AVG 7.5 Anti-Virus plus Firewall

Benutzerhandbuch

Document revision 75.1 (31.10.2006)

Inhalt

1. Einleitung

Dies ist ein umfassendes Benutzerhandbuch zu **AVG Anti-Virus plus Firewall 7.5.**

Verglichen mit **AVG Anti-Virus Professional Edition 7.5** bietet die **AVG Anti-Virus plus Firewall 7.5** Edition auf Grund der Komponente Firewall einen weitaus umfassenderen Schutz für Ihren Computer.

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 Systemregistrierung 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. AVG Firewall-Richtlinien

Computer, die nicht durch eine Firewall geschützt sind, bieten ein leichtes Ziel für Hacker und andere Datendiebe.

Eine Firewall ist ein System, das eine Zugangkontrolle zwischen zwei oder mehr Netzwerken einrichtet, indem der Datenverkehr geblockt oder zugelassen wird. Jede Firewall besitzt einen Satz Regeln, die das interne Netzwerk vor Attacken von außen (typischerweise aus dem Internet) schützen und zusätzlich die Kommunikation auf jedem Netzwerk-Port kontrollieren. Die Kommunikation wird anhand von vorher festgelegten Regeln untersucht und daraufhin entweder erlaubt oder verboten. Sobald die Firewall irgendeinen „Eindringungsversuch“ entdeckt, bekämpft sie diesen und lässt den Eindringling nicht in den Computer.

Die **Firewall** hilft Ihnen bei der Wahrung Ihrer Privatsphäre und schützt Ihre persönlichen Informationen vor einem versehentlichen Senden vom Computer ohne Ihre entsprechende Erlaubnis. Sie kontrolliert den Datenaustausch mit anderen Computern im Internet oder im lokalen Netzwerk. Innerhalb eines Unternehmens schützt die **Firewall** auch jede einzelne Arbeitsstation vor Angriffen durch interne Benutzer.

1.3. Unterstützte Betriebssysteme

AVG Anti-Virus plus Firewall 7.5 ist vorgesehen, Workstations mit den folgenden Betriebssystemen zu schützen: Windows NT/9x/Me/2000 Professional/XP einschließlich der 64-bit-Versionen.

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 Anti-Virus plus Firewall 7.5** 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

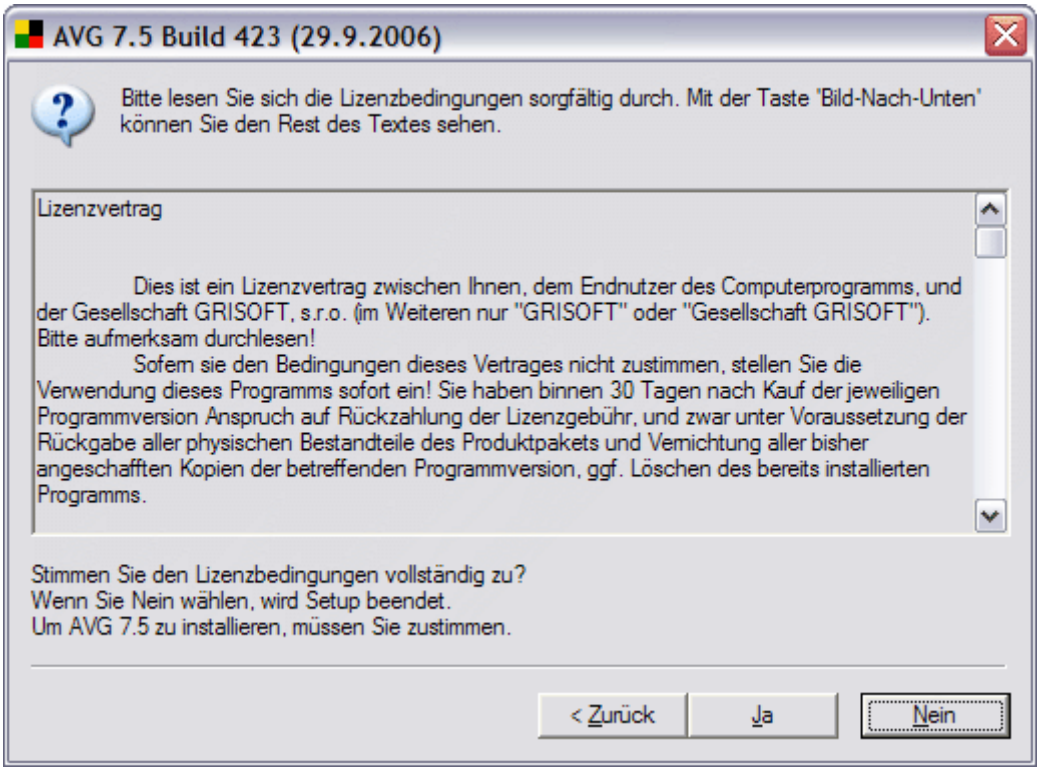
Im Installationsdialog Willkommen werden Sie aufgefordert, die Sprache für die Anwendung auszuwählen.

***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.

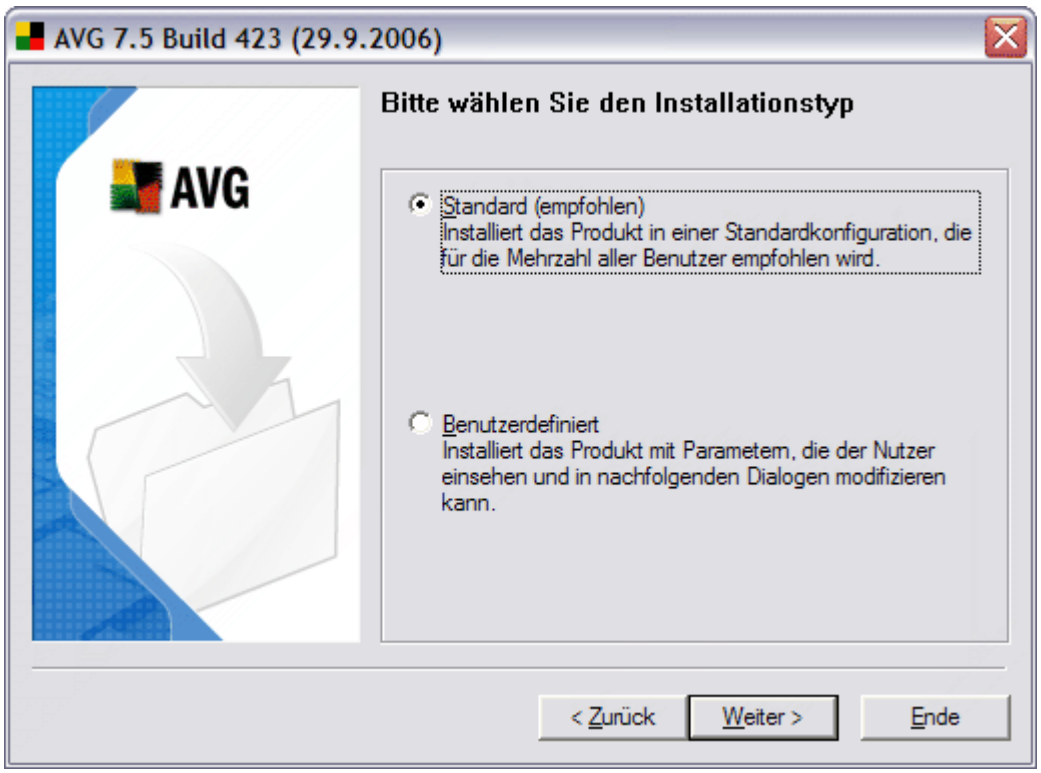


3.3. Installation – Auswahl des Installationstyps

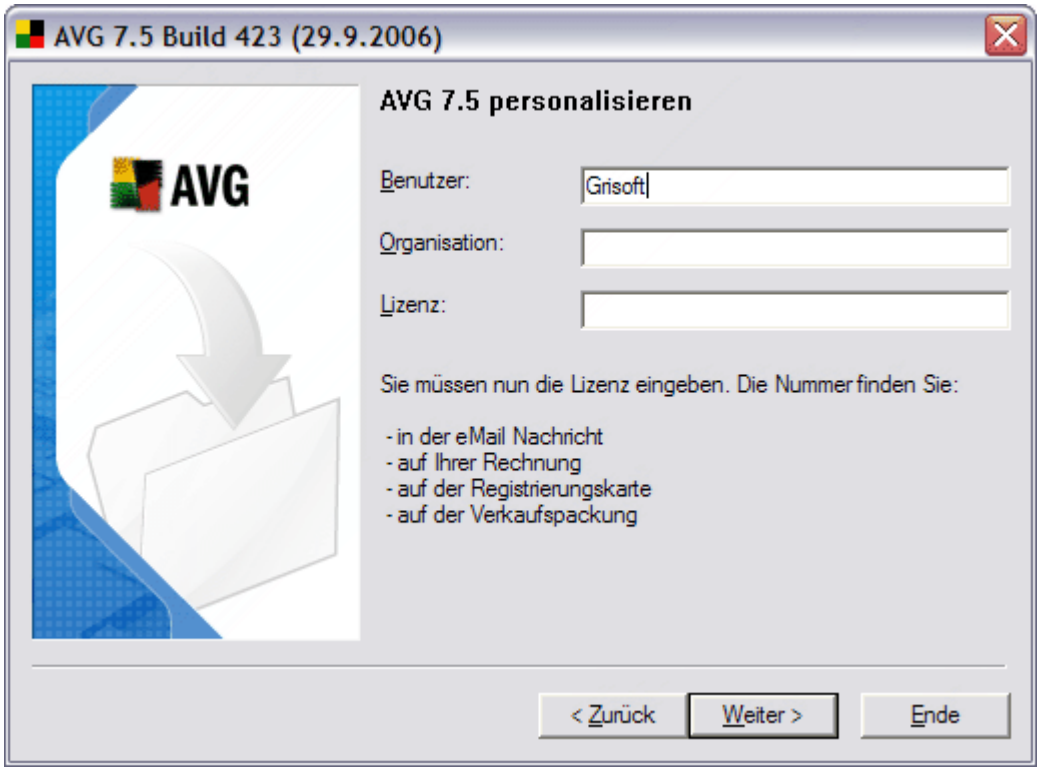
In diesem Dialogfenster müssen Sie sich zwischen zwei Installationstypen entscheiden: ***Standard*** und ***Benutzerdefiniert***.

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).



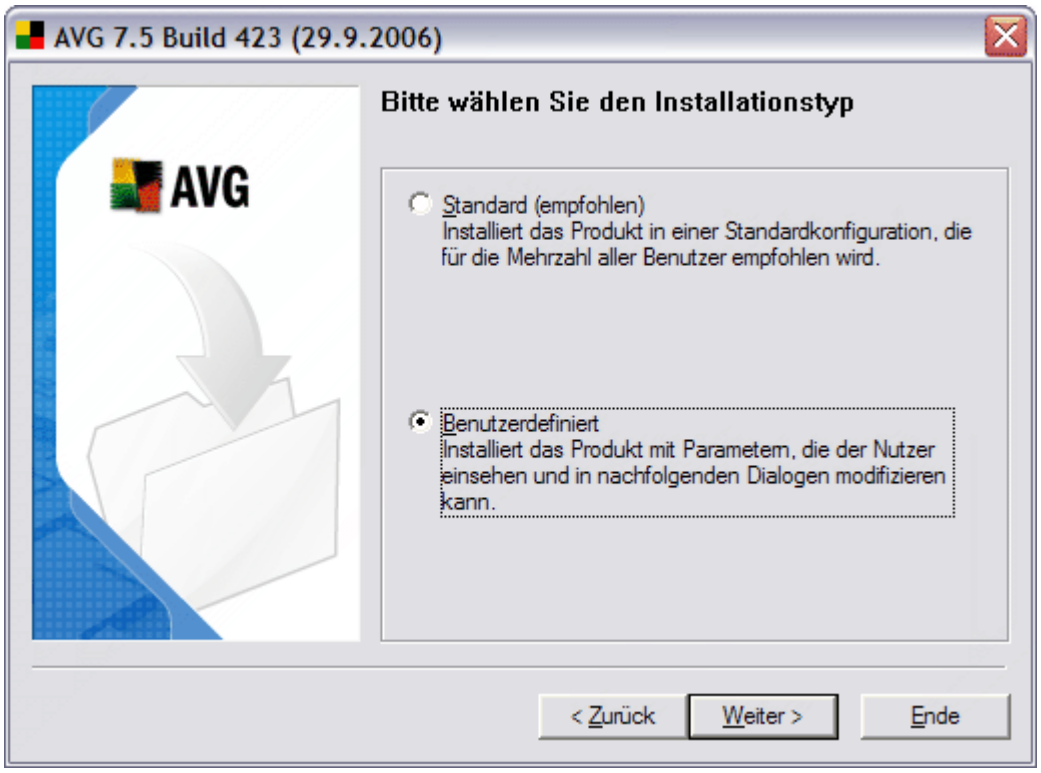
Bestätigen Sie die Option ***Standard*** durch Drücken der Schaltfläche ***Weiter***; Sie gelangen nun zum Dialog ***AVG 7.5 personalisieren***, in dem Sie Ihren Namen/Firmennamen und Ihre Lizenznummer angeben müssen:



Bestätigen Sie die eingegebenen Lizenzdaten wieder durch Drücken der Schaltfläche ***Weiter***. Danach gelangen Sie zum Dialog Installationszusammenfassung.

b) Benutzerdefinierte Installation

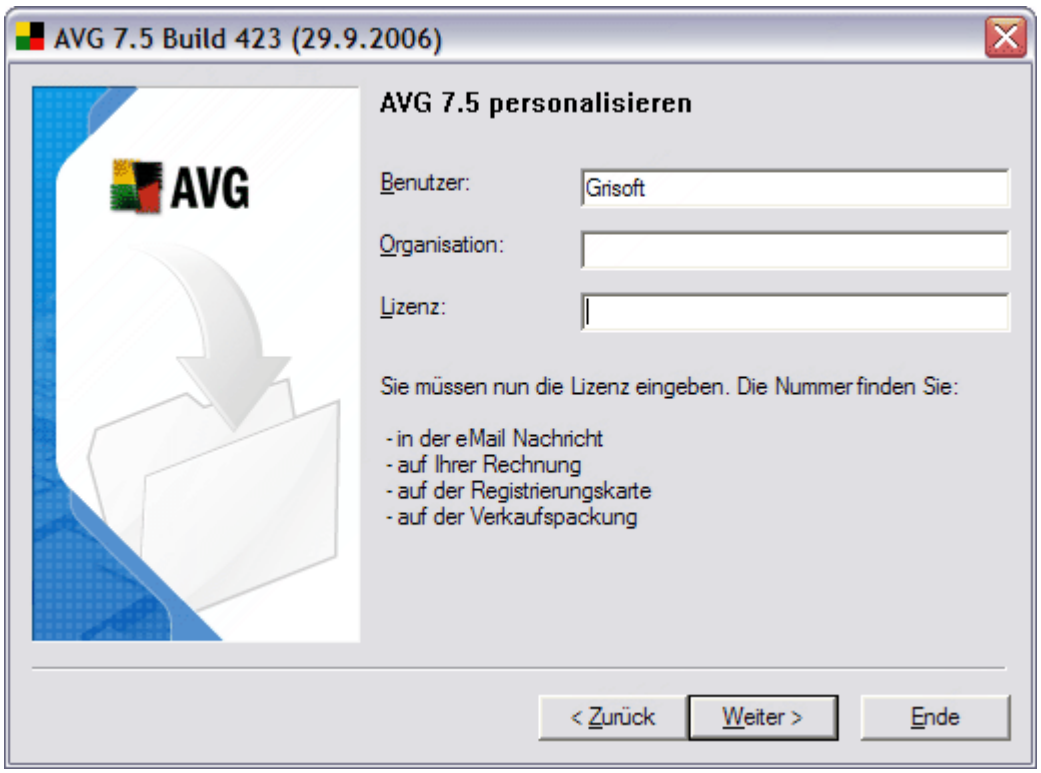
Die benutzerdefinierte Installation wird nur erfahrenen Benutzern empfohlen, die besondere Anforderungen an die Konfiguration der AVG-Komponenten haben und die die Einstellungen bereits während des Installationsprozesses vornehmen möchten. Sie haben jedoch auch die Möglichkeit, alle AVG-Komponenten nach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



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

- ***AVG 7.5 personalisieren***

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



o ***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.

o ***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.

o ***eMail Prüfung***

Im Dialog ***eMail Prüfung*** wählen Sie zwischen zwei Optionen für die Überwachung Ihrer eMails:

- ***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).

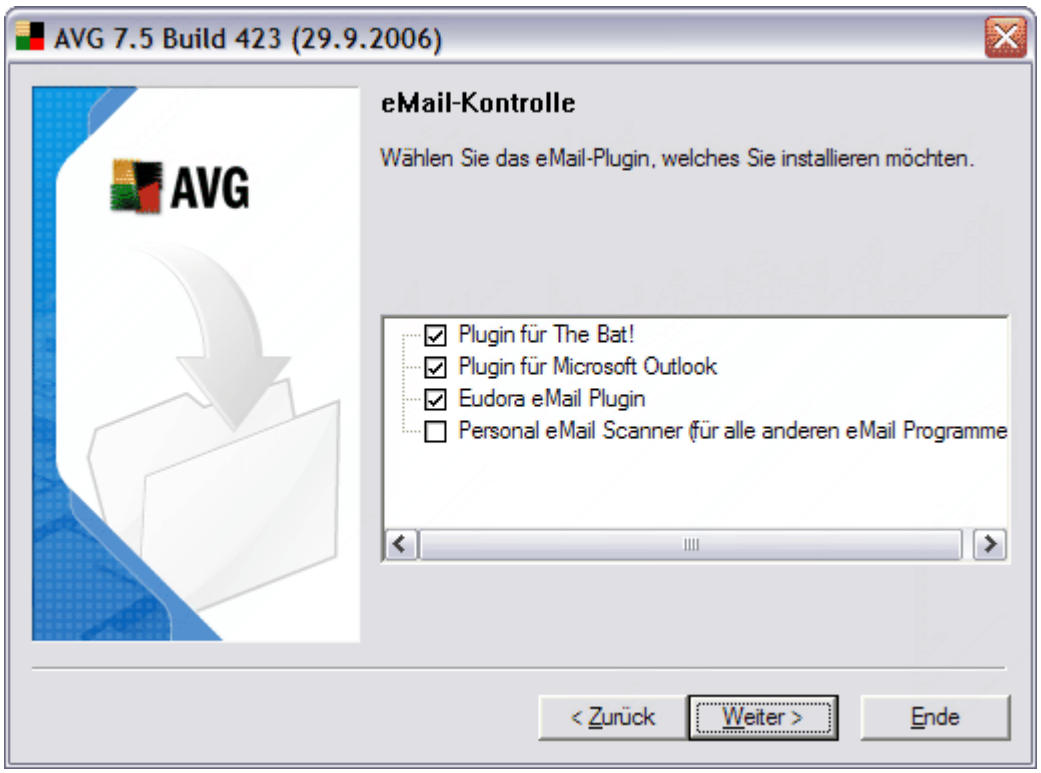
Für andere eMail-Programme stellt Ihnen AVG einen umfassenden eMail-Schutz unter Verwendung der Komponente ***eMail-Kontrolle*** zur Verfügung. Für diesen Fall bietet der Setup Dialog die empfohlene Option ***Personal eMail Scanner***.

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.*

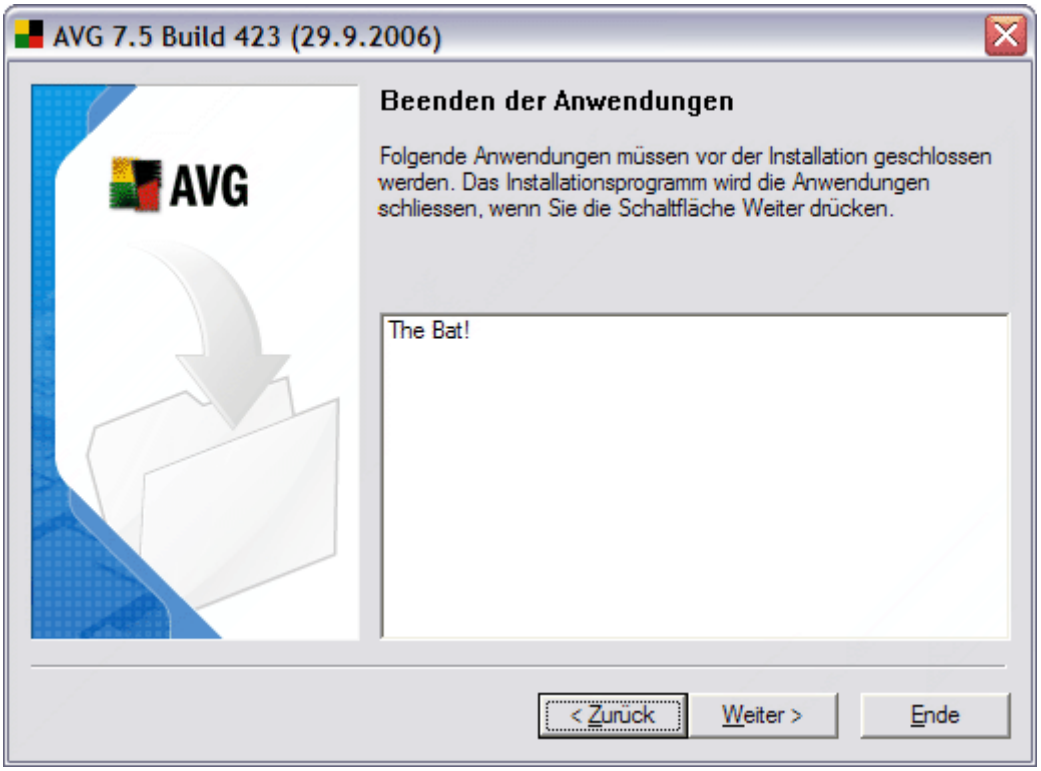
Drücken Sie die Schaltfläche ***Weiter***, um Ihre Auswahl zu bestätigen und um mit dem Dialog Zusammenfassung fortzufahren.

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***.

Vor dem Neustart Ihres Computers wird der Firewall Konfigurations-Assistent (Kapitel 10.6) gestartet- obwohl die Möglichkeit besteht, jederzeit während der Arbeit mit AVG die Konfiguration der **Firewall** zu bearbeiten, empfehlen wir dringendst, den Konfigurations-Assistenten zu durchlaufen und die Einstellungen der Firewall auf einfache Weise zu bestimmen.

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

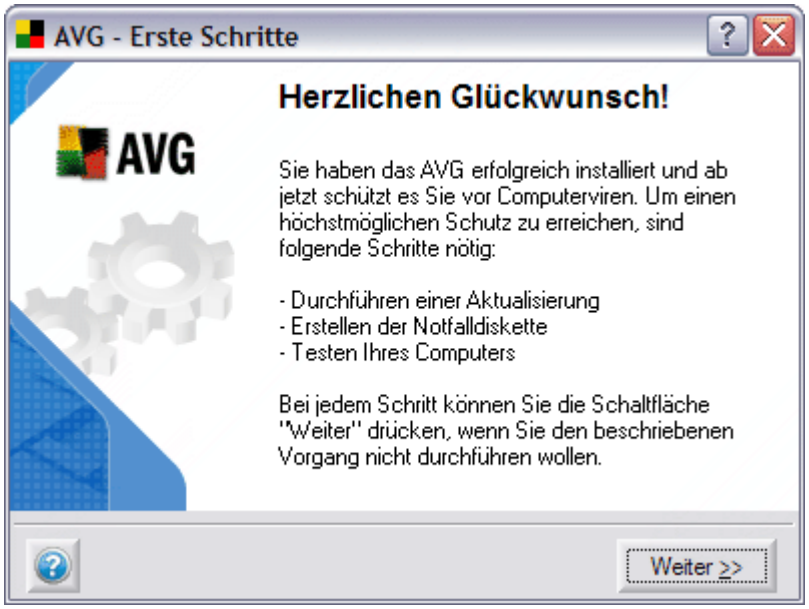
4.1. Erste Schritte-Assistent

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!

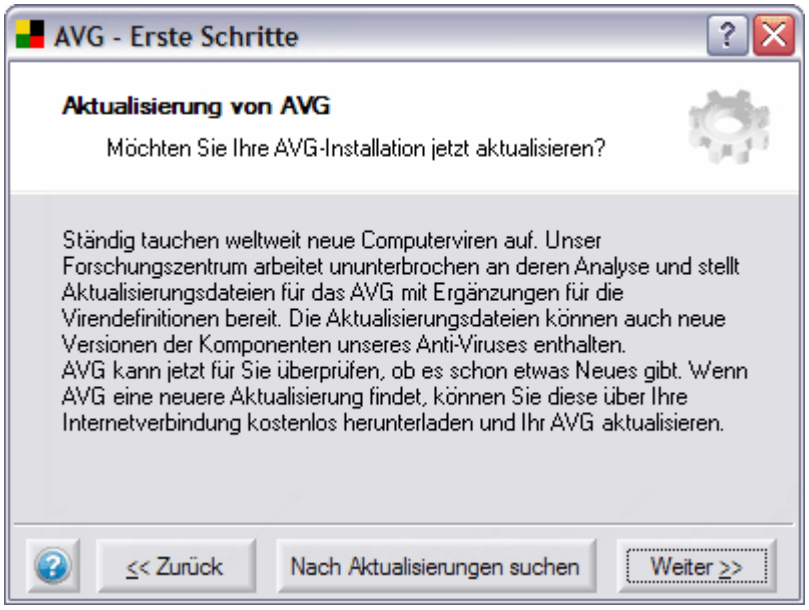
Der Willkommenbildschirm des ***AVG Erste Schritte-Assistenten*** zeigt kurz den aktuellen Status von AVG auf Ihrem Computer an und schlägt Ihnen daraufhin Schritte zur Vervollständigung Ihres Schutzes vor. Klicken Sie auf die Schaltfläche ***Weiter***, um fortzufahren:



Anmerkung: *Windows XP und höher unterstützt das Feature Rettungsdiskette nicht mehr!*

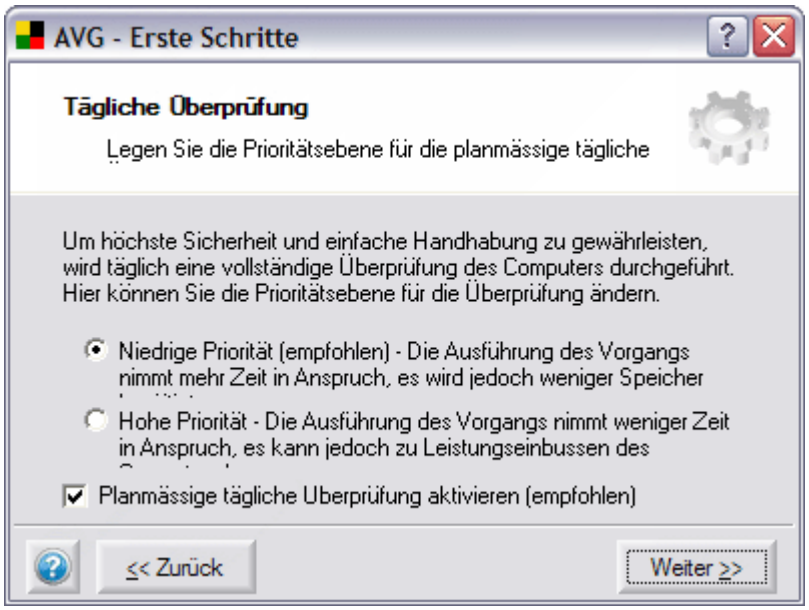
4.1.2. Erste Schritte-Assistent - Aktualisierung von AVG

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:



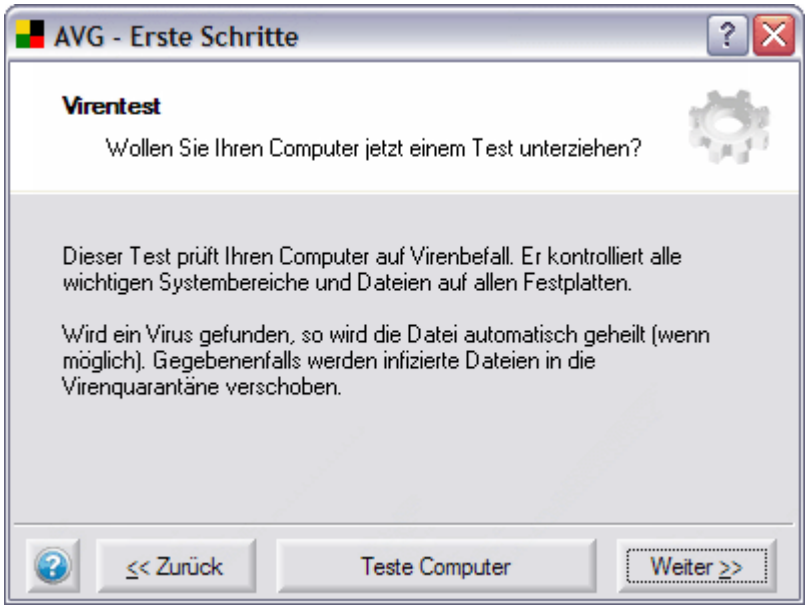
4.1.3. Erste Schritte-Assistent – Tägliche Überprüfung

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.



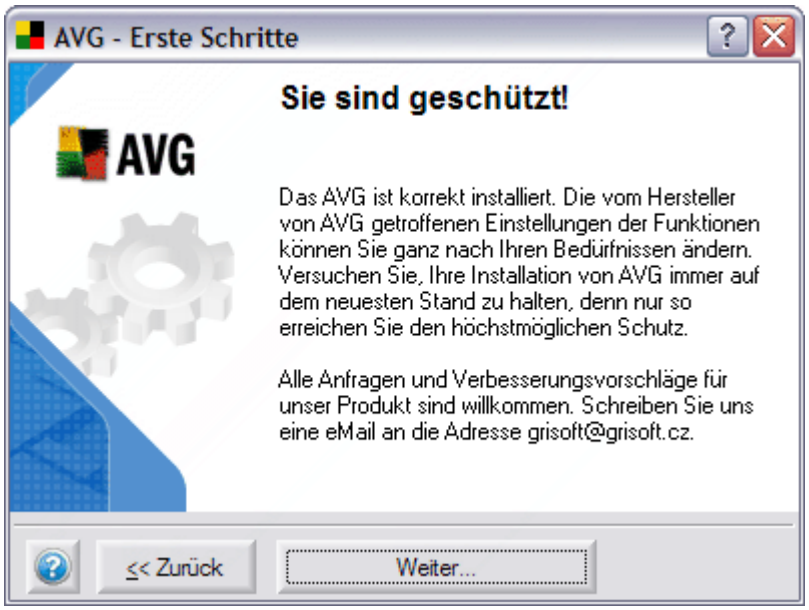
4.1.4. Erste Schritte-Assistent - Virentest

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 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

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.

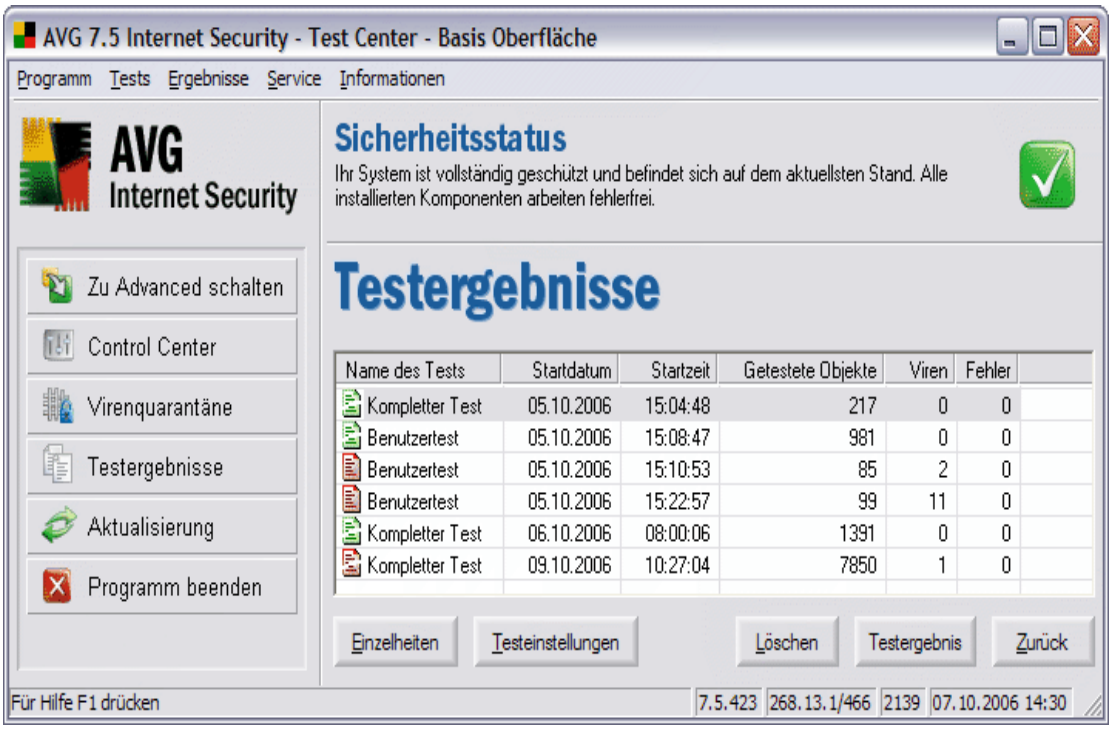
Für weitere Details zur **Virenquarantäne** lesen Sie bitte Kapitel 12. Virenquarantäne nach

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

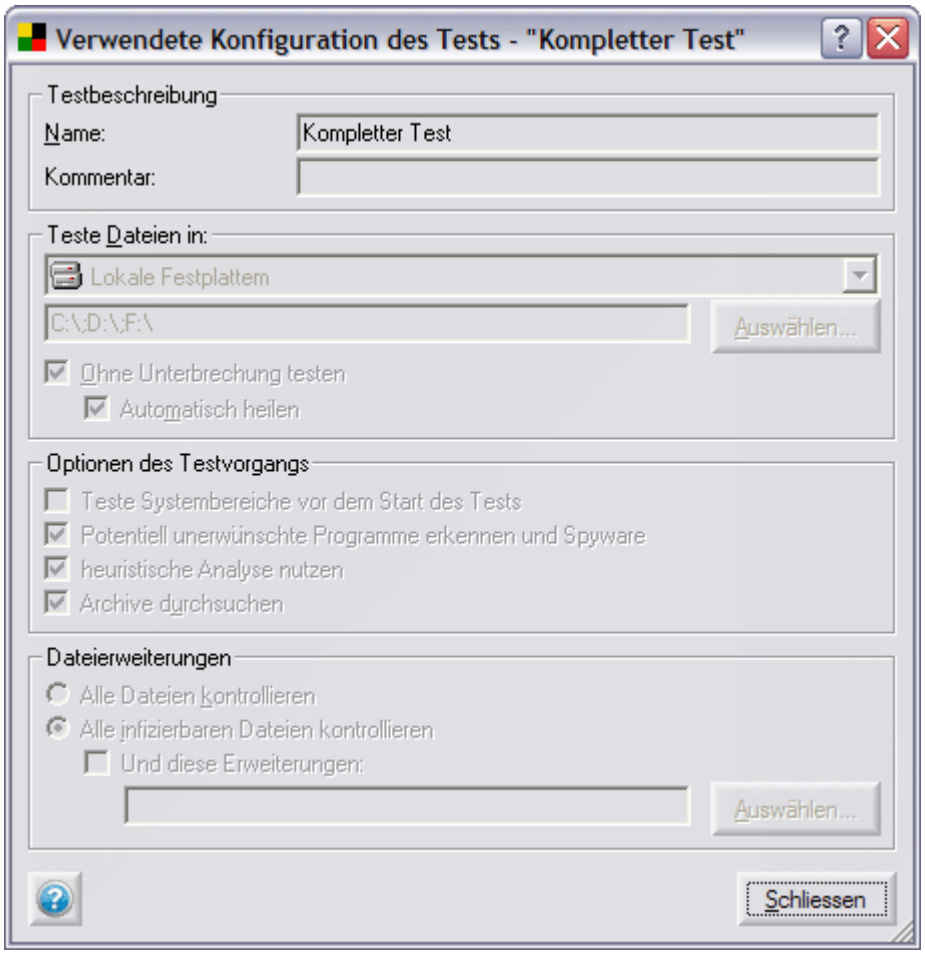
Die Schaltfläche ***Einzelheiten*** öffnet ein neues Dialogfenster, das Ihnen weitergehende Informationen über die durchgeführten Tests und deren Ergebnisse zeigt. Die Daten sind in zwei Gruppen unterteilt: ***Optionen*** (Testparameter und Testergebnisse) und ***Anzahl der Objekte*** (kontrollierte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

In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- o ***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)
- o ***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:

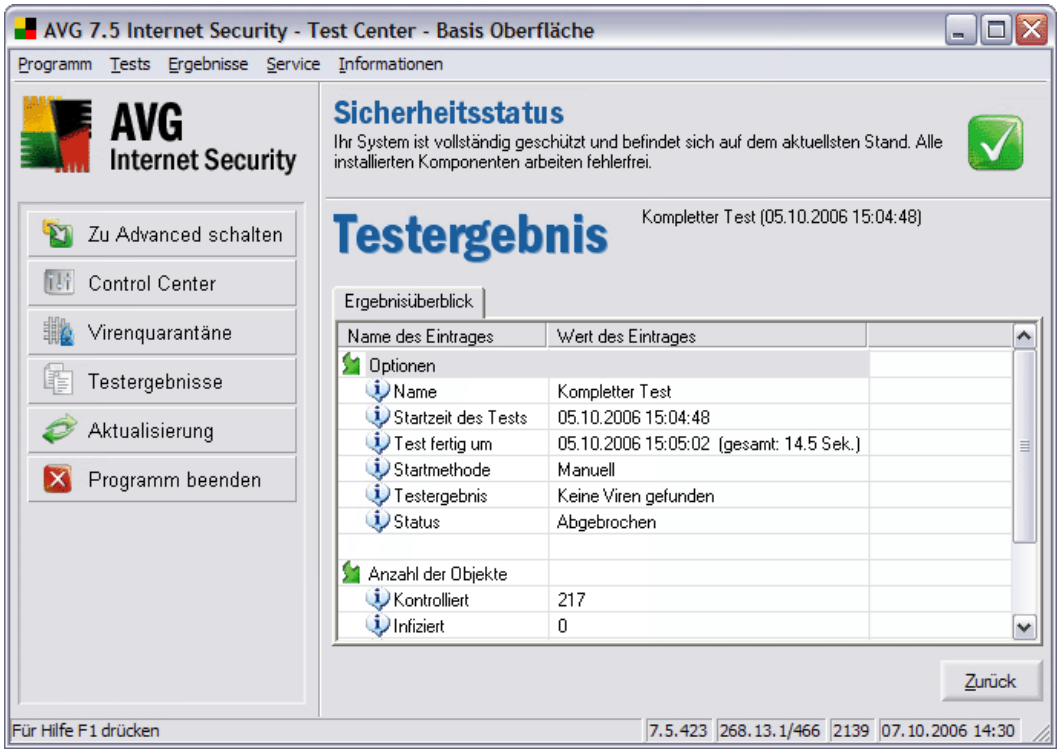


c) Löschen

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.



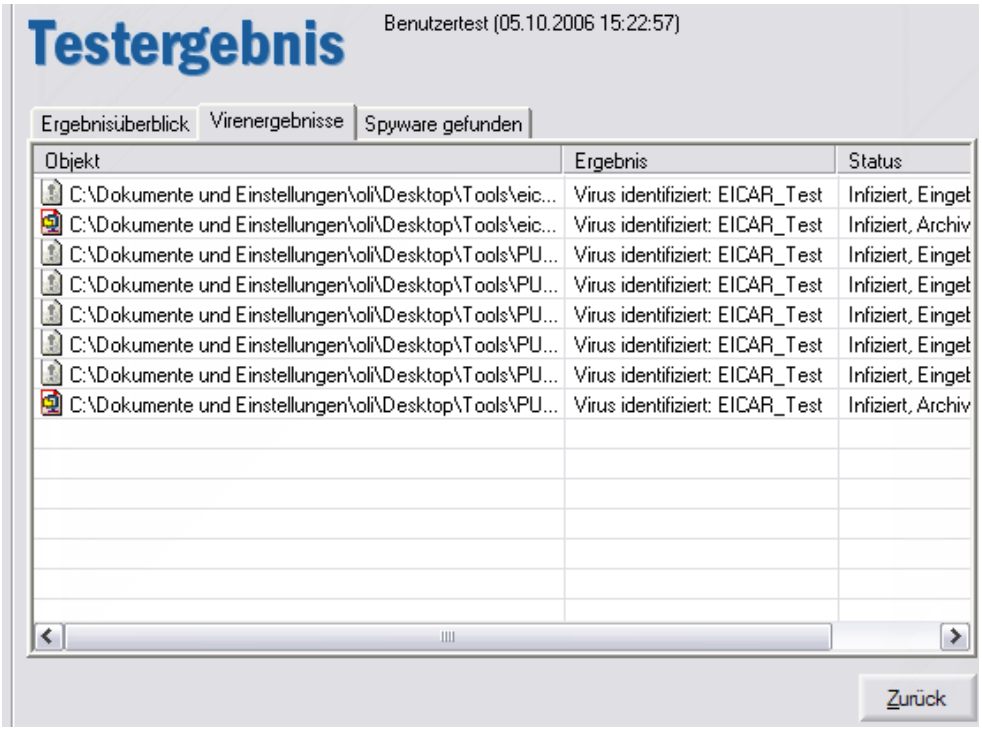
Dieser Dialog ist in verschiedene Reiter unterteilt:

- ***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.



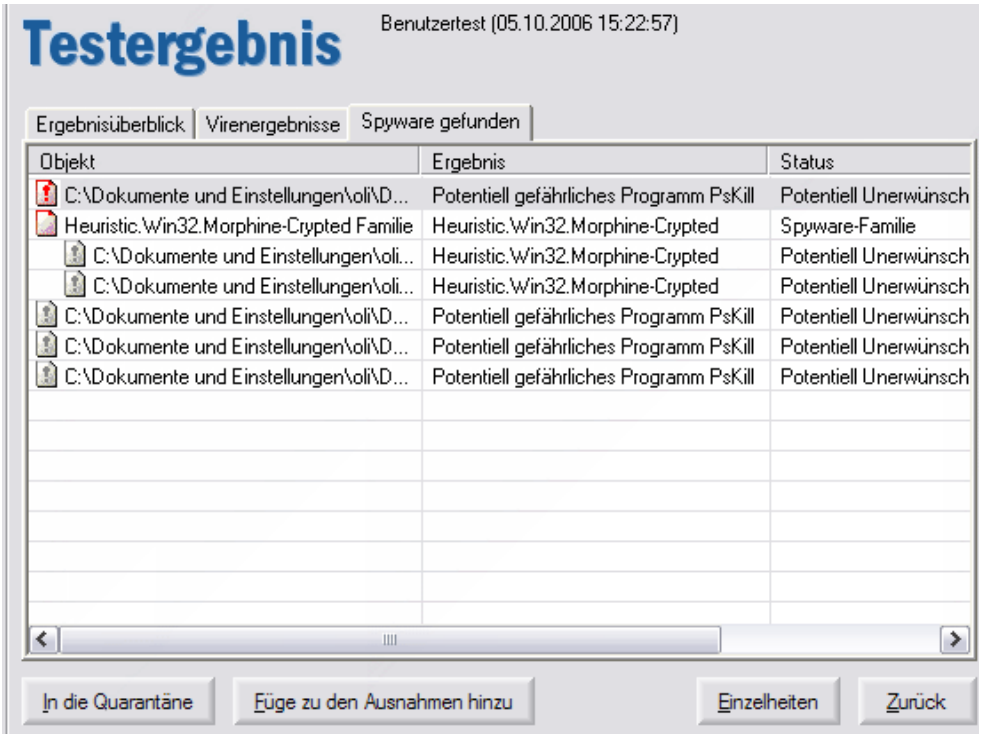
In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- ***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.

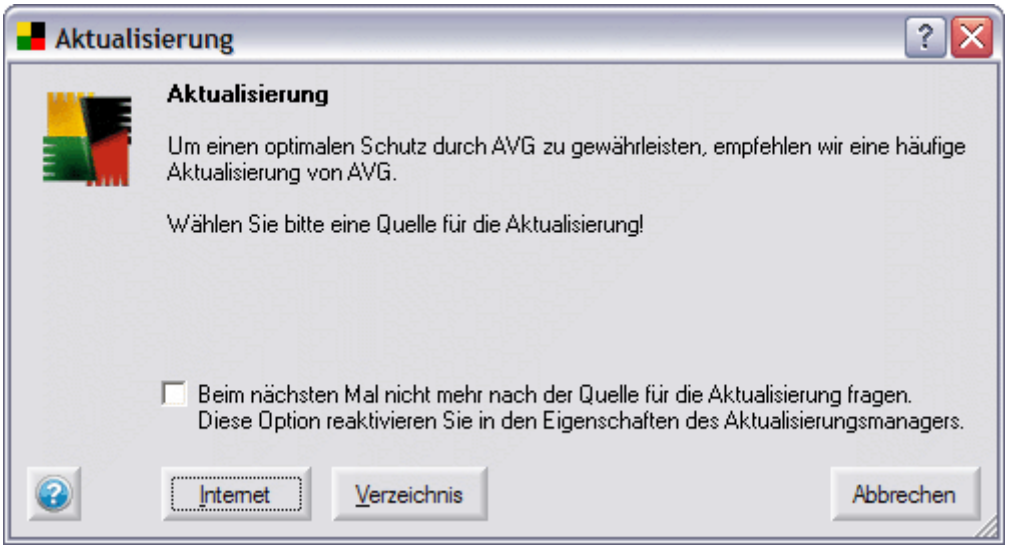
e) Zurück

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)

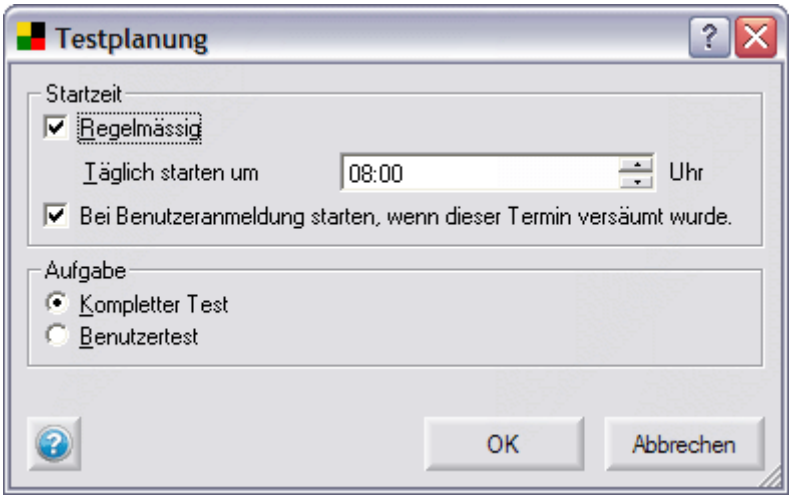
In diesem Abschnitt können Sie Ihre eigenen Parameter anstelle der Standardparameter des Herstellers für die AVG-Tests einstellen.

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

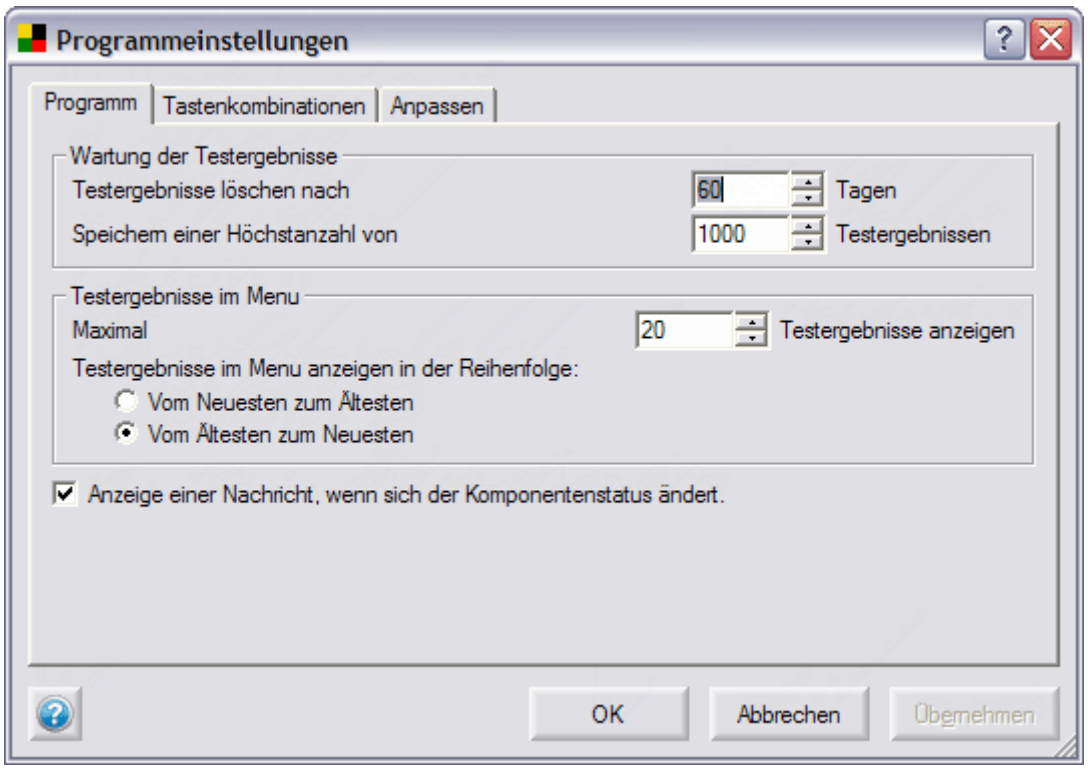
7.9. Programmeinstellungen

Service/Programmeinstellungen

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

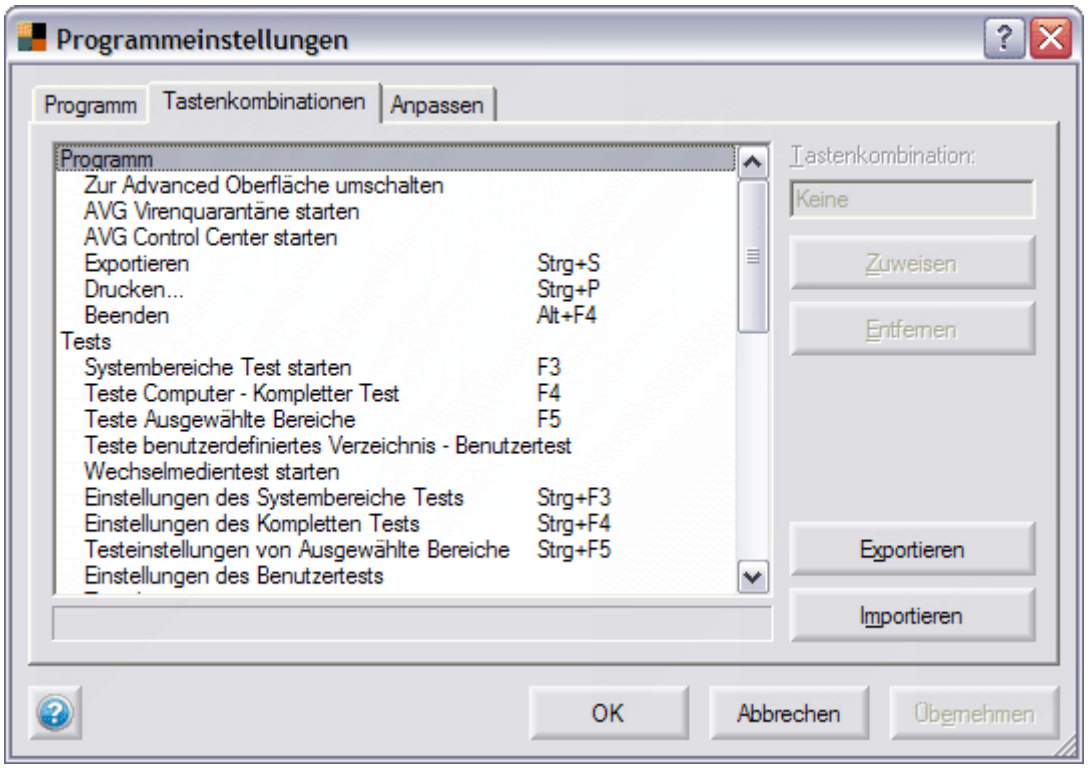
a) Programm

- 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



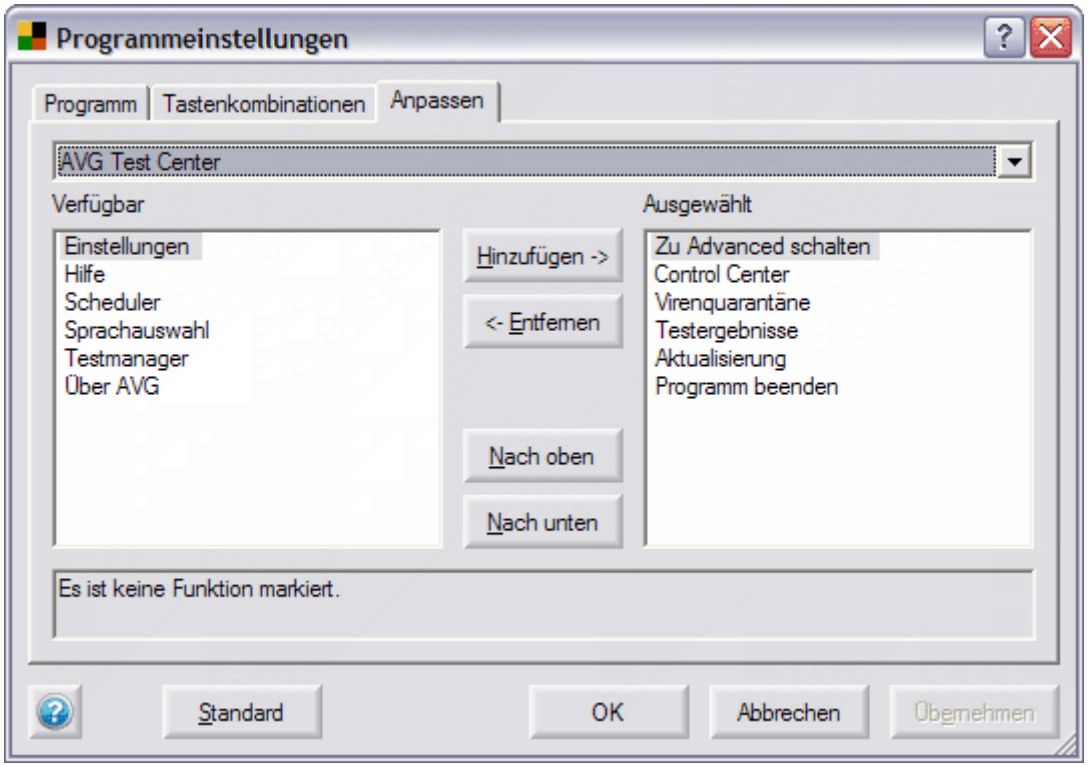
b) Tastenkombinationen

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

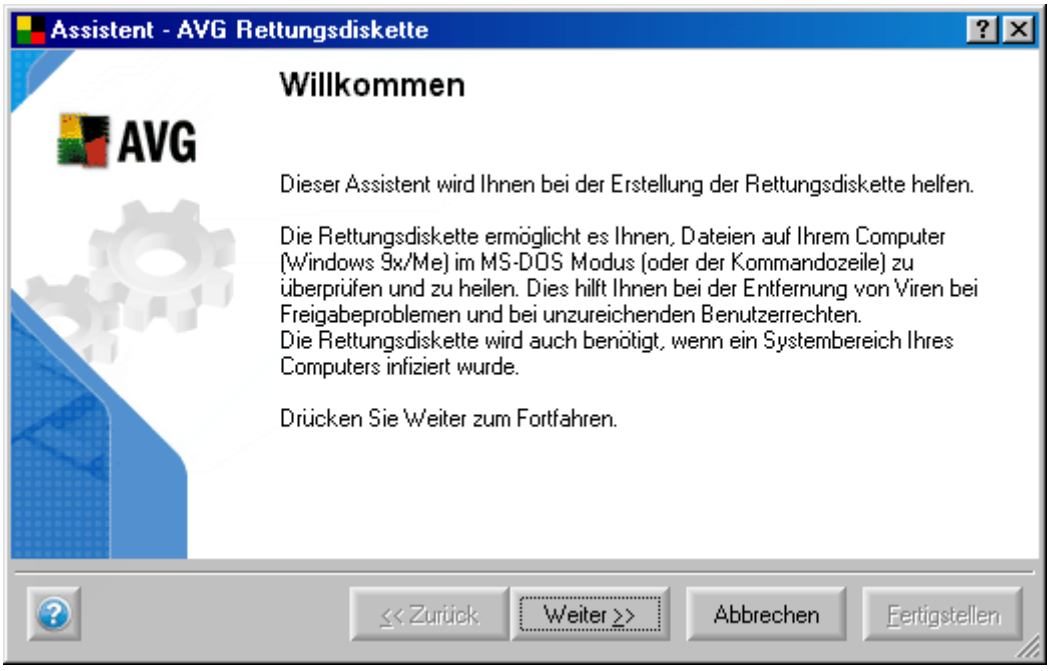
Ab Windows XP aufwärts wird dieses Feature nicht mehr unterstützt.

