

# Optionen/Aktion nach Suche

(Nur AntiVir Professional)

{button ,AL('toAktion nach',0,'')} siehe auch

In diesem Dialogfenster können Sie den Namen und Kommandozeilenparameter von einem beliebigen Programm eingeben, das nach einem Fund von Viren bzw. unerwünschten Programmen von AntiVir automatisch gestartet werden soll.

## Programmname (Alt+P)

Geben Sie hier den vollständigen Namen des Programms ein, das nach einem Suchlauf gestartet werden soll (Laufwerk, Pfad, Dateiname und Extension). Dieses Programm wird nur gestartet, wenn mindestens ein Virus oder unerwünschtes Programm erkannt wurde. Mit Hilfe der Ordner-Schaltfläche können Sie auf gewohnte Weise durch die Verzeichnisse blättern und Ihren Zielordner und Programm auswählen.

## Argumente (Alt+A)

Geben Sie hier gegebenenfalls Kommandozeilenparameter des zu startenden Programms ein.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## **{button OK,}**

Die Einträge aus dem Fenster "Aktion nach Suche" werden übernommen und das Dialogfenster geschlossen.

## **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

## **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Aktuelles

## News von der H+BEDV Datentechnik GmbH und aktuelle Features von AntiVir

### Optionsfenster neu gestaltet

Hier heißt es Abschied nehmen von den Registerkarten: Im Anzeigefeld auf der linken Seite dieses Fensters führt Sie stattdessen ein Verzeichnisbaum durch die Optionen.

### Wussten Sie schon, dass ...

- ... neben AntiVir MailGate für Linux auch Versionen für FreeBSD und OpenBSD verfügbar sind und somit ein leistungsfähiger SMTP Scanner für diese Betriebssysteme bereit stehen? Neben der Suche nach Viren und anderen unerwünschten Programmen kann AVMailGate auch zum Content Filtering eingesetzt werden. Weitere Informationen erhalten Sie unter [www.antivir.de/produkte/email/lrx\\_mailgate.htm](http://www.antivir.de/produkte/email/lrx_mailgate.htm).
- ... die neue AntiVir-Suchengine über 60.000 Viren bzw. Virenstämme erkennen kann?
- ... AntiVir auch für Windows NT/2000 Server verfügbar ist?
- ... AntiVir-Anwender bereits 2 Stunden nach dem ersten Auftreten des Virus VBS.LoveLetter (ILOVEYOU) mit einer aktualisierten VDF versorgt waren?
- ... AntiVir für Linux, FreeBSD und OpenBSD für den privaten, nicht kommerziellen Gebrauch kostenfrei ist? Sie müssen sich lediglich registrieren lassen. Weitere Informationen hierzu finden Sie im Internet unter [www.antivir.de](http://www.antivir.de).
- ... es für AntiVir Linux eine grafische Benutzeroberfläche namens TkAntiVir gibt? Das Produkt unterliegt der GNU General Public Licence (GPL) und kann kostenfrei von der Homepage des Autors, Sebastian Geiges ([www.sebastian-geiges.de/tkantivir/index.htm](http://www.sebastian-geiges.de/tkantivir/index.htm)), downgeloadet werden.
- ... die H+BEDV Datentechnik GmbH den weltweit ersten residenten Virenwächter für Linux entwickelt hat? Der AVGuard wurde speziell für Server unter dem freien Betriebssystem Linux (z.B. mit Mars, Samba) entwickelt.
- ... wir mit dem Secure AntiVirus Application Programming Interface (SAVAPI) eine Programmierschnittstelle für unsere Antivirensoftware anbieten, mit der Sie sich Ihr eigenen individuellen Antivirenprogramme erstellen können? Speziell Email Gateways, Firewalls und spezielle Client-Server-Lösungen sind prädestiniert für den Einsatz von SAVAPI.
- ... in Zusammenarbeit mit der AVM Computersysteme GmbH ein leistungsfähiger Schutz vor Viren sowie anderen unerwünschten Programmen für den ISD- bzw. DSL-Router KEN! entwickelt wurde? Mit "AntiVir für AVM KEN!" brauchen sich Anwender keine Gedanken mehr über die Sicherheit ihrer Emails zu machen, denn alle ein- und ausgehenden Emails werden auf Befehl gecheckt. "AntiVir für AVM KEN!" kann online bestellt werden: <http://www.antivir.de/ken.htm>
- ... die H+BEDV Datentechnik GmbH ein spezielles Plug-in für den Mail Transport Agent Sendmail anbietet? "AntiVir Milter für Sendmail" ermöglicht es, Emails auf unerwünschte Inhalte - etwa Viren - zu durchleuchten, auszusondern und ggf. zurückzuweisen.

**Weitere Informationen und Neuheiten finden Sie im Internet unter <http://www.antivir.de>**

# Suchen/AntiVir beenden

{button ,AL(`rtoSuchen',0,'')} siehe auch

Beenden Sie AntiVir entweder unter dem Menüpunkt "Suchen" mit "AntiVir beenden", durch Anklicken des Regenschirm-Icons in der linken oberen Ecke und scrollen auf den Befehl "Schließen" oder mit der üblichen Tastenkombination "Schließen" (Alt+F4).

Ist der Menüpunkt Optionen/Einstellungen beim Beenden speichern aktiviert, werden bei Beenden des Programms automatisch alle Einstellungen in der Datei AVWIN.INI gesichert. Ist dieser Menüpunkt nicht aktiv und wurden Einstellungen geändert, fragt AntiVir beim Beenden nach, ob diese Änderungen gesichert werden sollen.

## Backup

Und jetzt zum Lieblingsthema des Hauses: Backups.

Vollständige Backups sind der Unterschied zwischen einem halben Tag Arbeit und einem Desaster. Dabei stellen das Betriebssystem und die Programme noch das geringere Übel dar, dies lässt sich alles wieder von den Originaldatenträgern aus installieren. Viel wichtiger sind die von Ihnen selbst erstellten Daten, für die es ohne Backup keine Rettung mehr gibt.

Vergessen Sie bitte nicht: **AntiVir kann "nur" Viren sowie die unter Optionen/Selektion Meldungen genannten Programme entfernen, nicht aber die von diesen Programmen angerichteten Schäden beheben.** Dafür sind Sie allein verantwortlich. Überlegen Sie sich einmal ganz ehrlich, wann Sie das letzte Backup gemacht haben und ob Sie jetzt nicht die Hände über dem Kopf zusammenschlagen würden, wenn die Festplatte just in diesem Moment ihren Geist aufgeben würde.

Daten **müssen** regelmäßig gesichert und der Ablauf der Backups **muss** auf Vollständigkeit überwacht werden. Ganz wichtige Daten, wie etwaige Datenbanken oder wichtige Texte, sollten zweimal gesichert werden, denn ohne Backups gibt es keinen Weg, unersetzliche Daten wiederherzustellen.

# Bekanntermaßen gute DOS-Diskette

Mit dieser "bekanntermaßen guten DOS-Diskette" können Sie im Notfall Ihren Rechner wieder aufbauen. Auf diese Diskette - es dürfen auch zwei sein - gehören alle Programme und Hilfsmittel, mit denen sich Ihr Rechnersystem wieder zum Laufen bringen lässt.

Die Bedingung für die Erstellung einer "bekanntermaßen guten DOS-Diskette" ist ein absolut virenfrees System. Hat sich nämlich zu diesem Zeitpunkt ein Virus eingeschlichen, ist eine Virusinfektion sehr schwer festzustellen, da man ja immer davon ausgeht, dass diese Diskette absolut virenfrei ist.

Erstellen Sie mit dem DOS-Befehl FORMAT zuerst einmal eine startfähige Betriebssystemdiskette. Den Parameter /u (= UNDELETE) gibt es erst ab DOS 5.0, die Systemdiskette enthält dann keine Informationen zur Wiederherstellung von Daten:

```
format a: /s /u
```

Nach dem Formatieren ist diese Diskette auch schon startfähig.

Erstellen Sie nun eine AUTOEXEC.BAT und eine CONFIG.SYS auf dieser Diskette, diese Dateien könnten beispielsweise so aussehen:

## **CONFIG.SYS:**

```
DEVICE=A:\HIMEM.SYS  
FILES=40  
BUFFERS=20  
STACKS=9,256  
SHELL=A:\COMMAND.COM /E:1024 /P
```

## **AUTOEXEC.BAT:**

```
KEYB GR
```

Wenn Sie für einen erfolgreichen Start noch andere Treiber benötigen, kopieren Sie diese Treiber bitte auch auf diese Diskette und ändern Sie die CONFIG.SYS, entsprechend ab. Es gibt Treiber für Festplattenlaufwerke (SSTOR.SYS, HARDDRIVE.SYS, DMDRV.BIN), Diskettenlaufwerke (IBM PS/2 - DASDRVS.SYS) oder Netzwerke, deren Aufruf-Parameter Sie bitte den Anleitungen der Hersteller entnehmen. Auch der Tastaturtreiber kann anders heißen.

**Bitte tragen Sie in diese CONFIG.SYS Datei keine Programme oder Treiber ein, die über eine Festplatte geladen werden,**

d. h. verwenden Sie kein "C:" oder ähnliches!

Die Treiber für Ihr CD-ROM-Laufwerk sollten in keinem Fall fehlen, meistens handelt es sich dabei um einen \*.SYS-Treiber des Herstellers für die CONFIG.SYS und die MSCDEX.EXE Ihrer DOS-Version für die AUTOEXEC.BAT.

Kopieren Sie sich anschließend noch einige wichtige Betriebssystemprogramme auf diese Diskette, beispielsweise:

```
FDISK.*  
COMP.*  
KEYB.*  
FORMAT.*  
LABEL.*  
HIMEM.*  
SYS.*  
DISKCOPY.*  
DEBUG.*
```

## XCOPY.\*

Auch hier können Sie noch weitere Programme hinzufügen, auf die Sie nicht verzichten möchten.

Danach übertragen Sie bitte die wichtigsten Utilities auf diese Diskette. Zu diesen wichtigen Utilities gehören unbedingt Ihr Backup-Programm, sein zugehöriges Restore-Pendant und - soweit vorhanden - die Norton Utilities. Wenn nicht genügend Platz auf der Diskette ist, können Sie diese Programme auf weiteren bekanntermaßen guten Hilfsmitteldisketten unterbringen.

Zum guten Schluss schieben Sie bitte den Schreibschutzschieber auf "schreibgeschützt" (durchsichtig bei einer 3½" Diskette) und bewahren Sie diese Diskette gut (aber nicht zu gut) auf.

## **BIOS**

Basic Input/Output System. Hierunter versteht man allgemein die im ROM vorhandenen Betriebssystemroutinen. Dies sind die Kernroutinen des Betriebssystems, welche auf die verwendeten Hardware-Bausteine abgestimmt werden. Das BIOS ist beispielsweise für den Speichertest, die Initialisierung der Schnittstellen und der Tastatur sowie für den Start des Betriebssystems von Diskette oder Festplatte zuständig.

## **Bootsektor**

ist der erste Sektor des Betriebssystems, der von einer Diskette bzw. von einer Festplatte geladen und ausgeführt wird. Der Programmcode dieses Sektors ist für das Laden des Betriebssystems verantwortlich.



# Suchen/Bootsektoren

{button ,AL(`rtoSuchen',0,'')} —siehe auch

Im Menü "Suchen" wird mit Hilfe des Menüpunktes "Bootsektoren" das Fenster "Bootsektortest" aufgerufen. Dort können Sie die Laufwerke auswählen, deren Bootsektor getestet werden soll. Die Bootsektoren der markierten Laufwerke werden nach Viren durchsucht, wenn Sie die Schaltfläche "Suchen" betätigen. Von den ausgewählten Festplatten werden zusätzlich die Master-Bootsektoren durchsucht.

**Folgende Schaltflächen sind im Dialogfenster "Bootsektortest" vorhanden:**

## {button Suchen,}

Diese Schaltfläche ist aktiv, wenn mindestens ein Laufwerk ausgewählt ist. Wird diese Schaltfläche betätigt, startet sofort eine Suche nach Bootsektorviren in den markierten Laufwerken.

## {button Schließen,}

Dieses Fenster wird geschlossen und die Einträge werden übernommen.

## {button Report,}

Wird diese Schaltfläche betätigt, können Sie die Reportdatei zu dem zuletzt aus diesem Fenster heraus gestarteten Suchlauf ansehen. Dieser Punkt wird erst nach dem Start eines Suchlaufs aktiv.

## {button Hilfe,}

Diese Hilfe wird angezeigt.

## Bootsektorvirus

Diese Art von Virus nistet sich im Bootsektor ein.

Bootsektorviren infizieren in der Regel nur Disketten, bei Festplatten wird normalerweise der Master-Bootsektor infiziert. Bootsektorviren werden durch Booten mit einer infizierten Diskette im Laufwerk A: oder Starten eines Droppers bzw. eines mit einem Multipartite-Virus infizierten Programms übertragen. Ist der Virus aktiv, wird bei einem `DIR A:-` oder `DIR B:-` Befehl jede eingelegte nicht schreibgeschützte Diskette infiziert!

Zumeist verschiebt der Virus den originalen Bootsektor in einen Sicherungsbereich, bevor er seinen eigenen Programmcode in den Bootsektor schreibt. Beim Start des Rechners wird dann zuerst der Code des Bootsektorvirus aktiviert, der dann den Programmcode des originalen Bootsektors nachlädt und ausführt.

Bootsektorviren fallen normalerweise durch Reduzierung des Hauptspeichers auf. Der Rechner besitzt dann angeblich nur noch 638 oder 639 KB DOS-Speicher anstelle von 640 KB (655.360 Bytes).

# Optionen/CRC

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

In dieser Registerkarte wird der Modus für die CRC-Berechnung festgelegt. Eingaben werden nur akzeptiert, wenn das Feld "Prüfsummen berechnen" aktiv ist.

Bei der CRC-Prüfung werden ausschließlich Dateien in die CRC-Datenbank aufgenommen, in denen keine Viren sowie keine unerwünschten Programme gefunden wurden! Hat AntiVir eine betroffene Datei entdeckt, die NICHT repariert wurde, wird für diese Datei auch keine CRC-Summe berechnet.

AntiVir legt auf jedem Laufwerk im Hauptverzeichnis eine CRC-Datenbank an (mit dem Dateinamen, den Sie unter "Datenbankname" eingegeben haben oder mit dem Namen, der von AntiVir automatisch gefunden wurde), wenn die CRC-Summe berechnet werden soll.

## Prüfsummen berechnen (Alt+B)

Mit dieser Option wird die Funktion "CRC berechnen" eingeschaltet. Dies setzt voraus, dass Sie einen Datenbanknamen für die CRC-Datei angegeben haben. Wurde diese Option mit (OK) bestätigt, ohne dass ein Datenbankname eingegeben wurde, weist AntiVir Sie darauf hin und zeigt erneut die CRC-Registerkarte an.

## Datenbankname (Alt+T)

Tragen Sie hier einen Dateinamen ein, unter dem die Daten der CRC-Berechnung gespeichert werden sollen. Für diese Datei wird kein Name vorgegeben, da beispielsweise ein Virus diese Datei manipulieren könnte, wenn deren Name bekannt ist. Eine CRC-Datei mit diesem Namen wird in jedem Laufwerk im Hauptverzeichnis abgelegt.

Das Datenbankformat ist kompatibel zu AntiVir für DOS. Sie können also mit der alten CRC-Datenbank weiterarbeiten.

Ist kein Datenbankname vorhanden, sucht AntiVir beim Programmstart auf allen vorhandenen Festplatten nach einer CRC-Datenbank. Wird eine gültige Datenbank gefunden - dazu gehören auch unter AntiVir für DOS erstellte Datenbanken - wird der Name dieser Datei als Datenbankname übernommen.

## Änderungen bestätigen (Alt+N)

In diesem Modus wird jede Änderung der CRC-Summe gemeldet.

Hierbei gibt es eine Ausnahme: ist in dem Dialogfenster Optionen/Reparatur das Feld "Nur in Reportdatei aufzeichnen" aktiviert, wird auch eine Änderung der CRC nur in der Reportdatei aufgezeichnet. Sollen Daten nur aufgezeichnet werden, erkennen Sie dies daran, dass das Feld "Änderungen bestätigen" deaktiviert ist.

## Prüfmodus

Es stehen Ihnen zwei Modi zur CRC-Berechnung zur Verfügung: Im "Schnellvergleich" (Alt+S) wird zur Berechnung der CRC-Summe nur ein Teil der zu prüfenden Datei verwendet. Ist "Ganze Datei vergleichen" (Alt+G) eingestellt, wird die CRC-Summe über die ganze Datei berechnet.

Der "Turbo Modus" reicht im allgemeinen aus; dieser Modus ist wesentlich schneller, als wenn eine CRC-Summe für eine ganze Datei berechnet werden muss. Wird ein neuer Eintrag in die CRC-Datenbank aufgenommen, spielt diese Einstellung allerdings keine Rolle, da hier beide CRC-Werte berechnet werden.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

**{button CRC-Dateien,}**

Ist das Feld "Prüfsummen berechnen" aktiv, lässt sich mit dieser Schaltfläche ein Fenster aufrufen, in dem festgelegt wird, welche Dateien bei der CRC-Berechnung berücksichtigt werden.

### {button OK.}

Das Dialogfenster wird geschlossen und die aktuellen Einträge werden übernommen. Ist "Prüfsummen berechnen" aktiv, muss ein Datenbankname eingegeben werden, sonst erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen Datenbanknamen einzugeben.

### {button Abbrechen.}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### {button Hilfe.}

Diese Hilfe wird angezeigt.

## CRC

(Nur AntiVir Professional)

CRC (engl. Cyclic Redundancy Check) ist eine Methode, Prüfsummen zu berechnen. Wird auf einem virenfreien Rechner eine solche Prüfsumme erstellt und in einer Datenbank gespeichert, ist AntiVir in der Lage, diesen Wert mit einer später erstellten Prüfsumme zu vergleichen. Sind ausführbare Dateien, die in der Regel nicht verändert werden, beispielsweise mit einem unbekanntem Virus infiziert, kann dieser durch das Vergleichen der Prüfsummen entdeckt werden.

Im Menü Optionen/CRC können Sie wählen, ob und auf welche Weise und für welche Dateien das CRC-Verfahren eingesetzt werden soll.

# Optionen/CRC/CRC-Dateien

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

In diesem Fenster werden die Einstellungen für die CRC-Dateien festgelegt.

Sie können wählen, ob Sie alle Dateien einer CRC-Prüfung unterziehen wollen oder ob nur Programmdateien untersucht werden sollen.

Haben Sie "Alle Dateien" (Alt+A) gewählt, wird es häufiger vorkommen, dass Ihnen AntiVir eine Änderung der CRC melden wird, da Sie ja laufend an Ihrem Rechner arbeiten und auch beispielsweise Ihre Textdateien ändern. Sie sollten bei jedem Hinweis auf eine veränderte CRC-Summe die CRC aktualisieren, falls kein Virenverdacht besteht.

Haben Sie "Programmdateien" (Alt+G) gewählt, schlägt Ihnen AntiVir eine Liste mit den gebräuchlichsten Endungen vor. Sie können diese Endungen natürlich auch wie weiter unten beschrieben selbst an Ihr Dateiensystem anpassen. Wird Ihnen in diesem Modus eine CRC-Änderung gemeldet, sollten Sie überlegen, ob Sie die entsprechende Datei geändert (z.B. durch ein Update, Ihre Entwicklungsumgebung, in der ausführbare Dateien oft neu kompiliert werden) haben. Ist dies nicht der Fall, vergleichen Sie die entsprechende Datei mit dem Original (auf Diskette oder CD). Stellen Sie hier einen Unterschied beispielsweise in der Länge einiger ausführbaren Dateien fest, könnte dies auf ein unerwünschtes Programm hindeuten.

In dem Fenster "CRC-Dateien" können Sie in der Anzeigegruppe "Auszulassende Dateien" Dateinamen angeben, die nicht mit der CRC-Berechnung geprüft werden sollen. Dies ist z.B. bei Dateien sinnvoll, die häufig geändert werden (beispielsweise im Entwicklungsbereich). Um eine Datei in diese Liste einzufügen, klicken Sie auf die Schaltfläche "Einfügen" oder "Durchsuchen", um eine Datei zu löschen, markieren Sie diese Datei und klicken Sie auf die Schaltfläche "Löschen".

Haben Sie hier einen Dateinamen mit komplettem Pfad eingegeben, wird genau diese Datei keiner CRC-Prüfung unterzogen; falls Sie einen Dateinamen ohne Pfad eingeben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht mit der CRC-Berechnung geprüft.

## Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:

{button Endungen,JI(','OPTIONEN\_SCANNER\_ENDUNG')}

Mit dieser Schaltfläche wird in der Anzeigegruppe "Dateien" ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei der CRC-Berechnung im Modus "Programmdateien" untersucht werden.

