

# AntiVir Professional Edition

Neben der AntiVir Personal Edition bietet H+BEDV Datentechnik GmbH die **AntiVir 6 Professional Edition** an. AVGuard/XP und AVWin/XP (das Desktop-Programm) aus diesem Paket bieten eine stark erweiterte Funktionalität sowie eine flexible und preiswerte Lizenzierung, insbesondere bei Mehrfach-Lizenzen.

## Zusätzliche Features:

- Unterstützung von Netzlaufwerken.
- Unterstützung von Netzwerk-Warnungen.
- Unterstützung von Such-Profilen.
- Suche in Verzeichnissen.
- Durchsuchen von benutzerdefinierten Archive.
- Explizites Durchsuchen von Bootsektoren.
- Tools zur komfortablen Verteilung und Installation in Netzwerken (Intranet-Update-Wizard).
- Start externer Programme abhängig von Suchergebnissen.
- Scheduler (zeitgesteuerte Suchläufe).
- Passwortschutz für Konfiguration.
- Prüfsummen-Option.
- Stark erweiterte Konfigurationsmöglichkeiten des Such- und Reparatur-Engine.
- Weiter sind im Paket die E-Mail Scanner für MS Mail, Qualcomm Eudora, MS Outlook und MS Exchange Client sowie eine Lizenz von Antivir für DOS enthalten.

Die Professional Version ist derzeit für folgende Plattformen erhältlich: DOS, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD, OpenBSD, Novell NetWare, Windows NT Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client, MS Mail sowie also SMTP Lösung (AVMailGate) für Linux, FreeBSD und OpenBSD.

## **Weitere Informationen zu unseren AntiVir Professional Produkten erhalten Sie unter:**

H+BEDV Datentechnik GmbH  
Lindauer Straße 21  
D-88069 Tettnang  
Germany

Internet: <http://www.antivir.de>  
E-Mail: [info@antivir.de](mailto:info@antivir.de)  
Tel.: +49 (0) 7542-93040  
Fax: +49 (0) 7542-52510

# Bei Problemen

Ab Version 6.10.01.00 ist AVGuard unter den folgenden Betriebssystemen lauffähig: Windows NT, Windows 2000 Professional, Windows XP Home und Windows XP Professional. Falls AVGuard/XP nicht funktionieren sollte, bei Problemen mit AVGuard/XP oder bei einer Infektion, die Sie nicht selber bereinigen können, sollten Sie folgendes beachten oder prüfen:

- ▶ Ist der Dienst (engl. Service) aktiv? Das Icon (der kleine Regenschirm) rechts unten im System-Tray muss aufgespannt sein! Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste auf "Start / Einstellungen / Systemsteuerung". Starten Sie das Konfigurationspanel "Dienste" per Doppelklick. Suchen Sie nach dem Eintrag "AntiVir Service". Als Startart muss "Automatisch" eingetragen sein, bei "Anmelden als" muss "Systemkonto" angewählt sowie der Schalter für "Interaktive Beziehung mit Desktop erlauben" aktiviert sein. Der Status des Service muss "Gestartet" sein. Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche "Starten". Sollte eine Fehlermeldung auftreten, überprüfen Sie bitte die Ereignisanzeige. Ist dies nicht von Erfolg gekrönt, sollten Sie ggf. AntiVir/XP über "Start / Einstellungen / Systemsteuerung / Software" komplett deinstallieren, den Rechner neu starten und AntiVir/XP anschließend neu installieren.
  
- ▶ Falls der Dienst aktiv ist, prüfen Sie bitte folgendes: Im Kontrollprogramm unter "Konfiguration / Suchen" muss in der Gruppe Gerätemodus eine der beiden möglichen Checkboxen aktiviert sein.
  
- ▶ Weiter muss in der Gruppe Laufwerke die Option "Lokale Laufwerke" aktiviert sein.
  
- ▶ Überprüfen Sie die Einstellung in der Gruppe Durchsuchen. Falls hier "Nur Programmdateien" aktiviert ist, sollten Sie die Liste mit den Dateierweiterungen prüfen und ggf. auf die Standardwerte setzen.
  
- ▶ Um reparieren zu können, muss unbedingt unter "Konfiguration / Reparatur" die Einstellung Automatisch reparieren aktiviert sein!
  
- ▶ Hat AVGuard/XP die Datei überhaupt durchsucht? Stellen Sie hierzu unter Konfiguration / Report die Protokollierung auf "Vollständige Informationen". Testen Sie dann den Zugriff erneut und prüfen Sie dann das Logfile.
  
- ▶ Falls Sie in der Logdatei viele Einträge mit "Zugriff verweigert" finden, kontrollieren Sie bitte folgendes: Der AVGuard/XP Dienst "AntiVirService" benötigt zur Anzeige der Warnungen unbedingt Zugriffsrechte auf die Konsole. D.h., er muss unter dem lokalen Systemkonto "SYSTEM" angemeldet sein. Außerdem muss unbedingt in der Systemsteuerung unter den Diensteigenschaften die Option "Interaktion mit Desktop erlauben" aktiviert sein. Beachten Sie deshalb auch, dass das lokale Systemkonto "SYSTEM" volle Zugriffsrechte auf alle lokalen Festplatten und Laufwerke benötigt.

Weitere Informationen finden Sie in der Datei README.WRI im Rootverzeichnis Ihrer CD-Rom, in der Datei READ.ME im Programmverzeichnis von AVGuard/XP oder im Internet unter [www.free-av.de](http://www.free-av.de).

## AntiVir Support Forum

Um Ihnen Anfragen an den technischen Support zu erleichtern, haben wir für Sie das AntiVir Support Forum eingerichtet.

Sie finden dort häufig gestellte Fragen zu AntiVir und haben die Möglichkeit, ebenfalls technische Fragen zu stellen.

Das AntiVir Support Forum erreichen Sie im Internet unter: <http://www.free-av.de/forum>.

Sie können mit anderen Anwendern diskutieren und eigene Erfahrungen oder Hinweise zu den gestellten Fragen weitergeben. Moderiert wird das Forum durch unsere Support Mitarbeiter.