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

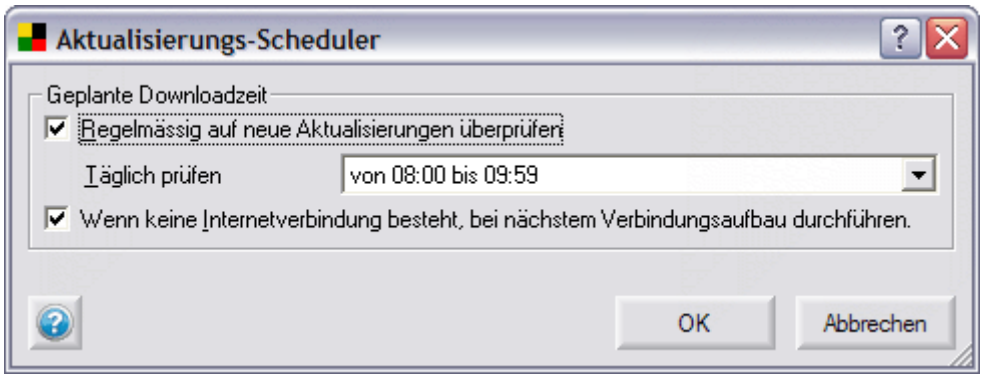
Der Menüeintrag ***Rettungsdiskette*** ruft einen Assistenten auf, der Sie durch den Erstellungsprozess einer Rettungsdiskette führen wird. Um die Rettungsdiskette zu erstellen, folgen Sie den Anweisungen des Assistenten:



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

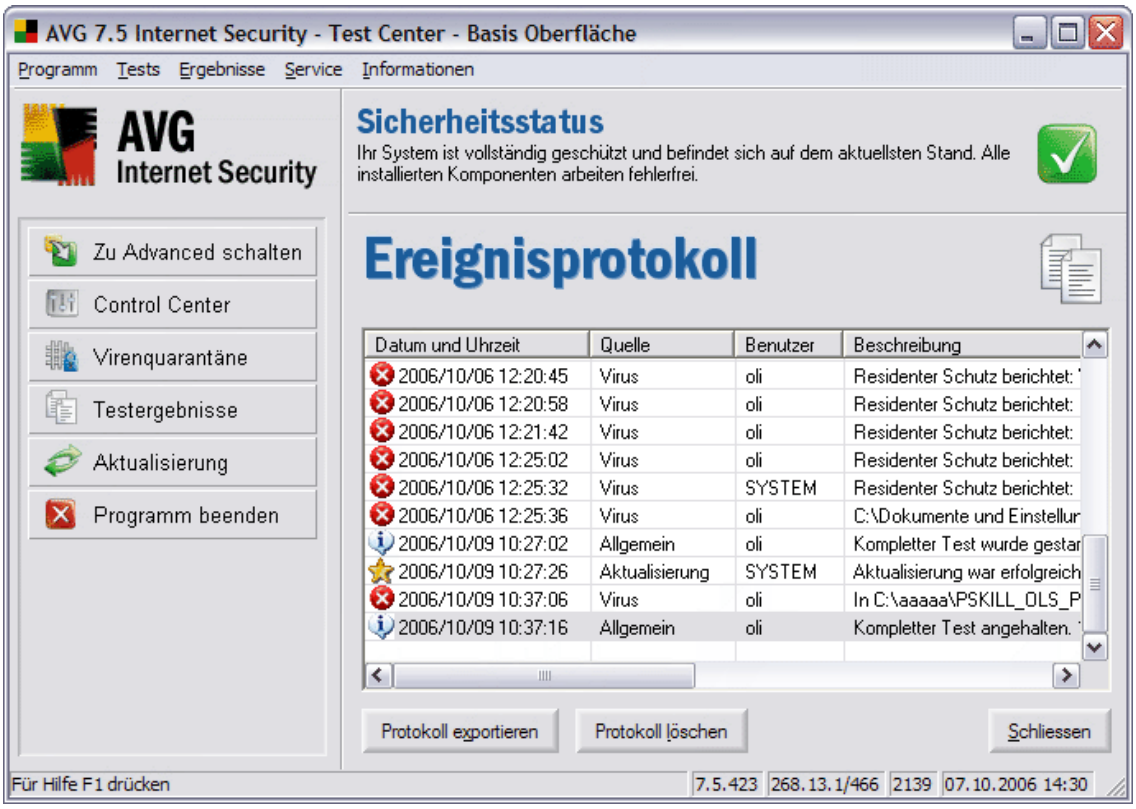
Service / Ereignisprotokoll

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.

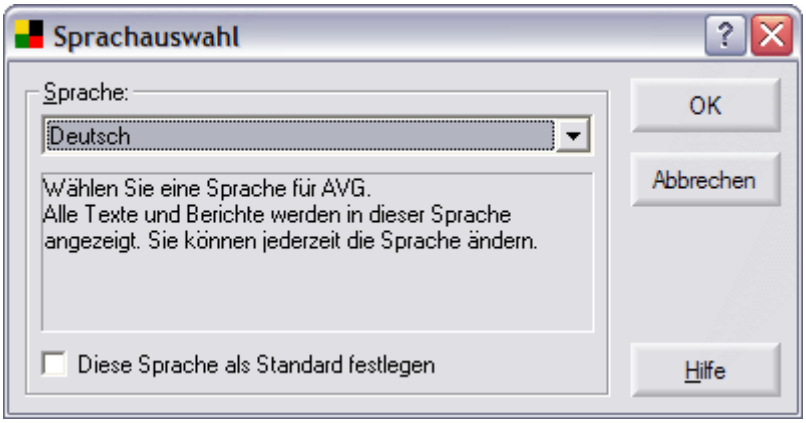


7.13. Sprachauswahl

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.*

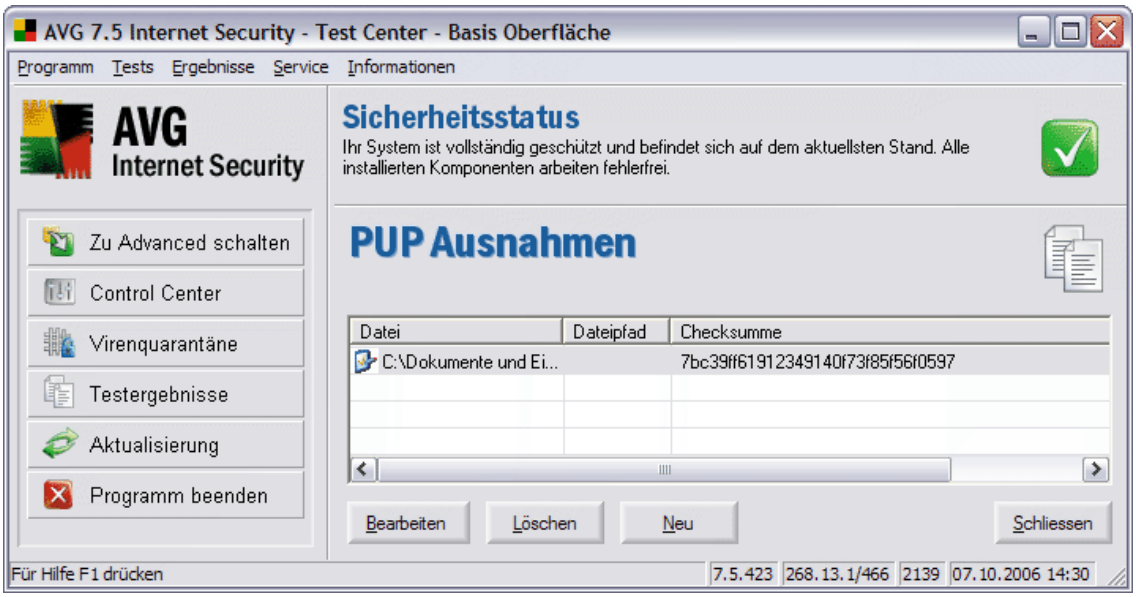


7.14. Potentiell unerwünschte Programme - Ausnahmen

Service / Potentiell unerwünschte Programme - Ausnahmen

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

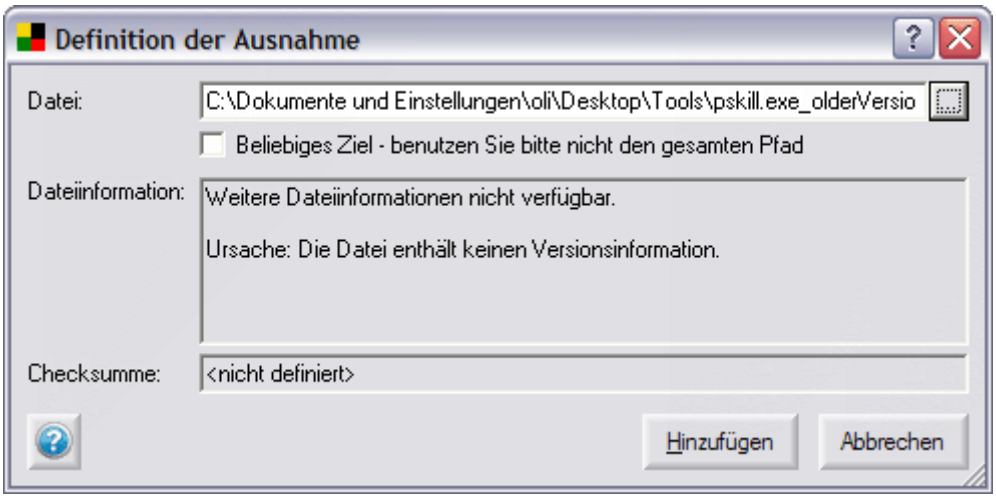
AVG kann ausführbare Anwendungen oder DLL-Bibliotheken, die innerhalb des Systems als potentiell unerwünscht angesehen werden, erkennen und analysieren. In einigen Fällen kann es vorkommen, dass der Benutzer bestimmte unerwünschte Programme auf dem Computer behalten möchte (Programme, die absichtlich 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.

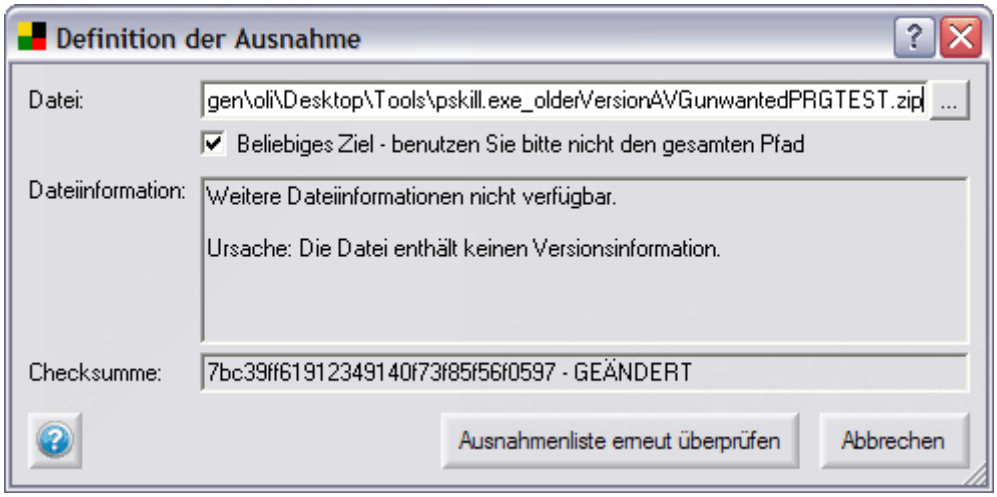
Falls zusätzliche Informationen über diese Datei verfügbar sind (Lizen/Versionsinformationen usw.), werden diese im Bereich ***Dateiniformation*** angezeigt.

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:



Währen 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

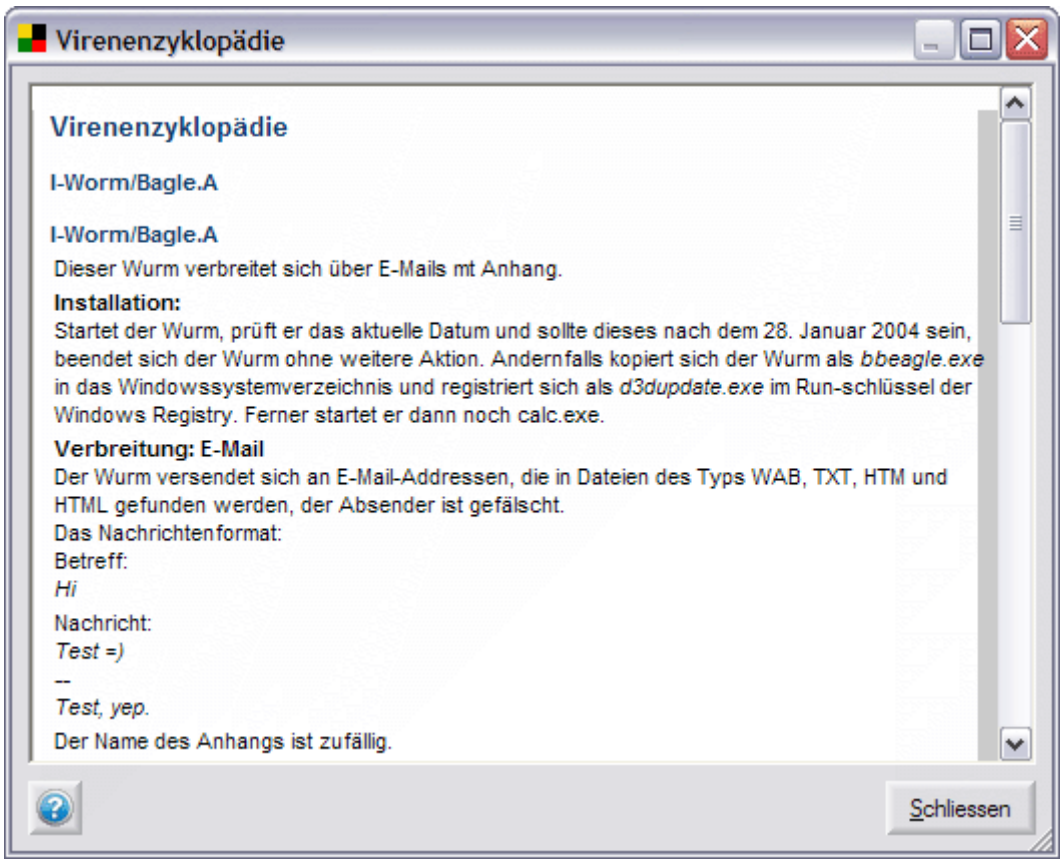
Beide Optionen öffnen ein Fenster mit fünf Reitern, die Informationen zu AVG bieten:

- ***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.

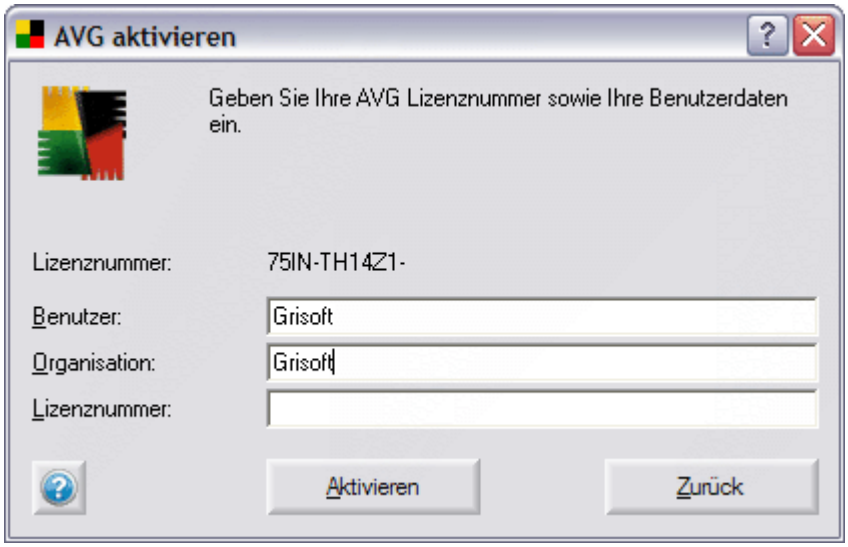
Anmerkung: *Das Hilfsprogramm AVG Diagnose sendet niemals persönliche oder andere sensible Daten von Ihrem Computer weiter, ohne besonderes Einverständnis des Benutzers. Der Benutzer kann den Inhalt aller gesammelten Dateien überprüfen und verhindern, dass diese an den technischen Support gesendet werden.*

d) Registrieren im Internet

Diese Option öffnet die AVG Registrierungs- Webseite.

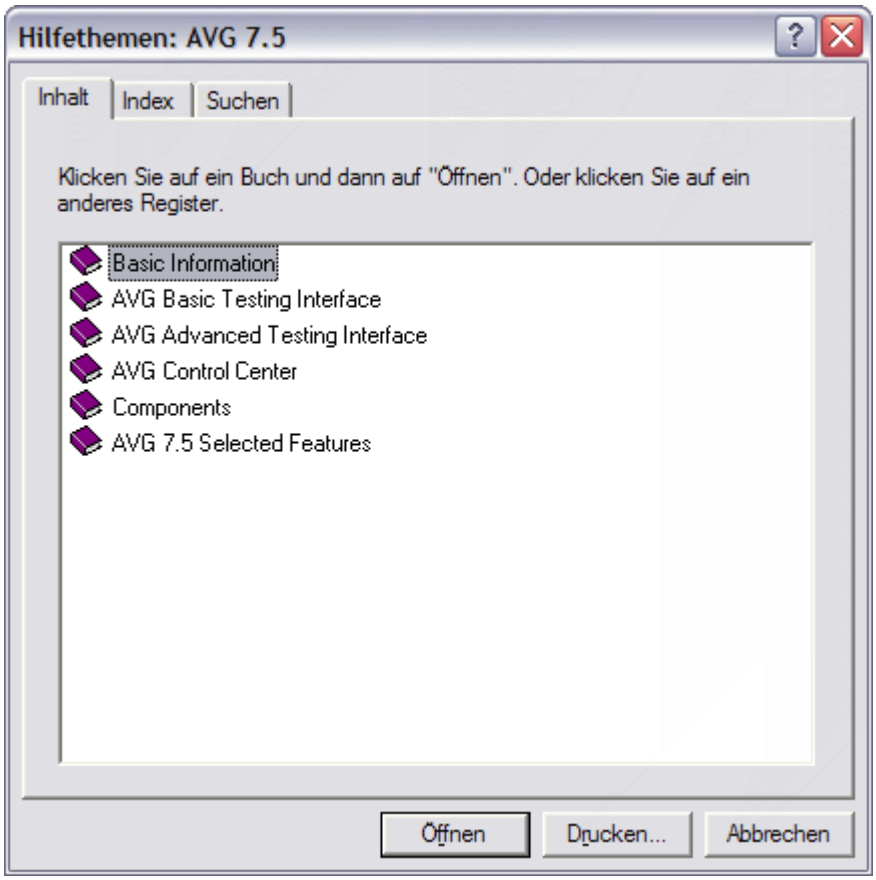
e) AVG aktivieren

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.



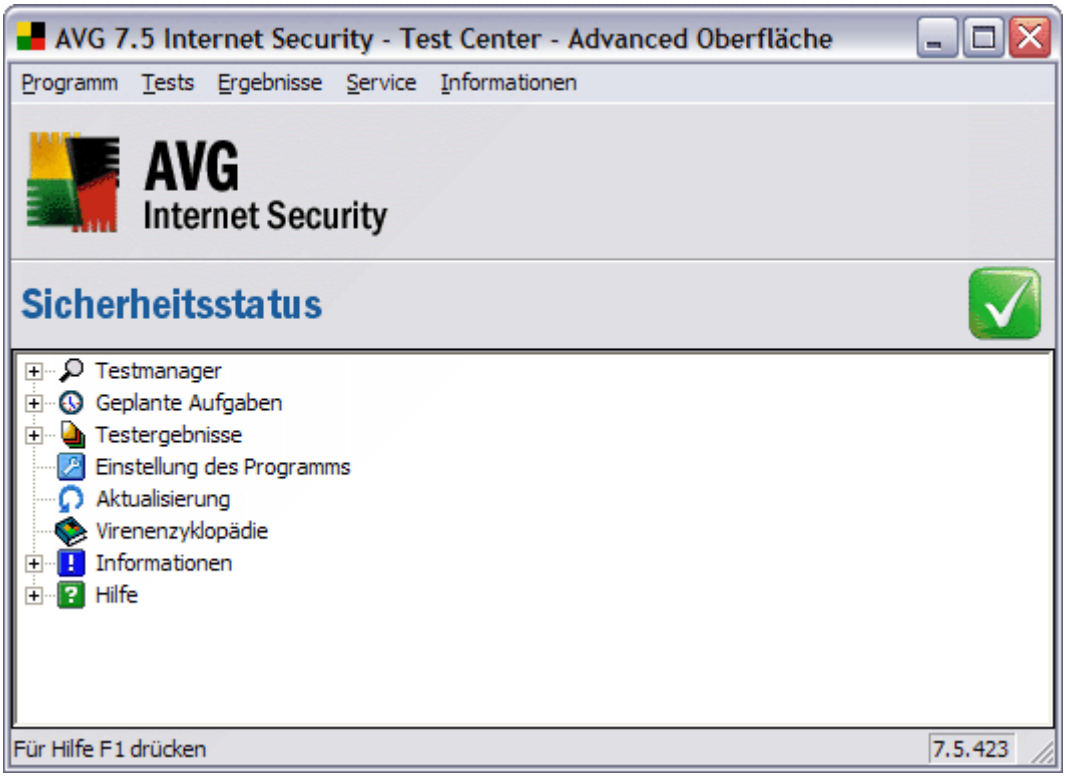
g) Hilfe zu AVG

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

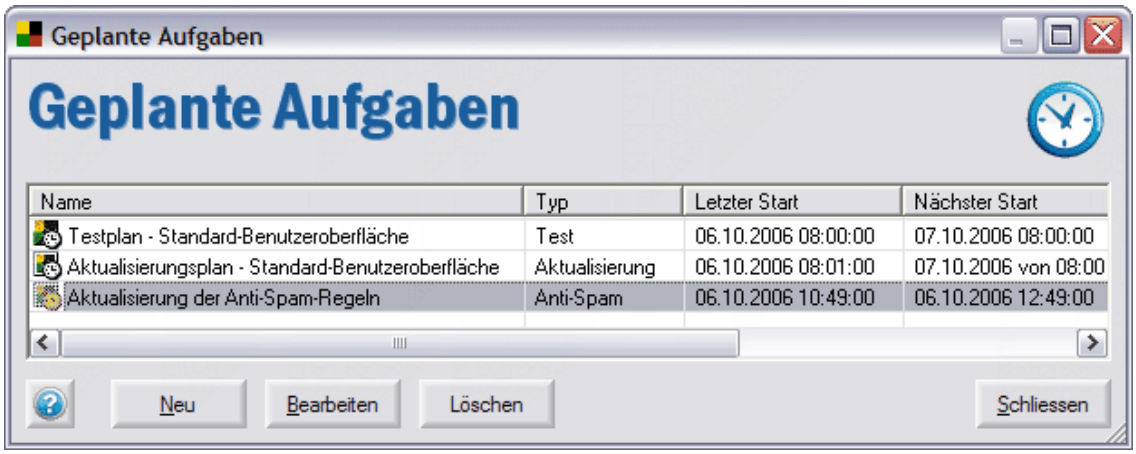
Der Abschnitt ***Testmanager*** enthält eine Liste der vordefinierten Tests, die mit AVG durchgeführt werden können. Sie können jeden dieser Tests von hier aus starten.

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***:



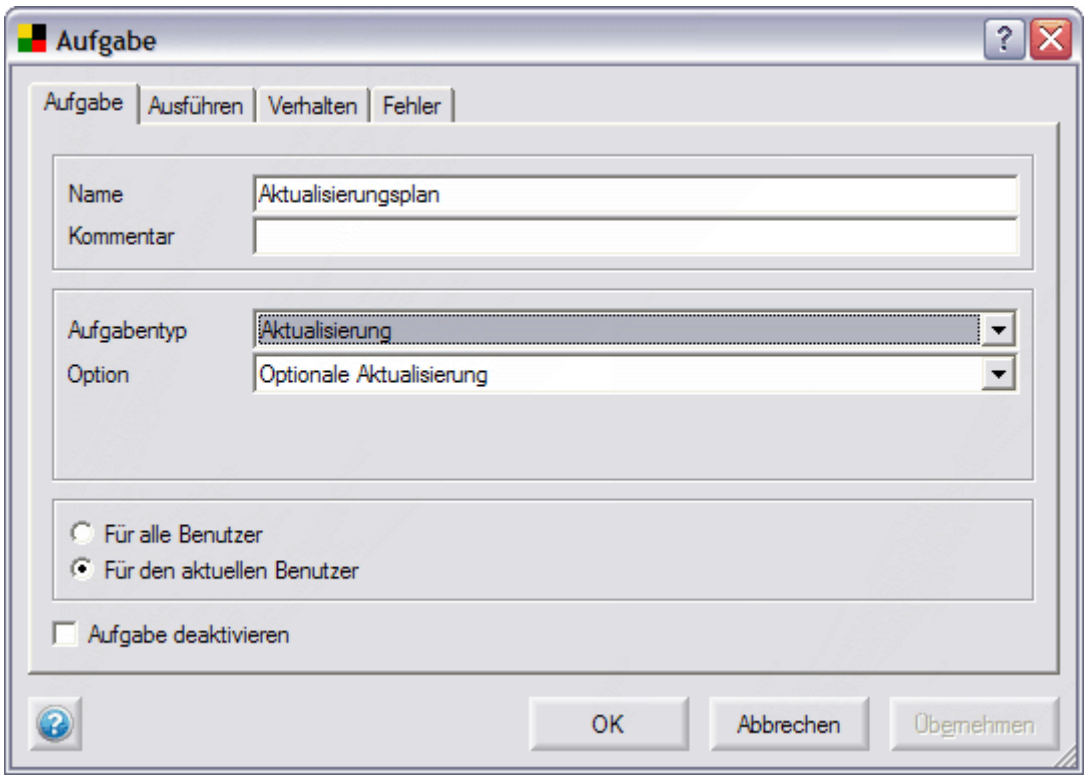
Dieses Dialogfenster bietet eine wesentlich ausführlichere Beschreibung aller geplanten Aufgaben:

- 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

- o ***Verhalten*** – Entscheidung, ob Sie informiert werden möchten, bevor die Aufgabe gestartet wird
- o ***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***.

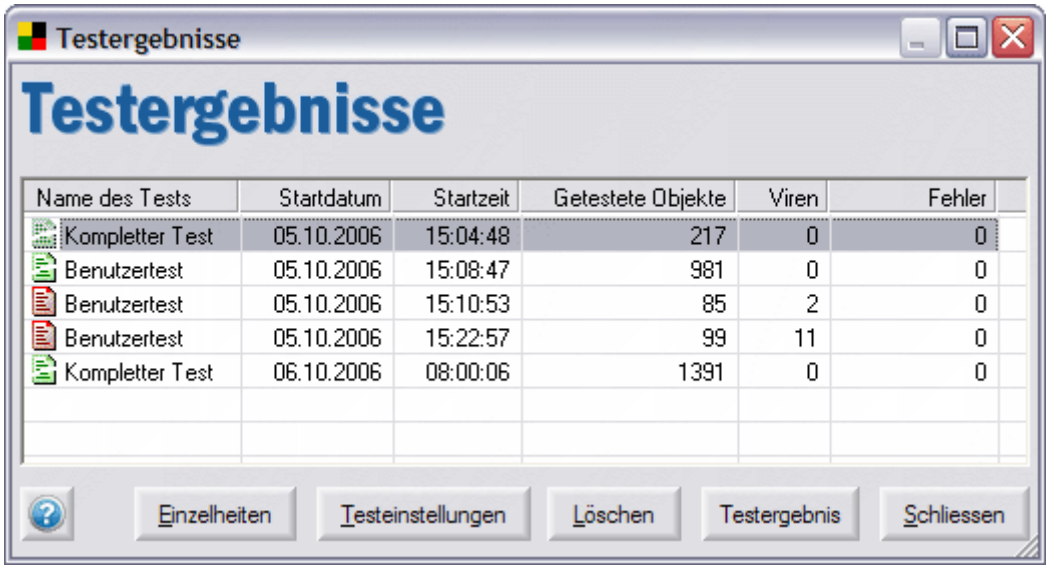
d) Schliessen

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:



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

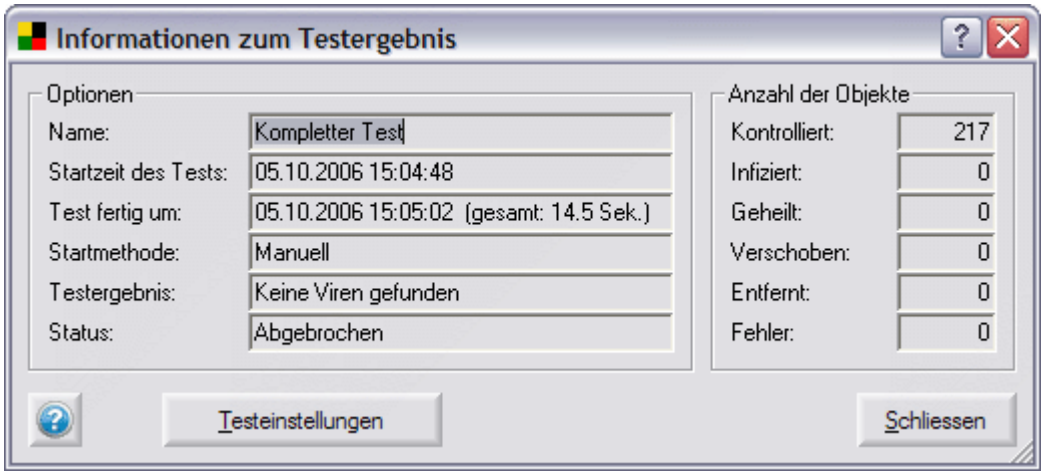
- **Viren** – Anzahl der gefundenen Viren (sollte ein Virus während des Tests gefunden worden sein, so erscheint das Testsymbol in rot; sollte der Test unterbrochen worden sein, dann erscheint das Testsymbol zerrissen)
- **Fehler** – Anzahl der Fehler, die während des Testdurchlaufs aufgetreten sind

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:

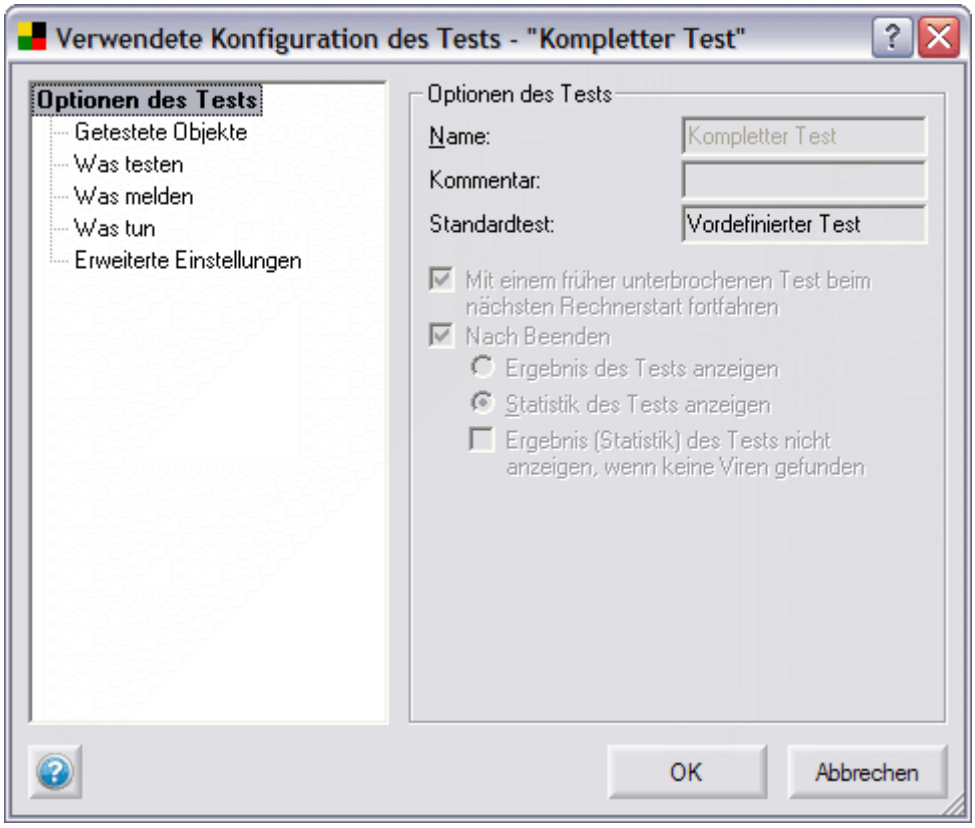


b) Testeinstellungen

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.*

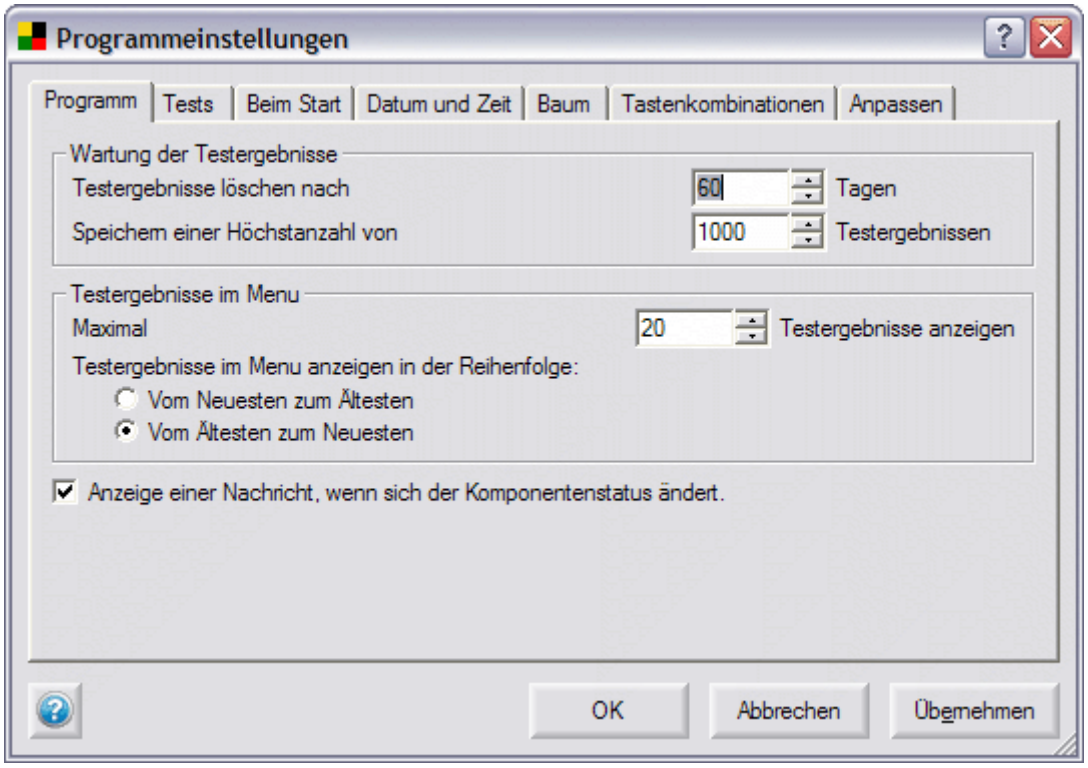
8.4. Programmeinstellungen

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

a) *Programm*

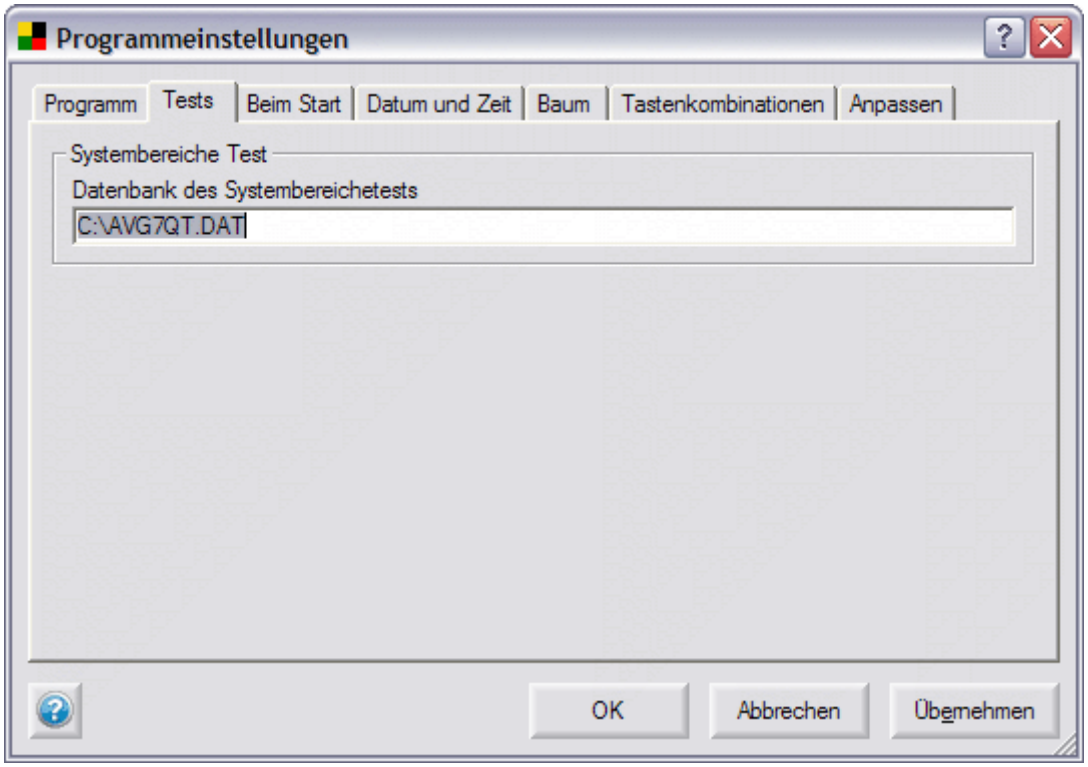
- *Wartung der Testergebnisse*
  - ***Testergebnisse löschen nach*** – geben Sie an, wie lange Sie die Testergebnisse speichern möchten
  - ***Speichern einer Höchstanzahl von*** – geben Sie an, wie viele der letzten Testergebnisse Sie speichern möchten
- *Testergebnisse im Menü*
  - ***Maximal*** – 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***.



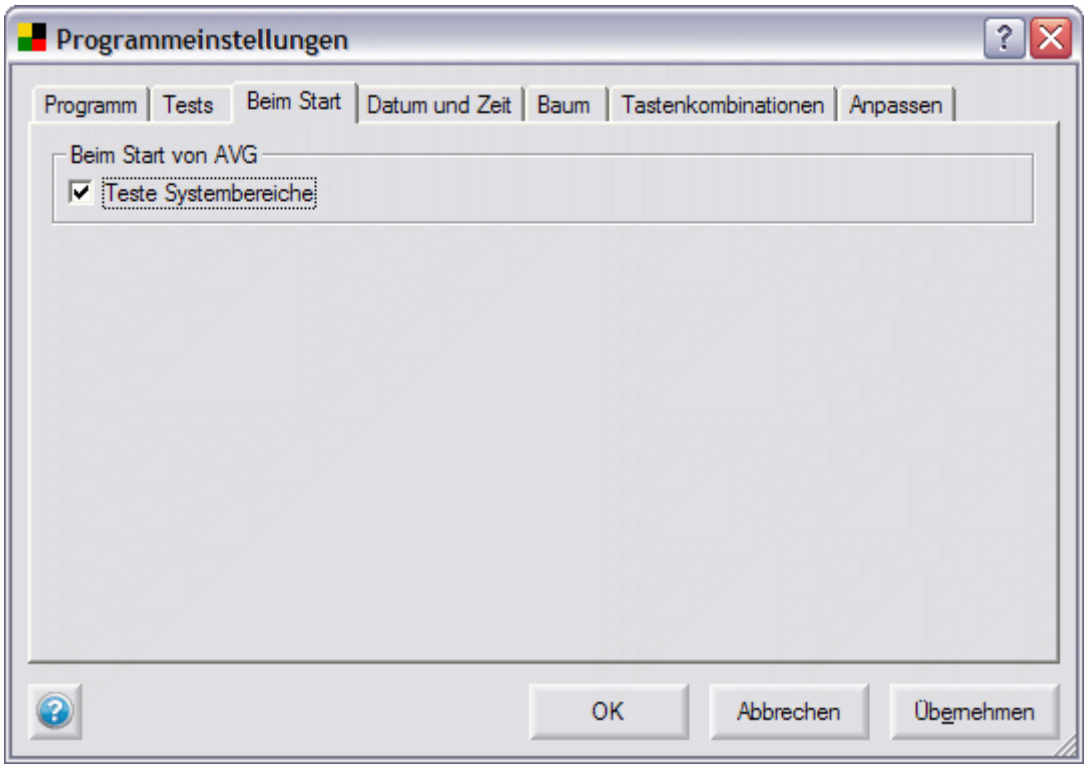
b) *Tests*

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



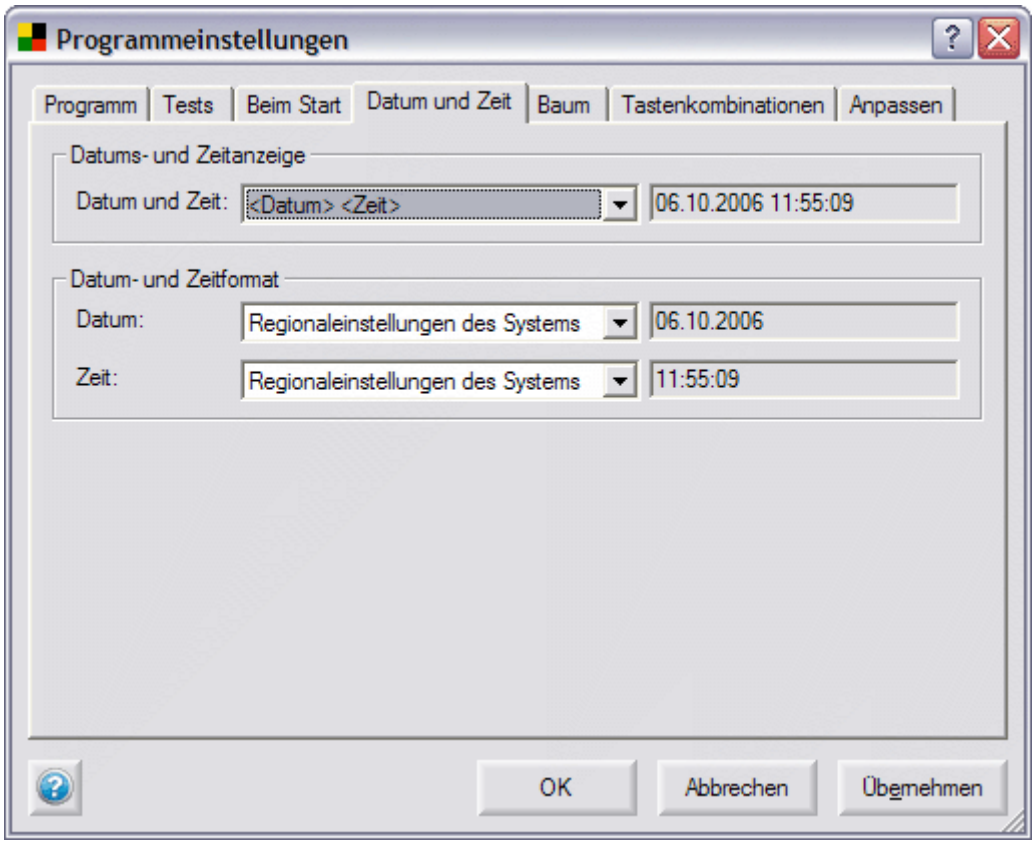
c) Beim Start

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

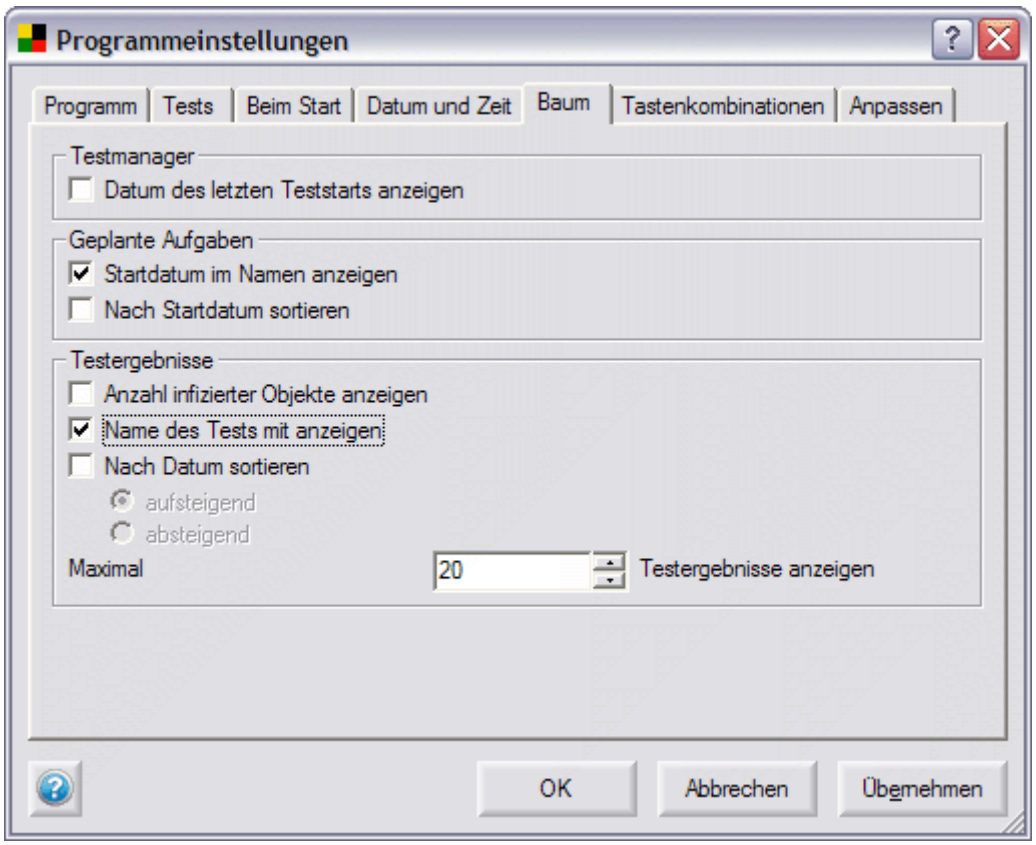


d) Datum und Zeit

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



e) Baum

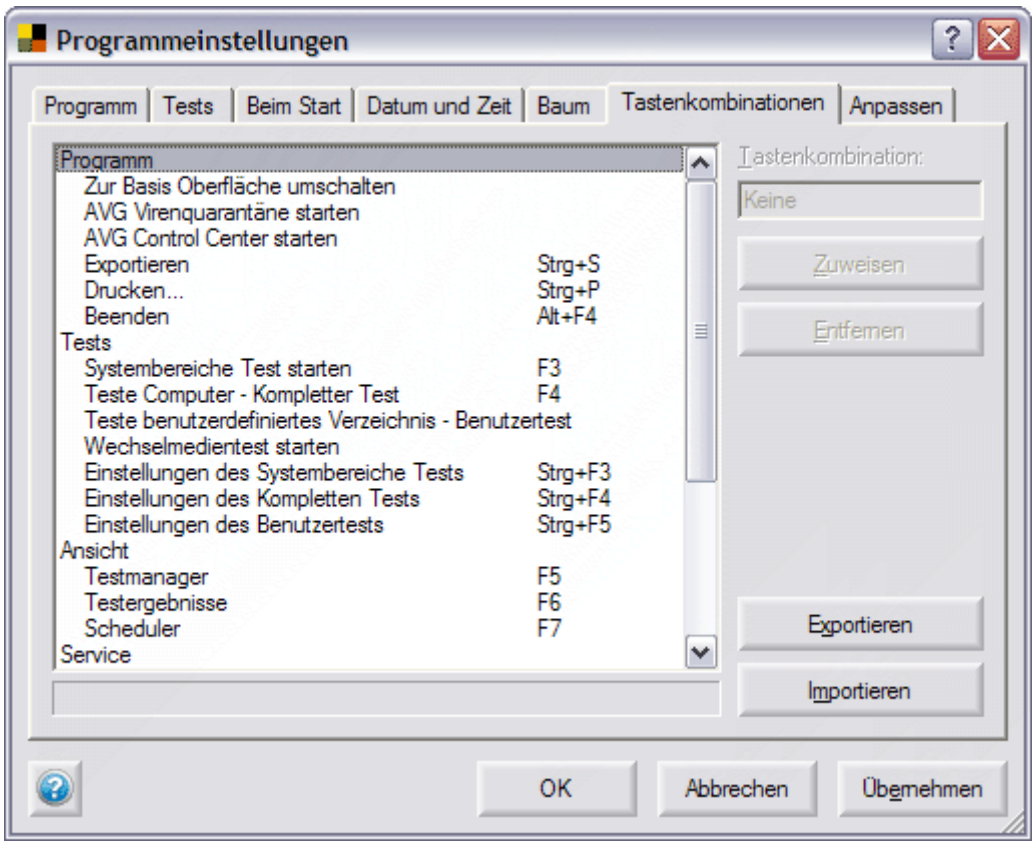


- Zweig ***Testmanager***
  - ***Datum des letzten Teststarts anzeigen*** – im Menü der ***Advanced Oberfläche*** aktivieren/deaktivieren Sie die Anzeige des letzten Startdatums
- Zweig ***Geplante Aufgaben***
  - ***Startdatum im Namen anzeigen -*** aktivieren/deaktivieren Sie die Anzeige des Datums 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

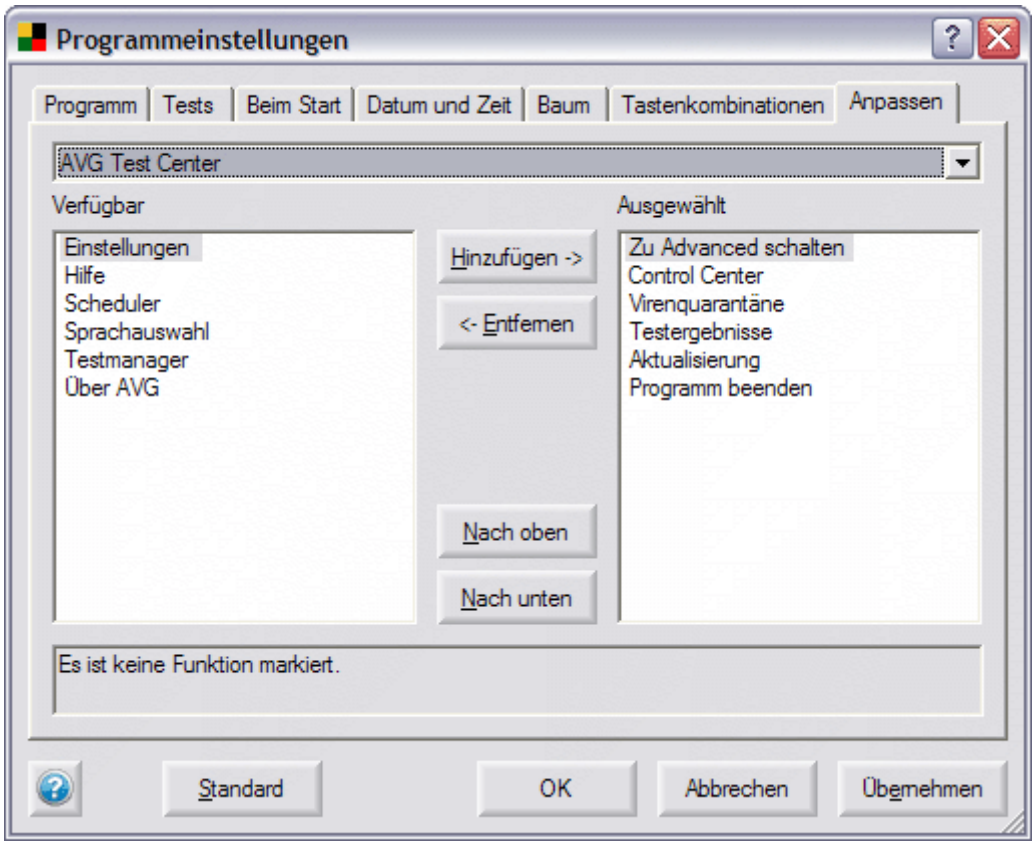
Der Reiter ***Tastenkombinationen*** erlaubt Ihnen das Einrichten eigener Tastenkombinationen mit Hilfe der folgenden Schaltflächen:

- ***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:



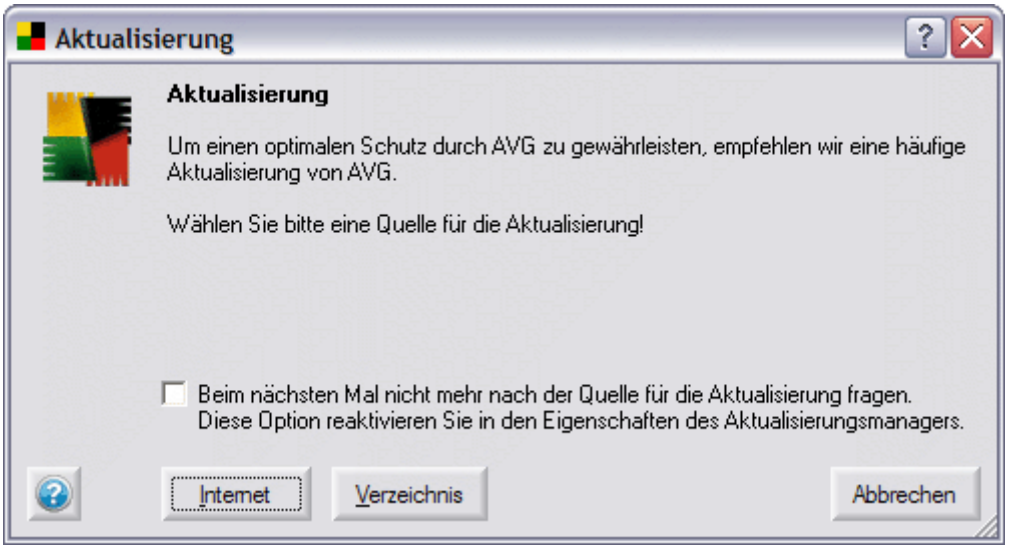
Verschiedene Reiter bieten die folgenden Schaltflächen an:

- ***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 **Aktualisierungs**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**.

