Programme, die absichtlich installiert wurden). Einige Programme, besonders kostenfreie Programme, enthalten Adware. Solche Adware kann erkannt werden und hierüber berichtet AVG als **potentiell unerwünschtes Programm**. Wenn Sie jedoch solch ein Programm auf Ihrem Computer beibehalten möchten, so können sie es als **Ausnahme zu potentiell unerwünschten Programmen** definieren:



Alle bereits definierten und aktuell gültigen Ausnahmen werden in diesem Dialog aufgelistet. Sie können eine neue Ausnahme hinzufügen, indem Sie die Schaltfläche **Neu** betätigen. Außerdem können Sie bereits bestehende Ausnahmen abändern, indem Sie die Schaltfläche **Bearbeiten** hierfür nutzen. Wenn Sie auf die Schaltfläche **Löschen** klicken, entfernen Sie die aktuell gewählte Ausnahme.

#### a) Definition einer neuen Ausnahmen zu einem potentiell unerwünschten Programm

Wenn Sie auf die Schaltfläche **Neu** klicken, können Sie manuell eine neue Ausnahme definieren:



Im Feld **Datei** geben Sie den vollständigen Pfad zu der Datei ein, die Sie als Ausnahme angeben möchten. Wenn Sie diese Datei als Ausnahme nur zu einem speziellen Speicherort definieren möchten, so setzen Sie kein Häkchen in das Kontrollkästchen **Beliebiges Ziel - benutzen Sie bitte nicht den gesamten Pfad**.

Wenn Sie das Häkchen in diesem Kontrollkästchen setzen, wird die gewählte Datei (und alle Kopien der Datei) als Ausnahme definiert; egal, auf welchem Speicherort sie sich befinden. Sie müssen jedoch den vollständigen Pfad zu der speziellen Datei eingeben, da diese als Musterdatei genutzt wird (falls mehr als eine 'unterschiedliche' Datei mit gleichem Dateinamen auf Ihrem Computer existiert).

Alternativ dazu können Sie auf die Schaltfläche **...** klicken, um einen Standard Explorer- Dialog für die Suche des Speicherorts der gewünschten Datei zu öffnen.

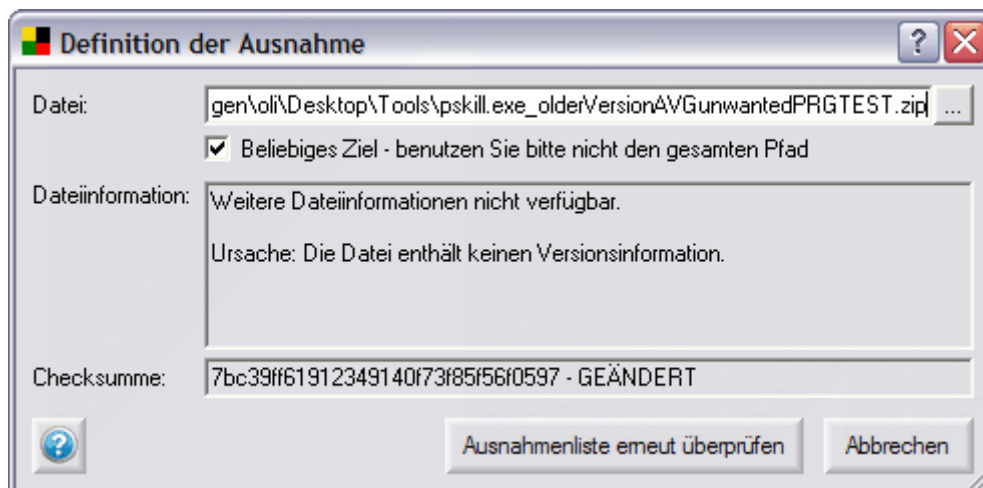
Falls zusätzliche Informationen über diese Datei verfügbar sind (Lizen/Versionsinformationen usw.), werden diese im Bereich **Dateiinformatio:n** angezeigt.

Das Feld **Checksumme** zeigt die einzigartige "Signatur" der gewählten Datei an. Diese Checksumme ist eine automatisch generierte Charakter-Zeichenfolge, mit der AVG eindeutig zwischen der gewählten Datei und anderen Dateien unterscheiden kann. Die Checksumme wird nach dem erfolgreichen Hinzufügen der Datei generiert und angezeigt.

Um die neue Ausnahme zu bestätigen und zu speichern, klicken Sie auf die Schaltfläche **Hinzufügen**.

**b) Bearbeiten einer bestehenden Ausnahme zu einem potentiell unerwünschten Programm**

Wenn Sie auf die Schaltfläche **Bearbeiten** klicken, können Sie manuell eine bestehende Ausnahme bearbeiten:



Während der Bearbeitung einer bestehenden Ausnahme, kann es passieren, dass das Feld [Checksumme](#) als GEÄNDERT angezeigt wird. Dies bedeutet, dass die Datei nach dem Hinzufügen geändert wurde und dass sie nicht mit der ursprünglich generierten Checksumme übereinstimmt. Wenn Sie die bearbeitete Datei als eine Ausnahme markieren möchten, klicken Sie auf die Schaltfläche **Ausnahmenliste erneut überprüfen**.

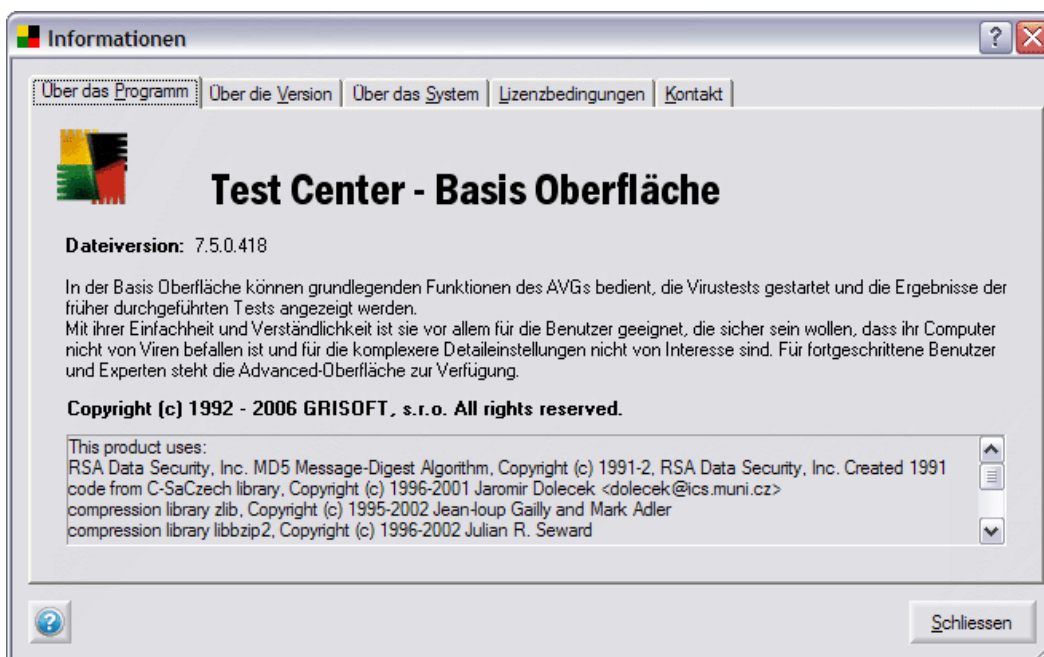
**7.15. Informationen****Informationen/...**

In diesem Abschnitt finden Sie allgemeine Informationen zu AVG und Informationen zum Support:

**a) Versionsinformationen, Kontakt**

Beide Optionen öffnen ein Fenster mit fünf Reitern, die Informationen zu AVG bieten:

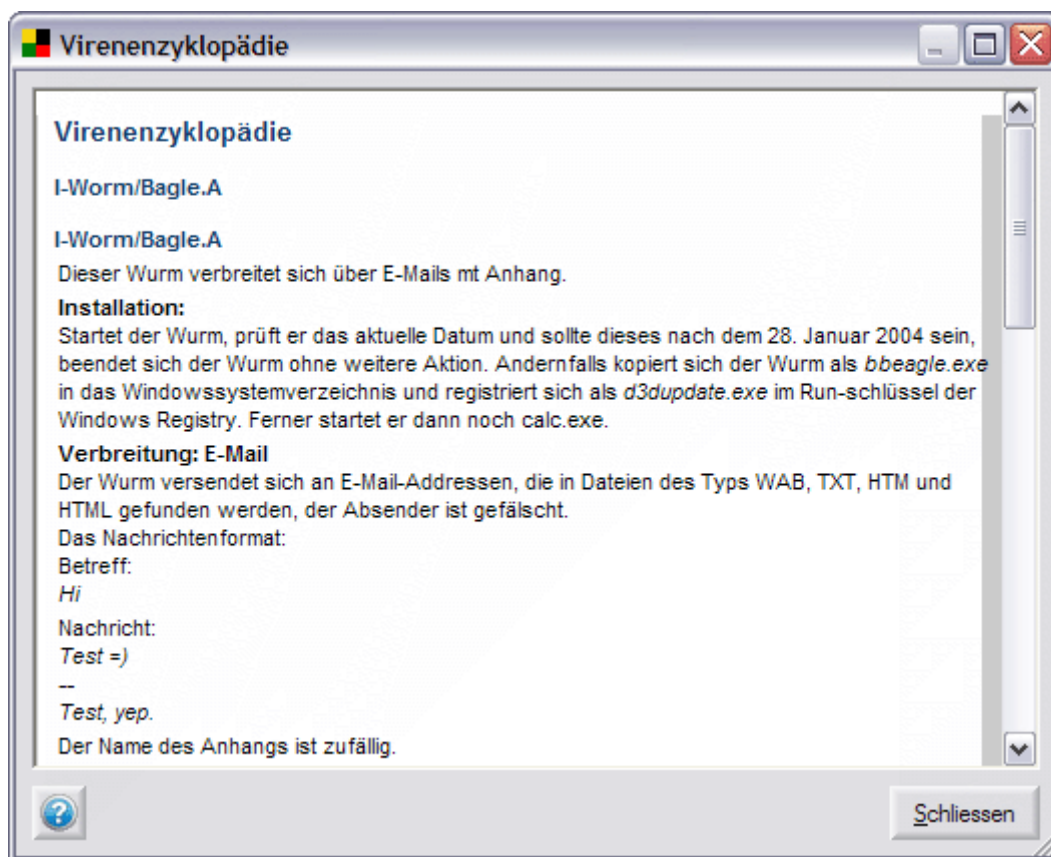
- **Über das Programm** – Informationen über die Basis Oberfläche von AVG
- **Über die Version** – Informationen zur AVG-Version und zur Virendatenbankversion
- **Über das System** – Informationen zum Status des Betriebssystems
- **Lizenzbedingungen** – vollständiger Wortlaut der Lizenzbedingungen
- **Kontakt** – Überblick über die weltweiten AVG-Händler und AVG-Vertriebskontakte



## b) Informationen über Viren

Die Option Informationen über Viren öffnet eine Online Virenenzyklopädie aller bekannten Viren mit der Möglichkeit, nach Informationen zu speziellen Viren zu suchen.

Da die Viren Enzyklopädie nur online angeboten wird, müssen Sie mit dem Internet verbunden sein, um darauf zugreifen zu können.



c) **Technischer Support per eMail**

**AVG Diagnose** ist ein Hilfsprogramm für die Diagnose, das vom AVG Technischen Support vertrieben wird. Das Hauptziel ist, Informationen vom Hauptcomputer zu erhalten. Diese Information hilft dem technischen Support, Ihr Problem mit AVG zu lösen, indem gesammelte Protokolle, Fehlerberichte, Systeminformationen, verdächtige Dateien, Ihre eigenen Kommentare und andere Daten analysiert werden.

Für weitere Einzelheiten zum Hilfsprogramm **AVG Diagnose** gehen Sie bitte zu Kapitel [15.1 AVG Diagnose-Hilfsprogramm](#).

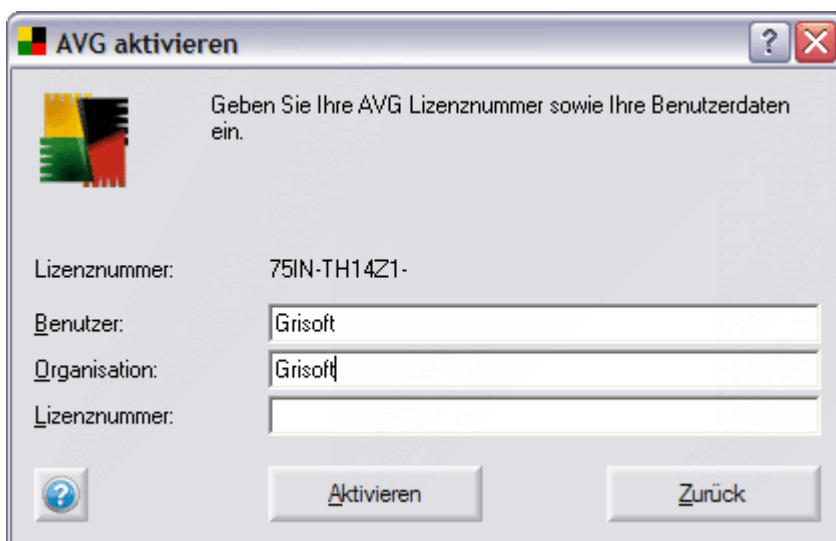
**Anmerkung:** Das Hilfsprogramm AVG Diagnose sendet niemals persönliche Daten oder andere sensible Daten von Ihrem Computer weiter, ohne besonderes Einverständnis des Benutzers. Der Benutzer kann den Inhalt aller gesammelten Dateien überprüfen und verhindern, dass diese an den technischen Support gesendet werden.

d) **Registrieren im Internet**

Diese Option öffnet die AVG Registrierungs- Webseite.

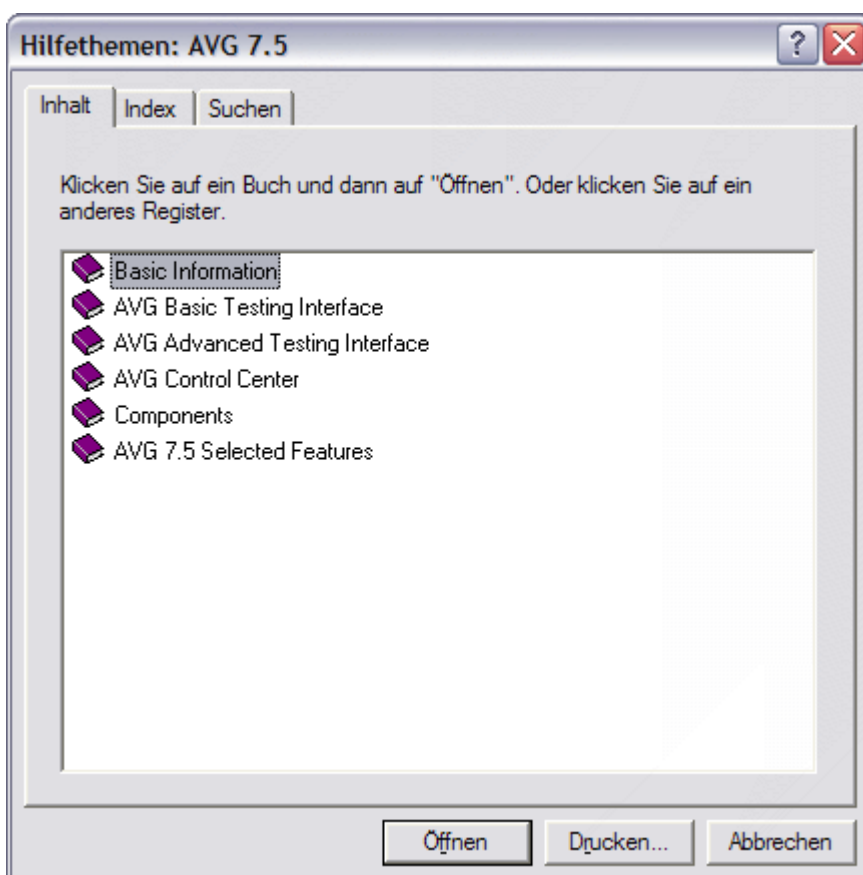
e) **AVG aktivieren**

Diese Option öffnet ein Fenster, in dem Sie Ihre Lizenznummer eintragen müssen, um Ihr AVG zu aktivieren



## f) Verzeichnis der Hilfethemen

Diese Option gibt einen Überblick über den Hilfe-Inhalt, Hilfe-Index und ermöglicht eine schnelle Suche innerhalb der Hilfethemen.



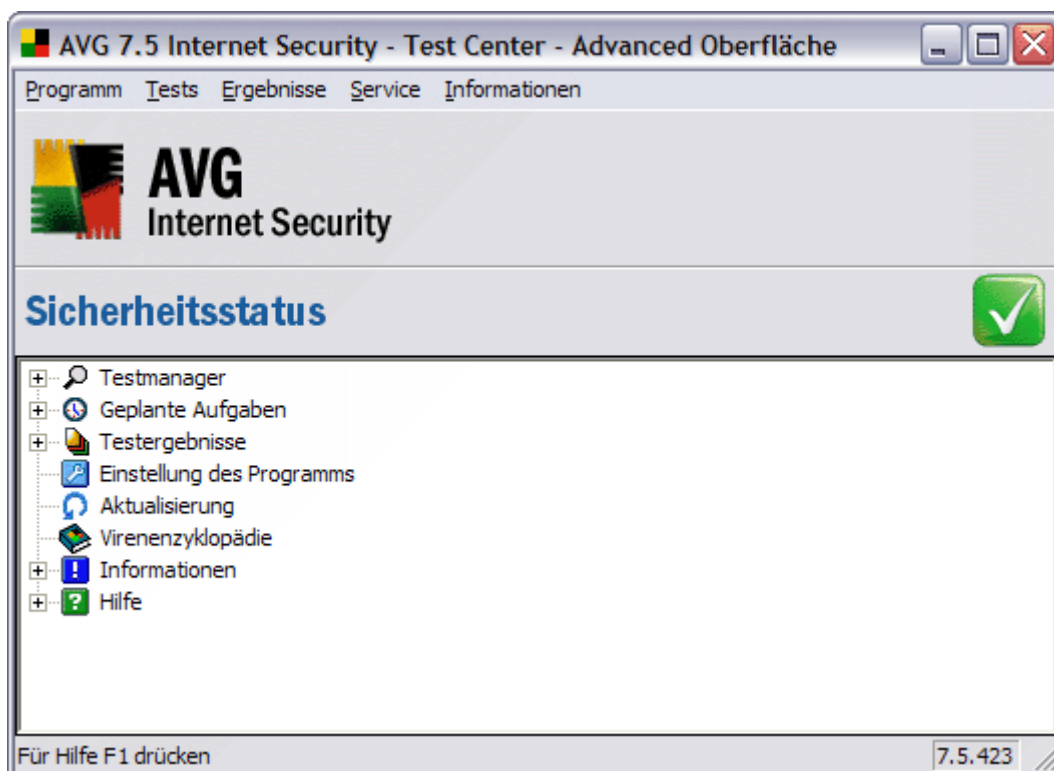
## g) Hilfe zu AVG

Diese Option öffnet ein neues Fenster mit kurzen Hilfetexten.




## 8. AVG Advanced Oberfläche

Die **Advanced Oberfläche** bietet alle AVG-Funktionen (Test, Aktualisierungen, Scheduler, vollständige Konfiguration) und bietet Ihnen gleichzeitig wesentlich mehr Kontrollmöglichkeiten über alle Funktionen von AVG.

Die Verwendung der **Advanced Oberfläche** wird fortgeschrittenen Nutzern empfohlen.



Zusätzlich können Sie den Sicherheitsstatus von AVG im Hauptbereich des Test Centers anzeigen lassen. Hierfür gibt es drei Möglichkeiten der Anzeige:

-  Ihr Computer ist vollständig geschützt, aktualisiert und alle installierte Komponenten arbeiten fehlerfrei
-  Eine oder mehrere Komponenten sind fehlerhaft konfiguriert und Sie sollten ihre Eigenschaften/Einstellungen überprüfen. Die Problem-Komponenten werden in der Benachrichtigung über den Status aufgelistet.
-  Zeigt an, dass Sie sich dafür entschieden haben, den fehlerhaften Status einer Komponente zu ignorieren.

**Anmerkung:** Zum schnellen Öffnen des Control Centers doppelklicken Sie einfach in den Bereich Sicherheitsstatus. Um auf die Basis Oberfläche umzuschalten wählen Sie aus dem Hauptmenü Programm/Zur Basis Oberfläche umschalten.

Im Menü der **Advanced Oberfläche** finden Sie die folgenden Einträge:

### 8.1. Testmanager

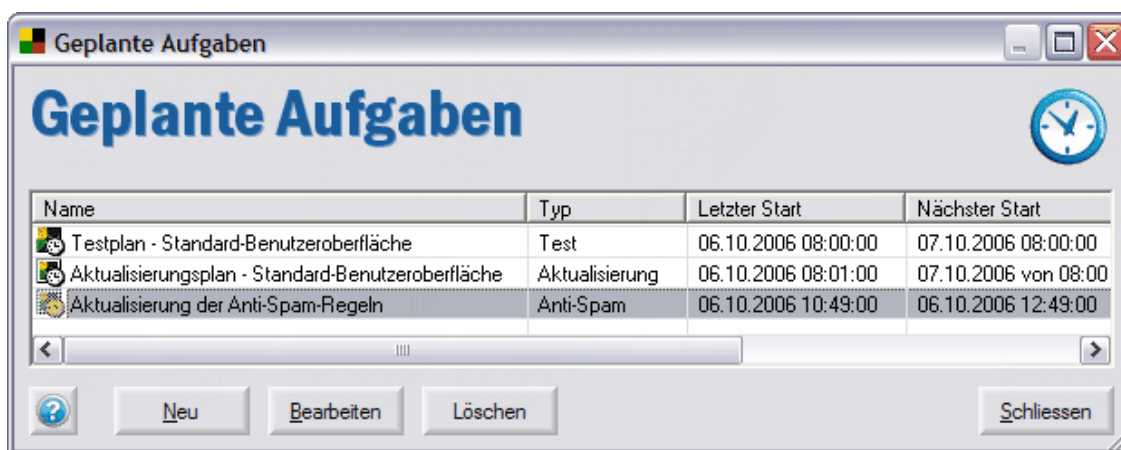
Der Abschnitt **Testmanager** enthält eine Liste der vordefinierten Tests, die mit AVG durchgeführt werden können. Sie können jeden dieser Tests von hier aus starten.

Für weitere Informationen zu den Test Arten lesen Sie bitte das Kapitel [13. Test Übersicht](#).

### 8.2. Geplante Aufgaben

Der Abschnitt **Geplante Aufgaben** enthält eine Liste aller geplanten AVG-Tests/AVG-Aktualisierungen.

Ein Doppelklick auf den Menüeintrag öffnet ein neues Dialogfenster **Geplante Aufgaben**:



Dieses Dialogfenster bietet eine wesentlich ausführlichere Beschreibung aller geplanten Aufgaben:

- Name – der vollständige Name der geplanten Aufgabe
- Typ – Art der geplanten Aufgabe (Aktualisierung/Test/Anti-Spam)
- Letzter Start – wann wurde die Aufgabe das letzte Mal durchgeführt (Datum und Zeit)
- Nächster Start – wann soll die Aufgabe das nächste Mal durchgeführt werden (Datum und Zeit)
- Status – zeigt den Status der Aufgabeneinstellung an
- Geplant für – zeigt an, für wen die Aufgabe geplant ist

Im unteren Bereich des Fensters finden Sie die Schaltflächen Neu/Bearbeiten, die Sie für geplante Aufgaben verwenden können:

#### a) Neue Aufgabe

Die Schaltfläche **Neu** öffnet ein Dialogfenster, in dem Sie eine neue Aufgabe und die dazugehörigen Parameter auf vier Reitern definieren können.

- **Aufgabe** – geben Sie den **Namen** und den **Kommentar** für die Aufgabe an, **Aufgabentyp** (Test/Aktualisierung/Aktualisierung der Anti-Spam-Regeln) und wenn möglich auch die **Option** (Priorität für Aktualisierungen und Art des Tests für Tests).

Sie können auch festlegen, ob die Aufgabe für alle Benutzer oder nur für den aktuellen Benutzer geplant werden soll

**Anmerkung:** Eine Aufgabe nur für den aktuellen Benutzer zu planen bedeutet, dass diese Aufgabe vom Control Center gestartet wird, nachdem sich dieser Benutzer angemeldet hat. Wenn Sie gewährleisten möchten, dass diese Aufgabe auch ausgeführt wird, wenn kein Benutzer angemeldet ist, empfehlen wir, die Aufgabe für eine Workstation zu planen; diese Aufgabe wird dann durch den Alarm Manager gestartet und ist nicht von einem laufenden Control Center abhängig.

Aufgaben, die sich auf ein Netzlaufwerk beziehen (wie z.B. Aktualisierung aus einem Netzlaufwerk oder Tests von Netzlaufwerken) müssen nur für den aktuellen Benutzer geplant werden und nicht für die ganze Station. Der Grund hierfür ist, dass der Alarm Manager über die lokalen Systemeinstellungen betrieben wird und die Netzlaufwerke nicht erkennt (dieses Problem tritt nur beim Windows NT-System, d.h. Windows 2000, Windows 2003, Windows XP PRO usw. auf, es gilt nicht für Windows 95, Windows 98, Windows ME und Windows XP Home).

Sie können das Kästchen **Diese Aufgabe deaktivieren** markieren, damit die Aufgabe nicht ausgeführt wird.

- **Ausführen** – definiert die Wiederholungsfrequenz der Aufgabe, exakte Zeiteinstellung sowie den Start/End Zeitpunkt

- **Verhalten** – Entscheidung, ob Sie informiert werden möchten, bevor die Aufgabe gestartet wird
- **Fehler** – wählt die Maßnahme aus, die durchgeführt werden soll, wenn die Aufgabe fehlschlägt

#### b) Bearbeiten

Die Schaltfläche **Bearbeiten** öffnet dasselbe Dialogfenster für eine schon definierte Aufgabe, d.h. der Aufgabenname und die notwendigen Parameter wurden bereits definiert und Sie haben nun die Möglichkeit, diese zu editieren.

#### c) Löschen

Die Schaltfläche **Löschen** löscht die ausgewählten Aufgaben (hervorgehoben) aus der Liste der Aufgaben im Dialogfenster **Geplante Aufgaben**.


#### d) Schliessen

Die Schaltfläche **Schliessen** beendet das Dialogfenster **Geplante Aufgaben**.

### 8.3. Testergebnisse

Im Menü **Testergebnisse** wird eine Liste der bislang durchgeführten Tests, deren Parameter und die entsprechenden Ergebnisse angezeigt.

Doppelklicken Sie auf den Eintrag **Testergebnisse**, um ein neues Dialogfenster **Testergebnisse** zu öffnen:



Name des Tests	Startdatum	Startzeit	Getestete Objekte	Viren	Fehler
Kompletter Test	05.10.2006	15:04:48	217	0	0
Benutzertest	05.10.2006	15:08:47	981	0	0
Benutzertest	05.10.2006	15:10:53	85	2	0
Benutzertest	05.10.2006	15:22:57	99	11	0
Kompletter Test	06.10.2006	08:00:06	1391	0	0

Buttons: Einzelheiten, Testeinstellungen, Löschen, Testergebnis, Schliessen

Das Dialogfenster bietet weitergehende Informationen zu den durchgeführten Tests:

- **Name des Tests** – vollständiger Name des durchgeführten Tests
- **Startdatum** – Datum, an dem der Test durchgeführt wurde
- **Startzeit** – exakter Zeitpunkt, an dem der Test durchgeführt wurde
- **Getestete Objekte** – Anzahl der Objekte, die während des Tests überprüft wurden

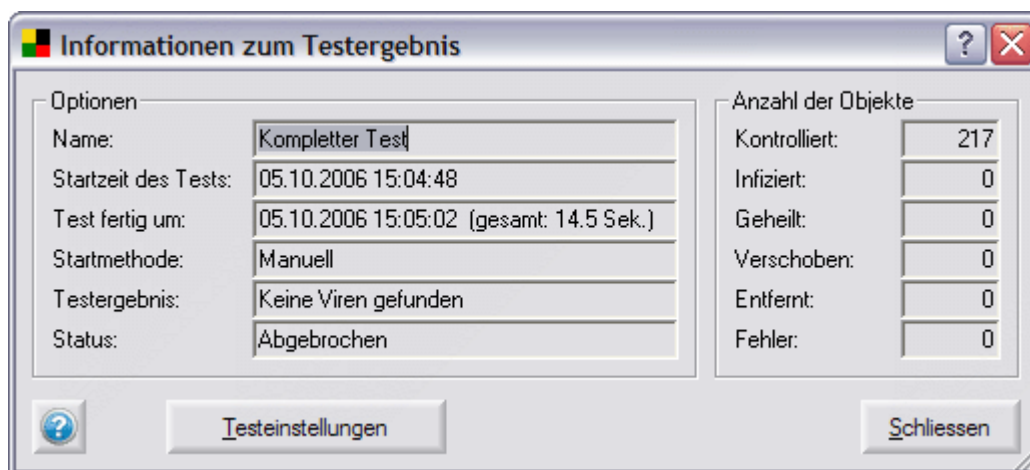
- **Viren** – Anzahl der gefundenen Viren (sollte ein Virus während des Tests gefunden worden sein, so erscheint das Testsymbol in rot; sollte der Test unterbrochen worden sein, dann erscheint das Testsymbol zerrissen)
- **Fehler** – Anzahl der Fehler, die während des Testdurchlaufs aufgetreten sind

**Anmerkung:** Für weitere Informationen zu den Testergebnissen lesen Sie bitte das Kapitel [13.1 d\) – Kompletter Test - Testergebnis](#). Dieses Kapitel beschreibt Warnungen, die über während des Tests gefundene verdächtige Dateien informieren, Erkennung infizierter Archive und die Möglichkeiten zur Behandlung von enthaltenen Dateien und Möglichkeiten zum Filtern der angezeigten Testergebnisse.

Der untere Bereich des Fensters bietet die folgenden Schaltflächen:

#### a) Einzelheiten

Die Schaltfläche **Einzelheiten** öffnet ein neues Fenster mit einem detaillierten Bericht über den ausgewählten Test:

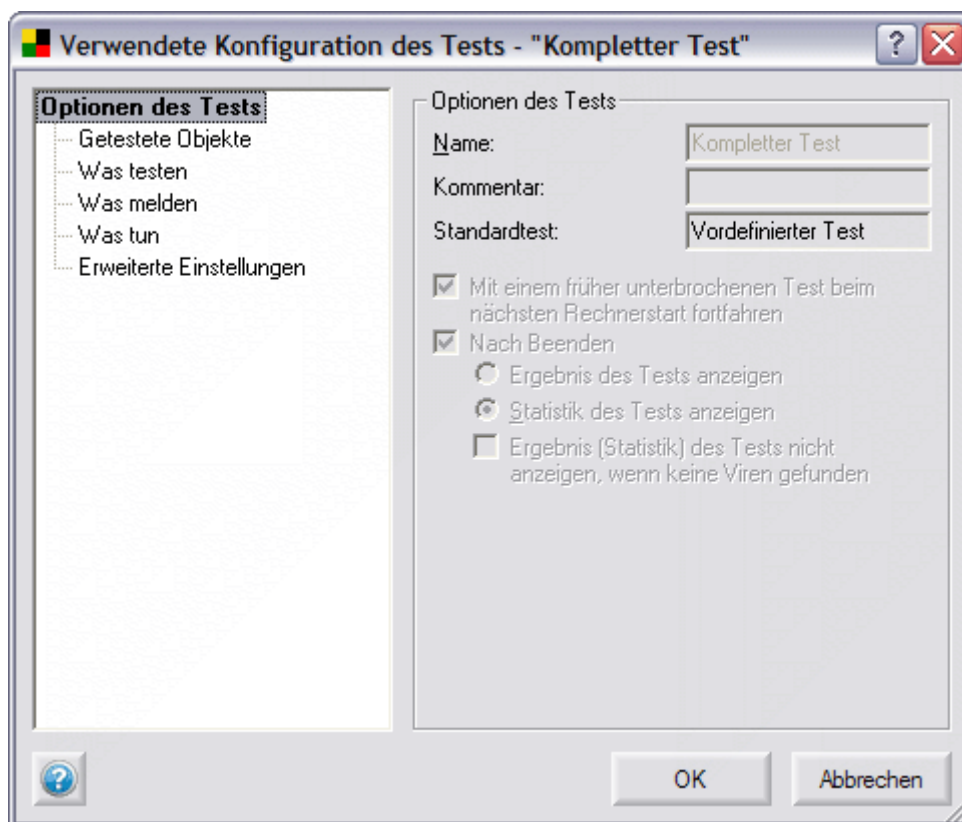


#### b) Testeinstellungen

Die Schaltfläche **Testeinstellungen** öffnet ein Fenster mit einem Bericht über die vollständige Testkonfiguration. In diesem Fenster können Sie sich verschiedene verwendete Testparameter anzeigen lassen, die sich zu Gruppen angeordnet im linken Menü befinden:

- **Optionen des Tests** – allgemeine Beschreibung des Tests
- **Getestete Objekte** – definiert, welche Objekte während des Tests überprüft werden sollen
- **Was testen** – definiert die verwendeten Testmethoden; anhand der Dateierweiterungen können Sie festlegen, ob Dateien überprüft/nicht überprüft werden sollen; weiterhin können Sie entscheiden, ob Archive getestet werden sollen
- **Was melden** – definiert, welche Ereignisse während eines Tests gemeldet werden sollen
- **Was tun** – definiert, was passieren soll, wenn ein Virus gefunden wird/eine Warnung angezeigt wird

- o **Erweiterte Einstellungen** – definiert Parameter der Testbenachrichtigung; es definiert, ob das Control Center nach Beendigung des Tests geschlossen werden soll und zeigt die Festlegung die Testpriorität und der Länge der Pausen zwischen einzelnen Tests an.



c) **Löschen**

Die Schaltfläche **Löschen** entfernt die ausgewählten (hervorgehobenen) Testergebnisse aus der Liste im Fenster **Testergebnisse**.

d) **Testergebnis**

Die Schaltfläche **Testergebnis** öffnet eine Übersicht mit Informationen über die detaillierten Testergebnisse des ausgewählten Tests. Weitere Informationen zu diesem Dialog erhalten Sie in Kapitel [7.4 Testergebnisse, Abschnitt d\)](#).

e) **Schliessen**

Die Schaltfläche **Schliessen** beendet das Dialogfenster **Einzelheiten des Testergebnisses**.

**Anmerkung:** Für weitere Informationen zu den Testergebnissen lesen Sie bitte auch Kapitel [13.1 d\) – Kompletter Test - Testergebnis](#).

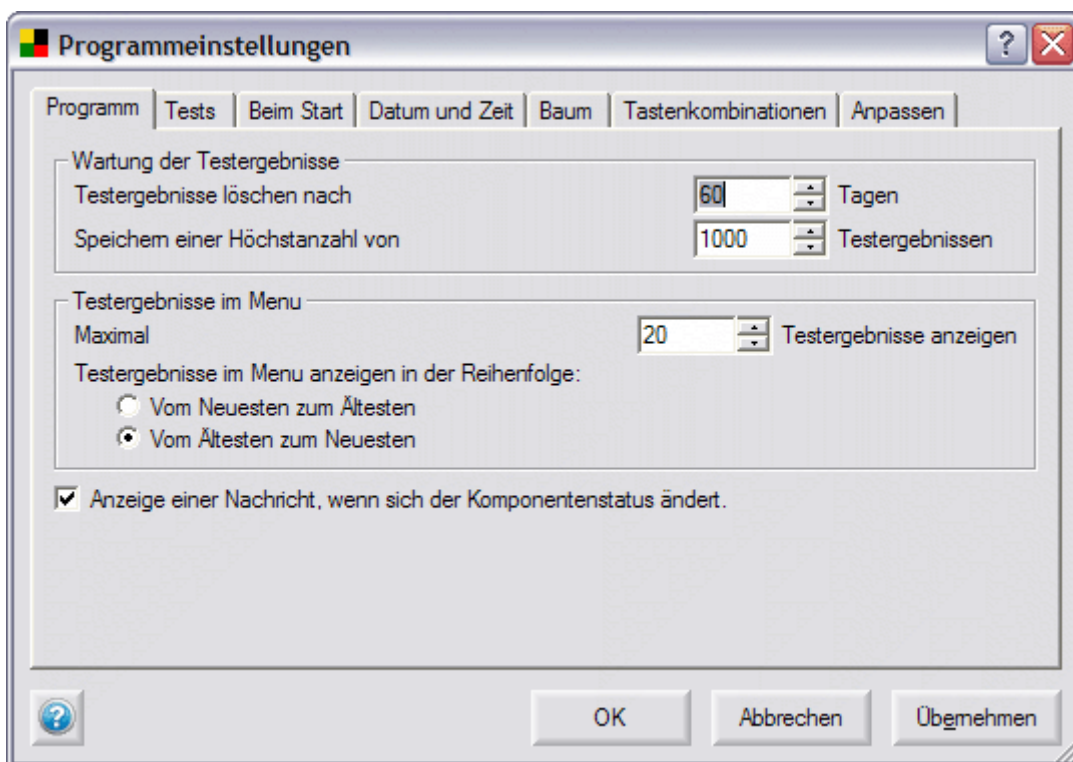
## 8.4. Programmeinstellungen

Der Menüeintrag **Programmeinstellungen** öffnet ein Fenster mit verschiedenen Reitern, die die Möglichkeit bieten, verschiedene Programmparameter zu definieren:

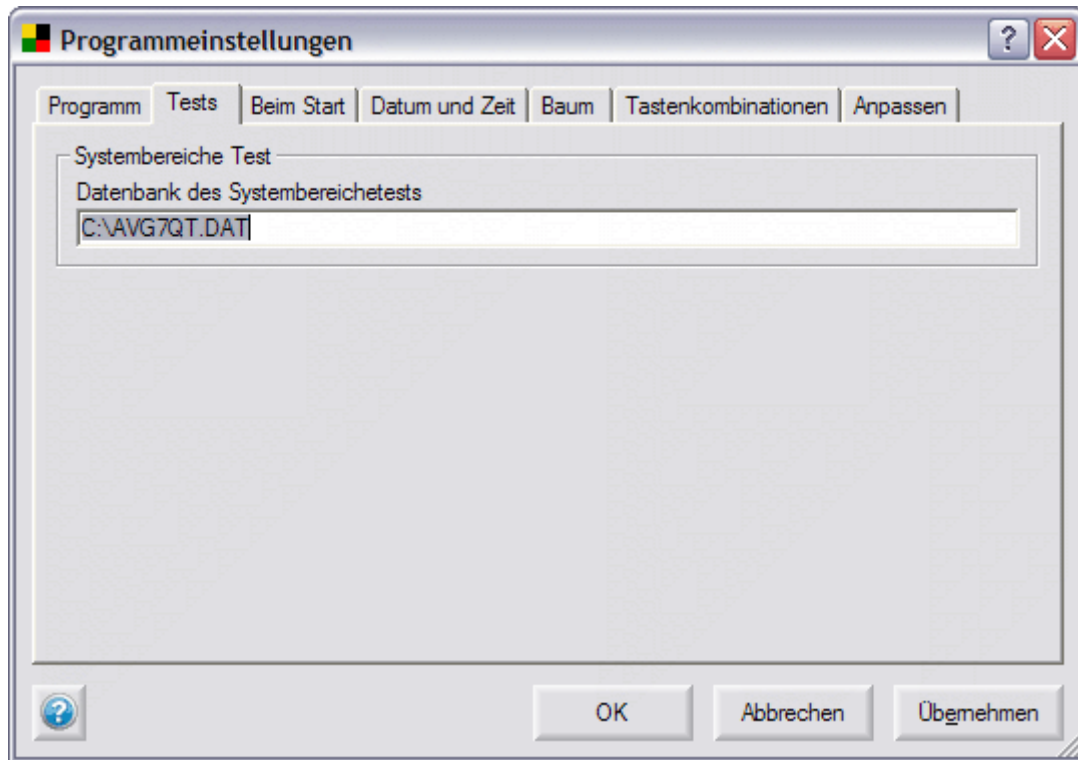
a) **Programm**

- **Wartung der Testergebnisse**
  - **Testergebnisse löschen nach** – geben Sie an, wie lange Sie die Testergebnisse speichern möchten
  - **Speichern einer Höchstanzahl von** – geben Sie an, wie viele der letzten Testergebnisse Sie speichern möchten
- **Testergebnisse im Menü**
  - **Maximal** – geben Sie an, wie viele der bislang durchgeführten Tests im Abschnitt **Testergebnisse** der **Advanced Oberfläche** angezeigt werden sollen
  - **Testergebnisse im Menü anzeigen in der Reihenfolge:**  
definieren Sie, welche Sortierung der Testergebnisse Sie bevorzugen

Sie können auch die Option auswählen **Anzeige einer Nachricht, wenn sich der Komponentenstatus ändert**.

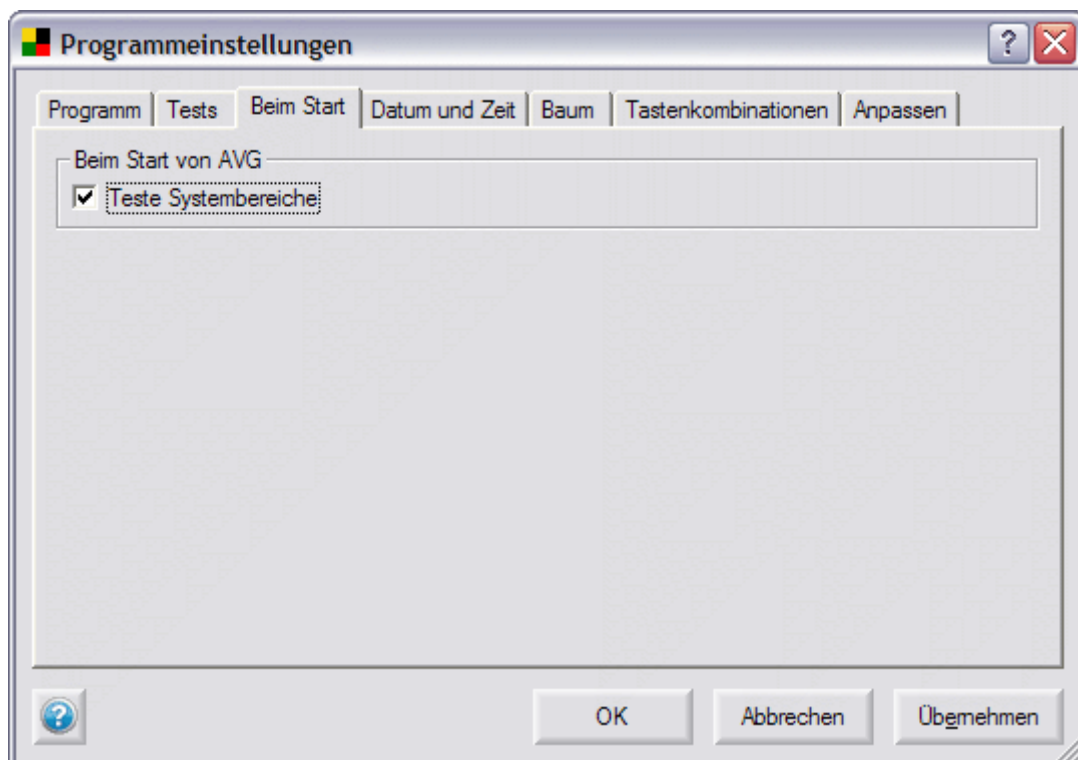
b) **Tests**

Bereich **Systembereichetest** – geben Sie den Namen und den Speicherort der Datenbank für den Systembereichetest an.