Um Einträge veröffentlichen zu können, lassen Sie sich bitte registrieren. Den Link "Registrieren" finden Sie auf der Startseite des Forum-Servers.

Damit wir Ihnen schnell und zuverlässig helfen können, sollten Sie in Ihrer Anfrage die folgenden Informationen angeben:

- Versionsnummern von VDF-Datei, Engine und Programm.
- Ihre Betriebssystemversion und eventuell installierte Service-Packs.
- Installierte Software-Pakete, z.B. weitere Antivirensoftware anderer Hersteller.
- Genaue (!) Meldungen des Programms oder der Logdatei.

**Technische Anfragen per Telefon/Fax/Brief oder via E-Mail können von uns nicht beantwortet werden!**

# Das Menü Datei

Dieses Menü enthält folgende Einträge:

## AVGuard aktivieren

Dieser Menüpunkt aktiviert AVGuard/XP. Nach einer Neuinstallation sollte AVGuard/XP immer bereits aktiviert sein. Sie können diesen Menüpunkt verwenden, wenn Sie vorher AVGuard/XP mit dem Menüpunkt "AVGuard deaktivieren" ausgeschaltet haben. Diese Funktion ist nur anwählbar, wenn der AVGuard/XP vorher deaktiviert war.

## AVGuard deaktivieren

Dieser Menüpunkt deaktiviert AVGuard/XP. Nach einer Neuinstallation sollte AVGuard/XP immer aktiviert sein. Sie können diesen Menüpunkt verwenden, um AVGuard/XP temporär zu deaktivieren. Diese Funktion ist nur anwählbar, wenn der AVGuard/XP vorher aktiviert war.

## AntiVir Hauptprogramm starten

Mit diesem Menüpunkt lässt sich vom AVGuard/XP aus das AntiVir Hauptprogramm einfach starten, z.B. um einen Suchlauf über das komplette Laufwerk C:\ durchzuführen.

## Internetupdate starten

Der Internetupdater lässt sich aber der Version 6.17 nun auch über diesen Menüpunkt starten. Dies vereinfacht die Bedienung, da Sie für den Start des Updaters nun nicht immer zuerst das Hauptprogramm starten müssen. Dieser Menüpunkt ist nur anwählbar, wenn der Internetupdater auch installiert und aktiviert wurde.

## Kontrollprogramm minimieren oder Tasten ALT+F4 oder Schaltfläche



Mit diesem Menüpunkt wird das Fenster des Kontrollprogramms geschlossen, das Programm aber nicht beendet. Das Kontrollprogramm wird verkleinert (minimiert), und Sie können anschließend das Programmicon rechts unten im Anzeigebereich der Task-Leiste (System-Tray) sehen.

## Kontrollprogramm schließen

Mit diesem Menüpunkt verlassen Sie das Kontrollprogramm des AVGuard/XP. Das Programm wird komplett beendet und kann anschließend nur noch über das entsprechende Icon im Programmordner von AntiVir/XP gestartet werden.

# Das Menü Hilfe

In diesem Menü finden Sie einige Informationen über AVGuard/XP sowie über die Bedienung.

## **Hilfe (F1) oder Schaltfläche**



Öffnet das kontext-sensitive Hilfe System (diese Seiten).

## **Hilfe verwenden**

Hier sehen Sie, wie Sie die kontext-sensitive Hilfe verwenden müssen.

## **Hilfe Index**

Zeigt eine Seite mit Querverweisen auf alle verfügbaren Hilfeseiten an.

## **Über AVGuard/XP**

Mit diesem Menüpunkt gelangen Sie in ein Fenster, das Ihnen erweiterte Informationen über AVGuard/XP, Ihre Lizenzinformationen sowie unsere Adressen anzeigt.

# Das Menü Optionen

Dieses Menü enthält folgende Einträge:

**Konfiguration** oder Taste F4 oder Schaltfläche



Wählen Sie diesen Menüpunkt, um AVGuard/XP zu konfigurieren.

**Reportdatei anzeigen**

Zeigt die Reportdatei des AVGuard/XP.

# Dateiaktion

In diesem Feld wird die aktuelle Aktion angezeigt, die AVGuard/XP im Falle eines Funds vornimmt. Bitte beachten Sie hierbei, dass diese Aktionen nur dann ausgeführt werden, wenn die infizierte Datei nicht repariert werden konnte.

## Datei reparieren

AVGuard/XP versucht eine infizierte Datei zu reparieren. Ist eine Reparatur nicht erfolgreich, wird die Aktion unter Aktion falls Datei nicht repariert ausgeführt.

## Datei löschen

Die infizierte Datei wird gelöscht, kann aber mit entsprechenden Tools (Undelete) wieder hergestellt werden. Die Signatur könnte unter Umständen auf Ihrem Volume wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "Wipen".

## Datei wipen

Die infizierte Datei wird mit einem Standardmuster überschrieben und gelöscht. Sie kann nicht wieder hergestellt werden.

## Datei verschieben

Die infizierte Datei wird in das unter Quarantäneverzeichnis angegebene Verzeichnis verschoben. Falls bereits eine Datei gleichen Namens existiert, wird die Datei verschoben und nach \*.001, \*.002, etc. umbenannt. Die Dateien in diesem Verzeichnis können später repariert werden oder - falls nötig - uns zu weiteren Untersuchungen zugesandt werden.

## Datei umbenennen

Die infizierte Datei wird nach \*.001, \*.002, etc. umbenannt. Ein direkter Shell-Zugriff auf diese Dateien (z.B. Doppelklick) sollte so nicht mehr möglich sein. Sie können diese Dateien später reparieren und zurückbenennen.

## Nur benachrichtigen

AVGuard/XP wird Sie nur über den Fund benachrichtigen, ansonsten werden keine weiteren Aktionen ausgeführt. Falls aktiviert, wird noch ein Eintrag ins Eventlog geschrieben.

# Dateierweiterungen

Diese Liste mit Dateierweiterungen wird von AVGuard/XP verwendet, wenn die Option "Nur Programmdateien" aktiviert ist.