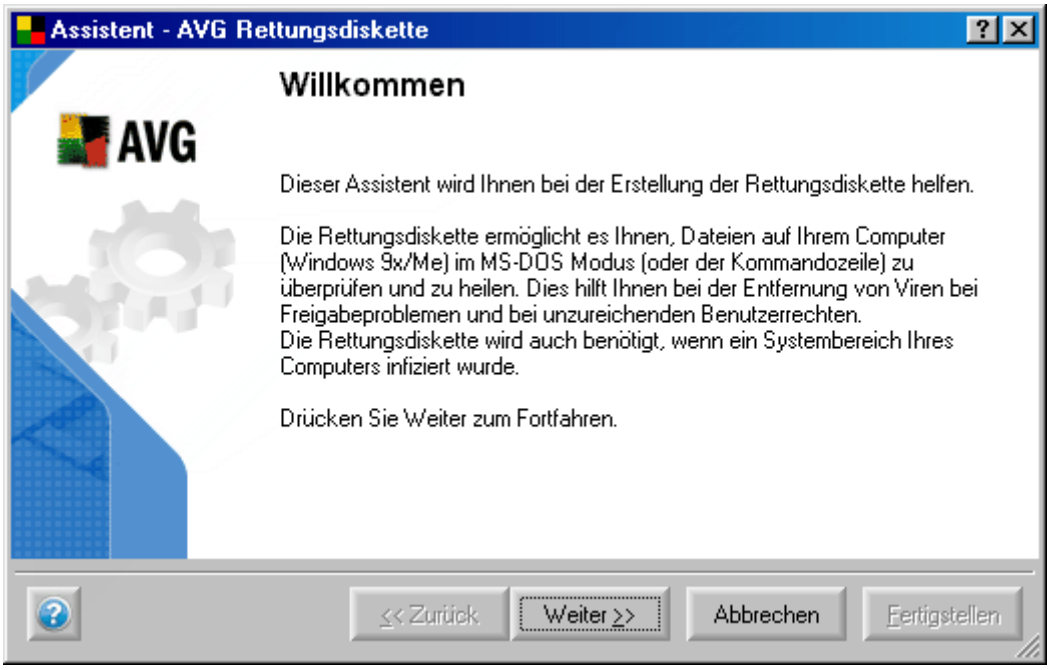
8.6. Rettungsdiskette

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

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

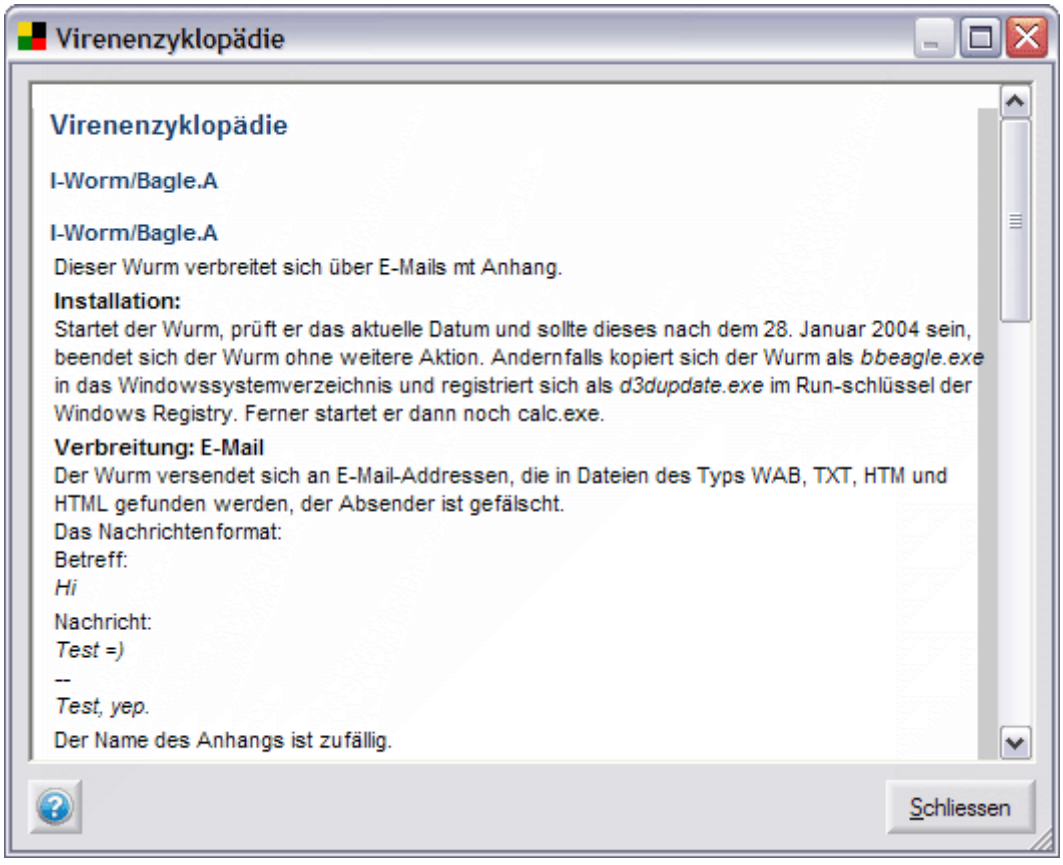
- der Freigabeprobleme besitzt
- für den Sie nicht die entsprechenden Zugriffsrechte besitzen
- bei dem die Systembereiche infiziert sind

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

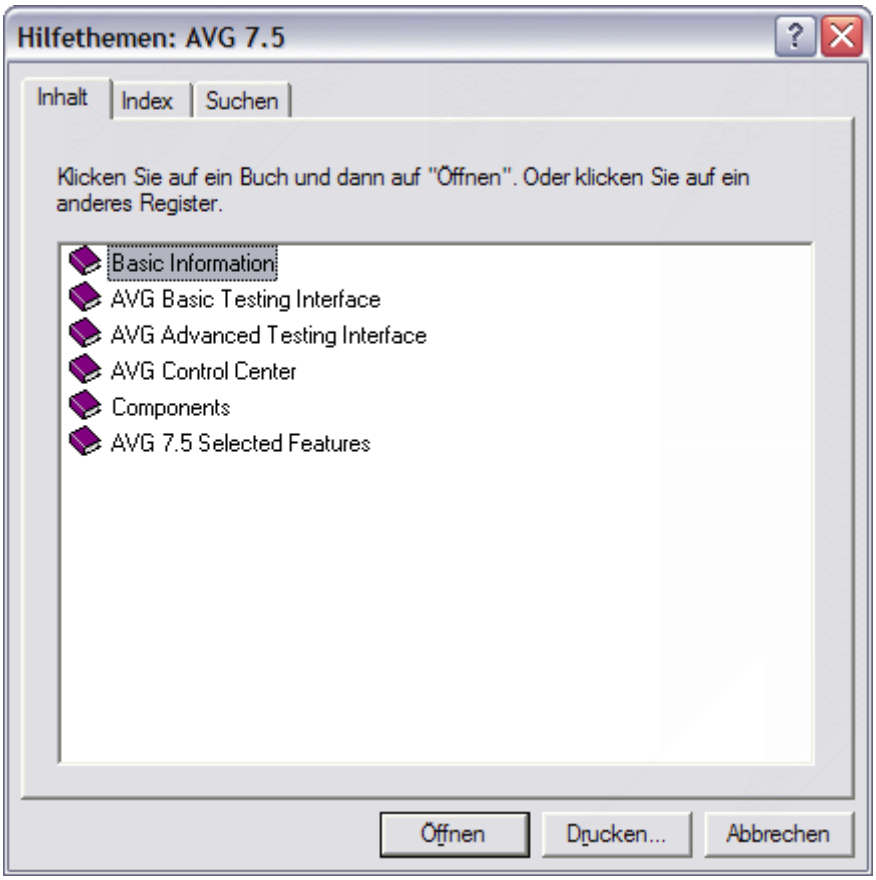
Der Menüeintrag ***Informationen*** enthält eine Liste von Untereinträgen, die sich auf spezielle Reiter des neu geöffneten Dialogfensters mit AVG-Informationen bezieht:

- **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 Anti-Virus plus Firewall 7.5** 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**.

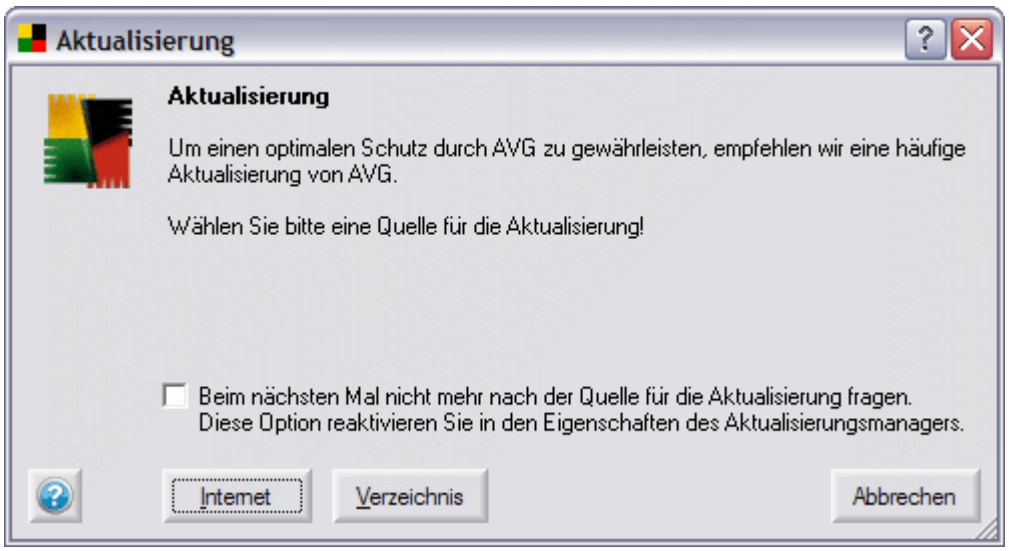
Für Details zur Basis/Advanced Oberfläche lesen Sie bitte die Kapitel 7. AVG Basic Oberfläche und 8. AVG Advanced Oberfläche.)

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***



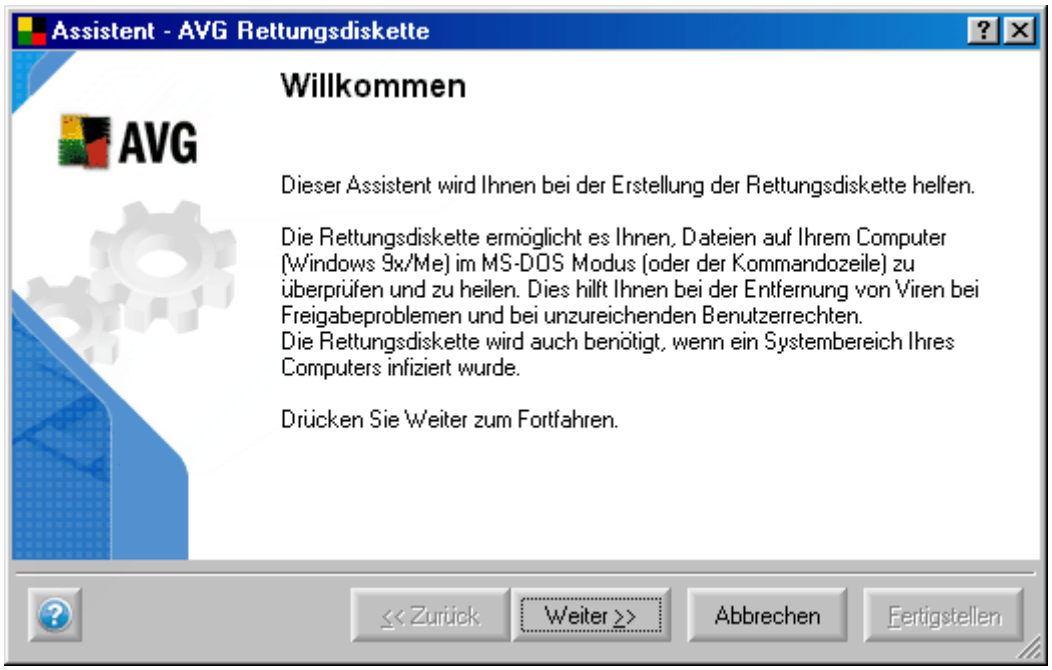
In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- ***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

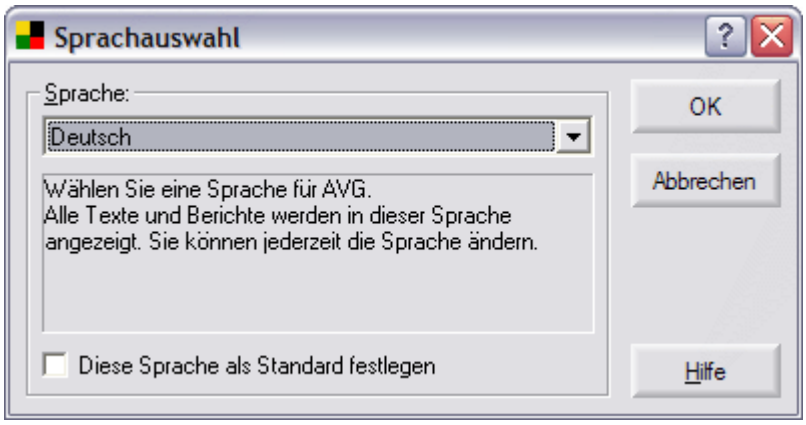
Der Menüeintrag ***Rettungsdiskette*** öffnet das Fenster des ***Assistenten*** zur Erstellung der ***Rettungsdiskette:***



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.



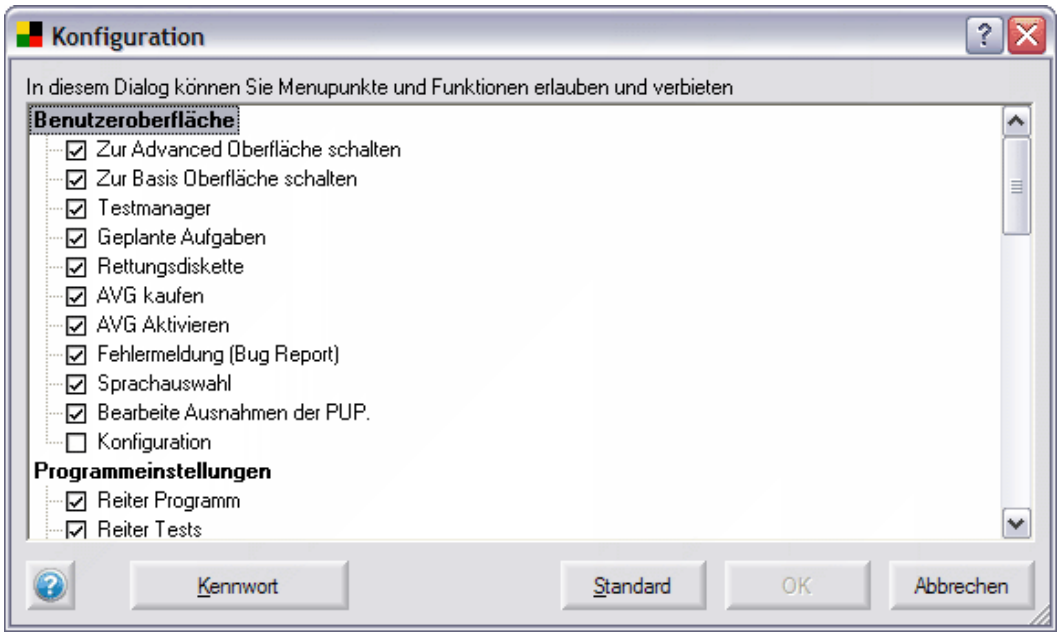
Anmerkung: Wenn Sie nur Englisch installiert haben, steht diese Schaltfläche nicht zur Verfügung.

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:

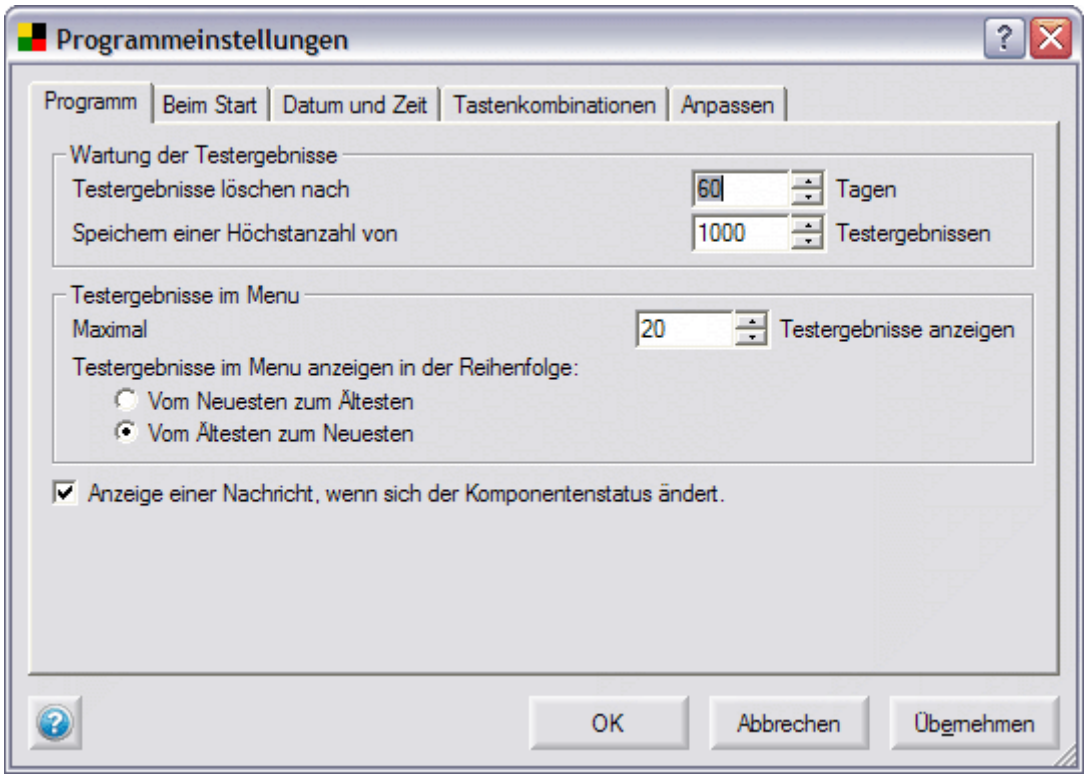
- ***Kennwort*** – definieren und bestätigen Sie ein Kennwort, das den Zugang zur Bearbeitung der **Administrator- Optionen** sichert.
- ***Standard*** – stellt die Administratoroptionen wieder auf die Standardwerte
- ***OK*** – akzeptiert alle vorgenommen Änderungen und schließt den Dialog
- ***Abbrechen*** – 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
-
- Firewall
- Scheduler
- Residenter Schutz
- Virenquarantäne
- Aktualisierungsmanager
- Shell-Erweiterung
- eMail-Kontrolle
- Lizenzbedingungen

9.7. Control Center – Anti-Virus

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

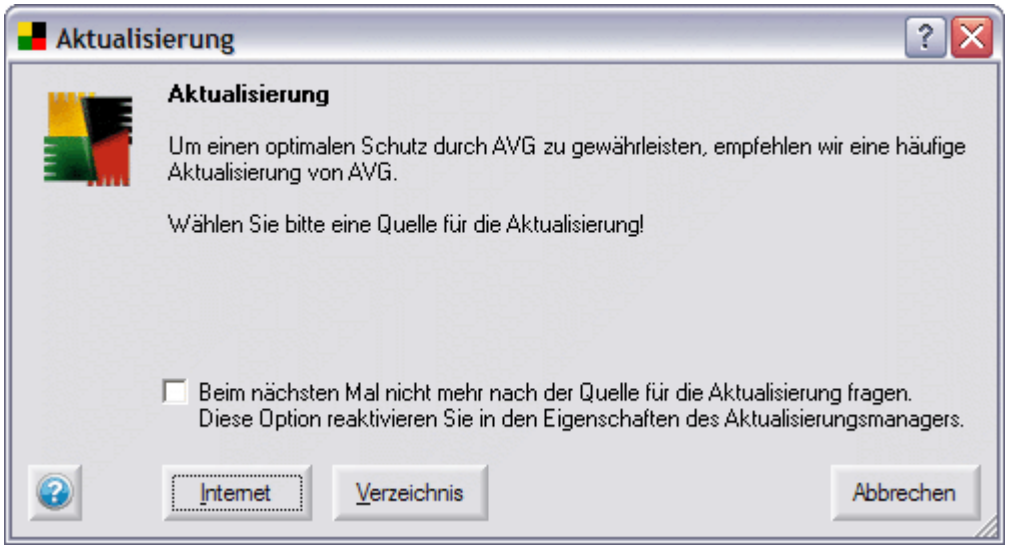
Wichtig: *Wenn die Virendatenbank älter als 7 Tage ist, wird sie als veraltet angesehen. Um dieses anzuzeigen, ändert die Komponente ihren internen Status auf fehlerhaft und wird rot angezeigt. Bitte bedenken Sie, dass ein verlässlicher Virenschutz nur erreicht werden kann, wenn Ihr Virenschutz-System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

Die Komponente **Anti-Spyware** gehört nicht zum Umfang **AVG Anti-Virus plus Firewall Edition.**

Sie ist Bestandteil dieser Editionen:

- AVG Internet Security
- AVG Anti-Malware
- AVG Anti-Spyware

Weitere Informationen finden Sie im Internet auf www.grisoft.de unter Prokukte.

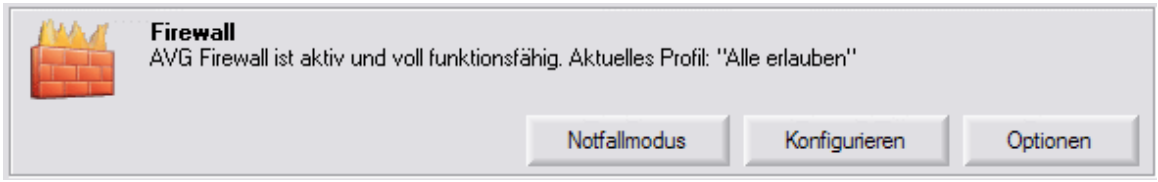
9.9. Control Center – Anti-Spam

Die Komponente ***Anti-Spam*** überprüft alle eingehenden eMails und markiert unerwünschte eMals als SPAM. Sie nutzt verschiedene Analyse-Methoden für die Bearbeitung jeder einzelnen eMail und bietet einen maximalen Schutz gegen unerwünschte eMails.

Sie fordert nur wenige Einstellungen während dem Benutzer ermöglicht wird, verschiedene Anti-Spam- Optionen anzupassen. Weitere Informationen zum Feature ***Anti-Spam*** erhalten Sie in

Die Komponente Anti-Spam ist in diesem Produkt nicht enthalten. Weitere Informationen zum Feature Anti-Spam erhalten Sie imKapitel 11. Anti-Spam.

9.10. Control Center - Firewall

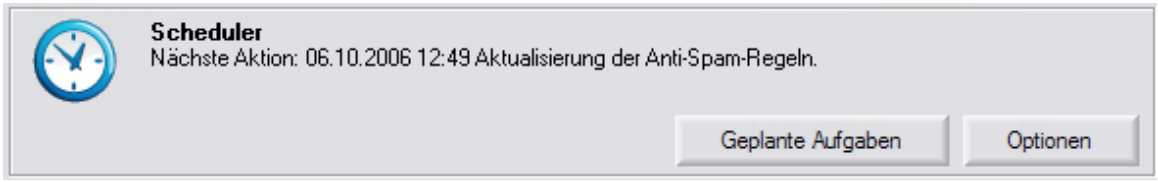


Die Komponente ***Firewall*** kontrolliert den gesamten Verkehr auf jedem Netzwerk-Port Ihres Computers. Basierend auf den definierten Regeln unterscheidet die **Firewall** Anwendungen, die entweder auf Ihrem Computer laufen und sich mit dem Netzwerk verbinden wollen (entweder mit dem lokalen Netzwerk oder dem Internet) und Anwendungen, die versuchen, Ihren Computer von außen zu erreichen. Die **Firewall** kann anschließend für jede Anwendung festlegen, ob die Kommunikation über die Netzwerk-Ports erlaubt oder verboten werden soll.

Weitere Informationen über die Features der **Firewall** und zu den Einstellungen erhalten Sie in Kapitel 10 Firewall

9.11. Control Center - Scheduler

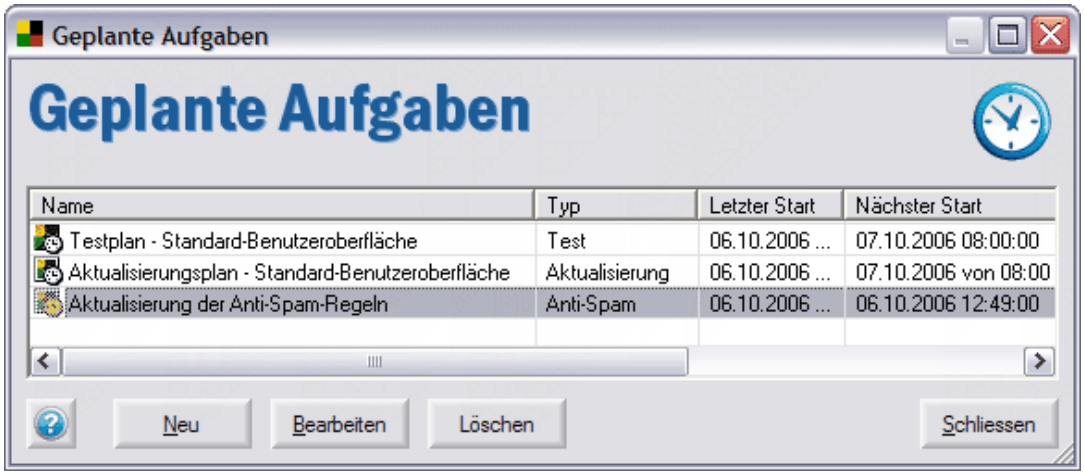
Der ***Scheduler*** kontrolliert geplante Aufgaben, wie das Aktualisieren und Tests.



Die Schaltflächen im ***Scheduler*** Fenster sind:

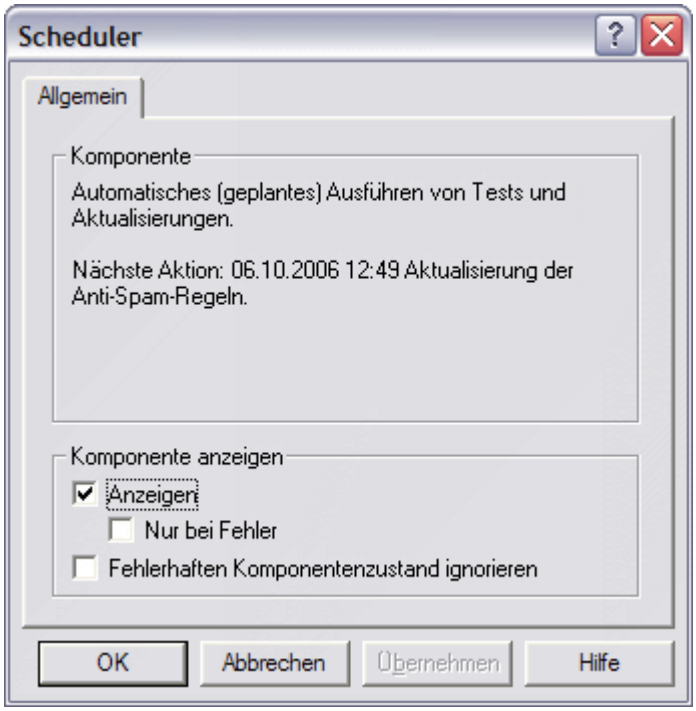
a) Geplante Aufgaben

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

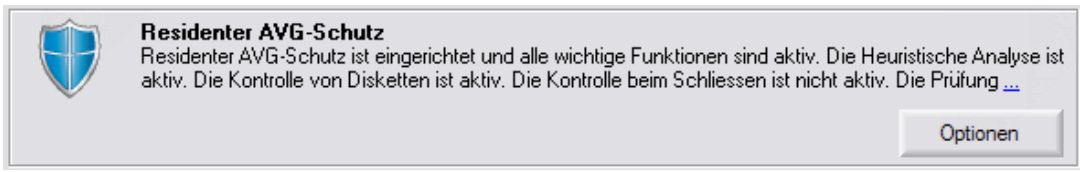
Die Schaltfläche ***Optionen*** zeigt allgemeine Informationen zur Komponente ***Scheduler*** an und lässt das Bearbeiten der Anzeige dieser Komponente zu:



9.12. Control Center - Residenter Schutz

a) Optionen des Residenten Schutzes

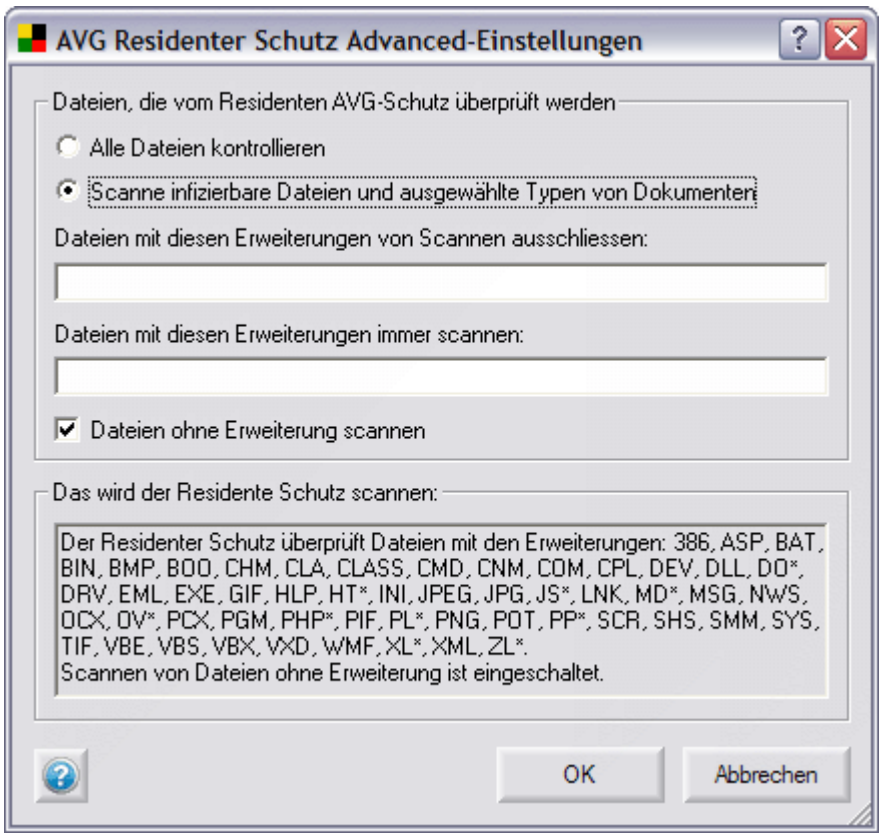
Die Komponente ***Residenter Schutz*** führt die Kontrolle auf Viren, Spyware und andere schädliche Programme von Dateien und Ordnern durch. Diese Option muss zuerst im Dialog **Optionen des Residenten Schutzes** aktiviert werden.



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:

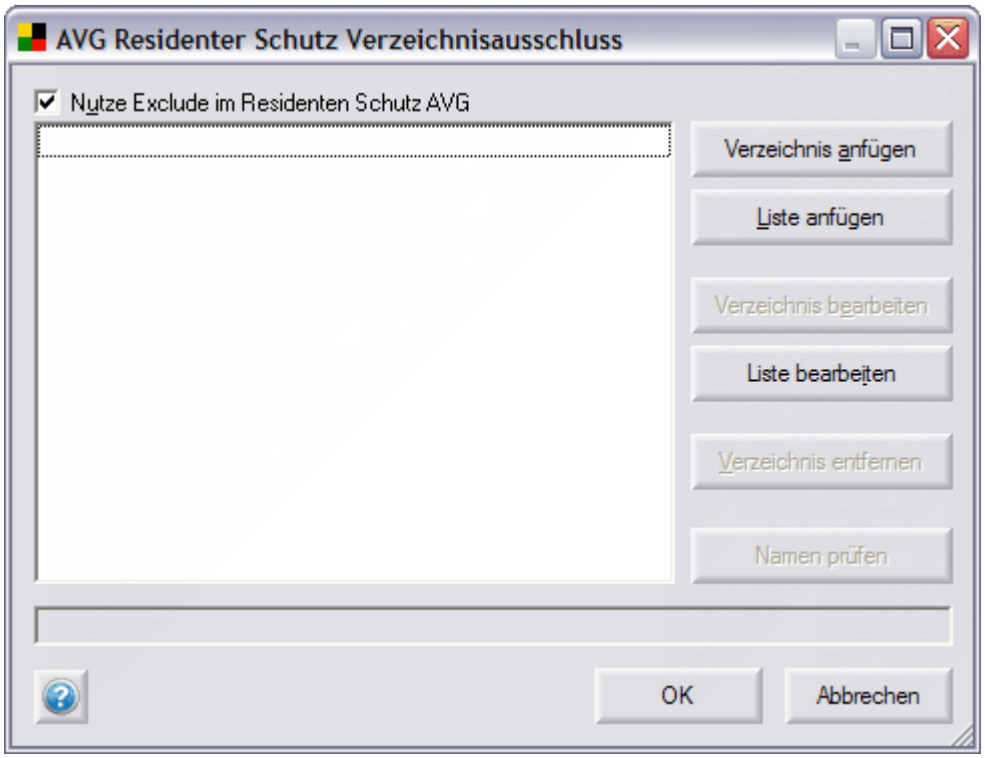
- ***Advanced Einstellungen –*** öffnet das Dialogfenster mit Optionen der ***erweiterten Einstellungen*** des ***Residenten Schutzes***. Die Überprüfung infizierbarer und weiterer ausgewählter Typen von Dokumenten kann konfiguriert werden oder Dateitypen von einer Überprüfung ausgenommen werden (nach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



o ***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:



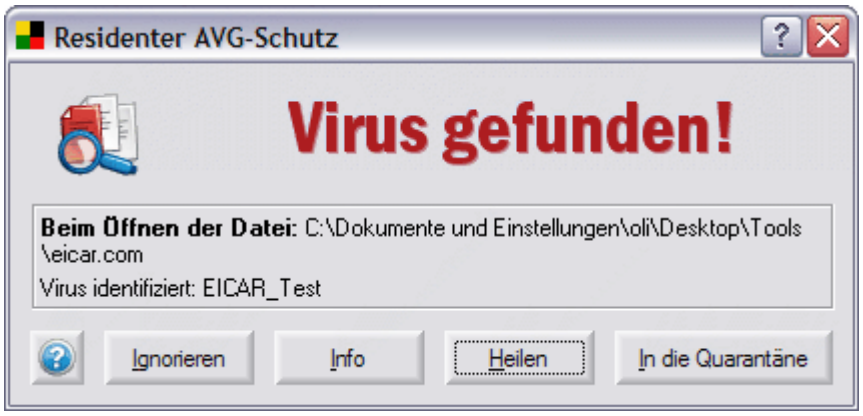
In diesem Dialogfenster stehen die folgenden Schaltflächen zur Verfügung:

- ***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

o ***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:

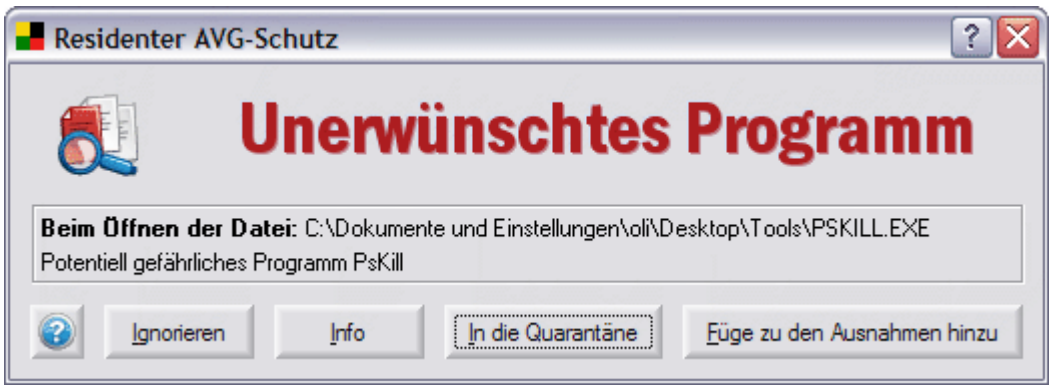


Das Dialogfenster **Residenter Schutz – Virus gefunden!** informiert Sie über den Arbeitsvorgang, bei dem die verdächtige Datei entdeckt wurde; weiterhin über den Speicherort der verdächtigen Datei und erkennt, wenn möglich, die Infektionsart (falls es sich um eine bekannte Infektion handelt). Das Dialogfenster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

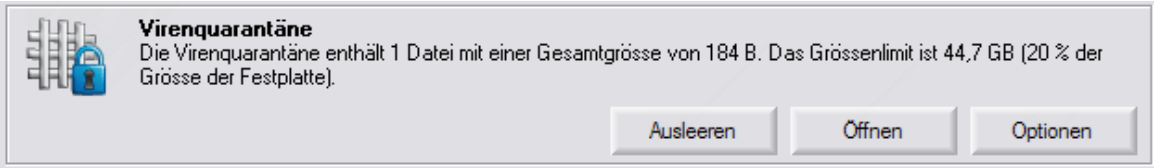


Dieser Dialog informiert Sie über den Speicherort des erkannten Potentiell unerwünschten Programms und bietet verschiedene Schaltflächen, die Sie für die weitere Bearbeitung der verdächtigen Datei nutzen können:

- ***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-Virenenzyklopädie, 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.

9.13. Control Center - Virenquarantäne

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



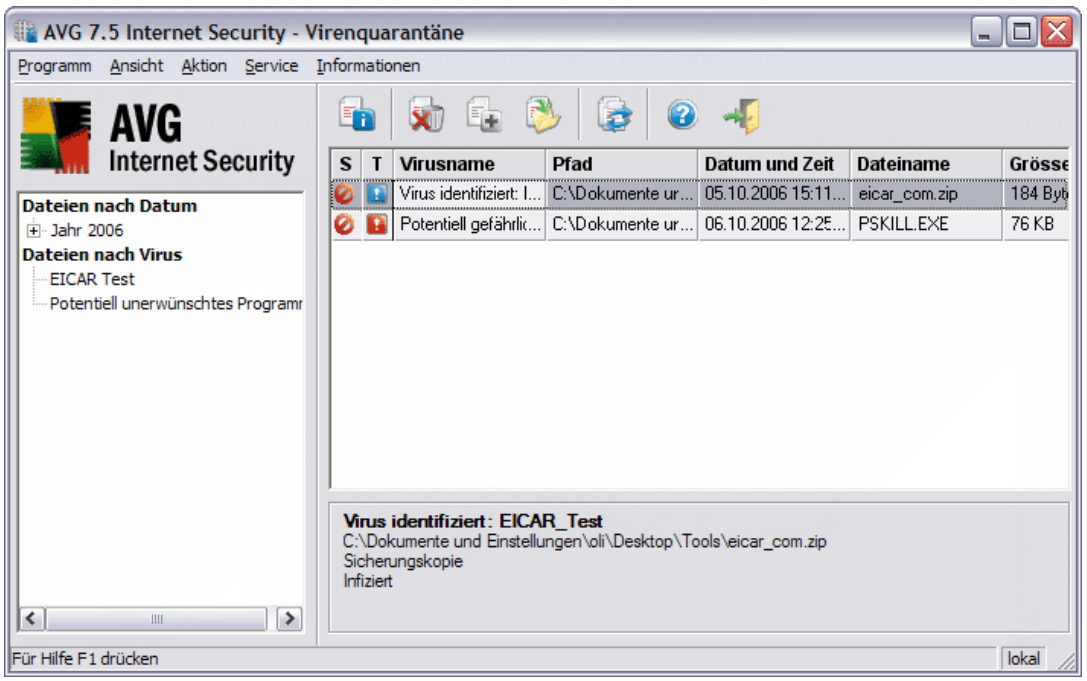
Im Bedienfeld ***Virenquarantäne*** gibt es folgende Schaltflächen:

a) Ausleeren

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

b) Öffnen

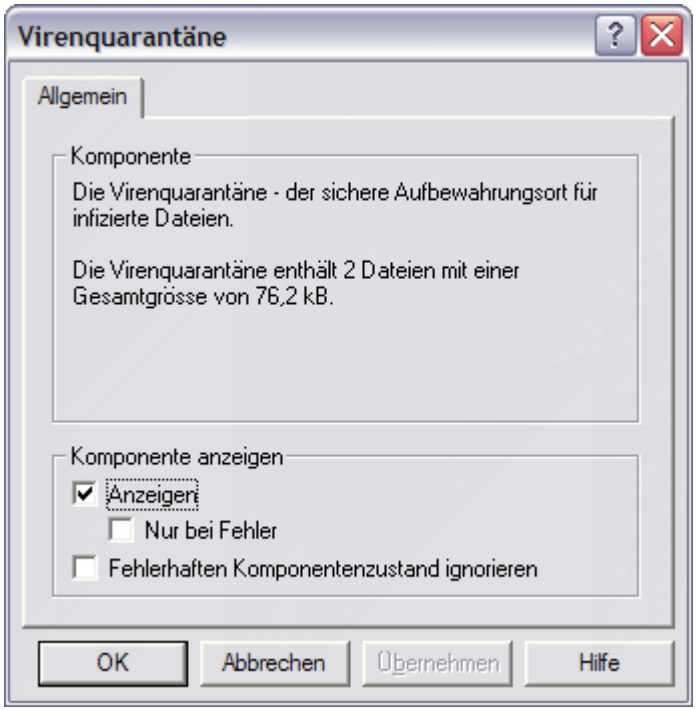
Öffnet die ***Virenquarantäne***:



Für zusätzliche Informationen zur Virenquarantäne lesen Sie bitte das Kapitel 12. Virenquarantäne.

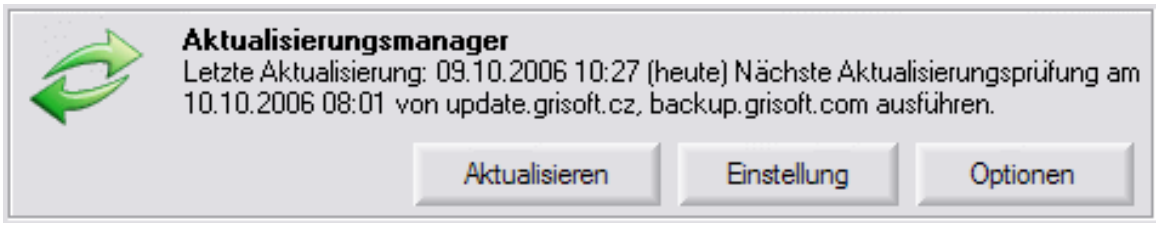
c) *Optionen*

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



9.14. AVG Control Center - Aktualisierungsmanager

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

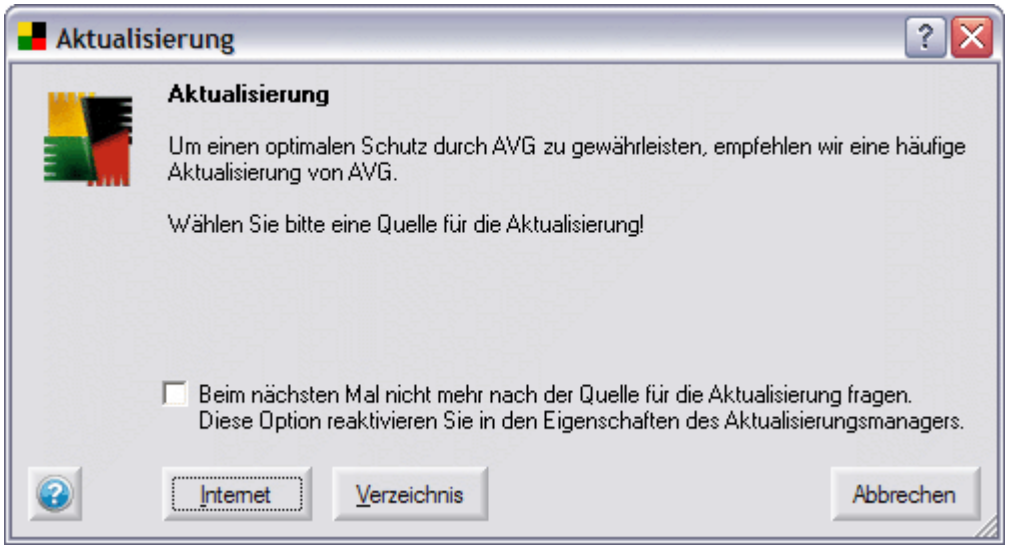


Im Bedienfeld des ***Aktualisierungsmanager*** gibt es folgende Schaltflächen:

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

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:

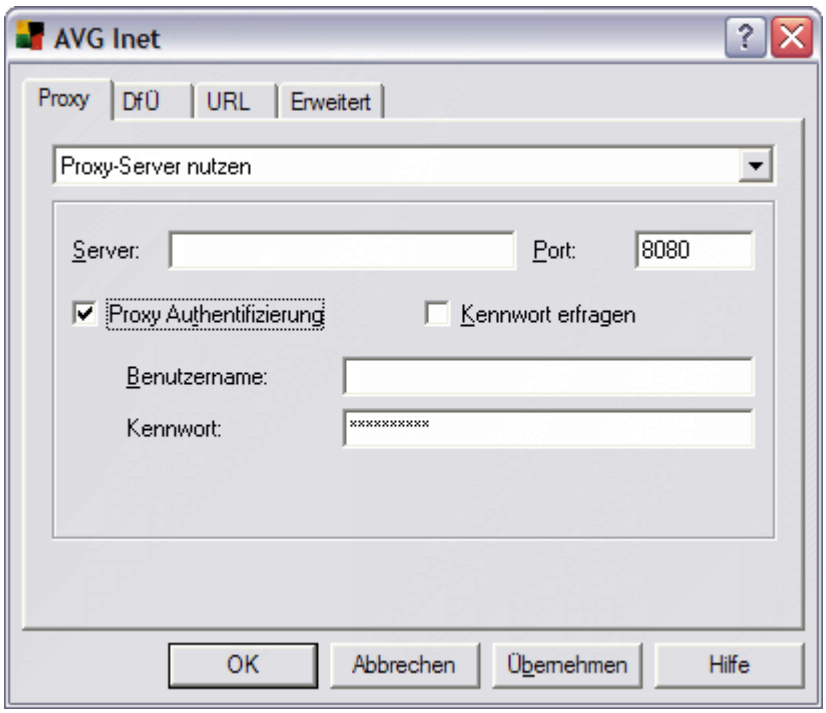
- Keinen Proxy-Server nutzen
- Proxy-Server nutzen
- Proxy-Server nutzen, bei Fehler direkt verbinden

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

- ***Server –*** *geben Sie die* Server IP-Adresse (oder den Namen des Servers) an
- ***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.