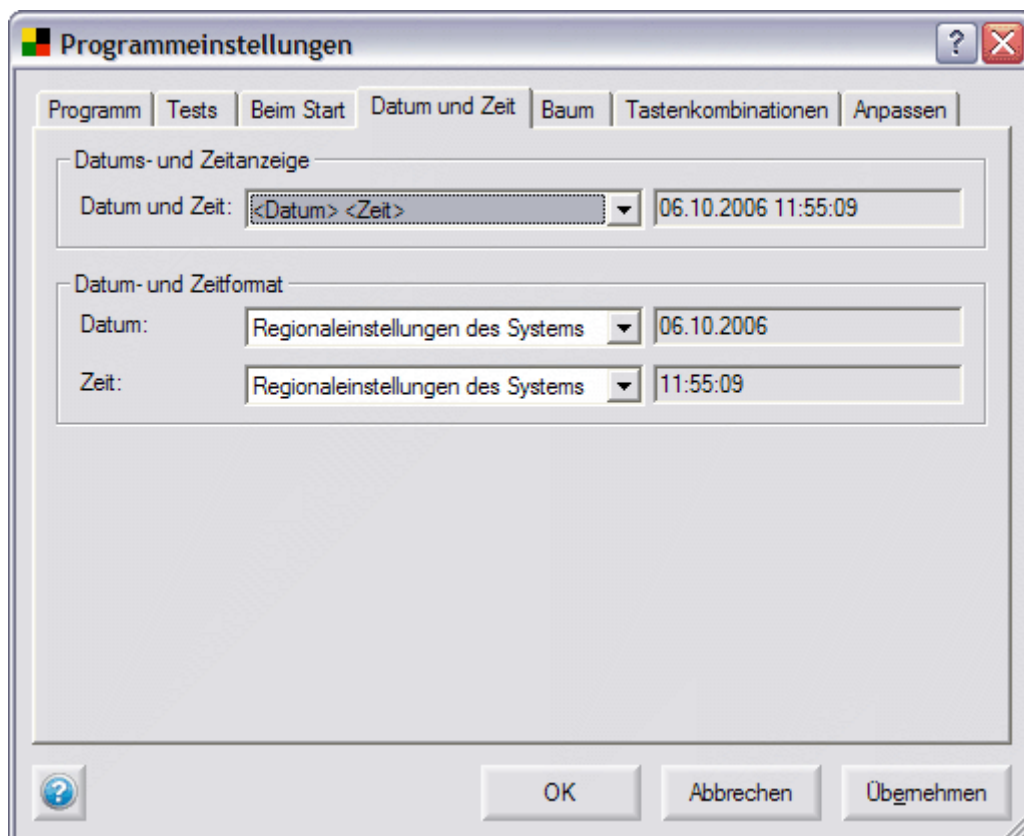
c) **Beim Start**

**Teste Systembereiche** – bestimmen Sie, ob der Systembereichstest beim Start von AVG durchgeführt werden soll

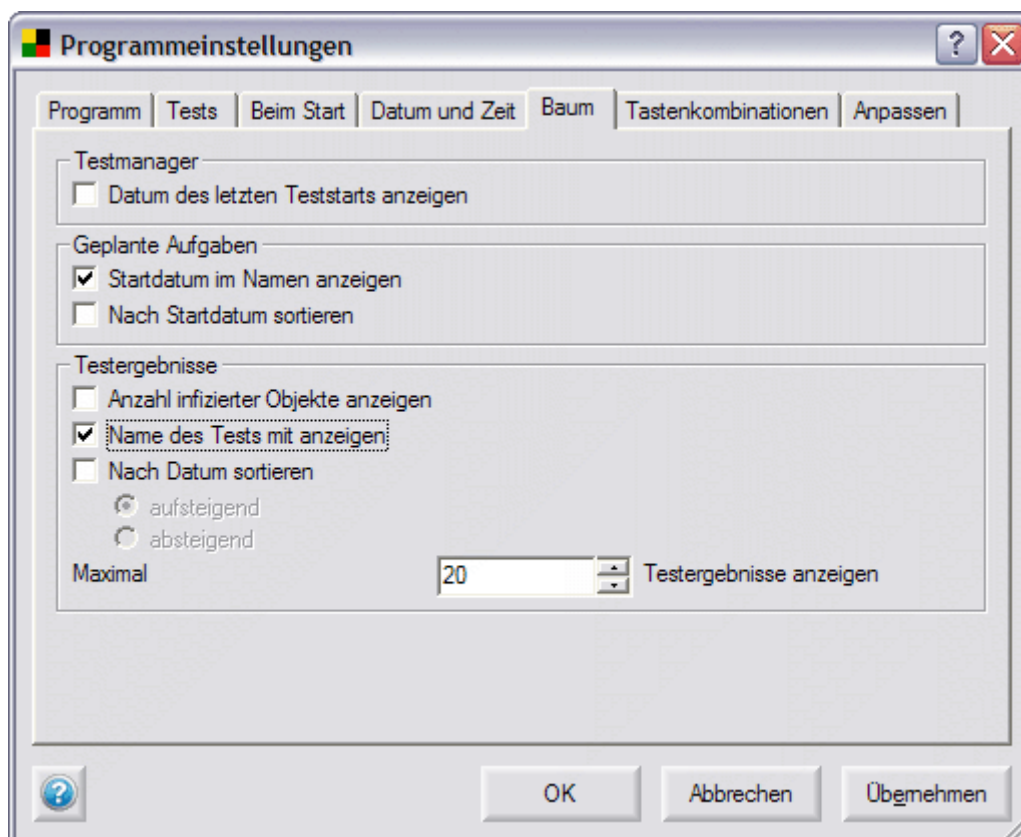


**d) Datum und Zeit**

- **Datums- und Zeitanzeige**
  - **Datum und Zeit** – wählen Sie die bevorzugte Anzeigart von Datum und Zeit (wenn das Datum und die Zeit zusammen angezeigt werden sollen)
- **Datum- und Zeitformat**
  - **Datum** – wählen Sie die bevorzugte Anzeigart des Datums aus
  - **Zeit** – wählen Sie die bevorzugte Anzeigart der Zeit aus



## e) Baum

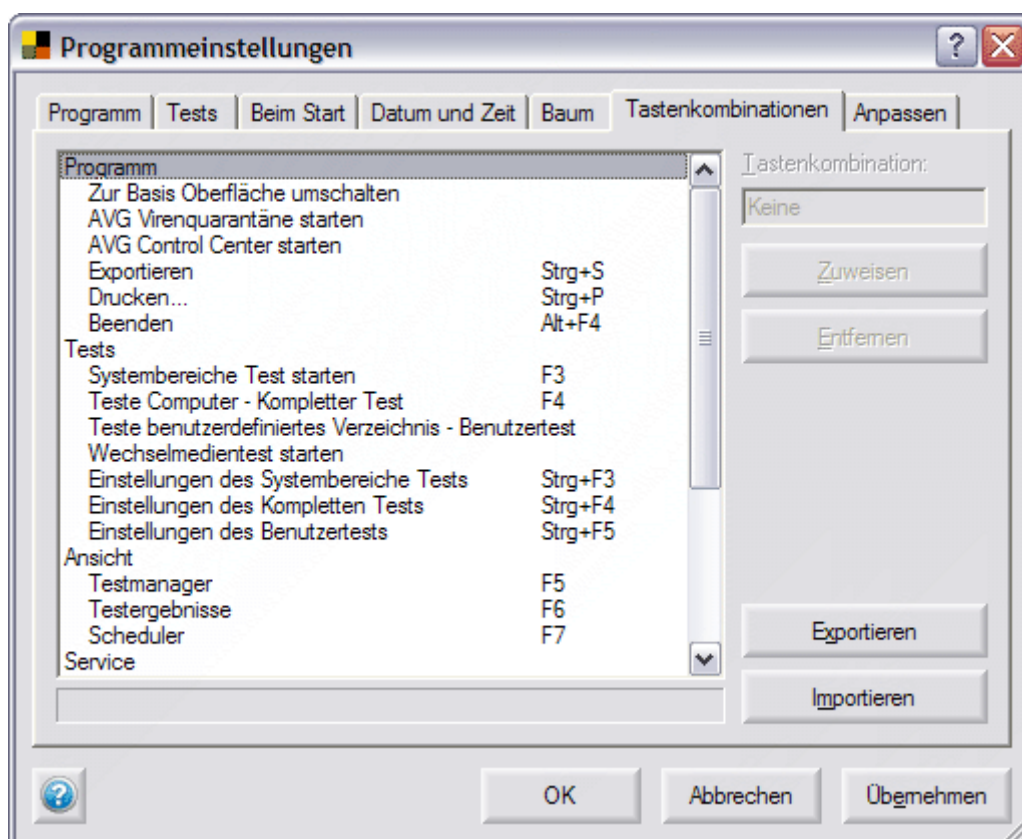


- Zweig **Testmanager**
  - **Datum des letzten Teststarts anzeigen** – im Menü der **Advanced Oberfläche** aktivieren/deaktivieren Sie die Anzeige des letzten Startdatums
- Zweig **Geplante Aufgaben**
  - **Startdatum im Namen anzeigen** - aktivieren/deaktivieren Sie die Anzeige des Datums der letzten geplanten Aufgabe zusammen mit dem Aufgabennamen
  - **Nach Startdatum sortieren** – bestimmen Sie, ob die geplanten Aufgaben entsprechend Ihrem Startdatum in chronologischer Reihenfolge angezeigt werden sollen
- Zweig **Testergebnisse**
  - **Anzahl infizierter Objekte anzeigen** – aktivieren/deaktivieren Sie die Anzeige der Anzahl der gefundenen infizierten Objekte
  - **Name des Tests mit anzeigen** – aktivieren/deaktivieren Sie die Anzeige des Testnamens zusammen mit der Information über das Testergebnis
  - **Nach Datum sortieren** – bestimmen Sie, ob die Testergebnisse aufsteigend/absteigend sortiert werden sollen
  - **Maximal** – bestimmen Sie die maximale Anzahl an Testergebnissen, die im Menü angezeigt werden sollen

### f) Tastenkombinationen

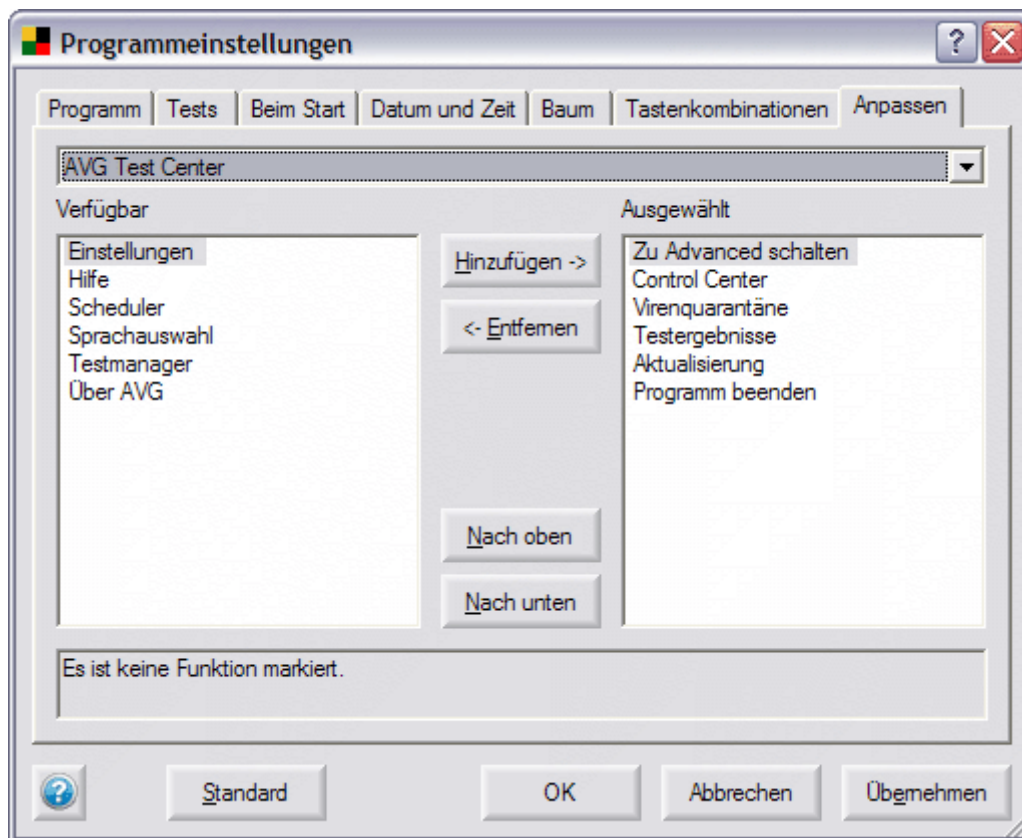
Der Reiter **Tastenkombinationen** erlaubt Ihnen das Einrichten eigener Tastenkombinationen mit Hilfe der folgenden Schaltflächen:

- **Zuweisen** – definieren Sie eine neue Tastenkombination für die ausgewählte Funktion
- **Entfernen** – entfernen Sie die aktuelle Tastenkombination für die ausgewählte Funktion
- **Exportieren** – wählen Sie ein Verzeichnis aus, in das Sie die aktuellen Einstellungen der Tastenkombinationen exportieren möchten
- **Importieren** – wählen Sie das Verzeichnis aus, aus dem Sie die neuen Tastenkombinationen importieren möchten



g) **Anpassen**

Der Reiter **Anpassen** erlaubt Ihnen die Wahl der AVG-Funktionen, die Sie im **Test Center/AVG Control Center** verwenden möchten:



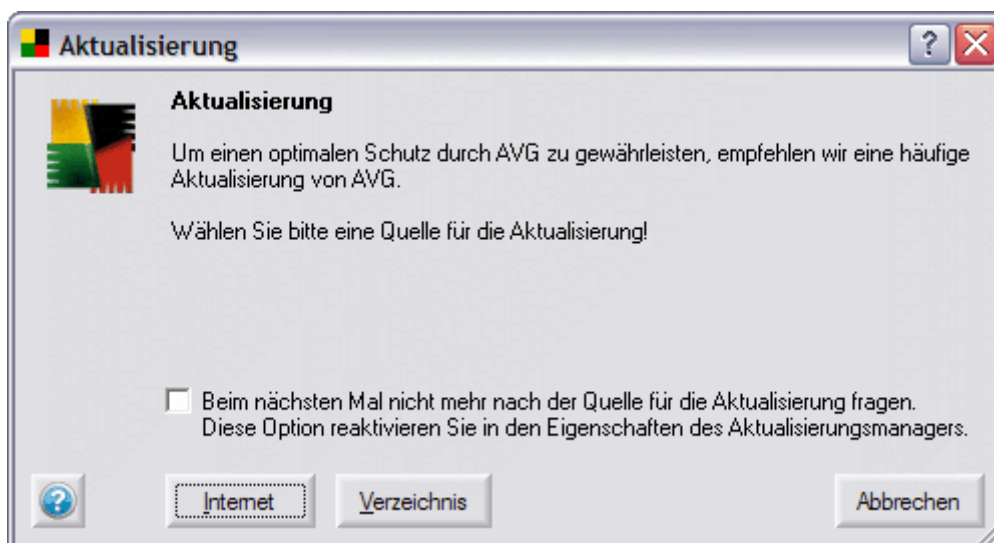
Verschiedene Reiter bieten die folgenden Schaltflächen an:

- **Standard** – die geänderten Konfigurationseinstellungen werden auf die Standardwerte zurückgesetzt
- **OK** – alle Änderungen an den Programmparametern werden übernommen und das Dialogfenster wird geschlossen
- **Abbrechen** – alle Änderungen an den Programmparametern werden verworfen und das Dialogfenster wird geschlossen
- **Übernehmen** – alle Änderungen der Programmparameter werden übernommen und das Dialogfenster bleibt geöffnet

### 8.5. Aktualisierung

Der Menüeintrag **Aktualisierung** ruft ein Fenster auf, das eine sofortige Aktualisierung von AVG bietet. Die Aktualisierung kann entweder über das Internet oder über ein Netzwerkverzeichnis vorgenommen werden. Um die Aktualisierung abzubrechen, klicken Sie auf die Schaltfläche **Abbrechen**.

(Für weitere Informationen zu Aktualisierungsmöglichkeiten lesen Sie bitte das Kapitel [14. Programm-Aktualisierungen](#).)



In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- **Internet** – startet die AVG-Aktualisierung aus dem Internet
- **Verzeichnis** – öffnet ein Dialogfenster, in dem Sie das Aktualisierungs-Quellverzeichnis (entweder lokal oder im Netzwerk) angeben müssen; drücken Sie die Schaltfläche **OK**, um die Auswahl zu bestätigen und die AVG-Aktualisierung zu starten
- **Abbrechen** – schließt das Dialogfenster Aktualisierung

Wenn Sie immer dieselbe Quelle für die Aktualisierungsdateien nutzen wollen, aktivieren Sie bitte die Option **Beim nächsten Mal nicht mehr nach der Quelle für die Aktualisierung fragen**. Bei der nächsten Aktualisierung werden Sie daraufhin nicht mehr nach der Aktualisierungsquelle gefragt und die Aktualisierung wird automatisch von der angegebenen Quelle aus durchgeführt.

Wenn Sie die Aktualisierungsquellen-Abfrage in Zukunft wieder im **Aktualisierung**dialog angezeigt bekommen möchten, können Sie diese in der Komponente **Aktualisierungsmanager** im Control Center einstellen – für eine detaillierte Beschreibung der Einstellungen lesen Sie bitte auch im Kapitel [9.14–AVG Control Center – Aktualisierungsmanager](#) den Abschnitt **Optionen**.

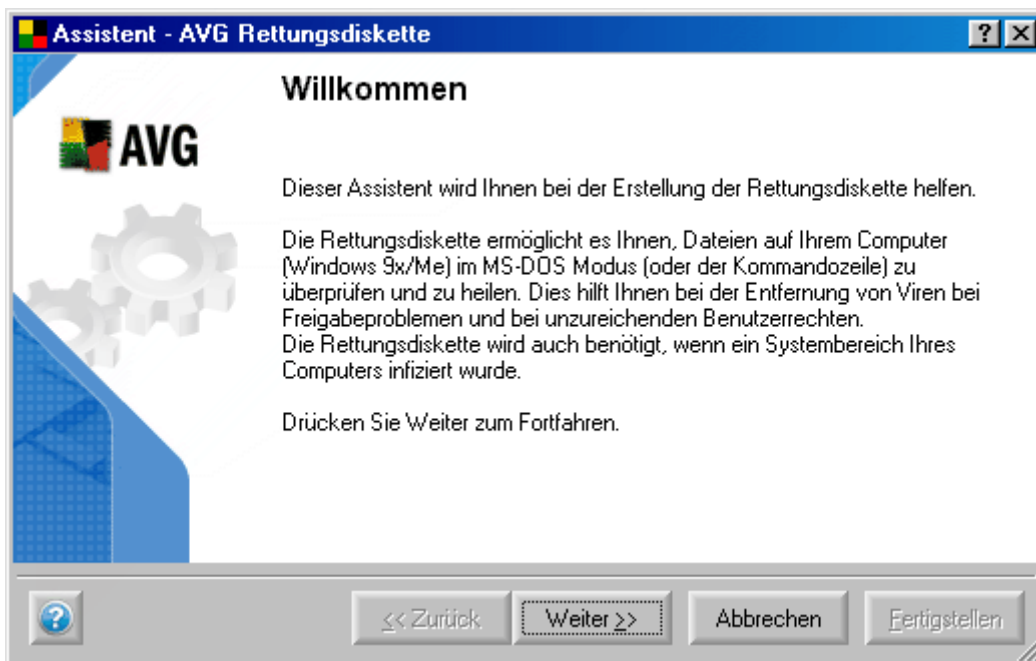
## 8.6. Rettungsdiskette

**Windows XP und aufwärts wird vom Feature Rettungsdiskette nicht mehr unterstützt.**

Diese Funktion ist hilfreich, wenn Sie Viren von einem Computer entfernen müssen:

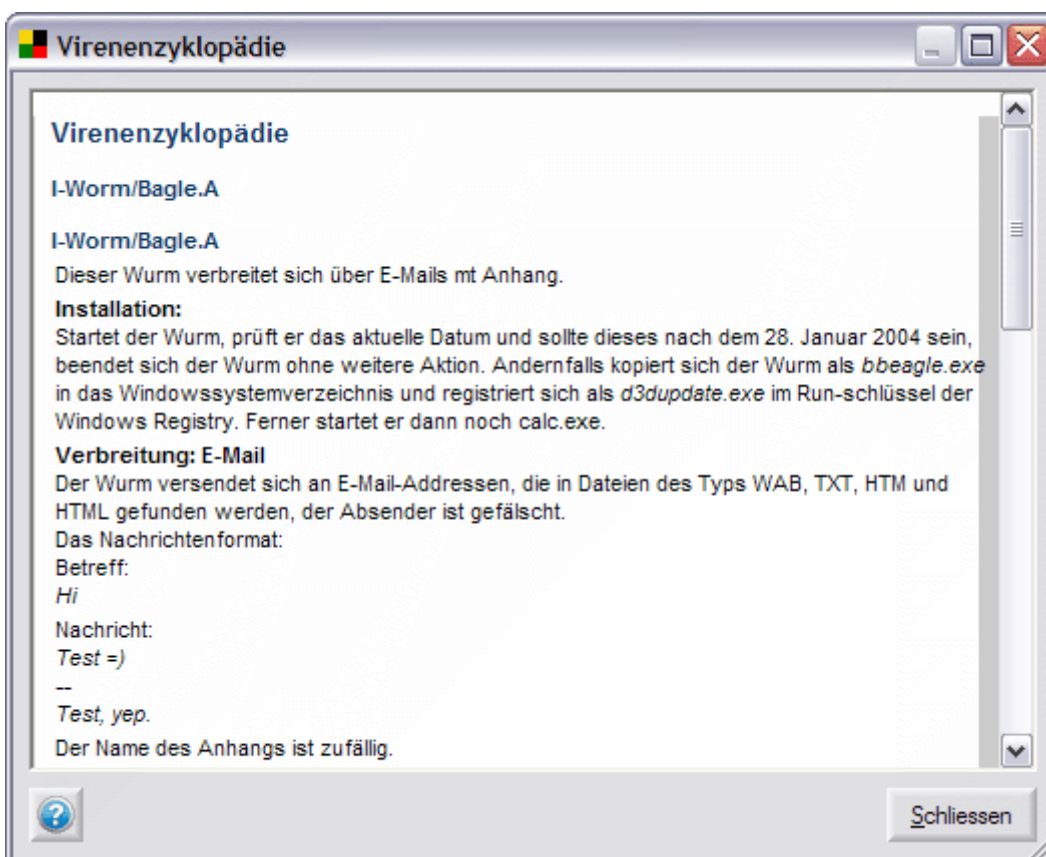
- der Freigabeprobleme besitzt
- für den Sie nicht die entsprechenden Zugriffsrechte besitzen
- bei dem die Systembereiche infiziert sind

Der Menüeintrag **Rettungsdiskette** ruft einen Assistenten auf, der Sie durch den Erstellungsprozess einer Rettungsdiskette führt. Um die **Rettungsdiskette** zu erstellen, folgen Sie bitte den Anweisungen im Assistenten.



### 8.7. Virenenzyklopädie

Der Menüeintrag **Virenenzyklopädie** öffnet ein Fenster, in dem Sie die Möglichkeit haben, Viren nach ihrem Namen in einer Datenbank aller bekannten Viren zu suchen. Die **Virenenzyklopädie** kann nur im Online-Modus genutzt werden!



### 8.8. Informationen

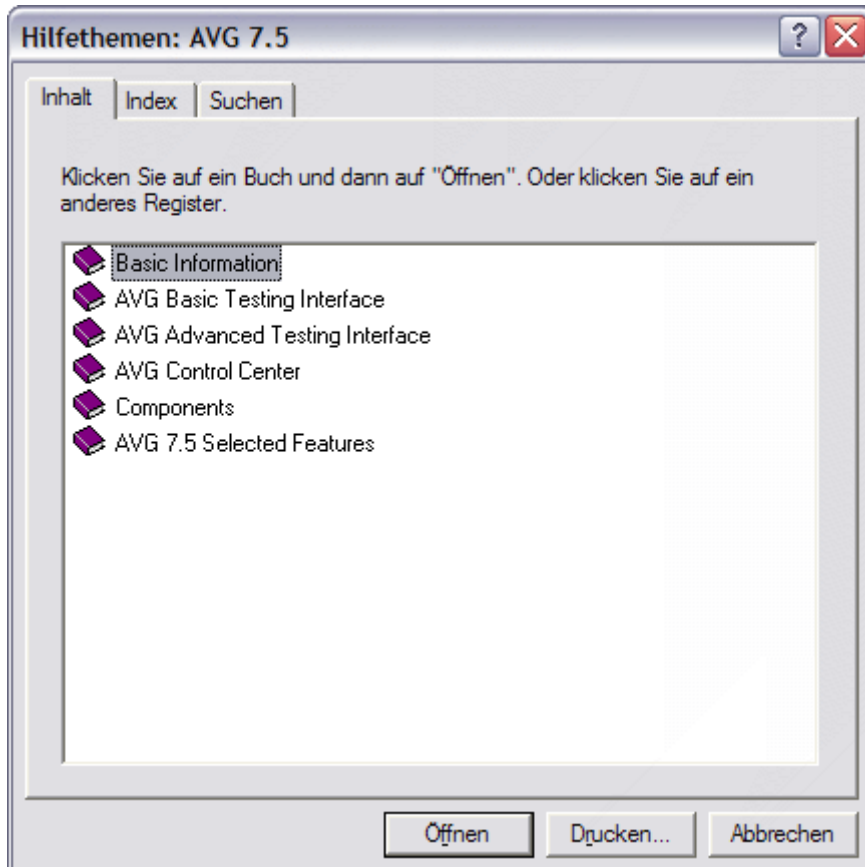
Der Menüeintrag **Informationen** enthält eine Liste von Untereinträgen, die sich auf spezielle Reiter des neu geöffneten Dialogfensters mit AVG-Informationen bezieht:

- **Über das Programm** – zeigt Informationen über die installierte AVG-Version an
- **Über die Version** – zeigt Informationen zur Lizenznummer, benutzerbezogene Daten, Programmversion, Version der Virendatenbank und zur Anti-Spyware-Version an.
- **Über das System** – zeigt einen Überblick über den aktuellen Status des Betriebssystems an
- **Lizenzbedingungen** – zeigt den vollständigen Wortlaut der Lizenzbedingungen von AVG an
- **Kontakt** – bietet einen Überblick über die weltweiten AVG-Händler und Vertriebskontakte

### 8.9. Hilfethemen

Der Menüeintrag **Verzeichnis der Hilfethemen** öffnet ein Fenster mit Informationen zur Schnellhilfe von AVG:

- **Inhalt** – Überschriften der AVG-Hilfe
- **Index** – detaillierte Beschreibung von AVG-Hilfethemen
- **Suchen** – schnelle Stichwortsuche innerhalb der Hilfedatenbank






## 9. Control Center

Das **Control Center** ist die Hauptkontroll-Komponente von **AVG**. Im **Control Center** finden Sie Fenster für alle installierten Komponenten von **AVG 7.5 Internet Security** und die entsprechenden Kontroll-Schaltflächen, mit denen Sie die verschiedenen Parameter einstellen und den Status jeder Komponente überwachen können.

Standardmäßig startet das **Control Center** im Basis Modus, bei dem jeder Eintrag im Textformat aufgelistet ist. Sie können jederzeit auf den erweiterten Modus über das Menü **Ansicht** umschalten, sh. Kapitel [9.3 Control Center-Hauptmenü – b\). Ansicht.](#)

Das farbige (gelb, schwarz, rot und grün) **Control Center**-Symbol in der Windows Taskleiste zeigt den vollständig funktionsfähigen Zustand aller **AVG**-Komponenten an. Ein graues Symbol zeigt ein Problem an (inaktive Komponente, Fehler usw.). Ein Doppelklick auf das Symbol öffnet das Hauptfenster vom **AVG Control Center** zum Bearbeiten der Komponente.

Zusätzlich können Sie den **Sicherheitsstatus** von AVG im Hauptbereich des Control Centers überprüfen. An dieser Stelle erscheinen drei mögliche Symbole:

-  Ihr Computer ist vollständig geschützt, aktualisiert und alle installierten Komponenten arbeiten fehlerfrei.
-  Eine oder mehrere Komponenten sind fehlerhaft konfiguriert und Sie sollten ihre Eigenschaften/Einstellungen überprüfen. Die Problem-Komponenten werden in der Benachrichtigung zum Statusfehler aufgelistet.
-  Zeigt an, dass Sie sich dafür entschieden haben, den fehlerhaften Status einer Komponente zu ignorieren.

### 9.1. Start des AVG Control Center

Um das **Control Center** zu starten:

- Drücken Sie die Schaltfläche **Control Center** im linken Menü der **Basis Oberfläche**
- Wählen Sie **Programm/Control Center starten** im Hauptmenü der **Basis** oder **Advanced Oberfläche**
- Doppelklicken Sie auf das AVG-Symbol in der Windows- Taskleiste

Das **Control Center** öffnet sich mit diesem Bildschirmfenster:



**Anmerkung:** Die Liste der Komponenten im Control Center kann sich je nach Konfiguration und installierten Komponenten unterscheiden.

## 9.2. AVG Control Center linkes Menü

Die links im Control Center dargestellte Navigation zeigt in der Standardeinstellung die folgenden Menüeinträge:

Die Menüeinträge können jedoch geändert werden, Details hierzu erhalten Sie im Kapitel [8.4 Programmeinstellungen d\) Tastenkombinationen](#)

### a) Test Center

Der Menüeintrag **Test Center** startet das **Test Center**.

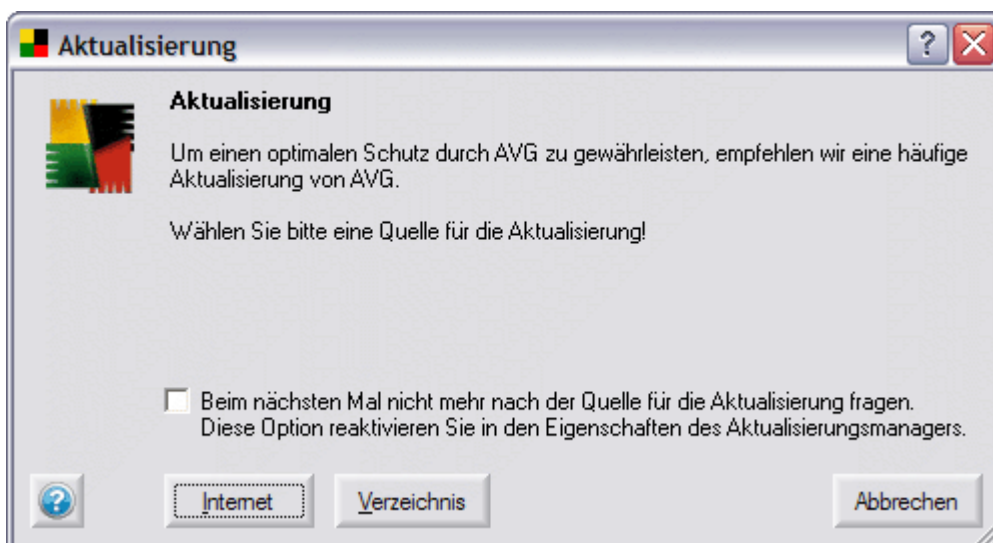
Für Details zur Basis/Advanced Oberfläche lesen Sie bitte die Kapitel [7. AVG Basic Oberfläche](#) und [8. AVG Advanced Oberfläche](#).)

### b) Hilfe

Der Menüeintrag **Hilfe** zeigt das Hilfefenster mit den entsprechenden Themen zum **Control Center** an:

### c) Aktualisierung

Der Menüeintrag **Aktualisierung** öffnet das Dialogfenster **Aktualisierung**



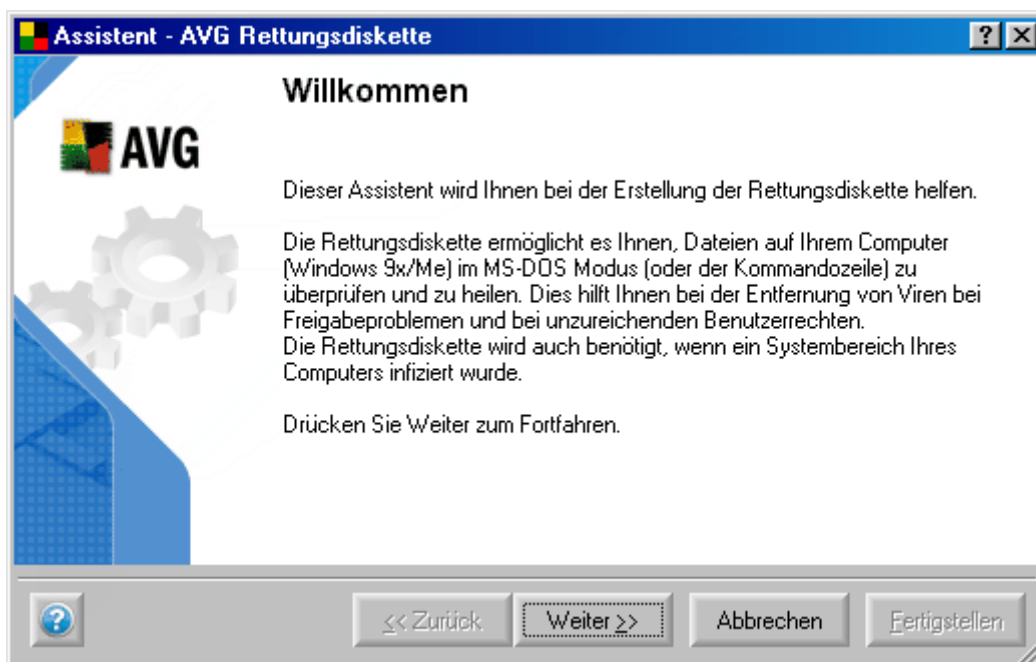
In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- **Internet** – startet die AVG-Aktualisierung aus dem Internet
- **Verzeichnis** – öffnet ein Dialogfenster, in dem Sie das Aktualisierungs-Quellverzeichnis (entweder lokal oder im Netzwerk) angeben müssen; drücken Sie die Schaltfläche OK, um die Auswahl zu bestätigen und um die AVG-Aktualisierung zu starten
- **Abbrechen** – schließt das Dialogfenster Aktualisierung

Für eine detaillierte Beschreibung der Aktualisierungsarten und der Möglichkeiten lesen Sie bitte auch Kapitel [14. Programm Aktualisierungen](#).

#### d) Rettungsdiskette

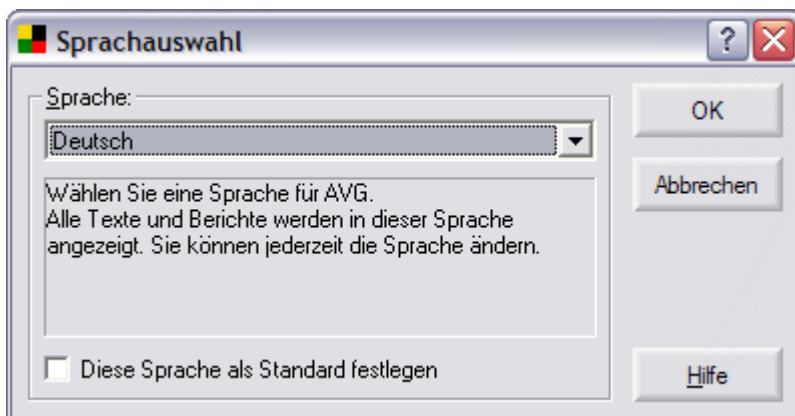
Der Menüeintrag **Rettungsdiskette** öffnet das Fenster des **Assistenten** zur Erstellung der **Rettungsdiskette**:



Für eine detaillierte Beschreibung zur Erstellung einer Rettungsdiskette lesen Sie bitte auch Kapitel [8.6 Rettungsdiskette](#).

## e) Sprachauswahl

Der Menüeintrag **Sprachauswahl** startet das Dialogfenster Sprachauswahl. Hier können Sie die Sprache für die Anwendung aus allen installierten Sprachen auswählen.



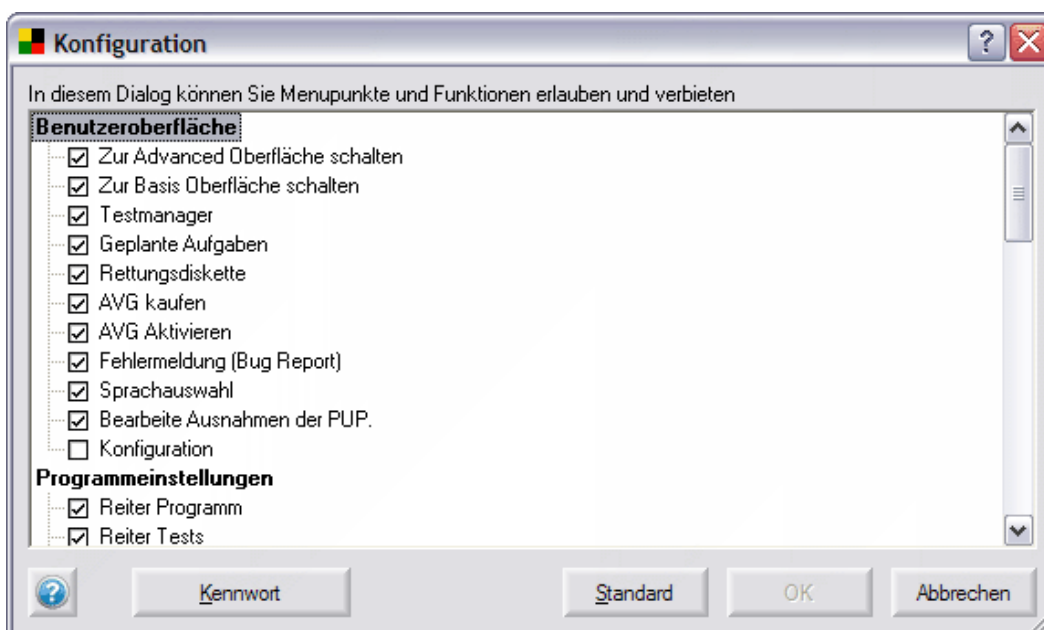
**Anmerkung:** Wenn Sie nur Englisch installiert haben, steht diese Schaltfläche nicht zur Verfügung.

## 9.3. AVG Control Center Hauptmenü

Neben den Standardmenüeinträgen (die für die **AVG**-Umgebung üblich sind) enthält das **Control Center** Hauptmenü folgende Optionen:

### a) Service/Optionen für den Administrator

Mit Hilfe dieser Option können Sie den Zugang zu verschiedenen Funktionen von **AVG** konfigurieren (gestatten/verbieten).



In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

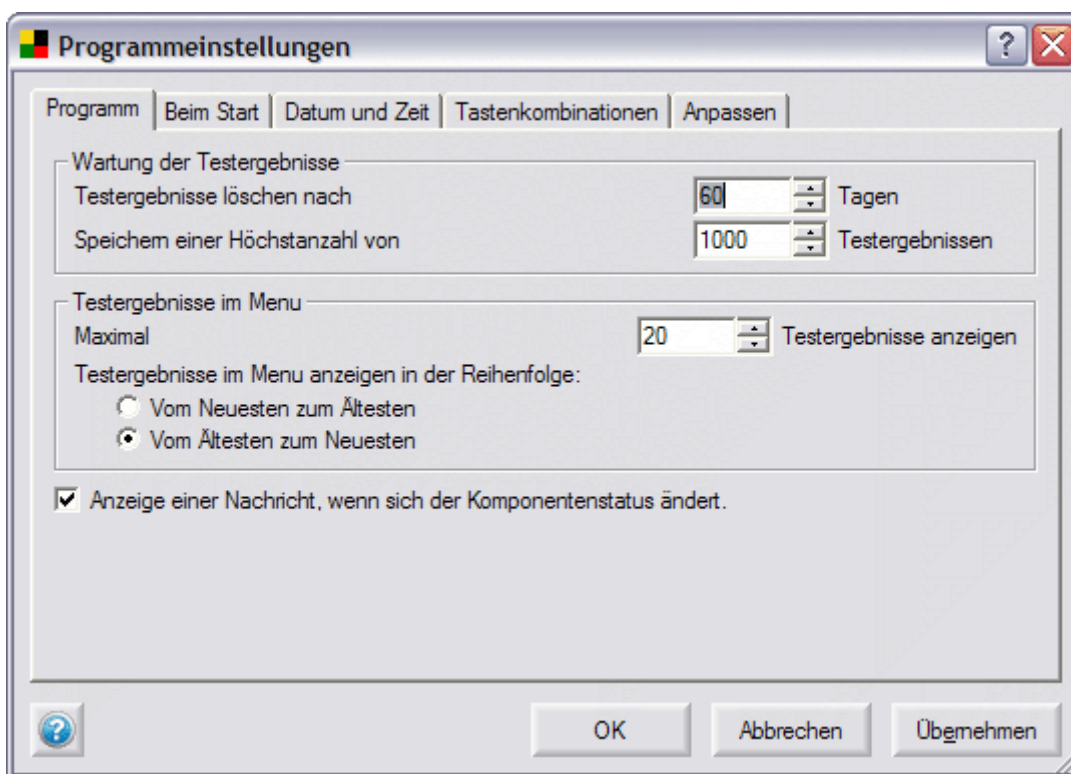
- **Kennwort** – definieren und bestätigen Sie ein Kennwort, das den Zugang zur Bearbeitung der **Administrator- Optionen** sichert.
- **Standard** – stellt die Administratoroptionen wieder auf die Standardwerte
- **OK** – akzeptiert alle vorgenommenen Änderungen und schließt den Dialog
- **Abbrechen** – schließt den Dialog und verwirft alle vorgenommenen Änderungen

#### b) Ansicht

Innerhalb des Menüs Ansicht können Sie auswählen, welche Komponenten im **Control Center** angezeigt werden sollen, in welchem Bereich und ob sie in einer verkürzten Form oder im Standardmodus angezeigt werden sollen.

#### c) Service/Programmeinstellungen

Diese Option startet das Fenster **Programmeinstellungen**, welches die Möglichkeit zur Konfiguration von **AVG-Programmeinstellungen** in fünf verschiedenen Reitern bietet. Für eine detaillierte Beschreibung der einzelnen Reiter lesen Sie bitte das Kapitel [8.4 Programmeinstellungen](#).



#### 9.4. AVG Komponenten im Control Center

Im Hauptbereich des **Control Center** können Sie verschiedene Fenster sehen, die die AVG-Komponenten (in verkürzter Form) oder Schaltflächen der AVG-Komponenten (in erweiterter Form) darstellen. Um die gewählte Komponente zu

bearbeiten, klicken Sie nur auf das entsprechende Fenster und verwenden die Schaltfläche Optionen im unteren Bereich des **Control Center** Fensters.

Wann immer ein Komponentenstatus fehlerhaft ist (z.B. die Aktualisierung der Virendatenbank wurde nicht rechtzeitig durchgeführt und ist abgelaufen), dann wird das Komponentenfenster rot hervorgehoben und das Programmsymbol in der Taskleiste wird grau angezeigt. Im erweiterten Modus wird das Komponentenfenster rot angezeigt. Es wird empfohlen, diesen Hinweis genau zu beachten, um den optimalen Status aller Komponenten zu gewährleisten, damit alle AVG-Funktionen einwandfrei arbeiten.

### 9.5. Control Center-Symbol in der Systemablage

Das **Control Center**-Symbol erscheint in der Systemablage und hilft Ihnen dabei, den aktuellen Status von AVG zu erkennen. Wenn alle Komponenten von AVG vollständig funktionsfähig sind, ist das Symbol farbig dargestellt. Färbt sich das Symbol jedoch grau, so ist mindestens eine AVG-Komponente fehlerhaft! In diesem Fall doppelklicken Sie auf das Symbol in der Systemablage, um das **Control Center** zu öffnen und sehen Sie sich den Status der einzelnen Komponenten an.

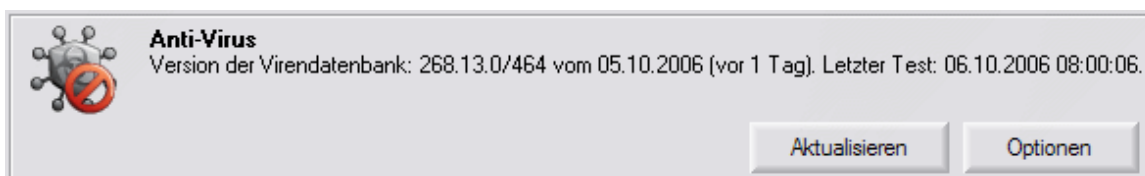
### 9.6. Komponenten, die vom AVG Control Center kontrolliert werden

Das **Control Center** ermöglicht die Verwaltung folgender AVG-Komponenten:

- [Anti-Virus](#)
- [Anti-Spyware](#)
- [Scheduler](#)
- [Residenter Schutz](#)
- [Virenquarantäne](#)
- [Aktualisierungsmanager](#)
- [Shell-Erweiterung](#)
- [eMail-Kontrolle](#)
- [Alarm Manager](#)
- [Lizenzbedingungen](#)

### 9.7. Control Center – Anti-Virus

Die Komponente **Anti-Virus** enthält Informationen über alle aktuell bekannten Viren.



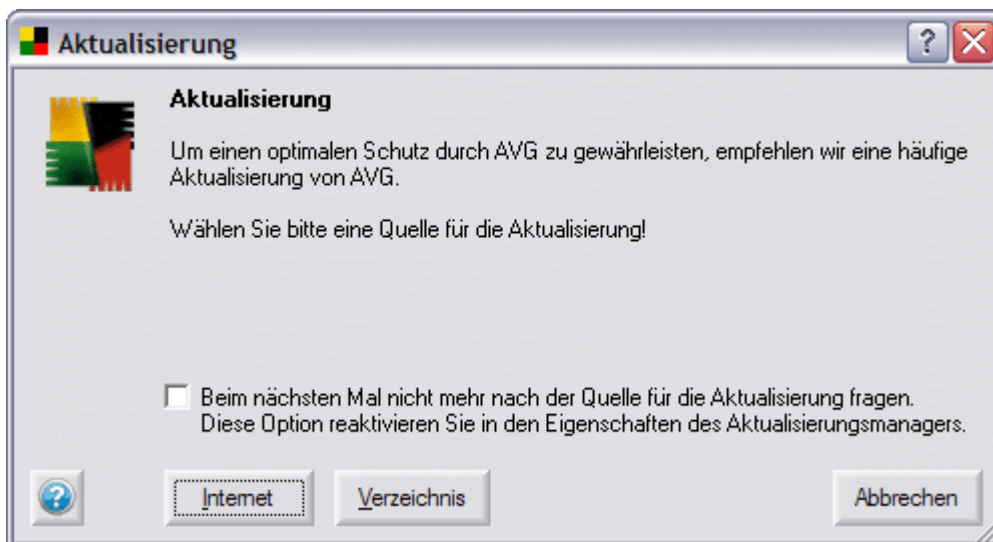
**Wichtig:** Wenn die Virendatenbank älter als 7 Tage ist, wird sie als veraltet angesehen. Um dieses anzuzeigen, ändert die Komponente ihren internen Status auf fehlerhaft und wird rot angezeigt. Bitte bedenken Sie, dass ein verlässlicher Virenschutz nur erreicht werden kann, wenn Ihr Virenschutz-System regelmäßig

und häufig aktualisiert wird. Weitere Informationen zu Aktualisierungen finden Sie in Kapitel [14 Programm-Aktualisierungen](#).

Die Schaltflächen zum Bearbeiten von **Anti-Virus** sind:

**a) Aktualisieren**

Die Schaltfläche **Aktualisieren** öffnet das Fenster zum manuellen Aktualisieren. Wenn nicht aktualisiert wird, ist die Datenbank von **Anti-Virus** nach 7 Tagen veraltet!