{button Einfügen,JI(','OPTIONEN\_CRC\_EINFUEGEN')}

Wird diese Schaltfläche betätigt, erscheint ein Dialogfenster, in dem Sie einen Dateinamen für die auszulassenden Dateien eingeben können.

Wird nur ein Dateiname angegeben, übergeht AntiVir *jede* Datei mit diesem Namen bei der CRC-Berechnung. Es spielt also keine Rolle, ob sich diese Datei auf dem Laufwerk C:, D: oder A: befindet. Soll die CRC nur für eine *bestimmte* Datei mit diesem Namen nicht berechnet werden, müssen Sie den kompletten Pfad eingeben.

{button Durchsuchen,}

Bei Aufruf dieser Funktion erscheint ein Dialogfenster, das Ihnen das Durchsuchen eines Datenträgers nach auszulassenden Dateien erleichtert. Verwenden Sie diese Schaltfläche, wenn Sie den Pfad oder den Dateinamen der auszulassenden Datei nicht genau wissen.

{button Löschen.}

Markierte Einträge werden aus der Liste auszulassender Dateien gelöscht. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

{button OK.}

Das Dialogfenster wird geschlossen und die aktuellen Einträge werden übernommen. Ist "Prüfsummen berechnen" aktiv, muss ein Datenbankname eingegeben werden, sonst erscheint eine Fehlermeldung, in der Sie aufgefordert werden, einen Datenbanknamen einzugeben.

{button Abbrechen.}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

{button Hilfe.}

Diese Hilfe wird angezeigt.

# Optionen/CRC/CRC-Dateien/Einfügen

(Nur AntiVir Professional)

{button ,AL('toAktion nach',0,'')} siehe auch

Wird im Fenster "CRC-Dateien" diese Schaltfläche betätigt, erscheint ein Dialogfenster, in dem Sie einen Dateinamen für die auszulassenden Dateien eingeben können.

Wird nur ein Dateiname angegeben, übergeht AntiVir *jede* Datei mit diesem Namen bei der CRC-Berechnung. Es spielt also keine Rolle, ob sich diese Datei auf dem Laufwerk C:, D: oder A: befindet. Soll die CRC nur für *eine bestimmte* Datei mit diesem Namen nicht berechnet werden, müssen Sie den vollständigen Pfad und Namen eingeben.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## **{button OK,}**

Die Einträge aus dem Fenster "Auszulassende Dateien eingeben" werden übernommen und das Dialogfenster geschlossen.

## **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

## **{button Hilfe,}**

Diese Hilfe wird angezeigt.



## **Dateiviren**

Befallene Dateien. Je nach eingestellter Option bietet AntiVir Ihnen an, die infizierte Datei wiederherzustellen.

Ist eine Datei nicht reparabel, schlägt AntiVir vor, diese Datei zu löschen. Prüfen Sie in diesem Fall bitte vorher, ob Sie ein Backup dieser Datei haben, sonst sind diese Daten nur noch von Spezialisten zu retten, wenn es überhaupt noch geht.

# Demo-Version

Wenn Sie AntiVir als Demo-Version (ohne eine gültige Lizenzdatei) installiert haben, ist das Programm auf folgende Funktionen begrenzt:

- \* AntiVir durchsucht ausschließlich den ersten Verzeichnisast.
- \* AntiVir repariert Dateien ausschließlich im Verzeichnis "AVTest", das vom Anwender im Verzeichnis von AntiVir selbst angelegt werden muss.
- \* AntiVir repariert **keine** Bootsektoren.
- \* Alle Netzwerkoptionen sind deaktiviert.

# Optionen/Diverses

{button ,AL('rtoAktion nach',0,'')} siehe auch

## Suchvorgang

### Stoppen zulassen (Alt+S)

Ist dieses Kontrollfeld markiert, lässt sich die Suche nach Viren oder unerwünschten Programmen jederzeit mit der Schaltfläche "Stop" beenden. Haben Sie diese Einstellung deaktiviert, wird die Schaltfläche "Stop" im Fenster Luke Filewalker grau unterlegt. Sie können die Suche nicht mehr vorzeitig beenden und müssen warten, bis AntiVir sein Werk vollendet hat.

## Temporärer Pfad

### Temporärer Pfad (Alt+T)

In diesem Eingabefeld tragen Sie den temporären Pfad ein, mit dem AntiVir arbeitet.

Dieser temporäre Pfad wird verwendet, um

- gepackte ausführbare Dateien zu entpacken und zu durchsuchen
- Reparaturen durchzuführen
- Archive zu entpacken.

Ist der Pfad für temporäre Dateien nicht mehr vorhanden oder beträgt der freie Platz auf diesem Laufwerk weniger als 1 MByte, werden Sie gefragt, welchen Pfad AntiVir verwenden soll.

Viele Programme (auch Microsoft Windows) verwenden die Umgebungsvariable "TEMP", um den Pfad für Auslagerungsdateien zu ermitteln. Dieser Pfad zeigt häufig auf eine Ramdisk oder ein anderes schnelles Medium, ist also wie geschaffen für AntiVir. Sie haben deshalb die Möglichkeit, die Umgebungsvariable "TEMP" oder "TMP" in Ihrer AUTOEXEC.BAT zu setzen (SET TMP=C:\RAMDISK).

Von AntiVir aus können Sie den Text %TEMP% als Platzhalter für die Umgebungsvariable angeben.

Ist in der Datei AVWIN.INI kein Eintrag vorhanden, sucht AntiVir zuerst nach der Umgebungsvariable "TEMP", anschließend nach "TMP". War in beiden Fällen kein Eintrag vorhanden, wird standardmäßig das Startverzeichnis von AntiVir verwendet.

## Folgende Kontrollfelder stehen noch in diesem Fenster zur Verfügung:

### Zu löschende Dateien überschreiben (Alt+Z)

Ist dieses Optionsfeld aktiv, werden die Daten einer zu löschenden Datei zuerst überschrieben und anschließend gelöscht.

Diese Einstellung sollte immer aktiv sein, da auf diese Weise ein Zurückholen der infizierten Datei (z.B. mit UNERASE) nicht mehr möglich ist.

### AntiVir beenden, wenn über Shell Erweiterung gestartet wurde (Alt+A)

Ist dieser Eintrag markiert, wird AntiVir nach einer Suche, bei der AntiVir über die Shell-Erweiterung gestartet wurde, wieder beendet. Soll AntiVir nach einer Suche nicht beendet werden, deaktivieren Sie diese Einstellung.

Diese Option ist nur wirksam, wenn AntiVir über die Shell-Erweiterung *gestartet* wird; ist AntiVir bereits aktiv und wird nur ein Suchlauf via Shell-Erweiterung gestartet, hat diese Option keine Wirkung.

### Keine Dateien und Pfade auf Netzlaufwerken untersuchen (Alt+W)

(Nur AntiVir Professional)

Ist dieser Punkt markiert, werden keine über ein Netzwerk erreichbaren Laufwerke untersucht. Dies macht Sinn, wenn der Server bzw. die anderen Workstations durch eine Antivirensoftware (vorzugsweise eine entsprechende AntiVir-Programmversion) geschützt werden.

### Guard beim Systemstart laden (Alt+G)

Ist dieser Punkt markiert, wird AVGuard automatisch beim Systemstart geladen. Um den automatischen Start zu unterbinden, deaktivieren Sie diesen Eintrag. Diese Option wirkt sich erst nach einem Neustart des Systems aus.

### Guard über das Kontrollprogramm starten (Alt+K)

(Nur AntiVir Professional für Win 9x, ME)

Ist dieser Punkt markiert, lässt sich AVGuard nur über das Kontrollprogramm aktivieren. AVGuard wird nicht mehr automatisch bei einem Programmstart aktiviert. Diese Option wirkt sich erst nach einem Neustart des Systems aus.

### Internet Updater (plugin) nutzen

(Nur AntiVir Professional)

Haben Sie diese Einstellung aktiviert, müssen Sie - nur dieses erste Mal! - AntiVir neu starten. Ist dies geschehen, findet sich der neue Menüpunkt: "Internet Updater" künftig in den "Optionen" unter "Konfigurationsmenü". In der Werkzeugleiste des AntiVir-Hauptmenü-Fensters ist jetzt das Schaltsymbol "Internet Updater" hinzugekommen.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

### **{button OK,}**

Die Einträge aus dem Fenster "Diverses" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

## **Download**

Dateien aus dem Internet oder von Mailboxen auf seinem Computer lokal speichern.

# Optionen/Drag&Drop

{button ,AL('rtoAktion nach',0,'')} siehe auch

Unter diesem Menüpunkt werden die Einstellungen für Drag&Drop festgelegt. Mit Drag&Drop können Sie Dateien und Verzeichnisse, die überprüft werden sollen, auf das Hauptfenster von AntiVir ziehen.

Wenn sie bestimmte Verzeichnisse oder Dateien häufiger durchsuchen lassen wollen, empfiehlt es sich, hierfür ein Profil anzulegen.

## Unterverzeichnisse durchsuchen (Alt+U)

Ist diese Funktion markiert, werden auch alle Unterverzeichnisse untersucht, wenn Sie einen oder mehrere Ordner vom Windows Explorer aus auf das Hauptfenster von AntiVir verschieben.

Ist diese Option nicht aktiv, werden die Ordner nur auf der Verzeichnisebene durchsucht, die per Drag&Drop auf das Hauptfenster von AntiVir gezogen wurde.

## **Dateien**

(Nur AntiVir Professional Edition)

### Alle Dateien (Alt+A)

Per Voreinstellung sucht AntiVir ausschließlich nach ausführbaren Dateien. Ist dieser Menüpunkt angewählt, werden bei der Suche sämtliche Dateien im entsprechenden Ordner berücksichtigt, die mit Drag&Drop auf das Hauptfenster von AntiVir gezogen wurden. Auch nicht ausführbare Dateien werden untersucht.

AntiVir benötigt mit dieser Einstellung mehr Zeit zur Suche nach Viren oder unerwünschten Programmen, da wesentlich mehr Dateien geprüft werden müssen. Ist "Alle Dateien" aktiv, lässt sich die Schaltfläche "Endungen" nicht betätigen.

### Dateien gemäß der Liste in Optionen/Suchen/Dateien/Endungen (Alt+O)

Mit Hilfe dieser Funktion werden nur die Dateien durchsucht, die Sie vorher im Menü Optionen/Suchen/Dateien/Endungen eingestellt haben.

### Programm- und Makrodateien (Alt+P)

Ist diese Funktion markiert, wird im entsprechenden Ordner ausschließlich nach Dateien mit vorgegebenen Endungen gesucht (z.B. \*.BIN, \*.COM, \*.EXE, usw.). Bei den vorgegebenen Endungen sind Standardwerte vorgegeben. Diese Einträge können Sie in dem Fenster ändern, das mit der Schaltfläche "Endungen" aufgerufen wird.

Ist dieser Punkt aktiviert und Sie haben aus der Liste mit Dateiendungen alle Einträge gelöscht, wird dies durch den Text "KEINE ENDUNGEN" unterhalb der Schaltfläche "Endungen" angezeigt.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

{button Endungen,JI('','OPTIONEN\_SCANNER\_ENDUNG')}

(Nur AntiVir Professional)

Ist die Funktion "Programmdateien" aktiviert, lässt sich dies Schaltfläche anwählen. Es erscheint das Dialogfenster Dateiendungen, in dem Sie die Dateiendungen derjenigen Dateien direkt eingeben können, die überprüft werden sollen.

**{button OK,}**

Die Einträge aus dem Fenster "Drag&Drop" werden übernommen und das Dialogfenster geschlossen.

**{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

**{button Hilfe,}**

Diese Hilfe wird angezeigt.

## Optionen/Einstellungen beim Beenden speichern

{button ,AL(`rtoAktion nach',0,'')} siehe auch

Ist dieser Menüpunkt im Menü "Optionen" aktiv (gekennzeichnet durch einen Haken am Anfang des Textes), werden alle Einstellungen von AntiVir beim Verlassen des Programms automatisch gespeichert. Werden Änderungen vorgenommen, wenn diese Funktion nicht aktiviert ist, wird vor Beenden von AntiVir nachgefragt, ob die Änderungen gespeichert werden sollen.



## Optionen/Einstellungen sichern

{button ,AL(`rtoAktion nach',0,'')} siehe auch

Wenn Sie diesen Menüpunkt im Menü "Optionen" anwählen, werden die aktuellen Einstellungen von AntiVir umgehend manuell in der Datei AVWIN.INI gespeichert.

# Tools/Erkennungsliste

{button ,AL('rtoTools',0,','')} siehe auch

Mit dieser Funktion werden die Namen der Viren und unerwünschten Programme aufgelistet, die AntiVir kennt. Eine komfortable Suchfunktion für die Namen ist integriert.

## Teilstring-Suche innerhalb der Namen (Alt+T)

Sie können hier eine zusammenhängende Buchstaben- oder Zeichenfolge auf der Tastatur eingeben, die Markierung springt auf die erste Stelle auf der Namensliste, an der diese Zeichenfolge - auch mitten in einem Namen - steht (Beispiel: "raxa" findet "Abraxas").

## Suche ab dem ersten Zeichen der Namen (Alt+E)

Sie können hier den Anfangsbuchstaben und die folgenden Zeichen auf der Tastatur eingeben, die Markierung blättert alphabetisch in der Namensliste (Beispiel: "Ra" findet "Rabbit").

## Suchen:

Geben Sie in diesem Feld den gesuchten Namen oder eine Zeichenfolge eines Namens ein. Ist der gesuchte Name bzw. die Zeichenfolge vorhanden, wird die Fundstelle in der Liste markiert.

Mit den Schaltflächen "Suche vorwärts" (Alt+V), "Suche zurück" (Alt+Z) und "Erste Fundstelle" (Alt+F) können Sie durch die Erkennungsliste navigieren, mit der Schaltfläche "Eingabe löschen" (Alt+L) entfernen Sie den Eintrag aus dem Textfeld "Suchen".

## Erkannte Programmnamen:

Unter diesem Titel befindet sich eine Liste mit Namen der Viren oder unerwünschten Programme, die AntiVir erkennen kann. Die meisten Einträge dieser Liste lassen sich auch mit AntiVir entfernen. Sie sind jeweils alphabetisch geordnet (zuerst Sonderzeichen und Zahlen, dann die Buchstaben). Benutzen Sie die Bildlaufleiste, um in der Liste weiter nach unten oder zurück nach oben zu gelangen.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

### {button Suche vorwärts,}

startet die Suche vorwärts in alphabetischer Reihenfolge.

### {button Suche zurück,}

startet die Suche rückwärts in alphabetischer Reihenfolge.

### {button Erste Fundstelle,}

springt in der Liste zum zuerst gefundenen Eintrag zurück.

### {button Eingabe löschen,}

entfernt den Eintrag aus dem Listenfeld "Suchen".

### {button Schließen,}

Die Erkennungsliste wird geschlossen.

### {button Hilfe,}

Diese Hilfe wird angezeigt.

# FAQ

[Wann soll ich nach einem Dialer suchen?](#)

[Wann soll ich nach Viren suchen?](#)

[Wie entferne ich Viren?](#)

[AntiVir kann den Form-Virus nicht von Festplatte entfernen](#)

[AntiVir kann irgendwelche Dateien nicht reparieren?](#)

[AntiVir kann irgendwelche Dateien nicht anlegen?](#)

[Im Netzbetrieb bekomme ich so viele Warnungen!](#)

[AntiVir findet in der Swap-Datei von Windows Viren?](#)

[Virus im Speicher, aber nicht nach einem Start von Diskette?](#)

[Virus im Speicher, auch nach einem Start von Diskette](#)

[AntiVir und Netzwerkkartentreiber?](#)

[Wie entferne ich residente Viren?](#)

[Erstellen einer Bootdiskette](#)

## Wann soll ich nach einem Dialer suchen?

Jeder, der im Internet surft, setzt sich der Gefahr aus, dass er sich unerwünschte Einwahlprogramme auf den Rechner lädt. Gewisse 0190-Dialer wissen sich geschickt zu tarnen und können sich sogar hinter Pop-ups, Textlinks oder Bildern verbergen. Beispielsweise wird vorgegaukelt, dem Anwender ein Sicherheitsprogramm oder ein nützliches Zusatz-Tool zur Verfügung zu stellen. Um den Download zu aktivieren, genügt ein Klick. Deshalb empfiehlt es sich, lieber einmal mehr als einmal zu wenig nach Dialern zu suchen.

## Wann soll ich nach Viren suchen?

Immer. Hier gilt folgende Analogie zum Auto: dort kennt man ja auch verschiedene Überwachungsmodi, den Ölwechsel, die Inspektion und den TÜV - vielleicht guckt man ab und zu auch nach seinen Blinkern und dem Licht. Der AntiVir Guard entspricht dabei den Kontrollinstrumenten auf dem Armaturenbrett: Sie fahren sicherlich nicht los, wenn dort eine Warnleuchte blinkt. Täglich ein Standard-Suchlauf über die Festplatte. Es werden auf der Festplatte ausführbare Programmdateien (.COM, .EXE etc.) im Turbo-Modus untersucht. Dies ist in etwa dem Ölwechsel gleichzusetzen. Die Inspektion im wöchentlichen Rhythmus könnte die Prüfung sein. Nun würden die ausführbaren Programmdateien komplett durchsucht werden. Der TÜV dann einmal im Monat. Hier wird AntiVir mit dem Parameter "Alle Dateien" aufgerufen, damit alle Dateien durchsucht werden. Ach ja, und dass Disketten immer auf Viren untersucht werden sollten, versteht sich von selbst. Und falls Sie immer den Licht- und Blinkertest vor dem Start machen, können Sie AntiVir mit dem Kommandozeilenparameter /B Ihren DOS-Ordner absuchen lassen.

## Wie entferne ich Viren?

Ganz einfach: mit AntiVir. Spaß beiseite, bitte booten Sie Ihr Rechnersystem immer vor einer möglichen Entseuchung von der berühmt-berüchtigten "bekanntermaßen guten DOS-Diskette". Anschließend installieren Sie AntiVir neu und lassen es über den in Frage kommenden Datenträger laufen. Handelt es sich um einen Bootsektorvirus oder Master-Bootsektorvirus, können Sie direkt mittels AntiVir reparieren (Ausnahme: Form auf Festplatte; bitte verwenden Sie hier das Kommando "SYS C:"). Handelt es sich um einen Dateivirus, dann lassen Sie bitte die ganze Festplatte durch AntiVir mit seinen Standardoptionen (nur Programmdateien) absuchen und reparieren. Wiederholen Sie jetzt den Vorgang im reinen Suchmodus (nicht reparieren) mit "Alle Dateien". Falls AntiVir jetzt noch auf Viren stößt, dann können dies Viren sein, müssen es aber nicht. AntiVir unterscheidet intern nur zwischen .EXE und Nicht-.EXE-Dateien. Overlays mit unüblichen Dateinamenserweiterungen können auch infiziert sein. Bitte prüfen Sie dies vor einer Reparatur. Der dritte Schritt ist zugleich auch der, bei dem Sie besonders gefordert sind. Lassen Sie AntiVir bitte im erweiterten Suchmodus (/FF) über den in Frage kommenden Datenträger laufen. In diesem Modus sind viele Sicherheitsabfragen abgeschaltet. Durch das Abschalten der Sicherheitsabfragen können

Fehlalarme auftreten (unwahrscheinlich, aber dennoch möglich). AntiVir sucht jetzt nach zerstörten Dateien und Mutationen. Besonders wichtig sind zerstörte Dateien. Viele Viren sind so schlampig programmiert, dass sie nicht in allen Fällen eine ordentliche Infektion zustande bringen. Mal wird nur ein Teil vom Virus hineinkopiert, mal werden nur die ersten 10 Byte verändert, mal überschreibt er wahllos Dateiteile mit sich selbst, mal ändert er nur den Programmeinsprung, vergisst aber, sich selber dranzukopieren, die Liste ist endlos. Ein weites Betätigungsfeld für AntiVir. Meldet AntiVir in diesem Modus etwas Besonderes, überprüfen Sie diese Dateien besonders genau und vergleichen Sie gemeldete Programmdateien mit den Originalen.