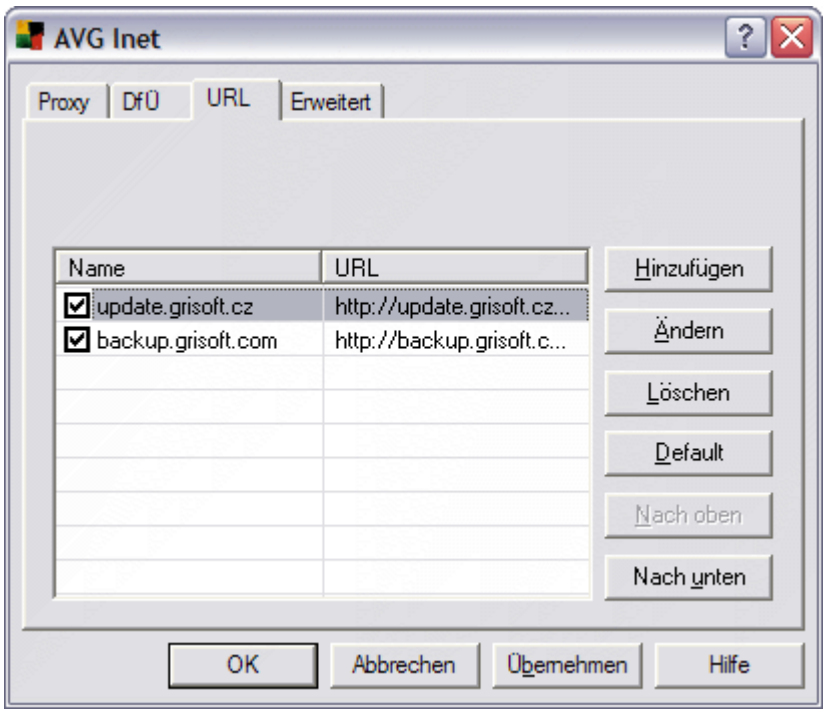
Bestimmen Sie, ob Sie einen automatischen Verbindungsaufbau zum Internet wünschen (***Die Verbindung automatisch aufbauen***) oder ob Sie jedes Mal die Verbindung manuell bestätigen möchten (***Bestätigungsdialog vor Verbindungsaufbau***). Wählen Sie für den automatischen Verbindungsaufbau aus der Liste 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***

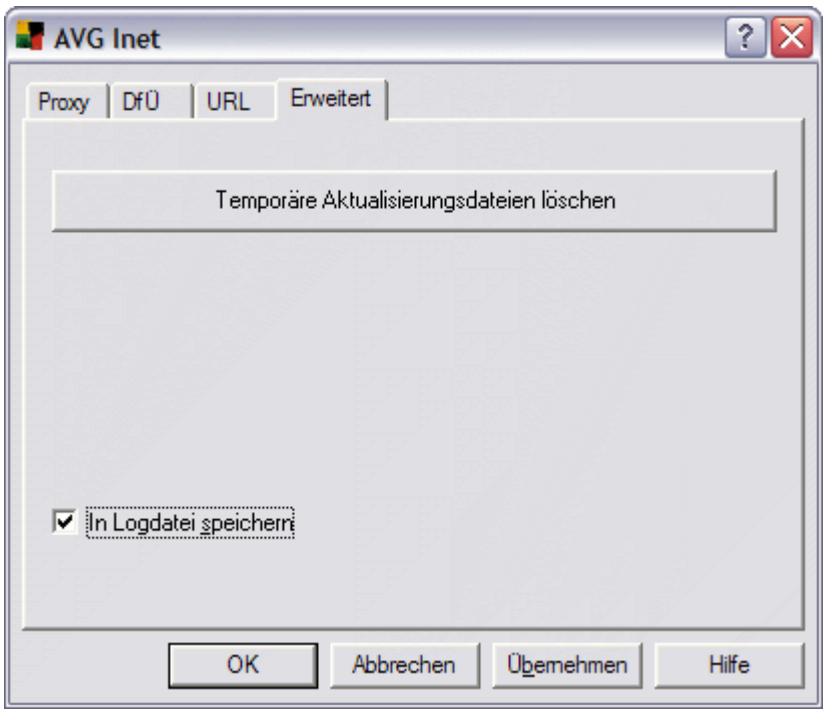
Der Reiter ***URL*** zeigt eine Liste von Internetadressen, von denen die Aktualisierungsdateien herunter geladen werden können. Die Liste und die enthaltenen Objekte können mit Hilfe der Schaltflächen bearbeitet werden:

- ***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***

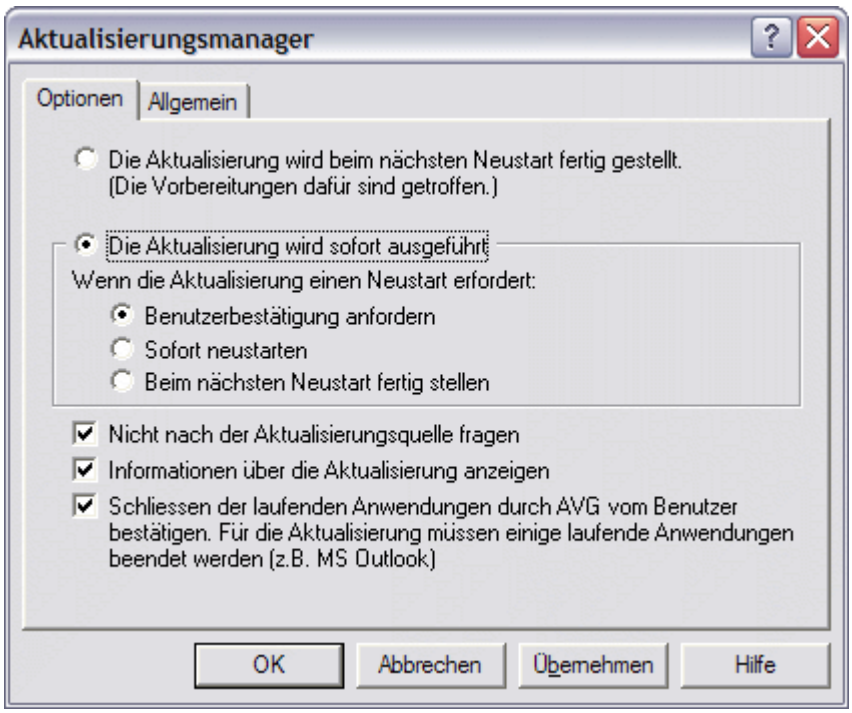
Der Reiter ***Advanced*** bietet die Möglichkeit, alle temporären Verzeichnisse für die Aktualisierung zu löschen, die AVG während der Aktualisierung angelegt hat. Zum Löschen all solcher Verzeichnisse klicken Sie einfach auf die Schaltfläche ***Temporäre Verzeichnisse für die Aktualisierung löschen.***



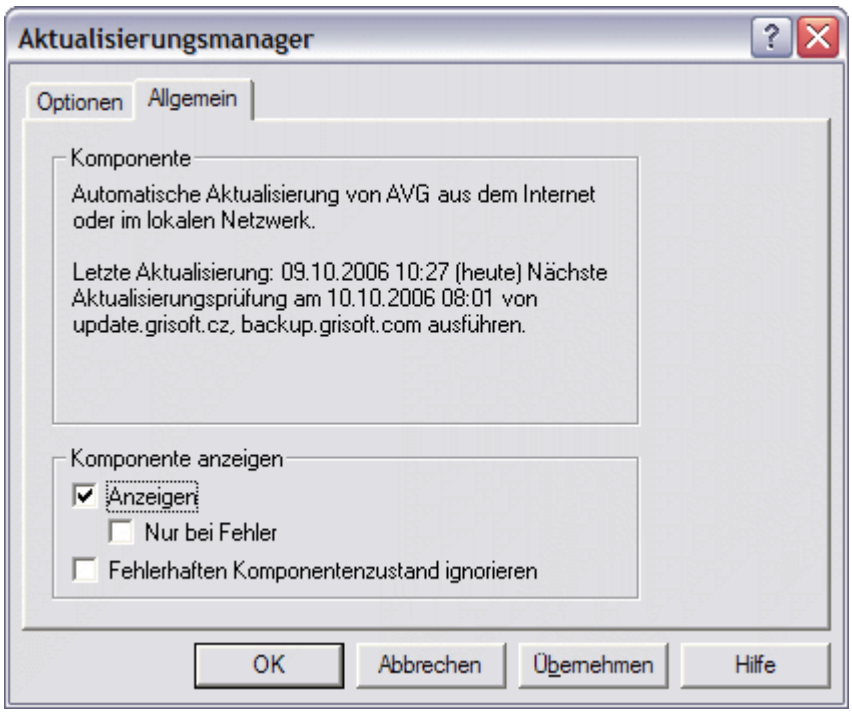
c) *Optionen*

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.

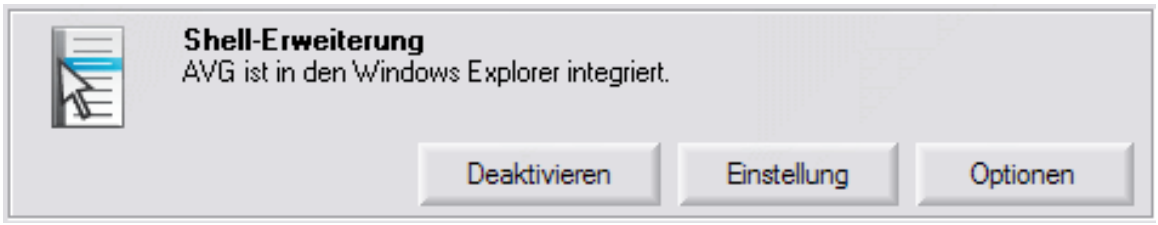


- ***Allgemein*** **–** dieser Reiter bietet einen kleinen Überblick über Informationen zur Komponente ***Aktualisierungsmanager*** und Sie können die Parameter für die Anzeige dieser Komponenten definieren:



9.15. 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:

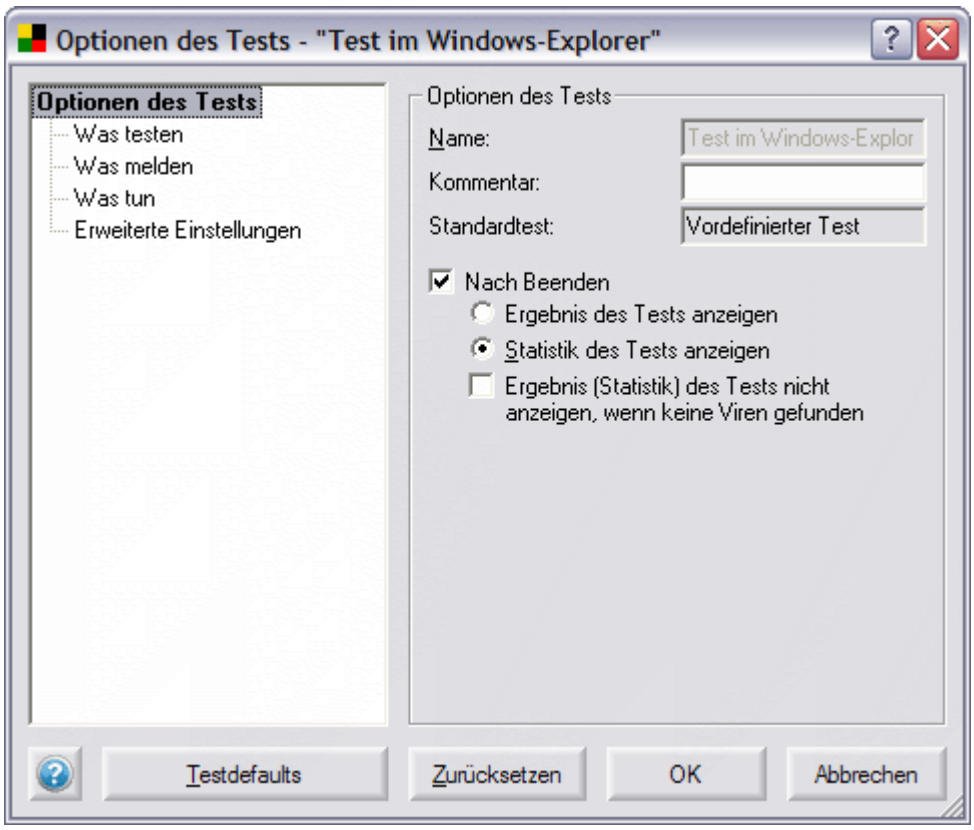
a) Deaktivieren

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***).

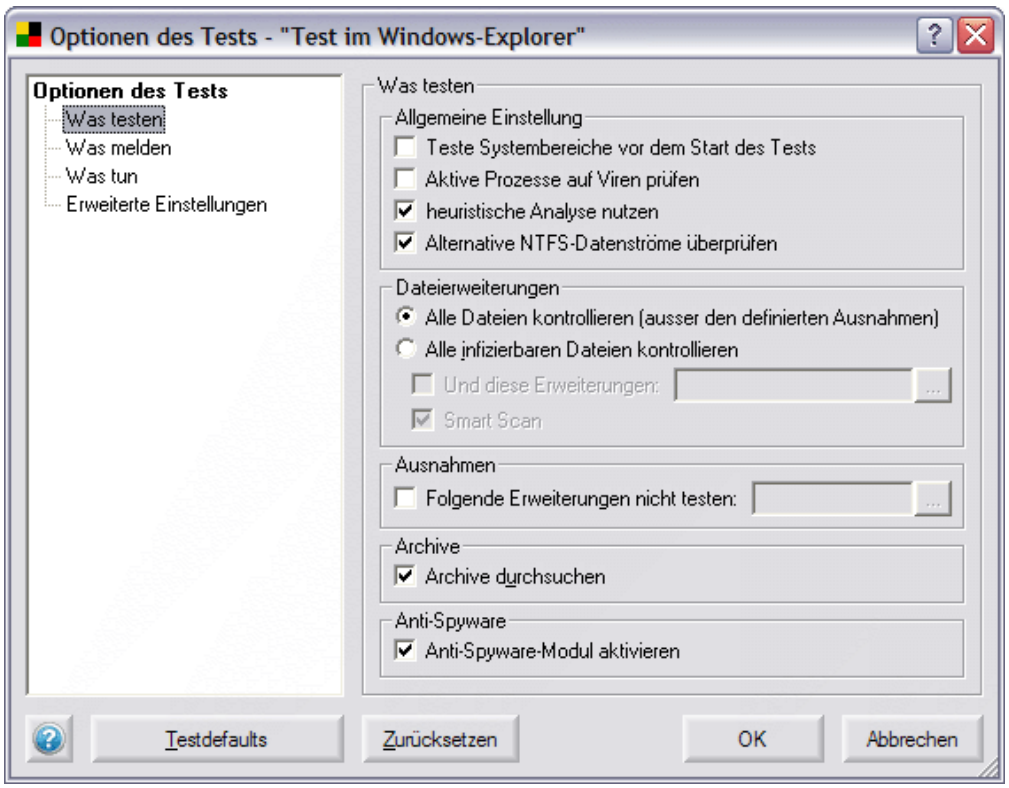


- ***Was testen*** – in diesem Dialog definieren Sie die Systembereiche, die überprüft werden sollen und welche Methoden für den Test verwendet werden (***Allgemeine Einstellung***). Wenn Sie nicht möchten, dass ***Alternative NTFS- Datenströme überprüfen*** durchgeführt wird, so lassen Sie dieses Kästchen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

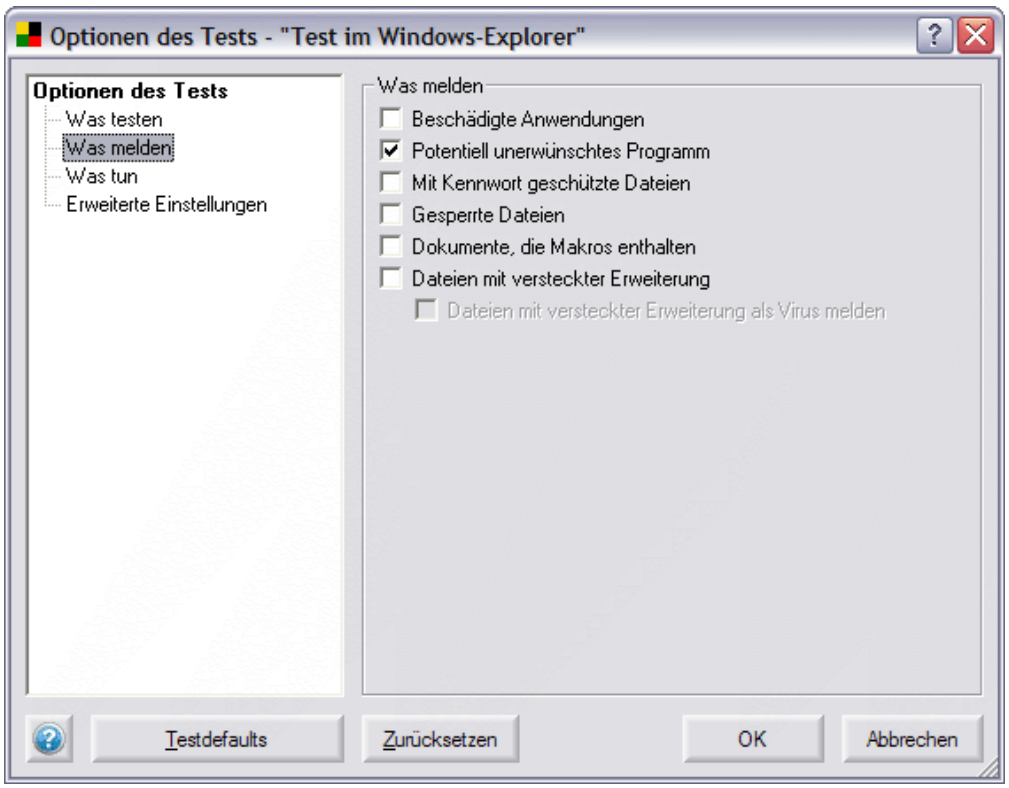
  Anmerkung: *Alternative NTFS-Datenströme ist ein Windows-Feature, das von Angreifern (meist Hackern) für versteckte Daten, besonders Rootkits, Viren, Trojanern usw. missbraucht wird. Daher wird empfohlen, diese Standard-Einstellung beizubehalten.*

  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***).

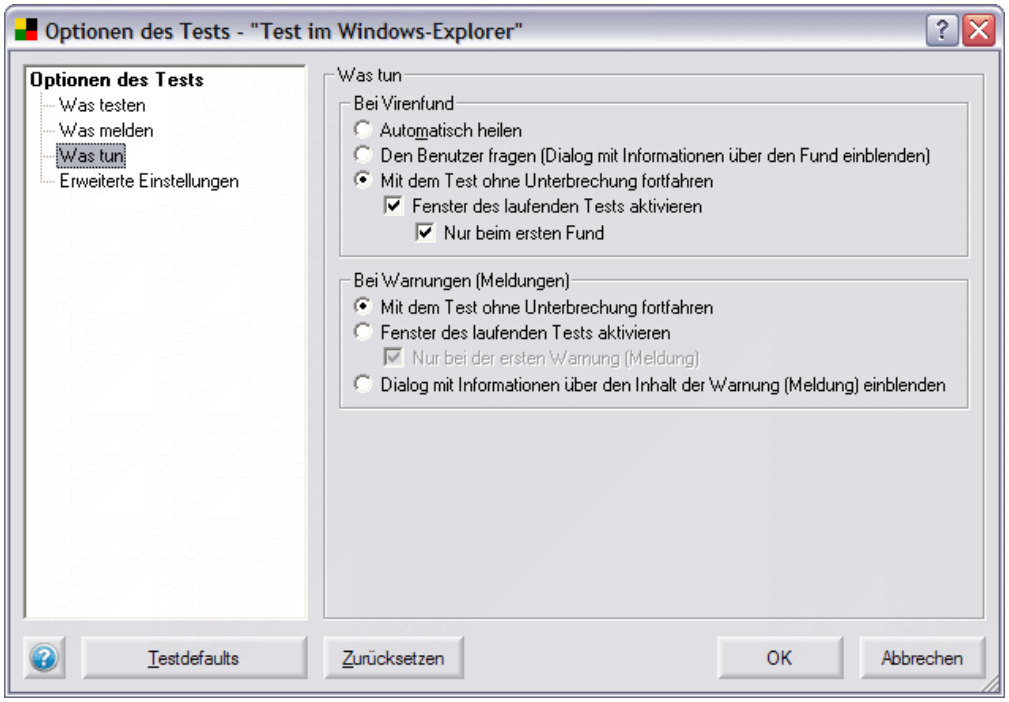


o ***Was melden*** – der Dialog ***Was melden*** zeigt eine Liste von Ereignissen an, die während eines Tests vorfallen können. Wählen Sie die Ereignisse aus, über die Sie informiert werden möchten:

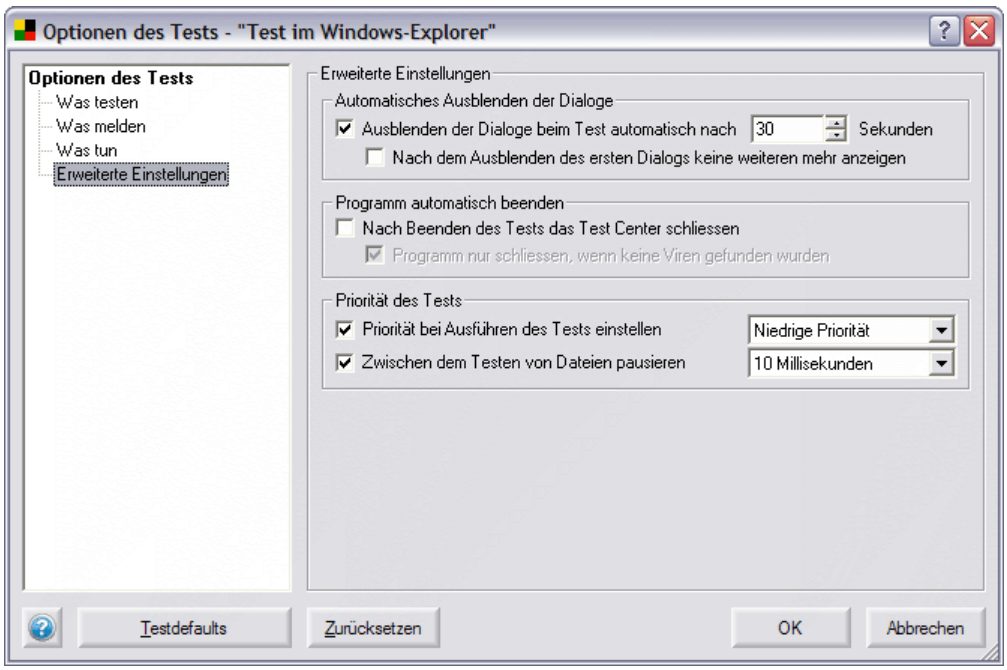


o ***Was tun*** – im nächsten Dialog bestimmen Sie, welche Maßnahmen durchgeführt werden sollen, wenn ein Virus gefunden wird (***Bei***

Virenfund) und wenn eine Warnmeldung (auf Grund der oben ausgewählten Ereignisse) angezeigt wird (***Bei Warnungen***).



- ***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

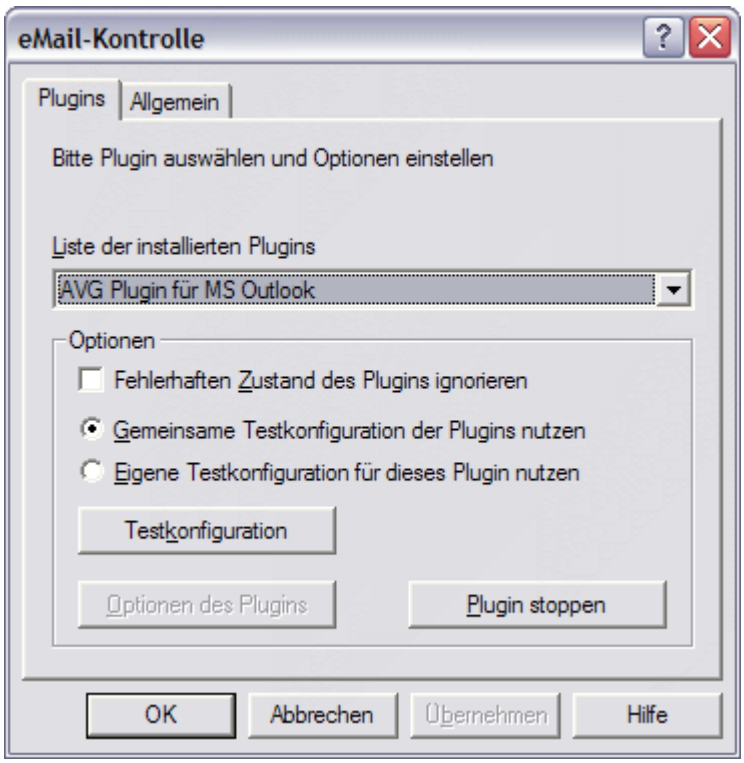
Die Schaltfläche ***Optionen*** zeigt die allgemeinen Informationen der Komponente ***Shell Erweiterung*** an und ermöglicht die Bearbeitung der Optionen zur Komponentenanzeige:

9.16. 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:



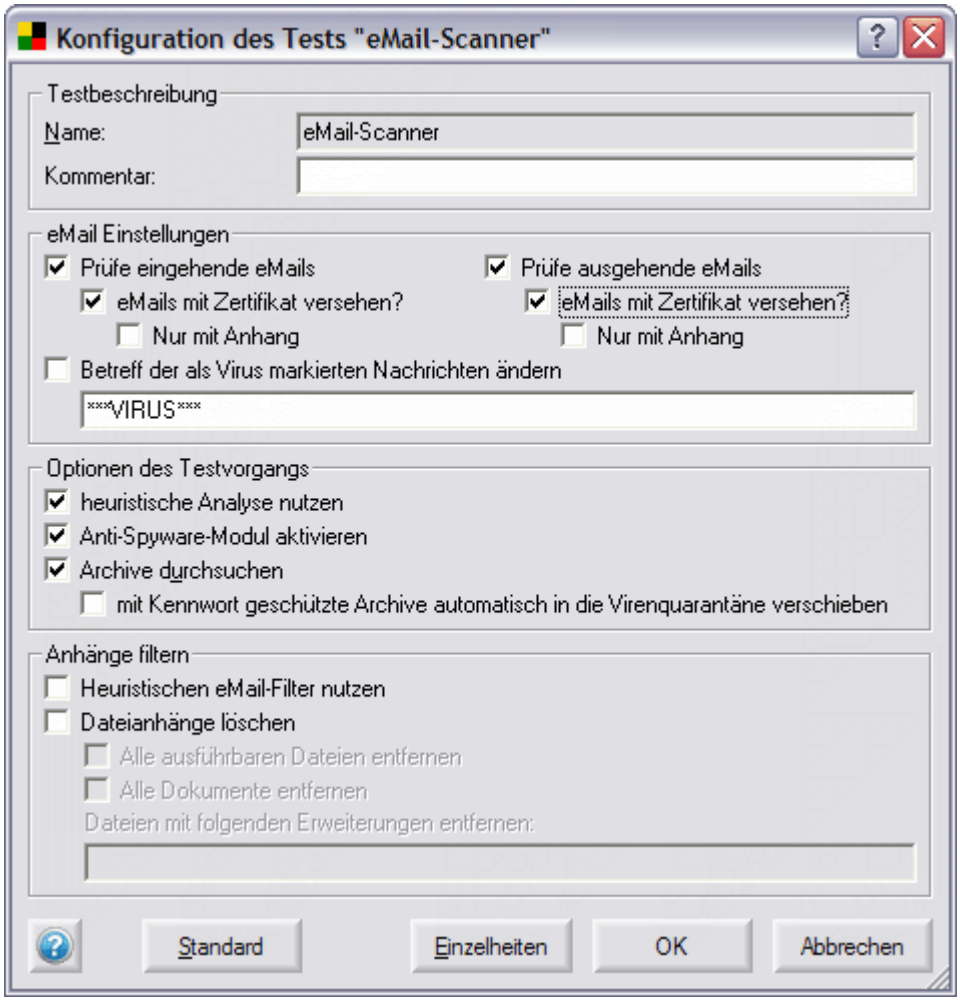
Im Abschnitt ***Optionen*** können Sie die folgenden Parameter einstellen:

- ***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 des 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***).

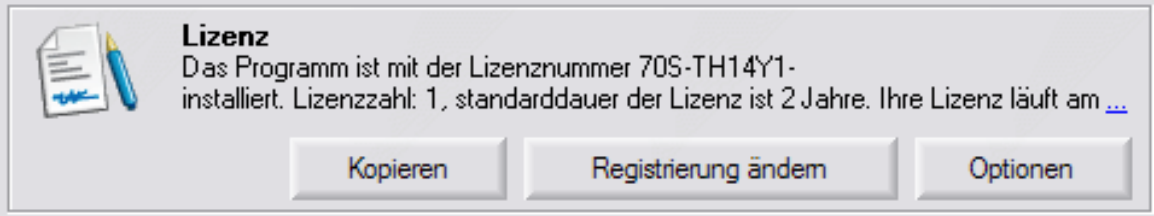
- ***Optionen des Testvorgangs*** – legen Sie fest, ob die heuristische Analyse genutzt werden soll (***heuristische Analyse nutzen***), ob Sie eingehende/ausgehende eMails auf Spyware/Adware überprüfen lassen möchten (***Anti-Spyware-Modul aktivieren***) und ob Archive getestet werden sollen (***Archive 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.

9.17. Control Center - Lizenz

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



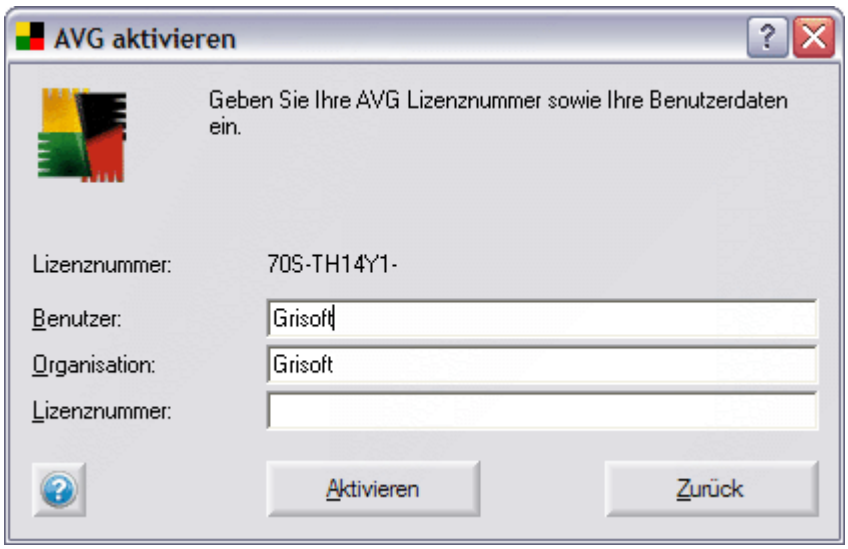
Im Dialogfenster ***Lizenz*** stehen die folgenden Schaltflächen zur Verfügung:

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.



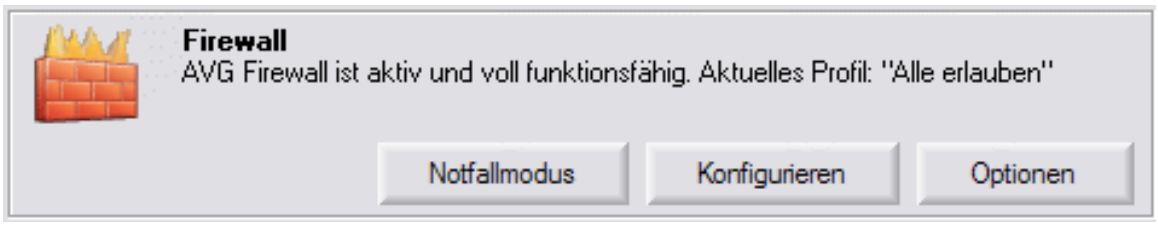
c) Optionen

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

10. Firewall

Die Komponente ***Firewall*** kontrolliert den Verkehr auf jedem Netzwerkport Ihres Computers. Die **Firewall** evaluiert nach vorgegebenen Regeln die Anwendungen, die entweder auf Ihrem Computer aktiv sind oder auf Ihr Netzwerk zugreifen wollen (sowohl interne, als auch aus dem Internet); ebenso werden Anwendungen, die versuchen, sich von außen mit Ihrem PC zu verbinden, evaluiert. Für jede dieser Anwendungen kann die **Firewall** dann die Kommunikation auf den Netzwerk-Ports zulassen oder unterbinden.

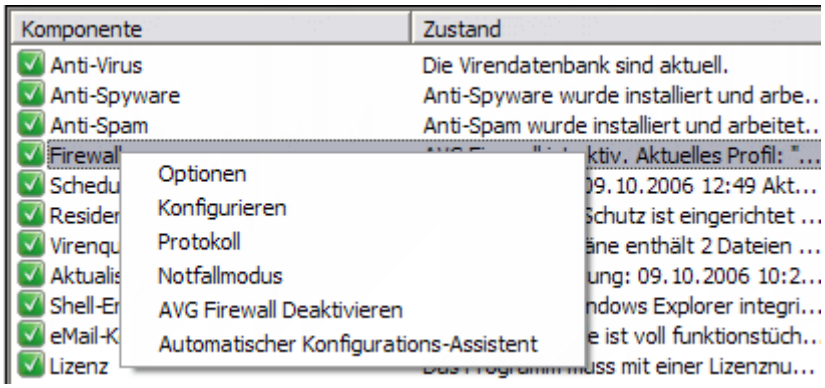
10.1. Die Firewall-Kontrolle im Control Center



Die ***Firewall*** wird mit diesen Schaltflächen im AVG Control Center gesteuert:

- Notfallmodus - die Firewall stoppt den Verkehr in beide Richtungen
- Konfigurieren – öffnet den Konfigurationsdialog der Firewall
- Optionen – öffnet den Dialog Optionen

Ein rechter Mausklick auf die Komponente **Firewall** öffnet das Kontextmenü mit folgenden Optionen:



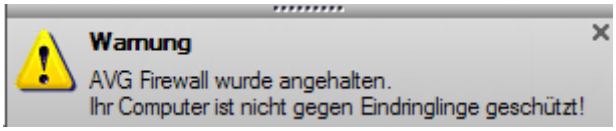
- Optionen – öffnet den Dialog Optionen
- Konfigurieren – öffnet den Konfigurationsdialog der Firewall
- Protokoll – öffnet die Liste der protokollierten Firewall-Aktionen und –Ereignisse im Firewall- Konfigurationsdialog
- Notfallmodus - die Firewall stoppt den Verkehr in beide Richtungen
- Firewall Deaktivieren – hält die Firewall an
- Automatischer Konfigurations-Assistent – startet den (automatischen) Firewall Konfigurationsassistenten

10.2. Firewall deaktivieren

Die **Firewall** kann über den Eintrag ***Firewall Deaktivieren*** im Kontextmenü der Komponente **Firewall -**aufgerufen durch einen rechten Mausklick auf die Komponente im **Control Center -** gestoppt werden.

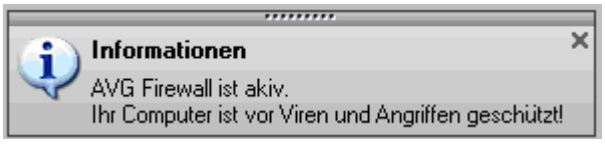
Mit der Schaltfläche ***Firewall Deaktivieren*** wird die **Firewall** Komponente im **Control Center** sofort – falls das erforderlich ist – abgeschaltet. Wenn Sie sich aus irgendeinem Grund entscheiden, die **Firewall** zu deaktivieren, bedenken Sie bitte, dass unmittelbar nach diesem Klick der Schutz Ihres PCs sowohl gegen innere, wie auch gegen äußere Netzwerkangriffe aufgehoben ist! Ihr Computer ist somit dem Risiko eines Angriffes ausgesetzt.

Wenn Sie die Schaltfläche ***AVG Firewall Deaktivieren*** betätigen, werden Sie über die möglichen Risiken gewarnt:



Ist die **Firewall** inaktiv, erscheinen im Kontrollbereich des **Control Centers** die drei Schaltflächen:

- ***Aktivieren*** – nutzen Sie die Schaltfläche ***Aktivieren***, um die zuvor angehaltene **Firewall** wieder zu aktivieren und alle Funktionen der Firewall wieder in Funktion zu setzen. Sie werden über diese Statusänderung informiert:

- ***Protokoll-*** öffnet die Liste der gespeicherten Aktionen der Firewall
- ***Optionen*** – diese Schaltfläche wird im Kontrollbereich des **Control Centers** immer angezeigt. Sie finden ausführliche Informationen über die Optionen der **Firewall** und ihrem aktuellen Status im Kapitel Firewall Optionen.

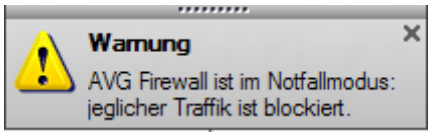
10.3. Der Notfallmodus der Firewall

Die **Firewall** kann jeglichen Netzwerkverkehr mit der Schaltfläche ***Notfallmodus*** über die Kontrollschaltfläche der **Firewall** innerhalb des **Control Centers** gestoppt werden.

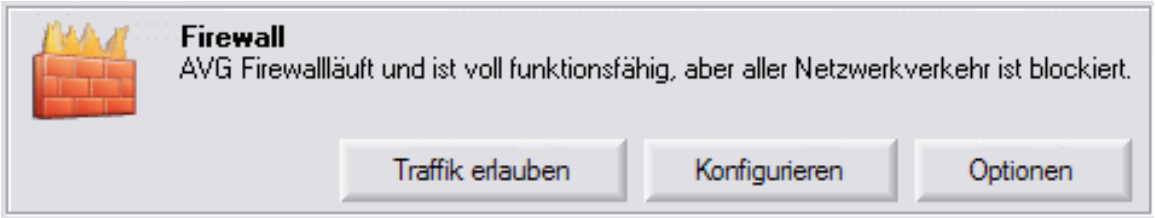
Die Schaltfläche ***Notfallmodus*** ist ein weiterer Schnellzugang für die Kontrolle der **Firewall** innerhalb des **AVG Control Centers**. Mit dieser Funktion ist es nicht erforderlich, die Konfiguration der Komponente zu ändern. Falls nötig kann mit

einem Klick jeglicher Netzwerkverkehr auf allen Ports blockiert werden: Die **Firewall** ist weiterhin in Betrieb, jedoch wird jeglicher Netzwerkverkehr unterbunden.

Wenn Sie die Schaltfläche ***Notfallmodus*** anklicken, werden Sie über den neuen Status der **Firewall** informiert:



Ist der Verkehr einmal angehalten, zeigt der Kontrollbereich der **Firewall** im **Control Center** eine neue Schaltfläche ***Traffik erlauben***, mit welcher der Notfallmodus aufgehoben wird und die Firewall wieder den Netzwerkverkehr zulässt, wie er im Regelwerk der **Firewall** Komponente erlaubt ist:



Wenn Sie nun die Schaltfläche ***Trafik erlauben*** betätigen, wird Sie die **AVG Firewall** über die Statusänderung informieren.

10.4. Aktionen der Firewall

Die **Firewall** kontrolliert den Verkehr auf Netzwerkports durch Zuordnung von Regeln zu Anwendungen, die über das Netzwerk kommunizieren wollen. Regeln werden den im Dialog Firewall – Konfiguration spezifischen Anwendungen zugeordnet. Jede Regel ist durch eine dieser Aktionen definiert:

a) Erlauben

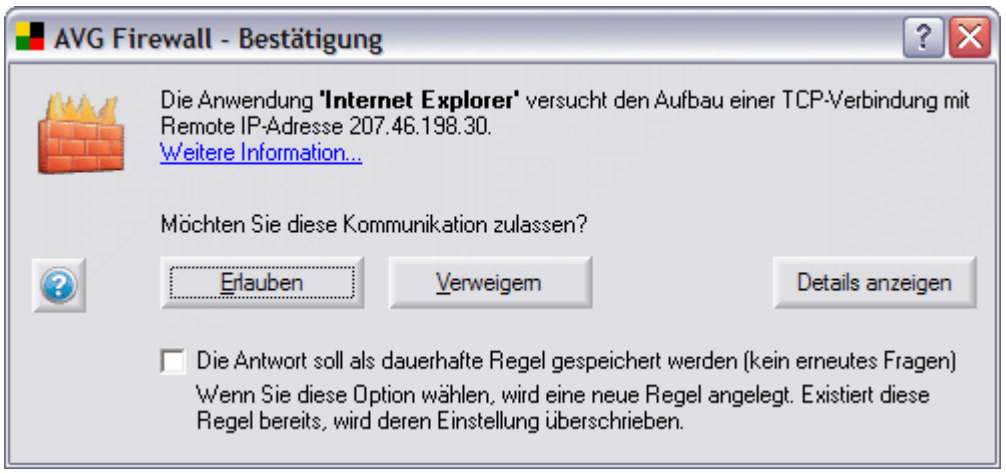
Die Regel besagt, dass jegliche Kommunikation dieser Anwendung erlaubt ist.

b) Verweigern

Nach dieser Regel ist der Anwendung jegliche Kommunikation verboten.

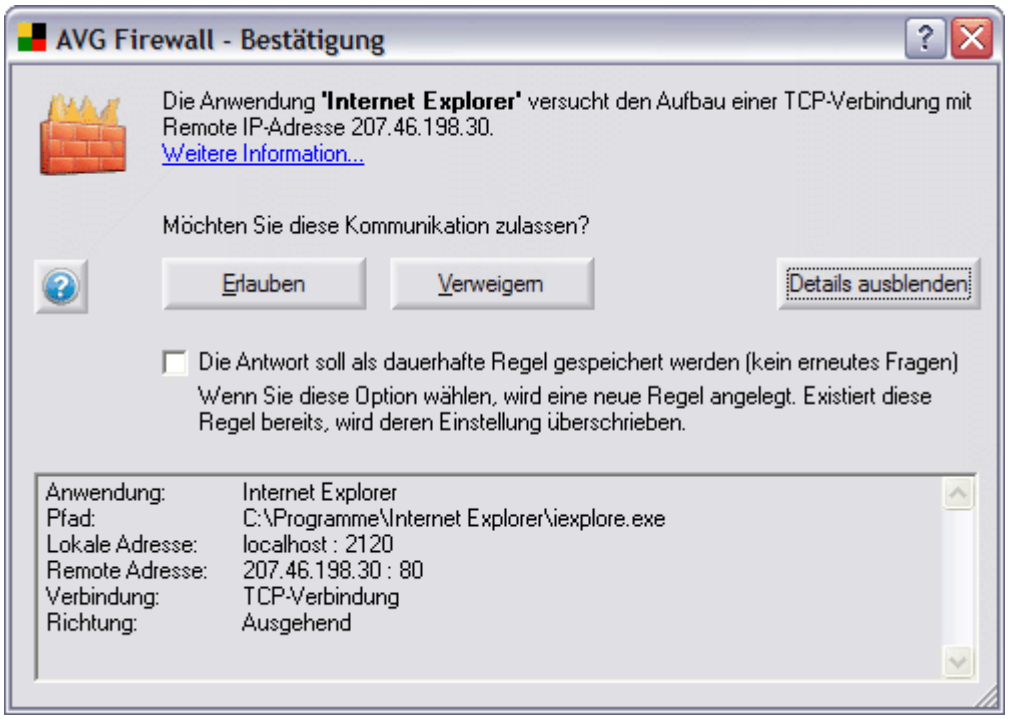
c) Details anzeigen

Keine Regel ist dieser Anwendung zugeordnet. Sie werden jedes Mal gefragt, was getan werden soll, wenn die Anwendung kommunizieren möchte. Wenn die Anwendung eine Kommunikation über irgendeinen Netzwerkport durchführen möchte, erscheint der Dialog **Firewall – Bestätigung**:



Der Dialog **Firewall – Bestätigung** bietet diese Optionen:

- ***Erlauben*** – Der Anwendung wird für dieses Mal gestattet, die Kommunikation auszuführen
- ***Verweigern*** - Der Anwendung wird es diesmal nicht gestattet, die Kommunikation auszuführen
- ***Die Anwort soll als dauerhafte Regel gespeichert werden*** – generiert für diese Anwendung eine neue Regel auf der Basis Ihrer momentanen Wahl (Erlauben/Verweigern); diese Regel wird in der Firewall-Konfiguration gespeichert.
- ***Details anzeigen / ausblenden*** – Hiermit können Sie sich ausführliche Informationen über die Anwendung und ihrer Parameter (Anwendungsname, Verzeichnis und Name der Anwendung auf der Festplatte, Adresse, Verbindungstyp, Richtung der Kommunikation) anzeigen lassen.



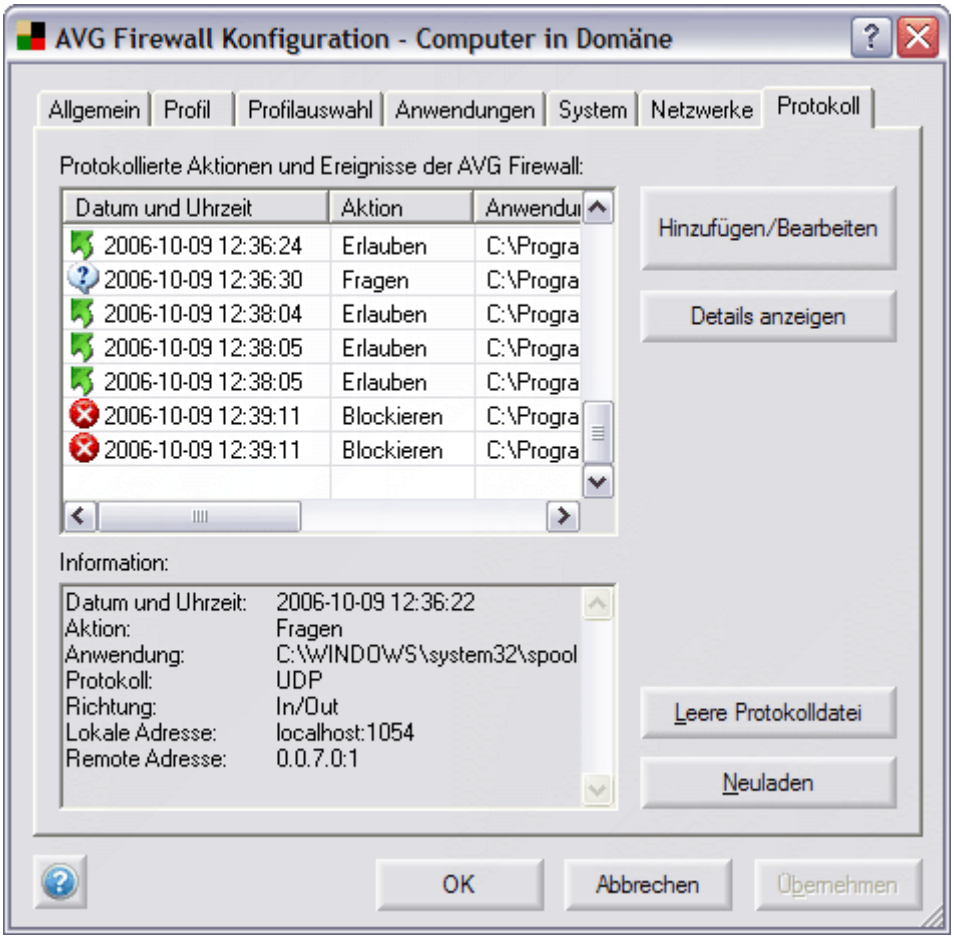
d) Advanced Konfiguration

Wenn Sie einer Anwendung die Advanced Konfiguration als Aktion zuordnen, können Sie die Regel detailliert definieren. Damit ist es möglich, für diese Anwendung unterschiedliche Regeln für unterschiedliche Anwendungsdienste, unterschiedliche Netzwerke usw. zu definieren. Sie konfigurieren diese Aktion über den Dialog **Firewall – Konfiguration**, der im Kapitel Konfiguration der Firewall beschrieben ist.

10.5. Firewall Protokoll

Sie können über die Schaltfläche ***Protokoll*** Information der **Firewall** anzeigen lassen. Sie erreichen das Kontextmenü mit dieser Schaltfläche durch einen rechten Mausklick auf die Komponente **Firewall** im **Control Center**. Während die **Firewall** deaktiviert ist, sind die gespeicherten Informationen über Ereignisse und Aktionen direkt über die Schaltfläche ***Protokoll*** im Kontrollbereich der **Firewall** Komponente im **Control Center** erreichbar.

Die Schaltfläche ***Protokoll*** öffnet einen neuen Dialog **Firewall Konfiguration** im Reiter **Protokoll**. In diesem Bereich können Sie alle aufgezeichneten **Firewall-**Aktionen und Ereignisse mit einer ausführlichen Beschreibung der relevanten Parameter einsehen.



Der Hauptbereich des Reiters ***Protokoll*** ist in zwei Bereiche unterteilt:

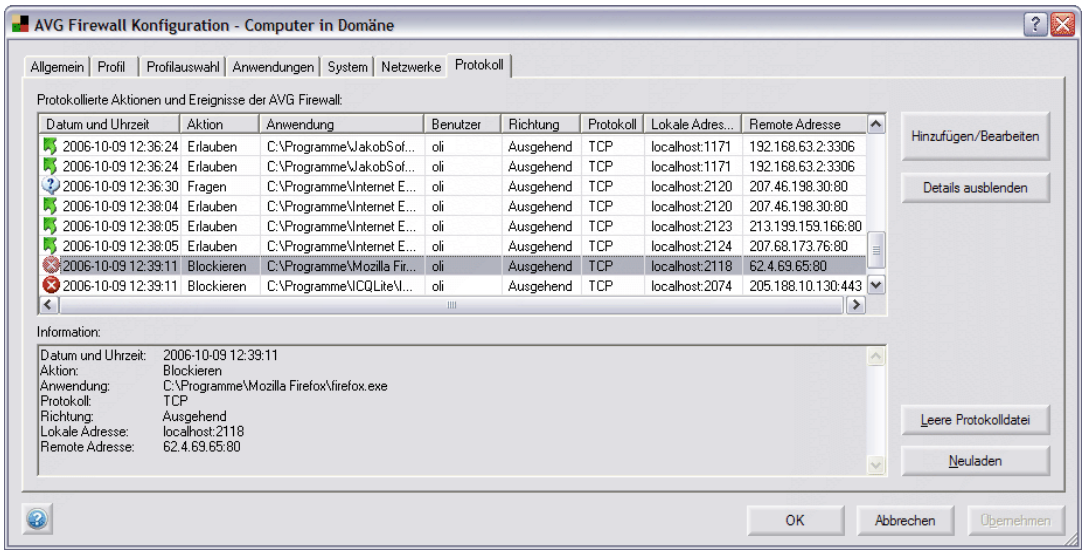
a) *Protokollierte Aktionen und Ereignisse der Firewall*

Dieser Bereich bietet Ihnen einen Überblick über alle Aktionen und Ereignisse, die von der **Firewall** ausgeführt und mit den Parametern protokolliert wurden.

Standardmäßig öffnet sich der Reiter ***Protokoll*** im Standardmodus, der folgende Parameter für jede aufgezeichnete Aktion darstellt:

- ***Datum und Uhrzeit*** – Der exakte Zeitpunkt, zu dem das Ereignis aufgetreten ist.
- ***Aktion*** – Art der Aktion, die ausgeführt wurde
- ***Anwendung*** – Der Pfad zur Anwendung, die von dieser Aktion betroffen ist.

Wenn Sie diese Darstellung als unzureichend empfinden, können Sie mit der Schaltfläche ***Details anzeigen*** in die ausführliche Darstellung wechseln:



Anschließend können Sie diese Parameter einsehen:

- ***Datum und Uhrzeit*** – Der exakte Zeitpunkt, an dem das Ereignis aufgetreten ist.
- ***Aktion*** – Art der Aktion, die ausgeführt wurde.
- ***Anwendung*** – Der Pfad zur Anwendung, die von dieser Aktion betroffen ist.
- ***Benutzer*** – Name des Benutzers, der diese Anwendung ausführt.
- ***Richtung*** – Die Richtung der Kommunikation der Anwendung (rein/raus oder in beide Richtungen).
- ***Protokoll*** – der benutzte Protokolltyp
- ***Lokale Adresse*** – die lokale Adresse dieser Verbindung
- ***Remote Adresse*** – die Remote-Adresse dieser Verbindung

In beiden Ansichten (Standard/ausführlich) können Sie die angezeigten Parameter nach einem Kriterium sortieren: Sie können chronologisch nach

Datum sortieren (klicken Sie in den Kopf der betreffenden Spalte auf Datum und Zeit), nach der Art der Aktion (Klicken Sie auf Aktion) usw.

b) Information

Der Bereich ***Information*** bietet einen komfortablen und klaren Überblick über die Liste der Parameter, die für das ausgewählte Ereignis aufgezeichnet wurden; dieses Ereignis ist aktuell im oberen Bereich ***Protokollierte Firewall Aktionen und Ereignisse*** markiert.

c) Schaltflächen Reiter Protokoll

Der Reiter ***Protokoll*** hat vier Schaltflächen:

- ***Hinzufügen / Bearbeiten*** – Sie können eine Anwendung zur Protokollierung hinzufügen, bzw. bearbeiten.
- ***Details anzeigen / ausblenden*** – schaltet zwischen der Standard- und der ausführlichen Ansicht um.
- ***Leere Protokolldatei*** – entfernt alle Informationen zu den protokollierten Ereignissen aus der Übersicht.
- ***Neuladen*** – aktualisiert die angezeigte Information.

10.6. Firewall - Konfigurationsassistent

Die anfängliche Konfiguration der **Firewall** kann mit dem ***Firewall-Automatischer Konfigurationsassistent*** erstellt werden. Auch wenn Sie die Parameter für die Firewall-Komponente später konfigurieren können (siehe Kapitel Firewall Konfiguration), empfehlen wir den Einsatz des Assistenten, damit Ihre **Firewall** fehlerfrei arbeitet.