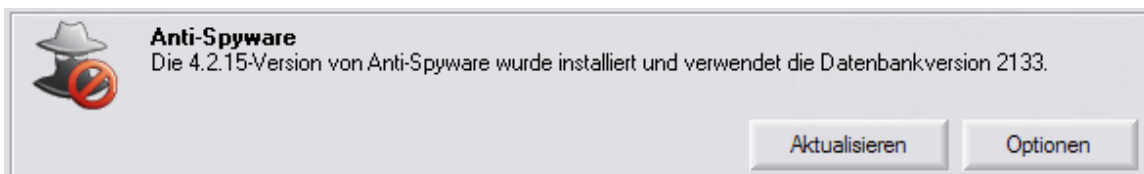
Einzelheiten zu Aktualisierungsarten und zu den Möglichkeiten erhalten Sie in Kapitel [14 Programm-Aktualisierungen](#)

**b) Eigenschaften**

Die Schaltfläche **Eigenschaften** zeigt einen kurzen Überblick über die Informationen zur Komponente **Aktualisieren**. Außerdem können Sie definieren, wie die Komponente im **Control Center** angezeigt werden soll:



### 9.8. Control Center – Anti-Spyware

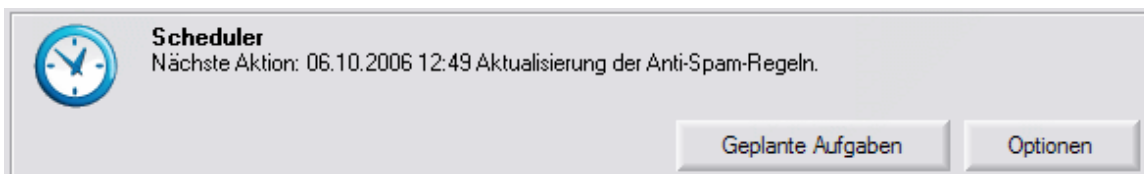


Als Spyware wird üblicherweise eine Art von schädlichem Programm angesehen, d.h. Software, die Informationen vom Computer eines Benutzers sammelt, ohne dass der Benutzer darüber informiert ist. Einige Arten von Spyware können auch absichtlich installiert werden und enthalten Werbungen, Pop-Ups oder verschiedene Arten unangenehmer Software.

Die Komponente **Anti-Spyware** in **AVG 7.5 Internet Security** ermöglicht Ihnen, Ihren Computer vollständig nach Malware/Spyware zu durchsuchen. Sie erkennt auch *schlafende und nicht-gefährliche* schädliche Programme, die herunter geladen wurden, bisher jedoch noch nicht aktiviert wurden.

### 9.9. Control Center - Scheduler

Der **Scheduler** kontrolliert geplante Aufgaben, wie das Aktualisieren und Tests.



Die Schaltflächen im **Scheduler** Fenster sind:

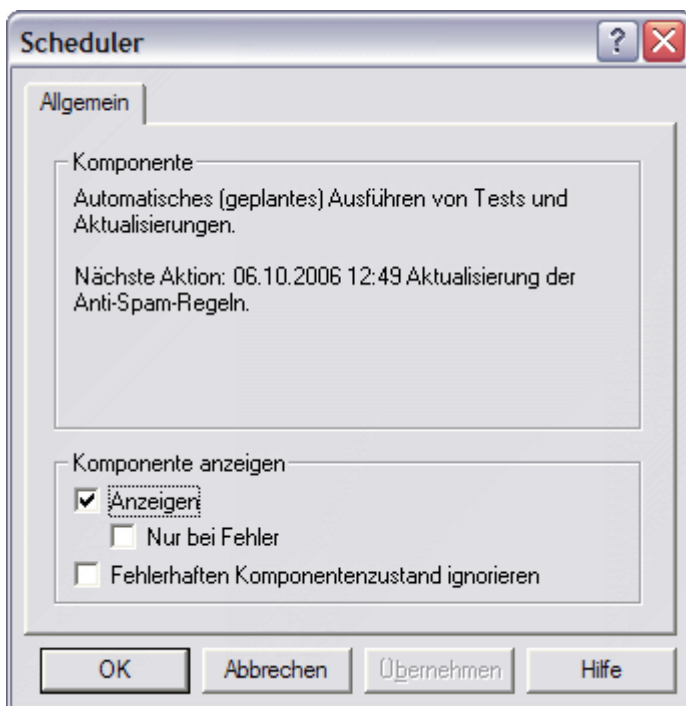
- a) **Geplante Aufgaben**

Die Schaltfläche **Geplante Aufgaben** startet das Fenster **Geplante Aufgaben**; der Dialog und die Optionen für die Aufgabenplanung sind detailliert im Kapitel [8.2 Geplante Aufgaben](#) beschrieben



**b) Optionen**

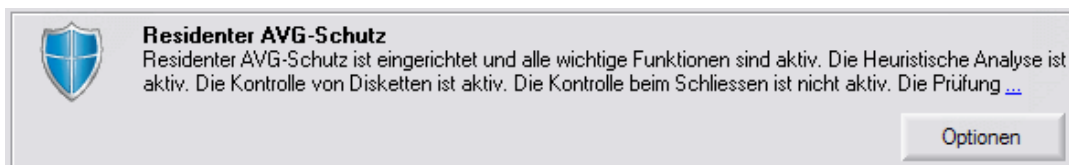
Die Schaltfläche **Optionen** zeigt allgemeine Informationen zur Komponente **Scheduler** an und lässt das Bearbeiten der Anzeige dieser Komponente zu:



**9.10. Control Center - Residenter Schutz**

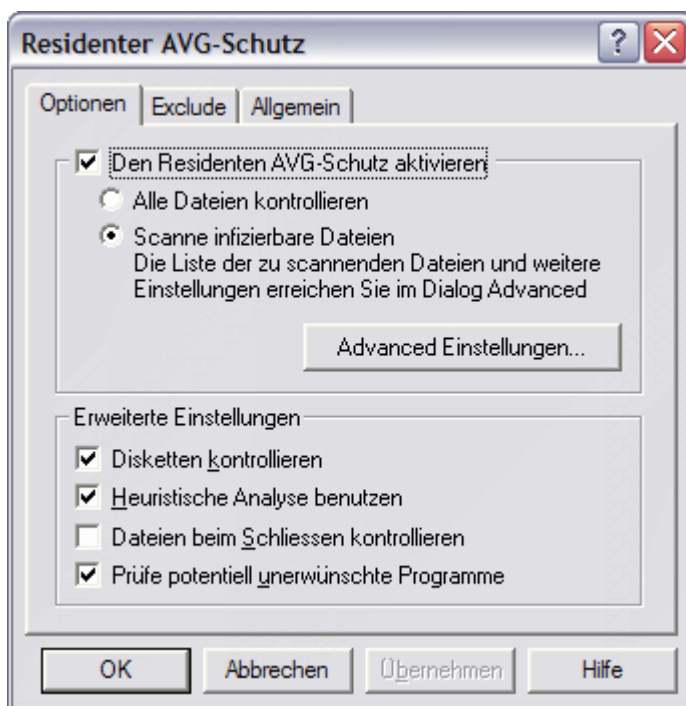
**a) Optionen des Residenten Schutzes**

Die Komponente **Residenter Schutz** führt die Kontrolle auf Viren, Spyware und andere schädliche Programme von Dateien und Ordnern durch. Diese Option muss zuerst im Dialog **Optionen des Residenten Schutzes** aktiviert werden.

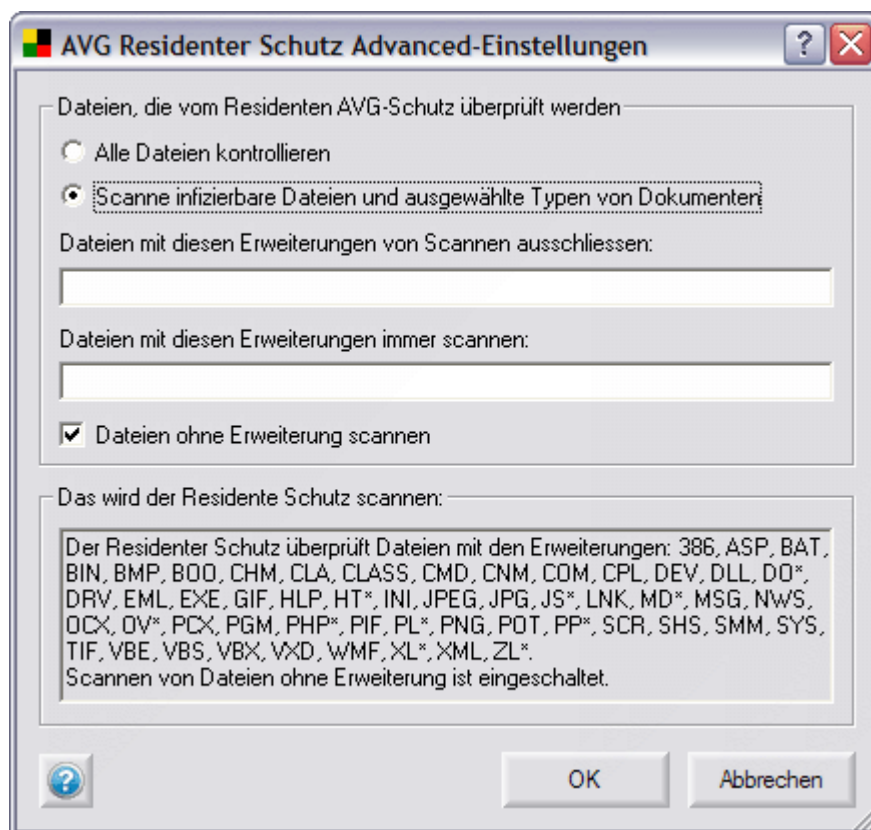


Verwenden Sie die Schaltfläche **Optionen**, um das Konfigurationsfenster der Komponente **Residenter Schutz** zu öffnen. Dieses Fenster enthält drei Reiter:

- **Optionen** – in diesem Reiter können Sie eine Vielzahl von Optionen zum Einstellen des Testverhaltens des **Residenten Schutzes** auswählen:



- **Advanced Einstellungen** – öffnet das Dialogfenster mit Optionen der **erweiterten Einstellungen** des **Residenten Schutzes**. Die Überprüfung infizierbarer und weiterer ausgewählter Typen von Dokumenten kann konfiguriert werden oder Dateitypen von einer Überprüfung ausgenommen werden (nach bestimmten Endungen). Dementsprechend werden Dateien mit jenen Endungen vom **Residenten Schutz** in die Überprüfung aufgenommen oder ignoriert.

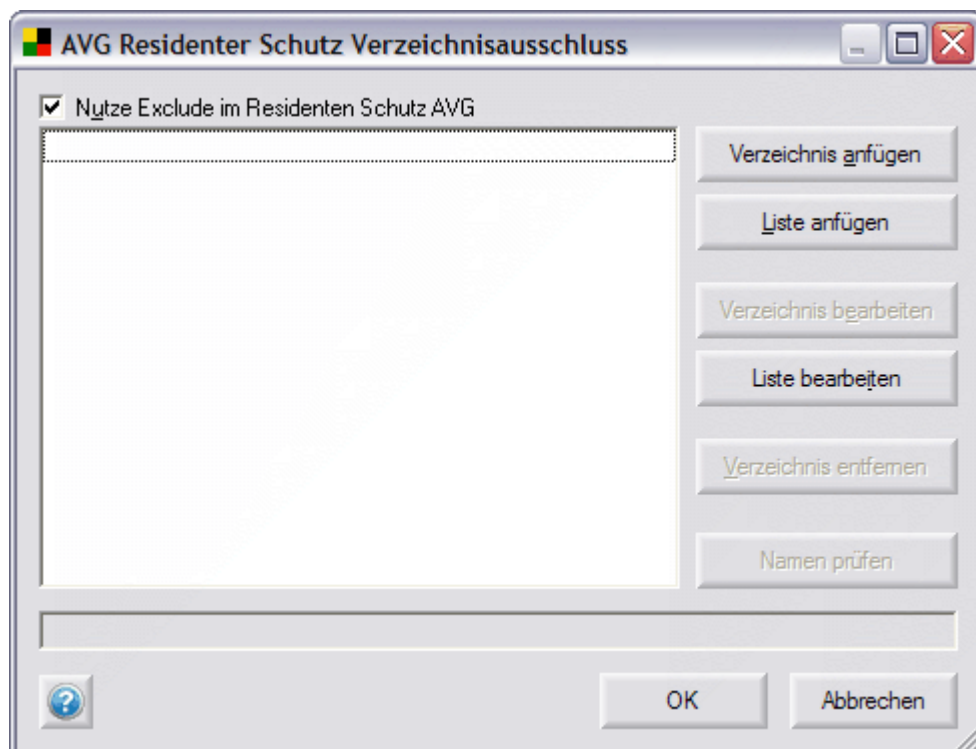


- **Exclude** – Der Reiter **Exclude** bietet Ihnen die Möglichkeit, Ordner anzugeben, die von der Überprüfung durch den **Residenten Schutz** ausgeschlossen werden sollen. Falls dies nicht zwingend erforderlich ist, empfehlen wir, keine Ausnahmen festzulegen! Wenn Sie sich dazu entschließen, einen Ordner von der Überprüfung durch den **Residenten Schutz** auszuschließen, markieren Sie bitte die Option **Dateien mit diesen Erweiterungen vom Scannen ausschliessen**. Die neuen Einstellungen werden erst mit einem Neustart des Computers übernommen!

**Bitte beachten Sie:** Ausnahmen zu Potentiell unerwünschten Programmen sollten in einem anderen Dialog definiert werden. Siehe Kapitel [7.14 Potentiell unerwünschte Programme - Ausnahmen](#)



Verwenden Sie die Schaltfläche **Exclude bearbeiten**, um ein Fenster zu öffnen, in dem Sie direkt das Verzeichnis angeben können, das vom Test ausgeschlossen werden soll:



In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

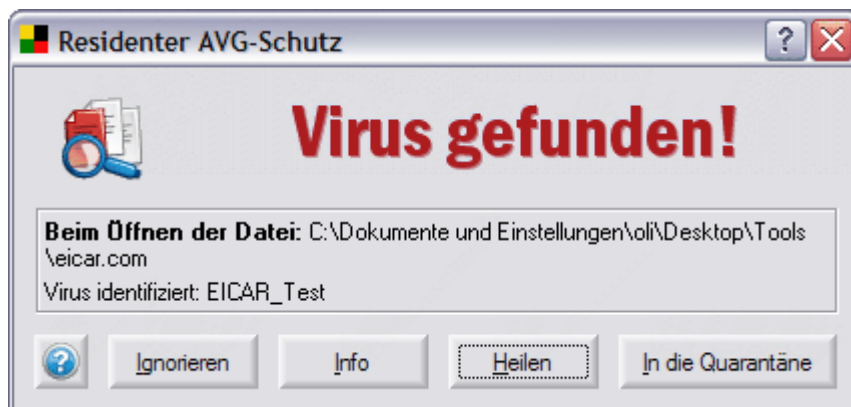
## AVG 7.5 File Server

- **Verzeichnis anfügen** – bietet Ihnen die Auswahlmöglichkeit von Verzeichnissen im Navigationsbaum der lokalen Festplatte an, die Sie ausschließen können
  - **Liste anfügen** – erlaubt Ihnen die Eingabe einer kompletten Verzeichnisliste, die von der Überprüfung durch den **Residenten Schutz** ausgeschlossen werden soll
  - **Verzeichnis bearbeiten** – erlaubt Ihnen die Änderung des Pfades zu einem ausgewählten Verzeichnis
  - **Liste bearbeiten** – erlaubt Ihnen das Bearbeiten der Verzeichnisliste
  - **Verzeichnis entfernen** – erlaubt Ihnen das Löschen einer Pfadangabe zu einem angegebenen Verzeichnis
  - **Namen prüfen** – überprüft, ob die angegebenen Pfade gültig sind und auf Ordner der lokalen Festplatte verweisen. Alle fehlerhaften Pfade werden entfernt
  - **OK** – alle Änderungen werden übernommen und das Dialogfenster wird geschlossen
  - **Abbrechen** – alle Änderungen werden verworfen und das Dialogfenster wird geschlossen
- **Allgemein** – Der Reiter **Allgemein** bietet Ihnen einen Überblick über die allgemeinen Informationen der Komponente **Residenter Schutz**. Sie können definieren, ob die Komponente immer angezeigt werden soll oder nur dann, wenn ein fehlerhafter Zustand vorliegt. Sie können auch festlegen, ob ein fehlerhafter Komponentenzustand ignoriert werden soll:



**b) Residenter Schutz - Virenfund**

Entsprechend der eingestellten Konfiguration überprüft der Residente Schutz kontinuierlich Ordner und Verzeichnisse, die geöffnet, geschlossen oder gespeichert werden. Falls ein verdächtiges Objekt gefunden wird, werden Sie sofort durch eine Warnmeldung informiert:

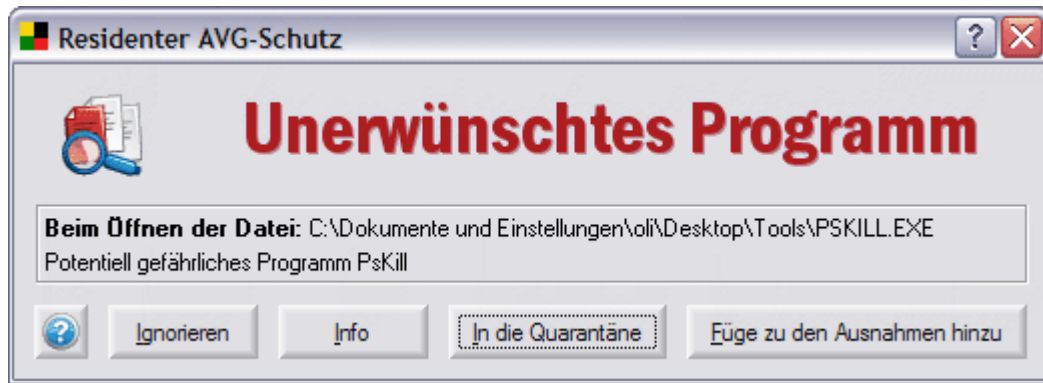


Das Dialogfenster **Residenter Schutz – Virus gefunden!** informiert Sie über den Arbeitsvorgang, bei dem die verdächtige Datei entdeckt wurde; weiterhin über den Speicherort der verdächtigen Datei und erkennt, wenn möglich, die Infektionsart (falls es sich um eine bekannte Infektion handelt). Das Dialogfenster bietet Ihnen verschiedene Schaltflächen für die weitere Behandlung des infizierten Objektes an:

- **Ignorieren** – ignoriert die Warnung Virus gefunden und erlaubt Ihnen das Fortsetzen der Arbeit (und verbietet gleichzeitig Zugriff auf diese Bedrohung)
- **Info** – öffnet die Online- Virenenzyklopädie, in der Sie weitere Informationen zum gefundenen Virus finden können
- **Heilen** – erlaubt Ihnen das Heilen der infizierten Datei, falls dies bei der entsprechenden Infektion möglich ist
- **In die Quarantäne** – verschiebt die infizierte Datei in die Viren-quarantäne (und entfernt sie vom aktuellen Speicherort).

AVG kann ausführbare Anwendungen und DLL-Bibliotheken erkennen und analysieren, die innerhalb des Systems potentiell unerwünscht sein könnten. Üblicherweise sind diese unter dem Namen **Potentiell unerwünschte Programme** (z.B. Spyware, Adware) bekannt.

Wenn ein **Potentiell unerwünschtes Programm** während einer durch den Residenten Schutz laufenden Überprüfung erkannt wird, werden Sie hierüber durch den folgenden Dialog benachrichtigt:

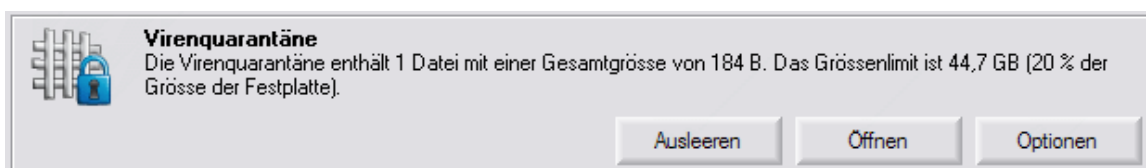


Dieser Dialog informiert Sie über den Speicherort des erkannten Potentiell unerwünschten Programms und bietet verschiedene Schaltflächen, die Sie für die weitere Bearbeitung der verdächtigen Datei nutzen können:

- **Ignorieren** – ignoriert die Warnung des Residenten Schutzes und ermöglicht Ihnen, mit der Arbeit fortzufahren (und bietet auch keinen Zugang zu dieser Bedrohung)
- **Info** – öffnet die Online-Virenzyklopädie, in der Sie detaillierte Informationen zu der erkannten Bedrohung erhalten
- **In die Quarantäne** – verschiebt das potentiell unerwünschte Objekt in die **Virenquarantäne** (und entfernt das Objekt von dem aktuellen Speicherort)
- **Füge zu den Ausnahmen hinzu** – ermöglicht Ihnen, das Potentiell unerwünschte Programm im System beizubehalten und es als eine [Potentiell unerwünschte Programme- Ausnahmen](#) zu definieren. Eine Bestätigung hierfür wird angezeigt.

### 9.11. Control Center - Virenquarantäne

Die **Virenquarantäne** arbeitet als ein Speicher für verdächtige/infizierte Objekte und bietet Optionen für die weitere Behandlung oder Heilung an.



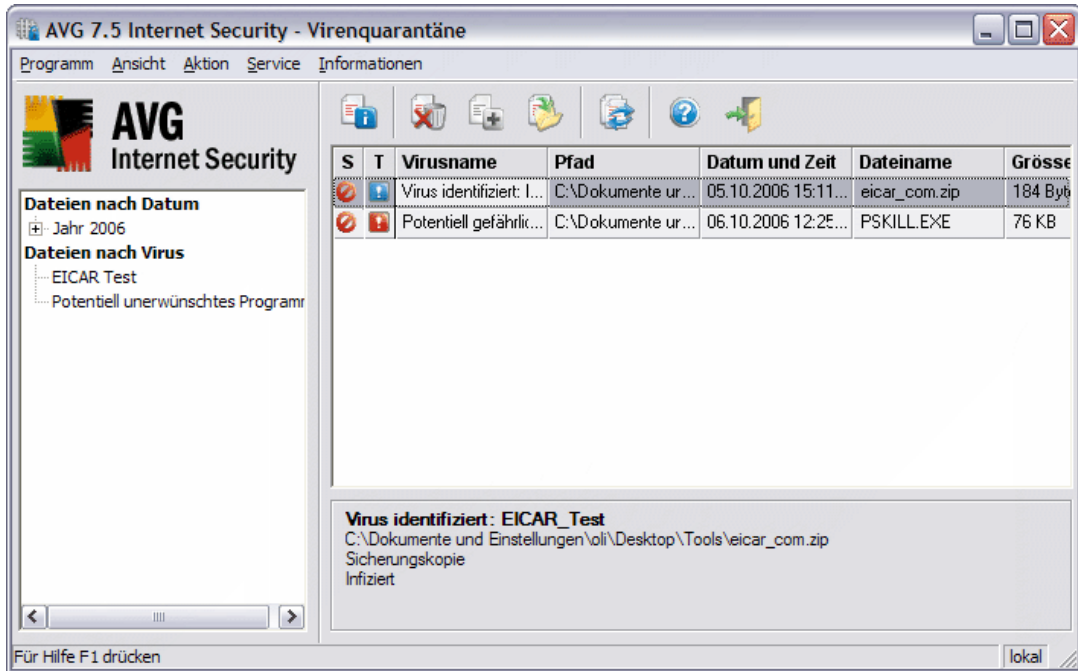
Im Bedienfeld **Virenquarantäne** gibt es folgende Schaltflächen:

**a) Ausleeren**

Löscht alle Objekte, die in der **Virenquarantäne** gespeichert sind.

**b) Öffnen**

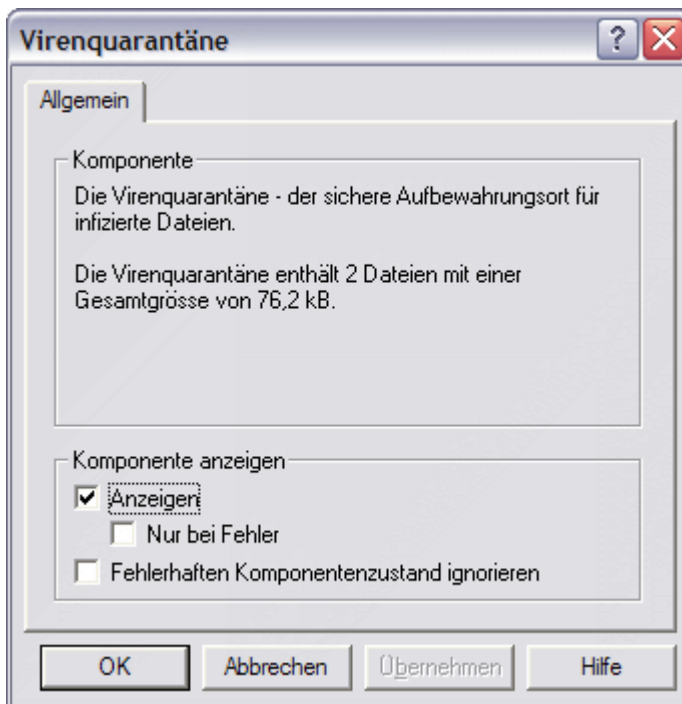
Öffnet die **Virenquarantäne**:



Für zusätzliche Informationen zur Virenquarantäne lesen Sie bitte das Kapitel [12. Virenquarantäne](#).

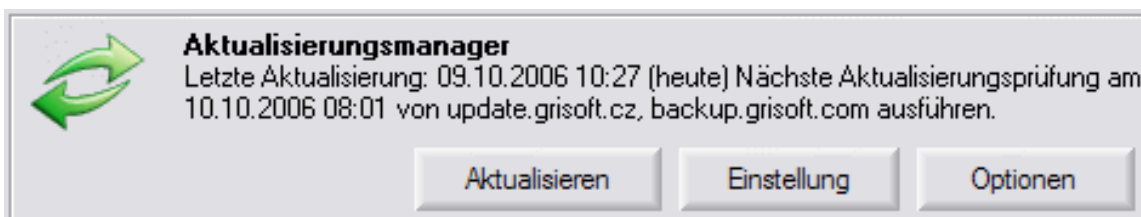
c) **Optionen**

Die Schaltfläche **Optionen** zeigt die allgemeinen Informationen der Komponente **Virenquarantäne** an und ermöglicht Ihnen die Bearbeitung der Komponentenanzeige:



## 9.12. AVG Control Center - Aktualisierungsmanager

Der **Aktualisierungsmanager** kontrolliert die Aktualisierungen von AVG.

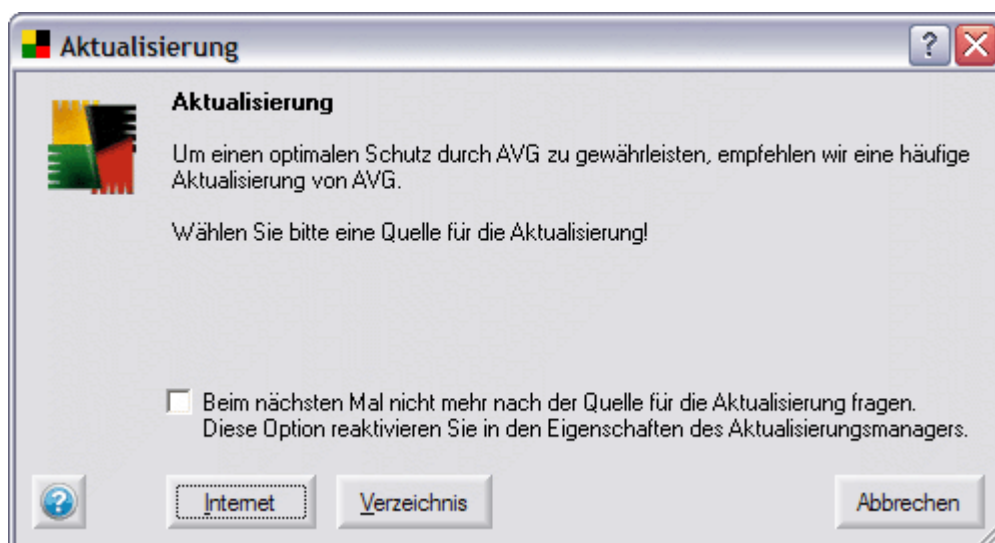


Im Bedienfeld des **Aktualisierungsmanager** gibt es folgende Schaltflächen:

### a) Aktualisierung

Die Schaltfläche **Aktualisierung** öffnet ein neues Dialogfenster, das die sofortige Aktualisierung von AVG anbietet. Die Aktualisierung kann durch die entsprechende Schaltfläche gestartet werden:

- **Internet** – lädt die Aktualisierungsdateien direkt aus dem Internet herunter
- **Verzeichnis** – führt die Aktualisierung aus einem Verzeichnis durch, in das zuvor die aktuelle Aktualisierungsdatei vom Grisoft Server gespeichert wurde



Für weitere Informationen zu Aktualisierungstypen und Möglichkeiten lesen Sie bitte auch Kapitel [14. Programm Aktualisierungen](#).

### b) Einstellungen

Die Schaltfläche **Einstellungen** öffnet das Dialogfenster **AVG Inet** mit drei Reitern, in denen Sie Ihre Internetverbindungsparameter und die Aktualisierungsquelle konfigurieren können:

- **Proxy**  
Der Proxy-Server ist ein einzelner (Standalone) Server oder ein Dienst, der auf dem Computer läuft und der eine sicherere Verbindung zum

## AVG 7.5 File Server

Internet garantiert. Entsprechend der angegebenen Netzwerkregeln können Sie auf das Internet entweder direkt oder über einen Proxy-Server zugreifen; beide Möglichkeiten können auch gleichzeitig erlaubt werden.

Auf dem Reiter **Proxy** sollten Sie angeben, ob Sie eine Verbindung mit dem Internet über einen Proxy-Server aufbauen möchten – entsprechend den Regeln, die in Ihrem Netzwerk festgelegt sind. Öffnen Sie die Auswahlbox, um eine der folgenden Optionen auszuwählen:

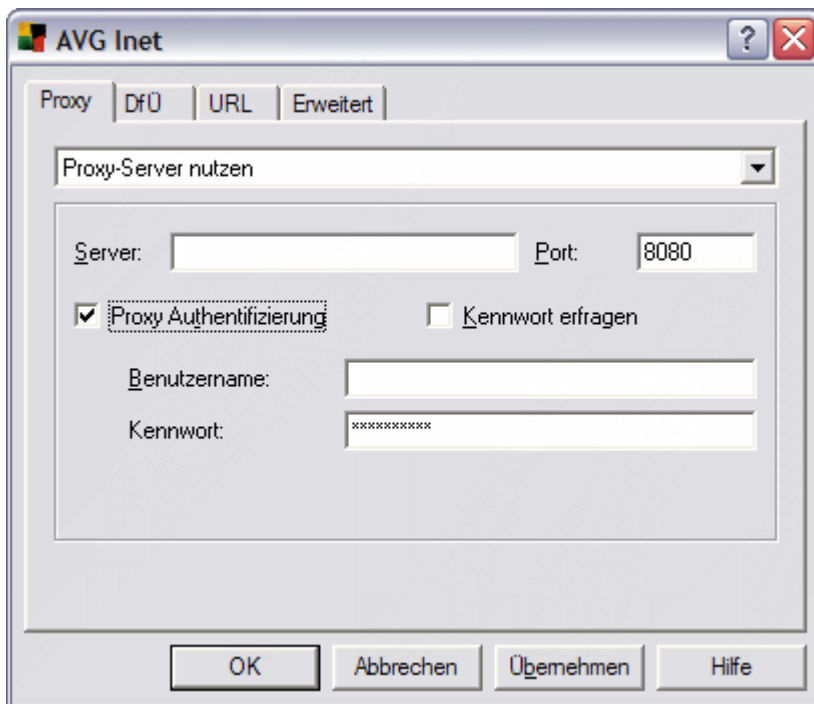
- Keinen Proxy-Server nutzen
- Proxy-Server nutzen
- Proxy-Server nutzen, bei Fehler direkt verbinden

Wenn Sie die Option **Proxy-Server nutzen, bei Fehler direkt verbinden** oder **Proxy-Server nutzen** verwenden, müssen Sie die folgenden Angaben machen:

- o **Server** – geben Sie die Server IP-Adresse (oder den Namen des Servers) an
- o **Port** – geben Sie die Nummer des Ports an, der den Internetzugang erlaubt (standardmäßig ist dieser Wert auf 8080 gesetzt, aber es können auch andere Werte verwendet werden – falls Sie sich nicht sicher sind, wenden Sie sich bitte Ihren Netzwerkadministrator)

Der Proxy-Server kann auch spezielle Regeln für jeden Benutzer enthalten. Falls Ihr Proxy-Server so konfiguriert ist, aktivieren Sie bitte die Option **Proxy Authentifizierung** und geben Sie dort bitte Ihren Benutzernamen und das Kennwort an, die für eine gültige Verbindung mit dem Internet notwendig sind, an (innerhalb dieses Dialoges sind die Optionen **Kennwort erfragen, Benutzername und Kennwort** aktiv).

Wenn die Option **Kennwort erfragen** aktiviert ist, wird das Kennwort nicht automatisch gespeichert und verwendet. Stattdessen werden Sie jedes Mal aufgefordert, Ihr Kennwort einzugeben, wenn Sie sich mit dem Proxy-Server verbinden, um ins Internet zu gelangen. Ansonsten können Sie auch Ihren **Benutzernamen** und Ihr **Kennwort** in diesem Dialog angeben; beim nächsten Start der Aktualisierung werden diese Daten automatisch verwendet, um eine Verbindung zum Proxy-Server herzustellen.

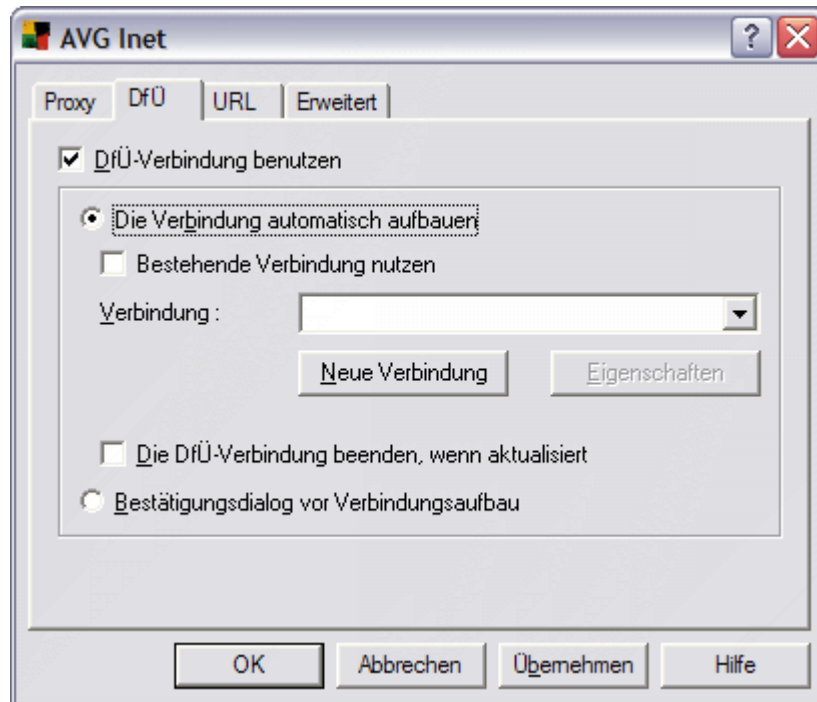


- o **DfÜ**

Alle Parameter, die optional im Reiter **DfÜ** definiert werden können, beziehen sich auf eine Einwahlverbindung in das Internet. Die Felder im Reiter bleiben inaktiv, bis Sie die Option **DfÜ Verbindung benutzen** aktivieren.

Bestimmen Sie, ob Sie einen automatischen Verbindungsaufbau zum Internet wünschen (**Die Verbindung automatisch aufbauen**) oder ob Sie jedes Mal die Verbindung manuell bestätigen möchten (**Bestätigungsdiallog vor Verbindungsaufbau**). Wählen Sie für den automatischen Verbindungsaufbau aus der Liste die Verbindung aus, die verwendet werden soll (**Verbindung**) oder erstellen Sie eine neue Verbindung (**Neue Verbindung**).

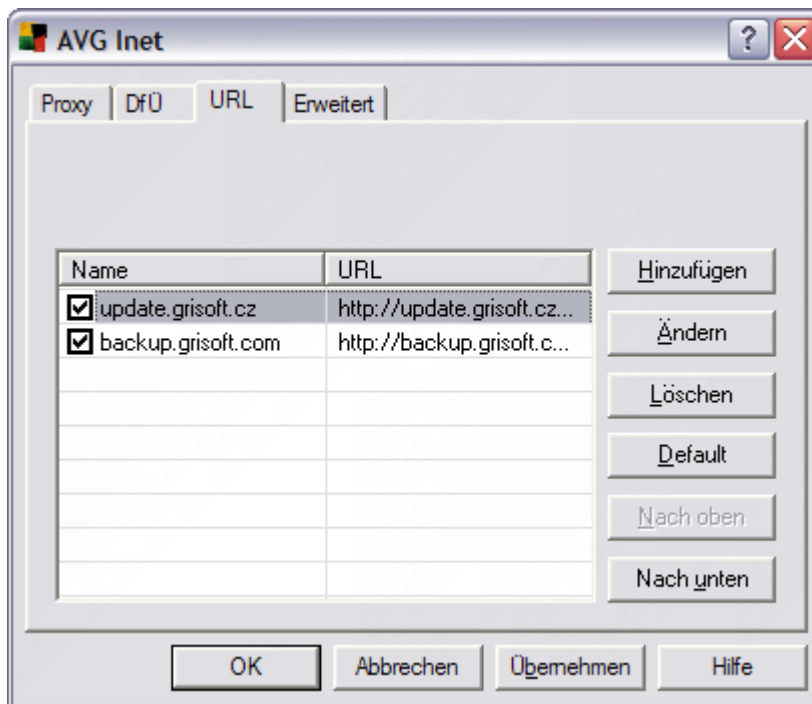
Weiterhin können Sie festlegen, ob die Verbindung nach Beendigung der Aktualisierung getrennt werden soll (**Die DfÜ Verbindung beenden, wenn aktualisiert**).



o **URL**

Der Reiter **URL** zeigt eine Liste von Internetadressen, von denen die Aktualisierungsdateien herunter geladen werden können. Die Liste und die enthaltenen Objekte können mit Hilfe der Schaltflächen bearbeitet werden:

- **Hinzufügen** – öffnet ein Dialogfenster, in dem Sie eine neue URL angeben können, die der Liste hinzugefügt werden soll.
- **Ändern** – öffnet ein Dialogfenster, in dem Sie die ausgewählte URL bearbeiten können
- **Löschen** – löscht die ausgewählte URL aus der Liste
- **Default** – stellt die Standardliste an URLs wieder her
- **Nach oben** – verschiebt die ausgewählte URL eine Position nach oben
- **Nach unten** – verschiebt die ausgewählte URL eine Position nach unten



o **Advanced**

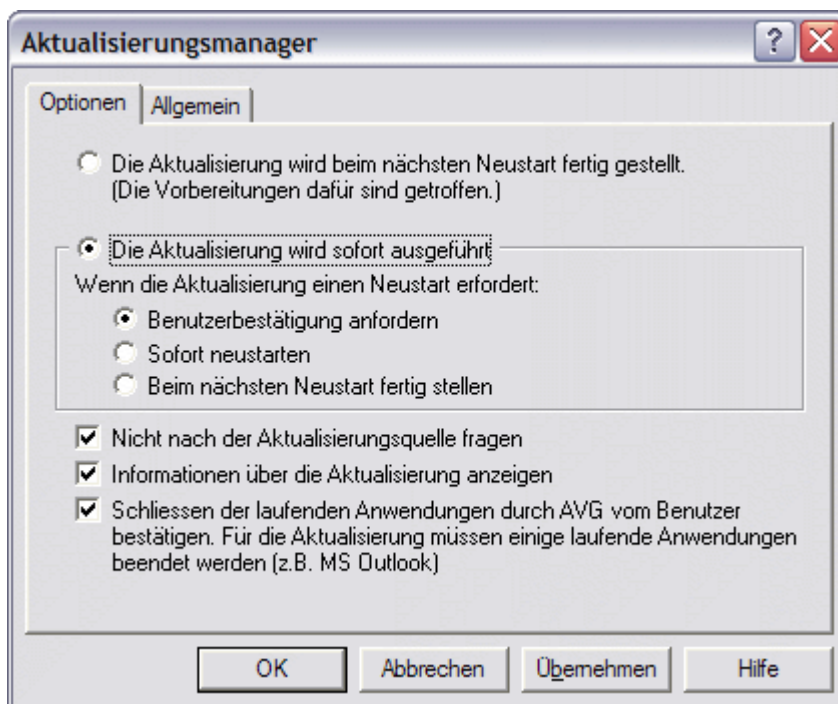
Der Reiter **Advanced** bietet die Möglichkeit, alle temporären Verzeichnisse für die Aktualisierung zu löschen, die AVG während der Aktualisierung angelegt hat. Zum Löschen all solcher Verzeichnisse klicken Sie einfach auf die Schaltfläche **Temporäre Verzeichnisse für die Aktualisierung löschen**.



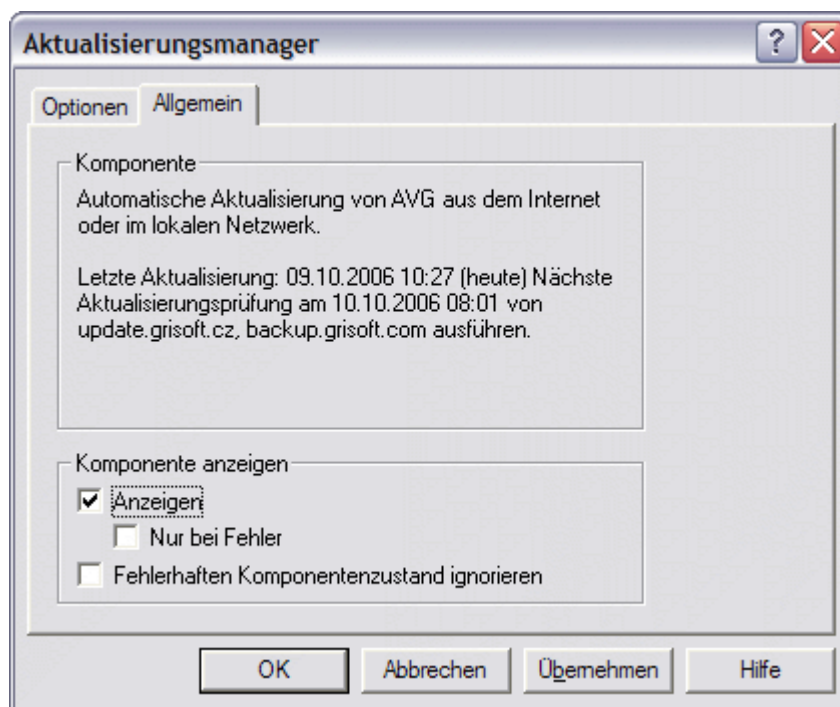
### c) Optionen

Die Schaltfläche **Optionen** öffnet den Dialog Aktualisierungsmanager mit den folgenden zwei Reitern:

- **Optionen** – in diesem Reiter können Sie angeben, ob die Aktualisierung nach dem Neustart Ihres Computers (die Aktualisierung wird beim nächsten Neustart fertig gestellt) oder sofort (die Aktualisierung wird sofort ausgeführt) durchgeführt werden soll. – bei dieser Option können Sie das weitere Verhalten von AVG einstellen, wenn der Computer neu gestartet werden muss.
- Der Eintrag **Nicht nach der Aktualisierungsquelle fragen** bietet Ihnen die Möglichkeit, die Option für die Wahl der Quelle für die Aktualisierung im Aktualisierungs-Dialog zu aktivieren/deaktivieren.
- Weiterhin können Sie Regeln für die Anzeige der Informationen über die Aktualisierung (**Informationen über die Aktualisierung anzeigen**) und über das Verhalten von AVG bei anderen laufenden Anwendungen, die evtl. mit der Aktualisierung kollidieren könnten, anzeigen lassen.

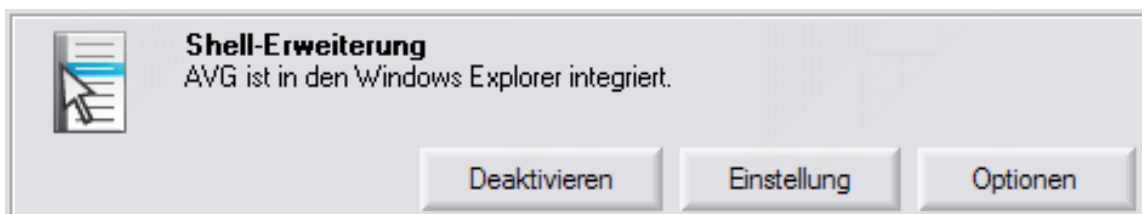


- **Allgemein** – dieser Reiter bietet einen kleinen Überblick über Informationen zur Komponente **Aktualisierungsmanager** und Sie können die Parameter für die Anzeige dieser Komponenten definieren:



### 9.13. Control Center - Shell Erweiterung

Die **Shell Erweiterung** aktiviert die AVG-Funktionen im Windows Explorer, damit Sie auch Verzeichnisse und Objekte innerhalb des Windows Explorer überprüfen können. Klicken Sie mit der rechten Maustaste darauf und wählen Sie die Option **Mit AVG testen**.