### **AntiVir kann den Form-Virus nicht von Festplatte entfernen**

Ja, von der Reparatur des Bootsektors (nicht Master-Bootsektors) einer Festplatte lässt AntiVir sicherheitshalber die Finger weg. Denn diesen Virus werden Sie auch mit eigenen Hausmitteln los. Starten Sie bitte von einer sauberen DOS-Diskette, die dasselbe Betriebssystem enthält, das auch auf Ihrer Festplatte installiert ist (sehr wichtig!). Auf dieser Diskette sollte sich auch die Datei SYS.COM oder SYS.EXE befinden. Nach dem Start von dieser Diskette geben Sie bitte den Befehl "SYS x:" ein, wobei "x" dem Laufwerksbuchstaben Ihrer Festplatte entspricht. Da dies vermutlich "C" sein dürfte, lautet der Befehl: "SYS C:". Der SYS-Befehl überträgt nun die beiden Systemdateien (IBMBIO.COM und IBMDOS.COM bzw. IO.SYS und MSDOS.SYS) auf die Festplatte und erstellt einen neuen Bootsektor (nicht Master-Bootsektor!). Durch diese Aktion wird der alte, infizierte Bootsektor überschrieben und der Käse ist gegessen.

### **AntiVir kann irgendwelche Dateien nicht reparieren?**

Dies hängt vermutlich auch mit der Einstellung "Pfad für temporäre Dateien" zusammen. AntiVir erstellt vor einer Reparatur eine Kopie der infizierten Datei und repariert diese - es wird niemals am Original repariert, denn bei Mehrfachinfektionen könnte es sich später herausstellen, dass die Datei doch nicht reparabel ist. Oder während der Reparatur würde der Strom während des Aktualisierens der FATs oder Directories ausfallen. Dann wäre unter Umständen gar nichts mehr da. Erst nach erfolgreicher Reparatur wird die reparierte, temporäre Kopie wieder zurückkopiert und die ehemals infizierte Datei überschrieben. Für diese temporäre Kopie wird derjenige Pfad hergenommen, auf den unter "Optionen/Diverses" verwiesen wird. Haben Sie Ihr Rechnersystem vor einer Reparatur von einer "bekanntermaßen guten DOS-Diskette" gestartet, dann verweist der "Pfad für temporäre Dateien" vermutlich auf "A:\". Ändern Sie die Pfadangabe auf einen vorhandenen, leeren Ordner (beispielsweise C:\TEMP), dann unterbleibt die Nachfrage.

### **AntiVir kann irgendwelche Dateien nicht anlegen?**

Dies hängt vermutlich mit den Archivdateien, .ZIP, .PAK oder .ARJ zusammen. AntiVir kann die in den Archivdateien enthaltenen Dateien nicht im Speicher entpacken. Entpackt wird also physikalisch in den Pfad, auf den unter "Optionen/Diverses" unter "temporärer Pfad" verwiesen wird. Falls dieser Pfad nicht existiert oder ungültig ist, bricht AntiVir das Entpacken für diese eine Datei ab. Bitte setzen Sie den temporären Pfad auf einen gültigen, am besten leeren Ordner. Achtung: diese Einstellung wird in der Datei AntiVir.INI abgespeichert.

### **Im Netzbetrieb bekomme ich so viele Warnungen!**

Das sind vermutlich die Dateien, auf die AntiVir nicht zugreifen darf, weil sie von der Netzwerk-Software selbst gesperrt wurden. AntiVir und beispielsweise auch ein Virus kommen nicht ohne weiteres an diese Dateien ran. Ein anderes Beispiel wären Druckerqueues.

### **AntiVir findet in der Swap-Datei von Windows Viren?**

In der Auslagerungsdatei von Windows können unter Umständen auch Viren entdeckt werden. Das Problem sind hier aber zumeist andere ausgelagerte Antiviren-Programme, deren unverschlüsselte Suchstrings nun in dieser Datei zu finden sind. Abhilfe: Swap-Datei auf temporär umstellen, fragliche Programme vor dem Scannen schließen, nach dem Lauf eines Defragmentierers (ggf. mit der Option Clear Free Clusters) die Swap-Datei neu erstellen.

## Virus im Speicher, aber nicht nach einem Start von Diskette?

Nach dem Start von Festplatte findet AntiVir einen Virus im Speicher, eine Überprüfung nach einem zweiten Start von einer "bekanntermaßen guten DOS-Diskette" bringt aber keinen Virenbefund. Bitte versuchen Sie, in diesem Fall durch schrittweises "REM"-en oder zeilenweises Abarbeiten der CONFIG.SYS bzw. AUTOEXEC.BAT dasjenige Programm herauszufinden, nach dessen Aufruf AVScan einen Virus im Speicher findet. Führt das zu keinem Ergebnis, sollte auch die WIN.INI überprüft werden. Sind Programme in der Autostart-Programmgruppe von Windows angemeldet, sollten auch diese kontrolliert werden. Meistens sind dies andere Antiviren-Programme oder residente Virenwächter. Manchmal hilft auch ein Optimieren bzw. Komprimieren der Festplatte. Anstelle des zeilenweisen Aus-"REM"-mens können ab DOS 6.0 wenigstens die Einträge aus der CONFIG.SYS schrittweise abgearbeitet werden. Hierzu muss beim Start des Rechnersystems die Taste F8 betätigt werden, wählen Sie dann den Modus "Einzelbestätigung" aus. DOS 6.20 erlaubt zusätzlich auch ein zeilenweises Abarbeiten der AUTOEXEC.BAT.

## Virus im Speicher, auch nach einem Start von Diskette

Sie haben von einer "bekanntermaßen guten DOS-Diskette" in Zusammenarbeit mit einer "bekanntermaßen guten Windows-Diskette" gestartet und erhalten trotzdem eine Meldung über einen Virus im Speicher. Lassen wir einmal die Möglichkeit außer Acht, dass diese Systemdisketten infiziert sein könnten. AntiVir kann im Speicher nur finden, was auch da ist, und wenn eine Signatur gefunden wird, dann ist sie auch vorhanden. Die entscheidende Frage ist, wie kommt sie in den Speicher. Nach einem sauberen Start von den Notfalldisketten geht man ja davon aus, dass kein Virus aktiv sein kann. Es ist auch kein Virus aktiv, nur der infizierte Master-Bootsektor der Festplatte wurde bereits von DOS in den Speicher (Buffers, SmartDrive) gelesen. DOS interpretiert die eingelesenen Daten nur, der Virus ist nicht aktiv. AntiVir macht hier aber keinen Unterschied, Signatur ist Signatur. Für die entscheidende Frage, wie der Master-Bootsektor der Festplatte in den Speicher kommt, gibt es zwei mögliche Erklärungen: Erstens: während des Startvorgangs wurde während des Abarbeitens der Dateien CONFIG.SYS bzw. AUTOEXEC.BAT auf "C:" zugegriffen. Dieser Zugriff kann ein DIR C: oder ein Laden eines Programms von der Festplatte gewesen sein. Überprüfen Sie bitte die Startdateien und vergewissern Sie sich, dass kein Zugriff auf C: stattfindet. Zweitens: Ihre Festplatte ist normalerweise gestackt, getroublespaced oder irgendwie anders komprimiert. Bitte betätigen Sie während des Startvorgangs Ihres Rechnersystems die linke Shift-Taste. Ein Laden der Kompressionstreiber unterbleibt dann ebenso wie ein Abarbeiten einer CONFIG.SYS bzw. AUTOEXEC.BAT.

## AntiVir und Netzwerkkartentreiber?

Einige Netzwerkkartentreiber rufen von sich aus im residenten Zustand öfters Mal den Interrupt 03 auf, was ein absolutes NO-NO ist. Vermutlich sind in diesen Treibern die Debugging-Routinen vergessen worden, was sie größer als unbedingt nötig macht und AntiVir außerdem zum Absturz bringt. Dies kann an dem hardware-nahen Treiber liegen. Von einem Kunden haben wir die Information erhalten, dass nach Auswechseln des eingesetzten DLLNDIS.EXE von der Developer CD von Novell mit dem der Retail-Version wieder alles in Ordnung war.

## Wie entferne ich residente Viren?

Um residente Viren von einer Diskette zu entfernen, lässt sich AVWin problemlos einsetzen. Um jedoch (Master-) Bootsekturviren von einer Festplatte zu entfernen, kommen Sie unter Windows nicht weiter. Sie haben aber folgende Möglichkeiten

1. Booten Sie von der bootfähigen AntiVir CD-ROM, wählen im Bootmanager "Das HBDOS InstantScan Betriebssystem starten" und dort den ersten Punkt "AVE32 - Alle Bootsektoren überprüfen/reparieren"
2. Reinigung mit dem Diskettensatz von AntiVir
3. Hausmittel "FDISK /MBR" (nicht bei allen Masterbootsekturviren geeignet)

Die ausführlichen Beschreibungen zu den beiden letztgenannten Möglichkeiten und wie man die "bekanntermaßen gute DOS-Diskette" erstellen kann, finden Sie in den Textdateien, die im beiliegenden ZIP-Archiv enthaltenen sind.

Tipp: Stellen Sie nach der Entfernung des Virus im BIOS die Bootreihenfolge von "A, C" auf "only C" bzw. "C, A" um. Das ist ein sehr guter und zudem kostenloser Schutz vor reinen Bootsektoviren.

## Erstellen einer Bootdiskette

Mit der "bekanntermaßen guten DOS-Diskette" können Sie im Notfall Ihren Rechner wieder aufbauen. Auf diese Diskette - es dürfen auch zwei sein - gehören alle Programme und Hilfsmittel, mit denen Ihr Computersystem wieder zum Laufen gebracht werden kann.

Die Bedingung für das Erstellen einer "bekanntermaßen guten DOS-Diskette" ist ein absolut VIRENFREIES System. Hat sich nämlich ein Virus eingeschlichen, ist dies sehr schwer festzustellen, da man ja später immer davon ausgeht, dass diese Diskette absolut virenfrei ist.

Erstellen Sie sich mit dem DOS-Befehl FORMAT zuerst eine startfähige Betriebssystemdiskette. Den Parameter /U (= UNFORMAT) gibt es ab DOS 5.0, die Systemdiskette enthält dann keine Informationen zur Wiederherstellung der Systemdaten (die Unformat-Informationen können einen infizierten Bootsektor enthalten):

```
format a: /s /u
```

Nach dem Formatieren ist diese Diskette auch schon startfähig. Erstellen Sie nun eine AUTOEXEC.BAT und eine CONFIG.SYS auf dieser Diskette.

CONFIG.SYS:

```
DEVICE=A:\HIMEM.SYS
FILES=40
BUFFERS=20
STACKS=9,256
SHELL=A:\COMMAND.COM /E:1024 /P
```

AUTOEXEC.BAT:

```
KEYB GR
```

Wenn Sie für einen erfolgreichen Start noch andere Treiber benötigen, kopieren Sie sich diese Treiber bitte auch auf diese Diskette und ändern Sie die CONFIG.SYS entsprechend ab. Es gibt Treiber für Festplattenlaufwerke (SSTOR.SYS, HARDRIVE.SYS, DMDRV.BIN), Diskettenlaufwerke (IBM PS/2 - DASDRVS.SYS), komprimierte Laufwerke (DRIVESPACE, DBLSPACE, STACKER) oder Netzwerke, deren Aufrufparameter Sie bitte den Anleitungen der Hersteller entnehmen. Auch der Tastaturtreiber kann anders als der Standardtreiber heißen.

Bitte tragen Sie in diese Datei CONFIG.SYS keine Programme oder Treiber ein, die über eine Festplatte geladen werden, d.h. verwenden Sie kein "C:" oder ähnliches! Kopieren Sie sich anschließend noch einige wichtige Betriebssystemprogramme und Treiber auf diese Diskette. z.B.:

```
FDISK.*   COMP.*   KEYB.*   FORMAT.*
LABEL.*   HIMEM.*  SYS.*    DISKCOPY.*
MSCDEX.*  DEBUG.*  XCOPY.*
```

Sie können selbstverständlich weitere Programme hinzufügen, auf die Sie nicht verzichten möchten.

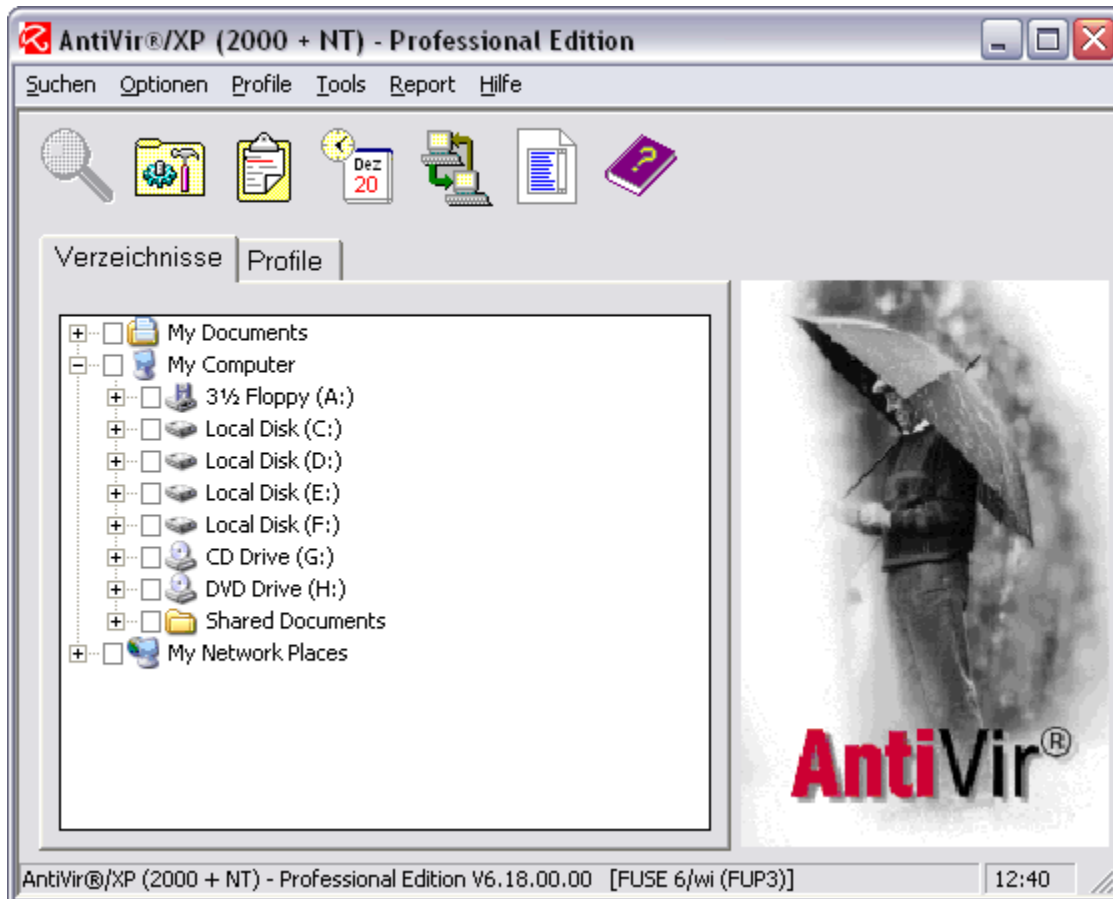
Danach übertragen Sie bitte die wichtigsten Utilities auf diese Diskette. Zu diesen wichtigen Tools

gehören unbedingt Ihr Backup-Programm, sein zugehöriges Restore-Pendant und die Norton Utilities oder ähnliches. Ist nicht genügend Platz auf einer Diskette, bringen Sie diese Programme auf weiteren bekanntermaßen guten Hilfsmittel-Disketten unter. Zum guten Schluss schieben Sie bitte noch den Schreibschutzschieber auf "schreibgeschützt" und bewahren Sie diese Diskette gut auf.



# Hauptfenster

Hier sehen Sie das Hauptfenster von AntiVir für Windows (Professional Edition). Unter Windows XP (XP&2000&NT) sieht die Programmoberfläche bis auf die Titelzeile und die Statuszeile identisch aus:



## Registerkarte "Verzeichnisse"

(Nur AntiVir Professional Edition)

In der Registerkarte "Verzeichnisse" des Hauptfensters können einzelne Laufwerke und Ordner ausgewählt werden, die gescannt werden sollen.

Im Auswahlfeld dieser Registerkarte werden Laufwerke und Verzeichnisse markiert. Die Darstellung und Handhabung in dieser Liste entspricht der des Windows-Explorers:

- Um Verzeichnisse zu wechseln, doppelklicken Sie auf das gewünschte Verzeichnis.
- Um Laufwerke zu wechseln, doppelklicken Sie auf den gewünschten Laufwerksbuchstaben.
- Zum Auswählen von Ordnern und Laufwerken können Sie auch auf das Zeichen + oder - vor einem Ordner- bzw. Laufwerkssymbol klicken.
- Mit Hilfe der Bildlaufleiste und den Bildlaufpfeilen können Sie durch die Menüstruktur navigieren.

Die Suche mit den entsprechenden Einstellungen wird mit der Schaltfläche "Suchen" in der Symbolleiste oder der Funktionstaste "F2" gestartet.

Ausgewählte Laufwerke sind durch einen Haken im Kästchen vor dem Namen gekennzeichnet.

**Hinweis:** Die gewählte Auswahl wird, je nach Option, beim Verlassen von AntiVir gespeichert.

### **Registerkarte "Profile"**

(Nur AntiVir Professional Edition)

Mit Hilfe dieser Registerkarte können Sie Dateien, Ordner und Laufwerke zu Profilen zusammenfassen und diese in einer Liste abspeichern. Diese Profile lassen sich dann zu einer gezielten Suche nach Viren und unerwünschten Programmen einsetzen, es müssen ja nicht immer alle Laufwerke durchsucht werden. Weitere Informationen zur Registerkarte "Profile" finden Sie [hier](#).

# Hilfe (Inhalt)

{button ,AL(`rtoHilfe',0,`,`')} siehe auch

## Im Menü "Hilfe" stehen Ihnen folgende Menüpunkte zur Verfügung:

### **Read Me (Alt+R)**

Mit dieser Funktion wird die aktuelle Read Me Datei angezeigt. Hier finden Sie wichtige Informationen über jede neue Version von AntiVir. Sollten Sie also einmal Probleme oder Fragen zu AntiVir haben, lesen Sie bitte in dieser Datei nach. In den allermeisten Fällen finden Sie hier eine Lösung für Ihr Problem.

### **Inhalt (F1)**

Mit "Inhalt" oder der Schaltfläche "Hilfe" können Sie sich das Inhaltsverzeichnis der Hilfedatei anzeigen lassen. Die Hilfefunktion von AntiVir entspricht der üblichen Handhabung der Windows-Hilfe.

### **Hilfe verwenden (Alt+H)**

Hier wird eine Übersicht angezeigt, wie Sie die Hilfefunktionen von Windows einsetzen können. Sie erhalten Informationen zu den einzelnen Stichworten, wenn Sie auf die entsprechenden Einträge doppelklicken.

### **Info ... (Alt+N)**

Durch diesen Menüpunkt gelangen Sie in ein Fenster, das Ihnen Informationen zur Versionsnummer des Guard, der Engine (AVE) und der Virendefinitionsdatei (VDF) anzeigt. Dort werden zusätzlich noch Copyright-Informationen und die Serviceadressen von der H+BEDV Datentechnik GmbH aufgeführt.

# Hilfe/Info

{button ,AL('rtoHilfe',0,'')} siehe auch

Im Fenster "Produktinformationen" werden Ihnen Informationen zur Versionsnummer des Hauptprogramms, der Engine (AVE) und der Virendefinitionsdatei (VDF) angezeigt. Zusätzlich sind noch Copyright-Informationen und die Serviceadressen von der H+BEDV Datentechnik GmbH aufgeführt.

## Hotline / Weitere Produktinformationen

Falls Sie technischen Support, Produktinformationen oder sonstige Auskünfte benötigen, können Sie uns unter einer der in dieser Sektion angegebenen Adressen erreichen:

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

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

## Für die Benutzer der AntiVir Personal Edition

**Technische Anfragen per Telefon/Fax/Brief oder via E-Mail können 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.