Der ***Firewall Automatischer Konfigurations-Assistent*** kann aus dem Startmenü in der Taskleiste gestartet werden:

Start / Programme / AVG 7.5 / Firewall–Konfigurationsassistent

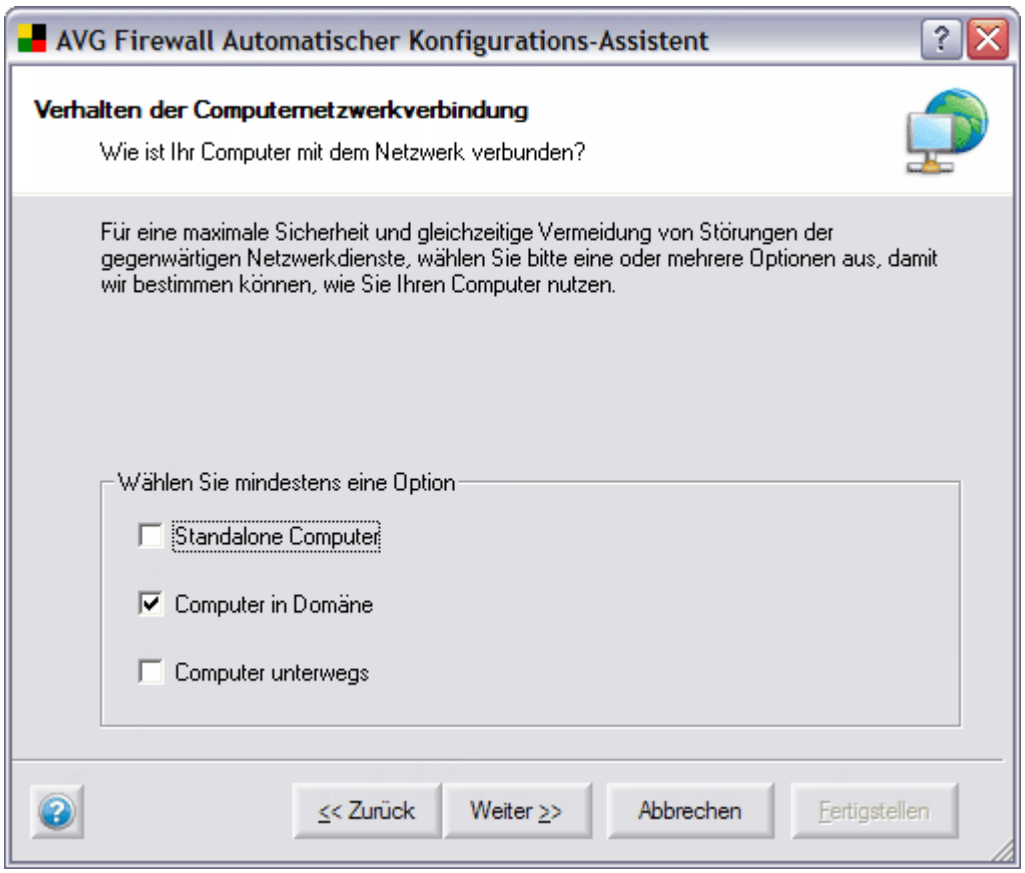
oder aus dem Kontextmenü der Komponente **Firewall** im **AVG Control Center** -> ***automatischer Konfigurationsassistent.***

Wenn sie den automatischen ***Konfigurations-Assistenten*** gestartet haben, sucht dieser nach einer bestehenden Konfiguration und startet in zwei möglichen Modi***:***

- Optionen der Netzwerkverbindung (a) Dieser Dialog erscheint, wenn keine bestehende Konfiguration gefunden wurde.
- Bestehende Konfiguration (b) – Dieser Dialog erscheint, wenn eine bereits bestehende Konfiguration gefunden wurde.

a) Optionen der Computernetzwerkverbindung (neue Konfiguration)

Wenn keine bereits bestehende Konfiguration gefunden wurde, startet der ***automatische Firewall Konfigurationsassistent*** diesen Dialog:



Der automatische ***Konfigurationsassistent der Firewall*** erfragt nun, wie Ihr Computer mit dem Internet verbunden ist. Wenn z.B. Ihr Notebook an vielen verschiedenen Orten mit dem Internet verbunden wird (Flugplatz, Hotelzimmer etc.), werden strengere Sicherheitsrichtlinien benötigt, als für einen Computer in einer Domäne (Firmennetzwerk etc.). Auf der Grundlage der Wahl des Verbindungstyps legt die **Firewall** nun die Default-Regeln für unterschiedliche Sicherheitsansprüche fest.

Sie können aus drei Vorgaben auswählen:

- ***Standalone Computer*** (Einzelplatzrechner)
- ***Computer in Domäne*** (Firmennetzwerk)
- ***Computer unterwegs*** (typischerweise ein Notebook)

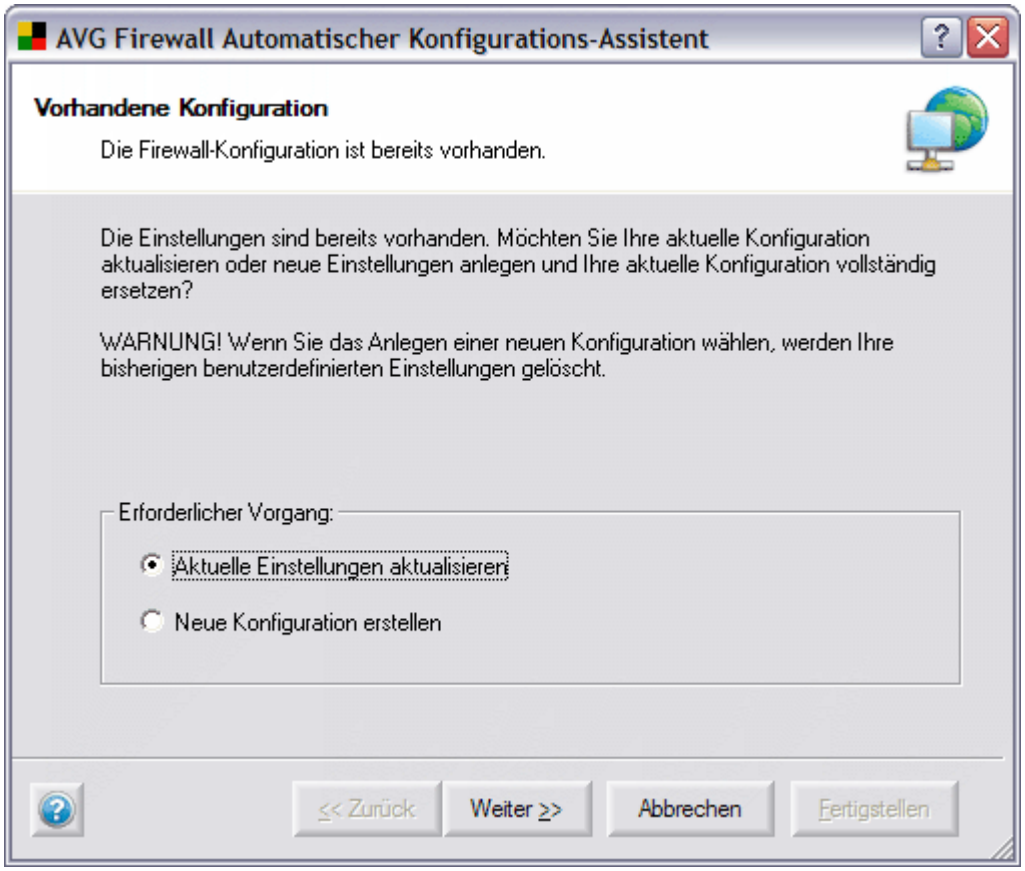
Wählen Sie bitte den(die) Verbindungsart(en), der(die) zu der normalen Nutzung Ihres Computer passen. Sie können mehrere Verbindungsarten, die Ihrem wechselnden Nutzungsprofil entsprechen, auswählen. Bestätigen Sie über die Schaltfläche „***Weiter>>***“ Ihre Auswahl und fahren bitte mit dem nächsten Dialog fort ***Scanne Ihren Computer***.

Wenn Sie Ihre entsprechende Wahl getroffen haben, gehen Sie bitte weiter zum nächsten Schritt: Scanne Ihren Computer (c).

b) Bestehende Konfiguration gefunden

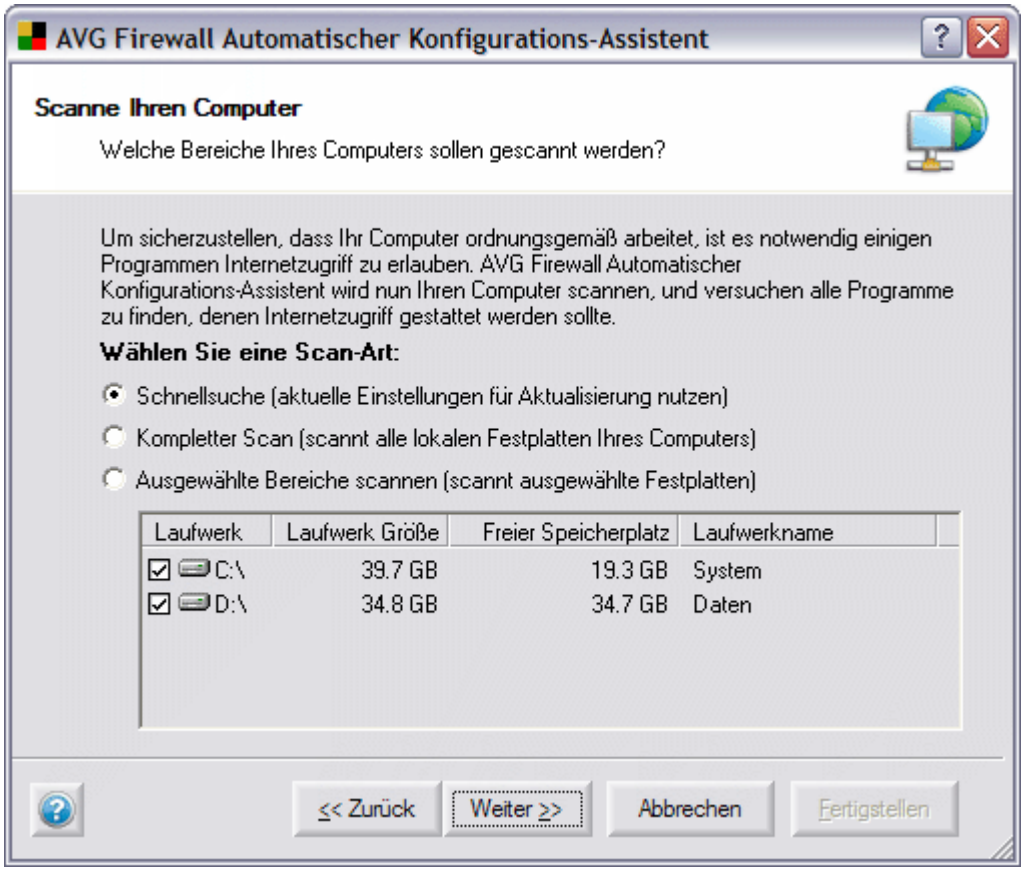
Um Konfigurationskonflikte zu vermeiden, erkennt der ***automatische Konfigurations-Assistent*** Ihre bereits bestehenden Einstellungen. Wenn

einige bestehende Konfigurations-Einstellungen erkannt werden, startet der AVG automatischer Konfigurations-Assistent mit dem folgenden Fenster:



Sie können zwischen ***Aktuelle Einstellungen aktualisieren*** oder Neue Konfiguration erstellen auswählen. Wenn Sie wählen, dass Ihre aktuellen Einstellungen aktualisiert werden sollen, wird der folgende Dialog angezeigt:

o **Aktualisierung der aktuellen Einstellungen**



In diesem Dialog müssen Sie sich entscheiden, ob Sie alle lokalen Festplatten Ihres Computers überprüfen möchten (***Kompletter Scan***), ob Sie festlegen möchten, welche Festplatten überprüft werden sollen (***Ausgewählte Bereiche scannen***) oder ob Sie fortfahren möchten mit ***Schnellsuche***.

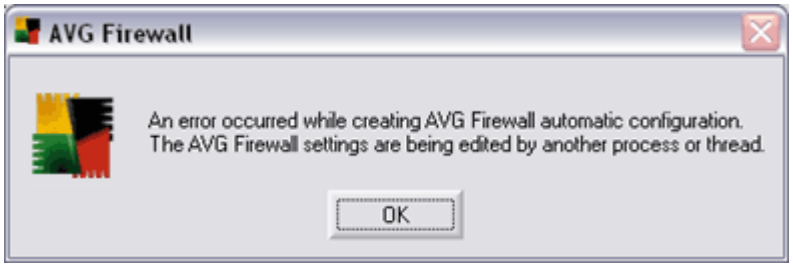
Anmerkung: *Wenn Sie die Optionen Kompletter Test oder Ausgewählte Bereiche scannen wählen, so erkennt der Assistent alle allgemein bekannten Anwendungen, die über das Netzwerk kommunizieren und definiert Regeln für diese Anwendungen. Jedoch erkennt er nicht alle dieser Anwendungen*.

Um die Wiederholung der Überprüfung zu vermeiden empfehlen wir für diesen Fall die Option ***Schnellsuche***. Die ***Schnellsuche*** durchsucht nicht die Festplatten, sondern bearbeitet nur Anwendungen, die kürzlich in der Konfiguration der Firewall gespeichert wurden und wendet die Regeln an, die in der neuen Standard-Konfiguration den bereits bestehenden Regeln zugeordnet wurden.

Das bedeutet, dass mit der ***Schnellsuche*** keine neuen Anwendungen erkannt werden. Alle Anwendungen, die in dem entsprechenden PC installiert sind und bisher nicht erkannt wurden (z.B. wenn bisher noch keine Konfiguration der Firewall durchgeführt wurde), haben niemals versucht, über das Netzwerk zu kommunizieren. Daher kann es gut möglich sein, dass diese nicht berücksichtigt werden müssen.

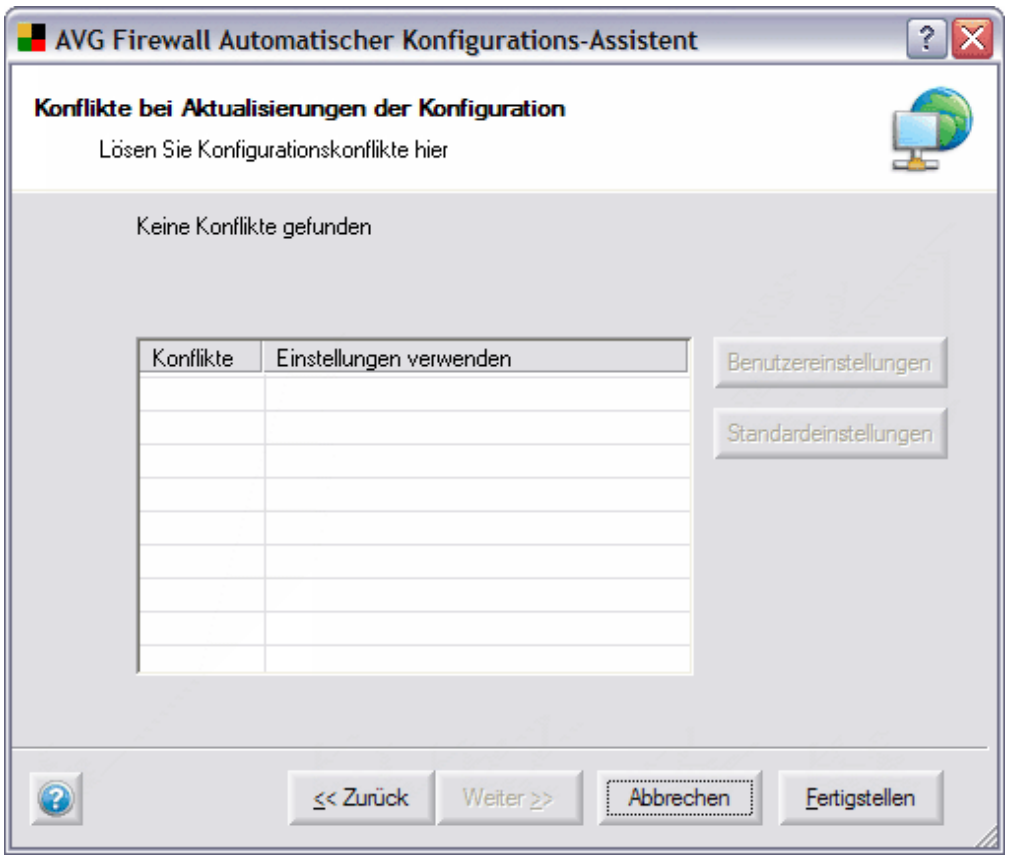
Wenn Sie die Option ***Schnellsuche*** wählen, wird der Dialog ***Konflikt bei der Konfigurations-Aktualisierung*** angezeigt.

Anmerkung: *In einigen Fällen erscheint zusätzlich diese Fehlerbenachrichtigung*:



Dies geschieht selten; nur wenn die Firewall-Konfiguration während des Durchlaufs des Konfigurations-Assistenten geändert wurde oder wenn die Firewall-Konfiguration im Control Center geöffnet ist. Um dieses Problem zu lösen beenden Sie einfach den Konfigurations-Assistenten und starten diesen neu im Startmenü oder durch einen Rechtsklick auf den Eintrag Firewall im Control Center; anschließend wählen Sie den automatischen Konfigurations-Assistenten aus der Liste aus.

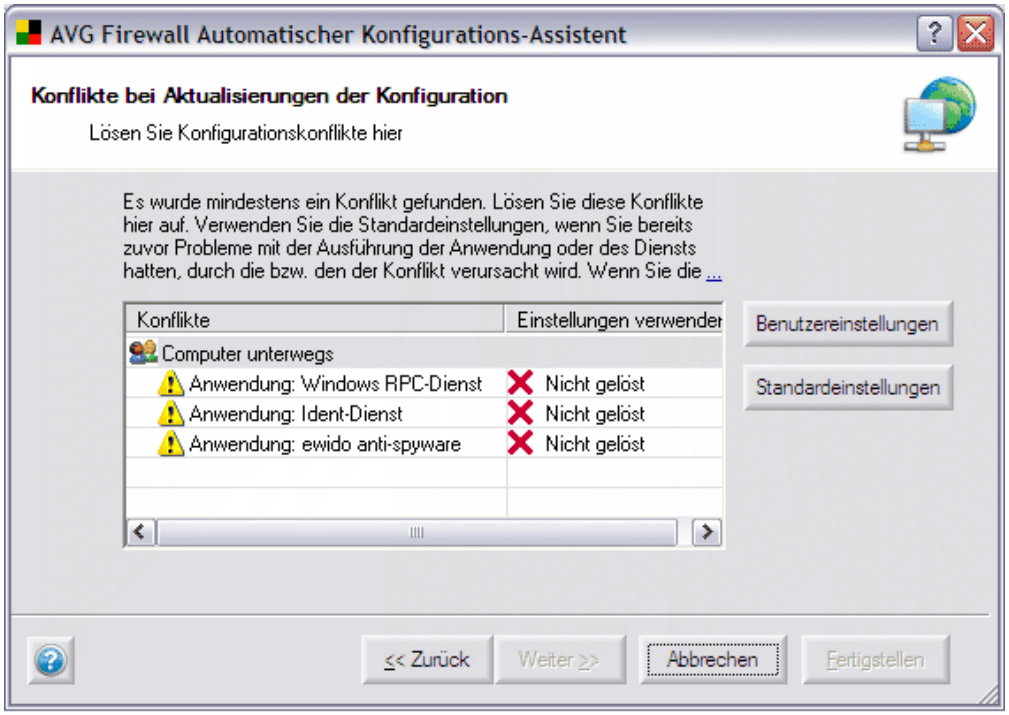
o ***Konflikte bei der Aktualisierung der Konfiguration***



Dieser Dialog bietet eine Übersicht über die Konflikte, die während der Zusammenführung der bestehenden Konfiguration der Firewall mit den empfohlenen Standardeinstellungen aufgetreten sind. Normalerweise ist die Liste in diesem Dialog leer – das bedeutet, dass beide Konfigurationseinstellungen ohne Problem zusammengeführt wurden und gespeichert und angewendet werden können.

Wenn jedoch der Benutzer die Regel für eine besondere Anwendung/einen Dienst in der letzten Zeit manuell geändert hat und die Standard-Regel für diese Anwendung/diesen Dienst auch geändert wurde, so entsteht ein Konflikt bei der Zusammenführung. Dieser Konflikt kann nicht automatisch gelöst werden und der Benutzer muss entscheiden, welche Konfiguration genutzt werden soll.

Dies ist ein Beispiel aus der Liste der Konflikte der Konfigurations-Zusammenführung:



Der Benutzer muss entscheiden, ob die ***Benutzereinstellungen*** oder ***Standard-Einstellungen*** genutzt werden sollen, bevor die Konfiguration gespeichert werden kann. Der Benutzer kann wählen:

- ***Alle Einträge sofort lösen*** – durch Klicken auf die Schaltflächen Benutzereinstellungen oder Standard-Einstellungen. Der Assistent ordnet die Wahl allen Einträgen dieser Liste zu.
- ***Individuelle Einträge lösen*** – durch Klicken auf die Reihe ***Ungelöst*** in der Spalte ***Nutze Einstellungen*** für jeden Eintrag und die Wahl der ***Benutzereinstellungen*** oder ***Standardeinstellungen***.

Anmerkung: *Standard-Einstellungen bedeuten, dass alle zur vorher gespeicherten Firewall-Konfiguration angepassten Änderungen mit Bezug auf die Konflikt-Anwendung mit der Grisoft-Standard-Regel überschrieben werden. Diese Option wird weniger erfahrenen Computerbenutzern empfohlen.*

Auch wenn Sie in der letzten Zeit irgendwelche Probleme mit der Konflikt-Abwicklung hatten, empfehlen wir Ihnen, dass Sie die Standard-Einstellungen für diese Anwendung wählen. Andernfalls können Sie die bereits bestehenden Einstellungen beibehalten.

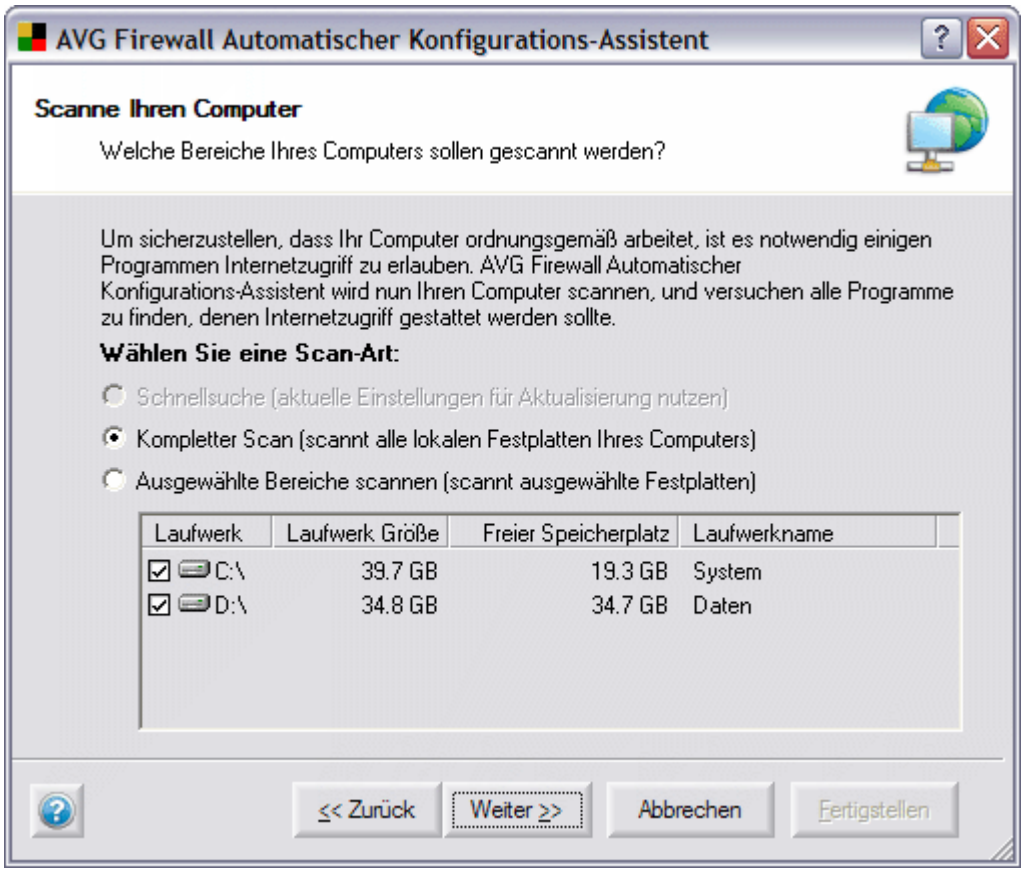
Wenn Sie die benutzerdefinierte Konfiguration wählen, wird die Konflikt-Anwendungsregel so beibehalten wie sie ist und keine von AVG empfohlenen Einstellungen werden hier angewendet.

Falls Sie sich dafür entscheiden, dass die Standard-Einstellungen bei einer Anwendung, die einige ganz besondere Parameter definiert hat (Spezielle Netzwerke, Adapter usw.), genutzt werden sollen, kann ein Bestätigungsdialog erscheinen. In diesem Fall wird empfohlen, die angepassten Konfigurations-Einstellungen beizubehalten, damit Sie keine speziellen Konfigurationsparameter verlieren, die ansonsten verloren gegangen wären.

Klicken Sie auf die Schaltfläche ***Beenden***, um den Konfigurationsvorgang abzuschliessen und zu speichern.

c) *Scanne Ihren Computer*

Wenn keine bereits bestehende Konfiguration der **Firewall** erkannt wurde, so startet der ***Firewall Automatischer Konfigurationsassistent*** und sucht auf Ihrem Computer nach Anwendungen, die sich mit dem Netzwerk verbinden.



Zur Einrichtung der anfänglichen Konfiguration der **Firewall** ist ein Test des Computers erforderlich. Hier werden alle Anwendungen und Systemdienste,

die über das Netzwerk kommunizieren, definiert und Standardregeln für die **Firewall** erstellt.

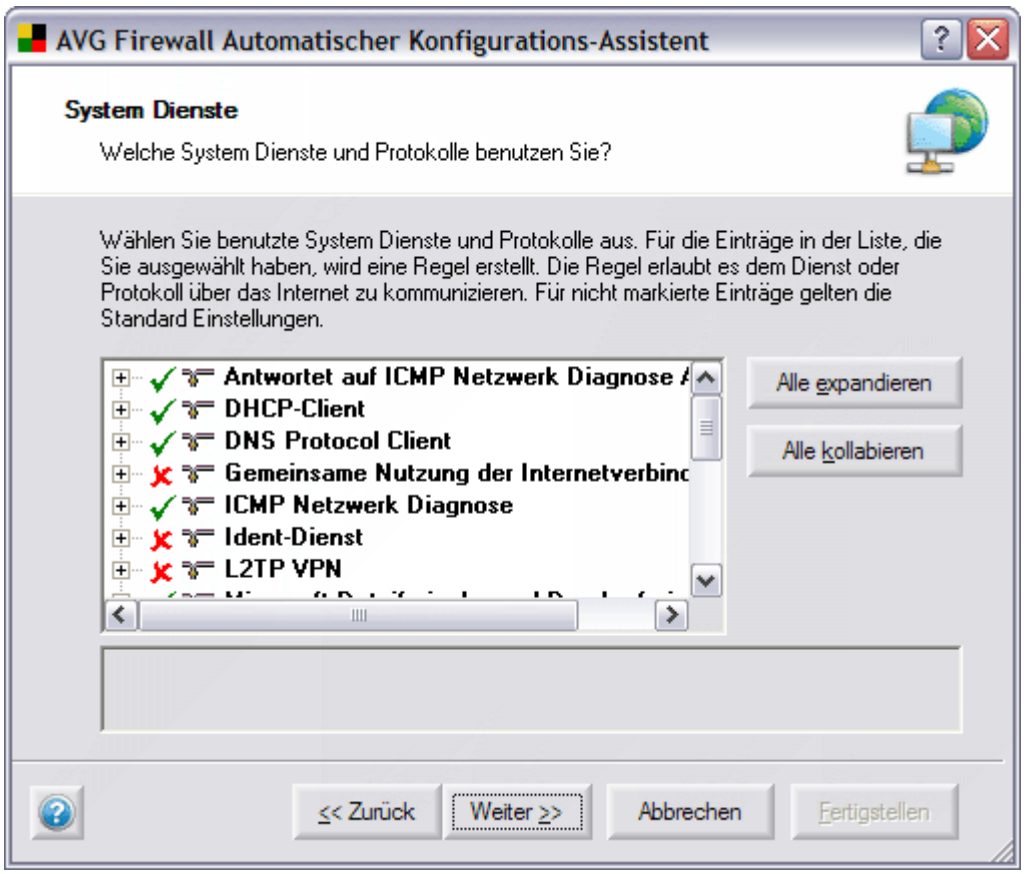
Hinweis: *Der Assistent erkennt alle allgemein bekannten Anwendungen, die über das Netzwerk kommunizieren und definiert Regeln für diese Anwendungen. Allerdings kann der Assistent nicht all diese Anwendungen erkennen.*

Mit dem Dialog ***Scanne Ihren Computer*** können Sie entscheiden, ob alle lokalen Festplatten des Computers (***Kompletter Scan***) oder nur bestimmte Festplatten überprüft werden sollen (***Ausgewählte Bereiche scannen***). Drücken Sie auf ***Weiter***, um die Auswahl zu bestätigen und um mit dem nächsten Dialog fortzufahren:

d) System Dienste

Der Dialog **System Dienste** zeigt eine Liste von Diensten und Protokollen, die auf Ihrem Rechner gefunden wurden und über das Netzwerk Informationen austauschen könnten, an. Markieren Sie in der Liste mit einem „grünen Haken“ alle Dienste/Protokolle, die Sie nutzen möchten.

Empfehlung: *Bitte stellen Sie sicher, dass wirklich nur Dienste und Protokolle in der Liste auf „Erlauben“ gesetzt sind, die Sie auch wirklich benötigen. Es wird für jeden dieser Dienste eine neue Firewall- Regel erstellt, die eine Kommunikation über das Netzwerk genehmigt.*



e) Programme und Anwendungen

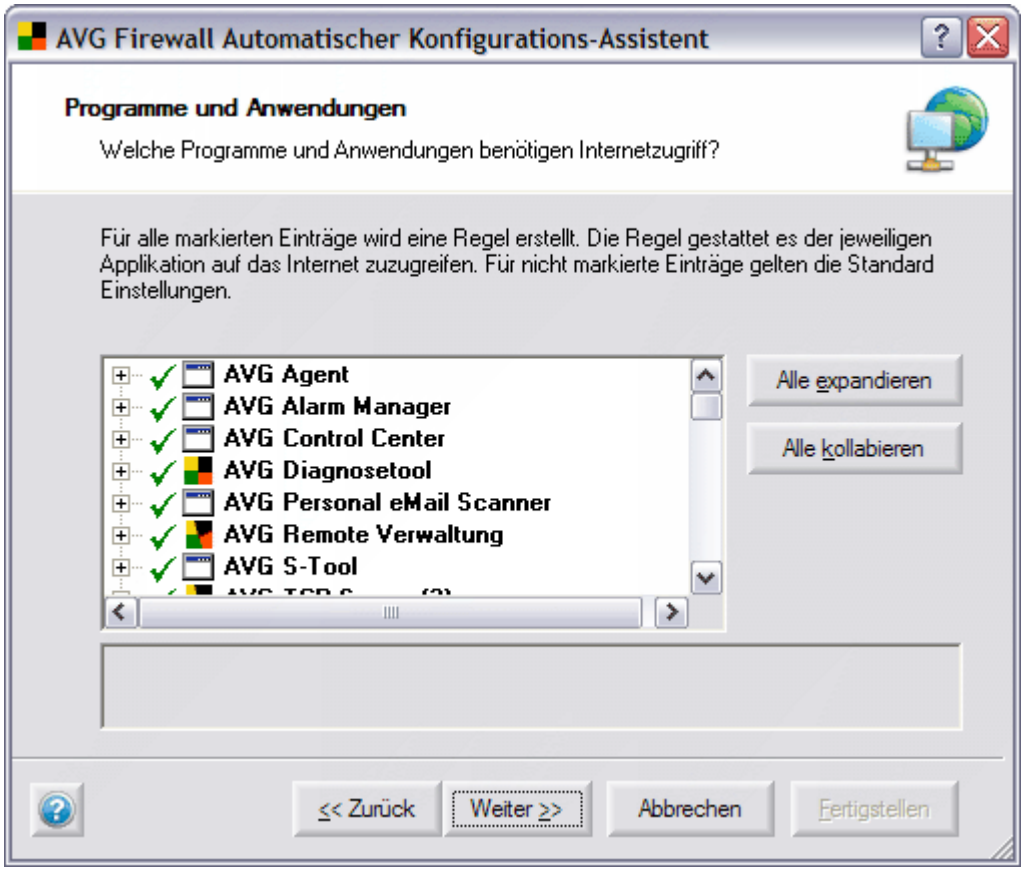
Der Dialog ***Programme und Anwendungen*** bietet eine Liste aller Programme und Anwendungen, die auf Ihrem Computer gefunden wurden und die über das Netzwerk kommunizieren könnten. In der Liste wählen Sie für jede Anwendung die benötigte Netzwerkverbindungsoption wie folgt aus:

✓ Erlauben

✗ Blockieren

? Fragen

⊘ Lege für diese Anwendung keine Regel an.

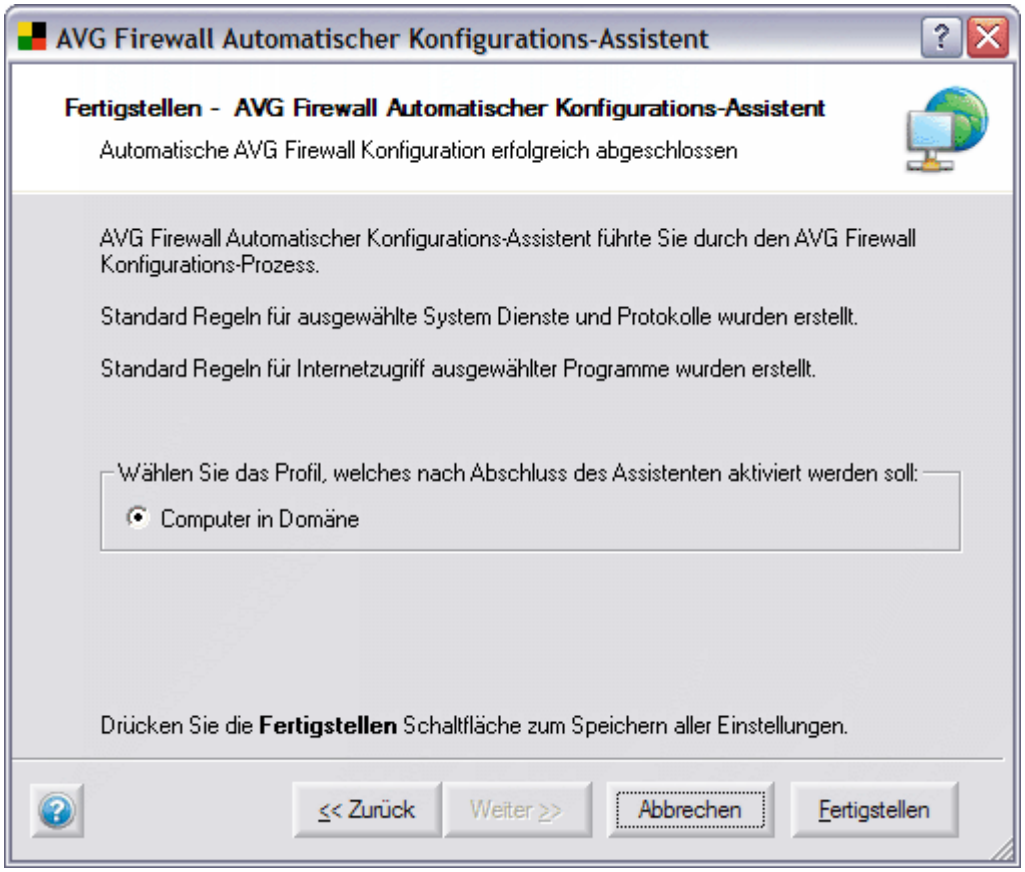


f) Den Firewall Automatischen Konfigurationsassistenten beenden

Im letzten Dialog werden Sie über die Konfiguration der **Firewall**, die Sie in den vorhergehenden Schritten angeben haben, informiert.

Bevor Sie den automatischen Konfigurationsassistenten der Firewall schließen ist es notwendig, ein Profil auszuwählen, das Sie auf Ihrem Rechner nutzen möchten. Sie können aus bis zu drei Profilen: Standalone Computer, Computer in Domäne und Computer unterwegs auswählen, basierend auf den Verbindungsparametern, die Sie im ersten Dialog des Assistenten ausgewählt haben. Später können Sie entsprechend Ihres aktuellen Nutzungsprofils zwischen den vordefinierten Profilen wechseln.

Diese Option bezieht sich auf ein speziell definiertes **Firewall-Profil**. Sie finden ausführliche Informationen im Kapitel 10.7 Firewall Konfiguration – b) Profil.



Drücken Sie auf ***Fertigstellen***, um die Konfiguration zu speichern und den Assistenten zu schließen:

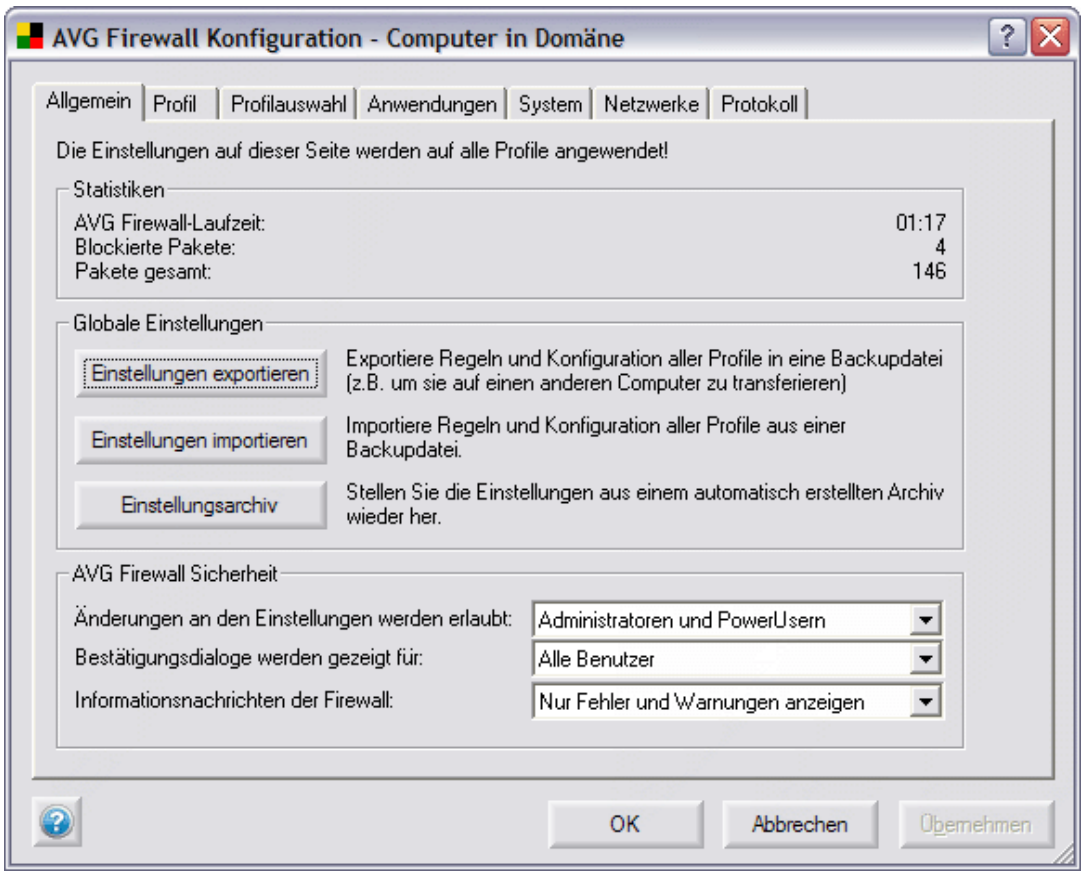
10.7. Konfiguration der Firewall

Die Konfiguration der **Firewall** erreichen Sie über die Schaltfläche ***Konfigurieren*** im Steuerbereich der **Firewall** Komponente im **Control Center**.

Diese Schaltfläche öffnet einen neuen Dialog ***Firewall Konfiguration*** mit sechs Reitern:

- Allgemein
- Profil
- Profilauswahl
- Anwendungen
- System
- Netzwerke
- Protokoll

a) Allgemein



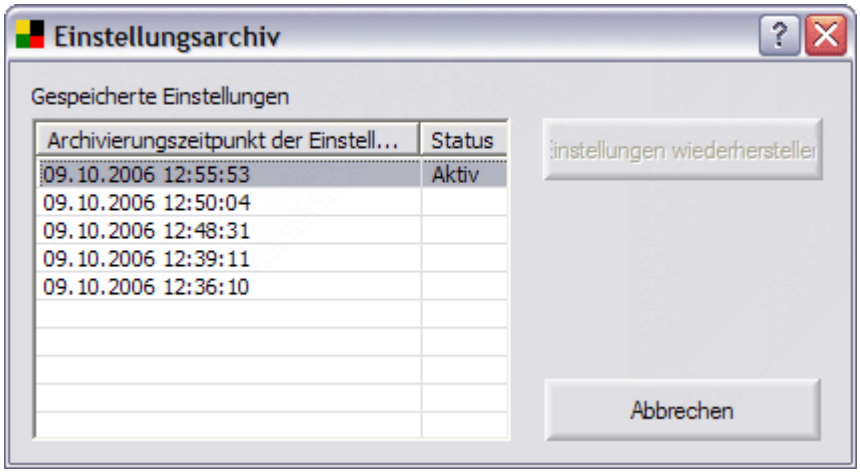
Der Reiter ***Allgemein*** bietet einen Überblick über die Einstelllungen der **Firewall**, die für alle Profile gelten. Dieser Reiter ist in drei Bereiche unterteilt:

- ***Statistiken*** – zeigt einen kurzen Überblick über den aktuellen Zustand der **Firewall** Komponente:
  - Über die Laufzeit der **Firewall** seit dem letzten Neustart
  - Anzahl der blockierten Kommunikationsversuche
  - Gesamtzahl der Kommunikationsversuche
- ***Globale Einstellungen*** – mit der Schaltfläche ***Einstellungen exportieren***/***Einstellungen importieren*** können Sie die definierten Regeln und Einstellungen der **Firewall** in eine Backup-Datei speichern oder eine gesamte Backup-Datei zurückspielen.
- ***Einstellungsarchiv***

  Nach jeder Änderung der Firewall-Konfiguration wird die gesamte Original-Konfiguration in einem Archiv gespeichert. Archivierte Konfigurationen können anschließend über die Schaltfläche Einstellungsarchiv erreicht werden.

  Wenn das Einstellungsarchiv leer ist bedeutet dies, dass keine Änderungen seit der Installation der Firewall vorgenommen wurden.

Sobald Einstellungen verändert und bestätigt werden erscheint ein Dialogfenster, das folgendermaßen aussieht:



In der Spalte Einstellungen wird der genaue Zeitpunkt angegeben, wann die Änderung durchgeführt wurde. Die Spalte Status zeigt an, welche Konfiguration aktiv ist.

Die aktuelle Konfiguration der Firewall wird markiert als ***Aktiv***. Aufzeichnungen werden immer chronologisch sortiert, wobei die Einstellungen, die an oberster Stelle stehen, die neuesten Einstellungen sind, die durchgeführt wurden.

Das Einstellungsarchiv verfolgt jede Änderung der Firewall-Konfiguration, jedoch nicht Profil- Änderungen (d.h. Umschalten von Computer in Domäne auf Computer unterwegs wird nicht erkannt). Änderungen werden archiviert, sobald sie die gewünschte Konfiguration bestätigen, indem Sie auf die Schaltfläche OK oder Anwenden klicken.

Die maximale Anzahl gespeicherter Aufzeichnungen ist 10. Wenn Sie weitere Aufzeichnungen speichern werden die ältesten Aufzeichnungen überschrieben.

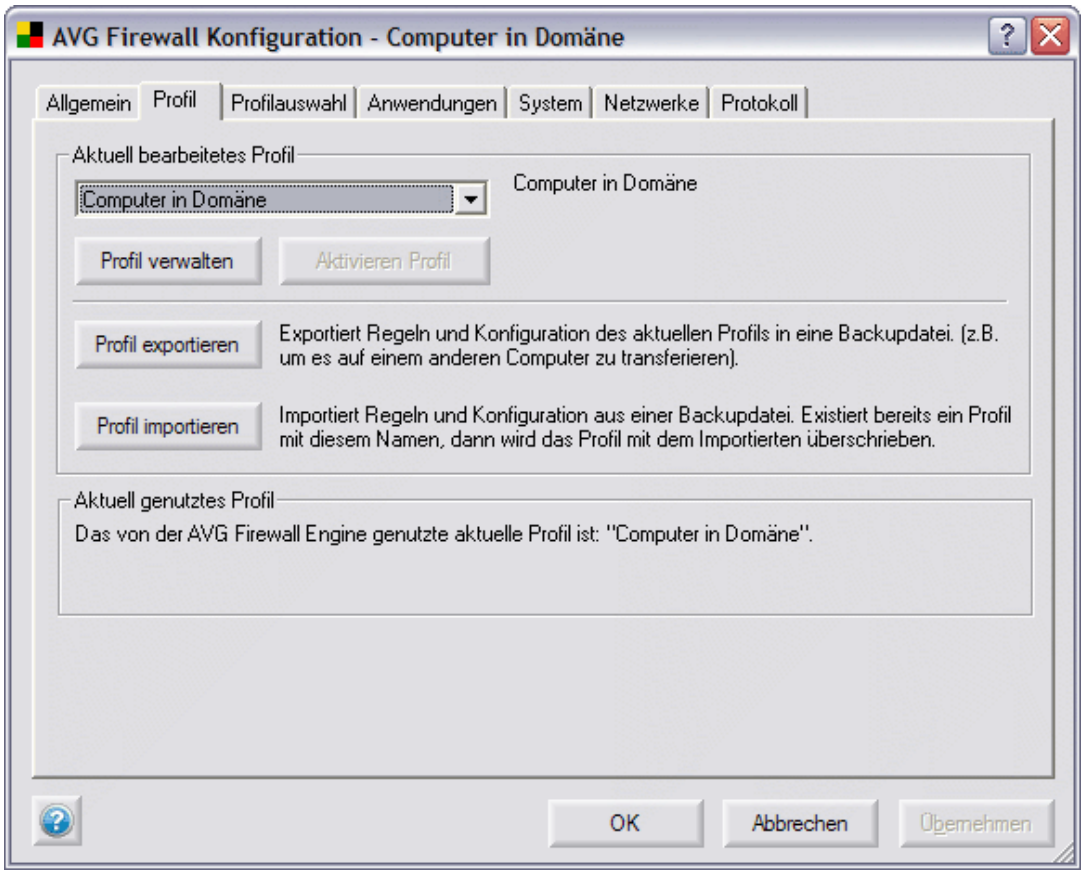
Das Aktivieren einer gespeicherten Einstellung kann über die Schaltfläche Einstellungen wiederherstellen durchgeführt werden. Hiermit wird die gewählte Konfiguration sofort wieder aktiv.

o ***Firewall-Sicherheit*** – in diesem Bereich können Sie Regeln für die Rechte für die Konfiguration der **Firewall** vergeben. Legen Sie fest, wer die Einstellungen der **Firewall** ändern darf und wem der Bestätigungsdialoge und die Firewall- Benachrichtigungen angezeigt werden sollen. Hierbei können Sie aus den folgenden drei Kategorien mit unterschiedlichem Autoritätslevel wählen:

- ***Administrator*** – kontrolliert vollständig den PC und hat das Recht, jeden Benutzer einer Gruppe mit speziell definierten Rechten zuzuordnen
- ***Administrator und PowerUser*** – der Administrator kann jeden Benutzer einer besonderen Gruppe zuordnen (PowerUser) und den Mitgliedern dieser Gruppe Rechte vergeben

- ***Alle Benutzer*** – andere Benutzer, die nicht einer bestimmten Gruppe zugeordnet sind

b) Profil



Im Reiter ***Profil*** können Sie das gewünschte **Firewall** Profil (die Option Profilspezifikation ist nur unter den folgenden Betriebssystemen verfügbar: Windows NT/Win2k/WinXP) auswählen. Das Hauptanliegen der **Profil**auswahl ist die Möglichkeit, unterschiedliche **Firewall** Sicherheitsniveaus vorzugeben.

Zum Beispiel**:** Betrachten Sie die zwei folgenden Profile – ***Computer unterwegs*** und ***Computer in Domäne***. Während einer Geschäftsreise möchten Sie sich im Hotel oder am Flughafen über Ihr Notebook mit dem Internet verbinden. Hierbei ist das Risiko für Sie deutlich höher als bei einer Verbindung zum Netz in Ihrer Firma. Aus diesem Grund empfehlen wir, dass Sie ein spezielles Profil ***Computer unterwegs*** mit Parametern, die ein höheres Sicherheitsniveau sicherstellen, anlegen. Im Gegensatz dazu kann das Profil ***Computer in Domäne*** mit einem niedrigeren Sicherheitsniveau definiert werden. Zusätzlich können im Profil ***Computer in Domäne*** einige Dienste, die während einer Geschäftsreise nicht benötigt werden oder gewünscht sind, zugelassen werden (z.B.: Datentausch).

Typischerweise können Sie aus den folgenden Profiloptionen auswählen:

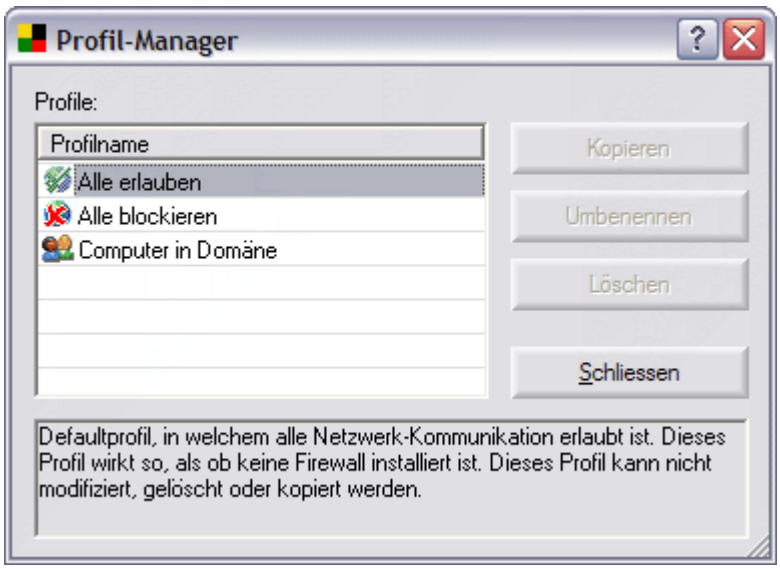
o Alle erlauben

- Alle blockieren
- Computer in Domäne (Geschäftsnetzwerk)
- Computer unterwegs (Notebook auf Reisen)
- Standalone Computer (Einzelplatzrechner)

Ausgangsbasis (Default) ist das Profil, das mit den Parametern gebildet wurde, die Sie im Firewall Konfigurationsassistenten angeben haben. Jedes Profil umfasst spezifische Einstellungen auf Ihrem PC und jedem ist ein angemessenes **Firewall-** Sicherheitsniveau zugewiesen. Die geeignete Profiloption kann aus dem Dropdown Menü ausgewählt werden; anschließend bestätigen Sie Ihre Auswahl mit der Schaltfläche ***Aktivieren Profil***.

Ein **Firewall-** Profil können Sie mit einer der folgenden zwei Schaltflächen setzen.

- ***Profil verwalten*** – öffnet einen neuen Dialog ***Profil-Manager***, in dem Sie jedes ausgewählte Profil editieren oder ein neues Benutzerprofil anlegen können.



  Es stehen die folgenden Schaltflächen zur Verfügung:

  - ***Kopieren*** – macht die Erstellung eines neuen Profils für Sie einfacher und komfortabler: Hierzu selektieren Sie bitte ein Profil in der Liste der Profile und klicken auf die Schaltfläche ***Kopieren***. Ein neues Profil wird mit genau den Einstellungen des geklonten Profils angelegt. Nun können Sie ganz einfach die Einstellungen des neuen Profils editieren und setzen.
  - ***Umbenennen*** – klicken Sie auf diese Schaltfläche, um den ausgewählten Profilnamen zu editieren
  - ***Löschen*** – klicken Sie auf diese Schaltfläche, um das ausgewählte Profil aus der Liste zu löschen (wenn es nicht gerade benutzt wird)
  - ***Schliessen*** – schliesst den Dialog ***Profil-Manager***

- ***Aktivieren Profil*** – bestätigen Sie mit dieser Schaltfläche die Profilauswahl oder jegliche Änderung an den Profileinstellungen

Im unteren Bereich des Reiters ***Profil*** finden Sie die Schaltflächen ***Profil exportieren/importieren***, die Ihnen ermöglichen, dass bestimmte Profile der **Firewall** in eine Backup-Datei exportiert oder die gesamten Profile aus einer Backup-Datei zurückgespielt werden.

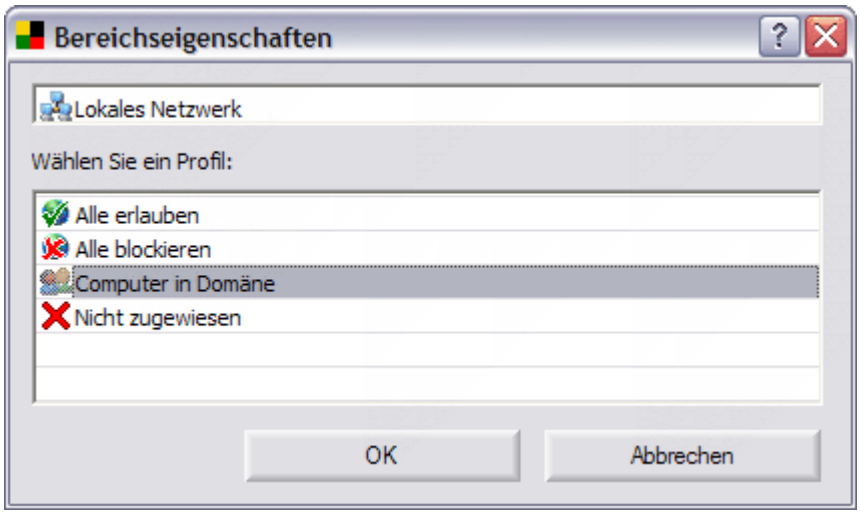
c) ***Profilauswahl***

Im Reiter Profil umschalten können Sie Netzwerkbereiche und lokale Netzwerk-Verbindungen verwalten. Sie können bestimmte Profile lokalen Verbindungen und Netzwerkbereichen zuweisen.