Im Bedienfeld **Shell Erweiterung** befinden sich folgende Schaltflächen:

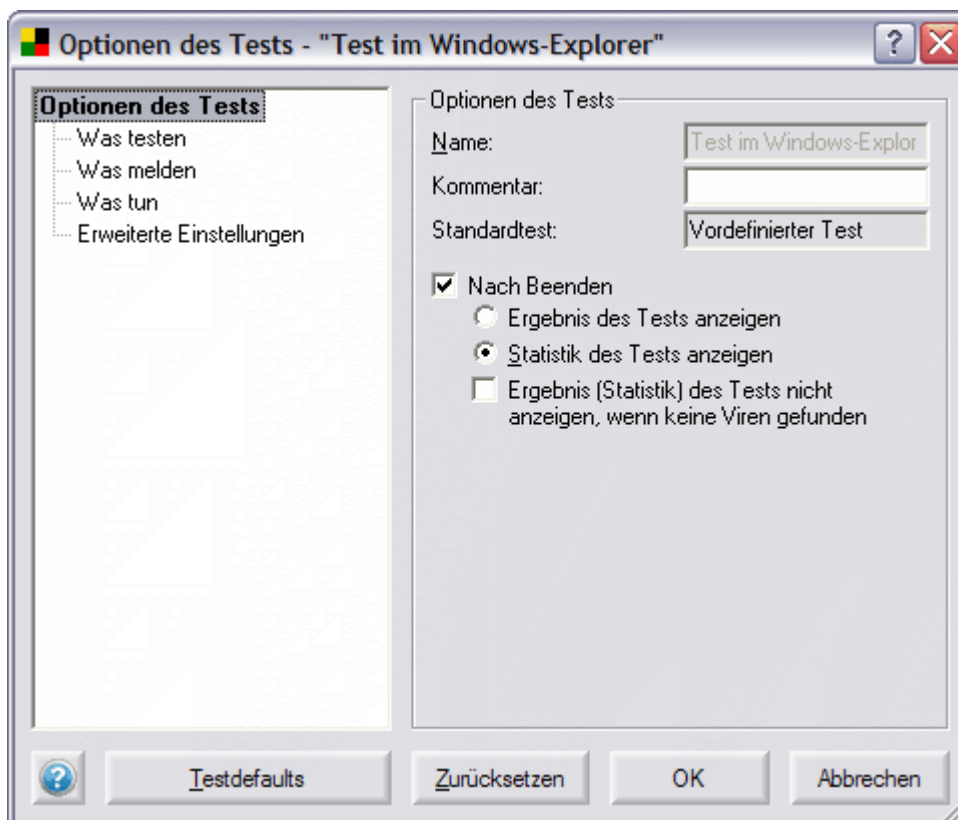
**a) Deaktivieren**

Die Schaltfläche **Deaktivieren** schaltet die Komponente **Shell Erweiterung** aus

**b) Einstellung**

Die Schaltfläche **Einstellung** öffnet das Dialogfenster **Optionen des Tests "Test im Windows-Explorer"**. Auf der linken Seite dieses Dialogfensters sehen Sie einen Navigationsbaum, dessen Zweige den „Reitern“ eines Dialogfensters entsprechen. Die folgenden Konfigurationsdialoge stehen Ihnen innerhalb dieses Navigationsbaumes zur Verfügung:

- **Optionen des Tests** – in diesem Dialog können Sie einen Testnamen (**Name**) und eine Testbeschreibung (**Kommentar**) eingeben. Im Abschnitt **Standardtest** wird angegeben, dass der Test auf einem vordefinierten Test des Herstellers basiert. Weiterhin können Sie festlegen, auf welche Weise die Testergebnisse angezeigt werden sollen (**Nach Beenden Ergebnis des Tests anzeigen**).



- **Was testen** – in diesem Dialog definieren Sie die Systembereiche, die überprüft werden sollen und welche Methoden für den Test verwendet werden (**Allgemeine Einstellung**). Wenn Sie nicht möchten, dass **Alternative NTFS- Datenströme überprüfen** durchgeführt wird, so lassen Sie dieses Kästchen unmarkiert.

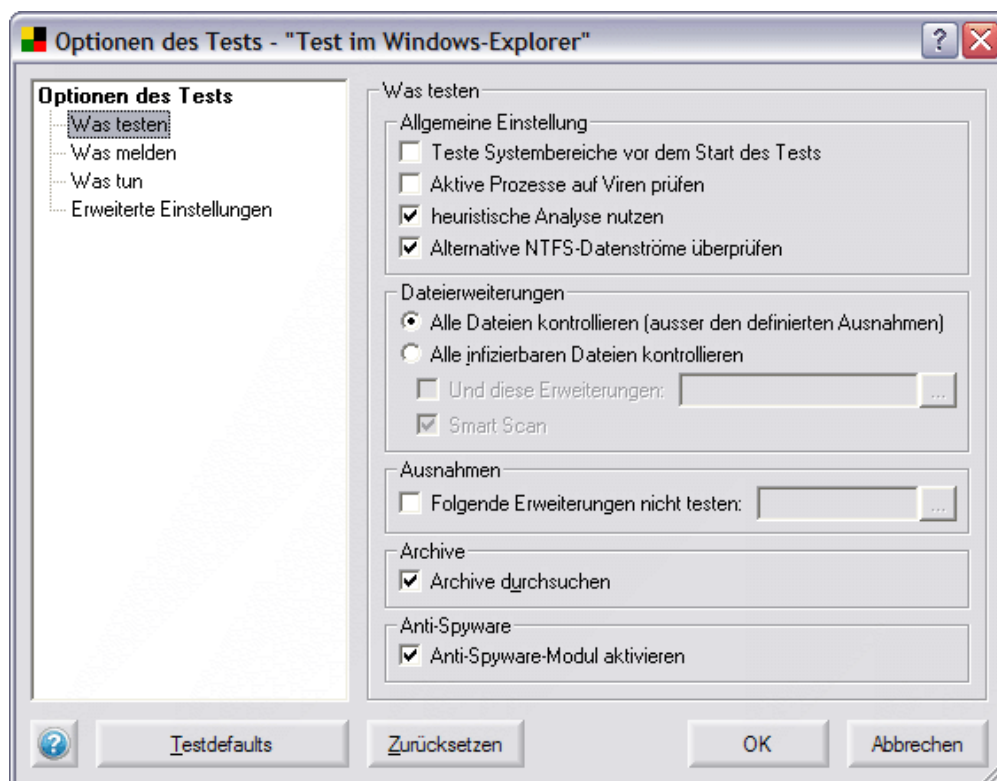
**Anmerkung:** *Alternative NTFS-Datenströme ist ein Windows-Feature, das von Angreifern (meist Hackern) für versteckte Daten, besonders Rootkits, Viren, Trojanern usw. missbraucht wird. Daher wird empfohlen, diese Standard-Einstellung beizubehalten.*

Sie können auch alle aktiven Prozesse des Betriebssystems überprüfen, indem Sie das Kästchen **Aktive Prozesse auf Viren prüfen** markieren. Ein aktiver Prozess ist grundsätzlich eine laufende Anwendung, die eine normale Software, aber auch ein Virus/Spyware/Malware oder eine andere Art von Bedrohung sein kann.

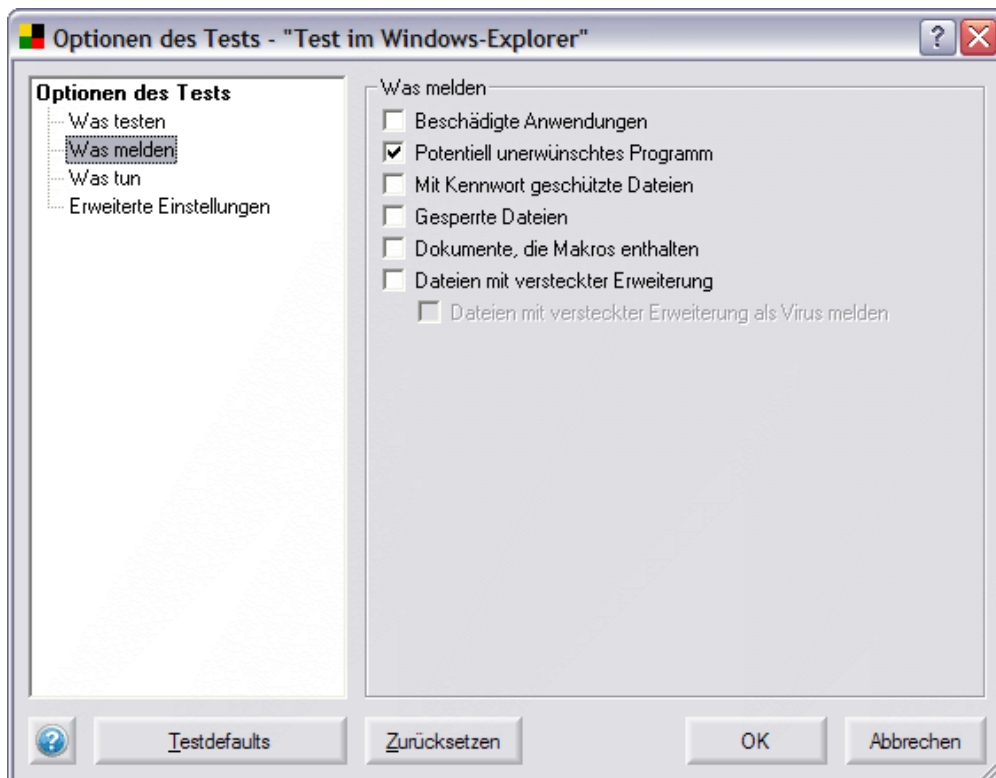
Sie legen weiterhin fest, ob alle Dateien oder nur infizierbare Dateien getestet werden sollen (**Dateierweiterungen**) und ob einige Dateierweiterungen von der Überprüfung ausgeschlossen werden sollen (**Ausnahmen**). Sie können auch die Option zum Durchsuchen von Archiven auswählen (**Archive**).

## AVG 7.5 File Server

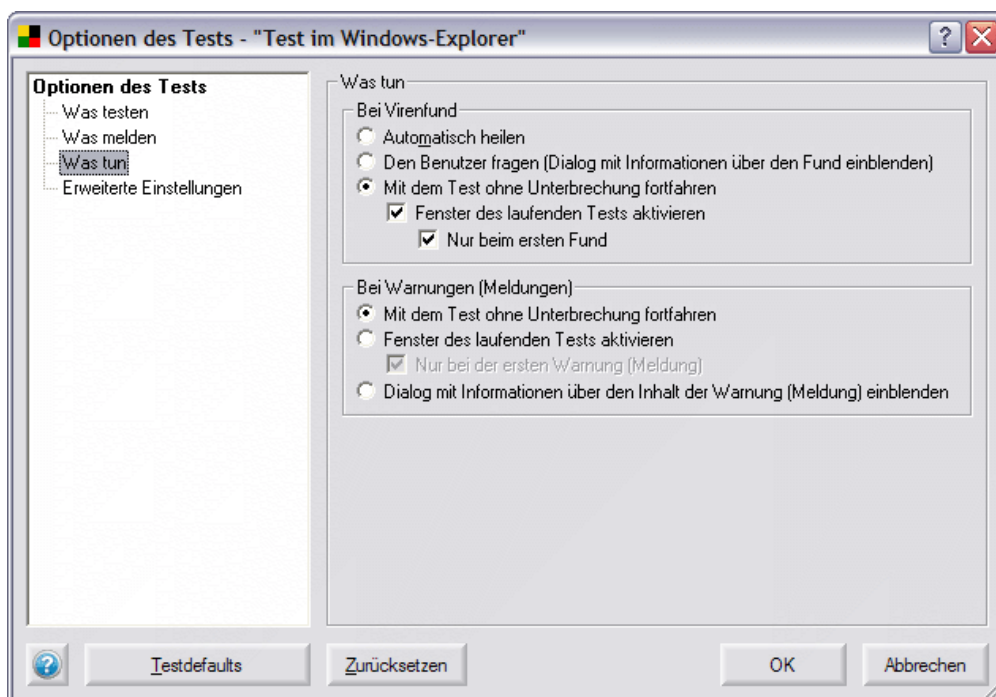
Im Bereich **Anti-Spyware** können Sie die Überprüfung nach Spyware/Malware über die Anti-Spyware-Engine aktivieren/deaktivieren (markieren Sie das Kästchen **Anti-Spyware-Modul aktivieren**).



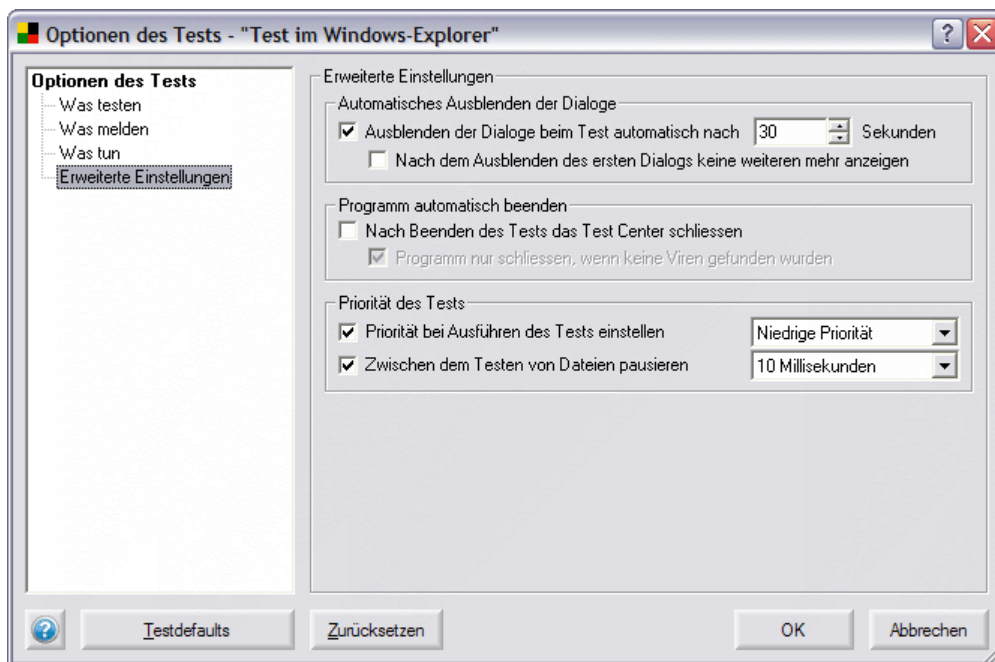
- **Was melden** – der Dialog **Was melden** zeigt eine Liste von Ereignissen an, die während eines Tests vorkommen können. Wählen Sie die Ereignisse aus, über die Sie informiert werden möchten:



- **Was tun** – im nächsten Dialog bestimmen Sie, welche Maßnahmen durchgeführt werden sollen, wenn ein Virus gefunden wird (**Bei Virenfund**) und wenn eine Warnmeldung (auf Grund der oben ausgewählten Ereignisse) angezeigt wird (**Bei Warnungen**).



- o **Erweiterte Einstellungen** – in diesem Dialog können Sie bestimmen, wie lange die AVG-Warnmeldungen angezeigt werden sollen (**Automatisches Ausblenden der Dialoge**) und ob das **AVG Test Center** nach Beendigung des Tests geschlossen werden soll (**Programm automatisch beenden**). Im Abschnitt **Priorität des Tests** können Sie auswählen, welche Priorität der Test besitzen soll und wie lange die Pausen zwischen den einzelnen getesteten Dateien sein sollen (je länger die Pausen sind, desto länger dauert auch der gesamte Test; gleichzeitig jedoch sinken auch die verwendeten Systemressourcen; diese Einstellung kann vor allen Dingen bei älteren und langsameren Computern hilfreich sein).

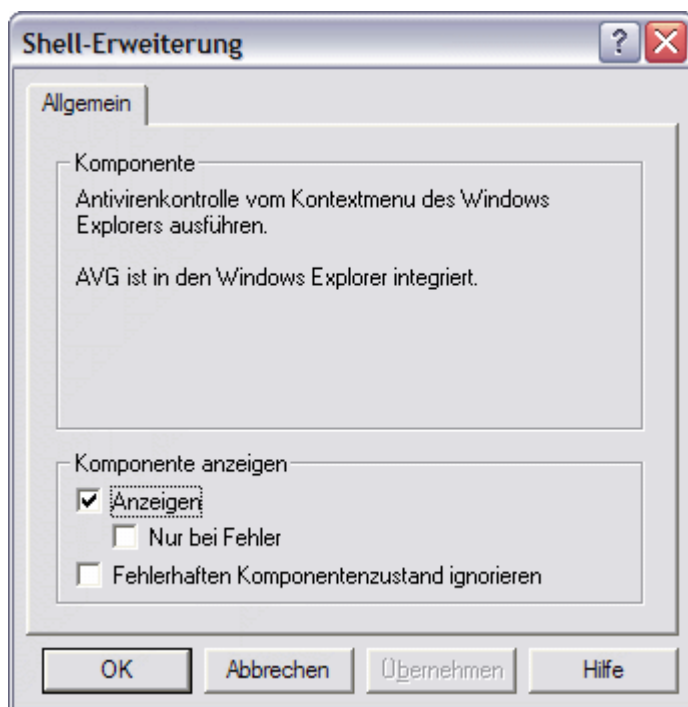


In allen Reitern des Dialogfensters **Optionen des Tests "Test im Windows-Explorer"** stehen Ihnen die folgenden Schaltflächen zur Verfügung:

- **Testdefaults** – stellt die Parameter in allen Dialogfenstern wieder auf die Standardwerte
- **Zurücksetzen** – stellt die Parameter auf der aktuellen Seite wieder auf die Standardwerte
- **OK** – übernimmt die Änderungen und schließt das Dialogfenster
- **Abbrechen** – schließt das Dialogfenster und verwirft alle Änderungen

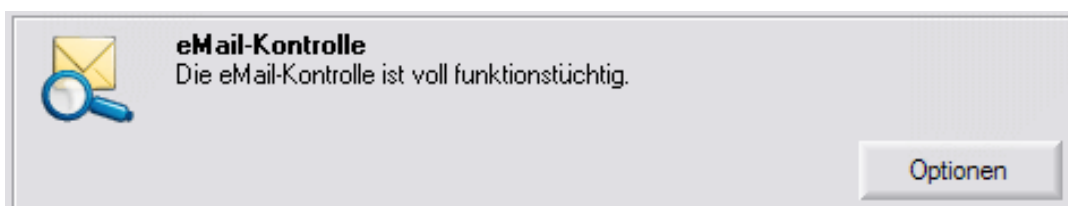
### c) Optionen

Die Schaltfläche **Optionen** zeigt die allgemeinen Informationen der Komponente **Shell Erweiterung** an und ermöglicht die Bearbeitung der Optionen zur Komponentenanzeige:



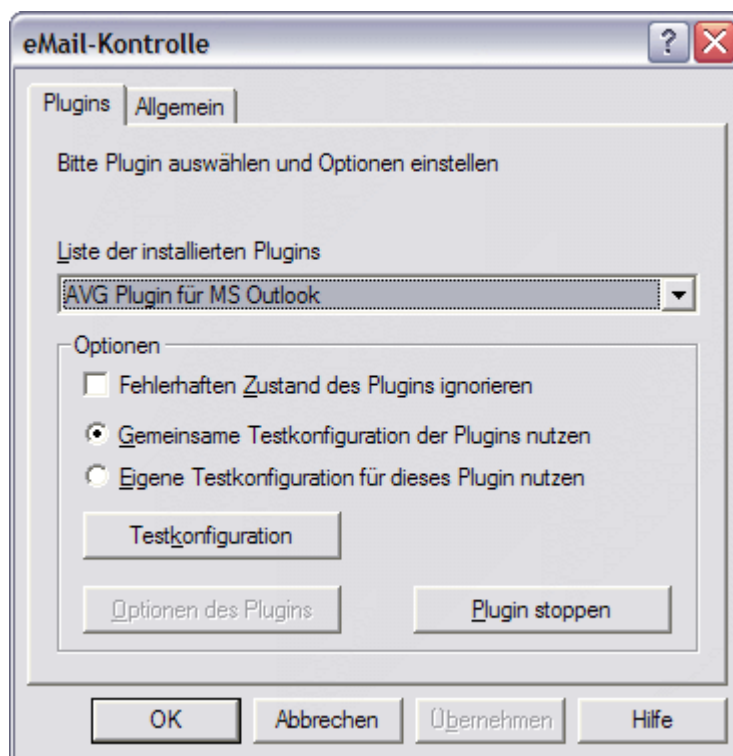
#### 9.14 AVG Control Center - eMail Kontrolle

Die **eMail-Kontrolle** überprüft ein- und ausgehende eMails.



Das Fenster **eMail Kontrolle** mit der Schaltfläche **Optionen** öffnet den Dialog zum Bearbeiten mit zwei Reitern:

- **Plugins** – Dieser Reiter konfiguriert die Handlungsweise aller AVG-Plugins für die entsprechenden eMail-Clients:



Im Abschnitt **Optionen** können Sie die folgenden Parameter einstellen:

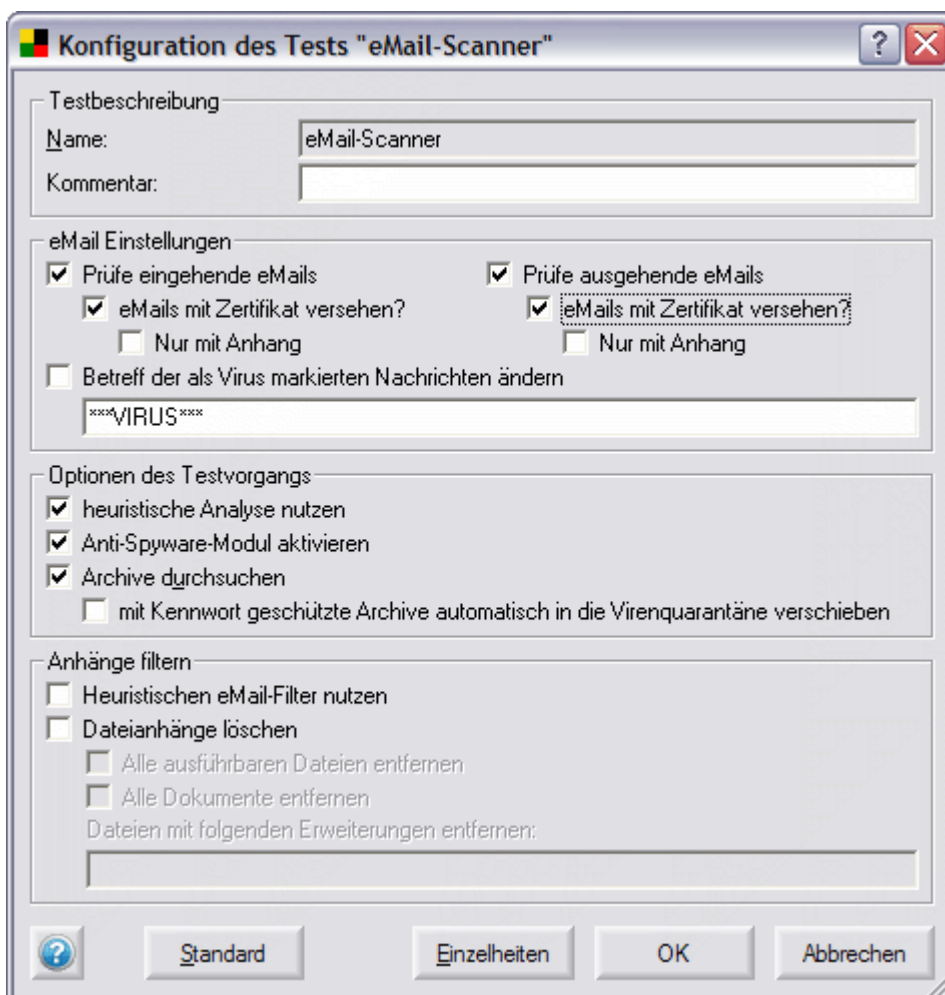
- **Fehlerhaften Zustand des Plugin ignorieren** – wählen Sie diese Option aus, wenn Sie keine Informationen über den aktuellen Komponentenzustand erhalten möchten
- **Testkonfiguration** – wenn Sie Ihre eigenen Konfiguration für die eMail-Überprüfung verwenden möchten, können Sie auswählen, ob diese Konfiguration allgemeingültig (**Gemeinsame Testkonfiguration der Plugins nutzen**) sein soll oder für jedes Plugin einzeln gültig (**Eigene Testkonfiguration für dieses Plugin nutzen**) sein soll. In beiden Fällen verwenden Sie die Schaltfläche **Testkonfiguration**, um das Dialogfenster zum Einstellen der Testkonfiguration zu öffnen. In dem neu geöffneten Fenster geben Sie bitte die folgenden Parameter an:
  - **Testbeschreibung** – geben Sie den Namen und die Beschreibung (optional) an
  - **eMail Einstellungen** – in diesem Abschnitt wählen Sie aus, ob die eingehenden/ausgehenden Nachrichten überprüft werden sollen und ob die Nachrichten zertifiziert werden sollen (immer oder nur eMails mit Anhängen).

**Anmerkung:** Eine Bestätigung, dass eine eMail virenfrei ist, wird im HTML/RTF-Format nicht unterstützt.

Zusätzlich können Sie wählen, ob Sie möchten, dass AVG den Betreff für Benachrichtigungen, die möglicherweise Viren enthalten, ändern soll. Markieren Sie das Kontrollkästchen **Betreff der als Virus markierten nachrichten ändern** und ändern Sie gegebenenfalls den Text (Standardeinstellung ist **\*\*\*VIRUS\*\*\***).

## AVG 7.5 File Server

- **Optionen des Testvorgangs** – legen Sie fest, ob die heuristische Analyse genutzt werden soll (**heuristische Analyse nutzen**), ob Sie eingehende/ausgehende eMails auf Spyware/Adware überprüfen lassen möchten (**Anti-Spyware-Modul aktivieren**) und ob Archive getestet werden sollen (**Archive durchsuchen**)
- **Anhänge filtern** – wählen Sie aus der Liste die Parameter aus, die für das Testen der eMail Anhänge verwendet werden sollen



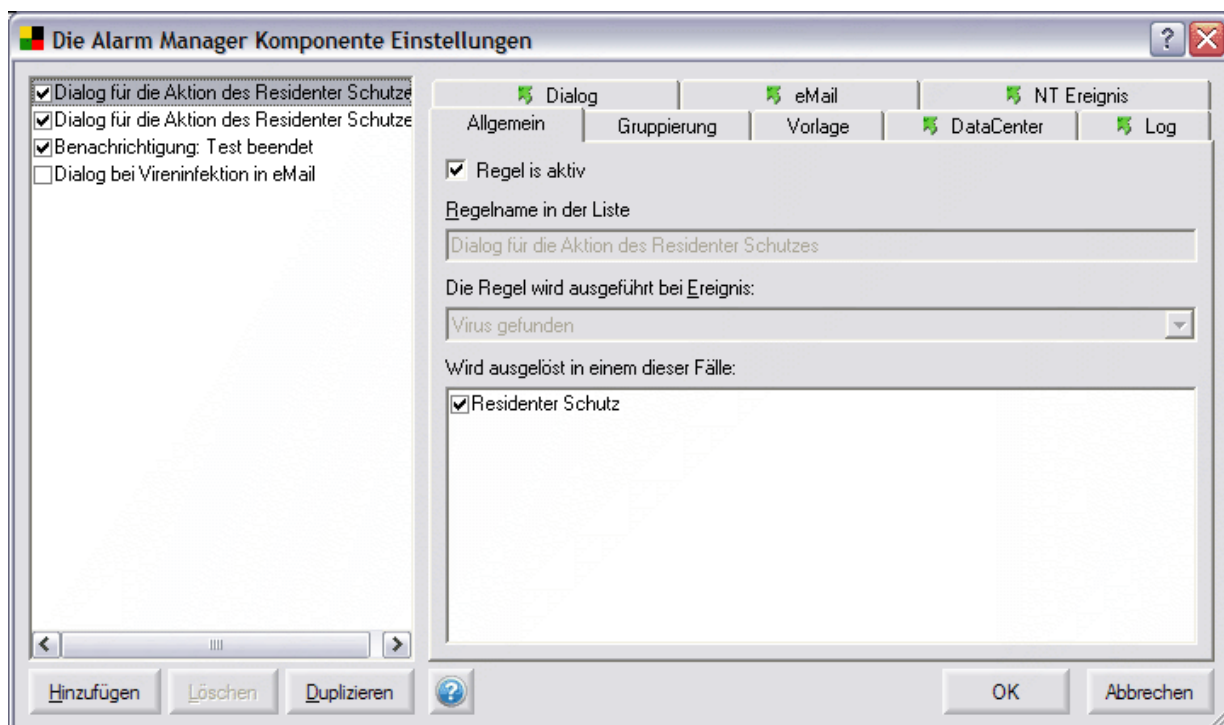
- o **Allgemein** – dieser Reiter zeigt allgemeine Informationen zu der Komponente **eMail-Kontrolle** an und lässt das Bearbeiten der Anzeige dieser Komponente zu.



## 10. Control Center Alarm Manager



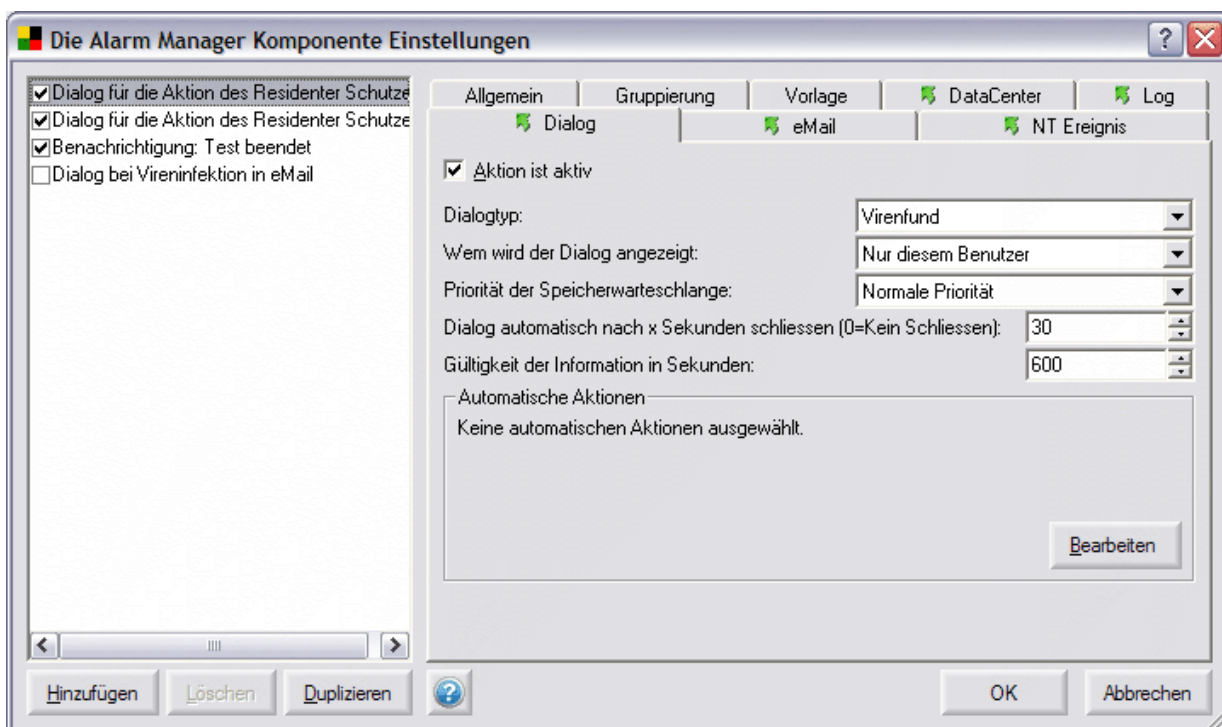
Drücken Sie die Schaltfläche **Einstellungen**, um den Dialog **Alarm Manager Komponenten Einstellungen** zu öffnen:



Auf der linken Seite des Fensters ist eine Liste mit Regeln. Aktive Regeln sind markiert. Auf der rechten Seite können Sie die ausgewählten Regeleinstellungen bearbeiten. Voreingestellte Regeln mit automatischen Einstellungen können nicht verändert werden (weder die Regel noch die Aktion).

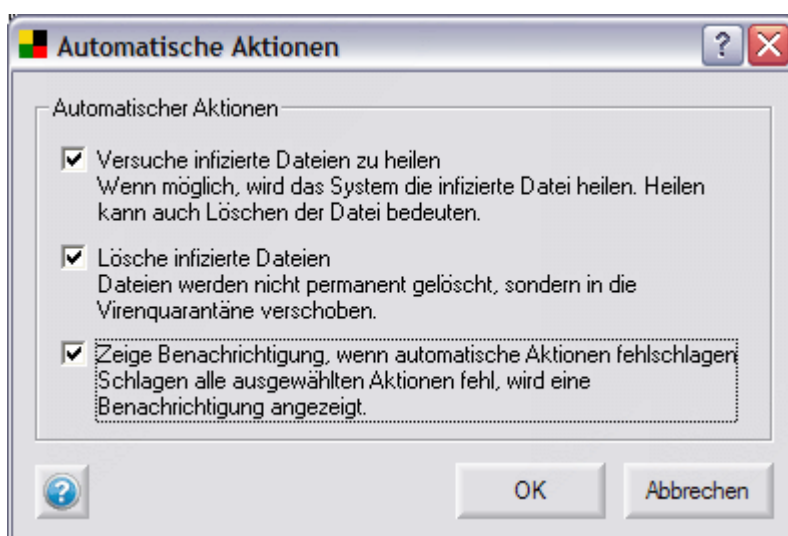
Allgemeine Eigenschaften, wie der Name einer Regel oder zusammenfassende Regeln sind für alle Regeln allgemeingültig. Reiter mit Aktionsdefinitionen sind durch grüne Pfeile gekennzeichnet. Für jede Regel kann mehr als eine Aktion definiert werden

Auf dem Screenshot unten können Sie ein Beispiel einer **Dialoganzeige** für definierte Aktionen der Regel **Dialog für die Aktion des Residenten AVG-Schutzes** sehen. Diese Regel läuft immer ab, wenn der **Residente AVG-Schutz** ein Virus entdeckt.



Auf dem Screenshot ist die Schaltfläche **Bearbeiten** hervorgehoben. Nach Drücken dieser Schaltfläche können Sie automatisch auszuführende Aktionen definieren. Als ein Beispiel sind alle möglichen Aktionen auf dem nächsten Screenshot ausgewählt:

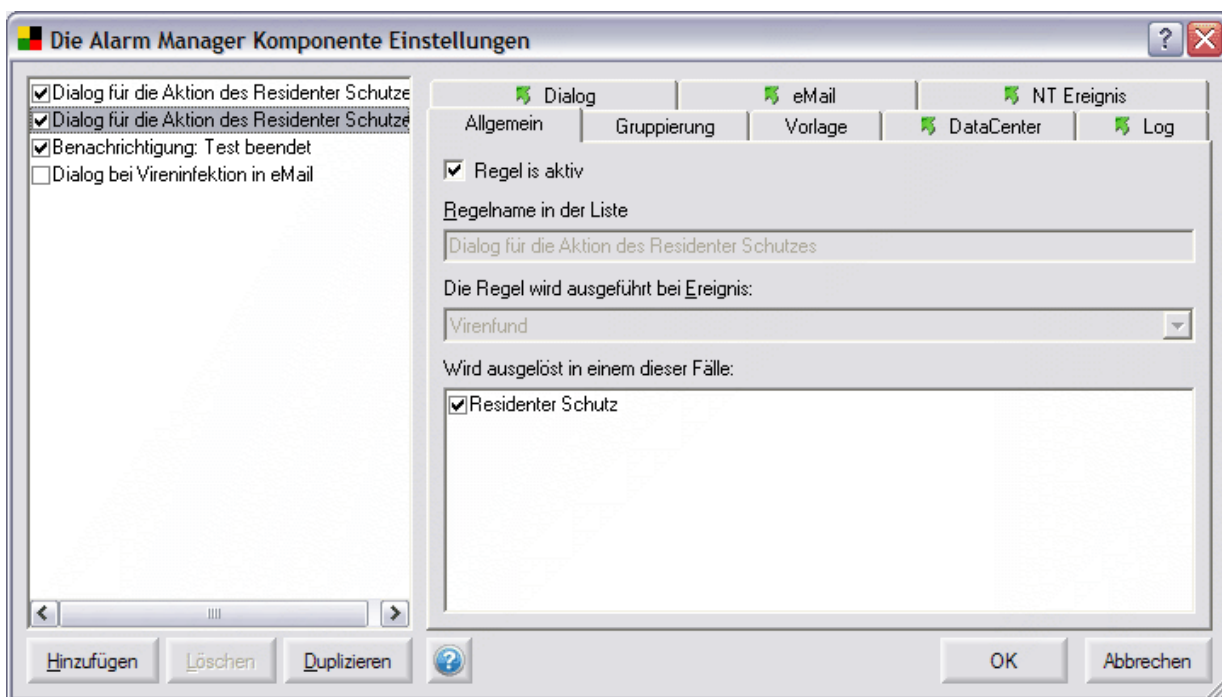
- **Versuche infizierte Dateien zu heilen – AVG** versucht, infizierte Dateien zu heilen (und wiederherzustellen).
- **Lösche infizierte Dateien – AVG** entfernt infizierte Dateien
- **Zeige Benachrichtigung, wenn automatische Aktionen fehlschlagen – AVG** zeigt dem Benutzer in einer Mitteilungsbox an, wenn ein automatischer Heilungsversuch fehlgeschlagen ist



Entsprechend der definierten Aktionen versucht **AVG** zuerst einmal eine infizierte Datei zu heilen. Sollte die Heilung nicht erfolgreich sein, versucht

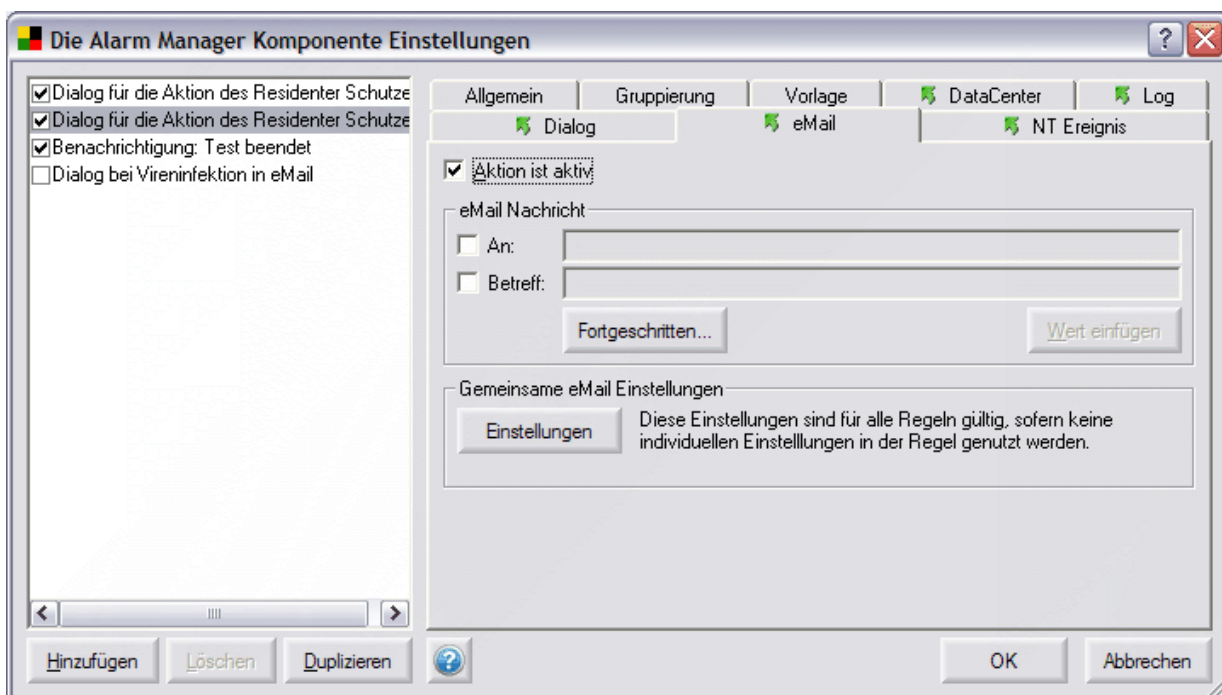
**AVG** die Datei zu löschen: wenn die Datei gelöscht werden soll, wird sie auf jeden Fall in die **AVG Virenquarantäne** verschoben. Wenn das Löschen ebenfalls fehlschlagen sollte, wird **AVG** schließlich eine entsprechende Mitteilung anzeigen.

Nachdem jede der oben genannten automatischen Aktionen durchgeführt wurde, wird ein **Virenfund**-Ereignis erstellt. Dieses Ereignis wird an eine weitere voreingestellte Regel weitergegeben - **Dialog für die Aktionen des Residenten AVG-Schutzes**:



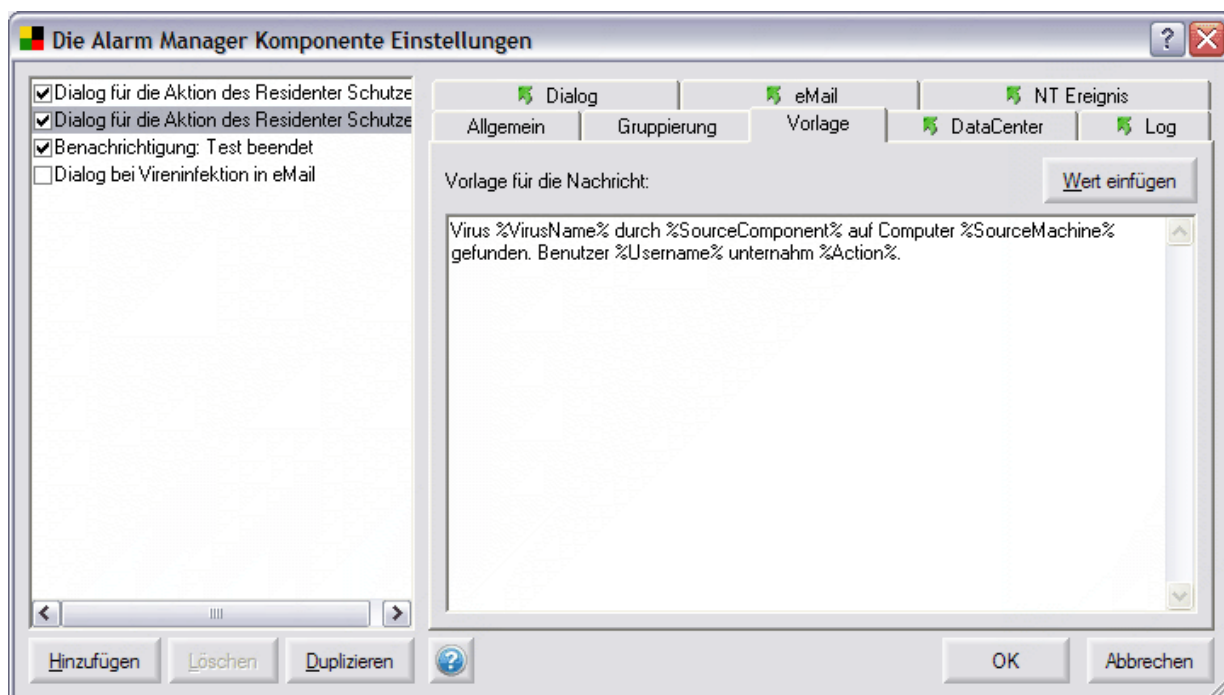
In den voreingestellten Einstellungen dieser Regel ist eine Aktion zum **Senden einer Mitteilung an das AVG DataCenter** definiert.

Für einige bestimmte Ausnahmefälle kann es auch angebracht sein, eine eMail zu senden – diese Option können Sie im Reiter **eMail** näher definieren:



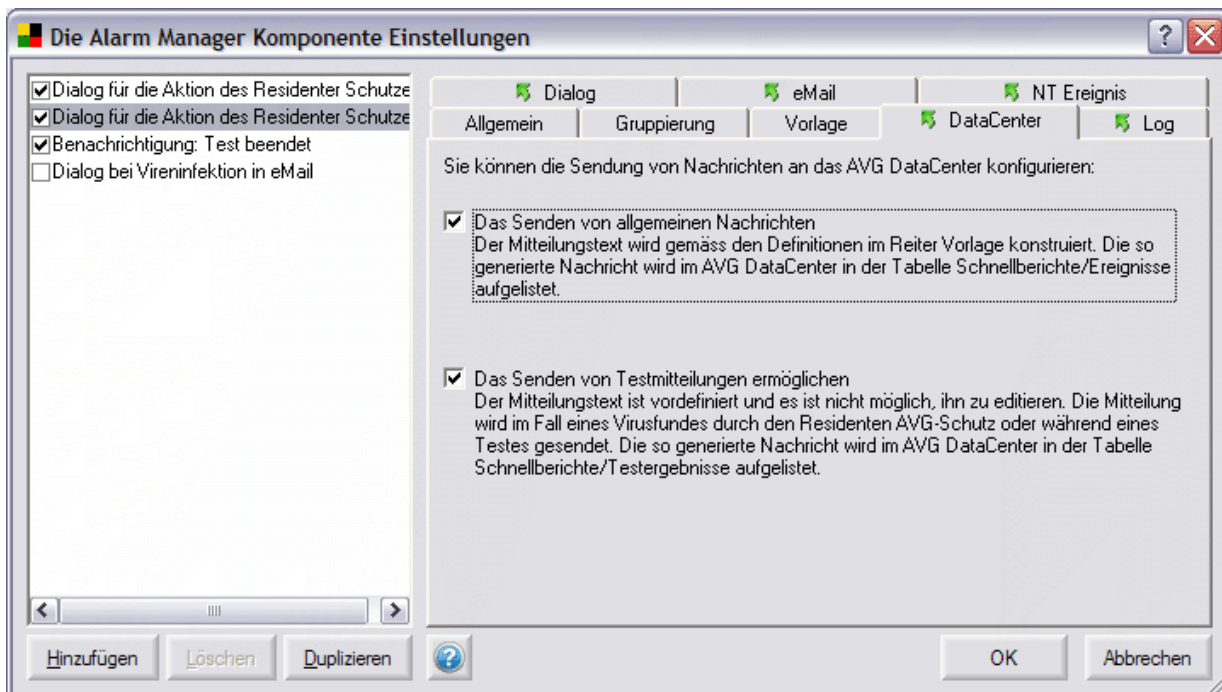
Die Schaltfläche **eMail Einstellungen** öffnet einen neuen Dialog, in dem Sie die allgemein gültigen Mail-Einstellungen bearbeiten können, die auch von allen anderen Regeln gemeinsam genutzt werden (Sendename, Adresse des Mail-Servers usw.).