Sie können die Liste folgendermaßen editieren:

{button OK,}

Schließt das Fenster und übernimmt die aktuelle Liste.

{button Abbruch,}

Die Bearbeitung wird abgebrochen und alle Änderungen verworfen.

{button Einfuegen,JI('`,`HELP\_EDIT\_EXTENSION')}

Öffnet ein weiteres Fenster, in das Sie eine neue einzufügende Dateierweiterung eingeben können.

{button Loeschen,}

Löscht den markierten Eintrag aus der Liste.

{button Standard,}

Diese Schaltfläche setzt die Defaulteinstellungen, wie sie im AVGuard/XP von uns ausgeliefert werden. Beachten Sie bitte, dass die Liste der Standarderweiterungen sich mit, beispielsweise neuartigen Viren, ändern kann. (Siehe READ.ME).

{button Hilfe,}

Zeigt diese Hilfe an.

# Demo-Version

## Demo-Version

Wenn Sie keine gültige Lizenzdatei besitzen, läuft AVGuard/XP Personal Edition im eingeschränkten Demo-Modus. D.h., es werden nur Dateien auf dem lokalen Laufwerk C: untersucht und repariert. Diese Lizenzdatei HBEDV.KEY ist im Normalfall bei einem Download der Personal Edition im Paket mit enthalten.

Zur Installation einer Vollversion brauchen Sie lediglich eine gültige Lizenzdatei, die in das Installationsverzeichnis von AntiVir/XP Personal Edition kopiert werden muss. Nach einem Neustart des AVGuard/XP Dienstes ist dieser als Vollprodukt aktiv.

# Dienst-Status

Dieses Feld gibt den aktuellen Status des AVGuard/XP Dienstes an.

## Geladen

bedeutet, dass der Dienst geladen und aktiv ist. Eine Kommunikation zwischen dem Kontrollprogramm und dem Dienst ist möglich. Der Dienst arbeitet entsprechend den Einstellungen.

**Hinweis:** Auch wenn AVGuard/XP aktiviert ist, wird nicht zwangsläufig nach Viren bzw. unerwünschten Programmen gesucht, da der Gerätetreiber, die zu überwachenden Laufwerke oder anderes eventuell deaktiviert sind.

## Nicht geladen

Das Kontrollprogramm von AVGuard/XP konnte auf dem Computer keinen aktiven AVGuard/XP Dienst finden bzw. die Kommunikation ist nicht möglich. Alle Dateien können das System unbehelligt passieren. Sie sind also vor Viren und unerwünschten Programmen **nicht** geschützt! Diese Angabe kann aber auch auf ein Problem hinweisen: Der Dienst ist nicht geladen oder wurde eventuell manuell beendet. Möglicherweise sind Kontrollprogramm und Dienst inkompatibel (unterschiedliche Versionen) oder es existiert ein Kommunikationsproblem. Beachten Sie ggf. das Eventlog auf dem Zielrechner.

# Durchsuchen

AVGuard/XP hat die Möglichkeit einen Dateierweiterungsfilter zu setzen, um die zu durchsuchenden Dateien auszuwählen:

## Alle Dateien

Alle Dateien, auf die zugegriffen wird, werden durchsucht. Der Filter ist deaktiviert.

## Nur Programmdateien

Nur Dateien mit einer Erweiterung wie in der Liste spezifiziert werden durchsucht. Dies ist die Standardeinstellung. Sie können diese Liste selber ändern. Beachten Sie bitte, dass die Standardliste sich von Version zu Version ändern kann.

# Gerätemodus

Hier wird der aktuelle Gerätemodus angezeigt:

## Deaktiviert

Der AVGuard/XP Dienst ist zwar geladen, jedoch deaktiviert. Sie sind nicht geschützt.

## Beim Öffnen durchsuchen

AVGuard/XP durchsucht alle Dateien, bevor Sie für die entsprechende Anwendung geöffnet werden.  
(Standard)

## Nach Schließen durchsuchen

AVGuard/XP durchsucht nur Dateien, die auf einem Volume neu erstellt oder verändert wurden.

## Bei Öffnen und Schließen suchen

AVGuard/XP durchsucht Dateien vor dem Öffnen (d.h. beim Lesen bzw. Starten) und nach dem Schließen (d.h. nach dem Schreiben oder Verändern) einer Datei.

# Hauptfenster

Das Hauptfenster von AntiVir Guard für Windows (Personal Edition) besteht im Prinzip aus 3 Bereichen. Der Menüleiste, der Toolbar und dem Anzeigebereich für die Statistikdaten. Erweiterte Statistikdaten sowie zusätzliche Konfigurationsmöglichkeiten bietet Ihnen unsere Profi-Variante: AntiVir 6 Professional.

## Die Optionen der Menüleiste

Datei  
Optionen  
Hilfe

## Anzeigegruppe Konfiguration

Dienst-Status: Zeigt den aktuellen Status des AVGuard/XP Dienst an.  
Dateiaktion: Dieses Feld zeigt die auszuführende Aktion an, wenn die Benutzerwarnungen deaktiviert sind.  
Gerätemodus: Gibt an, wann AVGuard/XP die Dateien untersuchen soll.  
Durchsuchen: Was ist zu durchsuchen: Alle Dateien oder nur Dateien mit speziellen Dateierweiterungen. (Programmdateien)

## Anzeigegruppe Statistik

In diesen Ausgabefeldern sehen Sie die aktuelle Statistik von AVGuard/XP. Beachten Sie bitte, dass diese - aus Performancegründen - nur zweimal pro Sekunde aktualisiert wird. Es sich bei allen statistischen Daten nur um einen "Snapshot", d.h. einen temporären Zustand des Dienstes und nicht um Echtzeitinformationen.

**Letzte Datei:** Gibt die letzte von AVGuard/XP durchsuchte Datei an.  
**Dateianzahl:** Die Anzahl der durchsuchten Dateien.  
**Letzte Meldung:** Der Name des letzten gefundenen Virus bzw. unerwünschten Programms.  
**Anzahl Meldungen:** Die Anzahl der gefundenen Viren bzw. unerwünschter Programme.  
**Repariert:** Die Anzahl erfolgreich reparierter Dateien.