# Inhalt

Die folgenden Seiten sind aktuell verfügbar:

[Aktion nach Suche](#)  
[Aktuelles](#)  
[AntiVir beenden](#)  
[Backup](#)  
[Bekanntermaßen gute DOS-Diskette](#)  
[BIOS](#)  
[Bootsektor](#)  
[Bootsektoren](#)  
[Bootsektorvirus](#)  
[CRC](#)  
[CRC Definition](#)  
[CRC/CRC-Dateien](#)  
[CRC/CRC-Dateien/Einfügen](#)  
[Dateivirus](#)  
[Demo Version](#)  
[Dialer gefunden](#)  
[Diverses](#)  
[Download](#)  
[Drag&Drop](#)  
[Einstellungen beim Beenden speichern](#)  
[Einstellungen sichern](#)  
[Endungen](#)  
[Endungen/Einfügen](#)  
[Erkennungsliste](#)  
[FAQ](#)  
[Hauptfenster](#)  
[Hilfe \(Inhalt\)](#)  
[Info...](#)  
[Internet Updater](#)  
[Intranet Update](#)  
[Kennwort](#)  
[Kommandozeile](#)  
[Kurzreport anzeigen](#)  
[Kurzreport löschen](#)  
[Laufwerksliste aktualisieren](#)  
[Lizenzdatei](#)  
[Lizenzdatei laden](#)  
[Luke Filewalker](#)  
[Makroviren](#)  
[Makroviren/Auszulassende Makros](#)  
[Makroviren/Auszulassende Makros/Einfügen](#)  
[Masterbootsektor](#)  
[Masterbootsektorvirus](#)  
[Mehrfachlizenz](#)  
[Netzwerkwarnungen](#)  
[Netzwerkwarnungen \(XP\)](#)  
[Optionen \(Inhalt\)](#)  
[Partitionstabelle ändern](#)  
[Profile](#)  
[Profile \(Inhalt\)](#)  
[Read Me](#)

[Registerkarte Profile](#)  
[Reparatur](#)  
[Report](#)  
[Report \(Inhalt\)](#)  
[Report anzeigen](#)  
[Report drucken](#)  
[Report löschen](#)  
[Report/Kurzreport](#)  
[Report/Warnungen](#)  
[Schaltfläche Erkennungsliste](#)  
[Schaltfläche Hilfe](#)  
[Schaltfläche Internet Updater](#)  
[Schaltfläche Optionen](#)  
[Schaltfläche Report](#)  
[Schaltfläche Scheduler](#)  
[Schaltfläche Suchen](#)  
[Scheduler](#)  
[Spiel \(Game\) gefunden](#)  
[Status](#)  
[Suche starten](#)  
[Suchen](#)  
[Suchen \(Inhalt\)](#)  
[Suchen/Archive](#)  
[Suchen/Auszulassende Dateien](#)  
[Suchen/Bootsektoren](#)  
[Systemdateien sichern](#)  
[Tastaturbefehle](#)  
[Tools \(Inhalt\)](#)  
[Unerwünschte Programme](#)  
[Unerwünschte Programme \(Auswahl\)](#)  
[UpdateWizard](#)  
[Verdächtiges Makro gefunden](#)  
[Viren sowie sonstige Malware](#)  
[Vireninfo](#)  
[Virus gefunden](#)  
[Wichtige Hinweise](#)

# Optionen/Internet Updater

{button ,AL('rtoAktion nach',0,'')} siehe auch

Der **Internet Updater** sorgt dafür, dass Ihr AntiVir-Programm stets auf dem neuesten Niveau arbeitet. Sie können mit Hilfe des [Schedulers](#) einstellen, ob und in welchen Abständen sich AntiVir ins Internet einwählen und einen Versionsabgleich durchführen soll. Sie können einen Zeitpunkt bzw. einen bestimmten Turnus definieren. Es ist aber auch jederzeit möglich, den Internet Updater manuell zu starten. Steht eine aktualisierte Version oder eine neue Virendefinitionsdatei von AntiVir zur Verfügung, wird automatisch ein Update-Vorgang durchgeführt.

**Hinweis:** Die Funktion des Internet Updaters steht Ihnen mit der AntiVir-**Einzellizenz** immer zur Verfügung. Sollten Sie Nutzer einer **Mehrfachlizenz** (ab drei User) sein, ist eine entsprechende Konfiguration des Internet Updaters erforderlich.

## Internet Updater installieren

Rufen Sie im AntiVir-Menü-Fenster unter "Optionen" den Punkt "Konfigurationsmenü" auf. Dort finden Sie den Menüpunkt [Optionen/Diverses](#). Wenn Sie ihn anklicken, zeigt Ihnen das Dialogfenster u. a. den Punkt "Internet Updater (plugin) nutzen".

### [Internet Updater \(plugin\) nutzen](#)

Haben Sie diese Einstellung aktiviert, müssen Sie - nur dieses erste Mal! - AntiVir neu starten. Ist dies geschehen, findet sich der neue Menüpunkt "Internet Updater" künftig in den "Optionen" unter "Konfigurationsmenü". In der Werkzeuggestreife des AntiVir-Hauptmenü-Fensters ist jetzt das Schaltsymbol "Internet Updater" hinzugekommen.

Wenn Sie im AntiVir-Hauptfenster diese Schaltfläche betätigen, wird der Internet Updater aufgerufen. Mit Hilfe des Internet Updaters können Sie jederzeit automatisch oder manuell Ihre AntiVir-Version bzw. Ihre Virendefinitionsdatei aktualisieren.

## Internetverbindung und Proxyserver

Dieses Dialogfenster enthält Informationen über die Art und Weise Ihrer Internetverbindung.

### [Netzwerk- oder Modem-Verbindungsaufbau durch Windows \(Alt+N\)](#)

Diese Einstellung wird angezeigt, wenn Ihre Verbindung zum Internet über ein Modem erfolgt. Im Info-Fenster wird darüber informiert, dass keine DFÜ-Verbindungen gefunden wurden.

### [Das Internet-Update-Programm wählt die Standardverbindung \(Alt+D\)](#)

Diese Einstellung wird angezeigt, wenn Ihre Verbindung zum Internet über einen jeweils konfigurierten Standard erfolgt.

### [Das Internet-Update Programm wählt die folgende Verbindung \(Alt+F\)](#)

Diese Einstellung wird angezeigt, wenn Sie Ihre Verbindung zum Internet individuell definieren.

### [Verbindung über einen Proxyserver Alt+X\)](#)

Wenn Ihre Verbindung zum Internet über einen Proxyserver erfolgt, können Sie hier den entsprechenden Adress-Pfad sowie den jeweiligen Anschluss eintragen.

### [Einstellungen für die Internetverbindung und den Proxyserver testen \(Alt+T\)](#)

Mit dieser Funktion können Sie prüfen, ob sich die Internetverbindung zum Updateserver erfolgreich aufgebaut hat und ob die Versionsinformationen fehlerfrei vom Server übertragen werden. Ist dies

der Fall, zeigt Ihnen ein Dialogfenster, dass Sie die momentanen Einstellungen für das Internet Update verwenden können.

#### Automatische Internet Update Downloads zulassen (Alt+U)

Haben Sie diese Funktion aktiviert, können sie unter {button Einstellungen,} zwei verschiedene Optionen aktivieren:

### **Einstellungen für automatische Internet Updates**

Wenn Sie die Option "Automatische Internet Update Downloads zulassen" aktivieren, haben Sie die Möglichkeit, über die bei {button Einstellungen,} hinterlegte Dialogbox weitere Konfigurationen vornehmen: Sie können "Eine Verknüpfung mit der Installationsdatei auf dem Desktop erzeugen" und/oder "Eine für das Internet Update geöffnete DFÜ-Verbindung wieder beenden". Des Weiteren ist es jetzt auch möglich, ein völlig automatisches Update (beispielsweise als Eintrag im Scheduler) durchzuführen.

#### Eine Verknüpfung mit der Installationsdatei auf dem Desktop erzeugen (Alt+D)

Haben Sie diese Funktion aktiviert, können Sie sich ein erfolgreich durchgeführtes Komplett-Update auf dem Desktop anzeigen lassen.

#### Eine für das Internet geöffnete DFÜ-Verbindung wieder beenden (Alt+B)

Haben Sie diese Funktion aktiviert, wird die für das Internet Update geöffnete DFÜ-Verbindung automatisch wieder unterbrochen, sobald der Download erfolgt ist.

### **Folgende weitere Schaltflächen sind in diesem Dialogfenster vorhanden:**

#### **{button OK,}**

Die Einträge aus dem Fenster "Internet Updater" werden übernommen und das Dialogfenster geschlossen.

#### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

#### **{button Hilfe,}**

Diese Hilfe wird angezeigt.



# Optionen/Intranet Update

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

In diesem Fenster können Sie einstellen, ob und in welchen Abständen AntiVir über das Intranet aktualisiert werden soll.

AntiVir startet zu diesem Zweck den Update Wizard. Dieser prüft den Pfad, in dem sich die aktuellen Programmdateien zentral auf dem Server befinden und kopiert - soweit vorhanden - neue Quelldateien in das AntiVir-Zielverzeichnis auf Ihrer Workstation.

Diese Funktion steht Ihnen nur bei einer AntiVir-Mehrfachlizenz (ab 3 Usern) zur Verfügung.

## Intranet Update

### Kein automatisches Update durchführen (Alt+K)

Ist diese Funktion angewählt, führt AntiVir kein automatisches Update durch.

### Suche nach neuen Dateien jeden 'xxx' Tag (Alt+S)

Soll AntiVir nur jeden x-ten Tag nach neuen Dateien suchen, wählen Sie diesen Eintrag und geben Sie in dem Eingabefeld ein, nach wie viel Tagen AntiVir nach neuen Dateien suchen soll.

### Suche nach neuen Dateien jeden 'Wochentag' (Alt+N)

Soll AntiVir nur an einem bestimmten Wochentag nach neuen Dateien suchen, wählen Sie dieses Optionsfeld aus und geben sie im Listenfeld den gewünschten Wochentag an.

### Suche nach neuen Dateien bei jedem Systemstart (Alt+J)

Soll AntiVir bei jedem Systemstart nach neuen Dateien suchen, wählen Sie dieses Optionsfeld aus.

### Pfad, in dem sich Quelldateien befinden (Alt+P)

Geben Sie hier den Pfad ein, in dem sich die aktuellen Dateien von AntiVir auf dem Server befinden. Wurde die Datenstruktur beim Übertragen der aktuellen Dateien auf den Server übernommen, befinden sich die aktuellen AntiVir-Dateien im Ordner Disk\_1.

Dieser Quellpfad könnte beispielsweise so aussehen: \\SERVERNAME\VOLUME\UPDATES\AVWIN9x\DISK\_1

Hinweis: Bleibt die Verzeichnisstruktur der AntiVir-Quelldateien unverändert, werden auch die parallel liegenden Ordner, wie Disk\_2, Disk\_3, Admin usw. durchsucht. Für ein erfolgreiches Intranet Update muss der Update-Pfad Disk\_1 unbedingt korrekt angegeben sein.

### Pfad, in der sich die Lizenzdatei befindet (Alt+L)

Hier können Sie den Pfad auf ein Verzeichnis auf dem Server angeben, über den Sie neue Lizenzdateien verteilen können.

Findet beispielsweise der Update-Wizard im angegebenen Verzeichnis eine neue Lizenzdatei (internes Erstellungsdatum), wird diese vor Durchführen eines Updates automatisch installiert und für den weiteren Update-Vorgang verwendet.

### Kopierdialog des Updateprogramms verstecken (Alt+U)

Wird der Update Wizard von AntiVir aus gestartet, beginnt dieser sofort mit der Prüfung der Quelldateien. Möchten Sie, dass der Anwender nichts vom Aktualisieren von AntiVir mitbekommt, wählen Sie diese Einstellung.

## Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:

### **{button Konfigurationshinweise,}**

Ausführliche Informationen zur Installation des Intranet Update Wizards finden Sie in der Datei ADMIN.HTM, die mit Hilfe dieser Schaltfläche aufgerufen wird. Diese Datei befindet sich auch auf der AntiVir CD-ROM im Verzeichnis: [\[sprache\]\PRODUCTS\WIN9X\SETUP\DISK\\_1\\_bzw.\\_\[sprache\]\PRODUCTS\WINNT\SETUP\DISK\\_1.](#)

### **{button OK,}**

Die Einträge aus dem Fenster "Intranet Update" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Optionen/Kennwort

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

Sie können den Zugriff auf die Optionen von AntiVir durch ein Kennwort schützen. Wurde ein Kennwort eingegeben, werden Sie jedes Mal nach diesem Kennwort gefragt, wenn Sie das Dialogfenster "Optionen" öffnen möchten.

## Bitte geben Sie Ihr Kennwort ein (Alt+B)

Geben Sie hier Ihr gewünschtes Kennwort ein.

**Wichtig:** Groß- und Kleinschreibung wird unterschieden!

## Bitte bestätigen Sie Ihr Kennwort (Alt+I)

Geben Sie Ihr Kennwort im zweiten Eingabefeld zur Bestätigung erneut ein.

Sobald das Menü Optionen beim nächsten Aufruf von AntiVir angewählt wird, erscheint ein Dialogfenster, in das Sie das Kennwort eintragen müssen.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

### **{button OK,}**

Die Einträge aus dem Fenster "Kennwort" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Kommandozeile

AntiVir stellt Ihnen mehrere Kommandozeilenparameter zur Verfügung, die in bestimmten Situationen sowohl bei der Anpassung an Ihre Rechnerumgebung als auch bei Problemen mit besonders hartnäckigen Viren und unerwünschten Programmen nützlich für Sie sein können.

Diese Parameter können Sie ändern, indem Sie auf dem Desktop das Icon von AntiVir markieren. Drücken Sie nun die rechte Maustaste und wählen im Kontextmenü den Eintrag "Eigenschaften". Wählen Sie nun die Registerkarte "Verknüpfung" aus und geben Sie im Feld "Ziel" nach dem Programmnamen die gewünschten Parameter ein.

Alternativ hierzu können Sie AntiVir zusammen mit den gewünschten Kommandozeilenparameter auch aus einer DOS-Box heraus starten: Wechseln Sie in das Installationsverzeichnis von AntiVir und geben dort einfach den Programmnamen mit Parametern ANTIVIR /<PARAMETER> ein.

## Beschreibung der Kommandozeilenparameter

### /AF

Alle Diskettenlaufwerke werden in der Laufwerksliste markiert. Die Einstellungen für die Laufwerke der Datei AVWIN.INI werden ignoriert.

### /AH

Alle Festplatten werden in der Laufwerksliste markiert. Die Einstellungen für die Laufwerke der Datei AVWIN.INI werden ignoriert.

### /AN

Alle Netzlaufwerke in der Laufwerksliste werden markiert. Die Einstellungen für die Laufwerke der Datei AVWIN.INI werden ignoriert.

### /B

Der automatische Batchmodus wird nur beendet, wenn im Speicher Viren bzw. unerwünschter Programmcode gefunden wurden oder wenn ein Bootsektor oder Master-Bootsektor infiziert ist. Dieser Modus arbeitet ansonsten genau so, als ob die unter Optionen/Reparatur die Funktion "Nur in Reportdatei aufzeichnen" gewählt haben. Sie sollten allerdings immer einen Namen für die Reportdatei angeben.

### /BASK

Automatischer Batchmodus, bei dem die Einstellungen von AntiVir beachtet werden. Haben Sie hier eingestellt, dass beispielsweise alle gefundenen infizierten Dateien automatisch repariert werden, wird dies in diesem Modus auch gemacht.

Wenn Sie diesen Parameter zusammen mit dem Parameter /B angeben, wird der Parameter /B ignoriert.

### /BASK+

Dieser Parameter ist identisch mit /BASK, bis auf den kleinen Unterschied, dass am Ende eines Suchlaufs die Statistik dieses Suchlaufs angezeigt wird.

### /CLA

Die Reportdatei wird nach jedem Schreibzugriff geschlossen.

Dieser Parameter dient ausschließlich Supportzwecken; Sie sollten diesen Parameter nur nach Aufforderung durch die H+BEDV Datentechnik GmbH verwenden, da durch das permanente Öffnen

und Schließen der Reportdatei die Performance sinkt.

#### /DY

Dieser Parameter ist nur im Batchmodus wirksam. Einer der folgenden Parameter muss zusätzlich gesetzt sein: /B, /BASK oder /BASK+. Sofern keine Viren bzw. unerwünschter Programmcode gefunden wurden und die Suche normal beendet wurde (also der Suchlauf nicht abgebrochen wurde), speichert AntiVir das momentane Datum in einer Datum-Log-Datei (AVWIN95.DLG). Wird AntiVir am gleichen Tag wiederholt mit den selben Parametern gestartet, wird nur der Selbsttest durchgeführt. Am folgenden Tag wird in jedem Fall beim ersten Aufruf von AntiVir wieder gemäß aller angegebenen Parameter gesucht.

#### /DYNoMsg

Dieser Parameter ist identisch mit /DY, bis auf den Unterschied, dass keine Meldung beim Beenden nach dem Selbsttest ausgegeben wird.

#### /FF

Die zu durchsuchenden Dateien werden vollständig durchsucht.

#### /IM

Mit diesem Parameter können Sie unter Optionen/Diverses einstellen, ob infizierte Dateien vor der Reparatur in das INFECTED-Verzeichnis von AntiVir verschoben werden sollen. Wurde AntiVir ohne diesen Parameter gestartet, sind die entsprechenden Einstellungen nicht möglich.

#### /NB

Mit diesem Parameter können Sie das Durchsuchen sämtlicher Bootsektoren unterbinden. Dieser Parameter sollte ausschließlich bei Problemen mit Bootsektoren angewendet werden.

#### /NOCOPYVIR

Standardmäßig schlägt Ihnen AntiVir vor, bestimmte Viren zur Qualitätssicherung unseres Produktes auf Diskette zu kopieren und uns diese ins Haus zu schicken. Durch Setzen dieses Parameters wird diese Meldung unterdrückt.

#### /NOESC

Verhindert ein Stoppen eines Suchlaufs. Die Schaltfläche "Stop" im Luke Filewalker ist deaktiviert. Dieser Parameter hat die gleiche Funktion wie die Einstellung "Prüfung stoppen" in Optionen/Diverses.

#### /NONETDRV

In der Laufwerkliste von AntiVir werden keine Netzlaufwerke angezeigt.

#### /NOUMB

Abschalten des Speichertests in den UMB-Bereichen (zwischen 640K und 1MB).

#### /NOHMA

Abschalten des Speichertests in der HMA (zwischen 1024K und 1088K).

#### /NS

Mit Hilfe dieses Parameters wird beim Start von AntiVir kein Startbild angezeigt.

#### /R0

Es wird keine Reportdatei erstellt. Dieser Parameter ist nur in Zusammenhang mit der Parameter /B wirksam. Dieser Parameter sollte nur zum Testen verwendet werden.

#### /SCF="Dateiname"

Mit diesem Parameter können Sie einzelne Dateien mit einer Kommandozeile scannen. Dies ist z.B. hilfreich nach einem Download. Dieses Feature ist nur in der Professional Edition verfügbar

#### /X:

Steht für einen Laufwerksbuchstaben. Die Einstellungen für die Laufwerke der Datei `AVWIN.INI` werden ignoriert, nur die in der Kommandozeile angegebenen Laufwerke werden überprüft. Hier sind maximal 26 Einträge möglich.

Die Kommandozeilenparameter lassen sich beliebig mischen.

Eine wichtige Ausnahme davon ist der Parameter /R0: Er lässt sich nur zusammen mit dem Parameter /B einsetzen (und ist auch nur dann sinnvoll; sonst befindet sich möglicherweise ein Virus auf dem Rechner und Sie merken nichts davon ...).

# Report/Kurzreport anzeigen

{button ,AL('rtoReport',0,','')} siehe auch

In diesem Fenster wird aufgezeichnet, wann und mit welchem Ergebnis Ihr Computer von AntiVir nach Viren und unerwünschten Programmen durchsucht wurde. Wurde eine Suche nach Viren sowie unerwünschten Programmen vom Benutzer abgebrochen, ist dies am Ende der Zeile mit (\*) markiert. Ist ein Eintrag mit ✓ markiert, wurde AntiVir bei diesem Suchlauf nicht fündig. Ist allerdings ein Eintrag mit → vorhanden, wurde ein Virus bzw. unerwünschtes Programm gefunden. Um genauere Informationen über einen Eintrag zu erhalten, doppelklicken Sie auf den gewünschten Eintrag.

## Die Schaltflächen dieses Dialogfensters:

**{button Schließen,}**

Das Dialogfenster wird ohne Übernahme der Änderungen geschlossen.

**{button Löschen,}**

Alle Einträge in den Kurzreport werden ohne weitere Nachfrage gelöscht.

**{button Hilfe,}**

Diese Hilfe wird angezeigt.

Im Dialogfenster Optionen/Kurzreport können Sie unter anderem einstellen, wie viele Einträge gespeichert werden sollen. Wird die Anzahl der maximalen Einträge überschritten, werden entsprechend viele Einträge am Anfang der Liste gelöscht. Unter Ausgabedatei können Sie einen Dateinamen angeben, in dem die Daten des Kurzreports gespeichert werden sollen. AntiVir gibt Ihnen den Namen AVWIN.ACT vor.

# Report/Kurzreport löschen

{button ,AL(`rtoReport',0,`,`')} siehe auch

Mit diesem Befehl wird die Datei, in der die Informationen für den Kurzreport gesichert sind, gelöscht. Wenn Sie diesen Menüpunkt wählen, erscheint ein Dialogfenster mit der Frage, ob Sie den Kurzreport wirklich löschen wollen. Ist kein Kurzreport vorhanden, werden alle den Kurzreport betreffenden Optionen außer "Kurzreport/Einstellungen" deaktiviert.

**Hinweis:** Es wird immer die gesamte Liste gelöscht, einzelne Einträge lassen sich auf diese Weise nicht aus der Liste entfernen!