Die Firewall kann das aktive Profil gemäß der aktuell genutzten Art von Netzwerkverbindung umschalten. Dieses Feature ist besonders hilfreich für:

- ***Benutzer mit Notebooks –*** die die gleiche Netzwerk-Verbindung zum Verbinden mit verschiedenen Netzwerken an verschiedenen Orten (Geschäftsreise, Heimarbeitsplatz usw.) nutzen.
- ***Benutzer, die mehr als eine Netzwerkverbindung nutzen –*** z.B. xDSL-Verbindungen für einige Backup-Verbindungen (Dial-Up, Wireless...)
- ***Benutzer mit mehr als einer Netzwerkverbindung***

Wann auch immer Sie sich mit einer neuen (unerkannten) Verbindung verbinden, erscheint der Dialog ***Neuer Bereich***. Hier können Sie das passendste Profil für die aktuelle Netzwerkverbindung wählen; anschließend klicken Sie auf die Schaltfläche ***Profil zuweisen.***

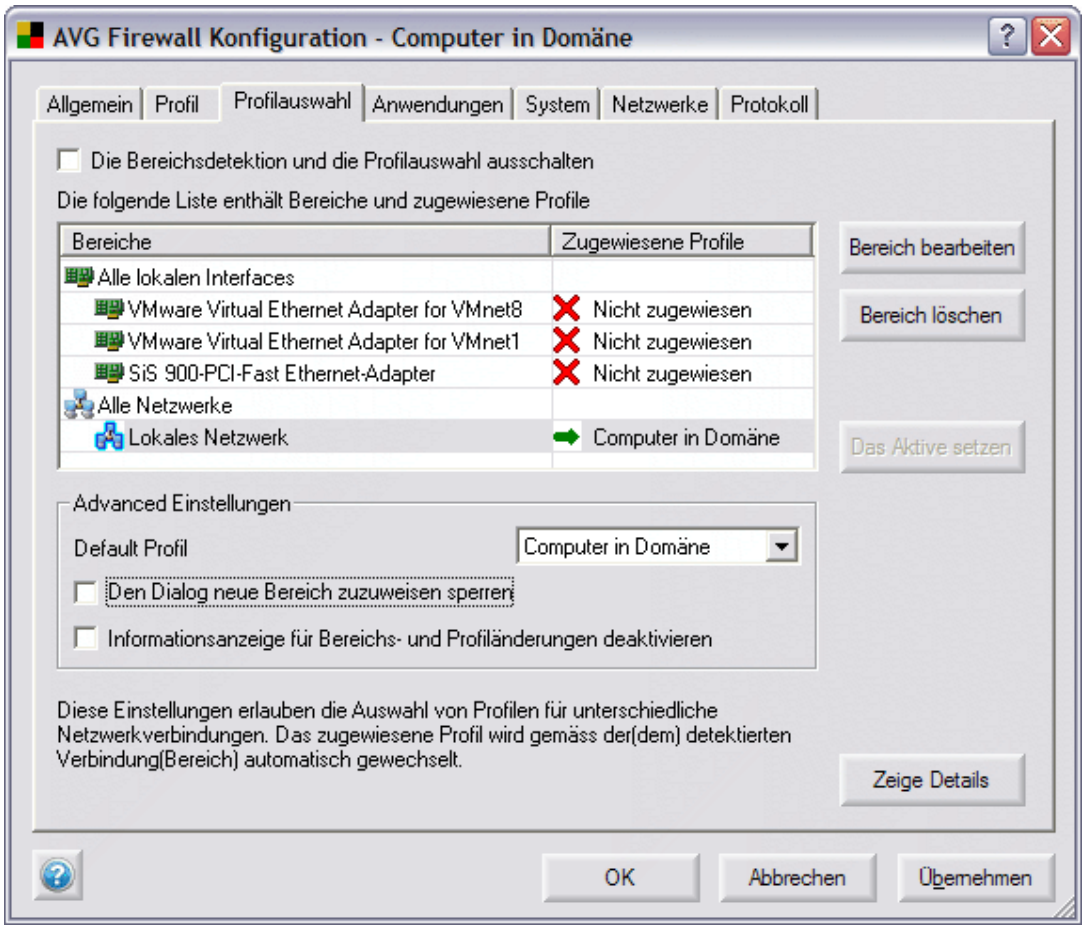


- ***Erkannter Bereich*** – gibt die Art der Netzwerkverbindung an, die erkannt wurde. Sie können diesen Bereich umbenennen, indem Sie auf das Textfeld klicken; somit wird es für Sie leichter, sich daran zu erinnern, dass Sie mehrere Verbindungen auf einer regulären Basis nutzen.
- **Profil auswählen** – enthält eine Liste aller verfügbaren Profile. Wählen Sie das Profil, das für Sie am geeignetsten ist.
- **Informationsanzeige für Bereichs- und Profiländerungen dekativieren** – markieren Sie dieses Kontrollkästchen, um das komplette Feature Profilerkennung zu deaktivieren.

- Den Dialog neuer Bereich zuzuweisen sperren – markieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass der Dialog Neuer Bereich weiterhin angezeigt werden soll. Anschließend wird das Standard-Profil automatisch zugewiesen.

  Die Bedienschaltflächen sind Folgende:

- ***Profil zuweisen*** - Wenn Sie auf diese Schaltfläche klicken wird das gewählte Profil immer automatisch dieser Verbindung zugeordnet und zukünftig wird dieser Dialog nicht mehr beim bei dieser Verbindung angezeigt.
- ***Kein Profil*** - klicken Sie auf diese Schaltfläche, um die Verbindungsart ohne ein Profil beizubehalten. Die Firewall wird Sie jedes Mal fragen, wenn diese Verbindungsart erkannt wird. Um dieses Fenster zu deaktivieren (vor der Bestätigung Ihrer Wahl) markieren Sie entweder das Kontrollkästchen ***Informationsanzeige für Bereichs- und Profiländerungen deaktivieren***, damit der gesamte Bereich des Erkennungssystems deaktiviert wird oder markieren Sie das Kontrollkästchen ***Den Dialog neuer Bereich zuzuweisen sperren***,um den Bestätigungsdialog zu deaktivieren (das Profil wird automatisch zugewiesen).

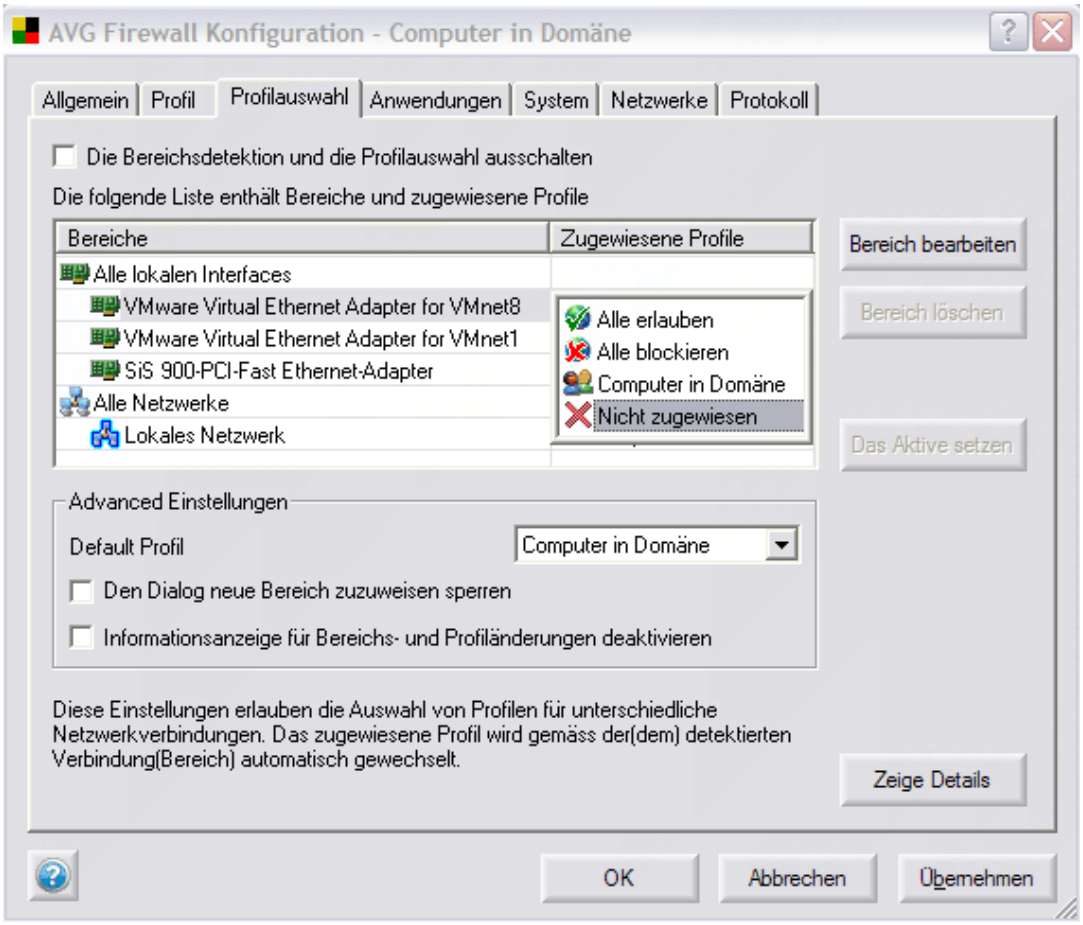


Benutzer können einzelne Profile für jede Verbindungsart und/oder Netzwerk-Verbindungen erstellen und diese anschließend nach Wunsch zuordnen.

Um diese Option zu deaktivieren markieren Sie einfach das Kontrollkästchen ***Informationsanzeige für Bereichs- und Profiländerungen deaktivieren***.

Weitere Einzelheiten zum gewählten Netzwerkbereich erhalten Sie über die Schaltfläche ***Zeige Details***.

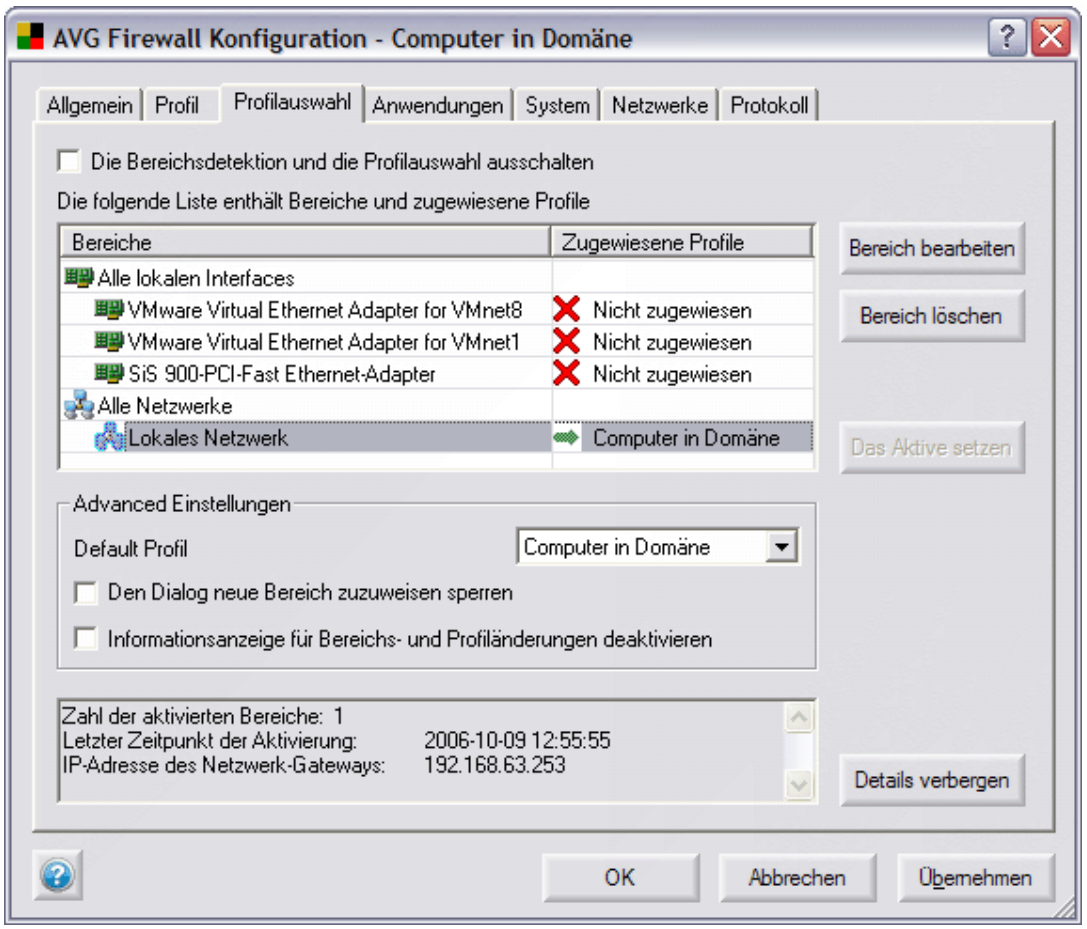
Die Hauptliste enthält Bereiche und zugehörige Profile Wenn Sie in die gewünschte Zeile in der Spalte *Zugewiesene Profile* klicken, wird eine Liste der Profile angezeigt, die aktuell zugeordnet werden können:



Wenn Sie kein Profil einer bestimmten Schnittstelle oder einem Bereich zuordnen möchten, lassen Sie diese Option als ***Nicht zugewiesen***.

- Um den Namen des Netzwerkbereichs zu ändern wählen Sie bitte den Bereich, den Sie umbenennen möchten und klicken auf die Schaltfläche ***Umbenennen***.
- Zum Löschen des Netzwerkbereichs wählen Sie den gewählten Bereich und klicken auf die Schaltfläche ***Löschen***.

  Bitte beachten Sie: *Wenn Sie alle Netzwerkbereiche löschen oder wenn in der Liste kein Netzwerkbereich angezeigt wird, erscheint eine neue Schaltfläche* ***Übernehmen****. Wenn Sie auf diese Schaltfläche klicken, können Sie einfach den aktuell aktiven Netzwerkbereich zuordnen.*



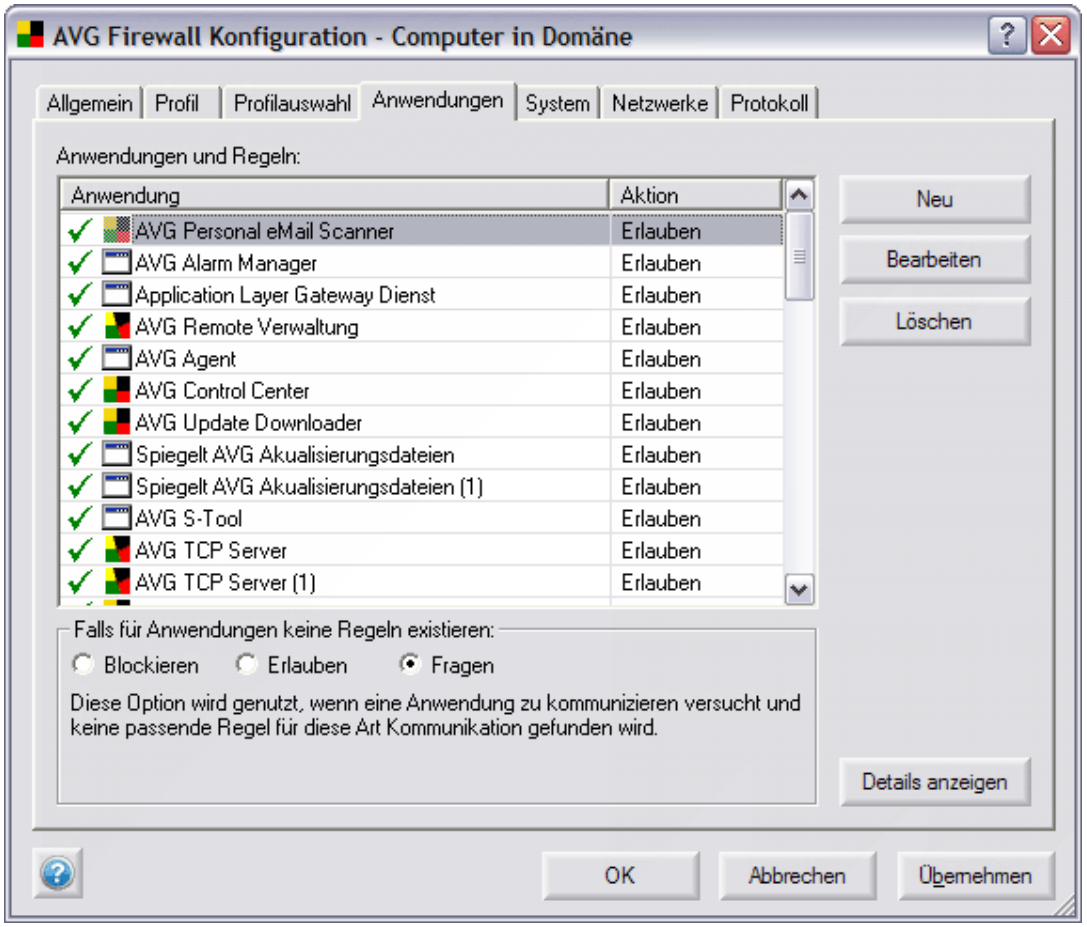
- o ***Standard-Profil*** - dieses Profil wird automatisch aktiviert, wenn:
  - Ein neuer Bereich erkannt wurde.
  - Ein Fehler während der Erkennung eines neuen Bereichs aufgetreten ist (wenn z.B. keine aktive Verbindung besteht).
  - Ein Bereich mit keinem zugehörigen Profil aktiv ist.
- o ***Den Dialog neuer Bereich zuweisen sperren*** - markieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass der Dialog ***Neuer Bereich*** angezeigt wird. Anschließend wird automatisch das Standard-Profil genutzt.
- o ***Informationsanzeige für Bereichs- und Profiländerungen deaktivieren*** - markieren Sie dieses Kontrollkästchen, um die Anzeige von Informationen über Bereiche oder Profiländerungen in der Systemanzeige zu deaktivieren.

Bitte beachten Sie:

(i) Ein Profil einer Netzwerk-Verbindung zuzuordnen hat höhere Priorität als die Zuordnung zu einem Netzwerkbereich. Dies bedeutet, dass Sie durch die Zuordnung eines Profils zu Ihrer Netzwerk-Verbindung dieses Profil immer genutzt wird, ohne Berücksichtigung des Netzwerkbereichs.

(ii) Im abgesicherten Modus werden automatische Profile deaktiviert.

d) Anwendungen - Basis-Einstellungen



Im Hauptbereich des Reiters ***Anwendungen*** können Sie die Liste aller Anwendungen sowie die Liste aller Regeln, die für jede Anwendung angelegt wurden, sehen. In der Liste der Anwendungen wird immer eins der unten aufgeführten Symbole links neben Programmsymbol dargestellt und der Name der Anwendung angegeben:

- Erlauben
- Blockieren
- Fragen
- Fortgeschrittene Konfiguration

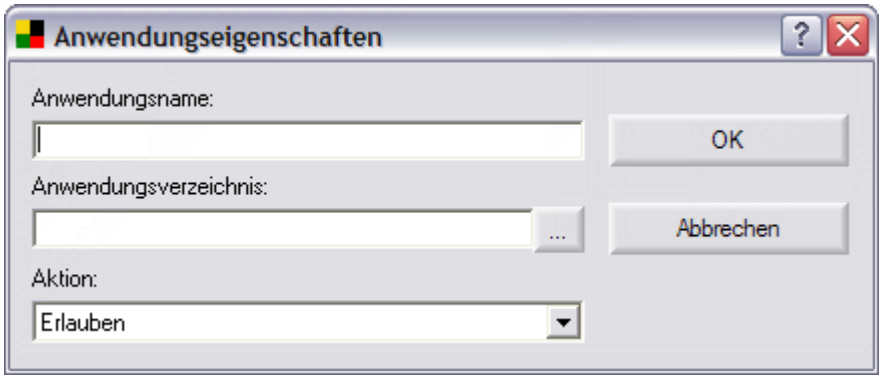
(Sie finden ausführliche Informationen über besondere Aktionen im Kapitel 10.4 – Aktionen der Firewall)

Klicken Sie auf dieses Symbol, wenn Sie die Regel zu der momentan hervorgehobenen Anwendung ändern möchten. Wählen Sie aus dem neu geöffneten Kontextmenü eine andere Aktion:

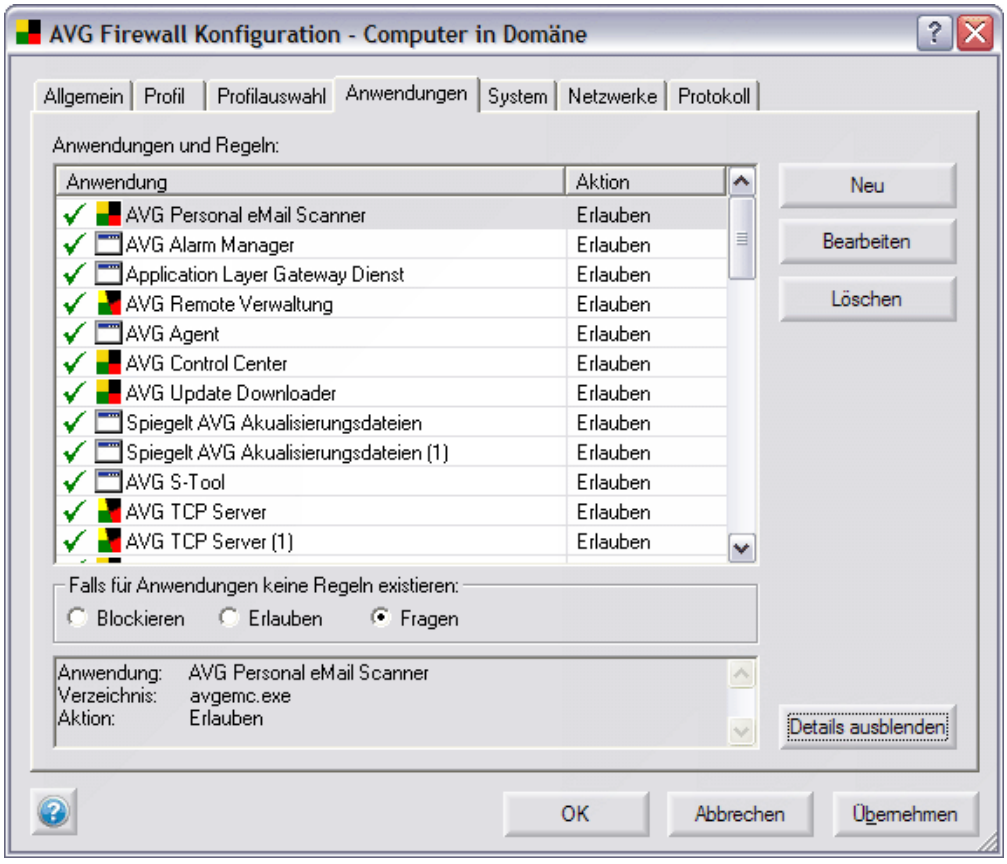
Drücken Sie die ***Eingabetaste*** der Tastatur, um Ihre Wahl zu bestätigen oder die Taste ***Esc.,*** um abzubrechen.

Der Reiter ***Anwendungen*** bietet die folgenden Schaltflächen:

- ***Neu/Bearbeiten*** – diese Schaltflächen öffnen ein neues Dialogfenster: ***Anwendungseigenschaften***, dort können Sie eine neue Regel für eine bestimmte Anwendung anlegen (editieren). Im Dialog müssen Sie den Anwendungsnamen angeben, den momentanen Pfad zu der Anwendung auf Ihrer Festplatte und Sie müssen der Anwendung die passende Aktion zuweisen (z.B. eine Aktion, die durchgeführt wird, wenn die Anwendung versucht, mit irgendeinem Netzwerkport zu kommunizieren).



- ***Löschen*** – mit dieser Schaltfläche löschen Sie die für eine bestimmte Anwendung definierte Regel und entfernen sie ihre passende Aktion aus der Liste im Reiter ***Anwendungen*** des Dialogfensters ***Firewall Konfiguration***.
- ***Details anzeigen/ausblenden*** – im gleichen Dialogfenster bietet diese Schaltfläche einen kurzen Überblick über detaillierte Informationen hinsichtlich der gerade in der Liste hervorgehobenen Anwendung:
  - ***Anwendungsname*** – Name der Anwendung
  - ***Anwendungsverzeichnis*** – momentaner Pfad zu der entsprechenden Anwendung
  - ***Aktion*** – Aktion, die dieser Anwendung zugewiesen ist



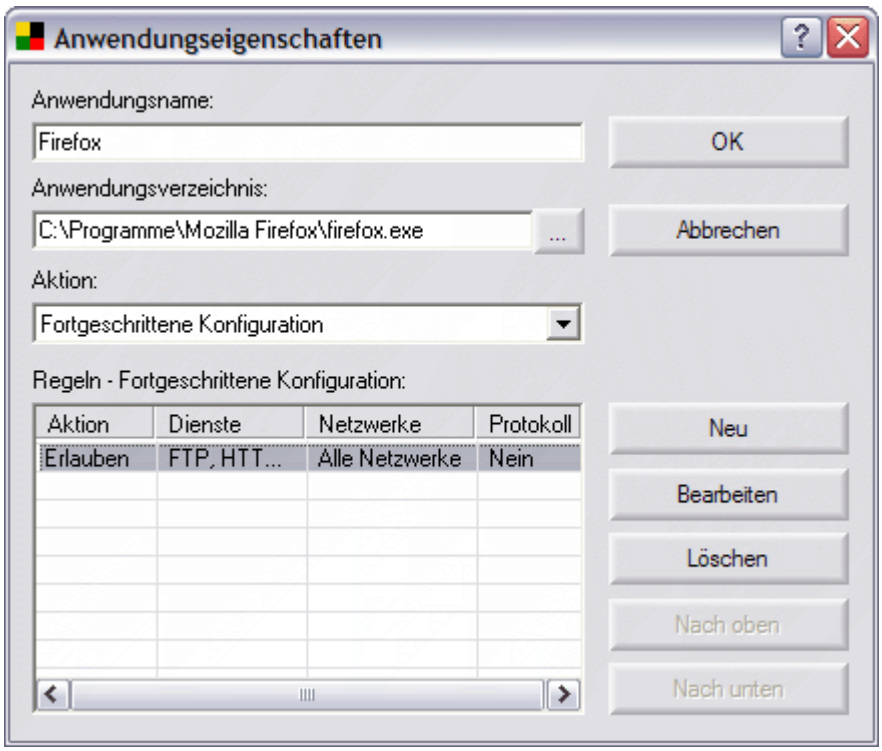
Im Reiter ***Anwendungen*** finden Sie außerdem einen Bereich ***Falls für Anwendungen keine Regeln existieren***; hier sollten Sie die Aktion angeben, die durchgeführt werden soll, falls eine neue Anwendung über das Netzwerk zu kommunizieren versucht und bisher noch keine Regel für diese Anwendung in der **Firewall** festgelegt wurde.

e) Anwendungen – Advanced Einstellungen

Vorsicht! Die Advanced Einstellungen sind nur für Benutzer mit Fachwissen und Erfahrung empfohlen!

Im Reiter ***Anwendungen*** können Sie die fortgeschrittene Einstellungen für ausgewählte Anwendungen konfigurieren. Bearbeiten Sie eine Anwendung zum ersten Mal, dann starten Sie über die Schaltfläche ***Neu*** einen neuen Dialog ***Anwendungseigenschaften*** und wählen im Bereich ***Aktion*** die Option ***Fortgeschrittene Konfiguration***.

Haben Sie aus der Liste der Anwendungen im Reiter ***Anwendungen*** eine Anwendung bereits ausgewählt, so öffnet sich der Dialog ***Anwendungseigenschaften*** in folgender erweiterter Form:



Im erweiterten Dialog ***Anwendungseigenschaften*** sind die folgenden Schaltflächen verfügbar:

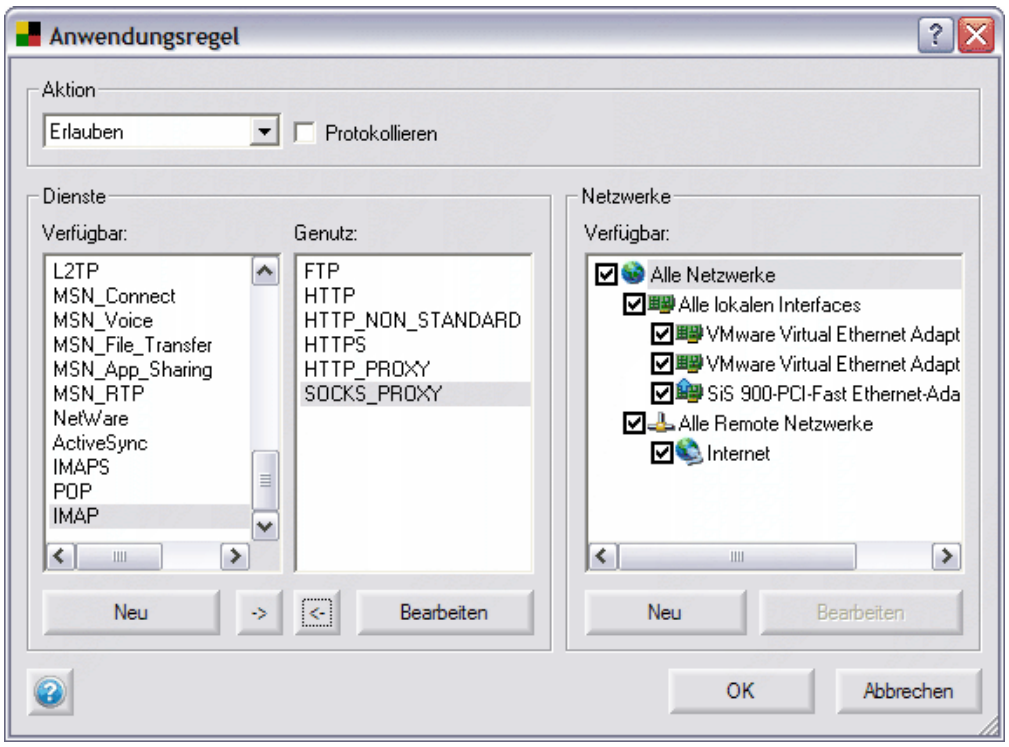
- ***Neu / Bearbeiten*** – öffnet einen neuen Dialog **Anwendungsregel**, in dem Sie die Parameter für eine neue Anwendungsregel definieren oder die Parameter einer existierenden Regel ändern können.
- ***Löschen*** – entfernt die zurzeit selektierte Regel aus der Liste der Regeln.
- ***Nach oben*** – schiebt die Regel in der Regelliste eine Position nach oben.
- ***Nach unten*** – schiebt die Regel in der Liste der Regeln nach unten.

Im unteren Bereich dieses Dialogs sehen Sie einen neuen Abschnitt, die ***Regeln – Fortgeschrittene Konfiguration***. Dieser Abschnitt enthält Informationen, aufgeteilt in vier Spalten:

- ***Aktion*** – zeigt die der ausgewählten Anwendung zugeordnete Art der Aktion an
- ***Dienste*** – zeigt zugewiesene Netzwerkdienste, auf die sich die Anwendungsregel bezieht
- ***Netzwerke*** – Informationen über ein Netzwerk, auf das die Anwendungsregel zielt
- ***Protokoll*** – informiert Sie, ob die ausgewählten Anwendungsereignisse in der Protokolldatei erfasst werden

Es sind die folgenden Schaltflächen verfügbar:

- ***Neu*** – öffnet einen neuen Dialog **Anwendungsregel**, dort können Sie eine neue Regel für die ausgewählte Anwendung erstellen:



Der Dialog ist in drei Abschnitte unterteilt:

- ***Aktion*** – aus dem Dropdown Menü wählen Sie eine Aktion aus, die durchgeführt werden soll, sofern alle Bedingungen der Netzwerkkommunikation (wie sie im unteren Teil dieses Dialogs gesetzt sind) erfüllt sind. Die verfügbaren Aktionen sind: Blockieren / Erlauben / Fragen (lesen Sie auch die Beschreibung der Aktionen im Kapitel 10.4 Aktionen der Firewall)

  Der Abschnitt ***Aktion*** enthält auch den Punkt ***Protokollieren*** – setzen Sie hier die Markierung, wenn Sie möchten, dass die Kommunikation der Anwendung in der **Firewall** Protokolldatei aufgezeichnet wird.

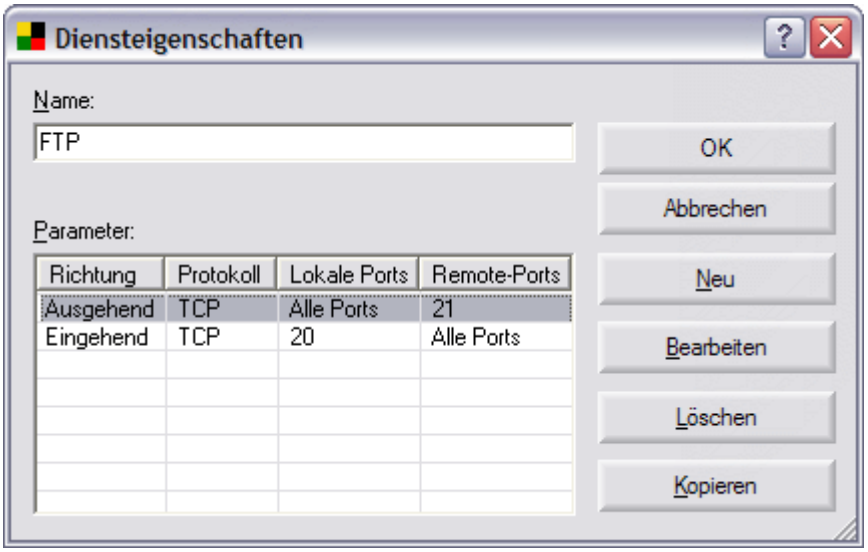
- ***Dienste*** – dieser Bereich biete zwei Listen von Diensten an:

  - ***Verfügbar*** – eine Liste von Diensten, die für die Anwendung in den Defaulteinstellungen festgelegt und Dienste, die schon durch den Benutzer definiert wurden
  - ***Genutzt*** – die Liste von Diensten, die durch die hier definierte Anwendungsregel abgedeckt werden. Diese Liste ist eine Teilmenge der Liste verfügbaren Dienste.

    Sie können mittels der Schaltflächen **->** oder **<-** die Einträge von einer Liste in die andere verschieben. Verschieben Sie einen Eintrag aus der Liste der ***verfügbaren Dienste*** in die Liste der ***genutzten Dienste***, so bedeutet das, dass dieser Dienst beim Anwenden dieser Regel auf diese Anwendung berücksichtigt wird.

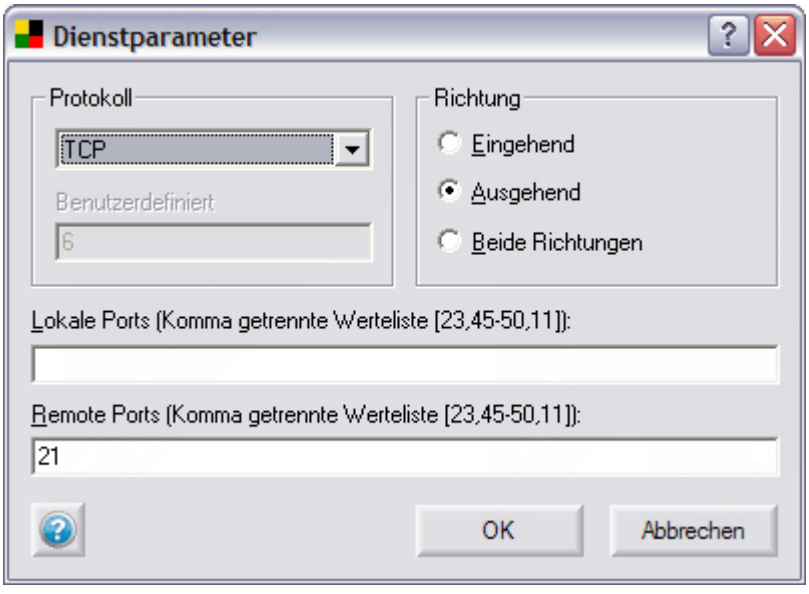
    Es gibt zwei Schaltflächen im Bereich ***Dienste***:

- ***Neu / Bearbeiten*** – öffnet einen neuen Dialog **Diensteigenschaften**, dort können Sie die neuen Dienstparameter angeben oder die schon für Dienste gesetzte Parameter editieren:



Im Dialog ***Diensteigenschaften*** geben Sie den Namen des Dienstes im Feld ***Name*** an. Der Dialog bietet die folgenden Schaltflächen:

- ***Neu / Bearbeiten*** – öffnet einen neuen Dialog ***Dienstparameter***, dort können Sie die Parameter für bestimmte Dienstelemente setzen/ abändern (Protokoll, Richtung der Kommunikation, Lokale Ports und Remote Ports):



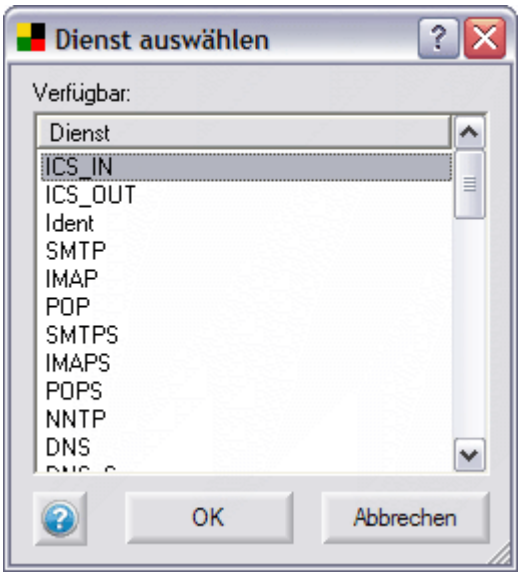
- ***Protokoll*** – wählen Sie aus dem Dropdown Menü ein vordefiniertes Protokoll oder wählen Sie die Option ***Benutzerdefiniert***, geben Sie dann die Standardprotokollnummer im Feld ***Benutzerdefiniert*** an (der Wert "0" steht für alle Protokolle).

  - Richtung – definiert die Richtung des Dienstes

- Lokal Ports – führt alle lokalen Ports auf oder definiert einen Bereich

- Remote Ports – führt alle Ports auf oder definiert einen Bereich

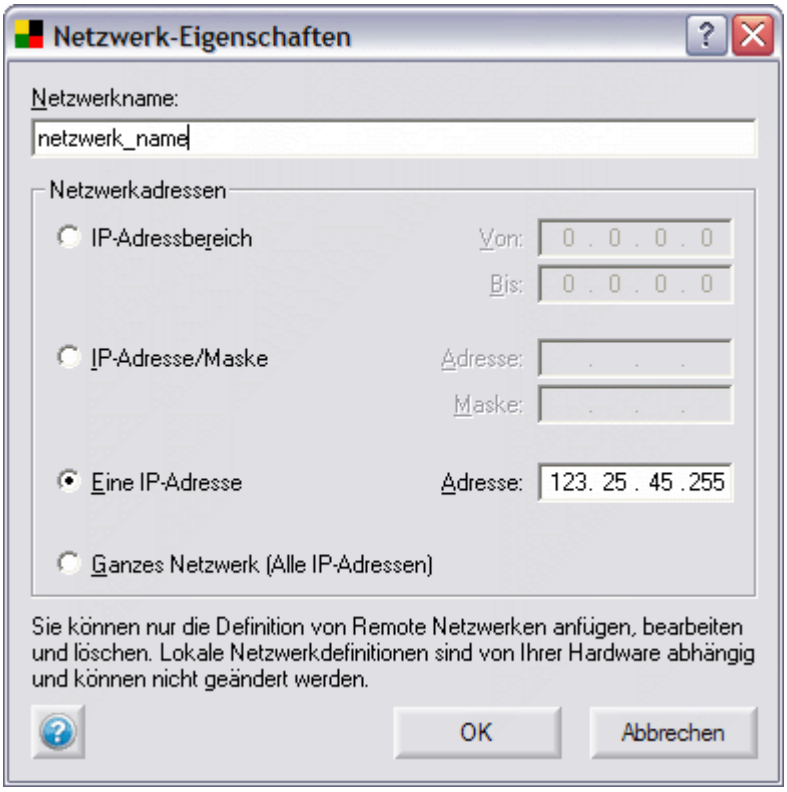
- ***Löschen*** – entfernt den ausgewählten Eintrag aus der Liste der Diensteigenschaften.
- ***Kopieren*** – macht es für Sie einfacher, eine neue Diensteigenschaft anzulegen, indem die bereits definierten Parameter eines existierenden Eintrags kopiert werden. Die Schaltfläche öffnet einen neuen Dialog **Dienst auswählen**, in dem Sie aus einer Liste von Diensten denjenigen auswählen, dessen Einträge Sie kopieren möchten:



o ***Netzwerke*** – dieser Bereich bietet einen Kontrollbaum mit einer Liste der verfügbaren Netzwerke. Setzen Sie einen Haken in das Kontrollkästchen für jedes Netzwerk, dem die jeweilige Anwendungsregel zugewiesen werden soll.

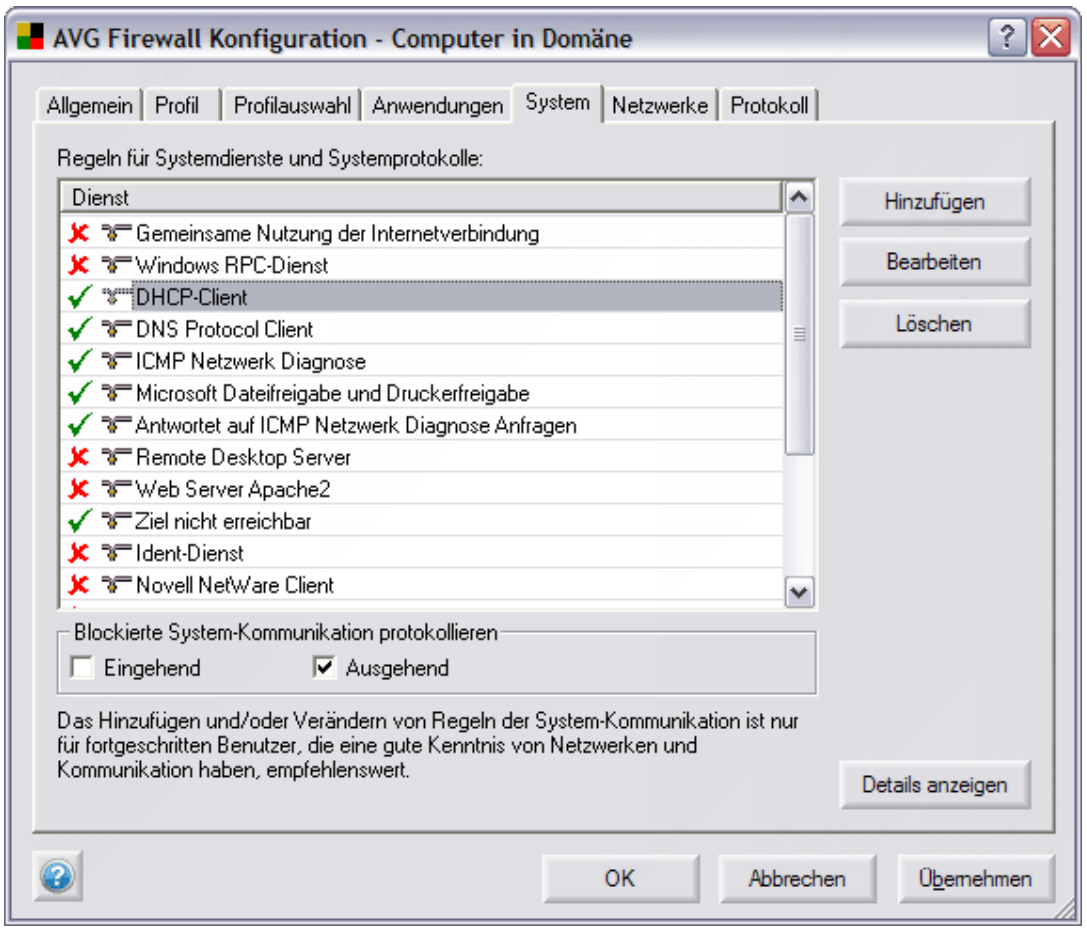
Es gibt zwei Schaltflächen im Bereich ***Netzwerke***:

- ***Neu / Bearbeiten*** – öffnet einen neuen Dialog ***Netzwerk-Eigenschaften***, in dem Sie neue Netzwerkparameter definieren (editieren) können: ***Netzwerkname*** und ***Netzwerkadressen*** (legt den IP-Adressbereich fest):



f) System

Jede Abänderung der Parameter im Reiter System wird nur erfahrenen Benutzern empfohlen!



Der Reiter ***System*** gibt einen Überblick der für Systemdienste angegebenen Regeln, die über das Netz kommunizieren müssen. Im Vergleich zu den Anwendungen können hier nur zwei Aktionen einem Systemdienst zugewiesen werden:

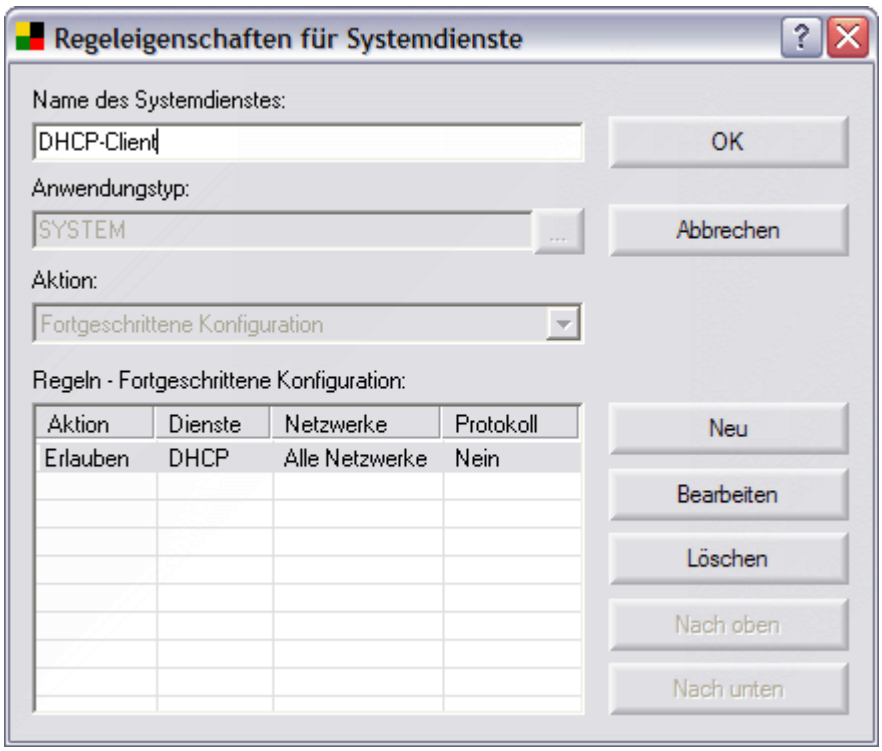
- ***Erlauben*** – angezeigt durch einen grünen Haken vor dem Namen des Systemdienstes
- ***Blockieren*** – angezeigt durch ein rotes Kreuz vor dem Namen des Systemdienstes

Falls Sie die Regel, die einem Systemdienst zugewiesen ist, ändern möchten, klicken Sie auf das farbige Symbol (grüner Haken / rotes Kreuz) in der Liste der Dienste und das Symbol wechselt automatisch zum Gegenteiligen (die Regel hat sich geändert).

Im Bereich ***Blockierte System-Kommunikation protokollieren*** können Sie festlegen, ob Sie entweder nur die eingehende oder die ausgehende blockierte oder die Kommunikation in beide Richtungen protokollieren möchten.