# Hilfe Inhalt

Die folgenden Seiten sind aktuell verfügbar:

[AntiVir Professional Edition](#)  
[Bei Problemen](#)  
[Das Menü Datei](#)  
[Das Menü Hilfe](#)  
[Das Menü Optionen](#)  
[Dateiaktionen](#)  
[Dateierweiterungen](#)  
[Demo Version](#)  
[Dienst-Status](#)  
[Durchsuchen](#)  
[Gerätemodus](#)  
[Hauptfenster](#)  
[Konfigurieren](#)  
[Kontrollprogramm minimieren](#)  
[Kontrollprogramm schließen](#)  
[Neue Dateierweiterung](#)  
[Registerkarte Aktion](#)  
[Registerkarte Heuristik](#)  
[Registerkarte Reparatur](#)  
[Registerkarte Report](#)  
[Registerkarte Suchen](#)  
[Registerkarte Unerwünschte Programme](#)  
[Über AVGuard/XP](#)  
[Unerwünschte Programme](#)  
[Virenbefall](#)

# Konfigurieren



Dieser Menüpunkt zeigt das Dialogfeld mit allen Konfigurationsmöglichkeiten an. Die Schaltfläche hat hierbei die gleiche Wirkung.

Das Dialogfeld enthält dabei die folgenden Registerkarten:

<u>Suchen</u>	Enthält alle Einstellungen, die für den Gerätetreiber bzw. die Suche verwendet werden.
<u>Aktion</u>	Hier werden die Aktionen definiert, die AVGuard/XP im Falle eines Fundes ausführen soll.
<u>Reparatur</u>	Einstellungen für die Reparatur.
<u>Heuristik</u>	Einstellungen für die Makroviren-Heuristik und die Behandlung von Dokumentenvorlagen.
<u>Report</u>	Einstellungen für die Reportdatei.
<u>Unerwünschte Programme</u>	Viren- bzw. Malware-Funde werden von AntiVir generell gemeldet. Darüber hinaus können Sie hier optional Einstellungen zur Meldung <u>unerwünschter Programme</u> vornehmen.

# Kontrollprogramm minimieren

oder Schaltfläche ▶

Wählen Sie diesen Eintrag, wenn Sie das AVGuard/XP Kontrollprogramm minimieren wollen, es jedoch nicht vollständig geschlossen werden soll. Es wird verkleinert (minimiert), und Sie können anschließend das Programmicon rechts unten im System-Tray sehen. Um es wieder zu vergrößern, machen Sie einfach einen Doppelklick auf das kleine Icon. Im verkleinerten Zustand benötigt das Programm keinerlei Rechenzeit. Haben Sie das Icon verkleinert, können Sie mit einem Klick der rechten Maustaste auf das kleine Icon das Kontext-Menü aufrufen.

## **Kontrollprogramm schließen**

Bitte wählen Sie diese Funktion um das AVGuard/XP Kontrollprogramm zu verlassen und komplett zu beenden. Das Programm kann anschließend nur noch über das entsprechende Icon im Programmordner von AVGuard/XP gestartet werden.

# Neue Dateierweiterung

In diesem Fenster können Sie eine neue Dateierweiterung eingeben, die in die Liste der Dateierweiterungen eingefügt wird. Die Maximallänge beträgt 6 Zeichen.

{button OK,}

Die neue Dateierweiterung wird in die Liste der Dateierweiterungen eingefügt.

{button Abbruch,}

Die aktuelle Erweiterung wird verworfen und nicht in die Liste eingefügt.

{button Hilfe,}

Zeigt diese Hilfe an.

# Registerkarte Aktion

In diesem Dialog werden die Aktionen konfiguriert, die AVGuard/XP ausführen soll, falls ein Virus oder unerwünschtes Programm gefunden wird.

## Aktion falls Datei nicht repariert

Wird der AVGuard/XP fündig, gibt AVGuard/XP eine Dialogbox aus, damit der Benutzer die nun auszuführende Aktion selber auswählen kann. Falls der Virus oder das unerwünschte Programm entfernt werden konnte und die automatische Reparatur aktiviert ist, kann der Benutzer unter anderem auch eine Reparatur der Datei wählen. Schlägt die Reparatur fehl, wird die in dieser Gruppe gewählte Aktion vorgenommen. Wählt der Benutzer in der angezeigten Dialogbox eine andere Option (z.B. Löschen), wird diese ausgeführt, egal wie die Voreinstellung in dieser Gruppe ist.

### Datei löschen

Die Datei wird gelöscht, kann jedoch mit einem entsprechenden Programm wieder hergestellt werden.

### Datei wipen

Die Datei wird überschrieben und gelöscht. Sie kann nicht wieder hergestellt werden.

### Datei verschieben

Die Datei wird in das Quarantäneverzeichnis verschoben, so dass kein direkter Zugriff mehr möglich ist. Bitte beachten Sie, dass nur der Administrator Zugriff auf dieses Verzeichnis haben sollte.

### Datei umbenennen nach \*.XXX

Die Datei wird nach \*.001, \*.002 etc. umbenannt. Sie kann so durch die Shell nicht mehr direkt ausgeführt werden.

### Datei ignorieren

Der Fund wird lediglich in der Reportdatei eingetragen, sofern diese aktiviert ist.

## Benachrichtigungen

### Ereignisprotokoll verwenden

Bei jedem Fund wird ein Eintrag in das Ereignisprotokoll geschrieben. Der Administrator kann eventuelle Funde erkennen und entsprechend reagieren.

### Warnton

Ist die Funktion aktiviert, spielt AVGuard/XP bei einem Fund eine Tonfolge ab.

## Quarantäneverzeichnis

Falls eine Datei verschoben werden soll, wird Sie AVGuard/XP in das in diesem Feld angegebene Verzeichnis verschieben.

# Registerkarte Heuristik

Diese Registerkarte enthält die Einstellungen für die Makrovirenheuristik sowie einige Einstellungen für den Umgang mit Word 6/7 Dokumentenvorlagen.