Der zu verwendende Text für eine ausgelöste Aktion (z. B. eMail-Text) wird auf dem Reiter **Vorlage** vordefiniert. Der Nachrichtentext kann durch spezielle Werte, die mit dem Ereignis verbunden sind, aufgefüllt werden. Diese Werte werden innerhalb der Zeichen **%** für den internen Ablauf angegeben. Um einen neuen Wert hinzuzufügen klicken Sie bitte auf die Schaltfläche **Wert einfügen**:



Standard-Regeln sind Mitteilungen, die bestimmte wichtige Ergebnisse an das **AVG DataCenter** übermitteln. Diese Mitteilungen werden sich immer auf bestimmte Übersichten auswirken. Zum Beispiel wird ein Testergebnis in Abhängigkeit zu den im **AVG DataCenter** festgelegten Bedingungen weiterverarbeitet (z. B. Aktivierung/Deaktivierung der Weitergabe von negativen Testergebnissen). Mit Ausnahme von eben diesen können Sie eine allgemeine Ereignis-Mitteilung an das **AVG DataCenter** senden. Diese Mitteilungen werden in der Ereignisübersicht aufgezeichnet.

Auf dem unten dargestellten Screenshot ist nur das Versenden von allgemeinen Textmitteilungen ermöglicht:

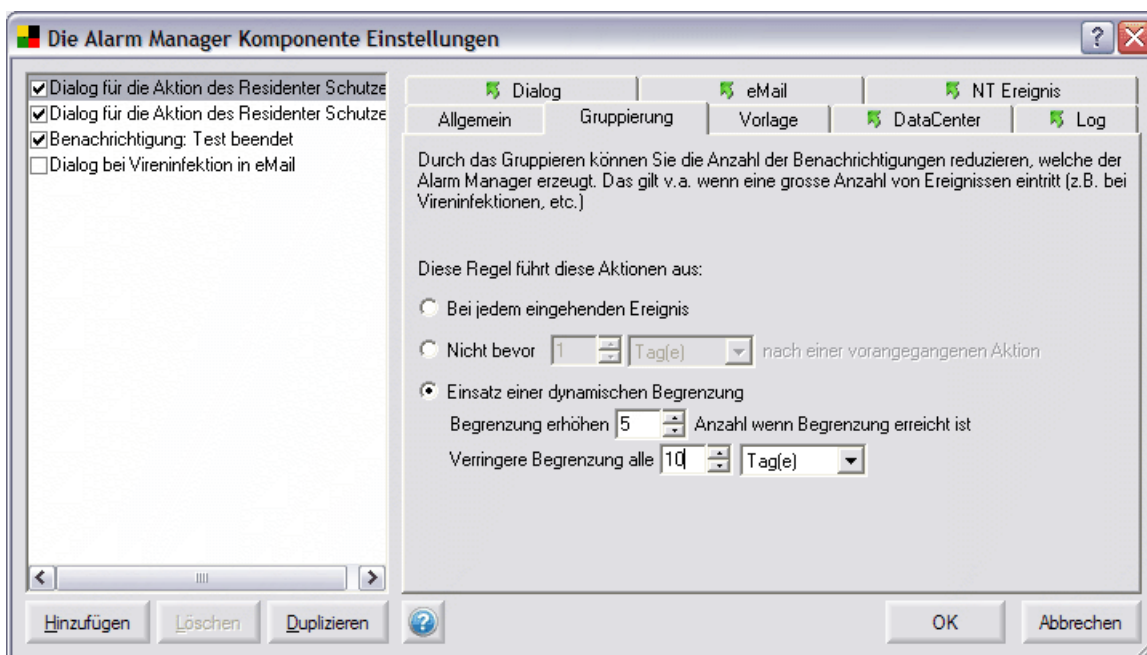


### **Achtung!**

Damit die AVG 7.5 File Server Edition richtig funktioniert, wird empfohlen, die Option **Aktiviere Senden von allgemeinen Textnachrichten** für voreingestellte Regeln nicht abzuschalten! Das Abschalten dieser Aktion macht ist nur in ganz besonderen Ausnahmefällen Sinnsinnvoll. Um eine allgemeine Textbenachrichtigung zu versenden, empfehlen wir die Erstellung einer neuen Regel!

#### **a) Gruppierung von Ereignissen**

Bei einem großen massiven Virenbefall kann die Frequenz der Mitteilungen sehr groß werden. Wenn im Falle eines Virenfundes die **eMail-Mitteilungsaktion** ausgelöst wurde, kann die Mailbox sowie der Mailserver des Empfängers sehr schnell überfüllt sein. Um eine derartige Flut von Ereignismitteilungen zu verhindern, können Sie für jede Regel Bedingungen für die Gruppierung von Ereignissen definieren.



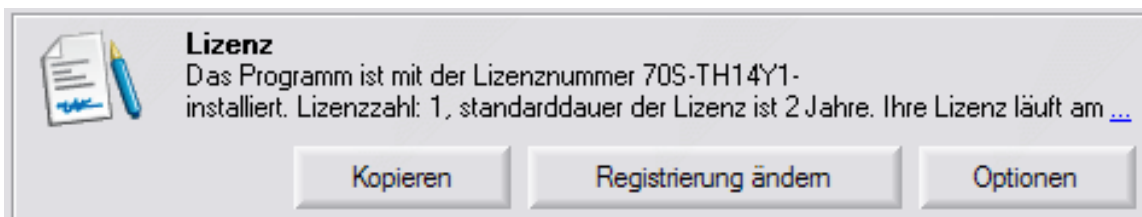
- **Bei jedem eingehenden Ereignis** – Standardmäßig wird bei jedem Ereignis eine Aktion ausgelöst.
- **Nicht bevor ... nach einer vorangegangenen** - Es ist jedoch möglich, das Auslösen der nächsten Aktion durch Festlegen eines minimalen Zeitfensters, in welchem ein wiederholt auftretendes Ereignis ignoriert wird, zu verzögern. Alle Ereignisse, die in diesem Intervall auftreten, werden in einer Gruppe zusammengefasst. Die nächste Aktion (z. B. Versenden der nächsten eMail) wird in einer Übersicht über die zusammengefassten Ereignisse wiedergegeben.
- **Nutzen einer dynamischen Begrenzung** - In diesem Modus wird jede ausgelöste Aktion die Grenze gruppierter Ereignisse n-fach erhöhen. Die erste Virenerkennung wird eine Aktion auslösen. Das gleiche nachfolgende Ereignis wird keine Aktion mehr auslösen – es wird stattdessen in einer Gruppe zusammengefasst. Auf dem Screenshot oben ist die Grenze mit 5 gesetzt, d. h., die nächste Aktion wird erst nach 5 erfolgreichen Virenerkennungen ausgelöst. Würde eine 6. Erkennung folgen, dann würde die Grenze nochmals 5-fach erhöht. Nach Ablauf des festgelegten Zeitraums wird die Grenze automatisch wieder zurückgesetzt.

Diese Eigenschaft gestattet eine flexible Anpassung an die vorherrschende Situation. Auf der einen Seite dient es bei einem einzelnen Ereignis der sofortigen Benachrichtigung des Administrators, zum anderen wird die Möglichkeit der Netzwerküberlastung im Falle eines dramatischen Virenbefalls minimiert.

## 10.2. Control Center - Lizenz

Das Fenster **Lizenz** zeigt den vollständigen Wortlaut der AVG-Lizenzbedingungen an.

## AVG 7.5 File Server



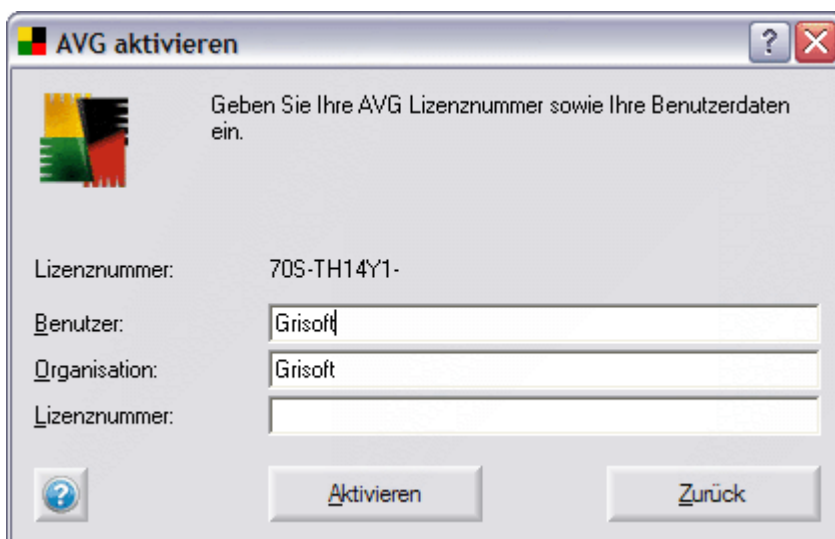
Im Dialogfenster **Lizenz** stehen die folgenden Schaltflächen zur Verfügung:

**a) Kopieren**

Die Schaltfläche **Kopieren** kopiert automatisch Ihre Lizenznummer in die Zwischenablage, so dass Sie diese - wenn nötig - einfügen können (dies kann sehr hilfreich bei einer AVG Online-Registrierung sein).

**b) Registrierung ändern**

Die Schaltfläche **Registrierung ändern** startet das Dialogfenster **AVG aktivieren**: geben Sie Ihre Lizenzdaten ein, um Ihr AVG zu aktivieren.



**c) Optionen**

- o Die Schaltfläche **Optionen** zeigt allgemeine Informationen zu der Komponente **Lizenz** an und lässt das Bearbeiten der Anzeige dieser Komponente zu:

## AVG 7.5 File Server



## 11. Virenquarantäne

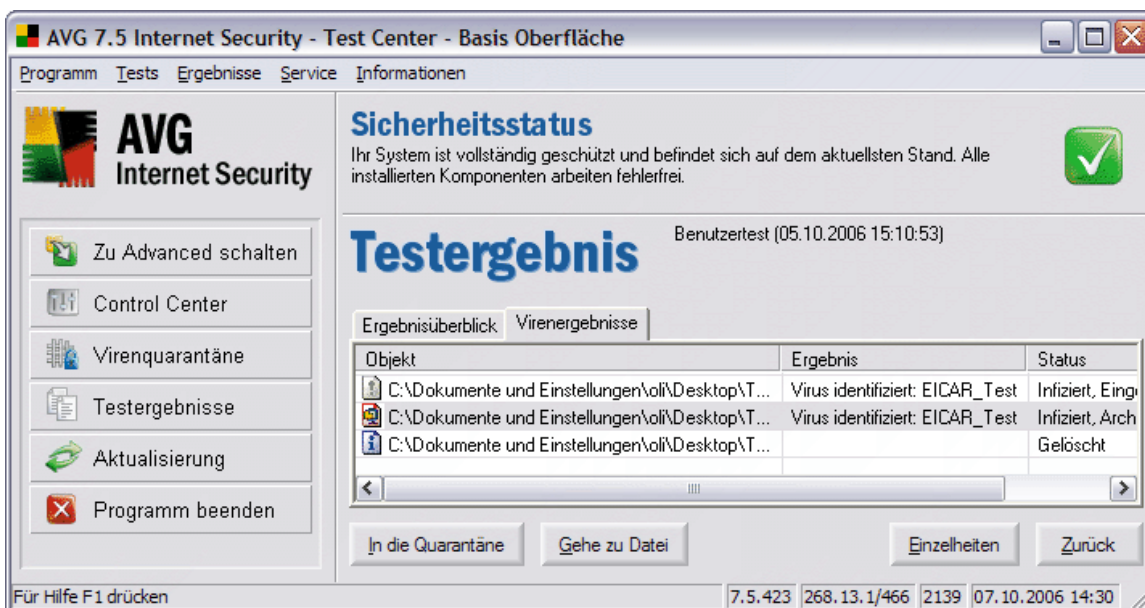
Die **Virenquarantäne** ist eine sichere Arbeitsumgebung für die Verwaltung verdächtiger/infizierter Objekte, die während der AVG Tests gefunden wurden.

Wenn während eines Tests ein infiziertes Objekt gefunden wird und AVG es nicht automatisch heilen kann, werden Sie gefragt, was mit dem verdächtigen Objekt geschehen soll. Die empfohlene Lösung ist, das verdächtige Objekt in die **Virenquarantäne** zur weiteren Bearbeitung zu verschieben.

### 11.1. Verschieben verdächtiger Objekte in die Virenquarantäne

Wenn ein verdächtiges/infiziertes Objekt während eines Tests gefunden und in den Testergebnissen angezeigt wird, sollten Sie dieses Objekt in die **Virenquarantäne** verschieben:

- Wählen Sie im Fenster **Testergebnis** (im entsprechenden Reiter-**Virenergebnisse** oder **Spyware gefunden**) die infizierte Datei (Virus, Eintrag in der Registry, Cookie usw.) aus, die Sie in die **Virenquarantäne** verschieben möchten
- Drücken Sie die Schaltfläche **In die Quarantäne**, um das Objekt in die Quarantäne zu verschieben



In der **Virenquarantäne** können Sie die Objekte untersuchen, löschen und gegebenenfalls auch heilen und reparieren, sobald eine neue Heilmethode für dieses Virus in das Programm implementiert wurde.

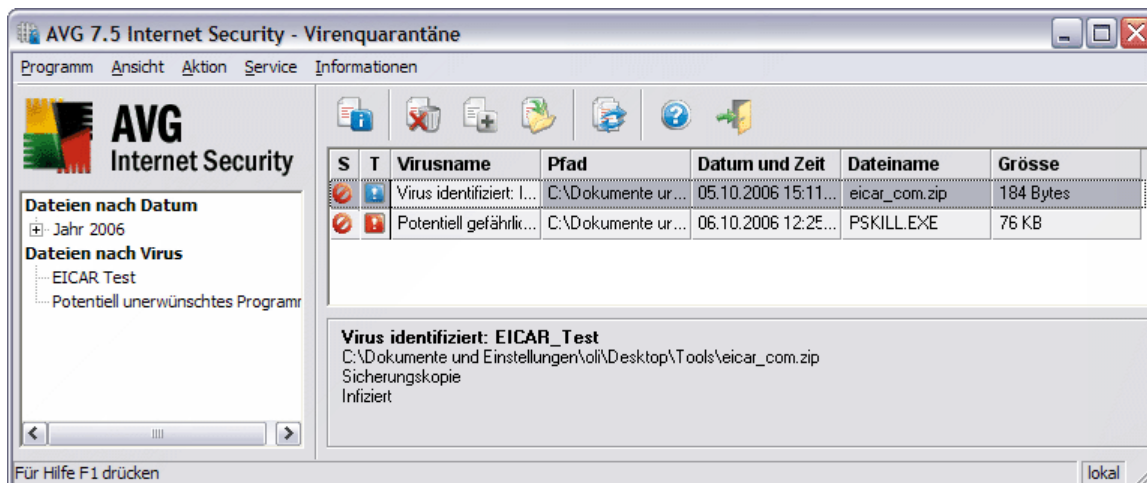
### 11.2. Virenquarantäne Umgebung

Öffnen der **Virenquarantäne**:

- Wählen Sie in der **Basis Oberfläche** im linken Menü **Virenquarantäne** aus
- Wählen Sie in der **Advanced Oberfläche** aus dem Hauptmenü **Programm/Virenquarantäne starten** aus

- Im Control Center wählen Sie bitte aus dem Hauptmenü **Programm/Virenquarantäne starten**

Aus dem Windows **Start** Menü: **Start/Programme/AVG 7.5/AVG Virenquarantäne**



Der Navigationsbaum im linken Bereich der **AVG Virenquarantäne** gibt Ihnen die Möglichkeit, infizierte Objekte zu sortieren:

- Nach Datum
- Nach Virennamen

Alle in der **Virenquarantäne** gespeicherten infizierten Objekte werden in einer Liste im Hauptbereich angezeigt; zu jedem Objekt gibt es folgende Informationen:

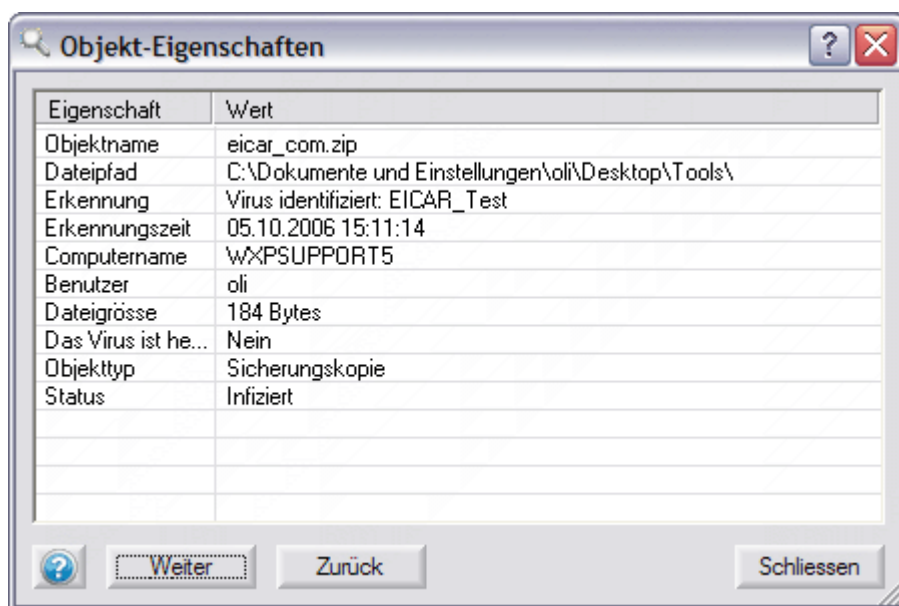
- **S** – Objektstatus:
  - infiziertes / verdächtiges Objekt (*Kreis mit rotem X*)
  - geheiltes Objekt (*rotes X*)
- **T** – Objekttyp
  - Objekt wurde in die **Virenquarantäne** verschoben (*Ausrufezeichen im roten Feld*)
  - Backup des Objekts wurde in der **Virenquarantäne** vor einem Heilungsversuch erstellt (*Ausrufezeichen im blauen Feld*)
- **Virusname** – vorgeschlagener Name der Infektion
- **Pfad** – vollständige Pfadangabe zum vorherigen Speicherplatz des verdächtigen Objekts
- **Datum und Zeit** – Datum und Zeit der Identifizierung als verdächtiges Objekt
- **Dateiname** – exakter Name der verdächtigen/infizierten Datei
- **Dateigröße** – exakte Größe der verdächtigen/infizierten Datei

### 11.3. Verwalten der Virenquarantäne

Um die Arbeitsumgebung der **Virenquarantäne** zu verwalten, wählen Sie bitte folgende Optionen aus dem Menüpunkt **Aktion** des Hauptmenüs aus:

- **Aktion/Objekt-Eigenschaften**

Anzeigen detaillierter Informationen über das infizierte Objekt



- **Aktion/Virenquarantäne ausleeren**

löscht den gesamten Inhalt der **Virenquarantäne**.

- **Aktion/Objekte heilen**

heilt das gewählte Objekt, falls eine Heilmöglichkeit zur Verfügung steht; sobald eine Datei geheilt wurde ändert sich der Status in **geheiltes Objekt**.

- **Aktion/Objekte löschen**

entfernt das gewählte Objekt aus der **Virenquarantäne**.

- **Aktion/Objekte speichern (Objekte speichern unter...)**

Wiederherstellen eines Objekts, das als verdächtig in die Virenquarantäne verschoben wurde; Sie werden nach dem Namen und dem Speicherort der wiederherzustellenden Datei gefragt.

Die Symbolleiste im oberen Bereich des Bildschirms stimmt mit den Hauptmenü-Optionen überein. Um die Symbolleiste anzuzeigen / auszublenden wählen Sie aus dem Hauptmenü **Ansicht/Symbolleiste** aus.

Die weiteren Menüpunkte des Hauptmenüs entsprechen denen der weiteren **AVG**-Anwendungen. Für detaillierte Informationen lesen Sie bitte das Kapitel [7. AVG Basis Oberfläche](#).

## 12. Test Übersicht

Eine der Hauptfunktionen von AVG ist die Überprüfung On-Demand. On-Demand-Tests wurden entwickelt, um verschiedene Bereiche Ihres Computers zu überprüfen, wenn ein Verdacht auf eine Vireninfektion vorliegt. Auf jeden Fall empfehlen wir eine regelmäßige Durchführung dieser Tests, auch wenn Sie glauben, dass kein Virus auf dem Computer gefunden wird. Das empfohlene Zeitintervall für diese Tests ist ungefähr 1 Woche.

Alle On-Demand Tests werden in der **Test Center** Umgebung gestartet. Die Tests können auch geplant und entsprechend der voreingestellten Pläne durchgeführt werden.

Für weitere Informationen zur Testplanung lesen Sie bitte Kapitel [7.9 AVG Basis Oberfläche / Testplanung](#) oder [8.2 AVG Advanced Oberfläche / Scheduler](#)

Standardmäßig sind verschiedene Testarten mit voreingestellten Parametern vorhanden.

- **Kompletter Test**
- **Benutzertest**
- **Ausgewählte Bereiche Test**
- **Ausführlicher Test**
- **Detaillierter Benutzer-Test** (erreichbar über den **Testmanager** in der **Advanced Oberfläche**)
- **Systembereiche Test** (erreichbar über den **Testmanager** in der **Advanced Oberfläche**)

Sie können die Testkonfiguration entsprechend Ihren eigenen Wünschen konfigurieren. Für weniger erfahrene Benutzer wird jedoch die Verwendung der Standardtests empfohlen.

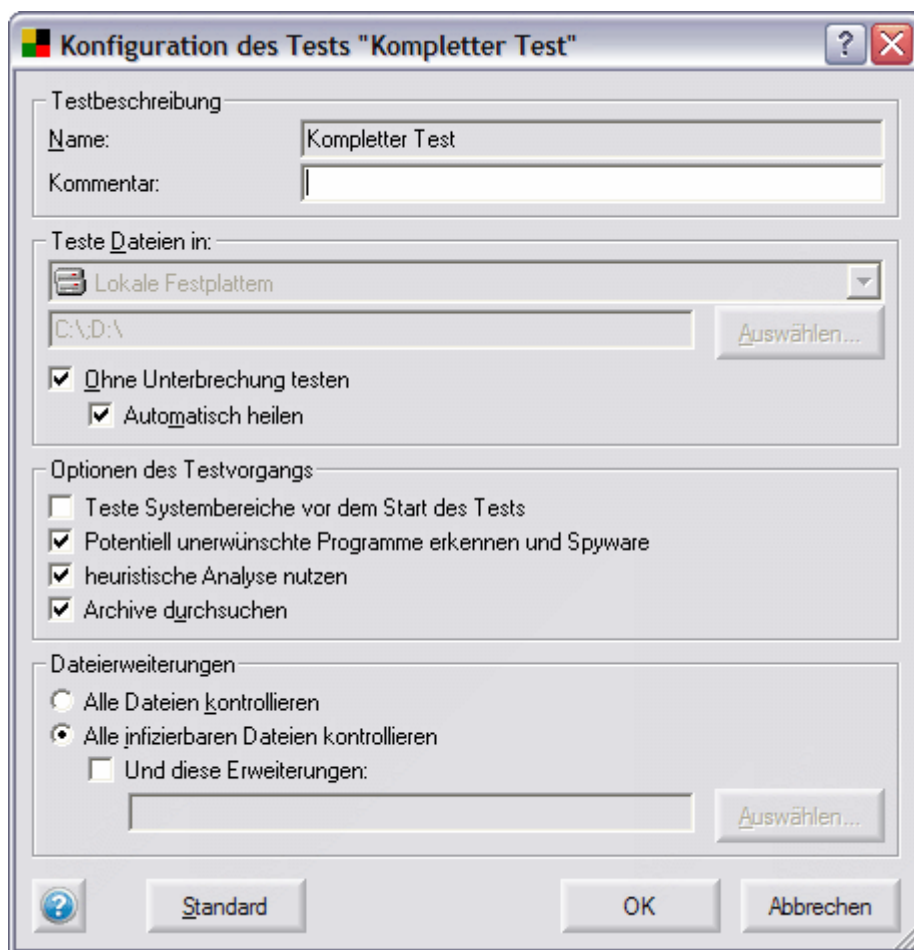
### 12.1. Kompletter Test

Der **Komplette Test** überprüft alle Festplatten auf Ihrem Computer und findet, heilt oder entfernt alle eventuell gefundenen Viren.

#### a) Kompletter Test – Einstellungen

Der **Komplette Test** kann entweder mit der vom Hersteller vordefinierten Standardkonfiguration verwendet werden, oder Sie können Ihre eigenen Testeinstellungen definieren (dies wird jedoch nur erfahrenen Anwendern empfohlen!). Zum Bearbeiten der Einstellungen des **Kompletten Tests** führen Sie bitte die folgenden Schritte aus:

- Wählen Sie in der **Basis Testoberfläche** aus dem Hauptmenü den Punkt **Tests/Einstellungen des Kompletten Tests** aus, um das Dialogfenster mit der grundlegenden Konfiguration des **Kompletten Test** zu öffnen:



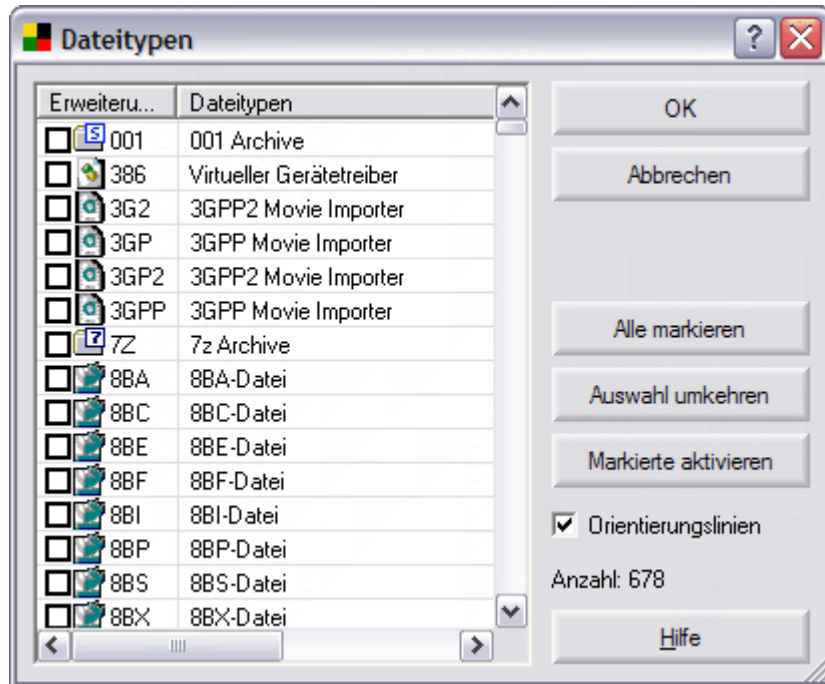
Dieser Dialog erlaubt Ihnen die Konfiguration der folgenden Parameter:

- **Name und Kommentar** – als **Name** wird standardmäßig der Text **Kompletter Test** voreingestellt; im Feld **Kommentar** können Sie zusätzliche Informationen über den Test angeben.
- **Teste Dateien in**– der komplette Test überprüft alle Festplatten Ihres PCs und in der **AVG Basis Oberfläche** können Sie diese Einstellung auch nicht verändern.
- **Optionen des Testvorgangs** – in diesem Abschnitt können Sie die gewünschte Testmethode definieren und die Funktionen aus einer Liste auswählen, die während eines Tests angewendet werden sollen. Wenn Sie nicht möchten, dass **potentiell unerwünschte Programme und Spyware** erkannt werden sollen, demarkieren Sie bitte diese Option. Weitere Informationen über **Potentiell Unerwünschte Programme** erhalten Sie in [Kapitel 7.14](#).
- **Dateierweiterungen** – bestimmen Sie, ob alle Dateien (**Alle Dateien kontrollieren**) oder nur infizierbare Dateien (**Alle infizierbaren Dateien kontrollieren**) überprüft werden sollen.

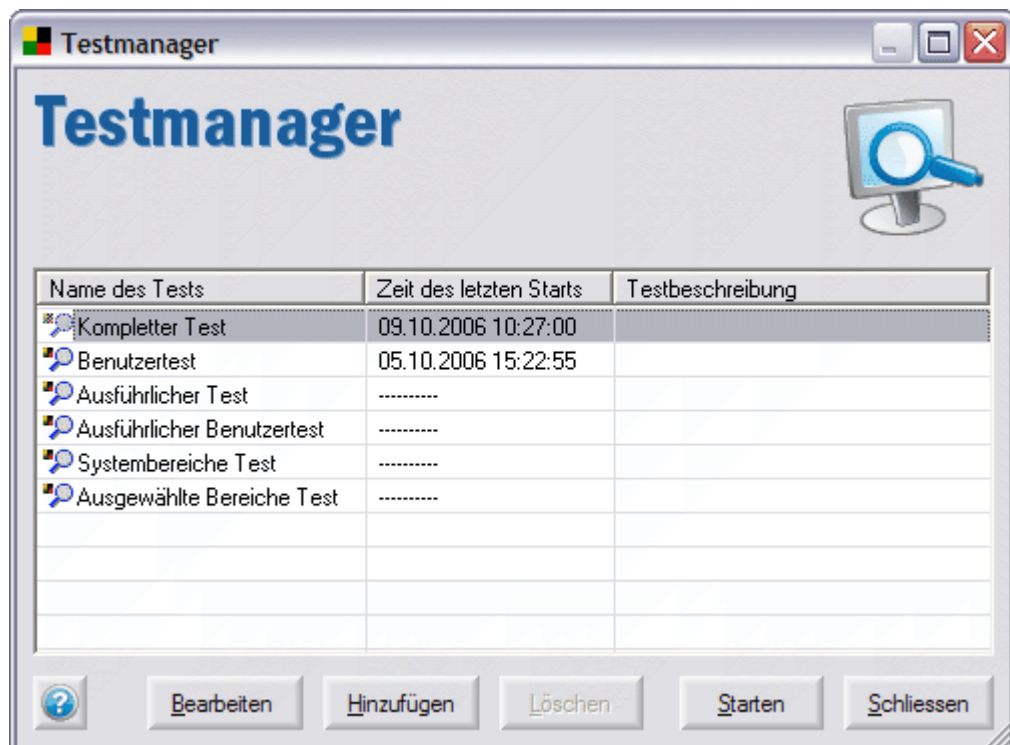
Wenn Sie sich für die Option alle infizierbaren Dateien kontrollieren entscheiden, können Sie auch bestimmte Dateierweiterungen auswählen. Markieren Sie die Auswahlbox **Und diese Erweiterungen**, um die Schaltfläche **Auswählen** zu aktivieren, die ein neues Dialogfenster öffnet. In diesem Fenster erscheint eine Liste mit den

# AVG 7.5 File Server

Dateierweiterungen und den dazugehörigen Dateitypen; wählen Sie diejenigen aus, die kontrolliert werden sollen:



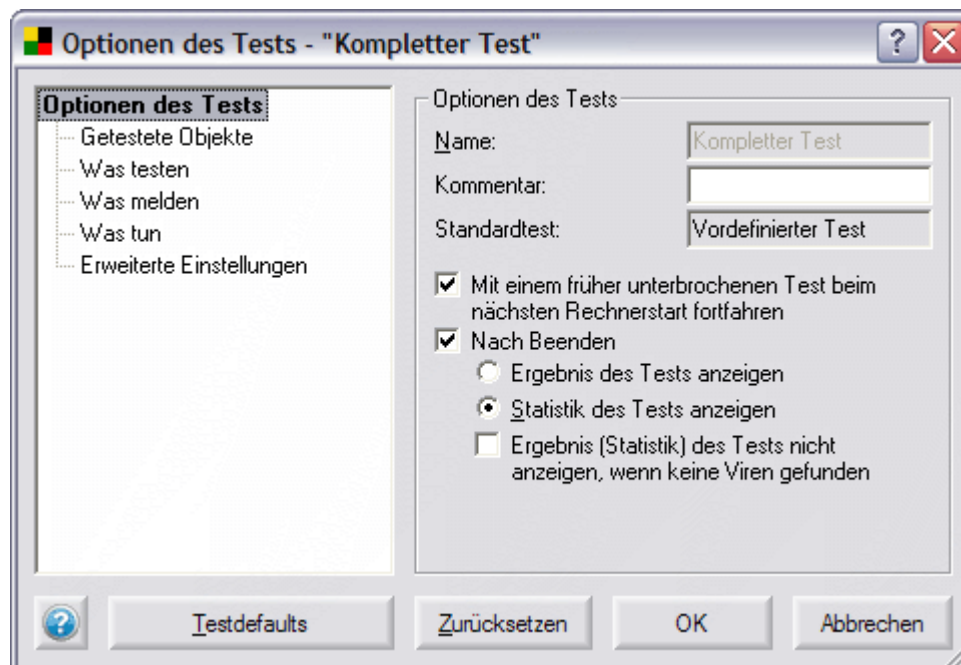
- o Wählen Sie in der **Advanced Testoberfläche** aus dem Hauptmenü den Eintrag **Tests/Testmanager/Kompletter Test**:



Drücken Sie die Schaltfläche **Bearbeiten** um ein Dialogfenster mit einer erweiterten Konfiguration des **Kompletten Test** mit sechs Reitern zu

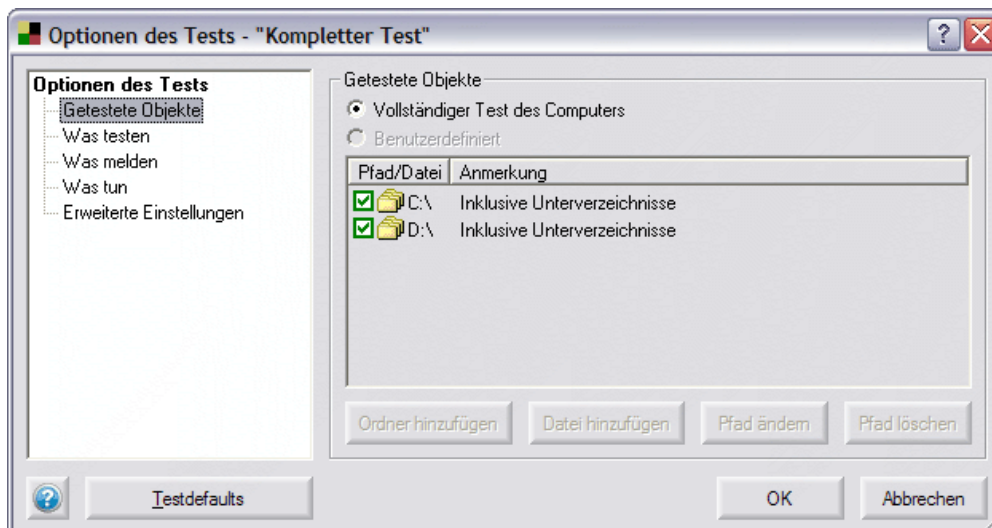
erhalten (diese können nacheinander im Navigationsbaum auf der linken Seite geöffnet werden):

- **Optionen des Tests**



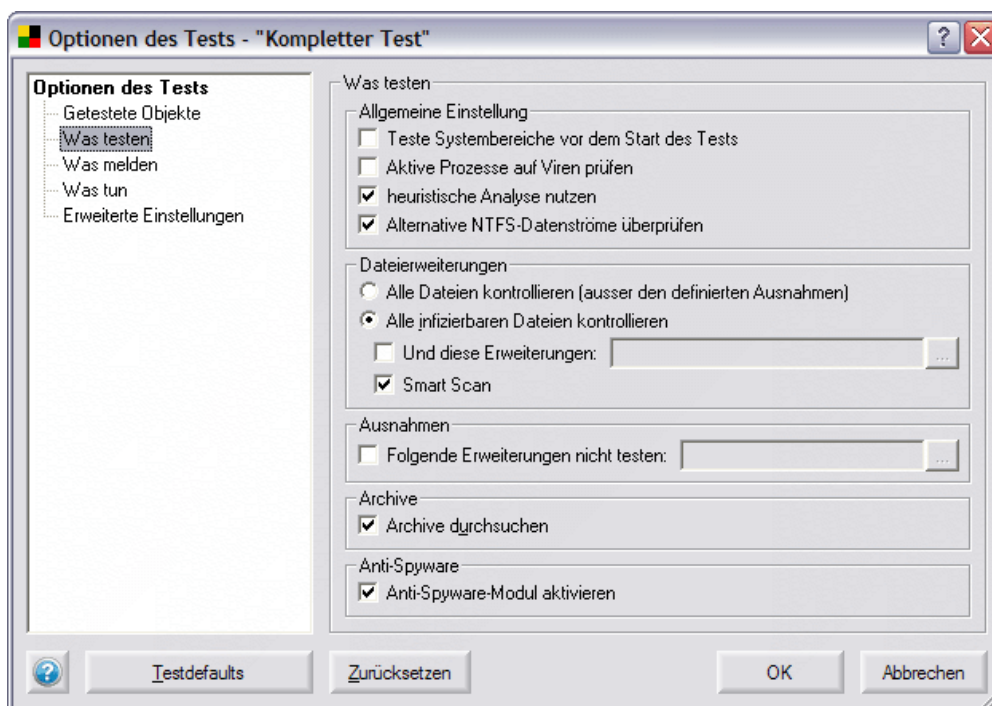
- **Name** – der Testname ist standardmäßig auf **Kompletter Test** eingestellt und kann nicht verändert werden
- **Kommentar** – in diesem Feld können Sie Ihre eigenen, ergänzenden Informationen zur Beschreibung des Tests hinzufügen (spezielle Einstellungen...)
- **Standardtest** – dieses Feld beinhaltet die Information, dass dieser Test vom Hersteller vordefiniert ist
- **Mit einem früher unterbrochenen Test beim nächsten Rechnerneustart fortfahren** – markieren Sie diese Option, wenn ein unterbrochener Test die Überprüfung fortführen soll (beim zweiten Start des Tests werden nur die Ordner überprüft, die vorher nicht getestet wurden)
- **Nach Beenden** – bestimmen Sie, welche Informationen nach Beendigung eines Tests angezeigt werden sollen

- **Getestete Objekte**



Standardmässig überprüft der **Komplette Test** alle Festplatten auf ihrem Computer und Sie können keine speziellen Pfade angeben.

o **Was testen**

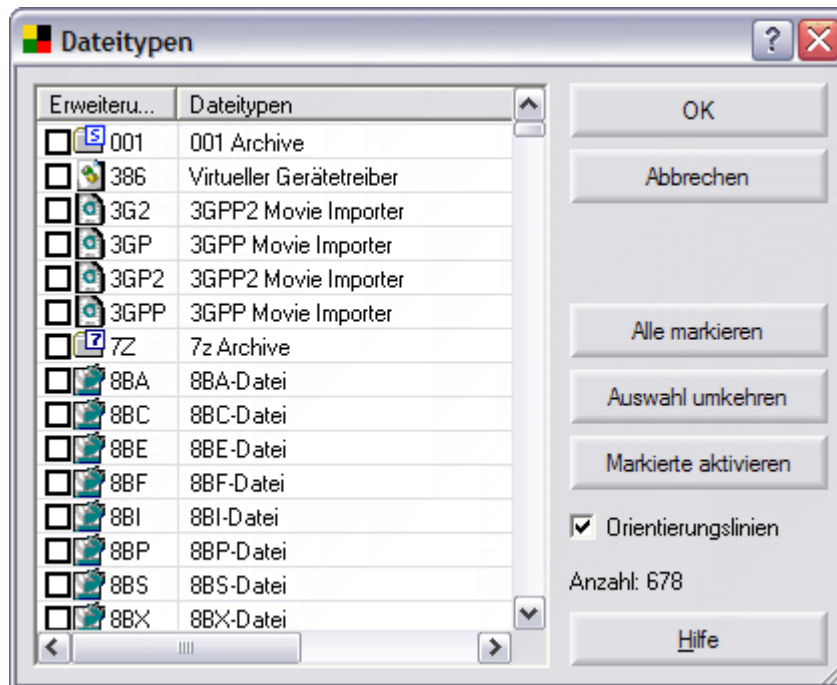


- **Allgemeine Einstellung** – in diesem Dialog können Sie definieren, ob die Systembereiche getestet werden sollen und ob hierfür die heuristische Analyse genutzt werden soll. Sie können auch alle aktiven Vorgänge des Betriebssystems testen, indem Sie auf die Schaltfläche **Aktive Prozesse auf Viren prüfen** klicken. Ein aktiver Prozess ist eine laufende Anwendung, die ein normales Software-Programm ein kann, aber auch ein Virus/Spyware/Malware oder ähnliche Art von Bedrohung. Hier können Sie auch wählen, dass **Alternative NTFS-Datenströme überprüfen** nicht getestet werden sollen.

## AVG 7.5 File Server

- **Anmerkung:** *Alternative NTFS-Datenströme ist ein Windows-Feature, das von Angreifern (meist Hackern) für versteckte Dateien, besonders Rootkits, Viren, Trojaner usw. missbraucht wird. Daher wird empfohlen, diese Einstellungen beizubehalten (standardmäßig eingestellt).*
- Sie können auch alle aktiven Prozesse des Betriebssystems testen, indem Sie das Häkchen unter **Aktive Prozesse auf Viren prüfen** setzen. Ein aktiver Prozess ist normalerweise eine laufende Anwendung, die eine normales Software sein kann, aber auch ein Virus/Spyware/Malware oder eine andere Art von Bedrohung
- Weiterhin entscheiden Sie, ob der Test für alle Dateien oder nur für infizierbare Dateien (**Dateierweiterungen**) durchgeführt werden soll und Sie sollten Dateierweiterungen (**Exclude**) angeben, die vom Test ausgenommen werden sollen. Sie können auch die Option wählen, dass Dateien innerhalb eines Archivs getestet werden.
- Im Bereich **Anti-Spyware** können Sie das Testen auf Spyware/Malware mit der Anti-Spyware-Engine aktivieren/deaktivieren (markieren Sie hierfür das Kästchen **Anti-Spyware Modul aktivieren**)

Wenn Sie sich für die Option alle infizierbaren Dateien kontrollieren entscheiden, können Sie auch bestimmte Dateierweiterungen auswählen, die kontrolliert werden sollen. Markieren Sie die Auswahlbox **Und diese Erweiterungen**, um die Schaltfläche **Auswählen** zu aktivieren, die das Dialogfenster **Dateierweiterungen** öffnet.