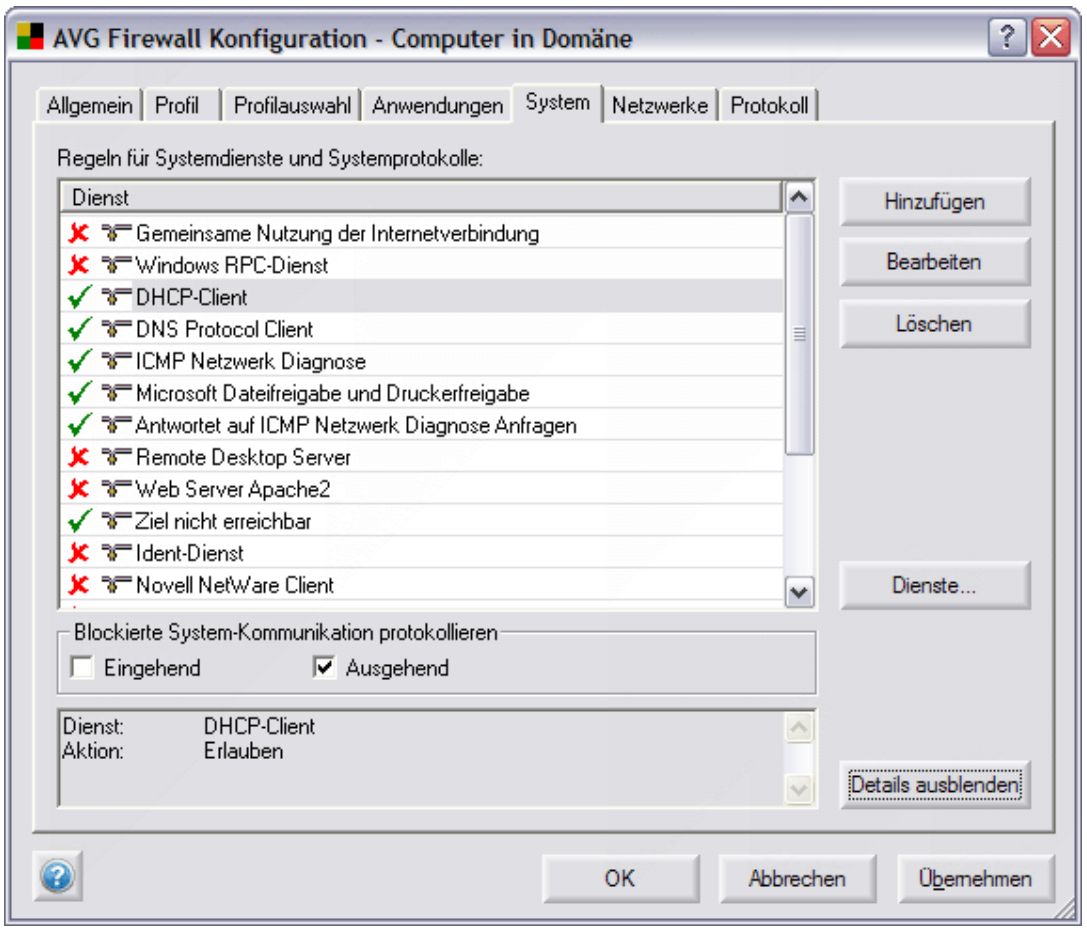
Der Reiter ***System*** bietet weiter die folgenden Schaltflächen:

- ***Hinzufügen / Bearbeiten*** – öffnet einen neuen Dialog, in dem Sie eine neue Systemdienstregel hinzufügen oder eine aktuelle abändern können:

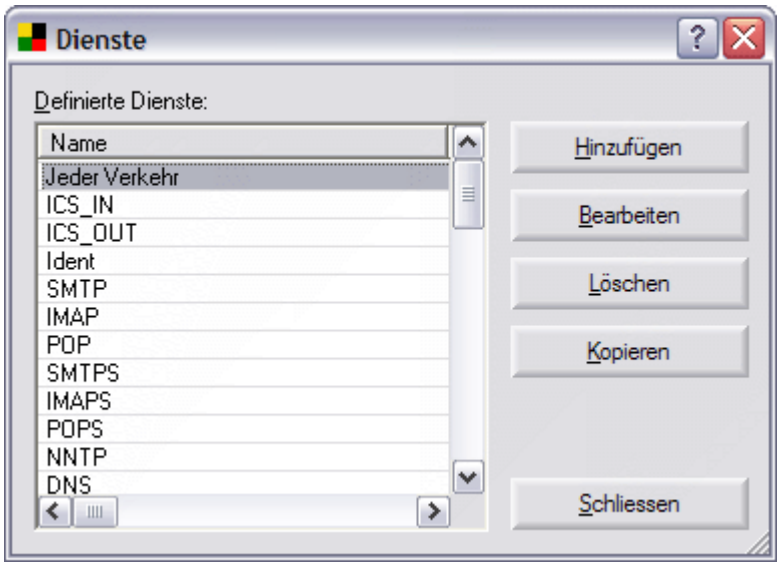


- ***Löschen*** – löscht die für den ausgewählten Systemdienst angelegte Regel
- ***Details anzeigen*** – im unteren Bereich des Dialogfensters zeigt diese Funktion einen Überblick der Informationen zu dem Systemdienst, der gerade in der Liste der Systemdienste und Protokolle selektiert ist:
  - ***Dienst*** – Name des Systemdienstes (oder Protokoll)
  - ***Regel*** – Regel, die dem Systemdienst (oder Protokoll) zuordnet ist

  Wurde die Option ***Details anzeigen*** gewählt, erscheint eine neue Schaltfläche ***Dienste...*** im Reiter ***System***:

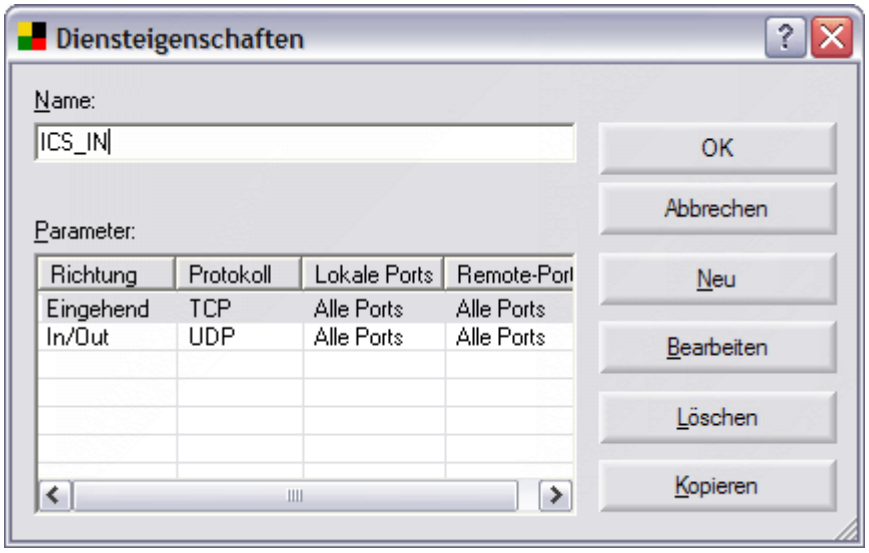


Die Schaltfläche ***Dienste*** öffnet einen neuen Dialog ***Dienste***, der einen detaillierten Überblick über die Systemdienste gibt und die Möglichkeit bietet, die Parameter der jeweiligen Systemdienste abzuändern:



Der Dialog ***Dienste*** bietet die folgenden Schaltflächen:

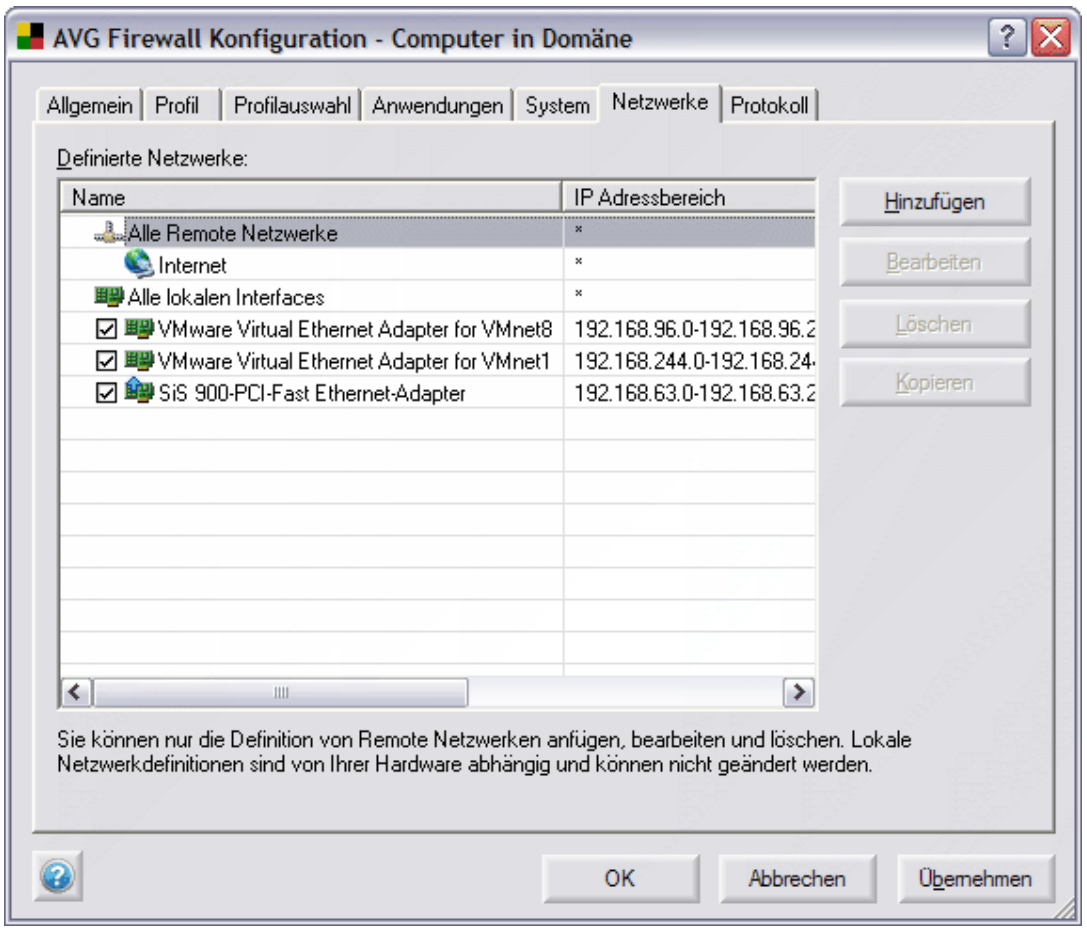
- ***Hinzufügen*** – öffnet einen neuen Dialog ***Diensteigenschaften***, in dem Sie den neuen Dienstnamen definieren und bestimmte Parameter dieses Dienstes setzen können (Richtung, Protokoll, lokale Ports, Remote Ports)



- ***Bearbeiten*** – öffnet den Dialog ***Diensteigenschaften***, dort können Sie die existierenden Parameter eines bestimmten Dienstes editieren.
- ***Löschen*** – löscht den definierten Dienst (und entfernt die Information über ihn aus der Liste der Dienste)
- ***Kopieren*** – macht für Sie das Anlegen eines neuen Diensteintrages leichter und bequemer: Um diese Option zu nutzen, heben Sie einen Dienst in der Liste der Dienste (Dialog ***Dienste***) hervor und gehen Sie über die Schaltfläche ***Kopieren***. Ein neuer Diensteintrag wird erstellt. Die Parameter werden von dem geklonten Dienst übernommen. Dann können Sie einfach die Parameter für den neuen Dienst editieren.

g) Netzwerke

Der Reiter ***Netzwerke*** bietet eine Liste der Netzwerke, über die die Anwendung kommuniziert. Sie können neue Netzwerke hinzufügen, Parameter der momentan definierten Netzwerke editieren und ein bestimmtes Netzwerk löschen:

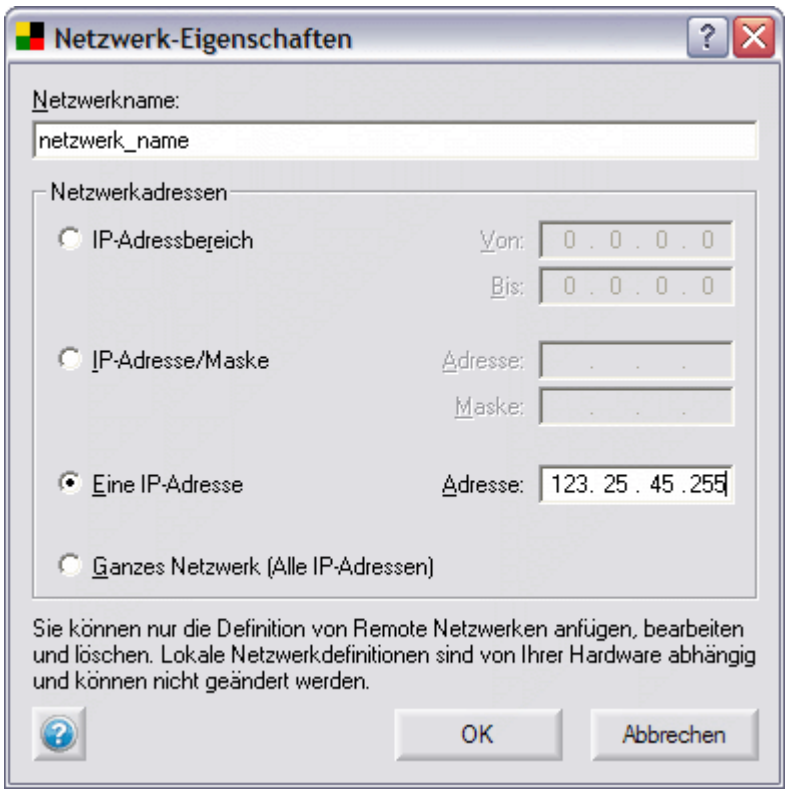


In der Liste der definierten Netzwerke können eine oder mehrere Netzwerk-Schnittstellen aufgelistet sein. Wenn Sie möchten, dass die Firewall das Filtern des Datenverkehrs über eine dieser Schnittstellen stoppen soll, so löschen Sie einfach die Markierung im entsprechenden Kontrollkästchen, das sich links neben dem Namen der Netzwerk-Verbindung befindet.

Das Filtern des Datenverkehrs für eine bestimmte Netzwerk-Verbindung zu stoppen kann für folgende Situation sehr hilfreich sein: Wenn Ihr Computer über eine Netzwerk-Verbindung mit dem Internet verbunden ist und über eine andere Schnittstelle mit dem lokalen Netzwerk (LAN) verbunden ist, kann das Filtern von Datenverkehr für die Internet-Verbindung gewählt werden und die LAN-Verbindung wird nicht gefiltert (da das LAN einem kleineren Risiko an Bedrohung ausgesetzt ist).

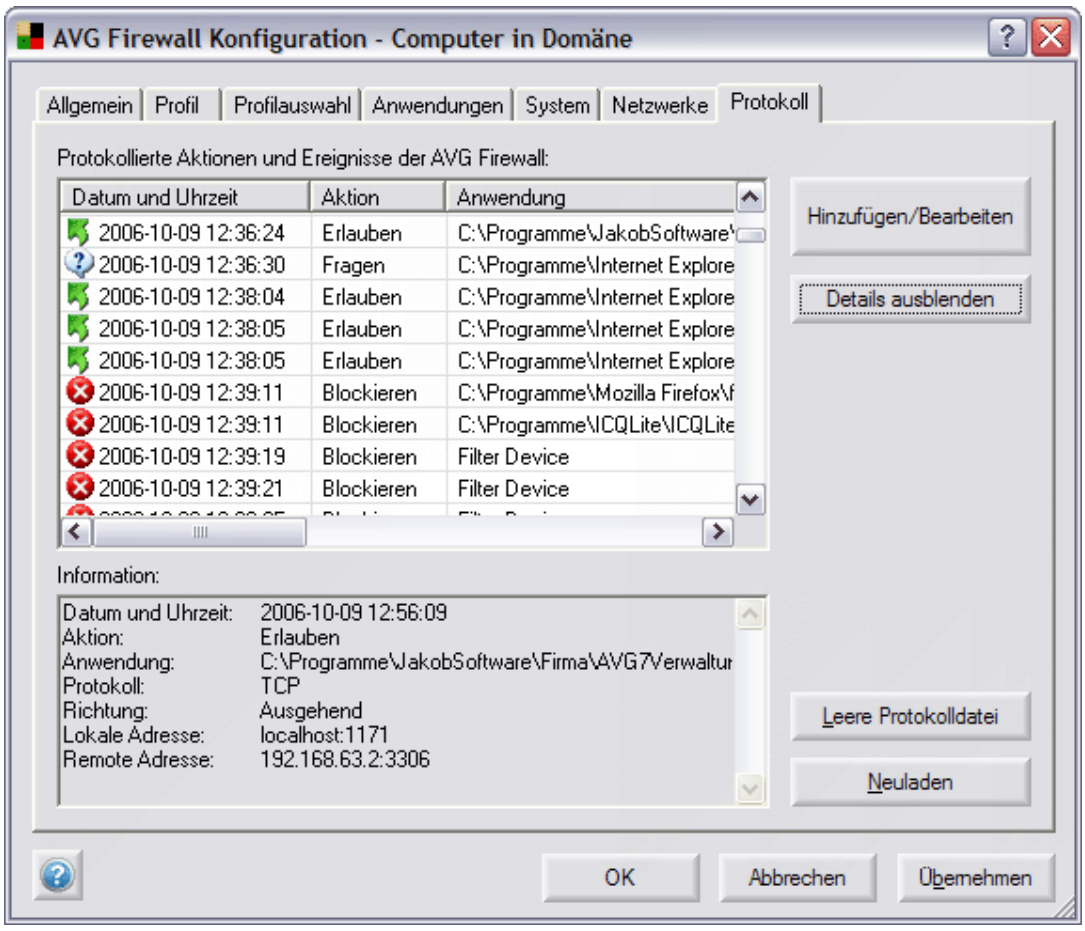
Das Dialogfenster stellt die folgenden Schaltflächen:

o ***Hinzufügen*** – öffnet einen neuen Dialog ***Netzwerk-Eigenschaften***, dort können Sie einen Netzwerknamen festlegen und seine Parameter setzen:



- ***Bearbeiten*** – öffnet den Dialog ***Netzwerk-Eigenschaften*** mit den schon gesetzten Parametern eines bestimmten Netzwerkes und ermöglicht Ihnen diese abzuändern
- ***Löschen*** – löscht ein bestimmtes Netzwerk aus der Liste der Netzwerke
- ***Kopieren*** – macht für Sie die Erstellung eines neuen Netzwerkeintrages leichter und bequemer: Hierzu markieren Sie in der Liste der Netzwerke ein Netzwerk (Dialog ***Netzwerke***) und gehen über die Schaltfläche ***Kopieren***. Ein geklonter Netzwerkeintrag wird erstellt. Dieser enthält die vordefinierten Parameter des geklonten Netzwerkes. Dann können Sie einfach die Parameter für den neuen Dienst abändern.

h) Protokoll



Im Reiter ***Protokoll*** können Sie die Liste aller protokollierten Aktionen und Ereignisse der **Firewall** einsehen.

Der Hauptteil des Reiters ***Protokoll*** ist in zwei Abschnitte aufgeteilt:

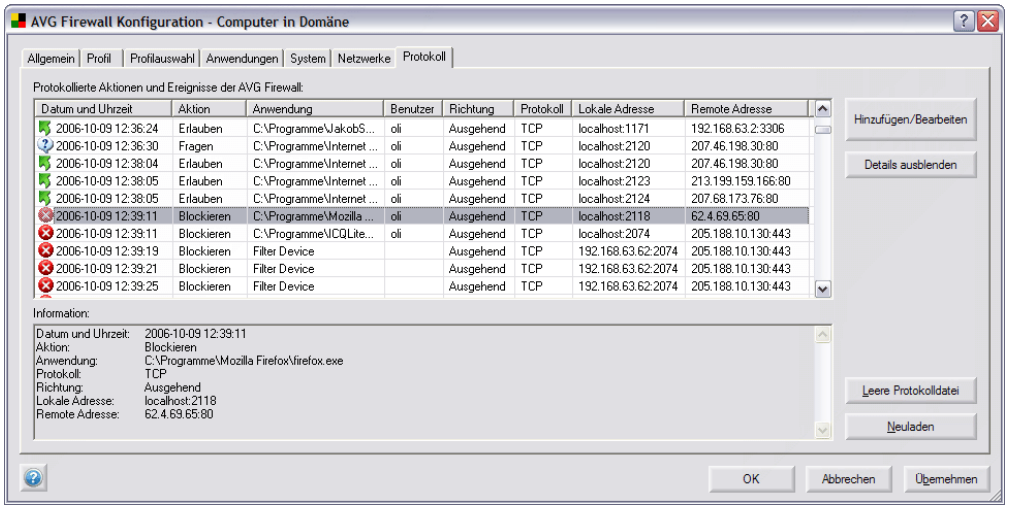
o **Protokollierte Aktionen und Ereignisse der Firewall**

Dieser Abschnitt bietet einen Überblick über alle Aktionen und Ereignisse im Zusammenhang mit der **Firewall**, die mit den jeweiligen Parametern in der Protokolldatei erfasst wurden.

Der Reiter ***Protokoll*** öffnet sich im Standardmodus, dabei werden die folgenden Parameter für jede protokollierte Aktion bereitgestellt:

- ***Datum und Uhrzeit*** – genaues Datum und Zeit, als das Ereignis auftrat
- ***Aktion*** – die durchgeführte Art der Aktion
- ***Anwendung*** – Name der Anwendung, auf die sich das protokollierte Ereignis bezieht

Falls Ihnen die zur Verfügung gestellten Parameter nicht ausreichen und Sie mehr sehen wollen, schalten Sie über die Schaltfläche ***Details anzeigen*** in den Advanced Protokolldateiüberblick um:



Nun sind Sie in der Lage, die folgenden Parameter zu überprüfen:

- ***Datum und Uhrzeit*** – genaues Datum und genaue Zeit beim Auftreten des Ereignisses
- ***Aktion*** – durchgeführte Art der Aktion
- ***Anwendung*** – der Name des Prozesses, auf den sich das protokollierte Ereignis bezieht
- ***Benutzer*** – der Name des Benutzers der Anwendung
- ***Richtung*** – Die Richtung der Kommunikation der Anwendung (in/out, oder beide Richtungen)
- ***Protokoll*** – Art des benutzten Protokolls
- ***Lokale Adresse*** – die lokale Adresse der Verbindung bezogen auf das protokollierte Ereignis
- ***Remote-Adresse*** – die Remote- Adresse der Verbindung hinsichtlich des protokollierten Ereignisses

In beiden Modi des Reiters ***Protokoll (***Standard/Advanced) können Sie immer die protokollierten Parameter nach einem ausgewählten Attribut sortieren: Sie können die Daten chronologisch sortieren (klicken Sie auf den Kopf der Spalte ***Datum und Uhrzeit***), nach der Art der Aktion (klicken Sie auf den Spaltenkopf ***Aktion***) usw.

o **Information**

Der Abschnitt ***Information*** bietet eine bequeme und leicht zu prüfende Liste von Parametern, die für ein bestimmtes, gerade im Dialogabschnitt ***Protokollierte Aktionen und Ereignisse der Firewall*** hervorgehobenes Ereignis protokolliert wurden.

o **Schaltflächen im Reiter Protokoll**

Der Reiter ***Protokoll*** bietet die folgenden Schaltflächen:

- ***Hinzufügen / Bearbeiten*** – füge hinzu oder editiere eine Anwendung, die der Protokollierung unterliegen soll

- ***Details ausblenden*** – schaltet zwischen den Modi (Standard/Advanced) der Protokolldateidarstellung (wie oben beschrieben) hin und her
- ***Leere Protokolldatei*** – löscht die Informationen, protokolliert für ein bestimmtes Ereignis, indem alle existierenden Einträge gelöscht werden
- ***Neuladen*** – aktualisiert die zur Zeit dargestellte Information

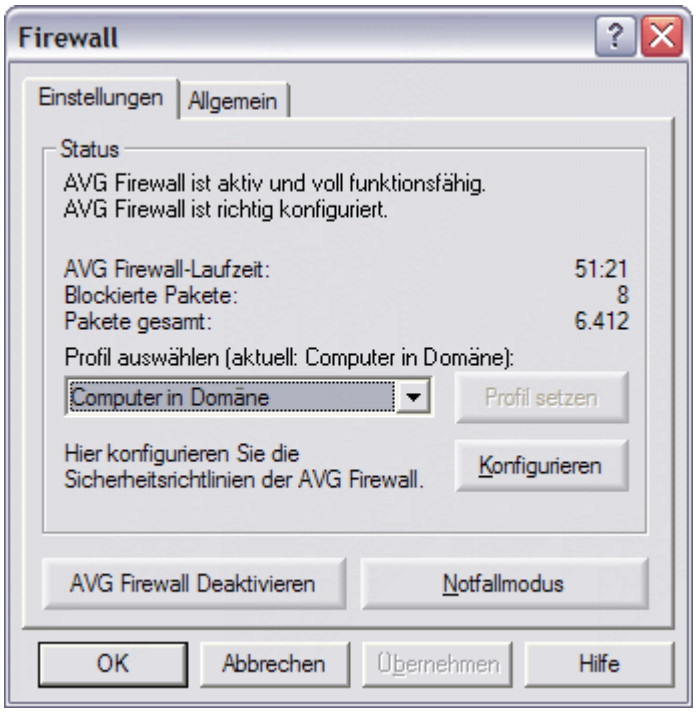
10.8. AVG Firewall Optionen

Die Optionen der Komponente **Firewall** können Sie über die Schaltfläche ***Optionen*** im Steuerbereich der Komponente **Firewall** im **Control Center** starten.

Der Dialog ***Optionen*** besitzt zwei Reiter:

- Einstellungen
- Allgemein

a) Einstellungen



Der Reiter ***Einstellungen*** zeigt eine kurze Statusinformation der **Firewall** im Bereich ***Status***:

- **Firewall** Status-Information: aktiv, angehalten
- Konfigurationsinfo der **Firewall**
- Information über die Laufzeit der **Firewall** seit dem letzten Neustart, über die Anzahl der blockierten Kommunikationsversuche sowie über die Gesamtzahl der Kommunikationsversuche.

Weiterhin können Sie das gewünschte Firewall Profil auswählen. Es gibt maximal fünf vordefinierte Profilvarianten, aus denen Sie auswählen können:

Alle erlauben, **Alle Blockieren**, **Computer in Domäne** (Geschäftsnetzwerk), **Computer unterwegs** (Notebook auf Reisen), **Einzelplatzrechner** (Standalone Computer). Jedes Profil deckt bestimmte Konfigurationen für Ihren PC ab und ein adäquates **Firewall** Sicherheitsniveau wurde jedem dieser Profile zugewiesen.

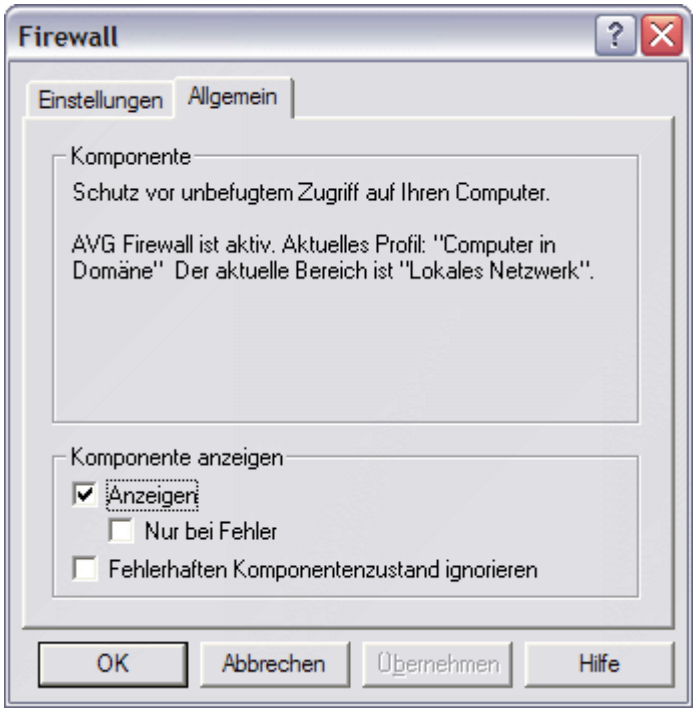
Das passende Profil kann im Dropdown Menü ausgewählt werden, danach bestätigen Sie Ihre Wahl mit der Schaltfläche ***Profil setzen.***

Im Bereich ***Firewall Status*** finden Sie auch die Schaltfläche ***Konfigurieren***, die den Dialog ***Firewall Konfiguration*** startet – für detaillierte Informationen hinsichtlich der Konfiguration wird auf das Kapitel Konfiguration der Firewall verwiesen.

Im unteren Bereich des Reiters ***Einstellungen*** sehen Sie zwei Schaltflächen für den Notfall:

- ***Firewall deaktivieren -*** Mit dieser Schaltfläche wird die Komponente **Firewall** sofort abgeschaltet – falls das erforderlich ist. Diese Option ist im Kapitel Firewall deaktivieren beschrieben
- ***Notfallmodus*** – Falls nötig kann mit einem Klick jeglicher Netzwerkverkehr auf allen Ports blockiert werden. Diese Option ist im Kapitel Der Notfallmodus der Firewall beschrieben

b) Allgemein



Der Reiter ***Allgemein*** ist in zwei Hauptbereiche unterteilt:

- ***Komponente*** – hier wird eine kurze Beschreibung der Komponente **Firewall** gegeben: Hauptzweck, Versionsnummer und Veröffentlichungsdatum. Hier wird auch der aktuelle Status der Komponente angezeigt.

o ***Komponente anzeigen*** – Im Bereich ***Komponente anzeigen*** können Sie die Anzeigeparameter für die Komponenten der **Firewall** anpassen; Sie können folgenden Optionen markieren/die Markierung entfernen:

- ***Anzeigen*** – Das ist die Standardeinstellung. Die Komponente **Firewall** ist im **Control Center** sichtbar.

  Wenn Sie die Komponente **Firewall** nicht im **Control Center** sehen möchten, deaktivieren Sie diese Option – nehmen Sie den Haken heraus.

  Ist eine Komponente erst einmal „unsichtbar“, können Sie diese immer über diesen Weg wieder im **Control Center** sichtbar machen: **Control Center**, Hauptmenü, wählen Sie das Menü ***Ansicht***, dort ***Komponenten / Firewall***.

  Unterhalb der Option ***Anzeigen*** können Sie auch angeben ***Nur bei Fehler***. Dann wird die Komponente **AVG Firewall** nur im **Control Center** angezeigt, wenn ein Problem vorliegt.

- ***Fehlerhaften Komponentenzustand ignorieren*** – wenn Sie diese Option aktivieren, wird die Komponente **Firewall** keine Standardinformationen über ihren aktuellen Status ausgeben. Ist die Komponente in einem fehlerhaften Status, wird üblicherweise das Symbol des **Control Centers** in der Taskleiste grau angezeigt und im **Control Center** die Komponente rot markiert.

11. Anti-Spam

Die Komponente ***Anti-Spam*** überprüft alle eingehenden eMails und markiert unerwünschte eMails als SPAM. Sie nutzt verschiedene Analyse-Methoden für die Bearbeitung jeder einzelnen eMail und bietet einen maximal verfügbaren Schutz gegen unerwünschte eMails. Die Komponente benötigt kaum Wartung, da der Benutzer verschiedene **Anti-Spam**-Optionen anpassen kann.

Die Funktion ist in dieser Lizenz nicht verfügbar. Die Komponente ***Anti-Spam*** ist in diesen Produkten enthalten:

- AVG Internet Security

Weitere Informationen finden Sie im Internet auf www.grisoft.de unter Punkt Prokukte

12. Virenquarantäne

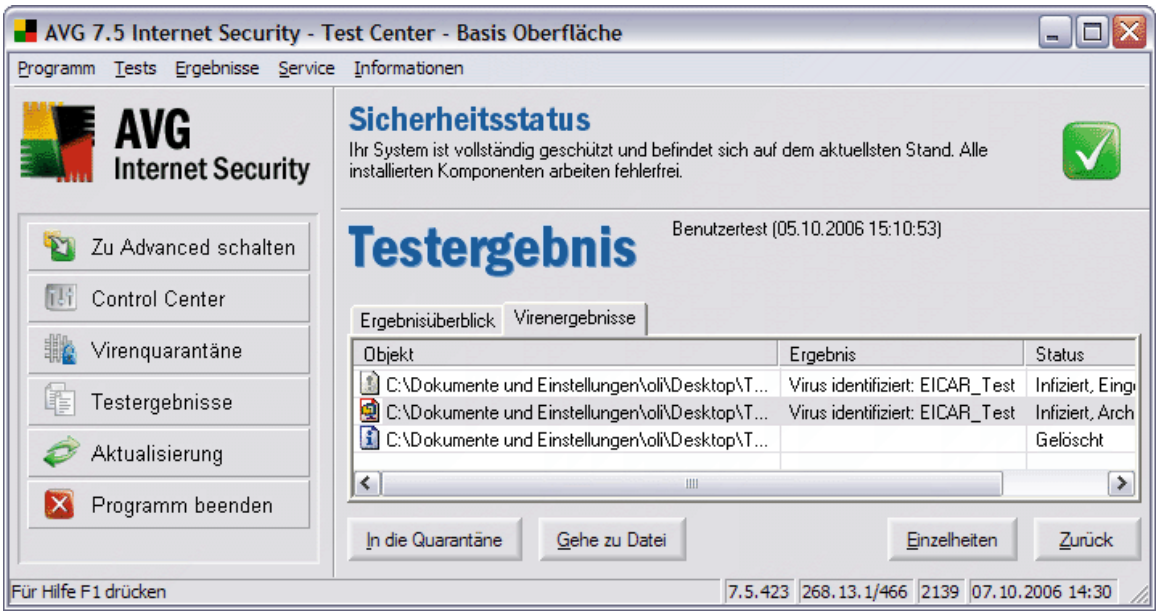
Die ***Virenquarantäne*** *i*st eine sichere Arbeitsumgebung für die Verwaltung verdächtiger/infizierter Objekte, die während der AVG Tests gefunden wurden.

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.

12.1. 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.

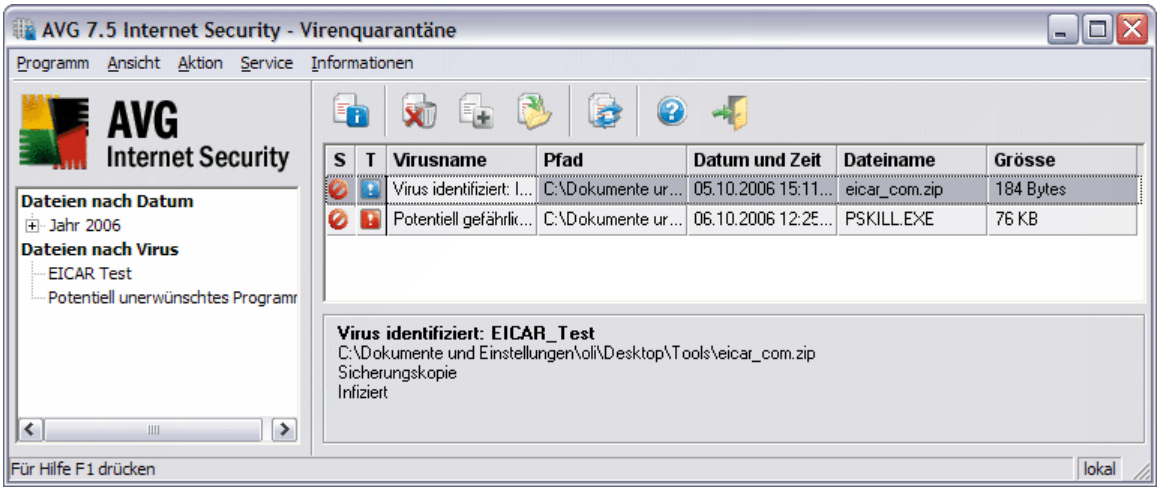
12.2. Virenquarantäne Umgebung

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:

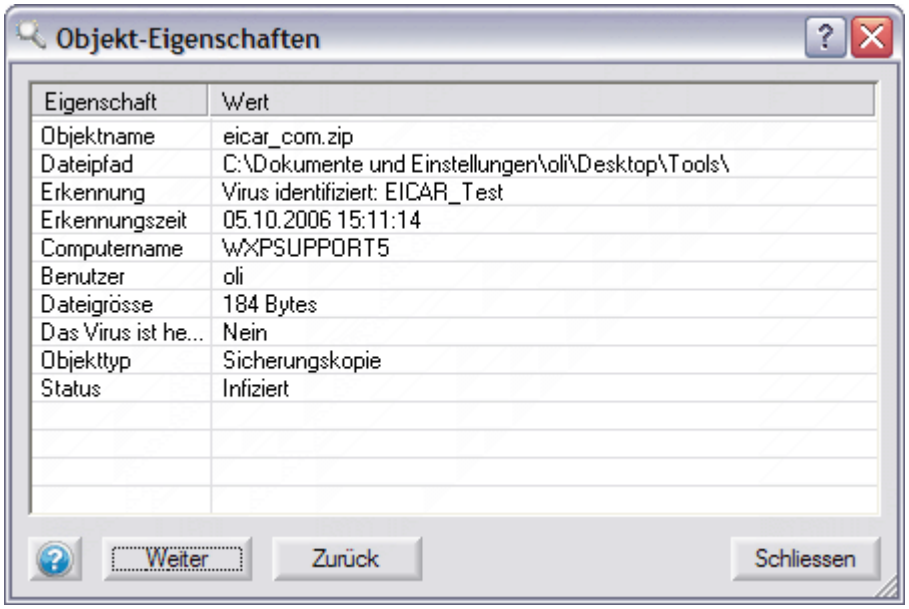
- ***S*** – Objektstatus:
  - infiziertes / verdächtiges Objekt *(Kreis mit rotem X)*
  - geheiltes Objekt *(rotes X)*
- ***T*** – Objekttyp
  - Objekt wurde in die ***Virenquarantäne*** verschoben *(Ausrufezeichen im roten Feld)*
  - Backup des Objekts wurde in der ***Virenquarantäne*** vor einem Heilungsversuch 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

12.3. 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 verschobenen 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.

13. 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.

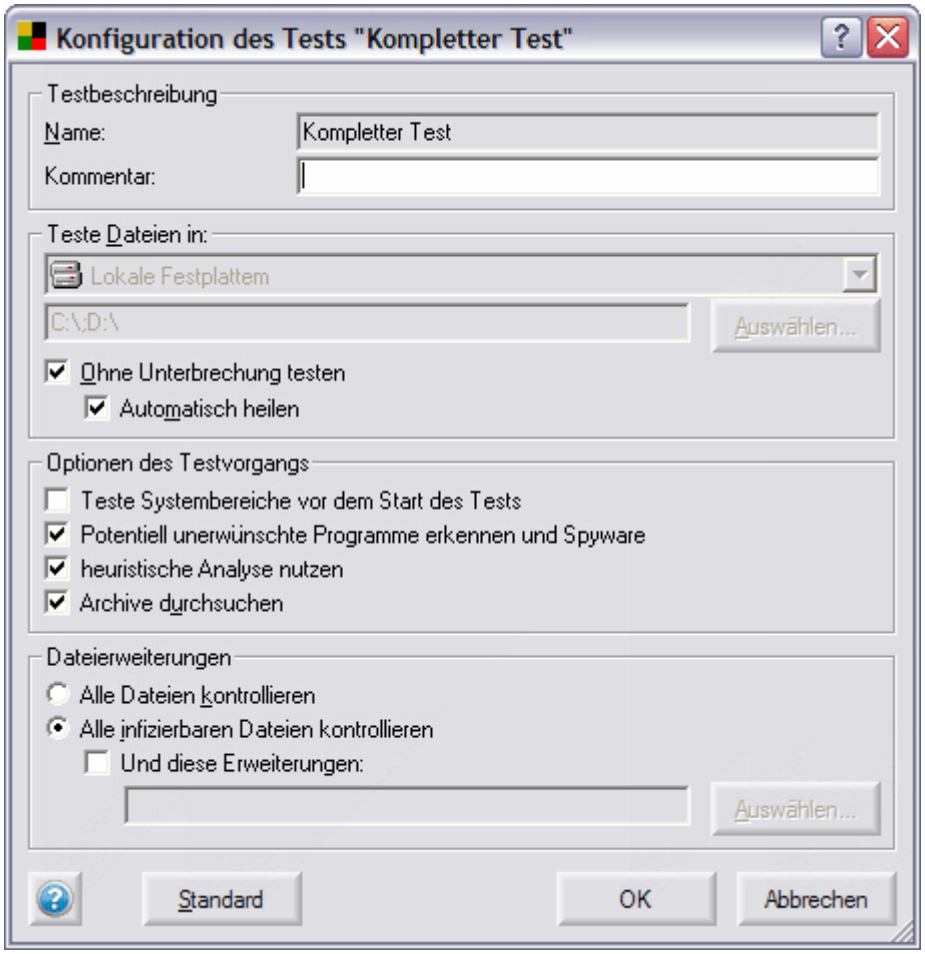
13.1. Kompletter Test

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 erfahrene*n* Anwender*n* 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:

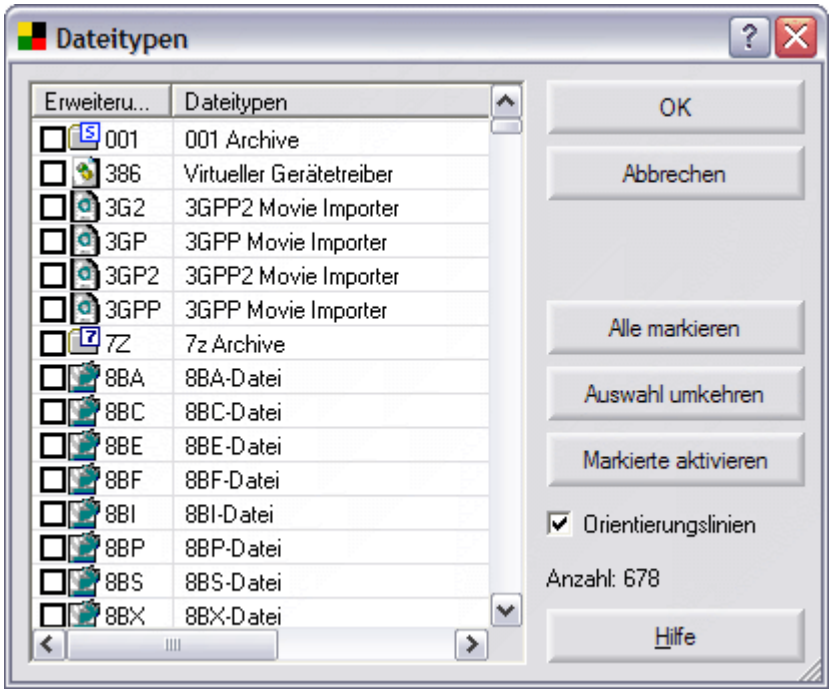


Dieser Dialog erlaubt Ihnen die Konfiguration der folgenden Parameter:

- ***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

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

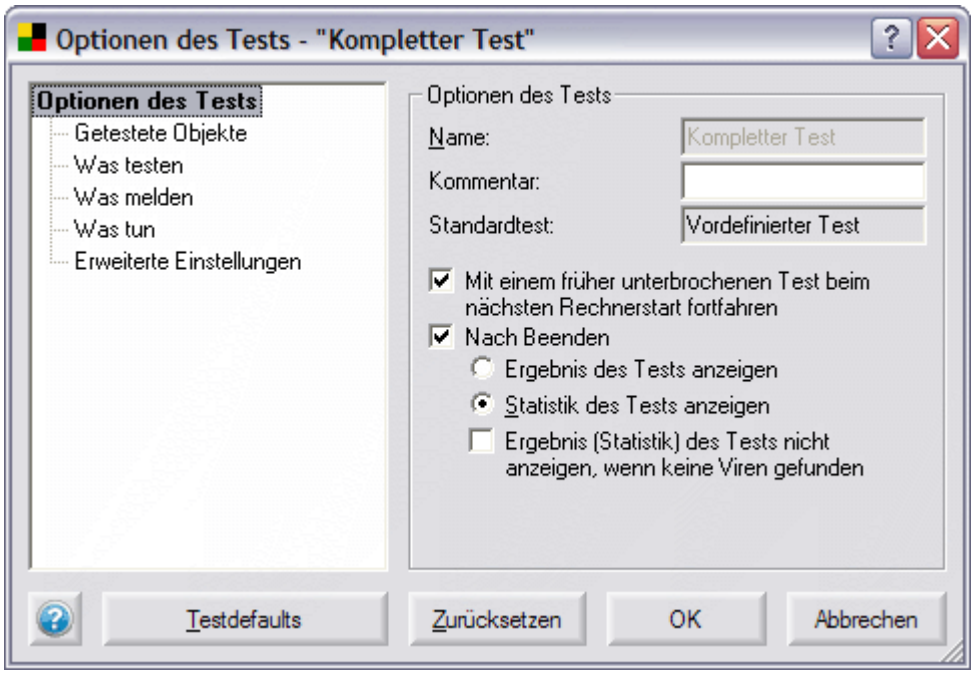


o Wählen Sie in der ***Advanced Testoberfläche*** aus dem Hauptmenü den Eintrag ***Tests/Testmanager/Kompletter Test***:

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

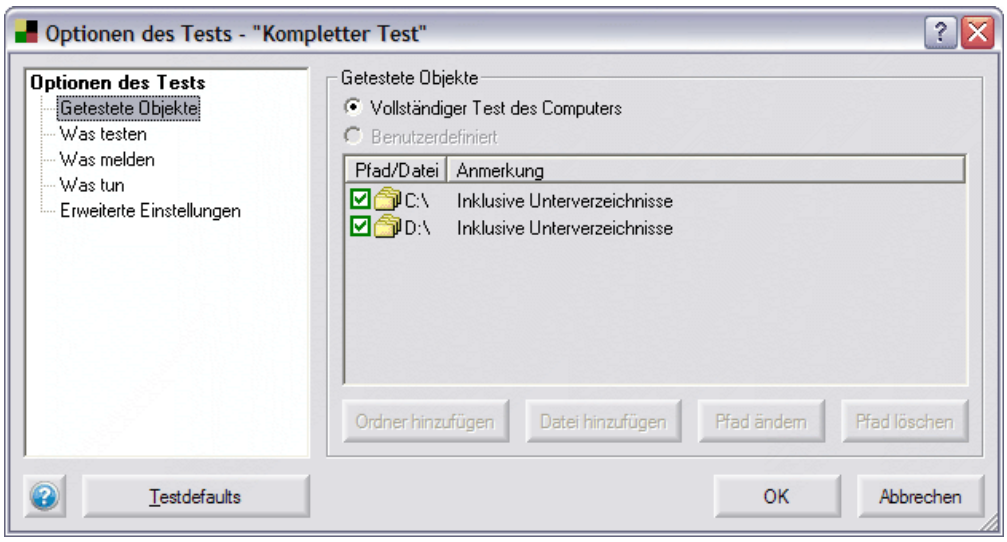
erhalten (diese können nacheinander im Navigationsbaum auf der linken Seite geöffnet werden):

o ***Optionen des Tests***



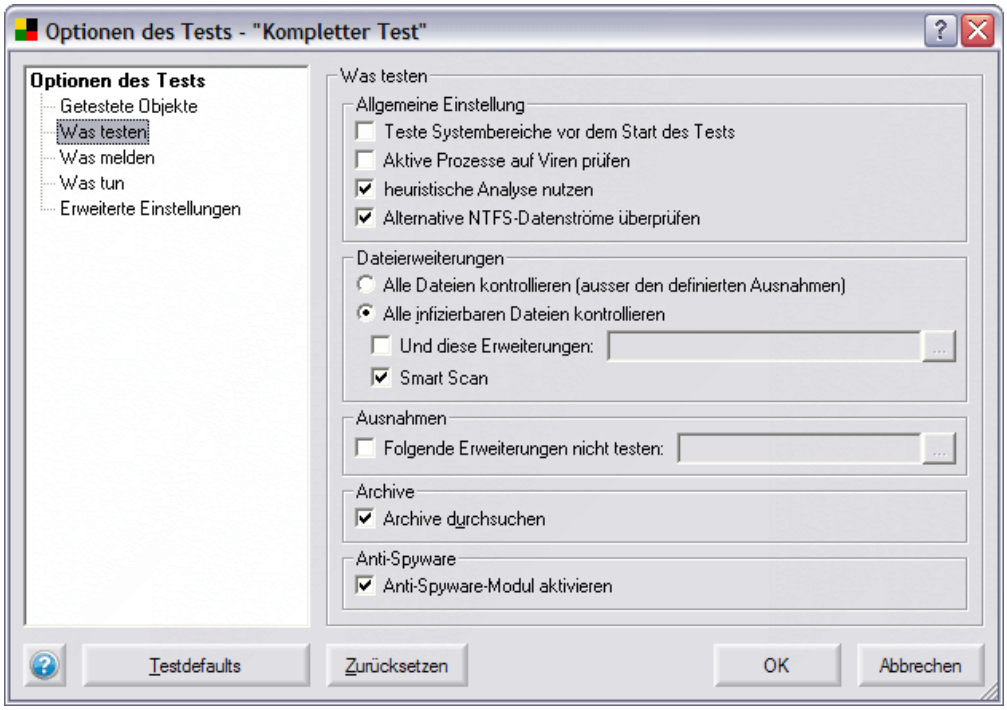
- ***Name*** – der Testname ist standardmäßig auf ***Kompletter Test*** eingestellt und kann nicht verändert werden
- ***Kommentar*** – in diesem Feld können Sie Ihre eigenen, ergänzenden Informationen zur Beschreibung des Tests hinzufügen (spezielle Einstellungen...)
- ***Standardtest*** – dieses Feld 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

o ***Getestete Objekte***



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

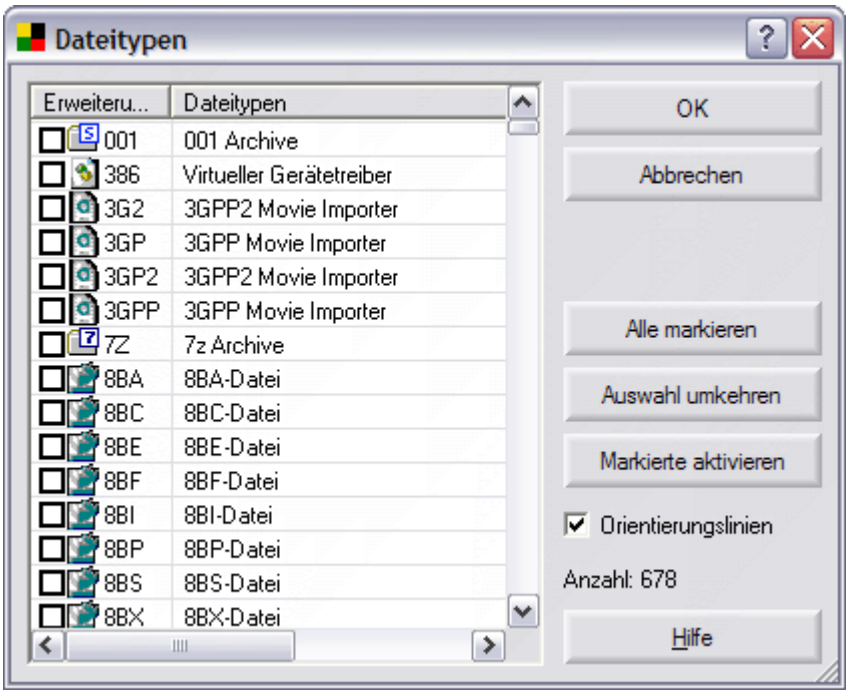
o ***Was testen***



- ***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.

- ***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.



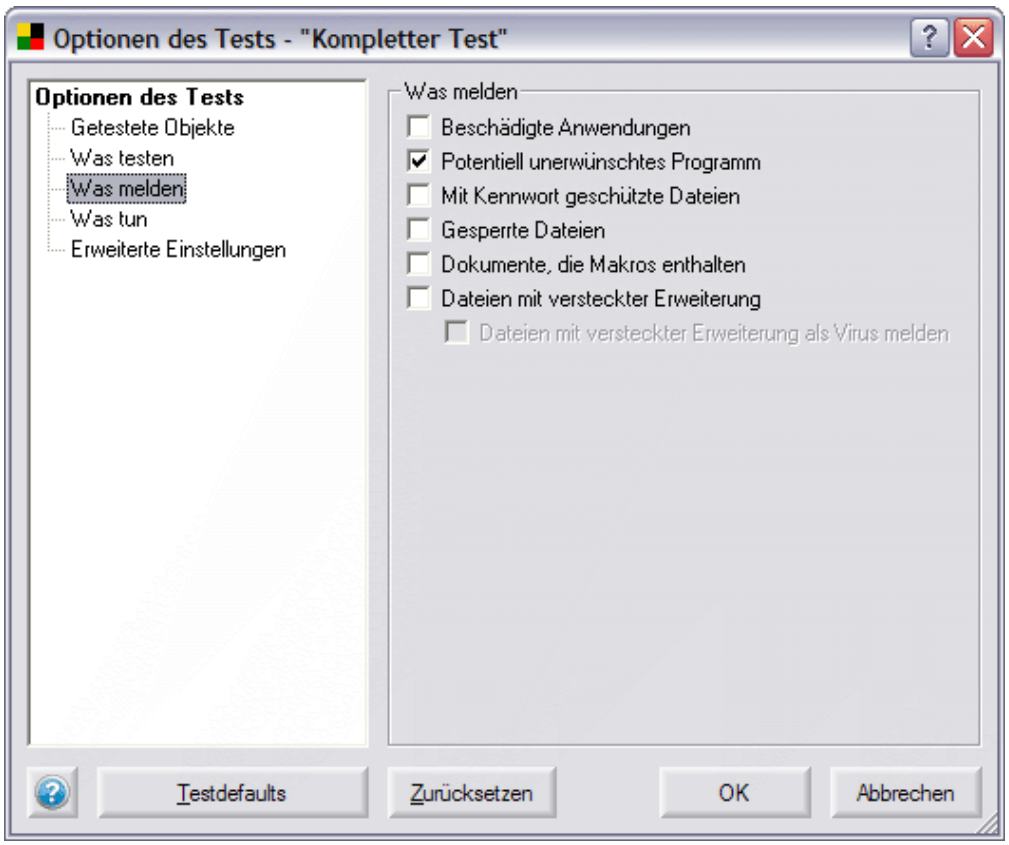
In diesem Dialog werden Sie dazu aufgefordert, aus der Liste der Dateierweiterungen und die entsprechenden Dateien auszuwählen, die überprüft werden sollen. Der Dialog ***Dateitypen*** beinhaltet die folgenden Kontrollschaltflächen:

- ***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, in dem 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*).

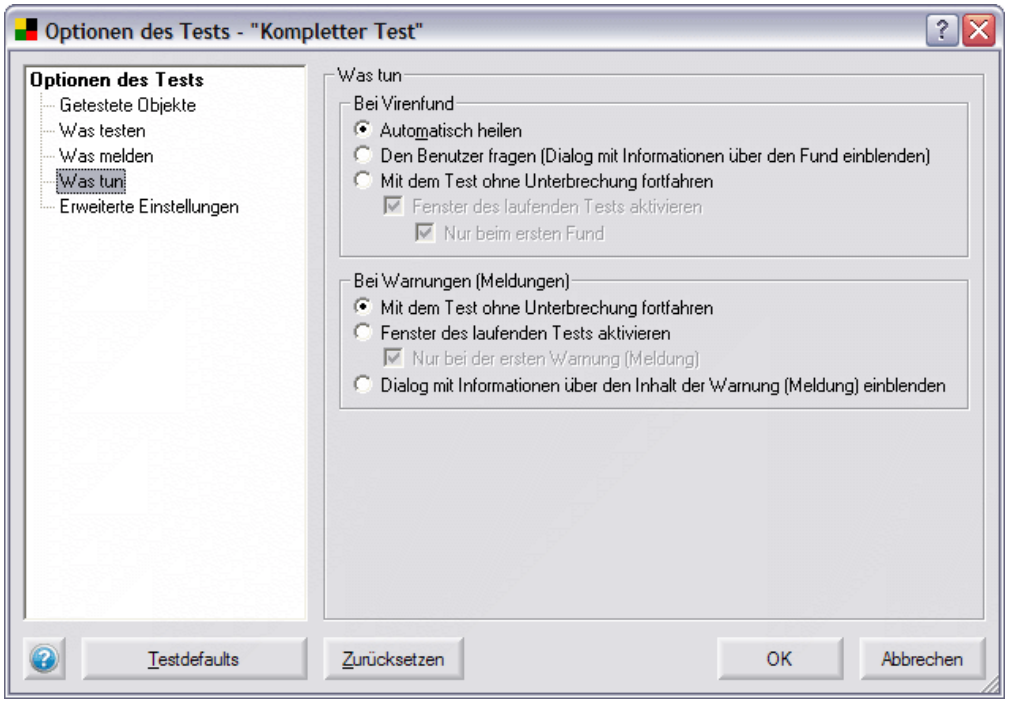
- ***Ausnahmen*** – in diesem Abschnitt können Sie Dateierweiterungen festlegen, die bei einem ***Kompletten Test*** ausgelassen werden sollen. Verwenden Sie die Schaltfläche (**...**) um den ***Dateierweiterungen*** Dialog erneut zu öffnen und legen Sie fest, welche Dateien überprüft werden sollen. 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***



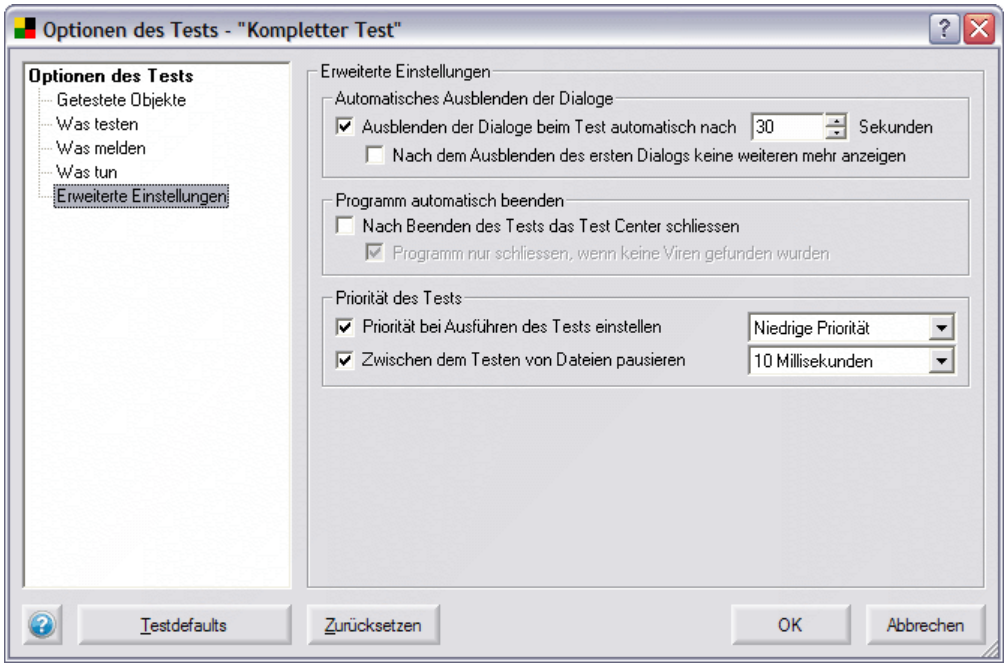
Dieser Dialog beinhaltet eine Liste von Ereignissen, die während des Tests auftreten können. Markieren Sie die Ereignisse, über deren Auftreten Sie informiert werden möchten.