## Suchen/Laufwerksliste aktualisieren

{button ,AL(`rtoSuchen',0,'')} siehe auch

Wird dieser Menüpunkt aufgerufen oder die Funktionstaste (F5) betätigt, wird die Laufwerksliste in der Registerkarte Verzeichnisse auf den aktuellen Stand gebracht.

Diese Funktion sollten Sie aufrufen, wenn Sie Ihre Workstation mit einem Netzlaufwerk verbinden oder von einem Netzlaufwerk trennen, während das Hauptfenster von AntiVir geöffnet ist. Bei einem Neustart von AntiVir werden alle erreichbaren Laufwerke in dieser Liste angezeigt.

## Lizenzdatei

Beim Kauf von AntiVir erhalten Sie eine entweder eine Lizenzdiskette, auf der sich unter anderem auch die Datei "HBEDV.KEY" befindet oder aber Sie erhalten diese Datei von uns per Email. Anhand dieser Datei kann AntiVir feststellen, ob Sie über eine Lizenz für das entsprechende Produkt verfügen.

Nur wenn Sie eine gültige Lizenzdatei haben, läuft AntiVir ohne Einschränkungen als Vollversion.

Die Lizenzdatei "HBEDV.KEY" muss sich im gleichen Verzeichnis wie das entsprechende AntiVir-Programmpaket befinden. Diese Datei wird entweder während des Setups oder nachträglich im Menü "Tools" mit Hilfe des Menüpunktes "Lizenzdatei kopieren" in das richtige Verzeichnis übertragen.

Wird AntiVir auch nach dem Kopieren der Lizenzdatei immer noch als Demo-Version gestartet (das können Sie an der Statuszeile im Hauptfenster erkennen), überprüfen Sie bitte, ob die richtige, zu Ihrem Betriebssystem passende AntiVir-Version freigeschaltet ist. Zusammen mit der Lizenzdatei erhalten Sie auch auch eine Datei "LIC\_INFO.TXT", in der Informationen zu Ihrer Lizenz angegeben sind:

<b>Produktname</b>	nennt die vollständige Bezeichnung des AntiVir-Pakets, das mit der Lizenzdatei freigeschaltet wird. Diese muss mit dem installierten AntiVir-Programmpaket übereinstimmen.
<b>Seriennummer</b>	gibt Ihre Seriennummer an.
<b>Lizenztyp</b>	informiert Sie darüber, welche Art von Lizenz freigeschaltet ist (Grundlizenz, Kombi-Paket, Fast Update-Service).
<b>Updates</b>	zeigt Ihnen, von welcher Versionsnummer Ihre Lizenz beginnt und wann diese abläuft.
<b>Lizenznehmer</b>	nennt den Namen, mit dem die Lizenz vereinbart wurde.

## Lizenzdatei laden

{button ,AL(`rtoTools',0,','')} siehe auch

Mit diesem Menüpunkt können Sie eine Lizenzdatei HBEDV.KEY einlesen. AntiVir kann diese Lizenzdatei von allen Datenträgern übernehmen, beispielsweise von Diskette, CD, Festplatte, Netzlaufwerk usw..

Wird keine Lizenzdatei aufgespielt, läuft AntiVir ausschließlich als Demoversion.

Sie erhalten beim Erwerb von AntiVir von uns den Lizenzkey, abhängig vom Lizenz-Modell, als Datei HBEDV.KEY auf einer Diskette oder per E-Mail.

Wenn Sie im Menü "Tools" auf diesen Menüpunkt scrollen, wird das Standard-Fenster zur Auswahl einer Datei geöffnet. Wählen Sie die Lizenzdatei im Auswahlfeld aus oder tragen Sie Laufwerk, Pfad und Dateinamen der Lizenzdatei (LW:\PFAD\HBEDV.KEY) direkt in das Feld "Dateiname" ein.

Wird die Lizenzdatei nicht an der angegebenen Stelle gefunden, vergewissern Sie sich bitte, ob sich die Datei im angegebenen Ordner befindet und korrigieren gegebenenfalls Ihre Einträge im Fenster "Öffnen".

# Luke Filewalker

Luke Filewalker ist der Scanbildschirm von AntiVir für Windows. Er gibt Aufschluss darüber, was AntiVir gerade durchsucht und welche Aktivitäten bereits abgeschlossen wurden.



## Letzte Meldung

Ist Ihr PC sauber, steht hier der Eintrag 'KEINE FUNDE'. Ist dies nicht der Fall, wird der Name des zuletzt gefundenen Virus bzw. unerwünschten Programms in roter Schrift angezeigt.

## Anzahl Dateien

Hier wird angezeigt, wie viel Dateien AntiVir bereits durchsucht hat.

## Zeit

Gibt die Suchzeit in "mm:ss" an.

## Funde

Informiert über die Anzahl gefundener Viren und unerwünschter Programme.

## Repariert

Informiert über die Anzahl der reparierten Dateien.

## Gelöscht

Informiert über die Anzahl der gelöschten Dateien.

## Ordner

Gibt den Namen des Ordners an, der gerade durchsucht wird.

### Datei

Gibt den Namen der gerade durchsuchten Datei an.

### Status

In dieser Zeile wird angezeigt, womit AntiVir gerade beschäftigt ist. Es gibt drei verschiedene Angaben: "Suchen", "Reparieren" und "Entpacken".

### STOP

Diese Schaltfläche bricht den Suchlauf so schnell wie möglich ab  
Ist diese Schaltfläche grau hinterlegt, lässt sich der Suchlauf nicht unterbrechen. In diesem Fall ist im Menü Optionen/Diverses in der Guppenbox "Suchvorgang" die Option "Stoppen zulassen" nicht aktiviert.

# Optionen/Makroviren

{button ,AL(`rtoAktion nach',0,',')} \_\_siehe auch

AntiVir sucht auch in Dokumenten bzw. in Formatvorlagen nach Makroviren. Die Entfernung bekannter Makroviren lässt sich über das Dialogfenster Optionen/Reparatur steuern.

## Verdächtige Makros

### Alle verdächtigen Makros löschen (Alt+V)

Ist dieses Optionsfeld markiert, werden alle verdächtigen Makros der entsprechenden Datei gelöscht.

Makroviren bestehen in der Regel aus mehreren Makros. Wird mindestens einer davon als verdächtig erkannt und gelöscht, ist meist noch ein Rest des Makrovirus in der Datei vorhanden. Da jetzt aber ein (meist wichtiger) Teil des Virus fehlt, ist dieser nun nicht mehr voll funktionsfähig.

### Alle Makros löschen, wenn eines verdächtig (Alt+M)

Ist diese Einstellung aktiviert, entfernt AntiVir ausnahmslos alle Makros aus der Datei, die gerade überprüft wird. Diese "Radikalkur" ist eigentlich die beste Methode, sich Makroviren zu entledigen. Vorsicht ist dann angebracht, wenn in der verdächtigen Datei noch weitere Makros vorhanden sind: Sie verlieren alle Makros, die nicht zu dem Virus gehören und die Sie vielleicht noch benötigen.

**Vorsicht:** Wenn Sie häufig Makros selbst programmieren, ist die Einstellung "Aktion nachfragen" anzuraten, damit Sie nicht um den Lohn Ihrer Arbeit gebracht werden.

### Aktion nachfragen (Alt+N)

Ist dieses Optionsfeld markiert, wird ein Dialogfenster geöffnet, sobald AntiVir einen Makrovirus findet. Sie können dann sofort in dieser Situation entscheiden, was mit dem möglicherweise infizierten Makro geschehen soll. Dieses Feld ist in der Voreinstellung von AntiVir markiert.

## Formatvorlagen konvertieren

Formatvorlagen bestehen, wie auch Dokumente, aus "normalem" Text, können jedoch zusätzliche Daten enthalten. Öffnet beispielsweise Word 6/7 ein Dokument, sucht es in der dazugehörigen Formatvorlage nach diesen Daten. AntiVir kann Formatvorlagen in das Dokumentformat umwandeln, wenn keine zusätzlichen Daten vorhanden sind, also wenn alle Makros gelöscht wurden und auch keine Menüs, Shortcuts, usw. in der Formatvorlage enthalten sind.

### Niemals (Alt+L)

Es werden keine Formatvorlagen umgewandelt.

### Nur bei .DOC-Dateien (Alt+D)

Ist dieses Optionsfeld markiert, werden nur Dokumente automatisch konvertiert, Formatvorlagen werden auch dann nicht umgewandelt, wenn Sie keine Makros enthalten.

Meist liegen Formatvorlagen als .DOT oder .WIZ vor, reine Dokumente in der Regel als .DOC. Schalten Sie diese Funktion an, wenn AntiVir alle reparierten Dokumente konvertieren soll.

### Immer (Alt+I)

Ist diese Einstellung aktiviert, werden Formatvorlagen immer in ein Dokument konvertiert, wenn ein Makrovirus gefunden und beseitigt wurde.

### Nachfragen (Alt+F)

Ist dieses Optionsfeld aktiviert, wartet AntiVir auf Ihre Bestätigung, ob die angezeigte Datei konvertiert werden soll. Dieses Feld ist in der Voreinstellung von AntiVir ausgewählt.

#### Formattabelle komprimieren (Alt+K)

Mit dieser Option wird festgelegt, ob AntiVir auch die Referenzen auf gelöschte Makros und deren Namen aus der Tabelle der Formatvorlagen entfernen soll.

Wurden Makros aus einer Datei gelöscht, steht immer noch der Name des Makros in der Datei. Das Makro selbst wurde überschrieben und als gelöscht markiert. Einige Antivirenprogramme suchen jedoch nicht nach dem Inhalt eines Virenmakros sondern nur nach dessen Namen und melden Viren, wo keine mehr sind.

#### **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

##### {button OK,}

Die Einträge aus dem Fenster "Makroviren" werden übernommen und das Dialogfenster geschlossen.

##### {button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

##### {button Hilfe,}

Diese Hilfe wird angezeigt.

# Optionen/Makroviren/Auszulassende Makros

{button ,AL('rtoAktion nach',0,','')} siehe auch

Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem alle Makros aufgelistet sind, die von der Virensuche ausgenommen werden.

**Vorsicht:** Diese Makros werden bei einem Suchlauf nicht berücksichtigt. Bitte tragen Sie hier so wenig wie möglich und wirklich nur Makros ein, die - aus welchen Gründen auch immer - bei einem Suchlauf nicht kontrolliert werden sollen. Wir empfehlen, diese Makros auf jeden Fall auf Viren zu untersuchen, *bevor* sie in diese Liste aufgenommen werden! Sie können uns diese Datei, die das entsprechende Makro enthält, auf jeden Fall ins Haus schicken! Sie können auf diese Weise sicherstellen, dass es sich um eine virenfreie Datei handelt.

In dem Listenfeld dieses Fensters sehen Sie die CRC-Summe (hexadezimal) und die entsprechende Länge der Makros, die von der Suche ausgenommen worden sind.

Mit der Schaltfläche {button Einfügen,JI('OPTIONEN\_MAKROVIREN\_AUSZULASSENGE\_DATEIEN\_EINFUEGEN')} wird ein Fenster geöffnet, in dem ein neues Makro in diese Liste aufgenommen werden kann. Um ein Makro wieder aus der Liste zu löschen, markieren Sie den entsprechenden Eintrag und betätigen anschließend die Schaltfläche {button Löschen,}.

**Folgende weitere Schaltflächen sind in diesem Dialogfenster vorhanden:**

{button OK,}

Die Einträge aus dem Fenster "Auszulassende Makros" werden übernommen und das Dialogfenster geschlossen.

{button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

{button Hilfe,}

Diese Hilfe wird angezeigt.



# Optionen/Makroviren/Auszulassende Makros/Einfügen

{button ,AL(`rtoAktion nach',0,'')} \_\_siehe auch

Um der Liste "Auszulassende Makros" einen Eintrag hinzuzufügen, klicken Sie im Menü "Optionen/Makroviren/Auszulassende Makros" auf die Schaltfläche "Einfügen".

Es erscheint ein Dialogfenster, in dem Sie die CRC-Summe (hexadezimal) und die Länge des auszulassenden Makros eingeben können. Diese Werte erfahren Sie aus der Reportdatei, bzw. aus dem Dialogfenster, welches Ihnen das verdächtige Makro meldet.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

### **{button OK,}**

Die Einträge aus dem Fenster "Auszulassendes Makro einfügen" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbruch,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

## **Master-Bootsektor**

ist der erste physikalische Sektor auf einer Festplatte und kommt ausschließlich auf Festplatten vor. Er erfüllt gleich zwei Funktionen: Zum einen enthält er die Partitionstabelle, in der steht, wie und für welches Betriebssystem welcher Platz reserviert wurde und welche Partition als aktiv gekennzeichnet ist. Der andere Teil des Programmcodes überprüft die Partitionstabelle auf Gültigkeit, sucht sich die aktive Partition heraus und lädt den ersten Sektor dieser aktiven Partition in den Speicher. Das ist dann der Bootsektor einer Festplatte.

## **Master-Bootsektorvirus**

ersetzt den Programmcode des Master-Bootsektors durch seinen Virencode, nachdem er (meist) den originalen Master-Bootsektor zwischengespeichert hat. Der Master-Bootsektorvirus bekommt dadurch nach dem BIOS als erstes Programm Kontrolle über das gesamte System.

## **Mehrfachlizenz**

Im Rahmen einer Mehrfachlizenz - beginnend ab drei User - können Sie AntiVir für Windows Workstations entsprechend der Useranzahl auch auf mehreren Plattformen einsetzen.

Es stehen Ihnen zusätzliche Netzwerkooptionen wie beispielsweise Netzwerkwarnungen zur Verfügung.

In einem Netzwerk dient Ihnen der Intranet-Update Wizard zur leichten Aktualisierung von AntiVir.

# Optionen/Netzwerkwarnungen

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

Diese Funktion steht Ihnen nur zur Verfügung, wenn Sie eine Mehrfachlizenz von AntiVir benutzen und in einem Novell NetWare Netzwerk arbeiten indem der NetWare-Client installiert ist.

In diesem Fenster lassen sich die Namen der Netzwerkbenutzer auswählen, die bei einer Meldung von Viren bzw. unerwünschten Programmen automatisch über das Netz gewarnt werden sollen. Sinnvoll ist auf jeden Fall, bei einem Fund den Administrator zu benachrichtigen, da infizierte Dateien über ein Netzwerk recht schnell verbreitet werden können.

Hat der Benutzer, der die Meldung erhalten soll, beispielsweise die NetWare Broadcast Messages mit dem Befehl "CASTOFF" ausgeschaltet, wird die Nachricht zwar an ihn gesendet, aber nicht angezeigt.

## Warnmeldung

Hier können Sie den Text der Warnmeldung eingeben, den AntiVir beim Fund eines Virus bzw. unerwünschten Programms versenden soll.

In diesem Text lassen sich die Platzhalter %NAME% und %VIRUS% verwenden. AntiVir ersetzt den Platzhalter %NAME% durch den Namen des Users, auf dessen Workstation AntiVir fündig wurde, %VIRUS% wird durch den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms ersetzt. Diese Warnmeldung wird am Schluss eines jeden Suchlaufes versandt, wenn AntiVir fündig wurde. Diese Meldung kann maximal 58 Zeichen übertragen, der Rest wird abgeschnitten.

## Warnungen an

Im Listenfeld "Typ" können Sie auswählen, ob Sie die Warnmeldungen an eine Gruppe oder einzelne User versenden wollen.

Im Auswahlfenster "Gruppe" oder "Benutzer" werden diejenigen Gruppen oder User aufgelistet, die eine Zugriffsberechtigung auf den Server besitzen, auf dem Sie selbst eingeloggt sind. Mit den Kontrollkästchen wählen Sie hier aus, an wen Sie eine Meldung versenden wollen. Haben Sie die Einträge mit "OK" bestätigt, bekommt jeder User der rechten Liste beim Fund eines Virus oder unerwünschten Programms die oben eingegebene Nachricht zugeschickt.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## **{button OK,}**

Die Einträge aus dem Fenster "Netzwerkwarnungen" werden übernommen und das Dialogfenster geschlossen.

## **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

## **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Optionen/Netzwerkwarnungen (XP)

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,','')} siehe auch

## Netzwerkwarnungen aktiviert

Um Netzwerkwarnungen innerhalb eines LAN zu versenden, muss dieser Menüpunkt aktiviert werden.

## Zu versendende Nachricht

Hier können Sie den Text der Warnmeldung eingeben, den AntiVir beim Fund eines Virus bzw. unerwünschten Programms versenden soll.

In diesem Text lassen sich die Platzhalter %NAME% und %VIRUS% verwenden. AntiVir ersetzt den Platzhalter %NAME% durch den Namen des Users, auf dessen Workstation AntiVir fündig wurde, %VIRUS% wird durch den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms ersetzt. Diese Warnmeldung wird am Schluss eines jeden Suchlaufes versandt, wenn AntiVir fündig wurde. Diese Meldung kann maximal 58 Zeichen übertragen, der Rest wird abgeschnitten.


Klickt man auf die Schaltfläche "**Standard**", so wird die Standardmeldung eingetragen. Die alte Meldung wird gelöscht.

## Nachricht senden an

In diesem Feld sind alle Rechner aufgelistet, die diese Warnung erhalten sollen. Empfangen werden diese Warnungen allerdings nur von XP-Rechnern. Mit der Schaltfläche Hinzufügen kann eine neue Arbeitsstation hinzugefügt werden. Mit der Schaltfläche Löschen wird eine zuvor in der Liste ausgewählten Arbeitsstation von den Warnungen wieder ausgenommen.

## {button Hinzufügen,}

In dem Dialog "Netzwerkrechner hinzufügen" haben Sie die Möglichkeit, eine Arbeitsstation in die Liste der Rechner, die eine Warnmeldung erhalten sollen, aufzunehmen. Sie können jetzt den Namen der Arbeitsstation direkt in das dafür vorgesehene Feld eingeben. Sie haben auch die

Möglichkeit mit der Schaltfläche  ein Auswahlménü vorhandener Rechner zu öffnen und hier den gewünschten Rechner auszuwählen.

**Folgende weitere Schaltflächen sind in diesem Dialogfenster vorhanden:**

## {button OK,}

Die Einträge aus dem Fenster "Netzwerkwarnungen (XP)" werden übernommen und das Dialogfenster geschlossen.

## {button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

## {button Hilfe,}

Diese Hilfe wird angezeigt.

# Optionen (Inhalt)

{button ,AL('rtoAktion nach',0,','')} siehe auch

**In diesem Fenster lassen sich mit Hilfe der Ordner-Symbole im linken Feld die Optionen zu folgenden Themenbereichen aufrufen:**

## Suchen

Unter diesem Menüpunkt legen Sie fest, wo und wie AntiVir nach Viren bzw. unerwünschten Programmen suchen soll.

## Reparatur

Hier lassen sich Einstellungen für die Reparatur infizierter Dateien vornehmen.

## Unerwünschte Programme

AntiVir schützt Sie vor Computerviren.  
Darüber hinaus haben Sie die Möglichkeit, hier differenziert nach kostenverursachenden Einwahlprogrammen (Dialer), Backdoor-Steuersoftware (BDC), Spiele (Games), Witzprogramme (Jokes) sowie nach möglicher schädlicher Software (PMS) suchen zu lassen.

## Makroviren

Hier werden alle Voreinstellungen zur Suche und Beseitigung von Makroviren ausgewählt.

## Drag&Drop

Hier können Sie einstellen, ob in Ordnern, die mit Drag&Drop auf das Hauptfenster von AntiVir gezogen werden, auch Unterverzeichnisse untersucht und welche Dateiformate berücksichtigt werden sollen.

## Report

Hier entscheiden Sie, welche Informationen in die Reportdatei aufgenommen werden sollen.

## Kurzreport

Unter diesem Punkt stellen Sie ein, ob und mit welchen Optionen ein Kurzreport erstellt wird.

## Aktion nach Suche

(Nur AntiVir Professional Edition)  
Geben Sie hier den Namen und Kommandozeilenparameter eines beliebigen Programms ein, das nach einer Suche gestartet werden soll.

## Kennwort

(Nur AntiVir Professional Edition)  
Hier lässt sich der Zugriff auf die Optionen von AntiVir durch ein Kennwort einschränken.

## Intranet Update

(Nur AntiVir Professional Edition)  
Mit diesem Feature lässt sich ein Update in einem Netzwerk sehr einfach automatisieren (ab einer 3-User-Lizenz freigeschaltet).

## Internet Update

Der Internet Updater sorgt dafür, dass Ihr AntiVir-Programm stets auf dem neuesten Niveau

arbeitet.

### **Profile**

(Nur AntiVir Professional Edition)

Bestimmen Sie hier, welche Dateiarten in einem Profil überprüft werden sollen und ob auch Unterverzeichnisse durchsucht werden sollen.