## Verdächtige Makros

AVGuard/XP enthält eine Makrovirenheuristik, die auch unbekannte (neue) Makroviren entdecken kann. Dies geschieht durch eine aufwendige Analyse und Untersuchung des Makro-Codes nach virentypischen Funktionen. Solche Makros werden dann als verdächtig gemeldet. Verdächtige Makros können gelöscht - was das einfachste - oder nur gemeldet werden. Da aber ein Virus normalerweise aus mehr als einem Makro besteht, stellt sich die Frage was mit den restlichen, möglicherweise nützlichen Makros geschehen soll.

### Verdächtige Makros löschen

Alle als verdächtig gemeldeten Makros werden gelöscht. Mit dieser Einstellung werden nützliche Makros dann nicht versehentlich gelöscht. Der Nachteil hierbei liegt darin, dass die restlichen zum Virus gehörenden Makros im Dokument verbleiben und von anderen Antivirenprogrammen gemeldet werden könnten.

### Alle Makros löschen falls eines verdächtig

Falls diese Option aktiviert ist, werden alle Makros eines Dokuments gelöscht, wenn im Dokument ein Makro als verdächtig gemeldet wurde. Der Nachteil hierbei ist, dass evtl. auch nützliche Makros mit gelöscht werden.

### Verdächtige Makros nur melden

Keine sehr gute Einstellung. Hiermit könnten Sie Ihre Applikationen leicht infizieren. Um sicher zu gehen, dass ein als verdächtig gemeldetes Dokument keinen Virus enthält, sollten Sie uns die Datei zur Überprüfung zusenden. Wir benachrichtigen Sie, falls es sich wirklich um einen Virus handelt.

## Dokumentenvorlagen

Word 6/7 Dokumentenvorlagen bestehen wie normale Dokumente aus Text, zusätzlich können Sie jedoch Daten enthalten. Wenn Word 6/7 solch eine Dokumentenvorlage öffnet, sucht es nach diesen Daten und wertet sie aus. Ein Virus kann nur Dokumentenvorlagen infizieren, deshalb werden Dokumente zur Infektion immer zuerst in das Vorlagen-Format gewandelt. AVGuard/XP kann nun solche Dokumentenvorlagen wieder zurück in das eigentliche Dokumentenformat wandeln, wenn keine zusätzlichen Daten vorhanden sind. Alle Makros müssen gelöscht sein, es sind keinerlei Menüs oder Shortcuts erlaubt.

### Nie konvertieren

Dokumentenvorlagen werden in keinem Fall in das Dokumentenformat gewandelt.

### Nur .DOC Dateien konvertieren

Dokumentenvorlagen haben meist die Dateierweiterung \*.DOT oder \*.WIZ. Reine Dokumente haben die Dateierweiterung \*.DOC. Aktivieren Sie diese Option, wenn AVGuard/XP reparierte Dokumentenvorlagen mit der Dateierweiterung \*.DOC zurück in das Dokumentenformat wandeln soll.

### Dokumentenvorlagen immer konvertieren

Ist diese Option aktiviert, konvertiert AVGuard/XP alle Word 6/7 Dokumentenvorlagen in das Dokumentenformat, sofern möglich.

### Dokumentenvorlagen komprimieren

Wenn ein Makro gelöscht wird, verbleibt sein Name immer noch im Dokument. Das Makro selber wurde überschrieben und als gelöscht markiert. Da einige Antivirenprogramme nur nach solchen Makronamen suchen, könnten Sie einen Virus melden, wo keiner mehr ist. AVGuard/XP kann nun mit dieser Option auch alle Referenzen auf gelöschte Makros und ihre Namen aus der Dokumentenvorlage löschen.

# Registerkarte Reparatur

Diese Registerkarte enthält die Einstellungen für die Reparatur von infizierten Dateien.

## Infizierte Dateien

### Automatisch reparieren

Falls aktiviert, versucht AVGuard/XP Dateien automatisch zu reparieren. Diese Option **muss auch dann aktiviert sein**, wenn der Benutzer in den Warnmeldungen die Reparatur auswählen können soll.

## Sicherheitskopie

AVGuard/XP kann von infizierten Dateien vor der Reparatur eine Sicherheitskopie (ein Backup) erstellen. Diese Funktion ist z.B. in mehreren Fällen sinnvoll. Zum einen zu Dokumentationszwecken, falls in Ihrem Betrieb beispielsweise ein Virenbefall dokumentiert und protokolliert wird, und zum anderen, falls bei eingeschalteter Reparatur ein Makrovirus "nur" von der Heuristik erkannt und repariert wird. Sie sollten uns dann die erstellte Sicherheitskopie zusenden, damit die Signatur für das nächste Update mit aufgenommen werden kann.

### Sicherheitskopie vor Reparatur

Falls aktiviert, kopiert AVGuard/XP jede zu reparierende Datei vor der eigentlichen Reparatur in das angegebene Verzeichnis, d.h. es wird ein Backup erstellt.

### Verzeichnis für Sicherheitskopien

In diesem Verzeichnis werden die Sicherheitskopien vor der Reparatur erstellt. Dies ist in der Standardeinstellung das Verzeichnis \BACKUP unterhalb des Installationsverzeichnisses von AntiVir/XP.

# Registerkarte Report

AVGuard/XP besitzt eine mächtige Protokollierfunktion, die einem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann. Sie können Anzahl der protokollierten Ereignisse in gewissem Umfang einstellen.

## Name und Pfad der Reportdatei

Dieser Eintrag enthält Pfad und Dateinamen der zu erstellenden Reportdatei. Alle Einträge werden an das Ende dieser Datei angefügt.

## Protokollierung

In dieser Gruppe wird der Umfang der Reportdatei festgelegt:

### Protokollierung aus

Die Protokollierung wird komplett deaktiviert. Dies ist nur dann sinnvoll, wenn bei Testläufen mit beispielsweise vielen Viren ein maximaler Durchsatz benötigt wird.