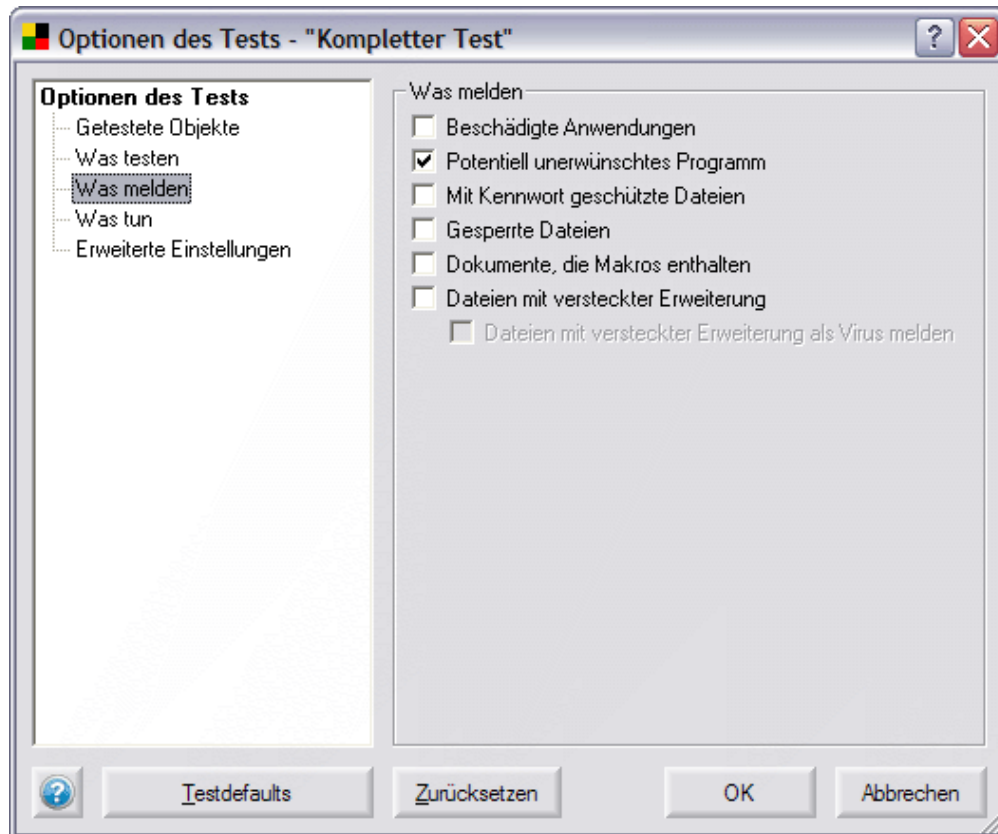
In diesem Dialog werden Sie dazu aufgefordert, aus der Liste der Dateierweiterungen und die entsprechenden Dateien auszuwählen, die überprüft werden sollen. Der Dialog **Dateitypen** beinhaltet die folgenden Kontrollschaltflächen:

## AVG 7.5 File Server

- **OK** – akzeptiert die ausgewählten Dateierweiterungen und fügt alle Dateien mit der entsprechenden Dateierweiterung dem **Kompletten Test** hinzu. Der Dialog **Dateitypen** wird geschlossen.
- **Abbrechen** – schließt das Dialogfenster **Dateierweiterungen**, ohne dass irgendwelche Veränderungen vorgenommen werden
- **Alle markieren** – wählt alle Dateierweiterungen in der Liste aus
- **Auswahl umkehren** – wenn Sie eine große Anzahl von Dateierweiterungen auswählen möchten, kann es sinnvoller sein, die Dateierweiterungen zu definieren, die Sie nicht überprüfen wollen und dann die Auswahl umzukehren
- **Markierte aktivieren** – Dateien mit einer bestimmten Dateierweiterung können direkt in der Liste ausgewählt werden, indem Sie auf den Dateinamen klicken (für mehrere Markierungen halten Sie bitte die **Shift** Taste zur selben Zeit gedrückt) und dann mit Hilfe der Schaltfläche **Auswahl markieren** hervorgehoben werden
- **Hilfe** – öffnet ein neues Dialogfenster mit der entsprechenden Hilfe-Information

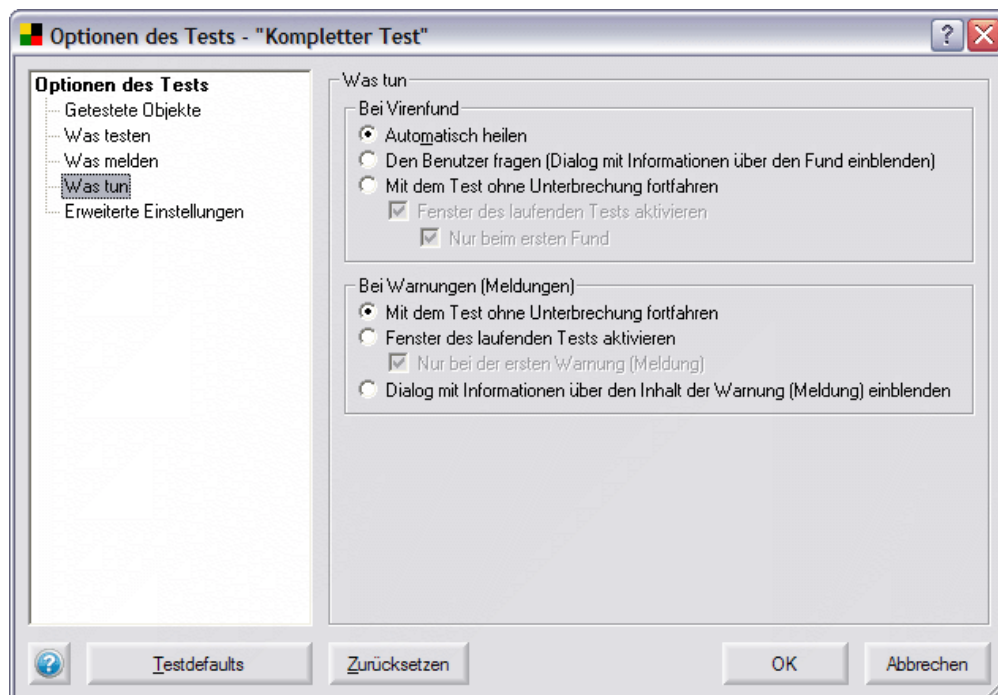
Im Abschnitt **Datei Erweiterungen** können Sie auch die Option **Smart Scan** auswählen. Diese Option kann jedoch nur ausgewählt werden, wenn Sie vorher die Option nur infizierbare Dateien kontrollieren ausgewählt haben. Die Funktion **Smart Scan** kann Dateitypen anhand Ihres Inhalts erkennen, ohne die Dateierweiterung zu beachten, d.h. dass Dateien überprüft werden, auch wenn die Dateiendungen nicht definiert wurden (z.B. *exe-Dateien die umbenannt wurden*).

- **Ausnahmen** – in diesem Abschnitt können Sie Dateierweiterungen festlegen, die bei einem **Kompletten Test** ausgelassen werden sollen. Verwenden Sie die Schaltfläche (...) um den **Dateierweiterungen** Dialog erneut zu öffnen und legen Sie fest, welche Dateien überprüft werden sollen. Für eine detaillierte Beschreibung dieses Dialogs lesen Sie bitte den vorangegangenen Absatz.
  - **Archive** – dieser Abschnitt enthält die Option **Archive durchsuchen**. Wenn diese Option ausgewählt ist, öffnet und durchsucht der **Komplette Test** auch alle Dateien die in üblichen Archiven gespeichert sind.
- o **Was melden**

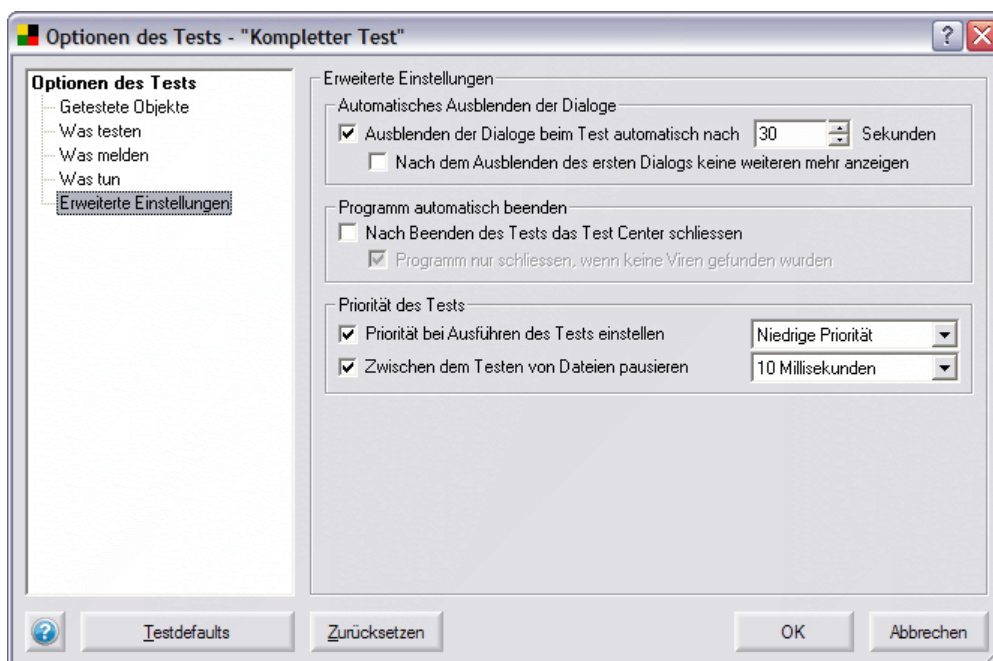


Dieser Dialog beinhaltet eine Liste von Ereignissen, die während des Tests auftreten können. Markieren Sie die Ereignisse, über deren Auftreten Sie informiert werden möchten.

o **Was tun**



- **Bei Virenfund** – falls während des Tests ein Virus gefunden wird, kann dieses Virus geheilt werden, falls ein Heilmittel verfügbar ist (Option **Automatisch heilen**). Falls das Virus nicht automatisch geheilt werden kann, können Sie das weitere Vorgehen von der Art des Virenfunds abhängig machen (Option **Den Benutzer fragen**) oder Sie können den Test ohne Unterbrechung beenden (Option **Mit dem Test ohne Unterbrechung fortfahren**). Wenn Sie sich dafür entscheiden den Test nicht zu unterbrechen, stehen ihnen die folgenden Optionen zur Verfügung (**Fenster des laufenden Tests aktivieren, Nur bei der ersten Warnung**), um das Programmverhalten festzulegen und um zu bestimmen, auf welche Art und Weise (wenn überhaupt) Sie über einen Virenfund informiert werden möchten.
  - **Bei Warnungen** – in diesem Abschnitt können Sie auf ähnliche Weise festlegen, wie sich das Programm bei einer Warnmeldung (die im vorangegangenen Abschnitt **Was melden** festgelegt wurden) zu verhalten hat.
- o **Erweiterte Einstellungen**



Dieser Dialog erlaubt das Einstellen der spezifischen Test-Parameter, die das Verhalten der Oberfläche des **Test Center** bestimmen:

- **Automatisches Ausblenden der Dialoge** – geben Sie an, wie lange die Warnmeldung angezeigt werden soll
- **Programm automatisch beenden** – wählen Sie aus, ob das **Test Center** nach Beendigung des Tests geschlossen werden soll, oder ob es nur in dem Fall geschlossen werden soll, wenn der Test mit einem negativen Ergebnis beendet wird
- **Priorität des Tests** – in diesem Abschnitt definieren/bearbeiten Sie die Testpriorität (im Vergleich zu anderen laufenden Programmen) und Sie können ebenfalls die Länge der Pausen während eines Tests festlegen.

Im Allgemeinen gilt: je niedriger die Testpriorität ist und je länger die Pausen zwischen den Tests sind, desto länger dauert der gesamte Test. Gleichzeitig sinkt jedoch die Systemauslastung. Diese Konfiguration empfiehlt sich vor allen Dingen, wenn Sie die Systemauslastung senken müssen, z.B. auf langsamen/ älteren Computern.

## b) Kompletter Test - Start

Die einfachste Art, den **Kompletten Test** zu starten, ist die Betätigung der Schaltfläche **Teste Computer** in der **Basis Oberfläche** des Test Center:



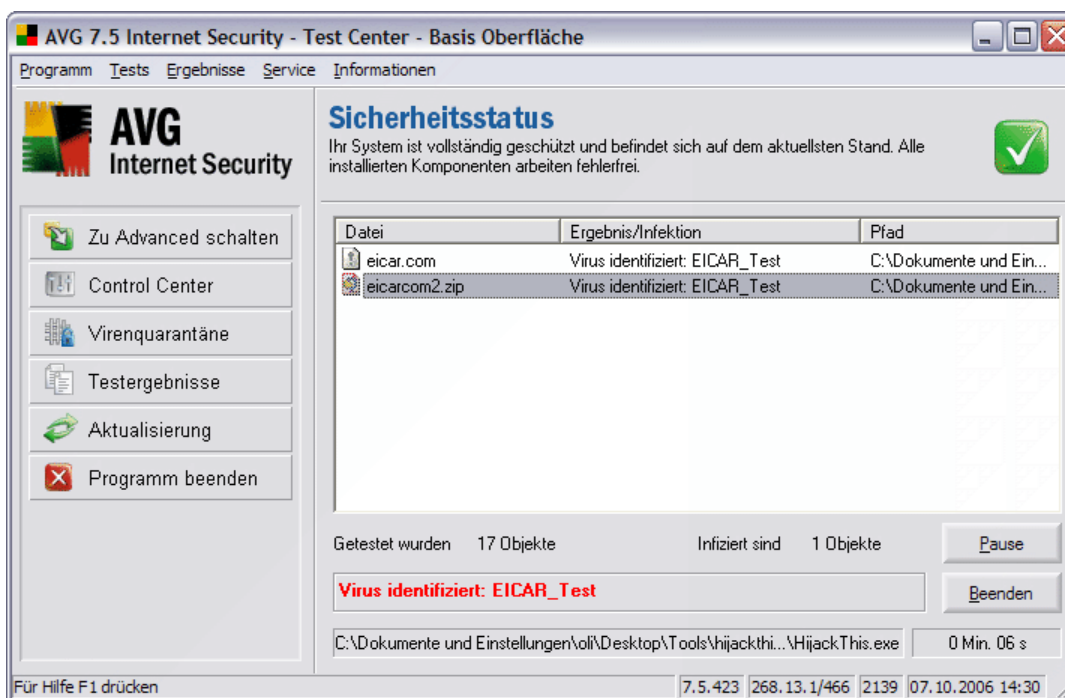
Ebenso können Sie den **Kompletten Test** starten:

- indem Sie in der **Basis Oberfläche** aus dem Hauptmenü: **Tests/Kompletter Test** auswählen
- indem Sie in der **Advanced Oberfläche** aus dem Hauptmenü: **Testmanager/Kompletter Test** wählen
- indem Sie im **Test Center** einfach die F4 Taste drücken

## c) Kompletter Test – Fortschritt

Wenn der **Komplette Test** startet, öffnet sich ein neuer Bildschirm und zeigt den Fortschritt sowie die Ergebnisse an. Falls verdächtige Dateien gefunden werden, sehen Sie diese im zentralen Feld des Bildschirms:

## AVG 7.5 File Server



Im neuen Fenster sehen Sie für jedes mögliche gefundene Virus:

- **Datei** – vollständiger Name der infizierten Datei
- **Ergebnis/Infektion** – Kurzinformation zur verdächtigen Infektion
- **Pfad** – vollständige Pfadangabe der infizierten Datei

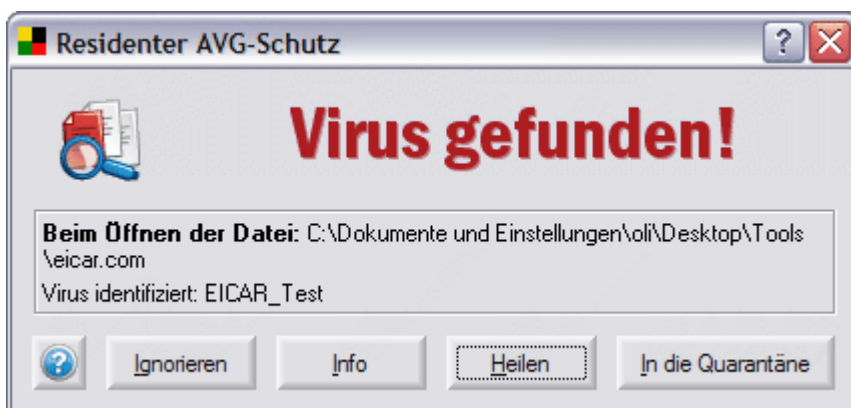
Im unteren Teil des Fensters können Sie kontinuierlich den Testfortschritt beobachten und Informationen finden zu:

- Anzahl der getesteten Objekte
- Anzahl infizierter Objekte
- Anzahl identifizierter Viren
- derzeitig gescannte Datei und Pfad
- Teststatus

Sie können hier ebenfalls den Test **Pausieren/Fortfahren** oder **Beenden**, indem Sie die entsprechende Schaltfläche drücken.

### d) Kompletter Test – Ergebnis

Fall ein Virus während des Tests identifiziert wurde, werden Sie sofort mit der folgenden Meldung benachrichtigt:



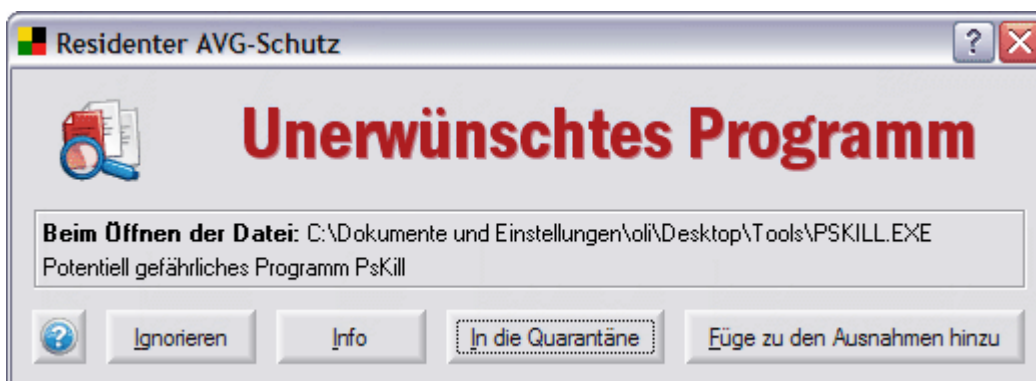
Der Dialog Virus gefunden! informiert Sie über die gefundene infizierte Datei und deren Speicherort. Wählen Sie die Option **Dialog nicht mehr anzeigen (teste Dateien ohne Unterbrechung)**, wenn Sie keine weiteren Meldungen über Testergebnisse erhalten möchten, bevor der Test beendet wurde.

Der Dialog Virus gefunden! enthält die folgenden Schaltflächen:

- **Ignorieren** – drücken Sie diese Schaltfläche, um die Meldung zu ignorieren und um mit dem Test fortzufahren
- **Info** – öffnet die online Virenenzyklopädie, in der Sie Informationen über den Virus finden können
- **Heilen** - ermöglicht Ihnen, das infizierte Objekt zu heilen, wenn für diese Art der Infektion eine Heilmethode verfügbar ist.
- **In die Quarantäne** – verschiebt die Datei in die [Virenquarantäne](#)
- **Unterbrechen** – unterbricht den aktuellen Test

AVG kann ausführbare Anwendungen und DLL-Bibliotheken erkennen und analysieren, die innerhalb des Systems potentiell unerwünscht sind. Allgemein sind diese bekannt unter dem Namen Potentiell unerwünschte Programme (PUP) (z.B. Spyware, Adware).

Wenn ein potentiell unerwünschtes Programm während eines Tests erkannt wird, werden Sie hierüber durch den folgenden Dialog informiert:



Dieser Dialog informiert Sie über den Speicherort des erkannten Potentiell unerwünschten Programms. Wählen Sie die Option **Diesen Dialog nicht wieder anzeigen (Dateien ohne Unterbrechung scannen)** zum Festlegen,

dass Sie vor Beendigung des Tests über Testergebnisse nicht informiert werden möchten.

Der Dialog bietet verschiedenen Schaltflächen, die Sie für die weitere Behandlung von einer verdächtigen Datei nutzen können:

- **Ignorieren** – ignoriert die Warnung des Residenten Schutzes und ermöglicht Ihnen, weiter zu arbeiten (und bietet auch keinen Zugriff auf die Bedrohung).
- **Info** – öffnet die Online-Virenzyklopädie, in der Sie nach detaillierten Informationen bezüglich der erkannten Bedrohung suchen können.
- **In die Quarantäne** – verschiebt das potentiell unerwünschte Objekt in die **Virenquarantäne** (und entfernt es von seinem aktuellen Speicherort)
- **Füge zu den Ausnahmen hinzu** – ermöglicht Ihnen, das **Potentiell unerwünschte Programm** im System beizubehalten und definiert es als [Potentiell unerwünschte Programm-Ausnahme](#). Ein Bestätigungsdialog wird angezeigt.
- **Unterbrechen** – unterbricht den aktuell laufenden Test.

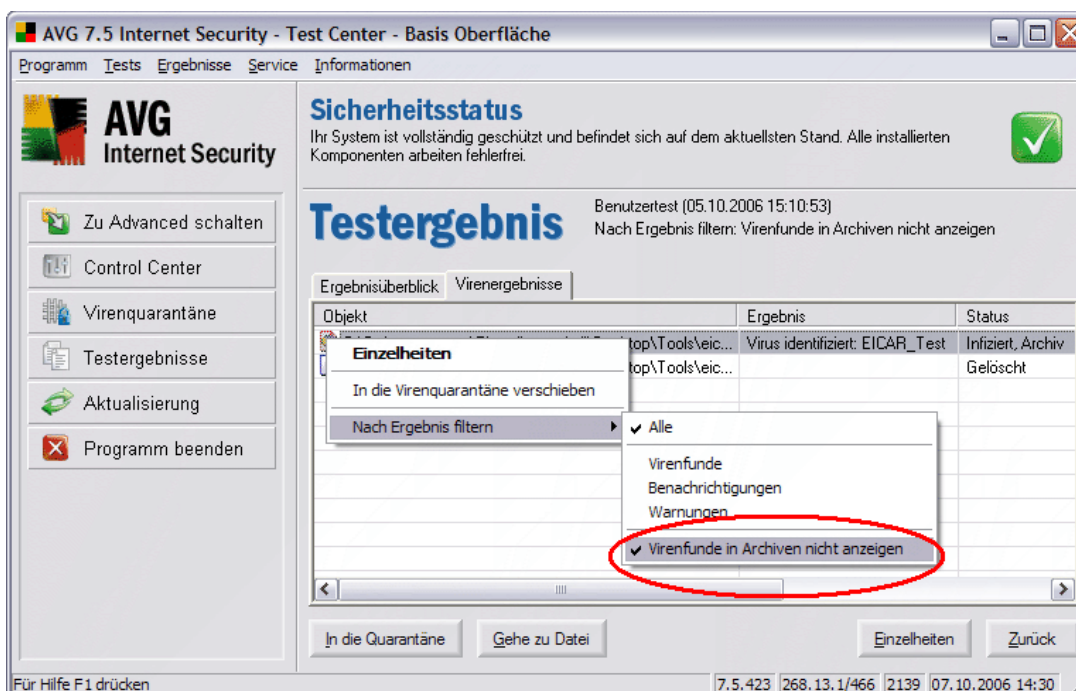
Der Test kann auch den Inhalt archivierter Dateien überprüfen. Wenn ein verdächtiges Objekt innerhalb eines überprüften Archivs erkannt wird, werden Sie hierüber mit dem gleichen Dialogfenster benachrichtigt, das bei normalen Virenfunden angezeigt wird. Der Dialog bezieht sich auf das gesamte Archiv und nicht nur auf eine einzelne infizierte Datei innerhalb dieses Archivs. Das bedeutet, dass Sie nur über den Namen des verdächtigen Archivs und des entsprechenden Speicherorts informiert werden.

Die Schaltfläche **In die Quarantäne** verschiebt das gesamte Archiv in die **Virenquarantäne**.

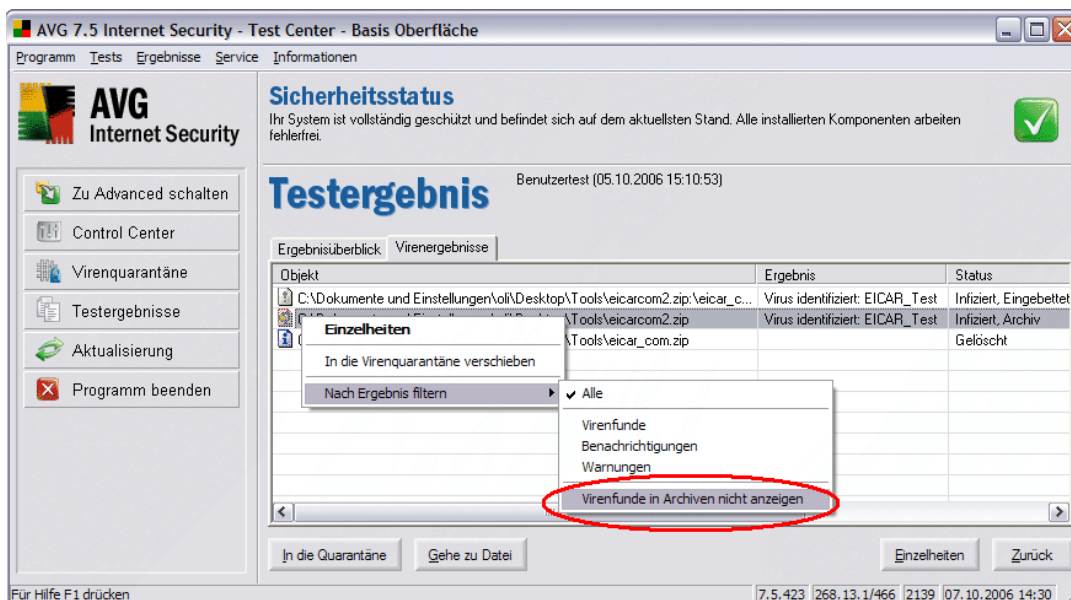
Die Übersicht **Testergebnis** kann Ihnen jedoch detaillierte Informationen zu infizierten Dateien innerhalb eines Archivs anzeigen. Hierfür gehen Sie auf den Reiter **Virenergebnisse** oder **Spyware gefunden** (dieser wird nur angezeigt, wenn auch Spyware/Malware erkannt wurde).

Im folgenden Screenshot werden nur die infizierten Archive mit dem infizierten Inhalt in der Übersicht des Testergebnisses angezeigt:

# AVG 7.5 File Server



Klicken Sie mit der rechten Maustaste auf das Gitter im Dialog **Testergebnis**, um das Kontextmenü zu öffnen: entfernen Sie die Markierung im Kontextmenü bei der Option **Virenfunde in Archiven nicht anzeigen**, um alle enthaltenen Dateien in dem infizierten Archiv zu sehen (in der Übersicht werden Archive/eingebettete Objekte zusätzlich durch unterschiedliche grafische Symbole unterschieden):



Neben den Informationen über den Testtyp und den Startzeitpunkt finden Sie in der oberen rechten Ecke dieses Dialogs die Informationen über den verwendeten Test.

e) **Kompletter Test – Statistik**

Nachdem der Test beendet ist, werden Sie über das Testergebnis durch den Dialog **Teststatistik** informiert, der umfassende Informationen über den Testfortschritt und das Ergebnis enthält:

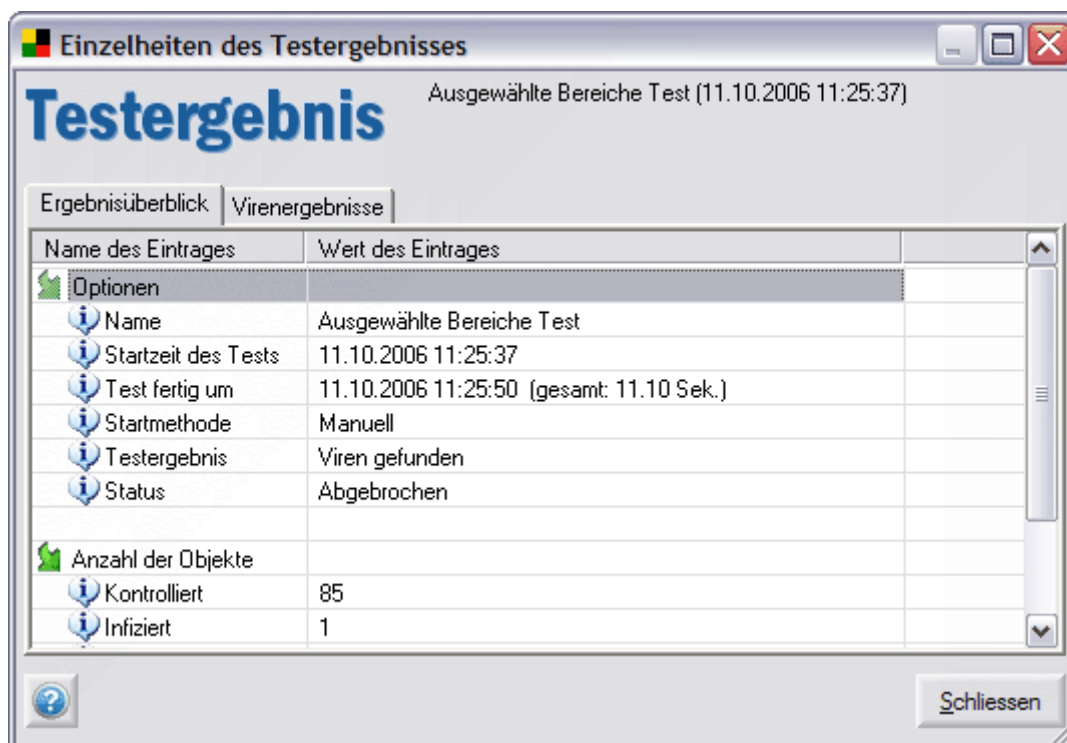


Wann immer eine Infektion erkannt wurde, versucht AVG diese automatisch zu heilen. Sollte es beim Heilen Probleme mit der infizierten Datei geben, werden Sie um weitere Angaben gebeten. Manchmal müssen Sie jedoch infizierte Dateien auch manuell bearbeiten. Der Lösungsvorschlag hierbei ist, die infizierten Dateien in die **Virenquarantäne** zu verschieben, um sie dort mit dem geringsten Risiko, andere, nicht befallene Bereiche Ihres Computers zu infizieren, weiter zu bearbeiten.

Für weiterführende Informationen zur Virenquarantäne lesen Sie bitte Kapitel [12. Virenquarantäne](#)

Einen detaillierten Überblick über die Ergebnisse des **Kompletten Tests** erhalten Sie im Dialogfenster **Testbericht – Mehr Details**. Zum Öffnen dieses Dialogs:

- Klicken Sie auf die Schaltfläche **Ergebnis anzeigen** im Fenster **Virus gefunden**
- Wählen Sie in der **Basis/Advanced Test Oberfläche** die Option **Testergebnis** aus dem linken Menü und wählen Sie den entsprechenden Test im Hauptfenster aus; drücken Sie dann die Schaltfläche **Details**



## 12.2. Benutzertest

Der **Benutzertest** erlaubt Ihnen, die Standardeinstellungen der vordefinierten Tests zu verwenden und anschließend die Parameter entsprechend Ihren Wünschen zu verändern. Die Konfiguration der Testoberfläche, der Teststart und Fortschritt und die Anzeige der Testergebnisse entsprechen denen des **Kompletten Tests**.

Um die Einstellungen für den **Benutzertest** zu bearbeiten müssen Sie folgendermaßen vorgehen:

- In der **Basis-Oberfläche** wählen Sie aus dem Hauptmenü **Tests/Einstellungen des Benutzertests**
- In der **Advanced Oberfläche** wählen Sie aus dem Hauptmenü **Tests/Testmanager/Benutzertest** und drücken die Schaltfläche **Bearbeiten**
- Im **Test Center** verwenden Sie die Tastenkombination **Strg + F5**  
Für weitere Optionen zu den Einstellungen von Benutzertests lesen Sie bitte den Abschnitt [Einstellungen des Kompletten Tests](#)

Um den **Benutzertest** zu starten können Sie:

- In der **Basis Oberfläche** wählen Sie aus dem Hauptmenü **Tests/Benutzertest starten**
- In der **Advanced Oberfläche** wählen Sie aus dem Hauptmenü **Tests/Testmanager/Benutzertest** und drücken die Schaltfläche **Starten**
- Im **Test Center** Arbeitsumgebung benutzen Sie die Taste **F5**

Für eine detaillierte Beschreibung der Dialoge lesen Sie bitte das Kapitel [13.1 Benutzertest](#)

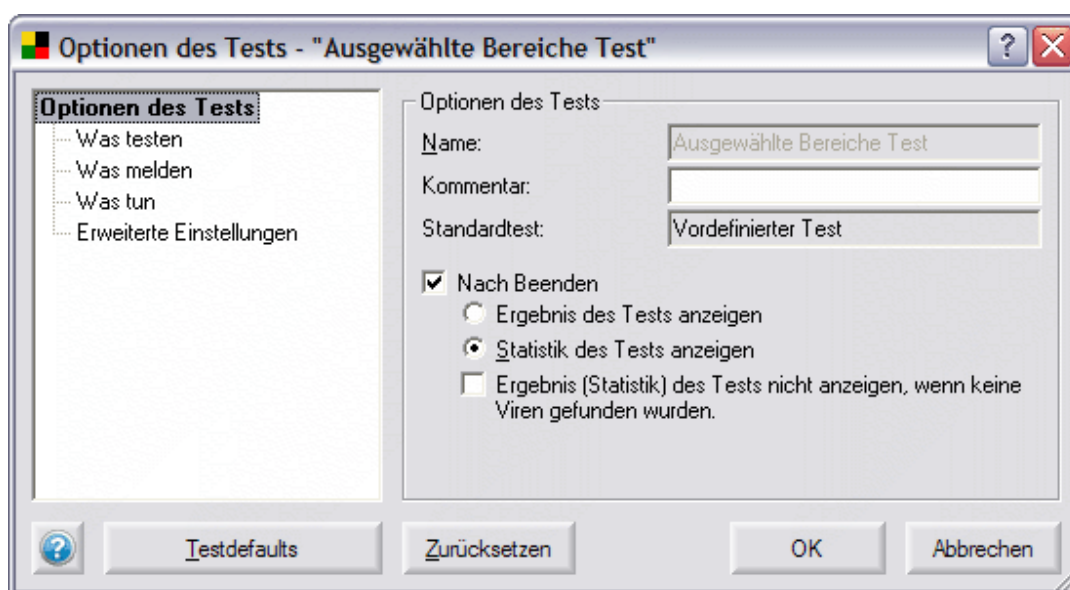
### 12.3. Ausgewählte Bereiche Test

**Ausgewählte Bereiche Test** überprüft nur die Computerbereiche, die Sie vorher als zu überprüfende definiert haben (ausgewählte Verzeichnisse, Festplatten, Diskettenlaufwerke, CDs usw.) Der weitere Testfortschritt im Falle eines Virenfunds und dessen Behandlung ist derselbe wie beim **Kompletten Test**.

#### a) Ausgewählte Bereiche Test– Konfiguration und Start

Der Konfigurationsdialog des **Ausgewählte Bereiche Test** kann folgendermaßen geöffnet werden:

- In der **Basis Oberfläche** wählen Sie den Schnellstartlink **Teste Ausgewählte Bereiche**
- In der **Advanced Oberfläche** wählen Sie die Option **Testmanager/Ausgewählte BereicheTest** im linken Menü



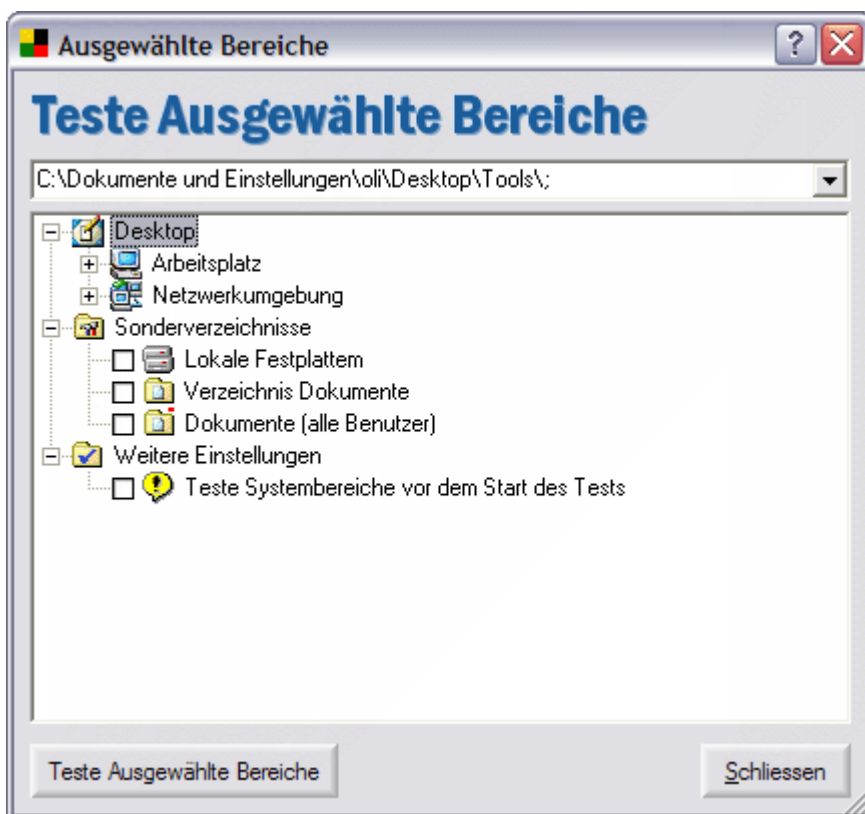
Im linken Abschnitt des neu geöffneten Dialogs können Sie aus verschiedenen Testkonfigurationen auswählen – die Testkonfiguration selbst ähnelt der Konfiguration des **Kompletten Tests**, siehe Kapitel [11.1 a\)– Kompletter Test - Einstellungen](#).

#### b) Ausgewählte Bereiche Test – Start und Fortschritt

**Der Ausgewählte Bereiche Test** kann folgendermaßen gestartet werden:

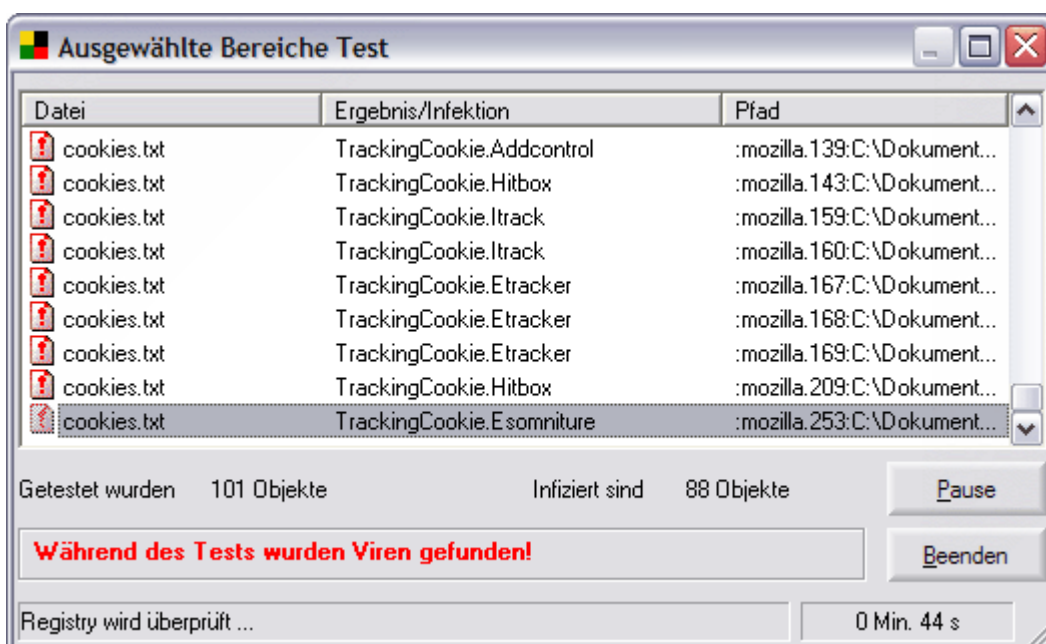
- In der **Basis Oberfläche** wählen Sie den Schnellstartlink **Ausgewählte Bereiche Test**
- In der **Advanced Oberfläche** wählen Sie die Option **Testmanager/Ausgewählte Bereiche Test/Teste ausgewählte Bereiche** im linken Menü

Diese Auswahl öffnet ein neues Dialogfenster **Ausgewählte Bereiche** mit einem Navigationsbaum, der Ihre Festplatte und die Netzwerkumgebung anzeigt; innerhalb dieses Baumes können Sie die Orte angeben, die überprüft werden sollen:



Sobald die Orte, die überprüft werden sollen, definiert sind, kann die Schaltfläche **Teste Ausgewählte Bereiche** aktiviert werden und Sie können diese dann zur Bestätigung der Auswahl und zum Starten des Tests drücken.

Der Testfortschritt kann im Dialogfenster **Ausgewählte Bereiche Test** überwacht werden:



In dem neuen Fenster können Sie alle gefundenen Viren sehen:

- **Datei** – Name der infizierten Datei
- **Ergebnis/Infektion** – kurze Information über die mögliche Infektion
- **Pfad** – Ort der infizierten Datei

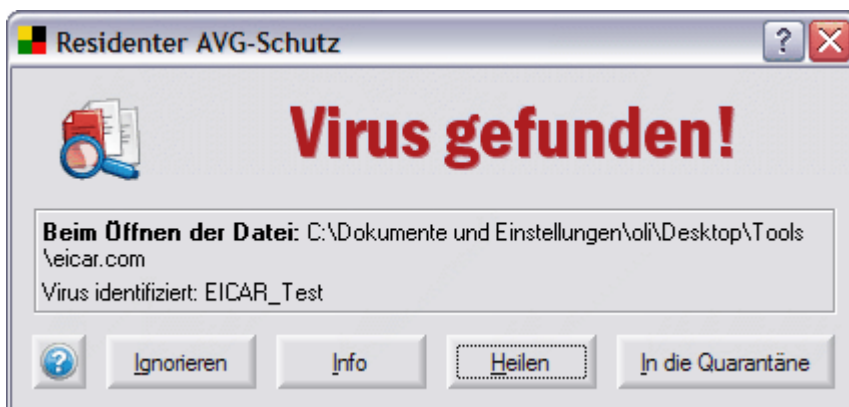
Im unteren Teil des Fensters können Sie kontinuierlich den Testfortschritt beobachten und Informationen finden zu:

- Anzahl der getesteten Objekte
- Anzahl infizierter Objekte
- Anzahl identifizierter Viren
- derzeitig gescannte Datei und Pfad
- Teststatus

Sie können hier ebenfalls den Test **Pausieren/Fortfahren** oder **Beenden**, indem Sie die entsprechende Schaltfläche drücken.

#### c) Ausgewählte Bereiche Test – Ergebnisse

Falls ein Virus während des Tests identifiziert wurde, werden Sie sofort mit der folgenden Meldung benachrichtigt. *Für eine detaillierte Beschreibung der Warnmeldungen lesen Sie bitte das Kapitel [13.1 d\) – Kompletter Test – Ergebnisse](#):*



#### d) Ausgewählte Bereiche Test – Statistiken

Nachdem der Test beendet ist, werden Sie über das Testergebnis durch den Dialog **Teststatistik** informiert, der umfassende Informationen über den Testfortschritt und das Ergebnis enthält:



Detaillierte Informationen zu den Testergebnissen können auch im Dialog **Testergebnis Details** gefunden werden, den Sie folgendermaßen erreichen:

- In der **Basis Oberfläche** wählen Sie die Schaltfläche **Testergebnis/entsprechender Test/Details**
- In der **Advanced Oberfläche** über die Option **Testergebnis/entsprechender Test**

#### 12.4. Ausführliche Tests

AVG bietet Ihnen ausführliche Alternativen zum **Kompletter Test/Benutzertest**. Diese Tests finden Sie nur in der **Advanced Oberfläche**. Die detaillierte Version eines jeden Tests führt den Test vergleichbar mit den Standard-Testeinstellungen durch, aber während jeder Standardtest nur mögliche infizierbare Dateien testet, überprüft der ausführliche Test alle Dateien.

#### 12.5. AVG eMail-Kontrolle

**EMS** steht für den **eMail Scanner** und ist die AVG-Komponente für die Überprüfung von eingehenden/ausgehenden eMails. Der **AVG eMail Scanner** kann über das **Control Center** kontrolliert werden – siehe auch **eMail-Kontrolle**.

Der **EMS** ist eine alternative Lösung für die Überprüfung von eMails in eMail Clients, die nicht direkt durch AVG Plugins unterstützt werden (in Form eines Programm Plugins).

**EMS** arbeitet als Filter zwischen dem von Ihnen verwendeten eMail-Programm (z.B. Outlook Express, Incredimail, Netscape usw.) und Ihrem Internet/eMail- Provider.

AVG sammelt sowohl eingehende als auch ausgehende Nachrichten, speichert diese dann in einem temporären Verzeichnis für die Virenüberprüfung und sendet oder empfängt anschließend die Nachrichten.

Verwendung des AVG eMail Scanners

Sie müssen den Namen und die Versionsnummer Ihres eMail Programms kennen, um entscheiden zu können, ob Sie den **eMail Scanner** installieren können oder nicht. Wenn Sie nicht sicher sind, welches eMail Programm Sie verwenden, starten Sie bitte Ihr eMail Programm und finden Sie die **Programm-Informationen** im Menü (oder einen entsprechenden Menüeintrag).

- a) **Sie müssen den AVG EMS nicht installieren**, wenn Sie eines der folgenden eMail-Programme verwenden:
- MS Outlook – Microsoft Outlook 97/98/2000/2003 (Bestandteil der Microsoft Office Installation)
  - MS Exchange Client 4.0 und höher
  - The BAT! 1.61 und höher
  - Qualcomm Eudora (32 Bit)

In diesem Fall schützt Sie AVG mit einem passenden Plugin für Ihr eMail Programm, das direkt bei der AVG-Installation integriert wird.

- b) **Sie müssen den AVG eMail Scanner installieren**, wenn Sie eines der folgenden eMail Programme verwenden:
- MS Outlook Express 4.0 und höher
  - Netscape Mail
  - Incredimail
  - Jedes andere eMail- Programm

In diesem Fall benötigen Sie den **eMail Scanner** für die Überwachung Ihrer eMails. Standardmäßig wird der **eMail Scanner** im automatischen Modus installiert. Wir empfehlen, diese Standardwerte beizubehalten, solange Sie keinen aktuellen Grund dafür haben, diese zu ändern.

Sie können die Konfiguration des **eMail Scanner** natürlich auch manuell Ihren Wünschen entsprechend anpassen.

### 12.6. Start eines Test von der Kommandozeile

Falls Sie den Test von der Kommandozeile aus starten müssen, nehmen Sie hierfür die Datei AVGSCAN.EXE, die sich in dem Verzeichnis befindet, in dem AVG installiert ist. Der Befehl sollte folgendermaßen aussehen:

**AVGSCAN.EXE C: /parameter**

Wenn Sie eine spezielle Datei/Verzeichnis testen möchten, bietet das o.g. Beispiel den Pfad zu dieser Datei/Verzeichnis anstelle C:

Folgende Parameter können genutzt werden:

## AVG 7.5 File Server

- ERRORLEVEL == 0/\* everything is o.k. \*/
- ERRORLEVEL == 1/\* user cancelled/interrupted test\*/
- ERRORLEVEL == 2/\* any error during the test – cannot open file etc.\*/
- ERRORLEVEL == 3/\* change identified\*/
- ERRORLEVEL == 4/\* suspicion detected by heuristic analysis\*/
- ERRORLEVEL == 5/\* virus found by heuristic analysis\*/
- ERRORLEVEL == 6/\* specific virus detected\*/
- ERRORLEVEL == 7/\* active virus in memory detected\*/
- ERRORLEVEL == 8/\* AVG corrupted\*/
- ERRORLEVEL == 9/\* double extension\*/
- ERRORLEVEL == 10/\* archive contains password protected files\*/

## 13. Programm Aktualisierungen

Jedes Virenschutz-System kann nur dann zuverlässigen Schutz gewährleisten, wenn regelmäßig Aktualisierungen durchgeführt werden. AVG stellt einen zuverlässigen und schnellen Aktualisierungsservice mit schnellen Antwortzeiten zur Verfügung. Moderne Viren verbreiten sich sehr schnell und infizieren eine grosse Anzahl Workstations innerhalb kürzester Zeit. Daher ist es unbedingt erforderlich, dass gerade Server so schnell wie möglich aktualisiert werden, damit die Bedrohung gestoppt werden kann, bevor Sie die Computer der Endanwender infizieren kann.