### **CRC**

(Nur AntiVir Professional Edition)

Bestimmen Sie hier, ob und auf welche Weise und für welche Dateien das CRC-Verfahren eingesetzt werden soll.

### **Netzwerkwarnungen**

#### **Netzwerkwarnungen (XP)**

(Nur AntiVir Professional Edition)

Ist ein Netzwerk eingerichtet, können Sie hier auswählen, welche Benutzer bei einem Fund von Viren und unerwünschten Programmen gewarnt werden sollen.

### **Diverses**

Hier lässt sich einstellen: der temporäre Pfad, ob sich die Prüfung nach Viren und unerwünschten Programmen abbrechen lässt und ob zu löschende Dateien überschrieben werden sollen.

**In dem Menüzeile finden Sie unter "Optionen" auch diese beiden Einträge:**

#### **Einstellungen sichern**

Sichert umgehend die Einstellungen von AntiVir.

#### **Einstellungen beim Beenden speichern**

Sichert alle Einstellungen von AntiVir automatisch beim Schließen des Programms.



## **Partitionstabelle ändern**

Ein Virus hat die Partitionstabelle verändert. AntiVir kann die Partitionstabelle nicht mehr wiederherstellen. Daher wird Ihnen hier angeboten, eine neue Partitionstabelle zu erstellen.

**Vorsicht: Bei dieser Aktion können Datenverluste auftreten, erstellen Sie auf jeden Fall vorher ein Backup!**

# Optionen/Profile

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

In diesem Fenster legen Sie fest, ob bei den Profilen auch die Unterverzeichnisse durchsucht und welche Dateitypen bei einer Suche nach Viren oder unerwünschten Programmen in einem Profil von AntiVir berücksichtigt werden.

## Unterverzeichnisse durchsuchen (Alt+U)

Ist dieses Optionsfeld markiert, werden in einem Profil mit einem oder mehreren Verzeichnissen auch alle Unterverzeichnisse durchsucht. Ist diese Option nicht aktiv, werden nur die Verzeichnisse durchsucht, die direkt in diesem Profil zusammengefasst wurden.

## Dateien

### Alle Dateien (Alt+A)

Per Voreinstellung sucht AntiVir ausschließlich nach ausführbaren Dateien. Ist dieser Menüpunkt angewählt, werden bei einem Suchlauf in einem Profil sämtliche Dateien im entsprechenden Verzeichnis berücksichtigt. Auch nicht ausführbare Dateien werden untersucht.

AntiVir benötigt in dieser Einstellung mehr Zeit zur Suche, da wesentlich mehr Dateien geprüft werden müssen. Ist "Alle Dateien" aktiv, lässt sich die Schaltfläche "Endungen" nicht betätigen.

### Dateien gemäß der Liste in Optionen/Suchen/Dateien/Endungen (Alt+O)

Mit Hilfe dieser Option werden nur die Dateien durchsucht, die Sie vorher im Menü Optionen/Suchen/Dateien/Endungen eingestellt haben.

### Programm- und Makrodateien (Alt+P)

Ist dieses Optionsfeld markiert, wird in den Profilen ausschließlich nach Dateien mit vorgegebenen Endungen gesucht (z. B. \*.BIN, \*.COM, \*.EXE, usw.). Bei den vorgegebenen Endungen sind Standardwerte vorgegeben. Diese Einträge können Sie mit der Schaltfläche {button Endungen,JI('`,`OPTIONEN\_SCANNER\_ENDUNG')} ändern. Ist dieser Punkt aktiv und Sie haben aus der Liste der Dateiendungen alle Einträge gelöscht, wird dies durch den Text "KEINE ENDUNGEN" unterhalb der Schaltfläche "Endungen" angezeigt.

## **Folgende weitere Schaltflächen sind in diesem Dialogfenster vorhanden:**

### **{button OK,}**

Die Einträge aus dem Fenster "Profile" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

## Hilfe/Read Me

{button ,AL(`rtoHilfe',0,`,`')} [siehe auch](#)

In dieser Datei finden Sie wichtige Informationen zu jeder neuen Version von AntiVir.

Durch die kurze Zeitspanne zwischen den Updates ist es uns leider nicht möglich, alle Neuerungen im Handbuch aufzunehmen. Diese Neuerungen werden deshalb in der Datei READ.ME beschrieben. Haben Sie also einmal Probleme oder Fragen zu AntiVir, bei denen das Handbuch nicht weiterhilft, lesen Sie in dieser Datei nach. In den allermeisten Fällen finden Sie spätestens hier eine Lösung für Ihr Problem.

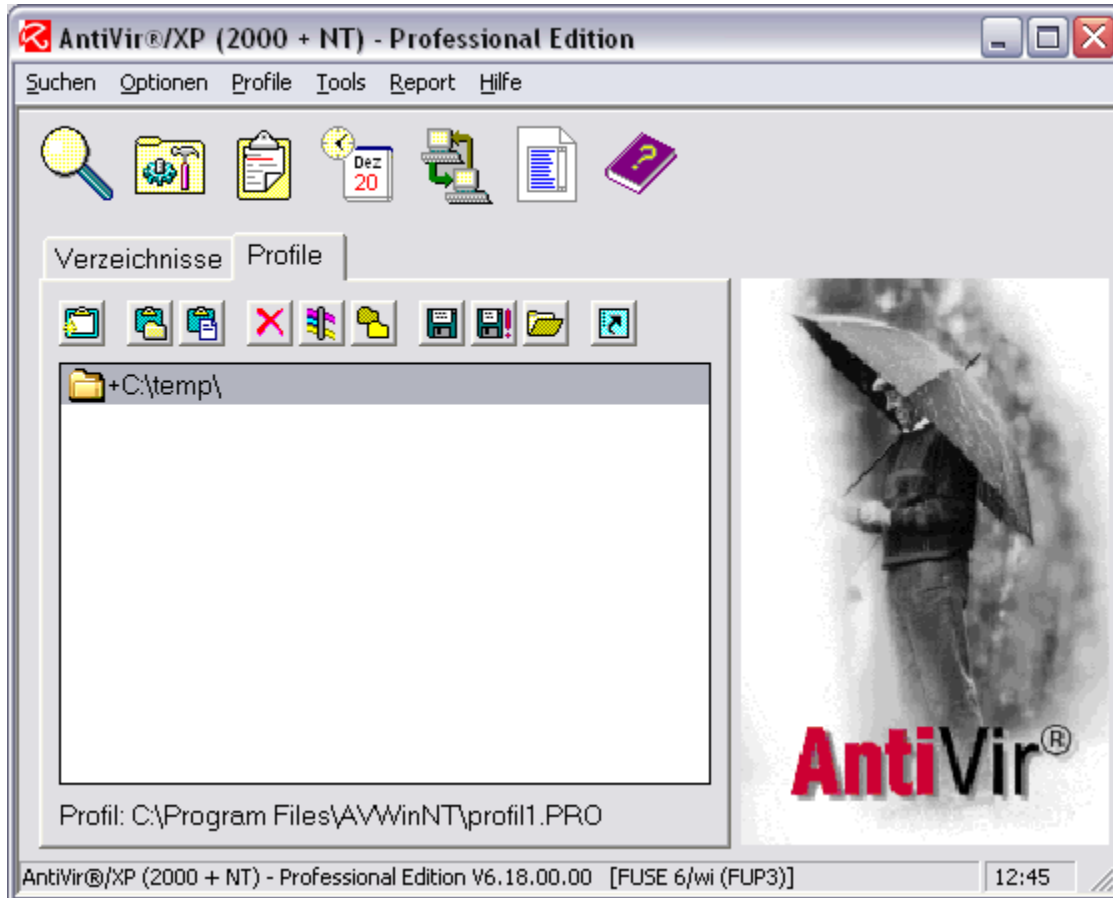
# Registerkarte Profile


(Nur AntiVir Professional)


{button ,AL('rtoProfiles',0,'')} siehe auch


Mit Hilfe dieser Registerkarte können Sie Dateien, Ordner und Laufwerke zu Profilen zusammenfassen und diese in einer Liste abspeichern. Diese Profile lassen sich dann zu einer schnellen, gezielten Suche nach Viren bzw. unerwünschten Programmen einsetzen.

Sobald Sie die Registerkarte "Profile" aufrufen, befindet sich diese Funktion im Edit-Modus.



 Soll ein bereits erstelltes Profil nach Viren bzw. unerwünschten Programmen durchsucht werden, öffnen Sie die Liste der Profile mit der Schaltfläche "Profil laden" und doppelklicken auf das entsprechende Profil in der Liste (Alternative: markieren und die Schaltfläche "Öffnen" betätigen). Noch einfacher ist der Aufruf eines Profiles, wenn eine Verknüpfung auf dem Desktop angelegt wurde (siehe weiter unten). Wird diese Verknüpfung auf dem Desktop angeklickt, startet AntiVir und durchsucht dieses Profils.

 Wird die Funktion "Ein neues Profil erstellen" mit dieser Schaltfläche aufgerufen, wird das zuletzt geladene Profil geschlossen und Sie können ein neues Profil erstellen.

 Hier können Sie mit der Schaltfläche "Ordner einfügen" ein Fenster aufrufen, in dem Sie einen Ordner auswählen können, der in das aktuelle Profil eingefügt werden soll. AntiVir durchsucht per

Voreinstellung alle Unterverzeichnisse des gewählten Ordners.



Mit Hilfe der Schaltfläche "Datei einfügen" lassen sich auf dem gleichen Weg einzelne Dateien in das aktuelle Profil einfügen.



Mit der Schaltfläche "Eintrag löschen" entfernen Sie markierte Ordner oder Dateien aus der Registerkarte "Profile".  
Sie können auch die zu löschenden Einträge markieren und mit der Taste "Entf" aus der Liste entfernen.



Mit der Schaltfläche "Dateifilter" wird ein Dialogfenster geöffnet, in dem Sie festlegen, welchen Dateitypen bei einem Suchlauf berücksichtigt werden sollen:

#### Gemäß der Suchmaske scannen (Alt+S)

Haben Sie diese Option ausgewählt, können Sie in dem Listenfeld dieses Fensters Dateiendungen von denjenigen Dateitypen eingeben, die durchsucht werden sollen. Für einen gezielten Suchlauf beispielsweise in allen .EXE-Dateien tragen Sie hier `*.EXE` ein.  
TIP: um .DOC **und** .DOT-Dokumente durchsuchen zu lassen, geben Sie einfach `*.do?` ein.

#### Die Profil-Standard Einstellungen verwenden (Alt+P)

Es werden nur die Dateitypen gescannt, die im Menü Optionen/Profile ausgewählt wurden.

#### Alle Dateien in diesem Pfad scannen (Alt+D)

Es werden alle Dateien untersucht.



Mit Hilfe der Schaltfläche "Unterverzeichnisse" können Sie festlegen, ob Sie vom ausgewählten Ordner auch die Unterverzeichnisse durchsuchen wollen.

Klicken Sie auf diese Schaltfläche, wird beim markierten Ordner das **+** durch ein **-** ersetzt.

- +** heißt: die Unterverzeichnisse werden durchsucht
- heißt: die Unterverzeichnisse werden nicht durchsucht

Standardmäßig scannt AntiVir alle Unterverzeichnisse des gewählten Ordners.



Mit der Schaltfläche "Profil speichern" wird ein Fenster aufgerufen, in dem Sie ein neu erstelltes oder bearbeitetes Profil speichern können.

Die Profildateien können Sie an der Endung `*.PRO` erkennen.

Haben Sie nach dem letzten Speichervorgang Änderungen in der Registerkarte "Profile" vorgenommen, erscheint beim Schließen eines Profils die Anfrage, ob Sie dieses Profil speichern möchten. Bestätigen Sie diese Meldung gemäß Ihren Wünschen mit "Ja" oder "Nein".



Mit der Schaltfläche "Als Standardprofil speichern" wird ein Fenster aufgerufen, in dem Sie ein neu erstelltes Profil als Standardprofil speichern können.  
Wenn Sie AntiVir neu starten, wird dieses Standardprofil automatisch in die Registerkarte geladen.



Mit der Schaltfläche "Verknüpfung erstellen" können Sie für ein Profil eine Verknüpfung mit dem Namen "AntiVir <Profilname>" auf dem Desktop erstellen.  
Wird diese Verknüpfung auf dem Desktop angeklickt, startet AntiVir und scannt alle Dateien und Ordner dieses Profils.



# Optionen/Reparatur

{button ,AL('rtoAktion nach',0,'')} siehe auch

In diesem Fenster legen Sie fest, wie AntiVir reagieren soll, wenn ein Virus bzw. ein unerwünschtes Programm gefunden wird. Die Bandbreite der Aktionen reicht vom Aufzeichnen der Ereignisse bis zur Reparatur der infizierten Dateien.

Die meisten Einstellungen in diesem Fenster können nur vorgenommen werden und sind auch nur wirksam, wenn "Nur in Reportdatei aufzeichnen" **nicht** aktiv ist!

## Infizierte Dateien

### Reparieren mit Rückfrage (Alt+M)

Ist diese Einstellung aktiviert, fragt AntiVir nach Auffinden einer reparablen Datei mit infiziertem Code zuerst zurück, ob die entsprechende Datei repariert werden soll.

### Reparieren ohne Rückfrage (Alt+K)

Es werden reparable Dateien mit infiziertem Code sofort ohne Rückfrage repariert.

### Löschen mit Rückfrage (Alt+F)

Infizierte Dateien werden nach Rückfrage gelöscht. Wollen Sie sicher gehen, dass diese Datei nicht wieder hergestellt werden kann (z.B. mit UNERASE), markieren Sie im Fenster Optionen/Diverses den Punkt "Zu löschende Dateien überschreiben".

Ist "Zu löschende Dateien überschreiben" aktiviert, werden auch infizierte Dateien gelöscht, die möglicherweise reparabel sind.

### Löschen ohne Rückfrage (Alt+R)

Infizierte Dateien werden ohne Rückfrage gelöscht. Wollen Sie sicher gehen, dass diese Datei nicht wieder hergestellt werden kann (z.B. mit UNERASE), markieren Sie im Dialog Optionen/Diverses den Punkt "Zu löschende Dateien überschreiben".

Ist "Zu löschende Dateien überschreiben" aktiviert, werden auch infizierte Dateien gelöscht, die möglicherweise reparabel sind.

## Infizierte zerstörte Dateien

Die Einstellungen in dieser Gruppe sind nur aktiv, wenn unter "Infizierte Dateien" eingestellt wurde, dass infizierte Dateien repariert werden sollen.

### Löschen mit Rückfrage (Alt+C)

Konnte eine infizierte Datei nicht repariert werden, weil sie beispielsweise durch einen Virus zerstört wurde, wird diese Datei nach Rückfrage gelöscht, wenn diese Einstellung aktiv ist. Wollen Sie sicher gehen, dass diese Datei nicht wieder hergestellt werden kann (z.B. mit UNERASE), markieren Sie im Dialogfenster Optionen/Diverses den Punkt "Zu löschende Dateien überschreiben".

### Löschen ohne Rückfrage (Alt+N)

Auch diese Einstellung ist nur wirksam, wenn AntiVir auf eine infizierte, nicht reparable Datei trifft. Ist dieser Punkt aktiviert, wird die entsprechende Datei ohne Rückfrage gelöscht. Wollen Sie sicher gehen, dass diese Datei nicht wieder hergestellt werden kann (z.B. mit UNERASE), markieren Sie im Dialog Optionen/Diverses den Punkt "Zu löschende Dateien überschreiben".

### Ignorieren (Alt+I)

Ist dieser Punkt markiert, wird eine nicht reparable Datei weder gelöscht noch repariert.

**Achtung:** Verbleibt solch eine Datei auf Ihrem System, müssen Sie vorsichtig sein: diese zerstörte Datei ist zwar wahrscheinlich nicht mehr lauffähig, aber sie enthält nach wie vor virulenten Code, der Schaden anrichten kann.

## Akustische Warnung

### Akustische Warnung (Alt+W)

Ist diese Funktion aktiviert, spielt AntiVir bei einem Fund eine kurze Tonfolge ab.

### Wave Datei (Alt+E)

Im Eingabefeld "Wave Datei" können Sie den Pfad und Namen eine Wave-Datei Ihrer Wahl eintragen. Ist dieses Feld leer, wird der Standardwarnton verwendet.

## Datum/Uhrzeit

Wird von AntiVir eine Datei repariert, erfolgt auf diese Datei ein schreibender Zugriff (der Code muss ja entfernt werden). Das Datum und die Uhrzeit dieser Datei werden dabei normalerweise auf das aktuelle Systemdatum gesetzt.

Die Einstellungen in dieser Anzeigegruppe sind nur aktiv, wenn unter "Infizierte Dateien" eingestellt wurde, dass infizierte Dateien repariert werden sollen.

### Nicht verändern (Alt+V)

Ist diese Einstellung aktiviert, wird das ursprüngliche Datum und die ursprüngliche Zeit beibehalten.

### Aktuelle Systemzeit (Alt+S)

Das Datum und die Zeitangabe einer reparierten Datei werden auf die aktuellen Systemwerte gesetzt.

### Datum korrigieren (Alt+D)

Manche Viren manipulieren das Datum oder die Zeitangabe einer Datei, um erkennen zu können, ob sie diese Datei bereits infiziert haben. Ein Beispiel hierfür ist der Vienna-Virus, der den Sekundeneintrag einer infizierten Datei auf 62 setzt.

Mit "Datum korrigieren" setzt AntiVir die Datums- und Zeitangaben nach einer Reparatur wieder auf einen gültigen Wert.

**Aber Vorsicht:** Haben Sie Spiele von der Firma Sierra auf Ihrem Rechner installiert, sollten Sie diese Einstellung nicht wählen. Sierra erhöht die Jahreszahl um 100 (warum die das machen, können wir nicht zwingend nachvollziehen). Ein Tremor-Virus macht das ebenfalls, er erhöht die Jahreszahl um 100, um erkennen zu können, ob eine Datei bereits infiziert ist. Und woher soll AntiVir bei der Korrektur der Jahreszahl nun wissen, ob es sich um Ihr heißgeliebtes Spiel oder um einen Virus handelt?

### Nur in Reportdatei aufzeichnen (Alt+U)

Ist diese Einstellung aktiviert, werden weder Reparaturen vorgenommen noch infizierte Dateien gelöscht.

**Achtung: Virenfunde sowie Funde unerwünschter Programme werden nur in der Reportdatei aufgezeichnet!  
Es verbleiben betroffene Dateien auf Ihrem Computer!**

Sie müssen bei einer Virenmeldung bzw. Funde unerwünschter Programme selbst entscheiden, was



mit den Dateien geschehen soll.

Damit immer eine Reportdatei erstellt wird, sollten Sie unter Optionen/Report die Reportdatei nicht ausschalten.

### **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

#### **{button Test akustische Warnung,}**

Diese Schaltfläche in der Anzeigegruppe "Akustische Warnung" dient zum Ausprobieren der ausgewählten Wave-Datei.

#### **{button OK,}**

Die Einträge aus dem Fenster "Reparatur" werden übernommen und das Dialogfenster geschlossen.

#### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

#### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Optionen/Report

{button ,AL(`rtoAktion nach',0,','')}\_ siehe auch

In diesem Fenster nehmen Sie die Einstellungen für die Reportdatei von AntiVir vor.

**Damit Sie bei einem Fund von Viren oder unerwünschten Programmen nachvollziehen können, welche Aktionen AntiVir ausgeführt hat, sollte immer eine Reportdatei erstellt werden.**

Dazu muss ein gültiger Dateiname für die Ausgabedatei vorhanden sein! Die Reportdatei wird immer im Programmverzeichnis von AntiVir abgelegt.

In der Reportdatei sind Felder vorgegeben, in denen Sie Ihren Namen eintragen können, falls Sie uns diese Reportdatei einmal zusenden müssen. Um in solch einem Fall nicht immer alles von Hand eingeben zu müssen, können Sie eine Datei mit dem Namen AVWIN.ADR im Verzeichnis von AntiVir anlegen, in die Sie alle benötigten Informationen eintragen. Diese Daten übernimmt AntiVir nun in jede Reportdatei.

Aufbau der Adressdatei:

[Adresse]

Institution=H+BEDV Datentechnik GmbH

Abteilung=Entwicklung

Name=Herr Mustermann

Straße=Lindauer Straße 21

Ort=88069 Tettngang

Telefon/Fax=07111/111111 07111/11112

Email=herr@mustermann.de

Diese Einstellungen können Sie zum Erstellen einer Reportdatei verändern:

## Dateimodus

### Kein Report erstellen (Alt+K)

AntiVir erstellt keine Reportdatei. Diese Einstellung sollte nur zum Testen verwendet werden, da die Reportdatei relativ groß werden kann. **Im normalen Betrieb sollten Sie immer eine Reportdatei erstellen lassen!**

### Report überschreiben (Alt+E)

AntiVir überschreibt eine bereits vorhandenen Reportdatei bei jedem neuen Suchlauf. Diese Einstellung sollte im Allgemeinen ausreichen und hat den Vorteil, dass die Reportdatei nie allzu groß wird.