### Standard Informationen

Alle wichtigen Informationen wie Funde, Warnungen oder Fehler werden mit in die Reportdatei aufgenommen. Weniger wichtige Dinge wie Zusatzinformationen werden ignoriert, um Ihnen einen schnellen Überblick über den aktuellen Zustand geben zu können.

### Erweiterte Informationen

Auch weniger wichtige Dinge wie Datei-Zusatzinformationen, etc. werden mit aufgenommen.

### Vollständige Informationen

Dateigrößen, -typen und -datumsangaben sowie der ganze Rest an verfügbaren Informationen wandern mit in die Reportdatei.

# Registerkarte Suchen

Die Einstellungen in dieser Registerkarte dienen der Konfiguration des Scanners von AVGuard/XP.

## Gerätemodus

Hiermit wird der Zeitpunkt für das Durchsuchen einer Datei beim Zugriff festgelegt.

### AVGuard deaktivieren

Mit dieser Funktion können Sie AVGuard/XP komplett deaktivieren. Beachten Sie aber, dass Ihr Computer dann nicht mehr geschützt ist. Sie sollten daher dieses Feature nur in Ausnahmefällen einsetzen.

### Beim Lesen durchsuchen

Falls aktiviert, werden die entsprechenden Dateien durchsucht, bevor sie von der Anwendung oder dem Betriebssystem gelesen oder ausgeführt werden können. D.h., dass AVGuard/XP jede Datei durchsucht, bevor Sie sie öffnen oder starten können. Sollte die Datei infiziert sein, wird ihnen der Zugriff auf diese Datei ggf. verweigert. Dies ist die Defaulteinstellung, da AVGuard/XP aufgrund seines internen Dateinamens-Cache die meisten Dateien nur einmal durchsucht.

### Beim Schreiben durchsuchen

Wenn diese Option aktiviert ist, werden Dateien sofort nach dem Schreiben auf das entsprechende Volume durchsucht. D.h. AVGuard/XP durchsucht Dateien nach dem Speichern beispielsweise auf Virenbefall, bevor Sie diese Datei wieder öffnen oder ausführen können. Diese Option ist z.B. für Internet-Downloads sinnvoll.

### Bei Öffnen und Schließen suchen

Hiermit können Sie AVGuard/XP veranlassen, Dateien vor dem eigentlichen Lesen (bzw. Starten) und nach dem Schreiben zu durchsuchen (siehe oben). Bitte beachten Sie aber, dass hierdurch die Performance des Systems beeinträchtigt werden kann.

## Laufwerke

AVGuard/XP kann so konfiguriert werden, dass nur Dateien auf einem bestimmten Satz von Laufwerken auf Ihrem Computer durchsucht werden. Dies sind in der Personal-Edition immer nur alle lokalen Laufwerke. Netzlaufwerke werden nur mit der "großen" AntiVir-Lösung AntiVir 6 Professional unterstützt.

### Lokale Laufwerke

Nur Dateien von lokalen Laufwerken wie Diskettenlaufwerke, Festplatte, CD-ROMs, ZIP-Drives, etc. werden durchsucht. Ist dieser Schalter deaktiviert, werden bei der Personal-Edition keine Dateien von AVGuard/XP durchsucht.

## Archive

AVGuard/XP ist in der Lage, komprimierte Dateien vor zu dekomprimieren und die enthaltenen Dateien dann zu durchsuchen. Bitte beachten Sie, dass sich dieser Prozess negativ auf die Performance auswirken kann.

### PKLite/LZExe

Ist diese Option gewählt, werden von PKLite und LZExe lauffzeit-gepackte Dateien vor der Suche dekomprimiert und erst dann durchsucht. Hierdurch können beispielsweise eventuelle Viren, die sich in diesen komprimierten Dateien verstecken, ebenfalls gefunden werden.

## Durchsuchen

Dateierweiterungen (engl. "file extensions") werden von Windows zur Bestimmung des Typs einer Datei verwendet. Ausführbare Dateien haben z.B. immer die Dateierweiterung ".EXE", Textdateien normalerweise die Endung ".TXT". AVGuard/XP kann nun einen Filter verwenden, um die Anzahl der zu durchsuchenden Dateien anhand einer Liste mit Dateierweiterungen einzuschränken.

### Alle Dateien

Ist diese Option gewählt, werden alle Dateien automatisch nach Viren bzw. unerwünschten Programmen durchsucht.

### Erweiterungsliste verwenden

Nur Dateien mit einer in der Liste enthaltenen Dateierweiterung werden durchsucht.

### {button Dateierweiterungen.JI('HELP\_FILE\_EXTENSIONS')}

Mit Hilfe der Schaltfläche "Dateierweiterungen" wird ein Fenster geöffnet, in dem eine Liste mit allen Endungen angezeigt wird, die der Guard bei einem Suchlauf berücksichtigt. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen. Beachten Sie bitte, dass sich die Standardliste von Version zu Version ändern kann.

# Registerkarte Unerwünschte Programme

AntiVir schützt Sie vor Computerviren.

Darüber hinaus haben Sie die Möglichkeit, differenziert nach kostenverursachenden Einwahlprogrammen (Dialer), Backdoor-Steuersoftware (BDC), Spiele (Games), Witzprogrammen (Jokes) sowie nach möglicher schädliche Software (PMS) suchen zu lassen.

- ▶ Backdoor-Steuersoftware (BDC)
- ▶ Kostenverursachende Einwahlprogramme (Dialer)
- ▶ Spiele (Games)
- ▶ Witzprogramme (Jokes)
- ▶ Mögliche schädliche Software (PMS)

Die Selektion aktivieren Sie durch einen Klick auf das entsprechende Kästchen.

Über [Alle aktivieren](#) werden sämtliche Typen aktiviert.

Wird ein Typ deaktiviert, werden Dateien, die als entsprechender Programmtyp erkannt werden, nicht mehr gemeldet. Es erfolgt auch kein Eintrag in die Reportdatei.