### 13.1. Aktualisierungslevels

AVG bietet drei Aktualisierungslevel zur Auswahl an:

- **Vorrangige Aktualisierung**  
Die vorrangige Aktualisierung enthält alle Neuerungen für zuverlässigen Virenschutz. Diese enthalten normalerweise keine Einzelheiten zum Code und führt nur eine Aktualisierung der Virendefinitionen- Datenbank durch. Diese Aktualisierung sollte durchgeführt werden **sobald sie verfügbar ist**.
- **Empfohlene Aktualisierung**  
Die empfohlene Aktualisierung enthält verschiedene Programmänderungen, Fehlerbehebungen und Verbesserungen.
- **Optionale Aktualisierung**  
Die optionale Aktualisierung spiegelt Änderungen wieder, die nicht unbedingt für die Funktion des Programms notwendig sind – Texte, Aktualisierung von Setup Komponenten usw. Optionale Aktualisierungen können zusammen mit empfohlenen Aktualisierungen heruntergeladen und angewendet werden, sind aber nicht so wichtig.

Wenn Sie eine Aktualisierung planen, können Sie auswählen welcher Aktualisierungslevel heruntergeladen und angewendet werden soll. Höhere Aktualisierungslevels enthalten automatisch auch kritischere Aktualisierungen.

### 13.2. Aktualisierungsarten

Sie können sich zwischen zwei Aktualisierungsarten entscheiden:

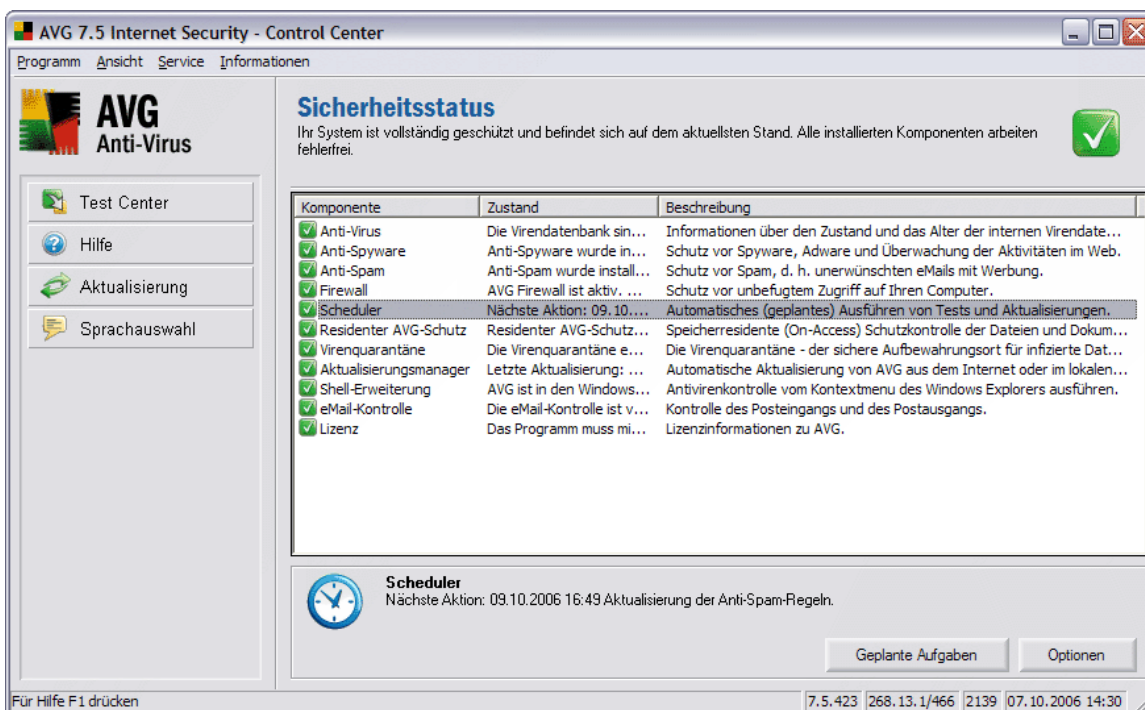
- **On-Demand Aktualisierung**  
Die On-Demand Aktualisierung ist eine sofortige Aktualisierung von AVG, welche jederzeit angewendet werden kann, sobald es notwendig erscheint.
- **Geplante Aktualisierung**  
Innerhalb von AVG ist es möglich, einen Aktualisierungsplan vorzugeben. Die geplante Aktualisierung wird dann periodisch zu den zuvor konfigurierten Terminen ausgeführt. Sobald eine neue Aktualisierungsdatei an angegebener Stelle erscheint, wird diese entweder direkt aus dem Internet oder aus dem Netzwerkverzeichnis heruntergeladen. Wenn keine Aktualisierungen erscheinen, die neuer als die bereits installierten sind, passiert nichts.

### 13.3. Aktualisierungsplan

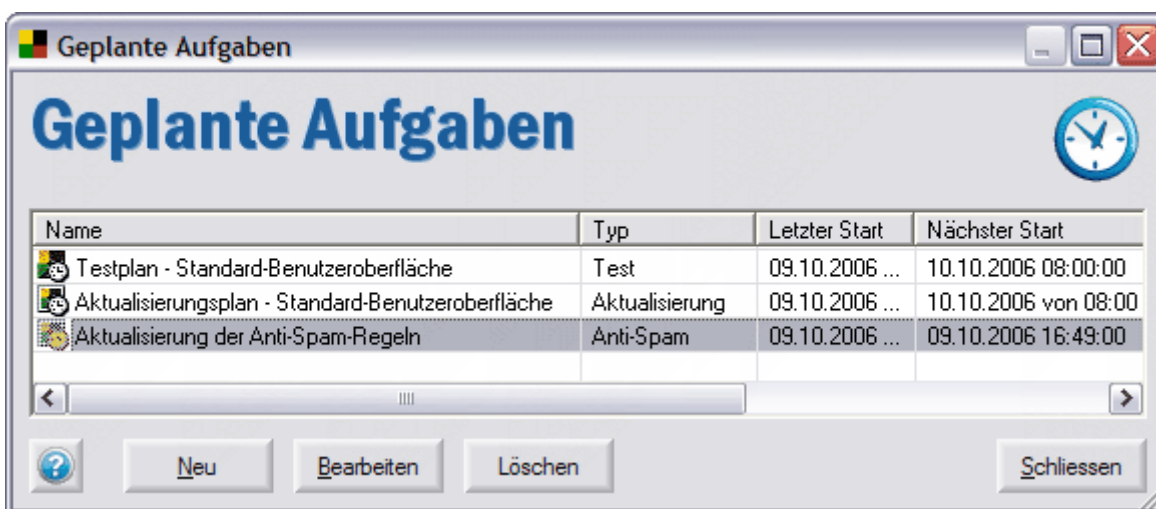
Die Aktualisierungsdateien können direkt aus dem Internet herunter geladen werden. Damit Sie immer die neueste Aktualisierungsversion erhalten, wird vorgeschlagen, einen Aktualisierungsplan anzulegen, der in regelmäßigen Intervallen im Internet nach neuen Aktualisierungen sucht.

**Folgen Sie bitte den folgenden Schritten, um einen Aktualisierungsplan anzulegen:**

Im **Control Center** wählen Sie das **Scheduler** Fenster aus und drücken Sie im unteren Teil des Dialogfensters die Schaltfläche **Geplante Aufgaben**:



Die Schaltfläche öffnet das Dialogfenster **Geplante Aufgaben** mit einer Übersicht über die aktuell geplanten Aufgaben:



Zum Erstellen eines neuen Aktualisierungsplanes drücken Sie bitte die Schaltfläche **Neu** die das Dialogfenster **Aufgabe** mit den folgenden vier Reitern öffnet:

- [Aufgabe](#)
- [Ausführen](#)
- [Verhalten](#)
- [Fehler](#)

a) **Aktualisierungsplan - Konfiguration / Reiter Aufgabe**

Der Reiter **Aufgabe** ermöglicht Ihnen das Einstellen der folgenden Parameter:

- **Name** – der Standardtext dieses Feldes lautet **Aktualisierungsplan** aber Sie können den Namen entsprechend Ihren Wünschen ändern
- **Kommentar** – im **Kommentarfeld** können Sie ihre eigenen zusätzlichen Informationen zur geplanten Aufgabe angeben
- **Aufgabentyp** – in dieser Auswahlbox werden Ihnen die unterschiedlichen Aufgabentypen zur Auswahl angeboten; Sie können sich zwischen **Aktualisierung** und **Test** entscheiden.
- **Option** – in dieser Auswahlbox werden Ihnen vordefiniert Optionen zur Auswahl angeboten.

Für eine Aktualisierung (die unter **Aufgabentyp** eingestellt wurde) können Sie den gewünschten Aktualisierungstyp auswählen:

- **Vorrangige Aktualisierung**
- **Empfohlene Aktualisierung**
- **Optionale Aktualisierung**

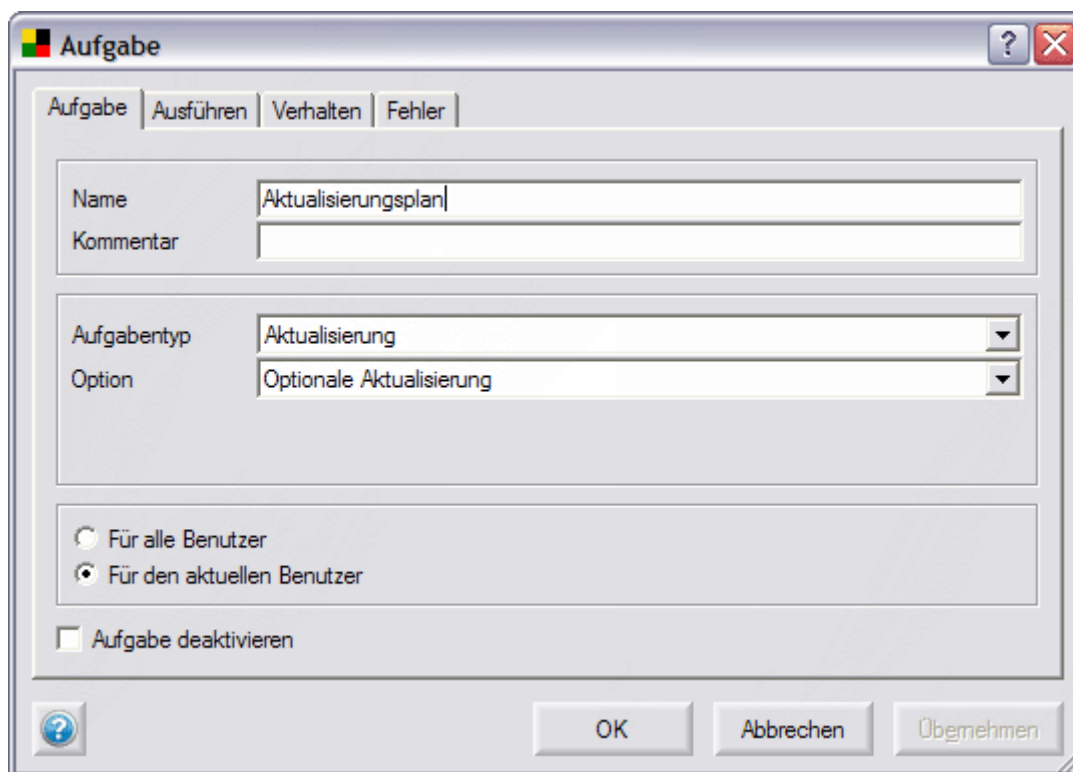
Für eine detaillierte Beschreibung der einzelnen Aktualisierungslevels lesen Sie bitte auch das Kapitel [14.1 Aktualisierungslevels](#)

Für einen Test (der unter **Aufgabentyp** eingestellt wurde) können Sie den gewünschten Testtyp auswählen:

- **Kompletter Test**
- **Benutzertest**
- **Detaillierter Kompletter Test**
- **Detaillierter Benutzertest**

(Für eine detaillierte Beschreibung der einzelnen Tests lesen Sie bitte auch das Kapitel [13. Test Übersicht.](#))

- **Für alle Benutzer /Für den aktuellen Benutzer** – bestimmen Sie, ob die neu erstellte Aufgabe nur für den aktuell angemeldeten Benutzer gültig sein soll oder ob diese Aufgabe für alle Benutzer dieser Station gelten soll.
- **Aufgabe deaktivieren** – Bestätigen Sie diese Option, wenn Sie die Aufgabe temporär deaktivieren möchten.



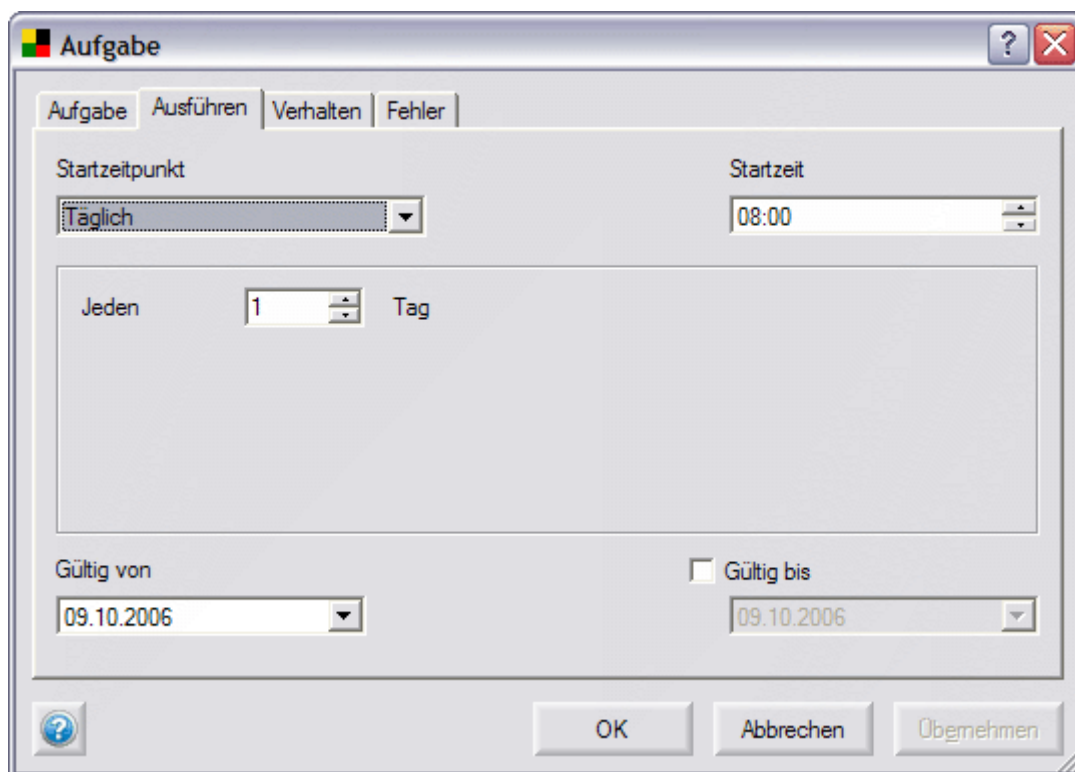
#### b) Aktualisierungsplan Konfiguration / Reiter Ausführen

Der Reiter **Ausführen** erlaubt Ihnen das Einstellen der folgenden Parameter:

- **Startzeitpunkt** – aus der Liste der Optionen im Abschnitt **Startzeitpunkt** können Sie auswählen, ob Sie die Aktualisierung nur einmal ausführen, oder ob sie regelmäßig gestartet werden soll. Geben Sie für diesen Fall bitte das Startintervall an.
- **Startzeit**– wenn Sie gerade eingestellt haben, dass die Aktualisierung nur **einmalig** gestartet werden soll oder wenn Sie ein spezielles Zeitintervall (**täglich, wöchentlich, monatlich**) ausgewählt haben, müssen Sie jetzt noch die reguläre Startzeit oder den speziellen Tag der Woche/des Monats festlegen.

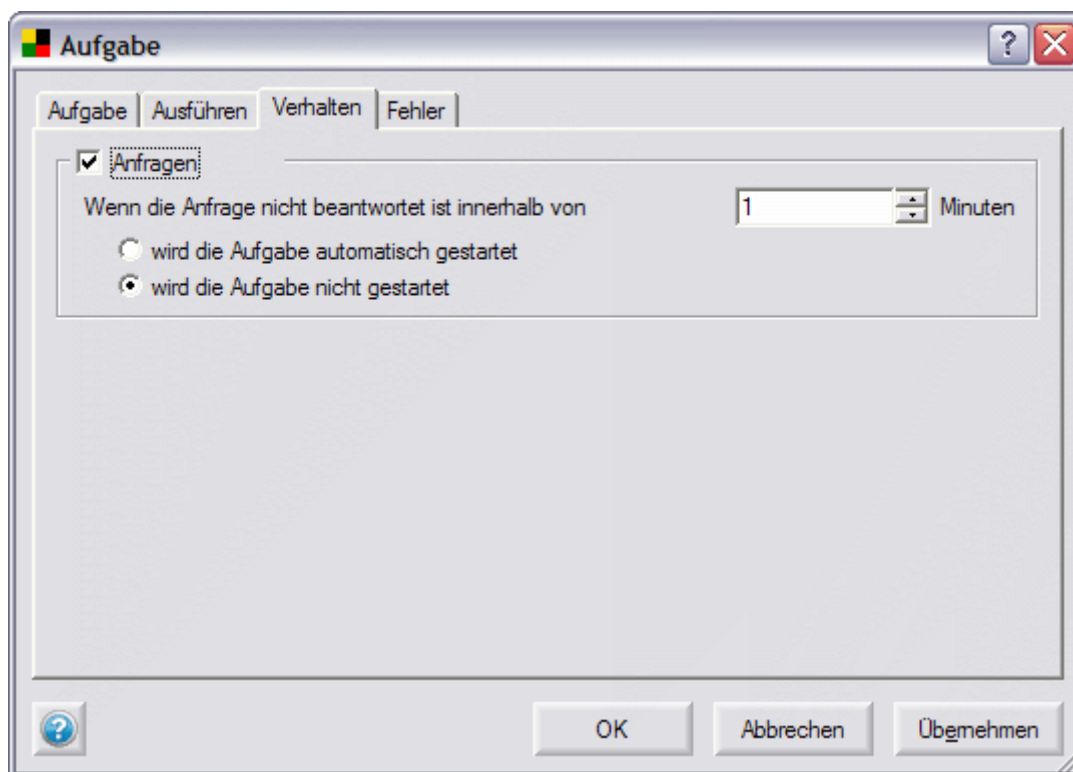
Wenn Sie die Option **Wiederholt (Intervall)** im Abschnitt **Startzeitpunkt** ausgewählt haben, müssen Sie jetzt noch die Intervalldauer in Stunden/Minuten angeben.

- **Gültig von** – geben Sie das Datum an, von dem an die Aufgabe ausgeführt werden soll
- **Gültig bis** – optional können Sie ein Datum angeben, an dem die Aufgabe ihre Gültigkeit verliert



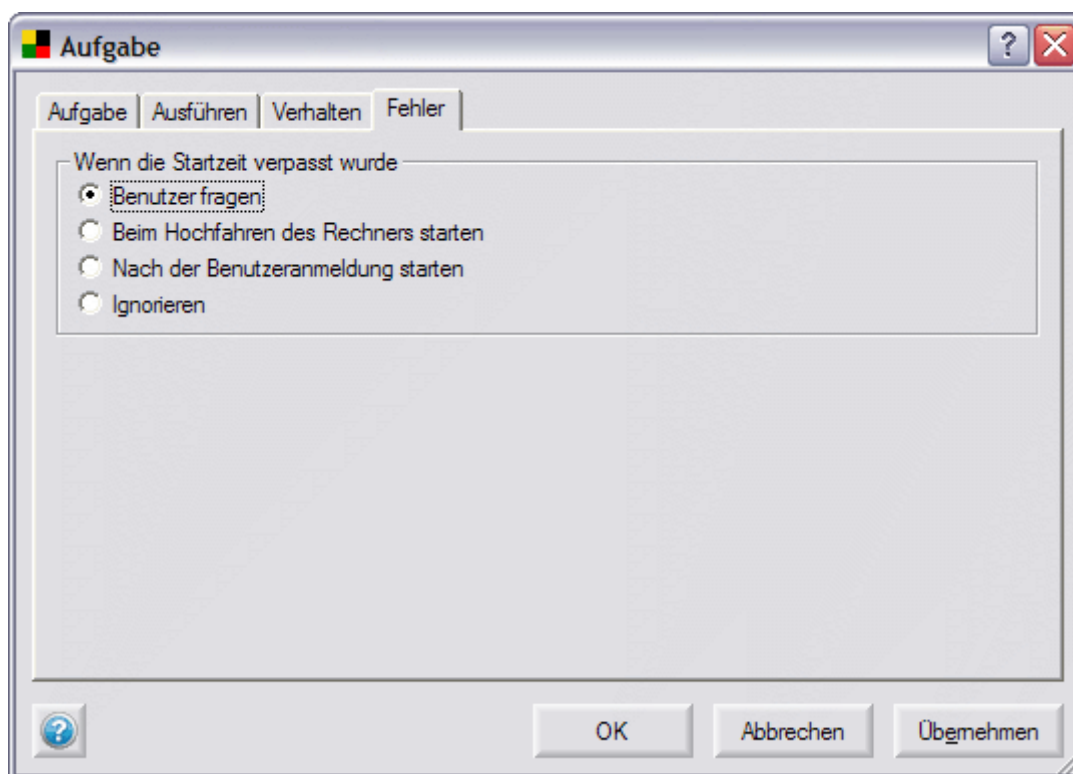
c) **Aktualisierungsplan Konfiguration / Reiter Verhalten**

Im Reiter **Verhalten** können Sie die Option **Anfragen** auswählen, wenn Sie informiert werden möchten, sobald die Aufgabe ausgeführt werden soll und Sie dieses jedes Mal manuell bestätigen möchten. Wenn Sie diese Option auswählen, können Sie weiterhin bestimmen, wie lange das Programm auf eine manuelle Bestätigung zum Start der Aufgabe warten soll und was passieren soll, wenn der Benutzer nicht rechtzeitig während der angegebenen Zeitspanne die Aufgabe bestätigt.



d) **Aktualisierungsplan Konfiguration / Reiter Fehler**

Der Reiter **Fehler** erlaubt Ihnen einzustellen, was geschehen soll, wenn die Aufgabe aus irgendeinem Grund nicht zur korrekten Zeit gestartet werden kann:



## 1. Terminal Services Server Modus

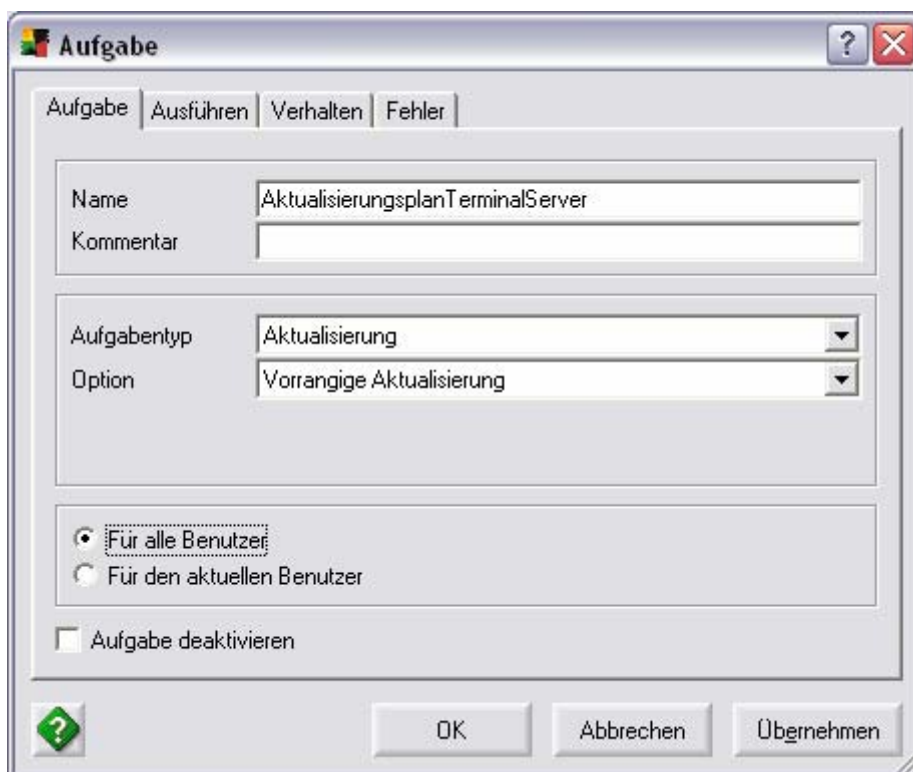
### 1.1 Installations-Hinweise

Falls Sie planen, den Server im Terminal-Server-Modus zu starten (entweder unter Verwendung der Microsoft Windows Terminal Services, Citrix WinFrames, oder einem ähnlichen Produkt), ist es empfehlenswert, dass das AVG Control Center nicht automatisch für jeden Benutzer gestartet wird, um den Verbrauch der Systemressourcen zu minimieren. In solchen Fällen kann die Installation von der Kommandozeile aus (unter Verwendung des Befehls **setup.exe** oder **avgsetup.exe** aus dem AVG Anti-Virus Installationsverzeichnis) mit dem Kommandozeilenparameter **/NO\_CC\_STARTUP** gestartet werden. Sie können diese Option auch während des Installationsprozesses einstellen.

Es ist jedoch empfehlenswert, die **AVG Control Center** Komponente dem Autostartverzeichnis des Administratorkontos (Profils) exklusiv hinzuzufügen, sinnvollerweise mit dem Parameter **/STARTUP**. Das **AVG Control Center** wird daraufhin als minimiertes Systemleisten Icon gestartet.

### 1.2 Geplante Aufgaben

Für AVG für Windows NT4/2000/2003 Installationen auf einem Terminal Server ist es besonders wichtig, alle grundlegenden Tests und Aktualisierungen für alle Benutzer zu planen (Konfigurationsfenster der **Optionen der Geplante Aufgaben** / Reiter **Aufgaben** / Option **für alle Benutzer** planen):



Siehe Abschnitt [9.2 AVG Advanced Oberfläche/Geplante Aufgaben](#) für detaillierte Informationen.)

Diese Einstellung sorgt dafür, dass alle Aufgaben auch ohne angemeldeten Benutzer gestartet werden. Außerdem wird auf diese Weise sichergestellt, dass keine Aufgabe mehrfach in unterschiedlichen Instanzen gestartet wird (z.B. wenn ein Benutzer

mehrere Sessions gleichzeitig verwendet), wodurch die Systemressourcenauslastung durch **AVG Anti-Virus** minimiert wird.

Wir empfehlen, den automatischen Start des **AVG Control Center** für jeden Benutzer zu unterbinden. Stattdessen sollte das AVG Control Center nur beim Start des Administratorkontos gestartet werden, um alle grundlegenden Aufgaben zentral verwalten und so viele Systemressourcen wie möglich einsparen zu können.

Sie sollten die Aktualisierung **für alle Benutzer** planen und nicht **für jeden** Benutzer einzeln einstellen (siehe Kapitel [14.3 Programmaktualisierung /Geplante Aktualisierung](#))! Dieses Vorgehen reduziert die Systemauslastung und sorgt gleichzeitig dafür, dass alle grundlegenden geplanten Aktualisierungen durchgeführt werden, auch wenn kein Benutzer angemeldet ist.

## 14. AVG Alarm Manager

### 14.1. Ereignisse und Aktionen

Jedes Mal, wenn der **Residente AVG-Schutz** ein Virus entdeckt hat, nachdem ein geplanter Test abgeschlossen wurde oder eine Aktualisierung abgeschlossen wurde und bei vielen anderen Gelegenheiten, wird durch AVG ein **Ereignis** angezeigt. Das Ereignis wird von der **AVG Alarm Manager**-Komponente bearbeitet, wobei eine **Aktion** in Abhängigkeit von festgelegten **Regeln** abläuft. Eine Ereignis-Mitteilung kann dem Benutzer angezeigt werden oder dem **AVG DataCenter** zugesandt werden.

Alle **AVG**-Installationshilfsmittel enthalten diese Komponente. Aber Benutzer der Netzwerk-Edition können diese **voreingestellten Regeln zusätzlich verändern** und auch **neue definieren**.

### 14.2. Alarm Manager-Regeln

Die Regeln definieren Beziehungen zwischen Aktionen und den entsprechenden Ereignissen. Jede Regel definiert:

- ein entsprechendes Ereignis.
- die Quellkomponente des Ereignisses. Einige Ereignisse können durch mehr als eine Komponente angezeigt werden, eine Regel kann Einschränkungen für bestimmte Ereignisse beinhalten.
- eine Aktion, die ausgeführt werden muss; durch jede Regel können mehrere Aktionen beschrieben werden (z.B. Event-Log-Eintrag und gleichzeitiges Senden einer Mitteilung an das **AVG DataCenter**).

Nach der **AVG**-Installation sind einige voreingestellte Regeln festgelegt, bei denen die Editiermöglichkeiten von Ereignissen und Quellkomponenten nicht eingeschaltet sind. Aber Sie können Aktionen einfügen, wenn es notwendig erscheint. Für den Fall neuer benutzerdefinierter Regeln ist es möglich, beides zu ändern, sowohl Ereignisse und Quellkomponenten, als auch Aktionen.

Die Voreinstellungen der Regeln sind wie folgt:

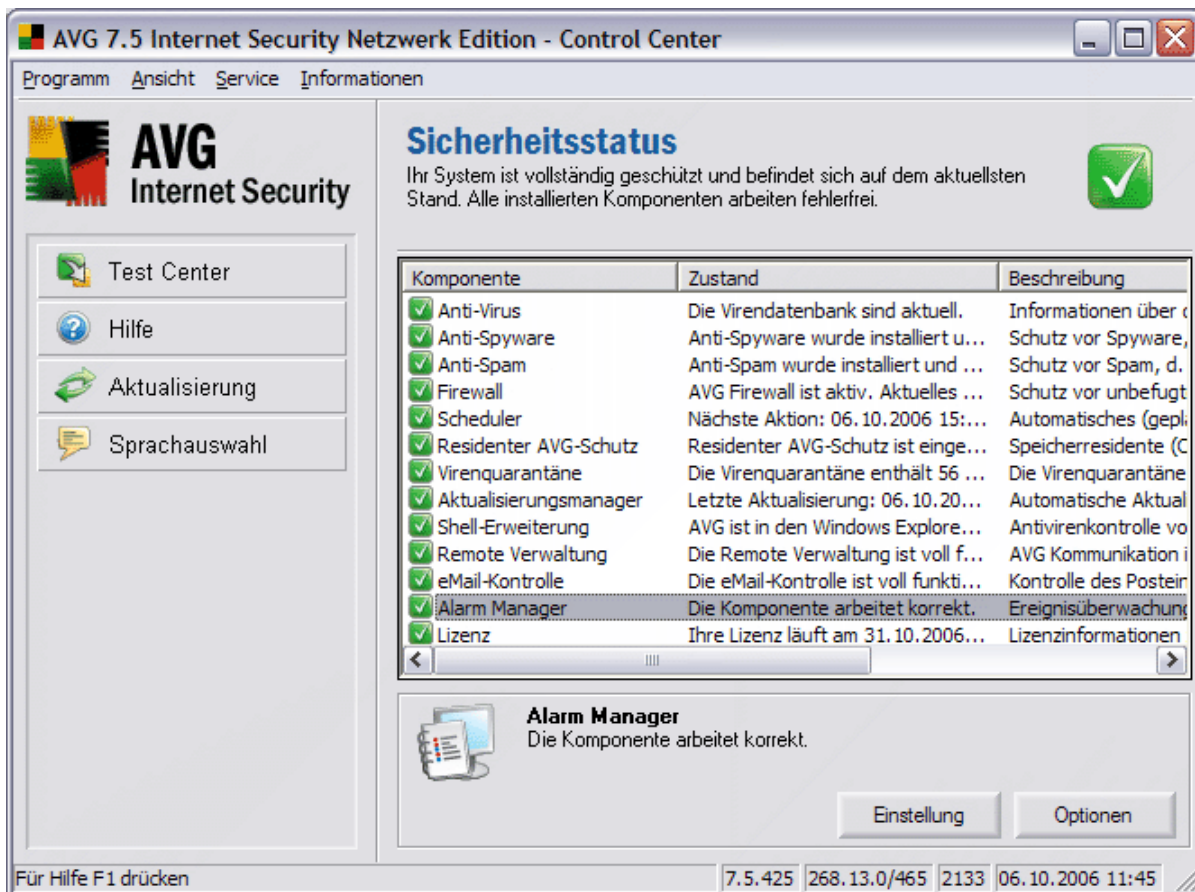
Ereignis	Anmerkung	Aktion
Entdeckung eines Virus durch den Residenten AVG-Schutz	Wenn der Residente AVG-Schutz ein Virus entdeckt	Öffnet ein Dialogfenster mit Informationen zum Virus und der Benutzer muss eine Aktion wählen. Es ist möglich, diesen Dialog automatisch abarbeiten zu lassen (infizierte Datei in Virenquarantäne verschieben usw.)
Dialog zu Aktionen des Residenten AVG-Schutzes	In dem Augenblick, indem ein Benutzer eine Aktion aus dem Dialog des Residenten AVG-Schutzes auswählt (siehe vorige Regel) oder wenn die Aktion automatisch ausgeführt wird	Informationen zum gefundenen Virus und zur ausgewählten Aktion werden an das AVG DataCenter übermittelt. Es ist z. B. möglich, einen Datensatz in das Ereignis-Protokoll zu schreiben
Anzeige des beendeten Tests	Nachdem ein geplanter oder manuell gestarteter Test abgeschlossen wurde	Information der Testergebnisse werden an das AVG DataCenter übermittelt

Neben diesen Standardregeln gibt es noch einige interne Systemregeln, die vor den Benutzern versteckt sind.

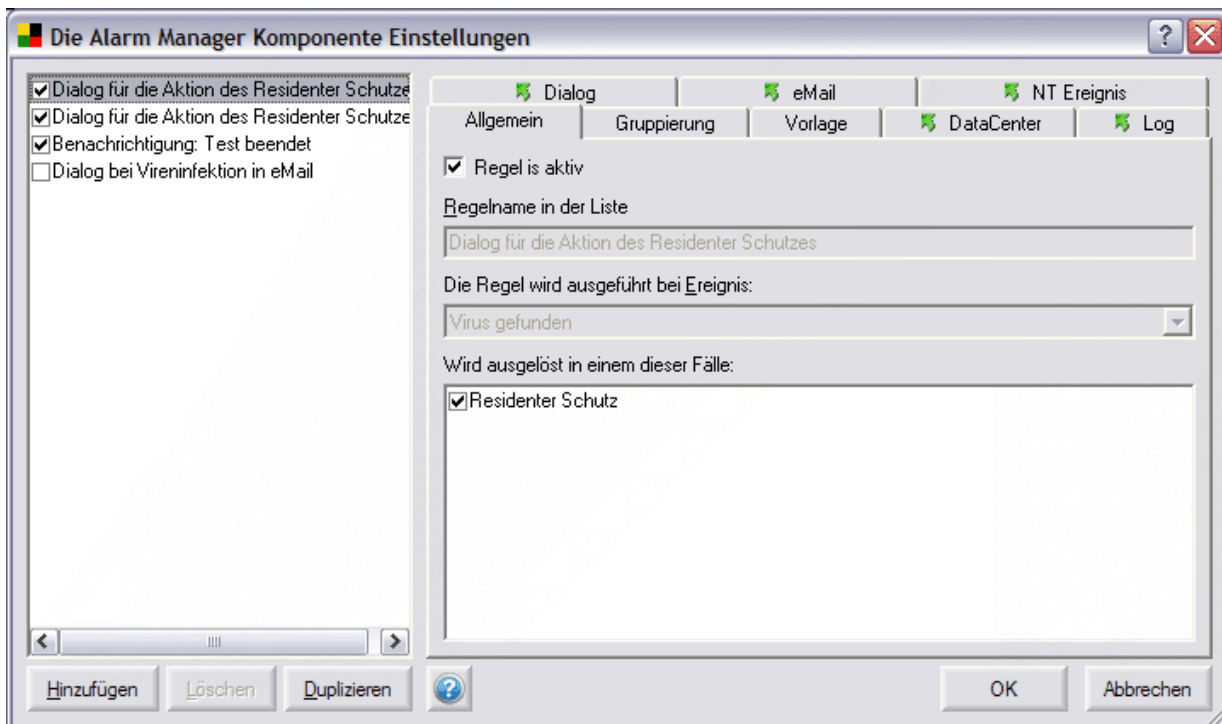
### 14.3. Regelkonfiguration

#### a) AVG Client Regelkonfiguration

Im Abschnitt Clients von **AVG** erreicht man das Konfigurationsfenster für das Ereignismanagement über die **AVG Control Center->Alarm Manager**-Komponente:



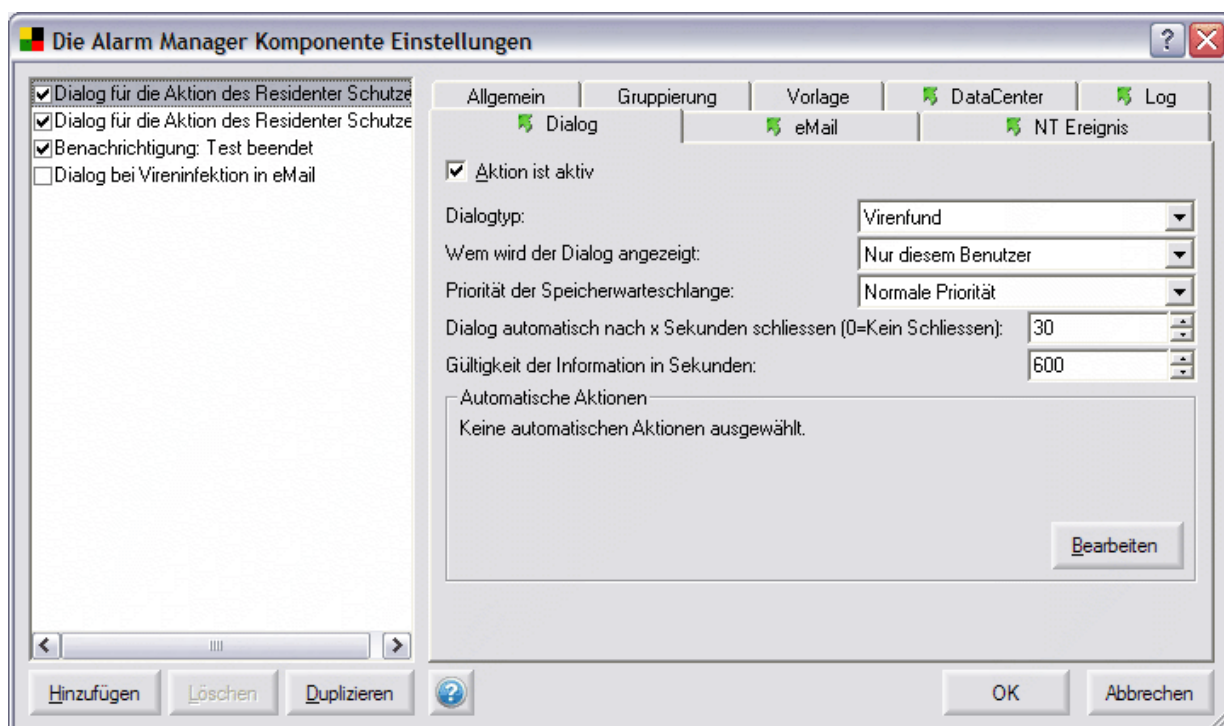
Drücken Sie die Schaltfläche **Einstellungen**, um den Dialog **Alarm Manager Komponenten Einstellungen** zu öffnen:



Auf der linken Seite des Fensters ist eine Liste mit Regeln. Aktive Regeln sind markiert. Auf der rechten Seite können Sie die ausgewählten Regeleinstellungen bearbeiten. Voreingestellte Regeln mit automatischen Einstellungen können nicht verändert werden (weder die Regel noch die Aktion).

Allgemeine Eigenschaften, wie der Name einer Regel oder zusammenfassende Regeln sind für alle Regeln allgemeingültig. Reiter mit Aktionsdefinitionen sind durch grüne Pfeile gekennzeichnet. Für jede Regel kann mehr als eine Aktion definiert werden

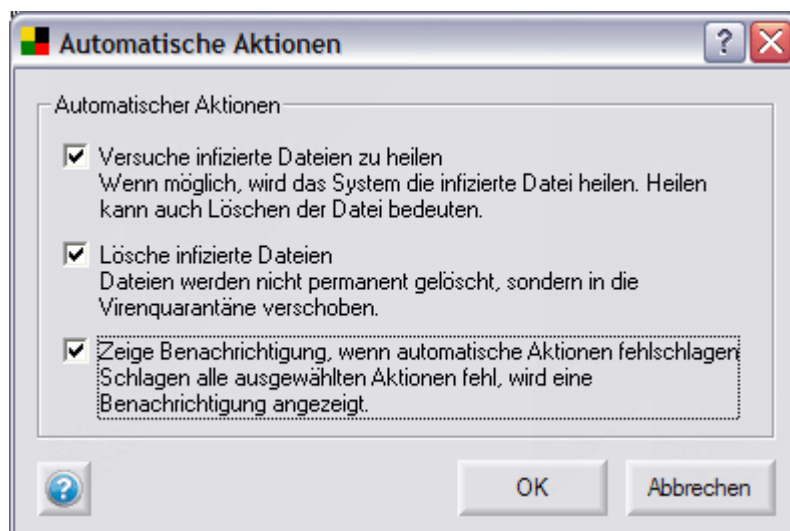
Auf dem Screenshot unten können Sie ein Beispiel einer **Dialoganzeige** für definierte Aktionen der Regel **Dialog für die Aktion des Residenten AVG-Schutzes** sehen. Diese Regel läuft immer ab, wenn der **Residente AVG-Schutz** ein Virus entdeckt.



Auf dem Screenshot ist die Schaltfläche **Bearbeiten** hervorgehoben. Nach Drücken dieser Schaltfläche können Sie automatisch auszuführende Aktionen definieren. Als ein Beispiel sind alle möglichen Aktionen auf dem nächsten Screenshot ausgewählt:

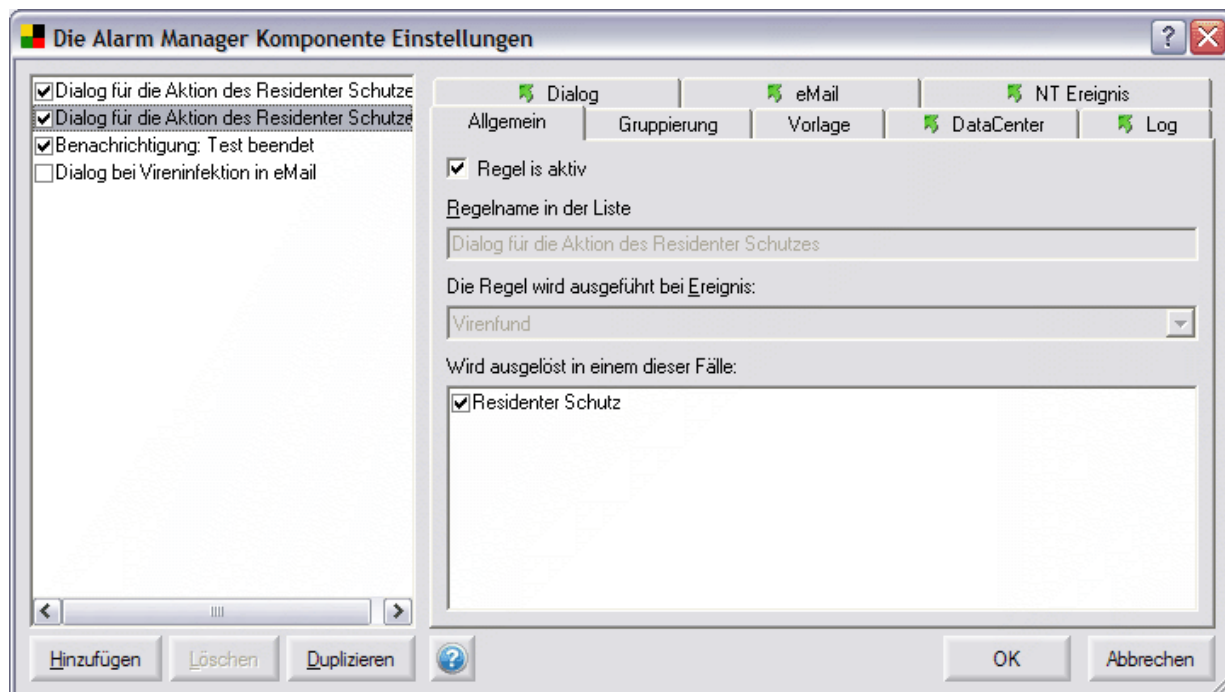
- **Versuche infizierte Dateien zu heilen – AVG** versucht, infizierte Dateien zu heilen (und wiederherzustellen).
- **Lösche infizierte Dateien – AVG** entfernt infizierte Dateien
- **Zeige Benachrichtigung, wenn automatische Aktionen fehlschlagen – AVG** zeigt dem Benutzer in einer Mitteilungsbox an, wenn ein automatischer Heilungsversuch fehlgeschlagen ist

## AVG 7.5 File Server



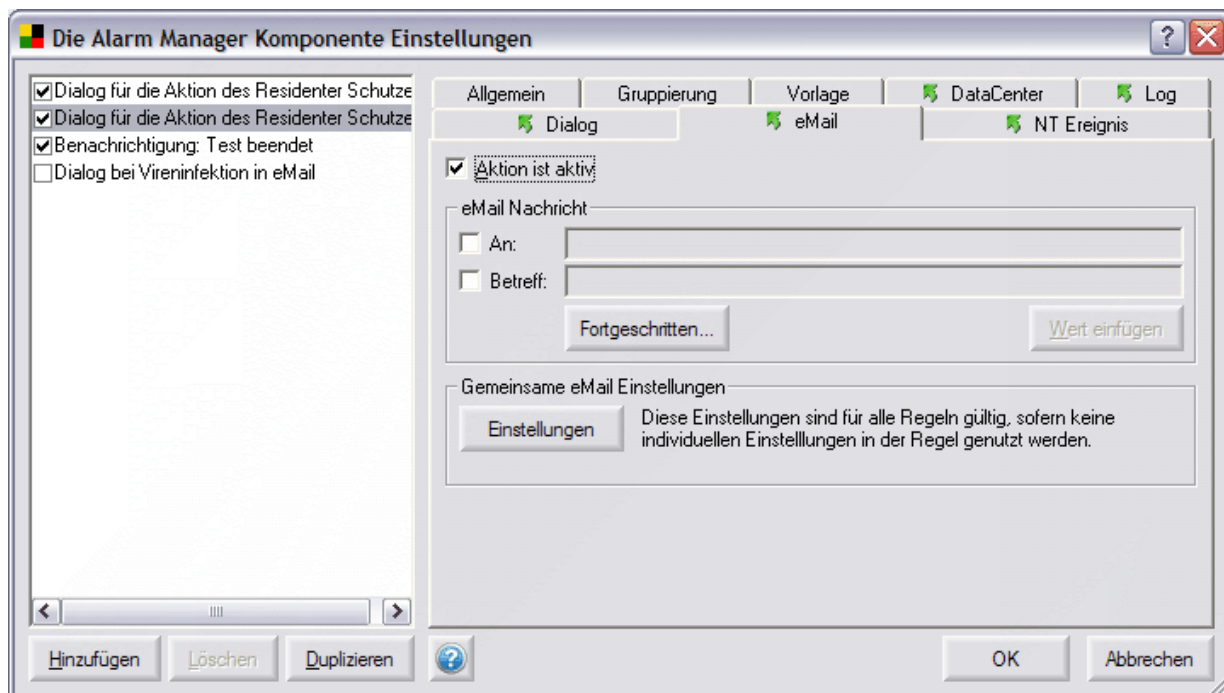
Entsprechend der definierten Aktionen versucht **AVG** zuerst einmal eine infizierte Datei zu heilen. Sollte die Heilung nicht erfolgreich sein, versucht **AVG** die Datei zu löschen: wenn die Datei gelöscht werden soll, wird sie auf jeden Fall in die **AVG Virenquarantäne** verschoben. Wenn das Löschen ebenfalls fehlschlagen sollte, wird **AVG** schließlich eine entsprechende Mitteilung anzeigen.