### Neuen Report anhängen (Alt+N)

AntiVir hängt die neue Reportdatei an eine bestehende Reportdatei an. Aber Vorsicht, bei regelmäßiger Benutzung von AntiVir und ständigem Anhängen an eine bestehende Datei wird diese größer und größer und dafür der Platz auf Ihrer Festplatte kleiner und kleiner. Wenn Sie mit dieser Einstellung arbeiten, sollten Sie Ihre Reportdatei von Zeit zu Zeit wieder löschen.

## Daten aufzeichnen

### Infizierte Dateien (Alt+I)

In der Reportdatei werden nur die Namen der infizierten Dateien mit Pfad aufgenommen.

#### Zusätzlich alle Pfade (Alt+P)

In der Reportdatei werden die Namen der infizierten Dateien und zusätzlich alle durchsuchten Pfade aufgenommen.

#### Alle durchsuchten Dateien (Alt+D)

In der Reportdatei werden alle Dateinamen und Pfade, die durchsucht wurden, aufgenommen.

#### Komplette Information (Alt+M)

Hier werden die gleichen Informationen wie unter dem Punkt "Alle durchsuchten Dateien" aufgezeichnet, außerdem aber noch Zusatzinformationen. Dabei handelt es sich um die folgenden Dateien: AUTOEXEC.BAT, CONFIG.SYS, WIN.INI und SYSTEM.INI. Sollten Sie uns einmal eine Reportdatei zusenden müssen (zur Fehlersuche), bitten wir Sie, diese Reportdatei in diesem Modus zu erstellen.

**Bei all diesen Einstellungen gilt: ist der Report ausgeschaltet, wird natürlich auch nichts in die Reportdatei geschrieben!**

#### **Ausgabedatei (Alt+G)**

Geben Sie in das Feld in dieser Gruppenbox den Namen der Datei ein, unter dem der Report abgelegt werden soll. Dieser Name kann für den Fall, dass Sie eine Reportdatei nicht gleich löschen wollen, für jeden Suchlauf geändert werden.

#### **Reportdatei kürzen (Alt+R)**

In dieser Gruppenbox legen Sie die maximale Größe der Reportdatei fest. Aktivieren Sie diesen Punkt und geben Sie die gewünschte Größe im Feld "Abschneiden nach ... KB" (Alt+S) ein. Diese Einstellung hat den Vorteil, dass die Reportdatei auf eine maximale Größe beschränkt werden kann. Stellen Sie sich vor, Sie arbeiten im anhängenden Modus und lassen bei jedem Suchlauf die kompletten Informationen in die Reportdatei schreiben. Benutzen Sie AntiVir nun auch noch häufig, wird der freie Platz auf Ihrer Festplatte permanent kleiner.

#### **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

##### **{button Warnungen,JI(';',`OPTIONEN\_REPORT\_WARNUNGEN')}**

Mit Hilfe dieser Schaltfläche wird das Fenster "Warnungen" geöffnet. Dort können Sie wählen, welche Warnungen in der Reportdatei aufgenommen werden sollen. Bei diesen Einstellungen handelt es sich ausschließlich um Warnungen, nicht aber um Virenfunde, Funde unerwünschter Programme oder beispielsweise CRC-Änderungen. Weitere Informationen finden Sie unter Optionen/Report/Warnungen.

##### **{button OK,}**

Die Einträge aus dem Fenster "Report" werden übernommen und das Dialogfenster geschlossen.

##### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

##### **{button Hilfe,}**

Diese Hilfe wird angezeigt.



# Report (Inhalt)

{button ,AL(`rtoReport',0,`,`')}\_ siehe auch

**In diesem Menü finden Sie alle Funktionen, die für die Reportdatei und für den Kurzreport von Bedeutung sind:**

## **Anzeigen**

öffnet das Programm AntiVir Report mit der zuletzt erstellten Reportdatei.

## **Einstellungen...**

öffnet das Fenster "Optionen", dort lassen sich Einstellungen für die Reportdatei vornehmen.

## **Löschen**

löscht die Reportdatei.

## **Drucken...**

druckt die Reportdatei.

## **Kurzreport anzeigen...**

zeigt den Kurzreport an.

## **Kurzreport Einstellungen...**

öffnet das Fenster "Optionen", dort lassen sich Einstellungen für den Kurzreport vornehmen.

## **Kurzreport löschen**

löscht den Kurzreport.

## Report/Anzeigen

{button ,AL(`rtoReport',0,`,`')}\_ siehe auch

Wenn Sie den Menüpunkt "Report anzeigen" aufrufen oder auf das entsprechende Symbol klicken, wird das Programm AntiVir Report aufgerufen. Dieses Hilfsprogramm ist ein eigenständiger Dateibetrachter, mit dem normalerweise die Reportdatei von AntiVir geladen und angezeigt wird.

Sie können auch .TXT oder .LOG-Dateien mit AntiVir Report betrachten. Diese Dateitypen lassen sich auch per Drag&Drop öffnen.

Nähere Informationen erhalten Sie in der Hilfedatei von Optionen/Report.

## Report/Drucken

{button ,AL(`rtoReport',0,`,`')}\_ siehe auch

Mit dem Menüpunkt "Drucken" starten Sie den Ausdruck der gerade angezeigten Datei, im Normalfall ist dies die Reportdatei von AntiVir.

Treten beim Drucken Probleme auf, müssen Sie den Drucker gegebenenfalls neu einrichten. Dazu steht Ihnen die Funktion "Drucker einrichten" zur Verfügung. Die hier vorgenommenen Einstellungen beziehen sich nur auf AntiVir Report, sie werden nicht generell geändert.

Informationen über die Druckerinstallation finden Sie in Ihrer Windows-Dokumentation.

## Report/Löschen

{button ,AL(`rtoReport',0,`,`')} siehe auch

Eine vorhandene Reportdatei kann mit Hilfe dieser Funktion gelöscht werden.

Wenn Sie diesen Menüpunkt wählen, erscheint ein Dialogfenster mit der Frage, ob Sie die Reportdatei wirklich löschen wollen. Ist keine Reportdatei vorhanden, werden die Schaltfläche "Report" und alle AntiVir Report betreffenden Optionen außer Report/Einstellungen deaktiviert.



# Optionen/Report/Kurzreport

{button ,AL(`rtoAktion nach',0,',')} \_\_siehe auch

In den Kurzreport werden Eckdaten für jeden Suchlauf von AntiVir geschrieben, mit denen sich die Aktivitäten von AntiVir über längere Zeit hinweg verfolgen lassen. Auf diese Weise können Sie die Begegnungen nachvollziehen, die Ihr System in letzter Zeit mit Viren oder unerwünschten Programmen hatte - vorausgesetzt, Sie haben "Kurzreport erstellen" aktiviert.

## Kurzreport erstellen (Alt+K)

Ist dieses Feld markiert, wird automatisch ein Kurzreport erstellt.

## Ausgabedatei (Alt+D)

Hier geben Sie einen Dateinamen an, unter dem die Daten des Kurzreports gespeichert werden. AntiVir gibt Ihnen den Namen AVWIN.ACT vor.

## Maximale Anzahl Einträge (Alt+M)

Mit dieser Einstellung beeinflussen Sie die Größe der Ausgabedatei. AntiVir legt nur so viele Einträge in der Ausgabedatei ab, wie hier eingestellt sind. Die maximale Anzahl beträgt 999 Einträge. Die Zahl der Einträge können Sie entweder direkt eingeben oder mit Hilfe der Bildlaufpfeile rechts vom Eingabefeld verändern. Wenn Sie einen dieser Pfeile anklicken, verändert sich der aktuelle Wert um 1, wenn Sie gleichzeitig die Strg-Taste gedrückt halten, um 10.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

### **{button OK,}**

Die Einträge aus dem Fenster "Kurzreport" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Optionen/Report/Warnungen

{button ,AL('rtoAktion nach',0,',')} siehe auch

In diesem Dialogfenster können Sie auswählen, welche Warnungen in der Reportdatei gemeldet werden sollen.

Bei diesen Einstellungen handelt es sich ausschließlich um Warnmeldungen, nicht um Virenfunde, Funde unerwünschter Programme oder beispielsweise CRC-Änderungen. Jede hier markierte Meldung wird - falls solch ein Ereignis auftritt - in die Reportdatei aufgenommen.

## Zugriffsfehler/Datei ist gesperrt (Alt+Z)

Auf diese Datei kann nicht zugegriffen werden, sie ist daher auch nicht nach Viren bzw. unerwünschten Programmen durchsucht worden. Diese Meldung tritt beispielsweise bei einer Swap-Datei (Auslagerungsdatei) von Windows auf. Die Swap-Datei bleibt solange Windows läuft permanent geöffnet und lässt sich daher nicht überprüfen.

## Falsche Dateigröße im Verzeichnis (Alt+F)

Die im Verzeichnis abgelegte Größe stimmt nicht mit der realen Dateigröße überein.

## Falsche Erstellungszeit im Verzeichnis (Alt+E)

Die Datei enthält einen falschen Datums- oder Zeiteintrag. Der Vienna-Virus verwendet z.B. im Sekundenfeld den Wert 62, wenn eine Datei infiziert ist. Tremor hingegen erhöht die Jahreszahl einer infizierten Datei um 100 als Kennung. Diese Änderungen der Zeit bzw. des Datums müssen aber nicht immer von einem Virus verursacht worden sein, beispielsweise erhöht auch der Spielehersteller Sierra die Jahreszahl um 100.

## COM-Datei zu groß (Alt+C)

Eine COM-Datei kann maximal 65536 Bytes groß sein. Diese Warnung wird ausgegeben, wenn eine größere COM-Datei gefunden wurde.

## Ungültige Startadresse (Alt+U)

Bei EXE-Dateien ist im EXE-Header die Startadresse des Programms in CS:IP abgelegt. Diese Warnung wird ausgegeben, wenn hier ein ungültiger Wert gefunden wurde.

## Ungültiger EXE-Header (Alt+G)

Im EXE-Header ist die Länge einer Datei abgelegt. Unterscheidet sich die dort angegebene Länge von der wirklichen Länge, wird diese Warnung ausgegeben.

## Möglicherweise beschädigt (Alt+M)

Diese Datei kann beispielsweise von Viren beschädigt worden sein. Treten beim Umgang mit dieser Datei Probleme auf, ersetzen Sie diese durch die Originaldatei.

## OLE-Datei ist beschädigt oder geschützt (Alt+L)

Eine Datei, die Informationen zum Object Linking and Embedding enthält, lässt sich nicht überprüfen.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## {button OK,}

Die Einträge aus dem Fenster "Warnungen im Report" werden übernommen und das Dialogfenster

geschlossen.

**{button Abbruch,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

**{button Hilfe,}**

Diese Hilfe wird angezeigt.

## Tools/Scheduler

{button ,AL(`rtoTools',0,`,`')} siehe auch

Wenn Sie diesen Menüpunkt wählen oder die entsprechende Schaltfläche betätigen, wird der Scheduler von AntiVir aufgerufen. Mit diesem eigenständigen Programm können Sie AntiVir zeitgesteuert starten. Sie müssen also nicht selbst an Ihrem Computer sitzen, um beispielsweise sehr große Festplatten zu durchsuchen, sondern sagen dem Scheduler einfach, er soll AntiVir jeden Freitagabend um 22.00 Uhr starten. Dazu müssen zu diesem Zeitpunkt allerdings sowohl das Rechnersystem in Betrieb als auch der Scheduler aktiviert sein.

Mit dem Scheduler können Meldungen zu bestimmten Zeiten aufgerufen sowie auch der Startzeitpunkt anderer Programme und Hilfsprogramme bestimmt werden. Sie haben ein einfach zu bedienendes Hilfsmittel, um regelmäßig wiederkehrende Routinen zu steuern.

Weitere Informationen finden Sie in der Hilfedatei des AntiVir Scheduler.

## **Internet Update starten**

Hier wird der AntiVir Internet Updater gestartet. Mit diesem Programm können Sie sich neue Updates aus dem Internet laden. Hilfe zur Konfiguration finden Sie unter [Optionen/Internet Updater](#).

## **Optionen beim scannen**

Hier werden die Optionen festgelegt, die AntiVir beim scannen verwenden soll. Weitere Informationen zu den umfangreichen Konfigurationsmöglichkeiten erhalten Sie, wenn Sie im Fenster "Optionen" die Hilfe zu den entsprechenden Registerkarten aufrufen.

## Report

Zeigt die Reportdatei zu dem letzten Suchlauf an.

Mehr Informationen finden Sie in der Hilfe zum Menü "Optionen" unter der Registerkarte Report.

## **Scheduler starten**

Hier wird der AntiVir Scheduler gestartet. Mit diesem Programm können Sie angeben, zu welchen Zeiten AntiVir automatisch einen Suchlauf starten soll. Mehr Informationen finden Sie in der Hilfe des Schedulers.



## **Suche starten**

Wird auf diese Schaltfläche geklickt, startet AntiVir einen Suchlauf.  
Diese Schaltfläche ist nur aktiv, wenn Sie ein Laufwerk, ein Verzeichnis oder eine Datei ausgewählt haben.

## **Erkennungsliste anzeigen**

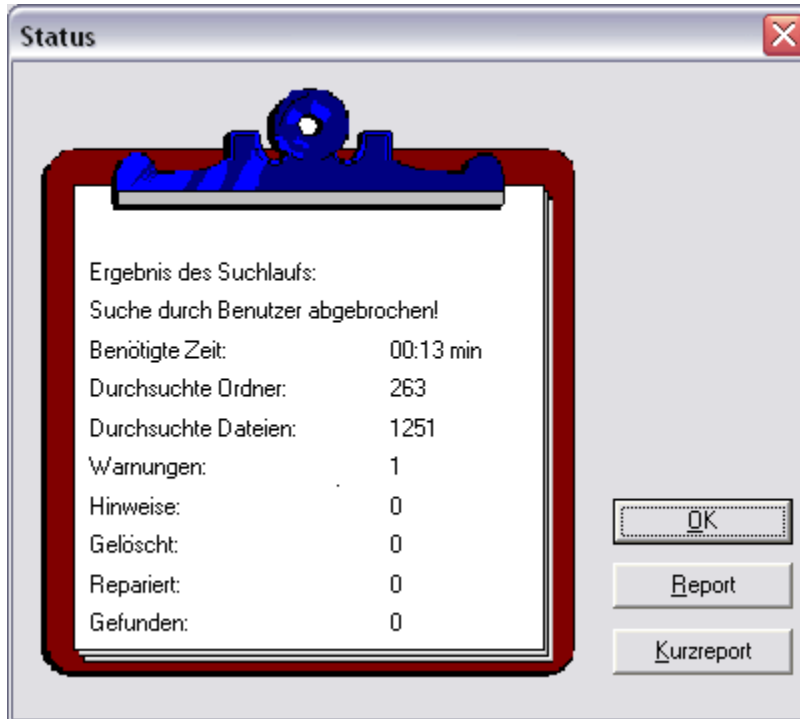
Hier wird eine Liste der Viren bzw. unerwünschten Programme die AntiVir erkennt, angezeigt.

# Status

Nach jedem Suchlauf öffnet AntiVir das Fenster "Status". Hier sehen Sie in einer Kurzfassung, welche Aktionen AntiVir durchgeführt hat.

Befindet sich rechts neben dem Notizblock ein **Ausrufezeichen**, weist dies darauf hin, dass AntiVir fündig geworden ist.

Unter der Zeile "Ergebnis des Suchlaufs" werden Sie darüber informiert, ob AntiVir seinen Suchlauf normal beendet hat oder die Suche vom Benutzer abgebrochen wurde.



Unter dieser Zeile werden folgende Einträge aufgelistet:

## Benötigte Zeit

Gibt die Suchzeit in mm:ss an.

## Durchsuchte Ordner

Anzahl der insgesamt durchsuchten Ordner.

## Durchsuchte Dateien

Anzahl der insgesamt durchsuchten Dateien.

## Warnungen

Anzahl der Warnungen, die ausgegeben wurden.

## Hinweise

Anzahl der Hinweise, die ausgegeben wurden.

## Gelöscht

Anzahl der insgesamt gelöschten Dateien.

#### Repariert

Anzahl der reparierten Dateien.

#### Gefundenen

Anzahl gefundener Viren und unerwünschter Programme.

### **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

#### {button OK.}

Das Informationsfenster "Status" wird geschlossen

#### {button Report.}

Zeigt den ausführlichen Report über den Suchlauf an  
Mehr Informationen zum Report

#### {button Kurzreport.}

Zeigt eine kurze Zusammenfassung der Ergebnisse aller Suchläufe an, die bisher (bzw. seit dem letzten Löschen des Kurzreportes) durchgeführt wurden  
Mehr Informationen zum Kurzreport

# Suchen/Suche starten




{button ,AL(`rtoSuchen',0,'')} siehe auch

## Suchen nach einem Virus bzw. unerwünschten Programmen

Dabei wird nach einer bestimmten Signatur gesucht, die praktisch einem "Fingerabdruck" eines unerwünschten Programms entspricht.

Mit Hilfe einer Datenbank mit den Kennungen - das entspricht der Verbrecherkartei - kann AntiVir diese Signatur bestimmen. Der Eindringling kann entdeckt und unschädlich gemacht werden, infizierte Dateien können repariert werden.

Sie können einen Suchlauf auf verschiedenen Wegen starten:

- ▶ Durch Anklicken der Schaltfläche "Suchen"
- ▶ über die Menüleiste "Suchen/Suche starten"
-  die Funktionstaste (F2)
-  mit Hilfe der Drag & Drop-Funktion
-  mit der Shell-Erweiterung (rechte Maustaste)

Der Scanbildschirm von AntiVir, Luke Filewalker, wird gestartet, und die Dateien in den ausgewählten Bereichen werden überprüft.

Luke Filewalker informiert Sie über den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms, die Anzahl der bisher durchsuchten Dateien, die benötigte Zeit, die Anzahl der Viren bzw. unerwünschten Programme sowie der reparierten und gelöschten Dateien. Auch Name und Pfad der gerade untersuchten Datei sowie der aktuelle Status (z.B. Teste Speicher, Teste Bootsektor, Suchen, Entpacken, Reparieren) werden angegeben.

Ist im Menü Optionen/Diverses das Feld "Stoppen zulassen" aktiviert, können Sie den Suchlauf mit der Schaltfläche "Stop" unterbrechen.

# Optionen/Suchen

{button ,AL('rtoAktion nach',0,'')} siehe auch

In diesem Fenster können Sie einstellen, welche Dateien wo und wie von AntiVir nach Viren bzw. unerwünschten Programmen untersucht werden sollen.

## Bootsektoren

### Bootsektor Suchlaufwerke (Alt+B)

Ist diese Funktion aktiviert, wird beim Start der Suche der Bootsektor aller zu durchsuchender Laufwerke auf Befehl geprüft. Dieser Punkt ist nur aktiv und kann auch nur dann geändert werden, wenn "Alle Bootsektoren" ausgeschaltet ist.

### Alle Bootsektoren (Alt+L)

(Nur AntiVir Professional Edition)

Bei dieser Einstellung werden sämtliche vorgewählten Bootsektoren - also auch die Bootsektoren derjenigen Laufwerke, die nicht vollständig durchsucht werden sollen - getestet. Ist dieser Einstellung aktiv, wird die Einstellung "Bootsektor Suchlaufwerke" deaktiviert und die Schaltfläche "Bootsektoren" aktiviert.

### {button Bootsektoren.JI('','OPTIONEN\_BOOTSEKTOR')}

Ist "Alle Bootsektoren" aktiv, lässt sich mit dieser Schaltfläche ein Fenster öffnen. Dort wird eingestellt, von welchen Laufwerkstypen die Bootsektoren bei jedem Suchstart geprüft werden sollen. Diese Laufwerkstypen sind Diskettenlaufwerke, Festplatten und Ramdisks.

## Dateien

### Alle Dateien (Alt+D)

Per Voreinstellung untersucht AntiVir ausschließlich Programmdateien. Ist dieser Menüpunkt angewählt, werden alle Dateien auf den entsprechenden Laufwerken nach Viren bzw. unerwünschten Programmen durchsucht, also werden auch nicht ausführbare Dateien gescannt.

**Hinweis:** Diese Einstellung sollte nur nach einem Virenfund bzw. Fund eines unerwünschten Programms aktiviert werden, um einmal alle Dateien zu überprüfen. Sollen alle Dateien durchsucht werden, dauert die Suche länger, da wesentlich mehr Dateien geprüft werden müssen. Ist "Alle Dateien" aktiv, lässt sich die Schaltfläche "Endungen" nicht anwählen.