# Über AVGuard/XP (2000+NT) Personal Edition

Die AntiVir Personal Edition mit dem integrierten residenten Virenwächter AVGuard/XP ist ein speziell für den Heimanwender entwickeltes Antivirenprogramm. Ab Version 6.10.01.00 ist AntiVir/XP auf folgenden Betriebssystemen lauffähig: Windows NT Workstation, Windows 2000 Professional, Windows XP Home und Windows XP Professional. Die Personal Edition ist für den privaten, nicht kommerziellen Einsatz kostenfrei und kann im Internet unter der folgenden Web-Adresse bezogen werden: <http://www.free-av.de>

## AntiVir 6 Professional

Sollten Sie Netzwerkunterstützung, Netzwerk-Integration oder eine stark erweiterte Funktionalität benötigen, empfehlen wir Ihnen die Profi-Version von AntiVir: AntiVir 6 Professional. AntiVir 6 ist in der Professional-Variante derzeit für die folgenden Plattformen erhältlich: DOS, Windows 3.1x, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD (i386), OpenBSD (i386), Novell NetWare, Windows NT Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client, MS Mail.

Informationen zu diesen Produkten erhalten Sie unter einer der folgenden Adressen oder im Internet unter:

**H+BEDV Datentechnik GmbH**  
Lindauer Straße 21  
D-88069 Tettnang  
Germany

Internet: <http://www.antivir.de>  
E-Mail: [info@antivir.de](mailto:info@antivir.de)  
Tel.: +49 (0) 7542-93040  
Fax +49 (0) 7542-52510

## Über AVGuard/XP

In dieser Dialogbox finden Sie einige Informationen über den AVGuard/XP Dienst, den Geräte-Treiber und das Kontrollprogramm.

## Versionsinformationen

In der ersten Zeile finden Sie die Version und das Erstellungsdatum des AVGuard/XP Kontrollprogramms. Die nächste Zeile enthält die Versionsnummer der verwendeten AntiVir-Suchengine. Die dritte Zeile schließlich enthält Version, Erstellungsdatum und den FUP - Typ der aktuell verwendeten Virendefinitionsdatei (VDF)

## Hotline

**Technische Anfragen per Telefon/Fax/Brief oder via E-Mail können von uns nicht beantwortet werden!**

Um Ihnen Anfragen an den technischen Support zu erleichtern, haben wir für Sie das AntiVir Support Forum eingerichtet.

Sie finden dort häufig gestellte Fragen zu AntiVir und haben die Möglichkeit, ebenfalls technische Fragen zu stellen.

Das AntiVir Support Forum erreichen Sie im Internet unter: <http://www.free-av.de/forum>.

Sie können mit anderen Anwendern diskutieren und eigene Erfahrungen oder Hinweise zu den gestellten Fragen weitergeben. Moderiert wird das Forum durch unsere Support Mitarbeiter. Um Einträge veröffentlichen zu können, lassen Sie sich bitte registrieren. Den Link "Registrieren" finden Sie auf der Startseite des Forum-Servers.

## Hotline / Weitere Produktinformationen

Falls Sie Produktinformationen oder sonstige weiterführende Auskünfte benötigen, können Sie uns

unter einer der in dieser Sektion angegebenen Adressen erreichen.

# Unerwünschte Programme

Kostenverursachende Einwahlprogramme (Dialer)

Spiele (Games)

Witzprogramme (Jokes)

Mögliche schädliche Software (PMS)

Backdoor-Steuerprogramme (BDC)

## Kostenverursachende Einwahlprogramme (Dialer)

Bestimmte im Internet angebotene Dienstleistungen sind kostenpflichtig. Die Abrechnung erfolgt in Deutschland über Einwahlprogramme mit 0190-Nummern (in Österreich und der Schweiz über 09x0-Nummern; in Deutschland wird mittelfristig auf 09x0 umgestellt). Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Die Vermarktung von Online-Inhalten über den Weg der Telefonrechnung ist legal und kann für den Nutzer vorteilhaft sein. Seriöse Dialer lassen deshalb keinen Zweifel daran aufkommen, dass sie vom Kunden bewusst und mit Bedacht eingesetzt werden. Sie installieren sich nur dann auf dem Anwender-Rechner, wenn der Nutzer dazu seine Zustimmung abgibt, wobei diese Zustimmung aufgrund einer völlig eindeutigen und klar erkennbaren Etikettierung bzw. Aufforderung erfolgt sein muss. Der Verbindungsaufbau seriöser Dialer-Programme wird unmissverständlich angezeigt. Außerdem informieren seriöse Dialer exakt und augenfällig über die Höhe der dabei entstehenden Kosten.

Leider jedoch gibt es Dialer, die sich unauffällig, auf fragwürdige Weise oder gar in betrügerischer Absicht auf Rechnern installieren. Sie ersetzen die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine kostenverursachende, oft horrend überbeuerte 0190-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

Um sich generell vor unerwünschten kostenverursachenden Einwahlprogrammen (0190-Dialern) zu schützen, empfehlen wir Ihnen, sich direkt bei Ihrem Telefon-Anbieter für diesen Nummernkreis sperren zu lassen.

Wenn Sie im Konfigurationsmenü von AntiVir unter Unerwünschte Programme die Option "Kostenverursachende Einwahlprogramme (Dialer)" aktiviert haben, erhalten Sie eine entsprechende Warnung, wenn AntiVir fündig geworden ist. Sie haben nun die Möglichkeit, den unerwünschten 0190-Dialer einfach zu löschen.

## Spiele (Games)

Computerspiele müssen sein - aber sie gehören nicht unbedingt an den Arbeitsplatz (die Mittagspause vielleicht einmal ausgenommen). Dennoch wird von Mitarbeitern in Unternehmen und Behörden so manches Moorhuhn erlegt und so mancher Karobube doppelgeklickt. Über das Internet kann eine Fülle von Spielen heruntergeladen werden. Auch Email-Games erfreuen sich wachsender Verbreitung: Vom simplen Schach bis zum "Flottenmanöver" (inklusive Torpedogefecht) sind zahlreiche Varianten in Umlauf: Die jeweiligen Spielzüge werden über Mailprogramme an Partner gesendet und von diesen beantwortet.