Nachdem jede der oben genannten automatischen Aktionen durchgeführt wurde, wird ein **Virenfund**-Ereignis erstellt. Dieses Ereignis wird an eine weitere voreingestellte Regel weitergegeben - **Dialog für die Aktionen des Residenten AVG-Schutzes**:



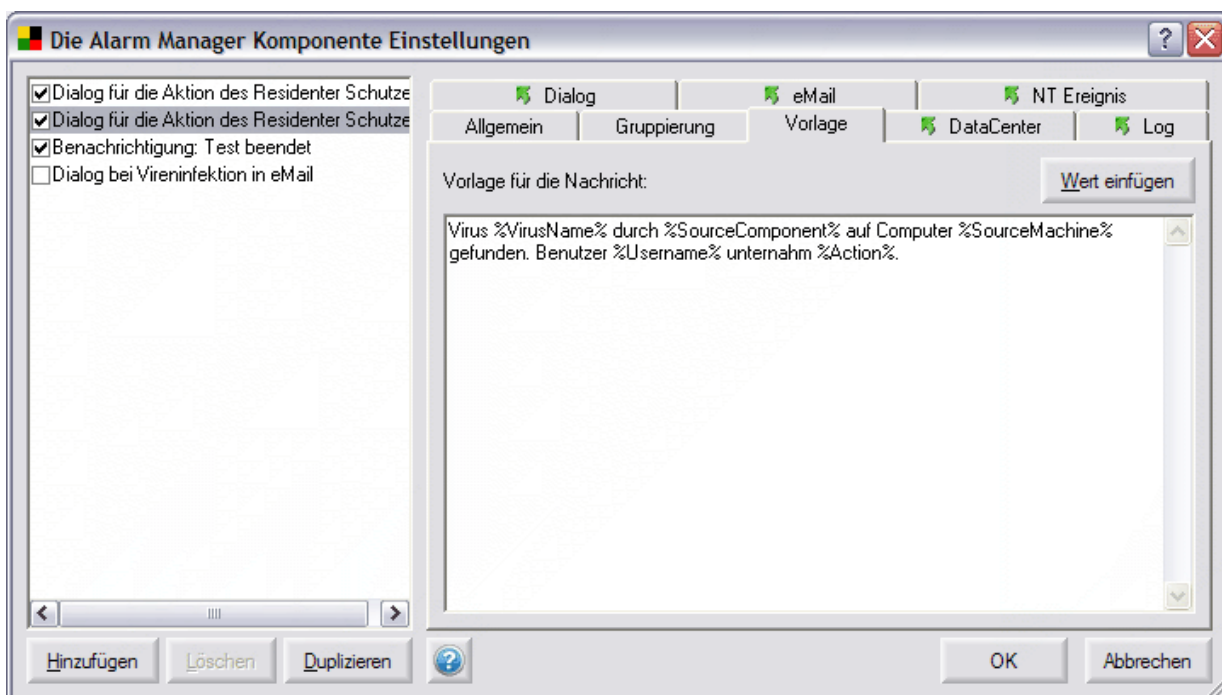
In den voreingestellten Einstellungen dieser Regel ist eine Aktion zum **Senden einer Mitteilung an das AVG DataCenter** definiert.

Für einige bestimmte Ausnahmefälle kann es auch angebracht sein, eine eMail zu senden – diese Option können Sie im Reiter **eMail** näher definieren:



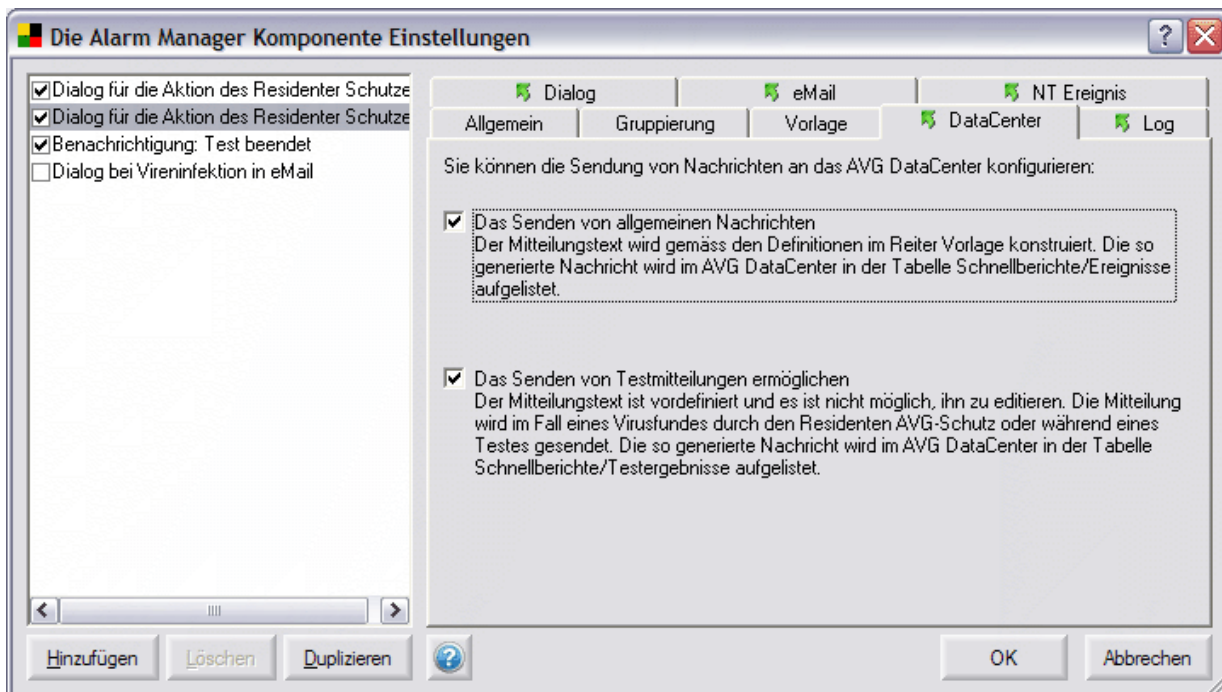
Die Schaltfläche **eMail Einstellungen** öffnet einen neuen Dialog, in dem Sie die allgemein gültigen Mail-Einstellungen bearbeiten können, die auch von allen anderen Regeln gemeinsam genutzt werden (Sendename, Adresse des Mail-Servers usw.).

Der zu verwendende Text für eine ausgelöste Aktion (z. B. eMail-Text) wird auf dem Reiter **Vorlage** vordefiniert. Der Nachrichtentext kann durch spezielle Werte, die mit dem Ereignis verbunden sind, aufgefüllt werden. Diese Werte werden innerhalb der Zeichen **%** für den internen Ablauf angegeben. Um einen neuen Wert hinzuzufügen klicken Sie bitte auf die Schaltfläche **Wert einfügen**:



Standard-Regeln sind Mitteilungen, die bestimmte wichtige Ergebnisse an das **AVG DataCenter** übermitteln. Diese Mitteilungen werden sich immer auf bestimmte Übersichten auswirken. Zum Beispiel wird ein Testergebnis in Abhängigkeit zu den im **AVG DataCenter** festgelegten Bedingungen weiterverarbeitet (z. B. Aktivierung/Deaktivierung der Weitergabe von negativen Testergebnissen). Mit Ausnahme von eben diesen können Sie eine allgemeine Ereignis-Mitteilung an das **AVG DataCenter** senden. Diese Mitteilungen werden in der Ereignisübersicht aufgezeichnet.

Auf dem unten dargestellten Screenshot ist nur das Versenden von allgemeinen Textmitteilungen ermöglicht:

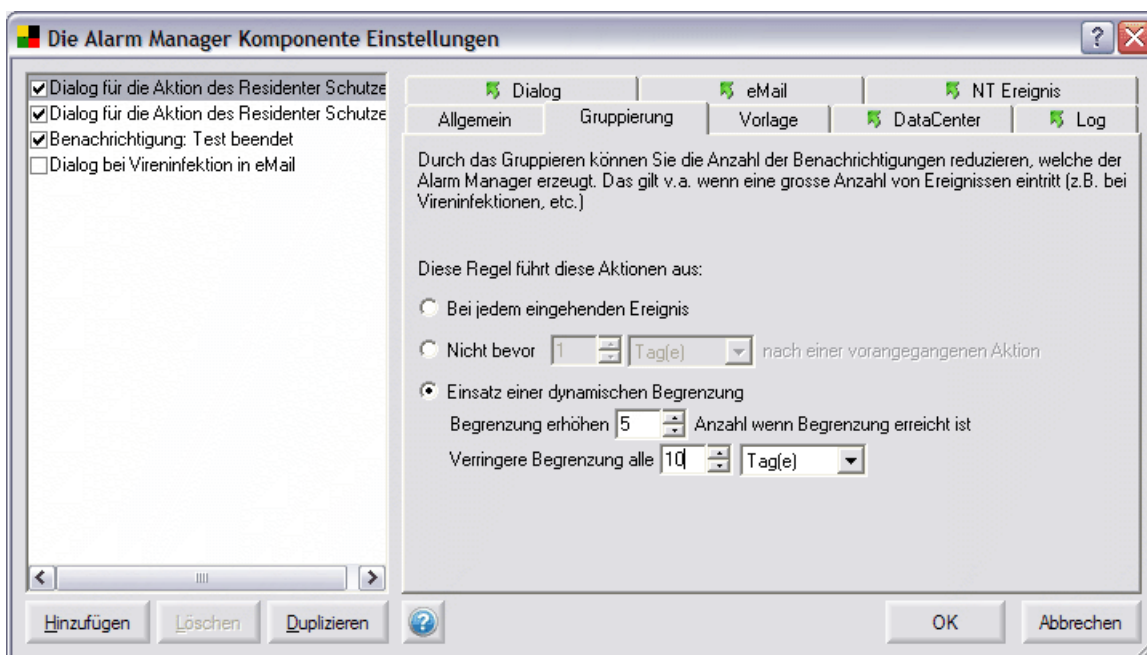


### **Achtung!**

Damit die AVG Internet Security Netzwerk Edition richtig funktioniert, wird empfohlen, die Option **Aktiviere Senden von allgemeinen Textnachrichten** für voreingestellte Regeln nicht abzuschalten! Das Abschalten dieser Aktion macht ist nur in ganz besonderen Ausnahmefällen Sinnvoll. Um eine allgemeine Textbenachrichtigung zu versenden, empfehlen wir die Erstellung einer neuen Regel!

### **b) Gruppierung von Ereignissen**

Bei einem großen massiven Virenbefall kann die Frequenz der Mitteilungen sehr groß werden. Wenn im Falle eines Virenfundes die **eMail-Mitteilungsaktion** ausgelöst wurde, kann die Mailbox sowie der Mailserver des Empfängers sehr schnell überfüllt sein. Um eine derartige Flut von Ereignismitteilungen zu verhindern, können Sie für jede Regel Bedingungen für die Gruppierung von Ereignissen definieren.



- **Bei jedem eingehenden Ereignis** – Standardmäßig wird bei jedem Ereignis eine Aktion ausgelöst.
- **Nicht bevor ... nach einer vorangegangenen** - Es ist jedoch möglich, das Auslösen der nächsten Aktion durch Festlegen eines minimalen Zeitfensters, in welchem ein wiederholt auftretendes Ereignis ignoriert wird, zu verzögern. Alle Ereignisse, die in diesem Intervall auftreten, werden in einer Gruppe zusammengefasst. Die nächste Aktion (z. B. Versenden der nächsten eMail) wird in einer Übersicht über die zusammengefassten Ereignisse wiedergegeben.
- **Nutzen einer dynamischen Begrenzung** - In diesem Modus wird jede ausgelöste Aktion die Grenze gruppierter Ereignisse n-fach erhöhen. Die erste Virenerkennung wird eine Aktion auslösen. Das gleiche nachfolgende Ereignis wird keine Aktion mehr auslösen – es wird stattdessen in einer Gruppe zusammengefasst. Auf dem Screenshot oben ist die Grenze mit 5 gesetzt, d. h., die nächste Aktion wird erst nach 5 erfolgreichen Virenerkennungen ausgelöst. Würde eine 6. Erkennung folgen, dann würde die Grenze nochmals 5-fach erhöht. Nach Ablauf des festgelegten Zeitraums wird die Grenze automatisch wieder zurückgesetzt.

Diese Eigenschaft gestattet eine flexible Anpassung an die vorherrschende Situation. Auf der einen Seite dient es bei einem einzelnen Ereignis der sofortigen Benachrichtigung des Administrators, zum anderen wird die Möglichkeit der Netzwerküberlastung im Falle eines dramatischen Virenbefalls minimiert.

## 15. FAQ und technischer Support

Sollten Sie irgendwelche Probleme mit Ihrem AVG-Produkt haben, kaufmännischer oder technischer Art, gehen Sie bitte zum FAQ Bereich auf der Webseite der Firma Grisoft unter <http://www.grisoft.de/> (FAQ).

Wenn Sie dort keine Hilfe finden, wenden Sie sich bitte an den Technischen Support unter [technicalsupport@grisoft.com](mailto:technicalsupport@grisoft.com). Bitte denken Sie daran, dass Sie Ihre Lizenznummer von AVG im Text der eMail mit angeben.

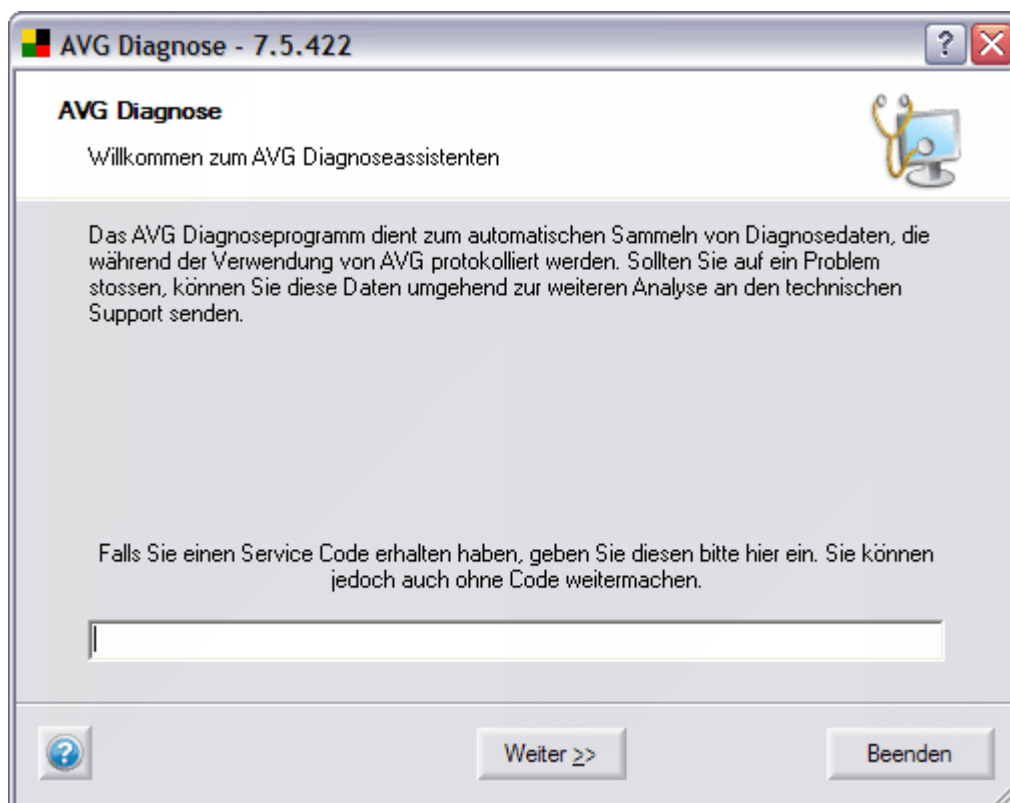
Wir empfehlen Ihnen jedoch die Kontaktaufnahme mit dem Technischen Support von Grisoft über das Dialogfenster, das aus allen AVG-Programmen erreichbar ist (z.B. **Test Center**, **Control Center**...). Zum Öffnen dieses Dialoges wählen Sie bitte die Option **Technischer Support per eMail** aus dem Menü **Informationen** aus. Nun gehen Sie bitte weiter zu Kapitel [15.1 AVG Diagnoseprogramm](#), um weitere Informationen zu erhalten, wie die Rückfragen des technischen Supports bearbeitet werden sollen.

### 15.1. AVG Diagnoseprogramm

**AVG Diagnose** ist ein unterstützendes Dienstprogramm, was über den Technischen Support von AVG bereitgestellt wird. Das primäre Anliegen dieses Programms ist, Informationen über den Computer zu erhalten. Diese Informationen helfen dem technischen Support, Ihr Problem mit dem AVG-Programm zu lösen, indem die gesammelten Protokolle, Fehlerbenachrichtigungen, Systeminformationen, verdächtige Dateien, Ihre eigenen Kommentare und andere Daten analysiert werden.

***Anmerkung:** Das Programm **AVG Diagnose** versendet niemals persönliche oder andere sensible Daten von Ihrem Computer ohne die ausdrückliche Erlaubnis des Benutzers. Der Benutzer kann den Inhalt aller gesammelten Dateien überprüfen und jede Datei von dem Versenden an den Technischen Support von AVG ausnehmen.*

- a) **AVG Diagnose** startet mit der folgenden Bildschirmanzeige, die Sie nach dem **AVG Diagnose Service Code** fragt:



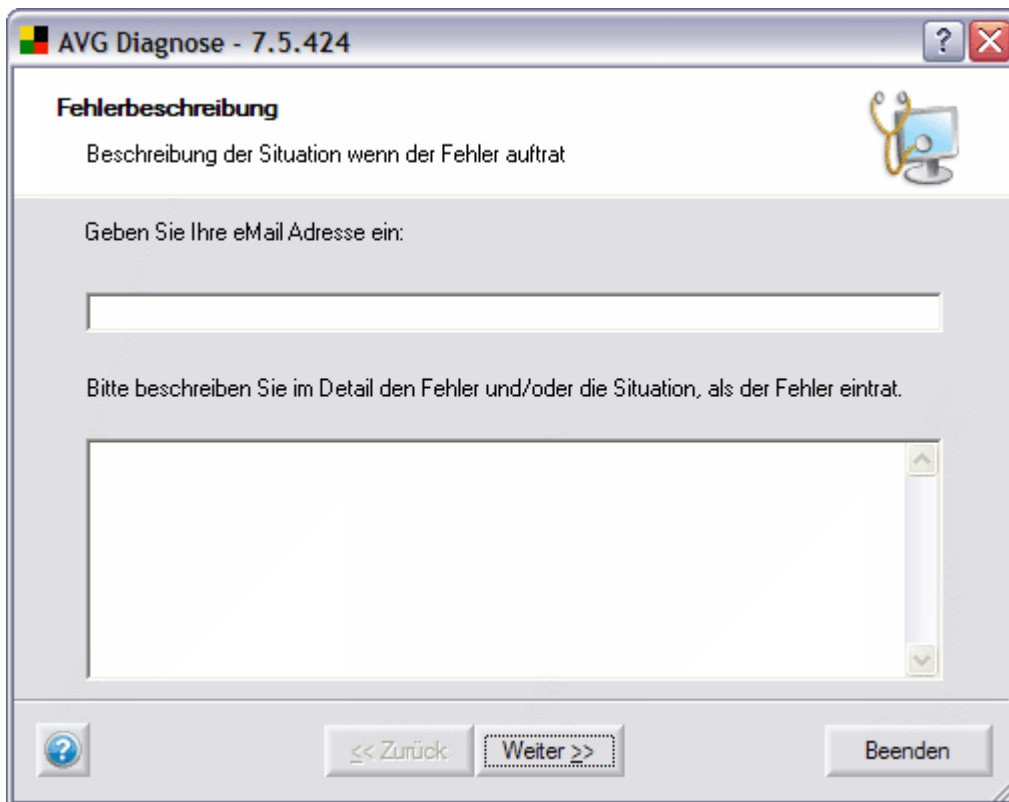
Wenn Sie einen Service Code erhalten haben, geben Sie diesen bitte in das Textfeld ein oder benutzen Sie hierfür die Methode Kopieren/Einfügen. Der Code startet automatisch den korrekten **AVG Diagnose Modus**, der gewährleistet, dass nur die erforderlichen (und nicht überflüssige) Daten während der **AVG Diagnose** gesammelt werden.

Wenn Sie keinen Service-Code haben, so können Sie eine der folgenden Optionen wählen:

- Nehmen Sie Kontakt mit dem [AVG Technical Support](#) auf und fragen nach einem **AVG Diagnose Service Code**. Wir empfehlen diese Option dringendst, wenn Sie ein Benutzer mit wenig Computererfahrung sind.
- Klicken Sie auf **Weiter** und starten Sie das Programm **AVG Diagnose** im Vollmodus (Standard). In diesem Fall fahren Sie fort mit Schritt [b - Fehlerbeschreibung](#).
- Wenn Sie ein Benutzer mit Computer-Fachwissen sind, können Sie **AVG Diagnose** schliessen und folgen den Anweisungen in Schritt [d\) Advanced Einstellungen - AVG Diagnose Modus](#).

#### b) Fehlerbeschreibung

In diesem Dialog können Sie Ihre Kommentare und Kontaktinformationen zu den Daten, die an den Technischen Support von Grisoft gesendet werden sollen, beifügen.

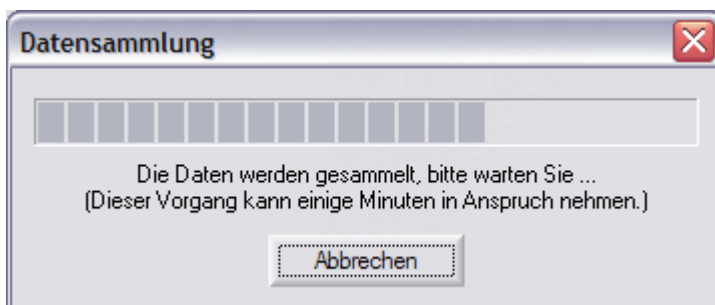


Beschreiben Sie so gut es geht im Detail, was für ein Problem Sie mit Ihrer AVG-Installation haben, unter welchen Umständen dieses Problem auftritt; bitte geben Sie jede Information ein, die dem technischen Support bei der Lösung des Problems helfen könnte.

Im unteren Feld können Sie Ihre eMail-Adresse eingeben, unter der Sie für den technischen Support erreichbar sind.

**Anmerkung:** In diesem Dialog sind die schwarzen Schaltflächen deaktiviert.; wenn Sie einen anderen AVG Diagnose Service code eingeben möchten, müssen Sie die aktuelle Anwendung beenden und AVG Diagnose neu starten.

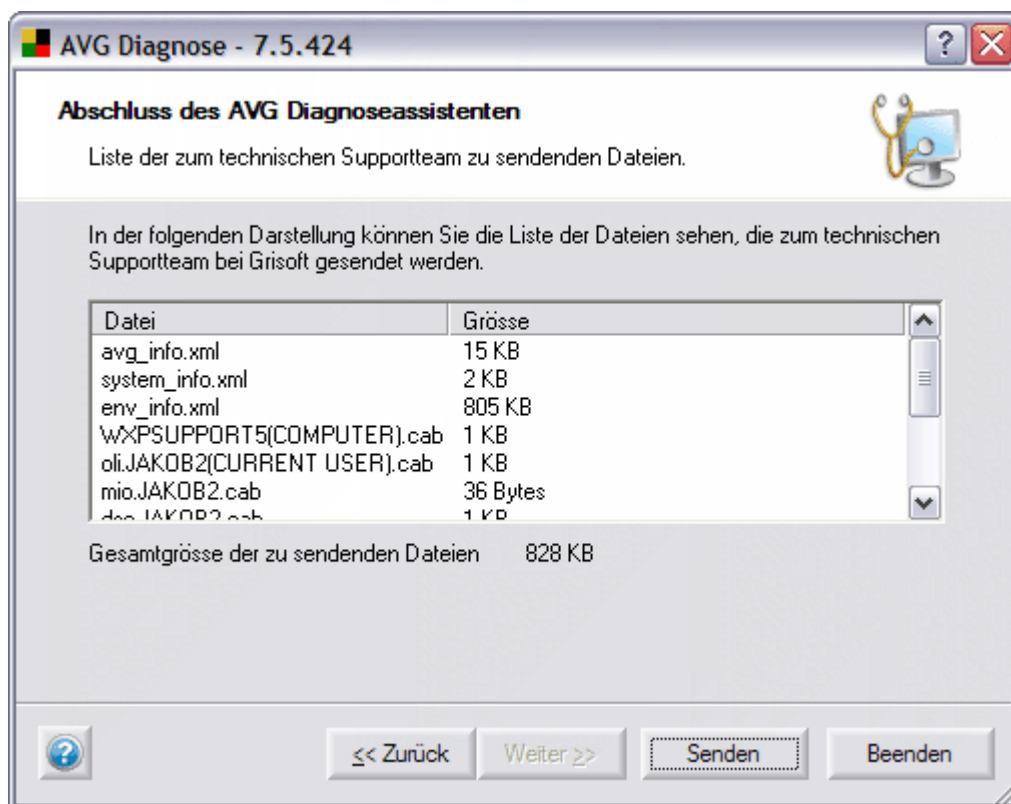
Wenn Sie ausgewählt haben klicken Sie auf die Schaltfläche **Weiter**. **AVG Diagnose** beginnt nun mit dem Sammeln von Daten. Dieser Vorgang kann einige Zeit dauern.



c) **AVG Diagnose - Beenden des Assistenten**

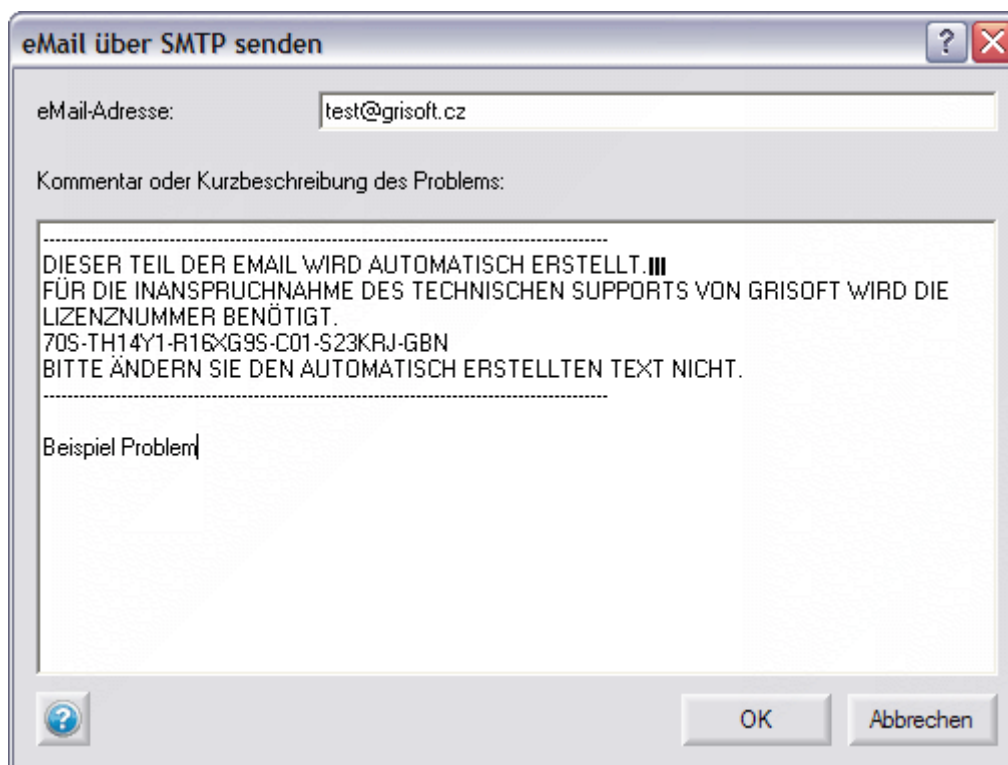
## AVG 7.5 File Server

Dieser Dialog zeigt eine Übersicht der Daten (Dateiname und Grösse), die an den technischen Support von Grisoft gesendet werden sollen. Darunter wird die Gesamtgröße der entsprechenden Daten angezeigt.



Bestätigen Sie den Vorgang durch Drücken der Schaltfläche **Senden**. Es erscheint ein neuer Dialog mit vorher eingegebenen Daten und Ihrer Lizenznummer.

**Anmerkung:** Wenn Sie den automatisch generierten Teil dieser eMail mit Angabe Ihrer Lizenznummer ändern, kann es vorkommen, dass Sie keine Antwort vom technischen Support der Firma Grisoft erhalten!



Um die Daten an den technischen Support von Grisoft zu senden klicken Sie auf die Schaltfläche **OK**. AVG Diagnostics wird anschließend automatisch die gesammelten Daten versenden.

**Anmerkung:** Wenn Sie die eMail nicht versenden können, überprüfen Sie bitte, ob Ihre Firewall die Übertragung nicht blockiert.

#### d) **Erweiterte Einstellungen - AVG Diagnose Modus**

**Anmerkung:** Befolgen Sie diese Anweisungen nur, wenn Sie mit den erweiterten Eigenschaften von **AVG Diagnose** vertraut sind.

Wenn **AVG Diagnose** bereits betrieben wird, schliessen Sie es bitte und starten Sie es von der Kommandozeile aus neu mit dem entsprechenden **AVG Diagnose Modus**-Parameter.

Der Modi der AVG diagnose sammeln nur die notwendigen und keine unnötigen diagnostischen Daten. Jeder Modus wirkt sich auf das Verhalten des Programms aus, so das nur die notwendigen Maßnahmen durchgeführt werden und zeigt nur die Dialogkästchen an, die für den Benutzer benötigt werden; damit wird der gesamte Prozess beträchtlich beschleunigt.

Der AVG Diagnose Modus kann gestartet werden:

- Automatisch über einen **AVG Diagnose Service Code** (den Sie über den AVG Technischen Support zusammen mit den Programm **AVG Diagnose** erhalten),
- Mit Start der **AVG Diagnose** von der Kommandozeile aus mit dem entsprechenden Parameter .

## AVG 7.5 File Server

Für den Start des **AVG Diagnose** von der Kommandozeile aus folgen Sie bitte auch Schritt [e\) AVG Diagnose - Vollständige Parameter Übersicht](#)

Für die Parameter und weitere Informationen zu jeder einzelnen AVG Diagnostik-Methode lesen Sie bitte das entsprechende Thema:

- ***Vollständige Diagnose***

Dies ist der Basis-Modus der AVG-Diagnose.

**AVG Diagnose** im Basis-Modus erstellt eine vollständige Zusammenstellung aller Informationen über den PC: Protokolle, Systeminformationen, Konfiguration, Lizenz, Netzwerkumgebung und andere wichtige Informationen, die für die Lösung eines Problems mit AVG von Wichtigkeit sein könnten.

**Parameter:** /MODE=FULL, or no parameter

- ***Das Senden einer verdächtigen Datei zur Analyse***

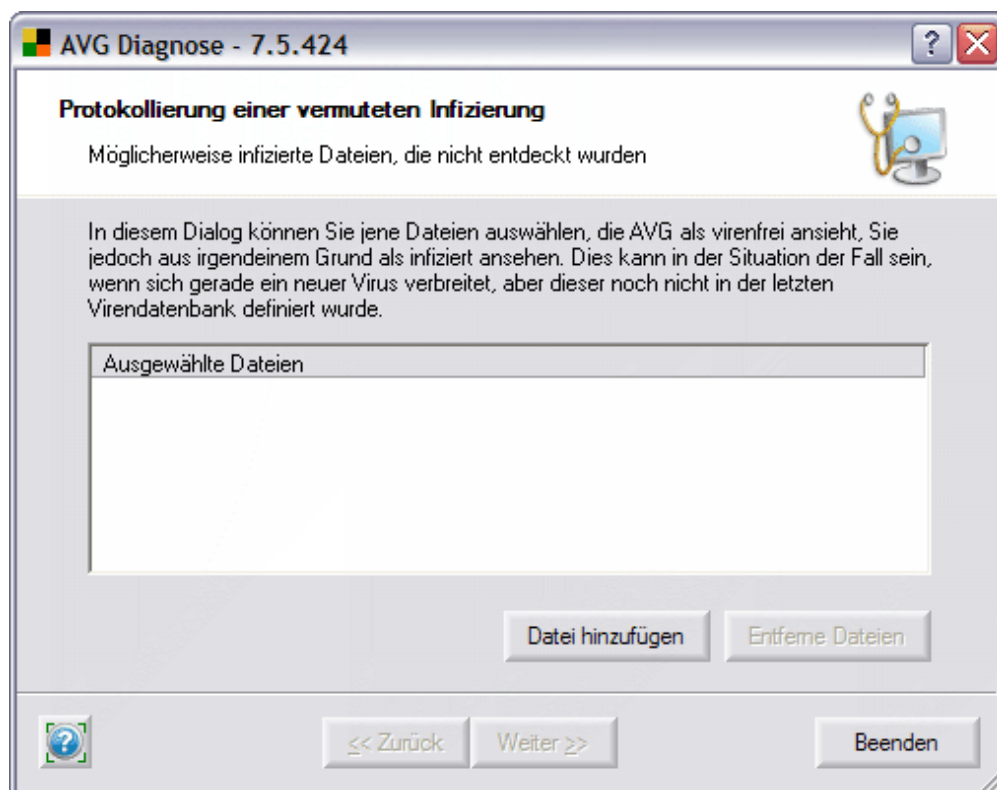
Mit **AVG Diagnose im Basis-Modus** können Sie eine verdächtige Datei (oder mehrere Dateien) zur Analyse an den technischen Support von Grisoft senden.

Etwas *Verdächtiges* ist normalerweise eine Datei, die von AVG nicht erkannt wurde, von der Sie jedoch aus irgendeinem Grund glauben, dass Sie infiziert sein könnte oder dass sie ein unerwünschtes Programm sein könnte.

**Parameter:** /MODE=VIRUS

**Zum direkten Lokalisieren der verdächtigen Datei:** /FILE= <file>

Der folgende Dialog erscheint **Protokollierung einer vermuteten Infizierung:**



In diesem Dialog können Sie eine Datei an die eMail anhängen, die an den technischen Support von Grisoft gesendet werden soll.

Sie können eine Datei hinzufügen, von der Sie glauben, sie sei infiziert, von AVG bisher jedoch noch nicht erkannt worden.

Klicken Sie auf **Datei hinzufügen**, um den Dialog zur Suche und zum Finden der Datei zu öffnen, die Sie in Verdacht haben. Sie können diese Schritte, so oft Sie dies für nötig halten, wiederholen.

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

Wenn Sie dies beendet haben klicken Sie auf die Schaltfläche **Weiter**.

- **Das Senden einer falschen Alarm-Datei zur Analyse**

Diese **AVG Diagnose** ermöglicht Ihnen, eine *falsche Alarm* -Datei (oder mehrere Dateien) zur Analyse an den technischen Support von Grisoft zu senden.

Ein falscher Alarm bedeutet eine Datei, die von AVG erkannt wurde, von der Sie aber glauben, dass Sie keine Viren enthält.

**Parameter:** /MODE=FALSE

**Für die direkte Lokalisierung der falschen Alarm-Datei:**

/FILE=<file>

- **Feedback des Kunden**

## AVG 7.5 File Server

Dieser **AVG Diagnose Modus** bietet Ihnen die Möglichkeit, Kommentare an den technischen Support von Grisoft zu senden.

AVG- Einstellungen und Systeminformationen werden der Nachricht beigefügt.

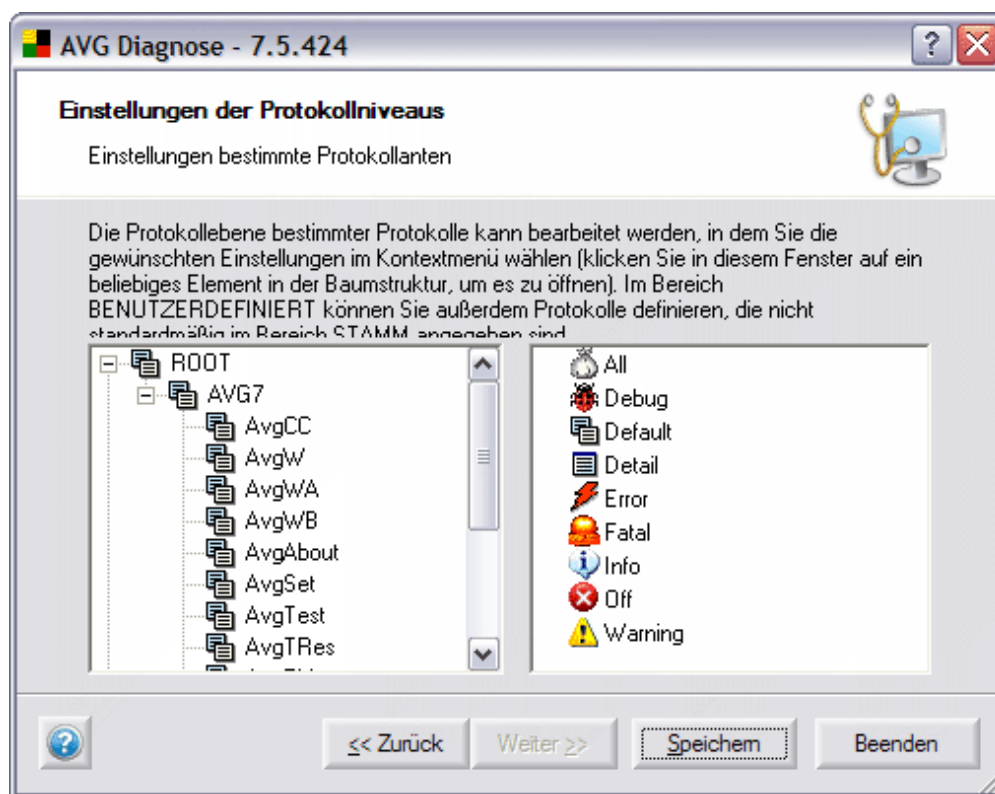
**Parameter:** /MODE=FEEDBACK

### o Einstellungen des Protokoll-Levels

Grundsätzlich ermöglicht Ihnen diese **AVG Diagnose**, das benötigte Protokolllevel für die AVG-Software einzustellen, damit nur die benötigten Informationen protokolliert werden; somit kann der technische Support von AVG hiermit effektiv arbeiten.

**Parameter:** /MODE=LOGLEVEL

**Nur für erfahrene Computerbenutzer empfohlen!**



Der linke Bereich zeigt einen erweiterten Protokollbaum an. Der Bereich AVG7 enthält alle Standard AVG-Protokolleinrichtungen; der Bereich ALLGEMEIN ermöglicht Ihnen, eine neue Einrichtung zum Protokollieren zu definieren (Doppelklick auf <new item>). Um einen Pfad für die Protokolleinrichtung anzugeben nutzen Sie bitte Punkte, z.B. AVG7.AvgWB.MyLogger.

Um eine benutzerdefinierte Protokolleinrichtung zu entfernen, rechtsklicken Sie darauf und wählen Sie die Option **Entfernen**.

## AVG 7.5 File Server

Sie können ein bestimmtes Level für die Protokolleinrichtung eines jeden Eintrags in dem Baum einstellen - verfügbare Levels für die Protokolleinrichtung werden im rechten Bereich des Dialogs angezeigt. Rechtsklicken Sie auf einen Eintrag und wählen das Protokolllevel aus dem Kontextmenü. Wenn Sie Ihre Wahl für alle untergeordneten Protokolleinrichtungen anwenden möchten, wählen Sie erst **Für alle anwenden**

Nach dem Beenden klicken Sie auf die Schaltfläche **Speichern**, damit die Einstellungen bestätigt und gespeichert werden. (Die Schaltfläche **Weiter** ist in diesem Dialog deaktiviert)

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

- o **AVG Erkennung einer Störung**

**AVG Diagnose** ermöglicht Ihnen, ERR und DMP-Dateien zu erkennen und zur Analyse zu senden (diese sind nur vorhanden, wenn Ihre Installation von AVG kürzlich ausgefallen ist). Das Fehlen dieser Dateien bedeutet, dass es keinen Ausfall von AVG gegeben hat.

Wenn ein Ausfall von AVG erkannt wurde, erscheint ein Bestätigungs-Dialog mit einem Überblick über Fehlerdateien und Sie werden gefragt, ob Sie diese zur Analyse versenden möchten.

Beim nächsten Betrieb von **AVG Diagnose** unter **Störungserkennung** wird nur über neu erkannte Fehlerdateien berichtet.

**Parameter:** /MODE=ERRDUMP

e) **AVG Diagnose - Übersicht über alle Parameter**

In der unten angezeigten Liste finden Sie einen vollständigen Überblick über alle **AVG Diagnose**-Parameter.

Parameter	Beschreibung
<i>Kein Parameter</i>	Startet AVG Diagnose im Vollmodus (Standard).
<i>/CODE=&lt;code&gt;</i>	Erlaubt Ihnen die Eingabe des AVG Diagnose Service Codes, den Sie vom AVG Technischen Support erhalten haben. Dieser Code startet automatisch den benötigten AVG Diagnose Modus.
<i>/MODE=FULL</i>	Startet AVG Diagnose im Vollmodus (Standard).
<i>/MODE=VIRUS</i>	Startet AVG Diagnose im Modus verdächtige Datei zur Analyse senden.
<i>/MODE=FALSE</i>	Startet AVG Diagnose im <i>falsche Alarm</i> Datei zur Analyse senden Modus.
<i>/MODE=FEEDBACK</i>	Startet AVG Diagnose im Kundenfeedback Modus.

## AVG 7.5 File Server

<code>/MODE=LOGLEVEL</code>	Startet AVG Diagnose im Protokolleinstellungsmodus.												
<code>/MODE=ERRDUMP</code>	Startet AVG Diagnose im Störungserkennungsmodus.												
<code>/LOGROOT= &lt;level&gt;</code>	Startet automatisch den Protokolleinstellungsmodus und erlaubt Ihnen, einen Protokolleinstellungsmodus direct auszuwählen.												
<code>/FILE= &lt;file&gt;</code>	In den Modi "verdächtige Datei zur Analyse senden" und "falsche Alarm Datei zur Analyse senden" können Sie die entsprechende Datei(en) direct angeben.  Im Vollmodus (Standard) ermöglicht es Ihnen, eine zusätzliche Datei an den Bericht anzuhängen.												
<code>/CLEARUPD</code>	Löscht alle überflüssigen und temporären Dateien.												
<code>/NOUI</code>	Minimiert die Anzahl der angezeigten Dialogfenster.												
<code>/LNG= &lt;lng&gt;</code>	Ermöglicht Ihnen, die Oberfläche der AVG Diagnose auf eine andere Sprache umzuschalten.  Verfügbare Sprachen und deren Codes: <table border="1" data-bbox="619 1048 1284 1326"> <tr> <td>CZ=0x0405</td> <td>GE=0x0407</td> <td>PB=0x0416</td> </tr> <tr> <td>SK=0x041b</td> <td>FR=0x040c</td> <td>PL=0x0415</td> </tr> <tr> <td>US=0x0409</td> <td>SP=0x040a</td> <td>SC=0x081a</td> </tr> <tr> <td>IT=0x0410</td> <td>HU=0x040e</td> <td>NL=0x0413</td> </tr> </table>	CZ=0x0405	GE=0x0407	PB=0x0416	SK=0x041b	FR=0x040c	PL=0x0415	US=0x0409	SP=0x040a	SC=0x081a	IT=0x0410	HU=0x040e	NL=0x0413
CZ=0x0405	GE=0x0407	PB=0x0416											
SK=0x041b	FR=0x040c	PL=0x0415											
US=0x0409	SP=0x040a	SC=0x081a											
IT=0x0410	HU=0x040e	NL=0x0413											