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

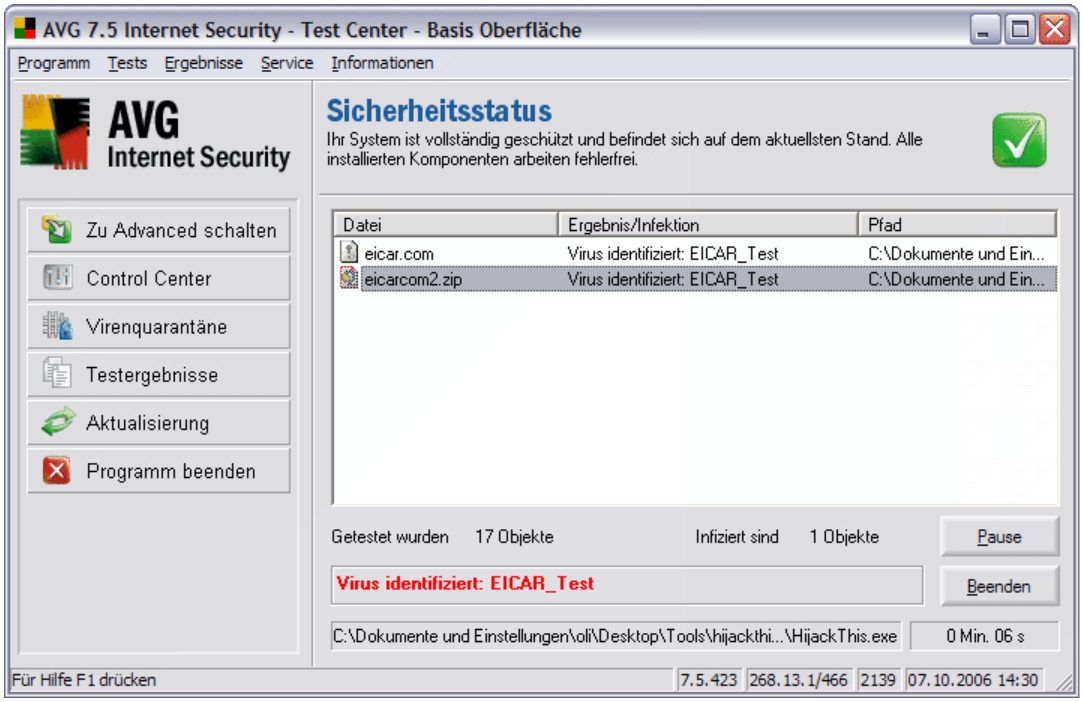
Die einfachste Art, den ***Kompletten Test*** zu starten, ist die Betätigung der Schaltfläche ***Teste Computer*** in der ***Basis Oberfläche*** des Test Center:

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:



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

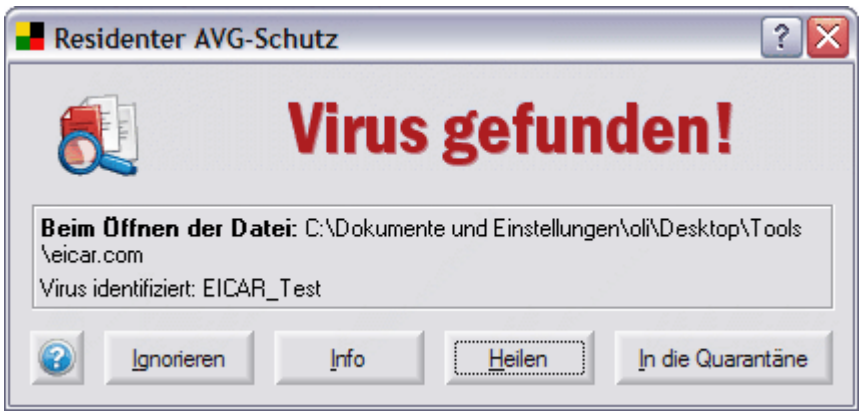
Im unteren Teil des Fensters können Sie kontinuierlich den Testfortschritt beobachten und Informationen finden zu:

- 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:



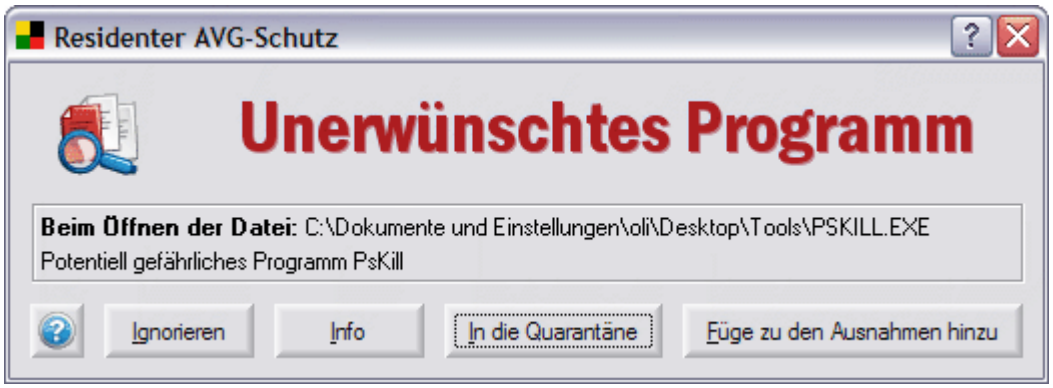
Der Dialog Virus gefunden! informiert Sie über die gefundene infizierte Datei und deren Speicherort. Wählen Sie die Option ***Dialog nicht mehr anzeigen (teste Dateien ohne Unterbrechung)***, wenn Sie keine weiteren Meldungen über Testergebnisse erhalten möchten, bevor der Test beendet wurde.

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

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:

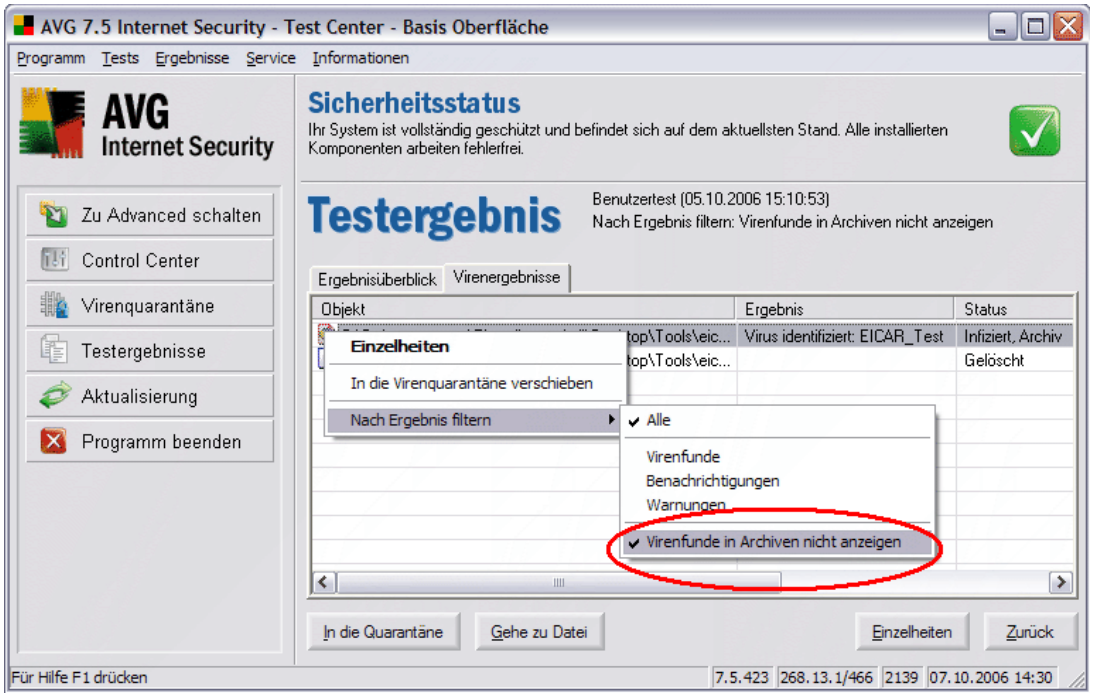
- ***Ignorieren*** – ignoriert die Warnung des Residenten Schutzes und ermöglicht Ihnen, weiter zu arbeiten (und bietet auch keinen Zugriff auf die Bedrohung).
- ***Info*** – öffnet die Online-Virenenzyklopädie, in der Sie nach detaillierten Informationen bezüglich der erkannten Bedrohung suchen können.
- ***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.

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.

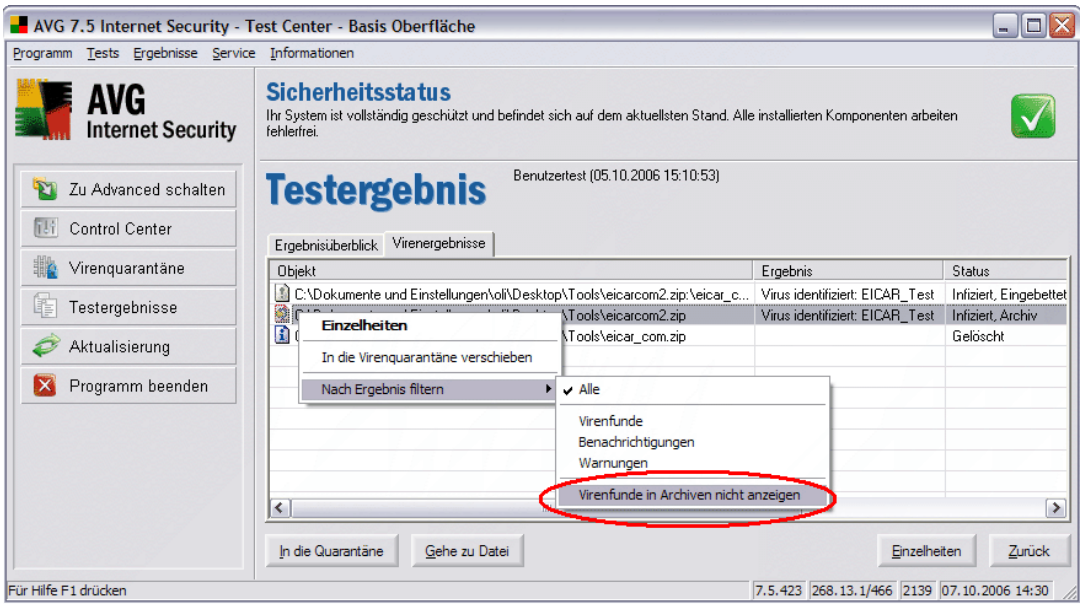
Die Schaltfläche ***In die Quarantäne*** verschiebt das gesamte Archiv in die **Virenquarantäne**.

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:



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

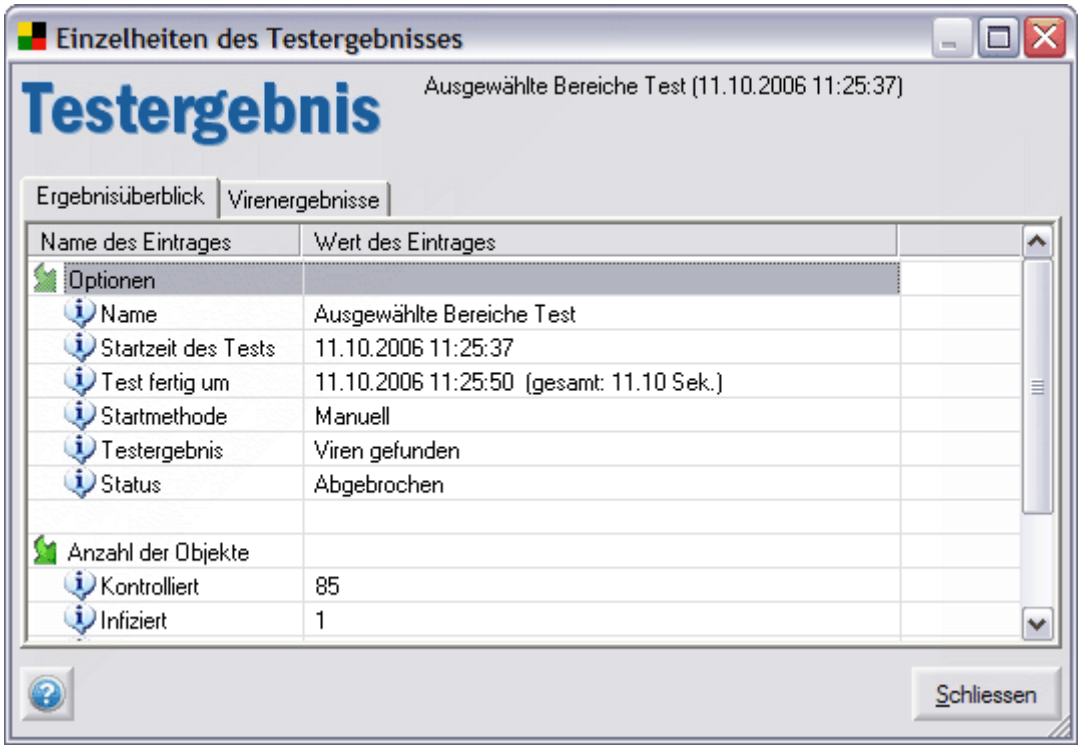
Nachdem der Test beendet ist, werden Sie über das Testergebnis durch den Dialog ***Teststatistik*** informiert, der umfassende Informationen über den Testfortschritt und das Ergebnis enthält:

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***



13.2. 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

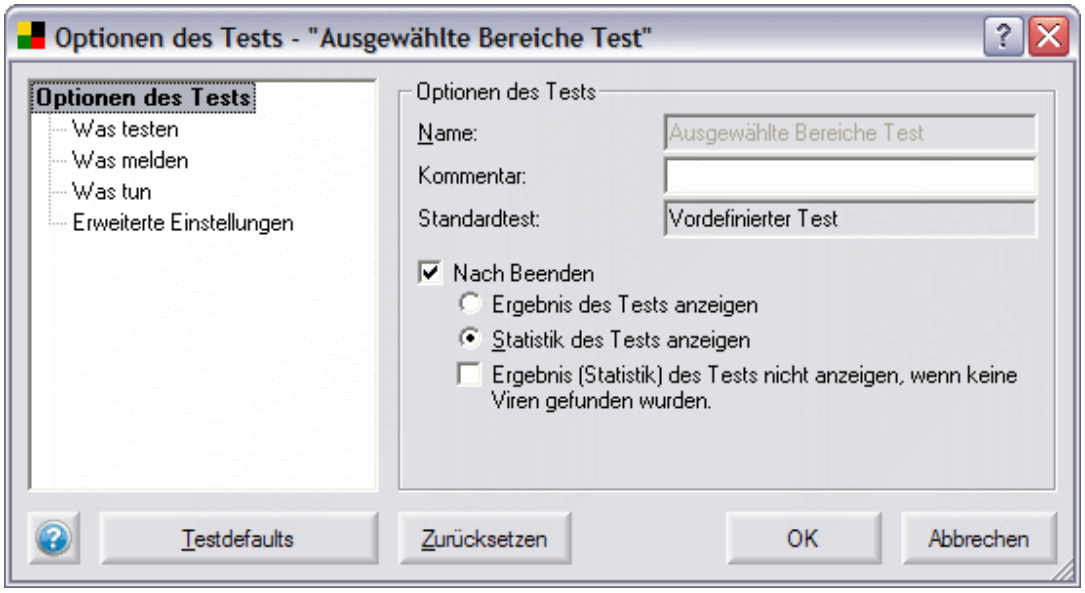
13.3. Ausgewählte Bereiche Test

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



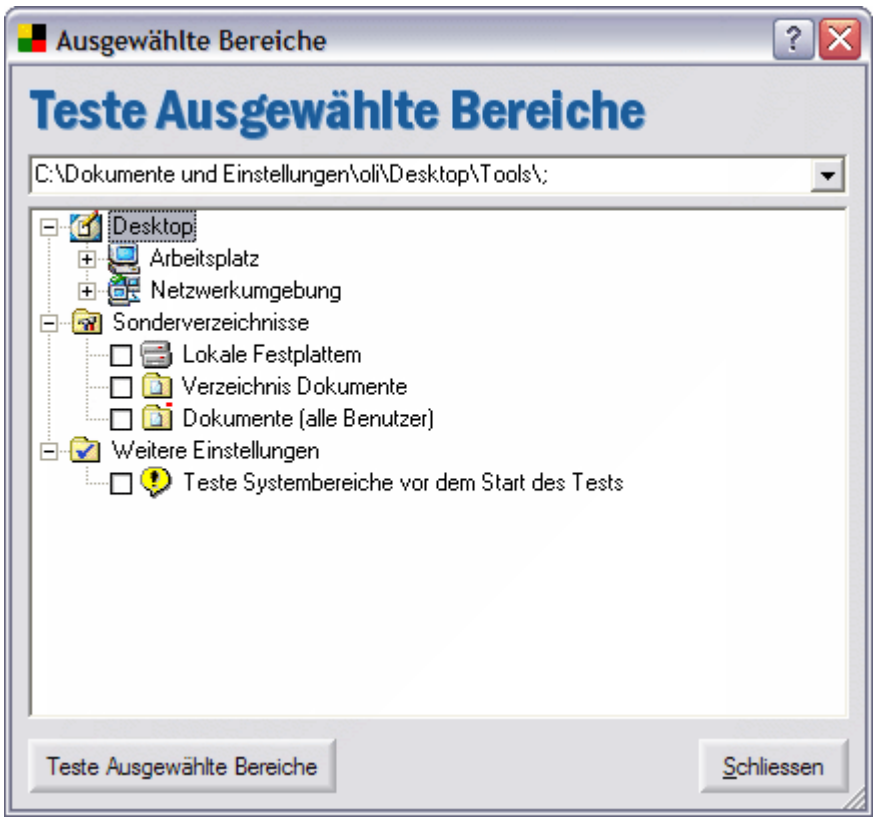
Im linken Abschnitt des neu geöffneten Dialogs können Sie aus verschiedenen Testkonfigurationen auswählen – die Testkonfiguration selbst ähnelt der Konfiguration des ***Kompletten Tests***, siehe Kapitel 11.1 a)– Kompletter Test - Einstellungen.

b) Ausgewählte Bereiche Test – Start und Verlauf

Der Ausgewählte Bereiche Test kann folgendermaßen gestartet werden:

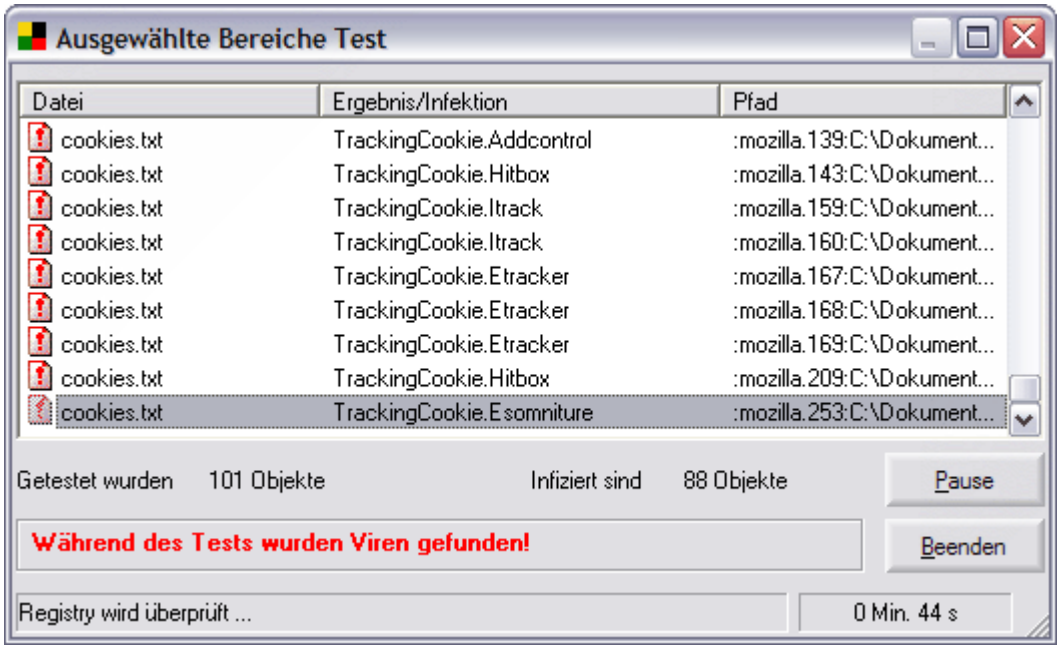
- In der ***Basis Oberfläche*** wählen Sie den Schnellstartlink ***Ausgewählte Bereiche Test***
- In der ***Advanced Oberfläche*** wählen Sie die Option ***Testmanager/Ausgewählte Bereiche Test/Teste ausgewählte Bereiche*** im linken Menü

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 Bereiche, 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 Testverlauf kann im Dialogfenster ***Ausgewählte Bereiche Test*** überwacht werden:



In dem neuen Fenster können Sie alle gefundenen Viren sehen:

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

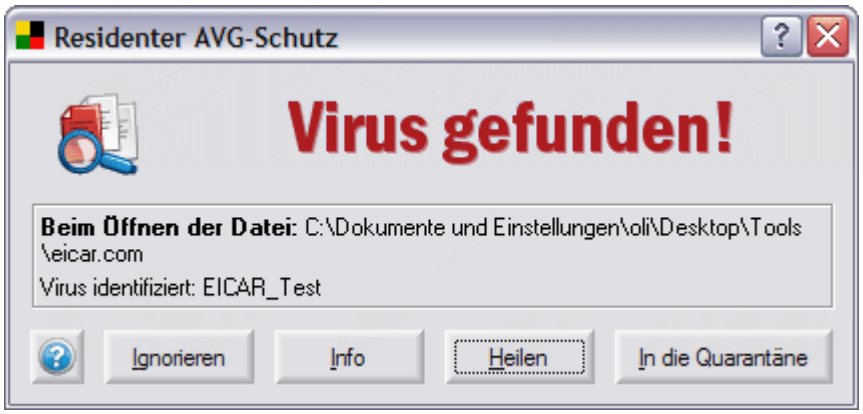
Im unteren Teil des Fensters können Sie kontinuierlich den Testfortschritt beobachten und Informationen finden zu:

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

13.4. 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.

13.5. AVG eMail-Kontrolle

EMS steht für den **eMail Scanner** und ist die AVG-Komponente für die Überprüfung von eingehenden/ausgehenden eMails. Der **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 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 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 EMS 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.

13.6. Start eines Test von der Kommandozeile aus

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:

- 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 detexted*/
- ERRORLEVEL == 7/* active virus in memory detected*/
- ERRORLEVEL == 8/* AVG corrupted*/
- ERRORLEVEL == 9/* double extension*/
- ERRORLEVEL == 10/* archive contains passwort protected files*/

14. 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.

14.1. 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 notwenig 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.

14.2. 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**

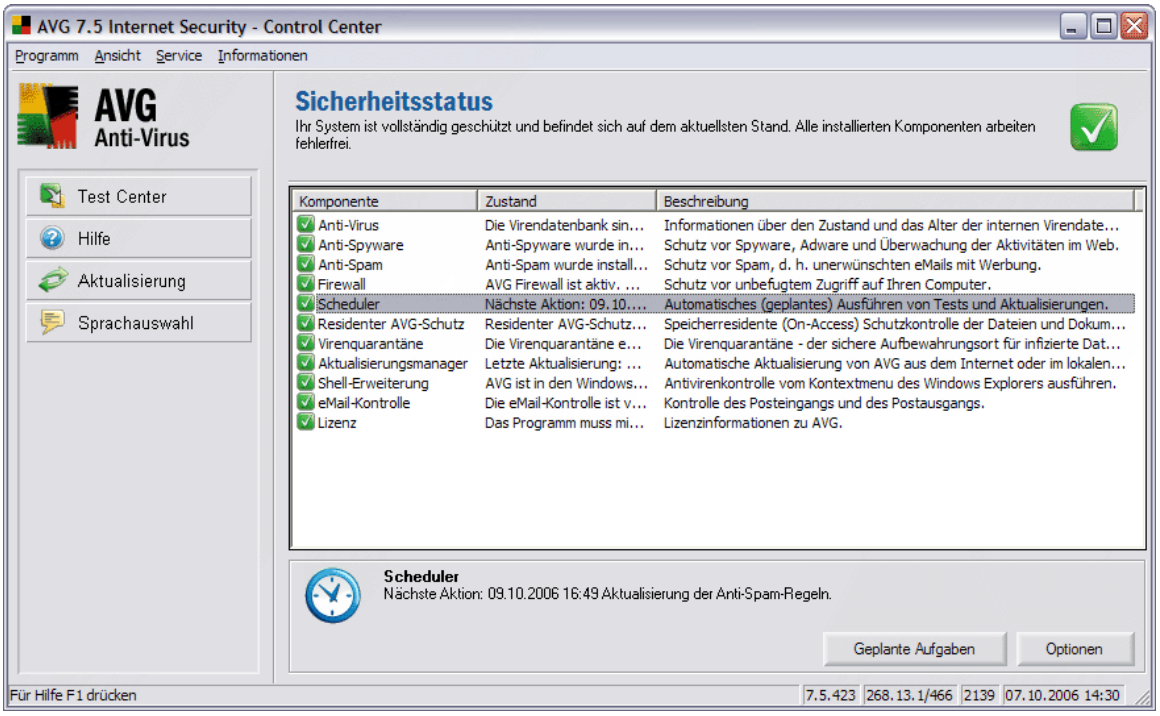
  Innerhalb von AVG ist es möglich, einen Aktualisierungsplan vorzugeben. Die geplante Aktualisierung wird dann periodisch zu den zuvor konfigurierten Terminen ausgeführt. Sobald eine neue Aktualisierungsdatei an angegebener Stelle erscheint, wird diese entweder direkt aus dem Internet oder aus dem Netzwerkverzeichnis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

14.3. Aktualisierungsplan

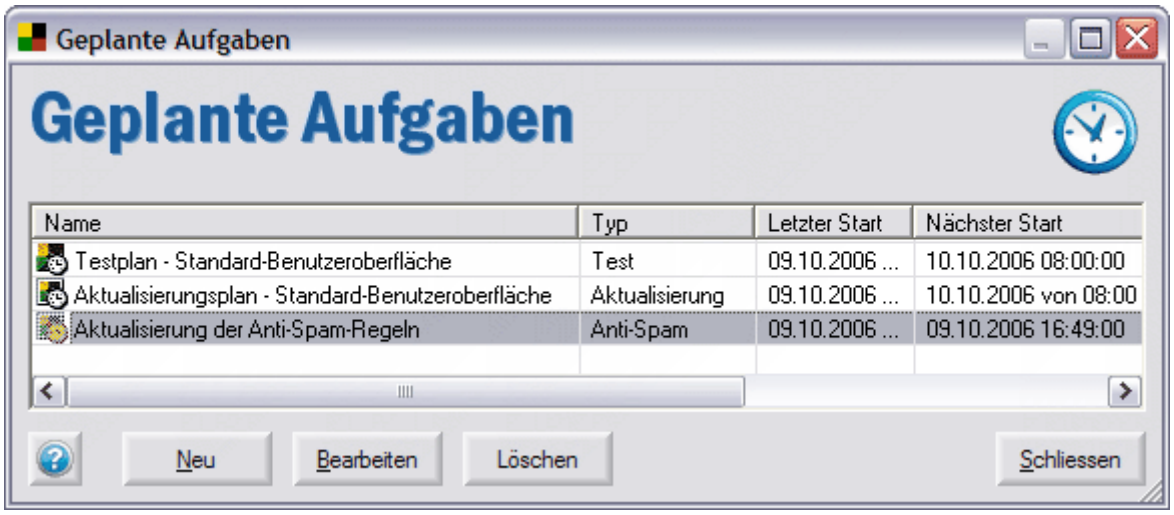
Die Aktualisierungsdateien können direkt aus dem Internet herunter geladen werden. Damit Sie immer die neueste Aktualisierungsversion erhalten, wird vorgeschlagen, einen Aktualisierungsplan anzulegen, der in regelmäßigen Intervallen im Internet nach neuen Aktualisierungen sucht.

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***

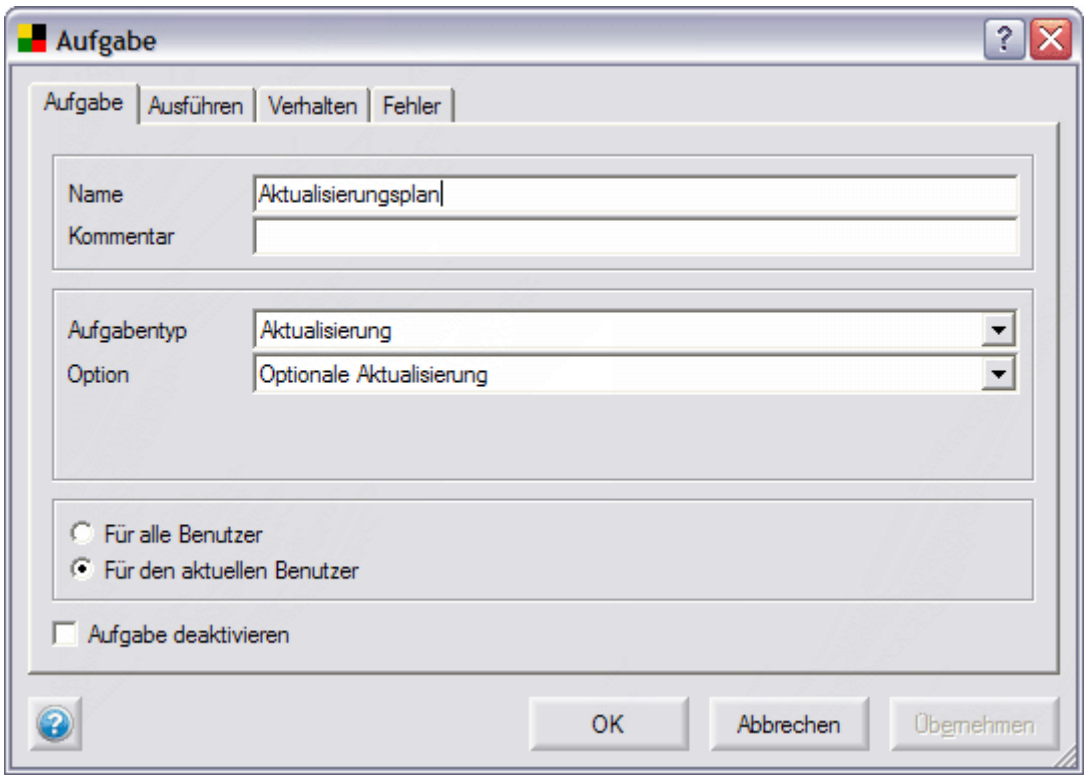
Für eine detaillierte Beschreibung der einzelnen Aktualisierungslevels lesen Sie bitte auch das Kapitel 14.1 Aktualisierungslevels

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.

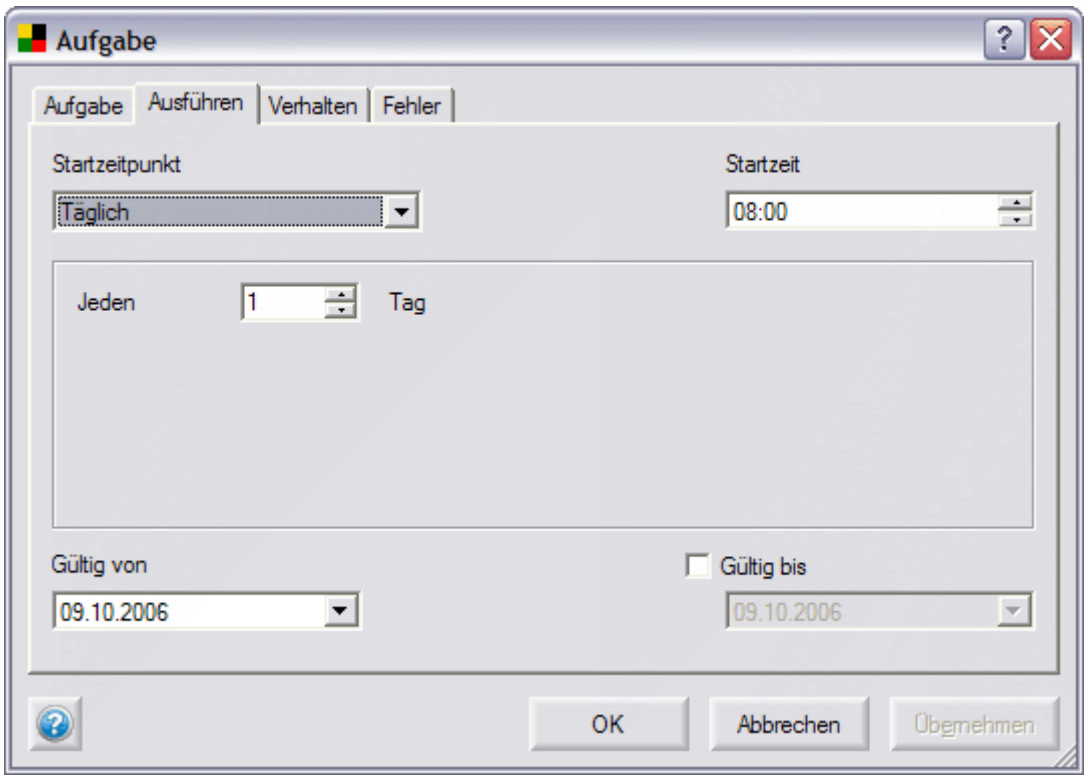


b) Aktualisierungsplan Konfiguration / Reiter Ausführen

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

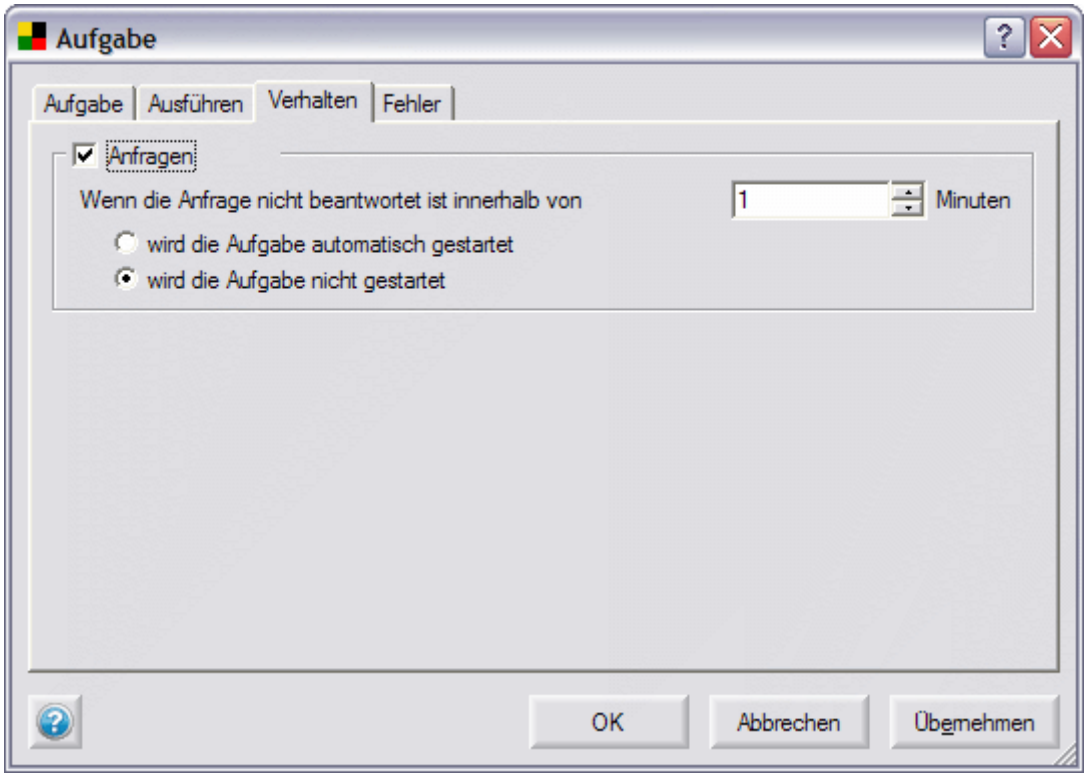
- ***Startzeitpunkt*** – aus der Liste der Optionen im Abschnitt ***Startzeitpunkt*** können Sie auswählen, ob Sie die Aktualisierung nur einmal ausführen, oder ob sie regelmäßig gestartet werden soll. Geben Sie für diesen Fall bitte das Startintervall an.
- ***Startzeit***– wenn Sie gerade eingestellt 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



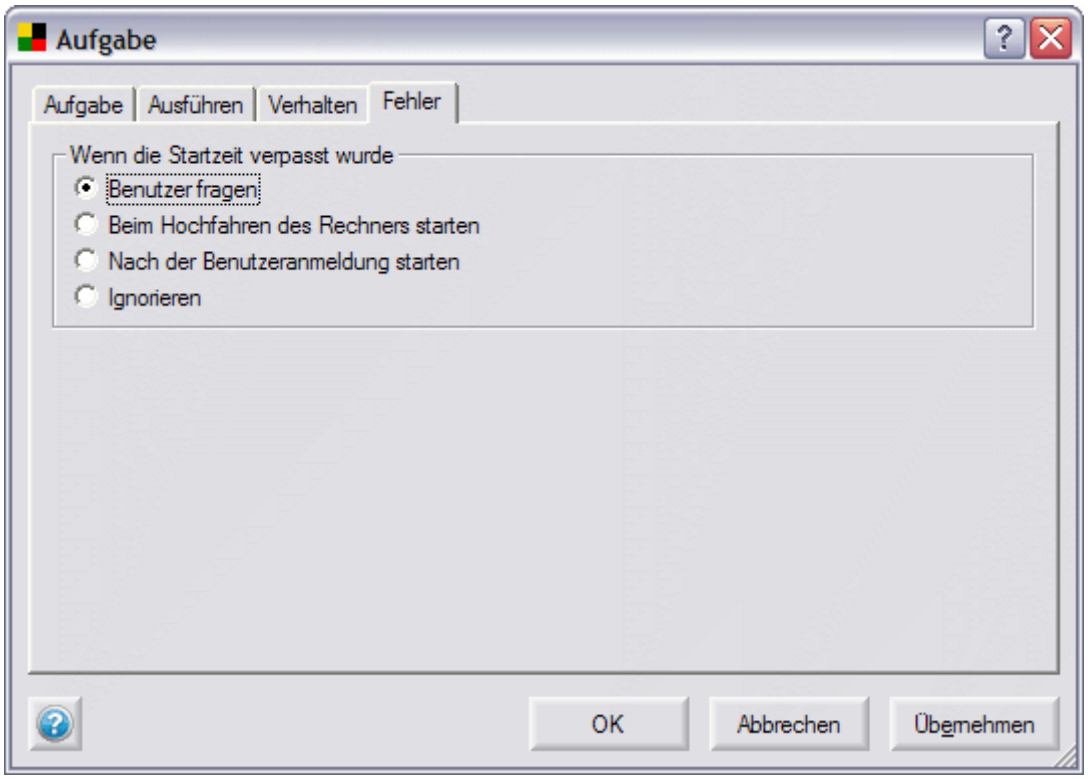
c) Aktualisierungsplan Konfiguration / Reiter Verhalten

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:



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. 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:

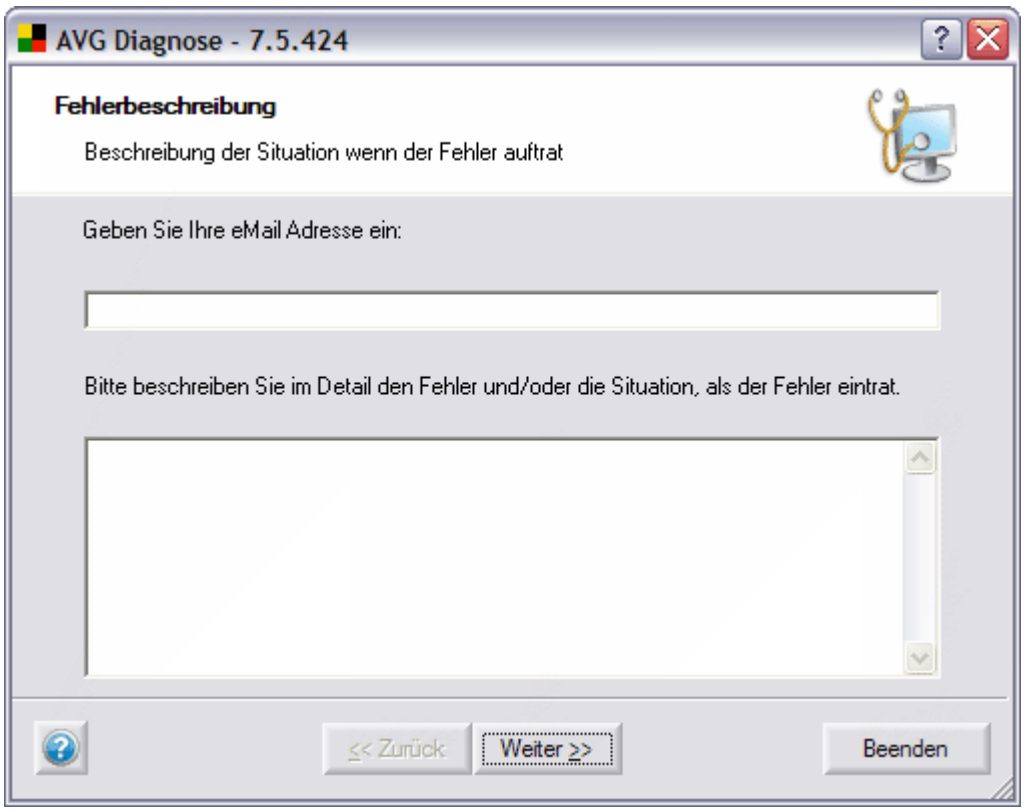
Wenn Sie einen Service Code erhalten haben, geben Sie diesen bitte in das Textfeld ein oder benutzen Sie hierfür die Methode Kopieren/Einfügen. Der Code startet automatisch den korrekten ***AVG Diagnose Modus***, der gewährleistet, dass nur die erforderlichen (und nicht überflüssige) Daten während der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

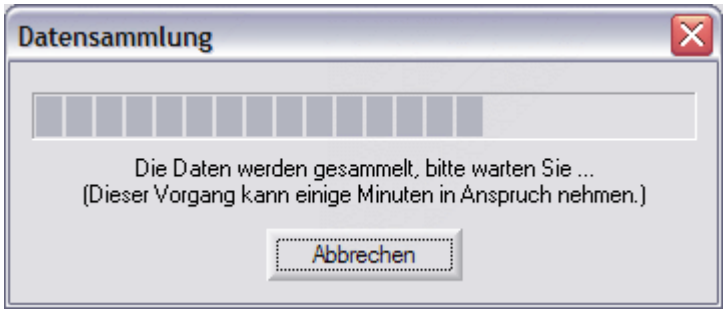


Beschreiben Sie so gut es geht im Detail, was für ein Problem Sie mit Ihrer AVG-Installation haben, unter welchen Umständen dieses Problem auftritt; bitte geben Sie jede Information ein, die dem technischen Support bei der Lösung des Problems helfen könnte.

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.

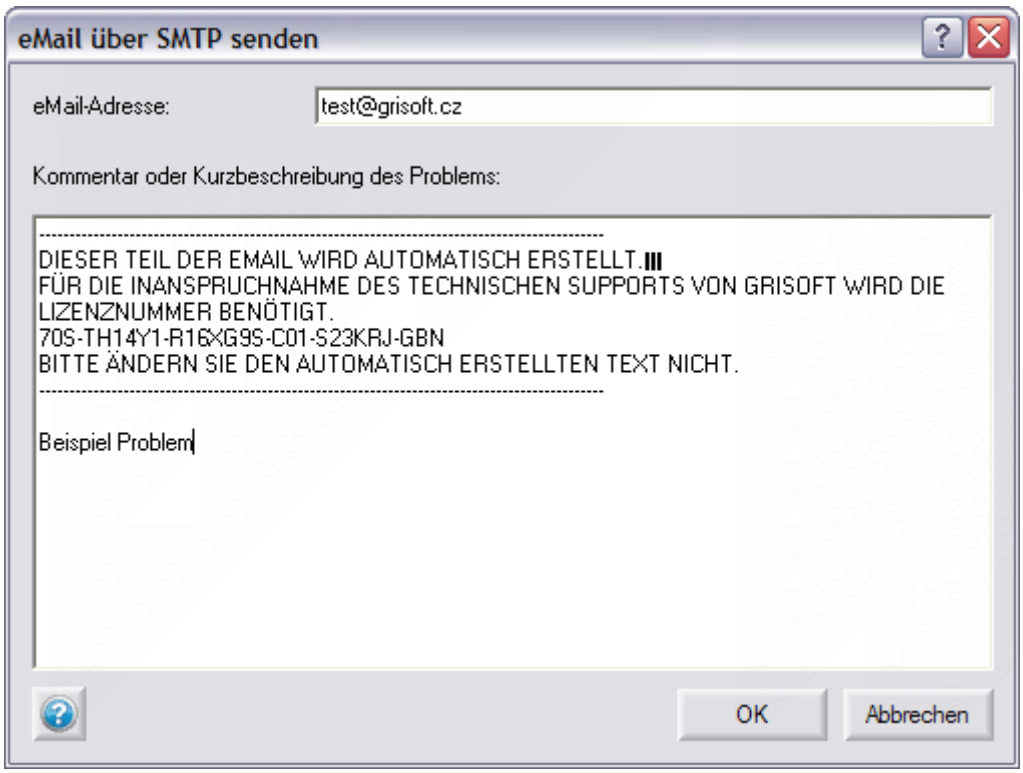


c) *AVG Diagnose* - Beenden des Assistenten

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.

Die 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 .

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 eine Problems mit AVG von Wichtigkeit sein könnten.

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

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

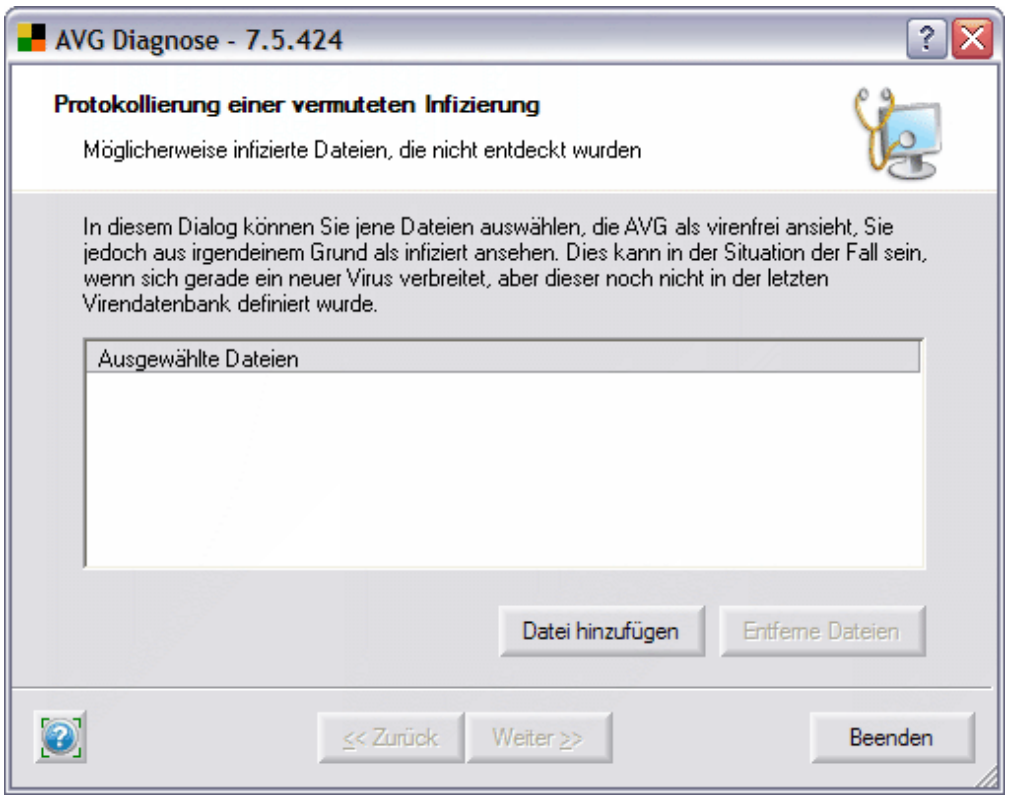
  Mit ***AVG Diagnose im Basis-Modus*** können Sie eine verdächtige Datei (oder mehrere Dateien) zur Analyse an den technischen Support von Grisoft senden.

  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***

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.

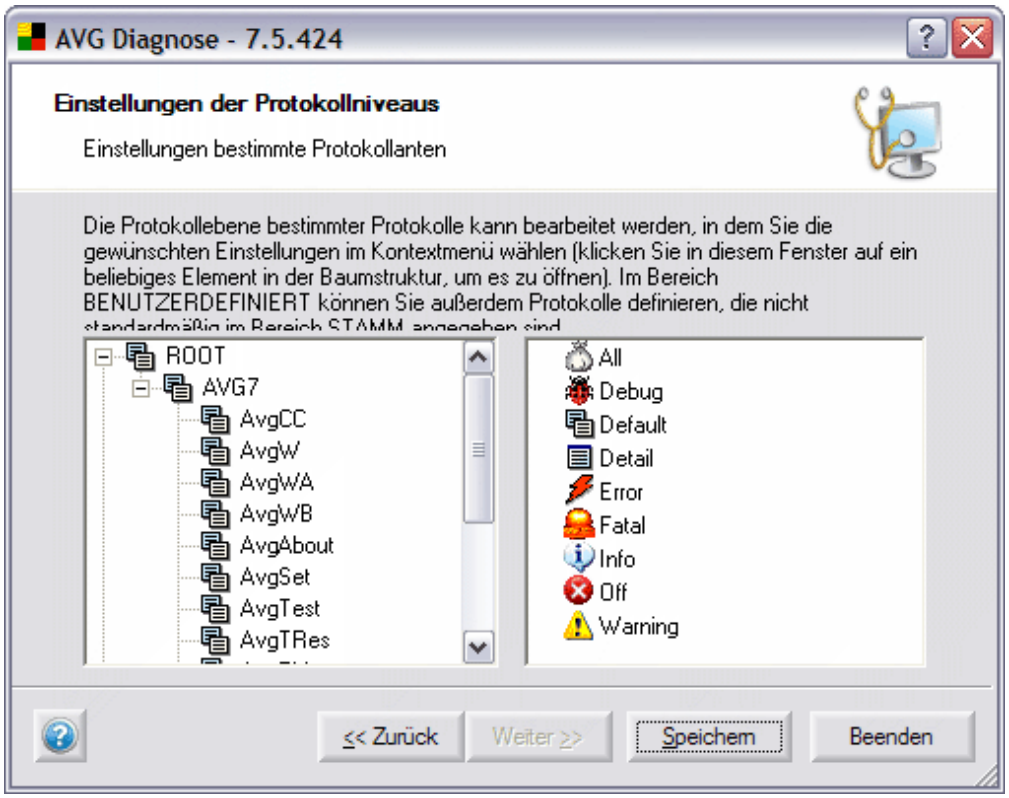
Parameter: /MODE=FEEDBACK

- **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.***

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 Schalfläche ***Weiter*** ist in diesem Dialog deaktiviert)

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

- **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
Kein Parameter	Startet AVG Diagnose im Vollmodus (Standard).
/CODE=<code>	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.
/MODE=FULL	Startet AVG Diagnose im Vollmodus (Standard).
/MODE=VIRUS	Startet AVG Diagnose im Modus verdächtige Datei zur Analyse senden.
/MODE=FALSE	Startet AVG Diagnose im *falsche Alarm* Datei zur Analyse senden Modus.
/MODE=FEEDBACK	Startet AVG Diagnose im Kundenfeedback Modus.

/MODE=LOGLEVEL	Startet AVG Diagnose im Protokolleveleinstellungsmodus.
/MODE=ERRDUMP	Startet AVG Diagnose im Störungserkennungsmodus.
/LOGROOT=<level>	Startet automatisch den Protokolleveleinstellungsmodus und erlaubt Ihnen, einen Protokollevel direct auszuwählen.
/FILE=<file>	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.
/CLEARUPD	Löscht alle überflüssigen und temporären Dateien.
/NOUI	Minimiert die Anzahl der angezeigten Dialogfenster.
/LNG=<lng>	Ermöglicht Ihnen, die Oberfläche der AVG Diagnose auf eine andere Sprache umzuschalten. Verfügbare Sprachen und deren Codes:

CZ=0x0405	GE=0x0407	PB=0x0416
SK=0x041b	FR=0x040c	PL=0x0415
US=0x0409	SP=0x040a	SC=0x081a
IT=0x0410	HU=0x040e	NL=0x0413