Untersuchungen haben ergeben, dass die zum Computerspielen verwendete Arbeitszeit längst wirtschaftlich relevante Größenordnungen erreicht hat. Umso verständlicher ist, dass immer mehr

Unternehmen Möglichkeiten in Betracht ziehen, Computerspiele von Arbeitsplatzrechnern fern zu halten.

AntiVir ist in der Lage, durch die Erweiterung seiner Such- und Identifikationsroutinen Spiele zu erkennen und es als unerwünschtes Programm ggf. zu eliminieren. Wenn Sie im Konfigurationsmenü unter Unerwünschte Programme die Option "Spiele (Games)" aktiviert haben, erhalten Sie eine entsprechende Warnung, wenn AntiVir fündig geworden ist. Das Spiel ist nun im wahrsten Sinne des Wortes aus, denn Sie haben die Möglichkeit, es einfach zu löschen.

### **Witzprogramme (Jokes)**

Die Witzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren. Meist fängt der Computer nach dem Aufruf eines Witzprogramms irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für Witzprogramme sind die Waschmaschine im Diskettenlaufwerk (DRAIN.COM) und der Bildschirmfresser (BUGSRES.COM). Aber Vorsicht! Alle Symptome von Witzprogrammen könnten auch von einem Virus oder einem Trojaner stammen. Zumindest bekommt man aber einen gehörigen Schreck oder richtet in Panik hinterher sogar selbst tatsächlichen Schaden an.

AntiVir ist in der Lage, durch die Erweiterung seiner Such- und Identifikationsroutinen Witzprogramme zu erkennen und es als unerwünschtes Programm ggf. zu eliminieren. Wer im Konfigurationsmenü unter Unerwünschte Programme die Option "Witzprogramme (Jokes)" mit einem Häkchen aktiviert, wird über entsprechende Funde informiert.

### **Mögliche schädliche Software (PMS)**

PMS (possible malicious software) richtet normalerweise keinen Schaden auf Ihrem Rechner an. Sie wurde programmiert, um anderen Anwendern Schaden zuzufügen. Beispiel: Mailbomber - mit einem solchen Programm kann ein Opfer mit Tausenden von Emails attackiert werden.

AntiVir erkennt "Mögliche Schädliche Software". Wenn Sie im Konfigurationsmenü unter Unerwünschte Programme die Option "Mögliche schädliche Software (PMS)" aktiviert haben, erhalten Sie eine entsprechende Warnung, wenn AntiVir fündig geworden ist.

### **Backdoor-Steuerprogramme (BDC)**

Um Daten zu stehlen oder Rechner zu manipulieren, wird "durch die Hintertür" ein Backdoor-Server-Programm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor Steuersoftware (Client) von Dritten gesteuert werden.

AntiVir erkennt "Backdoor-Steuerprogramme". Wenn Sie im Konfigurationsmenü unter Unerwünschte Programme die Option "Backdoor-Steuerprogramme (BDC)" aktiviert haben, erhalten Sie eine entsprechende Warnung, wenn AntiVir fündig geworden ist.

# Virenbefall

Hier erhalten Sie eine kurze Einführung in die Aktionen, die Sie vornehmen sollten, wenn AVGuard/XP beispielsweise einen Virus gefunden hat. Bitte beachten Sie, dass die AntiVir Personal Edition keine Netzlaufwerke unterstützt und auch in der Funktionalität teilweise eingeschränkt ist. Sollten Sie Netzlaufwerk-Unterstützung oder eine erweiterte Funktionalität benötigen, bieten wir Ihnen als Lösung AntiVir 6 Professional an.

## Wenn AVGuard/XP einen Virus gefunden hat ...

### *1. Geraten Sie nicht in Panik und bewahren Sie Ruhe!*

AVGuard/XP hat bei richtiger Konfiguration alle wichtigen Aufgaben bereits automatisch für Sie erledigt. Haben Sie unbewusst versucht, eine infizierte Datei zu starten oder zu laden, wird diese ggf. automatisch repariert oder verschoben, der Zugriff darauf verweigert. Nach einer Reparatur können Sie wie gewohnt weiter arbeiten. Ist eine Reparatur der Datei nicht möglich, wird die infizierte Datei (im Normalfall) in ein Quarantäneverzeichnis verschoben, und Sie werden gewarnt.

### *2. Gehen Sie systematisch vor, übereilen Sie nichts!*

Es ist wichtig, dass Sie nun Ihren Arbeitsplatzrechner und alle möglicherweise infizierten Disketten auf Viren hin überprüfen. Am besten verwenden Sie hierzu unser AntiVir/XP, das zusammen mit diesem Paket installiert wurde. Reparieren Sie infizierte Dateien oder Bootsektoren. Bitten Sie ggf. Ihren Fachhändler oder uns um Unterstützung, falls Probleme auftauchen sollten. Eventuell sollten Sie die automatische Reparatur bei AVGuard/XP aktivieren. Sollte AntiVir den Virus nicht entfernen können, senden Sie uns bitte ein Exemplar zur Überprüfung zu. Wir werden Ihnen dann umgehend eine Lösung anbieten. Versuchen Sie festzustellen woher der Virus gekommen ist oder von wem die infizierte Datei stammt. Überprüfen Sie ggf. Ihr Antiviren-Konzept, um weiteren Infektionen vorzubeugen.

### *3. Informieren Sie Ihre Kollegen / Freunde*

Auch wenn es Ihnen unangenehm ist: Information ist wichtig! Speziell wenn der Virus von außen eingeschleppt worden ist. Informieren Sie deshalb unbedingt Ihre Kollegen / Freunde über die Infektion. Unterrichten Sie vor allem denjenigen, von dem Sie die infizierte Datei / Mail erhalten haben.

### *4. Unbekannte neue Viren und unerwünschte Dateien*

Bitte senden Sie für AntiVir unbekannte, neue Viren oder unerwünschte Dateien als verschlüsseltes Archiv im Anhang einer E-Mail an [virus@free-av.de](mailto:virus@free-av.de). Bitte vergessen Sie dabei nicht, das Passwort, und evtl. Angaben über die Datei oder das Problem in Ihrer Mail zu erwähnen.