### Programm- und Makrodateien (Alt+G)

Haben Sie diese Option ausgewählt, werden nur Dateien mit einer vorgegebenen Endung durchsucht (z.B. \*.BIN, \*.COM, \*.EXE, usw.). Bei den Endungen sind in der Default-Einstellung Standardwerte vorgegeben. Wenn Sie die Schaltfläche "Endungen" betätigen, lassen sich diese Einträge in dem neu aufgerufenen Fenster ändern.

Ist diese Funktion aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "Keine Endungen" unterhalb der Schaltfläche "Endungen" angezeigt.

### {button Endungen.JI('','OPTIONEN\_SCANNER\_ENDUNG')}

Mit dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus "Programm- und Makrodateien" untersucht werden. Voreingestellt sind die gebräuchlichsten Endungen dieser Dateitypen.

## Speicher

### Speicher bei Suchstart (Alt+S)

Ist dieses Kontrollfeld markiert, wird der Hauptspeicher Ihres Computers bei jedem Suchlauf nach unerwünschtem Programmcode oder unerwünschten Programmen durchsucht.

**Wichtig:** Diese Funktion sollte immer aktiv sein, um einen größtmöglichen Schutz vor Viren bzw. unerwünschten Programmen zu erhalten. Ist ein Virus oder unerwünschtes Programm im Speicher aktiv, können alle Dateien, die durchsucht werden, unter Umständen infiziert werden. Starten Sie in diesem Fall Ihr System von einer infektionsfreien, schreibgeschützten Systemdiskette neu.

### Priorität (Alt+P)

In dem Listenfeld in dieser Gruppenbox können Sie die Priorität des Suchvorgangs zwischen "niedrig", "mittel" und "hoch" auswählen. Bei "niedrig" wird der Prozessor in langen Zeitabständen, bei "hoch" in erheblich kürzeren Abständen für einen Suchlauf freigegeben. Diese Priorität bezieht sich sowohl auf die Vordergrund- als auch auf die Hintergrundpriorität.

## In diesem Fenster sind noch folgende weitere Schaltflächen vorhanden:

### {button OK.}

Die Einträge aus dem Fenster "Suchen" werden übernommen und das Dialogfenster geschlossen.

### {button Abbrechen.}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### {button Hilfe.}

Diese Hilfe wird angezeigt.

# Suchen (Inhalt)

{button ,AL(`rtoSuchen',0,'')} siehe auch

**In diesem Menü lassen sich sowohl der Suchlauf in den markierten Laufwerken starten, als auch auswählen, was untersucht werden soll sowie AntiVir beenden.**

## **Suche starten (F2)**

Alle Laufwerke, die im Hauptfenster markiert sind, werden durchsucht.

## **Bootsektoren...**

Ein Fenster wird geöffnet, in dem Sie die Laufwerke markieren können, deren Bootsektoren durchsucht werden sollen.

## **Laufwerksliste aktualisieren (F5)**

Die in der Registerkarte Verzeichnisse angezeigte Laufwerksliste wird aktualisiert.

## **AntiVir beenden**

Beenden von AntiVir für Windows.



# Optionen/Suchen/Archive

{button ,AL('rtoAktion nach',0,','')} siehe auch

AntiVir arbeitet bei den zur Auswahl stehenden Archiven mit internen Entpack-Routinen. Die entsprechenden DOS Entpacker werden nicht benötigt.

## Archiv-Liste

In diesem Dialogfenster können Sie einstellen, welche Archive AntiVir durchsuchen soll. Sie müssen dazu die entsprechenden Einträge markieren.

## Archive durchsuchen (Alt+D)

Ist diese Option markiert, werden Archive mit den internen Entpackroutinen durchsucht.

## Alle Archiv-Typen (Alt+A)

Ist diese Option markiert, werden alle von AntiVir unterstützten Archiv-Typen aus der Liste markiert und durchsucht.

## Smart Extensions aktivieren (Alt+M)

(Nur AntiVir Professional Edition)

Ist diese Option markiert, untersucht das Programm auch solche Archive, deren Archivtypbezeichnungen abweichen. Ist beispielsweise ein ZIP-Archiv mit der Datei-Endung "XYZ" versehen, entpacken die internen Routinen auch dieses Archiv. Bei Nichtaktivierung der "Smart Extensions" würden sie das "XYZ"-Archiv ignorieren.

## Rekursionstiefe einschränken

(Nur AntiVir Professional Edition)

Die Rekursionstiefe für zu durchsuchende Archive kann frei gewählt werden. Damit ist es möglich, die Suche nach Viren sowie unerwünschten Programmen in mehrfach gepackten Archiven auf eine bestimmte, jeweils gewünschte Anzahl von Pack-Ebenen zu beschränken. Dies hilft, Zeit- und Rechnerressourcen einzusparen.

**Hinweis:** um einen Virus bzw. ein unerwünschtes Programm innerhalb eines Archivs zu ermitteln, muss der Scanner bis zu der Rekursions-Ebene scannen, in der sich der Virus bzw. das unerwünschte Programm befindet.

## Maximale Rekursionstiefe

(Nur AntiVir Professional Edition)

Um die maximale Rekursionstiefe eingeben zu können, muss die Option "Rekursionstiefe einschränken" aktiviert sein.

Sie können die gewünschte Rekursionstiefe entweder direkt eingeben oder aber mittels der Pfeiltasten rechts vom Eingabefeld ändern.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## {button OK,}

Die Einträge aus dem Fenster "Archive" werden übernommen und das Dialogfenster geschlossen.

## {button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

{button Hilfe.}

Diese Hilfe wird angezeigt.

# Optionen/Suchen/Auszulassende Dateien

{button ,AL(`rtoAktion nach',0,','')} siehe auch

Hier können Sie Dateien und Pfade eingeben, die bei der Suche nach Viren bzw. unerwünschten Programmen nicht berücksichtigt werden sollen.

**Warnung: Diese Dateien werden bei einem Suchlauf nicht berücksichtigt!**

Bitte tragen Sie hier so wenig Ausnahmen wie möglich und wirklich nur Dateien ein, die, aus welchen Gründen auch immer, bei einem normalen Suchlauf nicht geprüft werden sollen. Wir empfehlen, diese Dateien auf jeden Fall auf Viren bzw. unerwünschte Programme zu untersuchen, bevor sie in diese Liste aufgenommen werden!

**Hinweis:** Die in dieser Liste aufgenommenen Dateien werden in der Reportdatei vermerkt. Kontrollieren Sie bitte von Zeit zu Zeit die Reportdatei nach diesen nicht überprüften Dateien, denn vielleicht gibt es den Grund, aus dem Sie eine Datei hier ausgenommen haben gar nicht mehr. Dann sollten Sie den Namen dieser Datei aus dem Fenster "Auszulassende Dateien und Ordner" wieder entfernen.

Um eine Datei in diese Liste einzufügen, klicken Sie in diesem Fenster auf die Schaltfläche {button Einfügen,} oder wählen eine Datei mit Hilfe des Browsers aus, der mit der Schaltfläche {button Durchsuchen,} aufgerufen wird. Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht auf Befehl überprüft. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht gescannt.

Um einen Eintrag zu löschen, markieren Sie diesen und klicken auf die Schaltfläche {button Löschen,}.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

{button OK,}

Die Einträge aus dem Fenster "Auszulassende Dateien" werden übernommen und das Dialogfenster geschlossen.

{button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

{button Hilfe,}

Diese Hilfe wird angezeigt.

# Optionen/Suchen/Bootsektoren

(Nur AntiVir Professional)

{button ,AL('rtoAktion nach',0,'')} siehe auch

Mit Hilfe dieser Schaltfläche gelangen Sie in ein Dialogfenster, in dem Sie einstellen können, welche Bootsektoren untersucht werden sollen. Dazu muss die Einstellung "Alle Bootsektoren" im Fenster Optionen/Suchen aktiviert sein. Per Voreinstellung sind alle Laufwerktypen aktiviert.

Markieren Sie in diesem Dialogfenster die Laufwerktypen (Diskettenlaufwerke, Festplatten, Ramdisk), die untersucht werden sollen.

Mit dieser Einstellung kann beispielsweise das Durchsuchen der Diskettenlaufwerke ausgenommen werden: Häufig befinden sich keine Disketten in den Laufwerken, AntiVir muss aber trotzdem auf dieses langsame Medium zugreifen, um zu überprüfen, ob eine Diskette vorhanden ist. Diese Prüfung wird dann bei jedem Suchlauf von AntiVir durchgeführt, was deutlich Zeit kostet.

## Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:

### **{button OK,}**

Die Einträge aus dem Fenster "Bootsektoren" werden übernommen und das Dialogfenster geschlossen.

### **{button Abbruch,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

### **{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Endungen

{button ,AL('rtoAktion nach',0,'')} siehe auch

Per Voreinstellung untersucht AntiVir ausschließlich Programmdateien. Die Endungen der Programmdateien (Extensions) werden in der Liste im Fenster "Dateiendungen" angezeigt. Die Liste in diesem Fenster enthält die Endungen der gebräuchlichsten Programmdateien sowie Dokumente, die Makros enthalten können. Haben Sie Programmdateien oder Dokumente mit anderen Endungen auf Ihrem Rechner installiert, fügen Sie diese Extensions in die Liste mit Dateiendungen ein (Schaltfläche Einfügen betätigen).

Geben Sie bitte keine Endungen von nicht ausführbaren Dateien ein; dies würde die Suchleistung von AntiVir beeinträchtigen.

## Folgende Schaltflächen sind im Fenster "Dateiendungen" vorhanden:

### {button OK,}

Die Einträge aus dem Fenster "Dateiendungen" werden übernommen und das Dialogfenster geschlossen.

### {button Abbruch,}

Das Dialogfenster wird geschlossen, ohne die aktuellen Einstellungen zu übernehmen.

### {button Einfügen,}

Einfügen einer neuen Dateiendung. Siehe unter Einfügen.

### {button Löschen,}

Markierte Dateiendungen werden aus der Liste gelöscht. Dateien mit diesen Endungen werden nicht mehr auf Befehl überprüft.

### {button Standard,}

Diese Schaltfläche setzt die Liste wieder auf die Voreinstellungen zurück, wie sie bei AntiVir von uns ausgeliefert werden. Diese Liste der Standarderweiterungen kann sich ändern, wenn beispielsweise neuartige Virentypen auftreten (Siehe READ.ME).

**Hinweis:** Änderungen der Liste und eigene Einträge gehen durch das Zurücksetzen auf die Voreinstellung verloren.

### {button Hilfe,}

Diese Hilfe wird angezeigt.

# Endungen/Einfügen

{button ,AL(`rtoAktion nach',0,','')} siehe auch

Wird die Schaltfläche "Einfügen" betätigt, erscheint ein Dialogfenster, in dem Sie Dateiendungen für die Suche von AntiVir eingeben können. Es werden maximal 255 Zeichen akzeptiert, der führende Punkt wird nicht mit eingegeben. Ein ungültiges Zeichen wird nicht akzeptiert. Wildcards (\* und ?) sind als Stellvertreter erlaubt.

Ist in der Anzeigegruppe "Dateien" die Einstellung "Programm- und Makrodateien" bzw. "Programmdateien" ausgewählt, werden nach Bestätigung mit "OK" ab dem nächsten Suchlauf Dateien mit der neu eingetragenen Endung ebenfalls geprüft.

## **Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

{button OK,}

Die Daten aus diesem Fenster werden übernommen und das Dialogfenster wird geschlossen.

{button Abbrechen,}

Das Dialogfenster wird geschlossen, ohne den aktuellen Eintrag zu übernehmen.

{button Hilfe,}

Diese Hilfe wird angezeigt.

# Tools/Systemdateien sichern

(Nur AntiVir Professional Edition)

{button ,AL('rtoTools',0,'','')} siehe auch

Mit Hilfe dieses Dialogfensters können Sie die Systemdateien, den Bootsektor des Laufwerks C: und das CMOS sichern. Diese Daten werden in dem Verzeichnis SYSSAVE unterhalb des AntiVir Installationsverzeichnis gesichert.

## Bootsektor des Laufwerks C: (Alt+B)

Markieren Sie diesen Eintrag, um den Bootsektor des Laufwerks C: in das Verzeichnis SYSSAVE unterhalb des Installationsverzeichnis von AntiVir zu übertragen. Der Sektor wird in der Datei BootRecC.DAT gesichert.

## Systemdateien (Alt+Y)

Ist dieser Punkt markiert, werden alle Systemdateien aus dem Rootverzeichnis des Laufwerks C: in das Verzeichnis SYSSAVE unterhalb des Installationsverzeichnis übertragen. Zu den Systemdateien gehören alle Dateien mit dem Systemflag (außer Auslagerungsdateien!). Folgende Dateien werden immer kopiert, auch wenn das Systemflag nicht vorhanden ist:

COMMAND.COM  
IO.SYS  
MSDOS.SYS  
AUTOEXEC.BAT  
CONFIG.SYS

## CMOS (Alt+C)

Der Inhalt des CMOS wird in das Verzeichnis SYSSAVE unterhalb des Programmverzeichnis von AntiVir kopiert.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

## {button Sichern.}

Die Einträge aus dem Fenster "Systemdateien sichern" werden übernommen und das Dialogfenster geschlossen.

## {button Abbruch.}

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

## {button Hilfe.}

Diese Hilfe wird angezeigt.

# Tastaturbefehle

Mit den folgenden Tastaturbefehlen und Tastenkombinationen werden die entsprechenden AntiVir-Funktionen aktiviert:

- F1** Hilfe aufrufen
- F2** Suche starten
- F5** Laufwerke aktualisieren
- ESC** Dialogfenster schließen
- Alt+F4** AntiVir für Windows beenden



# Tools (Inhalt)

{button ,AL(`rtoTools',0,`,`')}\_ siehe auch

## **AntiVir bietet in diesem Menü folgende Hilfsmittel:**

### **Systemdateien sichern...**

(Nur AntiVir Professional Edition)

Mit diesem Menüpunkt wird ein Dialogfenster aufgerufen, in dem Sie auswählen können, ob Sie den Bootsektor des Laufwerks C:, die Systemdateien aus dem Hauptverzeichnis des Laufwerks C: sowie den Inhalt des CMOS im Verzeichnis SYSSAVE unterhalb des Programmverzeichnisses von AntiVir sichern wollen.

### **Scheduler...**

startet den Scheduler von AntiVir.

### **Erkennungsliste...**

zeigt die Namen der Viren und unerwünschten Programme an, die AntiVir erkennt.

### **Vireninformation...**

ruft eine Windows-Hilfdatei auf, in der Vireninformationen zu finden sind.

### **Intranet Update starten**

(Nur AntiVir Professional Edition)

Mit diesem Menüpunkt sucht der Intranet-Update Wizard sofort im angegebenen Quellverzeichnis nach aktualisierten Programmdateien.

Hilfe zur Konfiguration finden Sie unter Optionen/Intranet Updater.

### **Internet Updater starten**

Mit diesem Menüpunkt können Sie den AntiVir Internet Updater starten. Mit diesem können Sie sich neue Updates aus dem Internet laden.

Hilfe zur Konfiguration finden Sie unter Optionen/Internet Updater.

### **Lizenzdatei lesen...**

(Nur AntiVir Professional Edition)

liest die Lizenzdatei ein, um aus einer Demoversion eine registrierte Vollversion zu machen.

### **VDF Datei aktualisieren...**

(Nur AntiVir Professional Edition)

Mit dieser Funktion wird das Standard-Fenster zur Auswahl einer Datei geöffnet, und zwar im Programmordner von AntiVir.

## Update Wizard

(Nur AntiVir Professional Edition)

Zur Update-Versorgung der Arbeitsplatzrechner in einem Netzwerk haben wir den Intranet-Update Wizard entwickelt. Diese Funktion steht Ihnen nur bei einer AntiVir-Mehrfachlizenz (ab 3 Usern) zur Verfügung.

Dieses Hilfsprogramm sorgt bei entsprechender Konfiguration dafür, dass sich Ihre Arbeitsplatzrechner automatisch selber mit den neuesten Updates von AntiVir versorgen. Der Update Wizard wird hierbei bereits bei der Installation in den RUN-Key der Windows-Registry eingetragen und überprüft bei jedem Anmelden an das System, ob neue AntiVir-Programme oder neue Signaturen von Viren oder unerwünschter Programme in einem bestimmten Verzeichnis auf einem bestimmten Server vorliegen.

Nähere Informationen zur Installation des Intranet-Update Wizard befindet sich auf der AntiVir CD-ROM in der Datei

[\[sprache\]/PRODUCTS/WIN9X/SETUP/DISK\\_1/ADMIN.HTM](#)

# Verdächtiges Makro gefunden

AntiVir hat in einem Dokument ein verdächtiges Makro entdeckt und Sie haben unter Optionen/Makroviren eingestellt, dass AntiVir nachfragt, was mit diesem Makro geschehen soll.

Sie können in dem Fenster unter folgenden Möglichkeiten wählen:

## Dieses Makro löschen

AntiVir löscht das verdächtige Makro. Handelt es sich bei dem Makro um einen Virus oder einen Teil eines Virus, so ist dieser nicht mehr funktionsfähig.

## Alle verdächtigen Makros löschen

Es werden alle verdächtigen Makros im Dokument ohne Nachfrage gelöscht.

**Achtung:** Selbst erstellte Makros gehen möglicherweise verloren.

## Alle Makros löschen

Es werden alle Makros im Dokument ohne Nachfrage gelöscht.

**Achtung:** Selbst erstellte Makros gehen möglicherweise verloren.

## Makro nicht löschen

Das verdächtige Makro wird nicht gelöscht.

**Vorsicht:** Ist diese Einstellung aktiviert, verbleiben infizierte Daten auf Ihrem Computer!

## Diese Datei überspringen

AntiVir beendet die Überprüfung des Dokuments.

**Vorsicht:** Ist diese Einstellung aktiviert, verbleiben infizierte Daten auf Ihrem Computer!

# Vireinfo

Aktuelle Informationen zu Viren finden Sie entweder unter dem Menüpunkt Tools/Vireninformationen oder aber im Internet unter [www.antivir.de](http://www.antivir.de).

An dieser Stelle finden Sie Informationen über zwei Viren, die in letzter Zeit für Aufsehen gesorgt haben: dies sind zum einen der [ExploreZip Virus](#) und zum anderen der [CIH Virus](#).

## Erkennung des ExploreZip-Virus durch AntiVir

### Allgemeine Informationen:

#### **W32/ExploreZip (in unseren Produkten gelistet unter Tr.ExploreZip.Worm)**

<b>Alias:</b>	Worm.Explore.Zip Zipped Files Troj.Explore.Zip
<b>Merkmale:</b>	Trojanisches Pferd, Wurm
<b>Textstring:</b>	zipped_files
<b>Länge:</b>	210432 Bytes
<b>Plattform:</b>	Windows 9x/Windows NT

W32/ExploreZip verbreitet sich über E-Mail auf Windows 9x- und Windows NT-Rechnersystemen. Als E-Mailprogramm kommt jeder MAPI-fähige E-Mail-Client in Betracht. Hierzu gehören unter anderem:

- MS Outlook
- NetScape Mail
- MS Exchange
- Outlook Express

Im aktiven Zustand verteilt er sich über MAPI-Kommandos weiter, indem er sich selbst als Attachment mit dem Namen "zipped\_files.exe" versendet. Im Gegensatz zu Melissa versendet sich W32/ExploreZip selbständig an die Adressen unbeantworteter E-Mail im Posteingang. Melissa hingegen verschickte Kopien von sich selbst an bis zu 50 Empfänger aus dem Adreßbuch.

Durch diesen Trick sieht die E-Mail beim Empfänger ganz unverfänglich aus. Ist sie doch eine Antwort auf die - an einen bekannten Empfänger - versandte Nachricht.

Eine infizierende E-Mail sieht folgendermaßen aus:

From: *[Name des Email-Absenders]*

Subject: re: *[Subject der unbeantworteten Nachricht]*

To: *[Name des Email-Empfängers]*

Hi *[Name des Email-Empfängers]* !

I received your email and I shall send you a reply ASAP.

Till then, take a look at the attached zipped docs.

Bye oder sincerely

*[Name des Email-Absenders]*

Attachment: zipped\_files.exe

Zu diesem Zeitpunkt ist der Virus aber schon aktiv und "arbeitet". Er kopiert sich selbst entweder unter dem Namen "Explore.exe" oder "\_setup.exe" in das jeweilige System-Verzeichnis. Dies ist %windir%\System (üblicherweise c:\windows\system) unter Windows 9x, bzw. %windir%\System32 (üblicherweise c:\winnt\system32) unter Windows NT.

Anschließend modifiziert er die WIN.INI unter Windows 9x, bzw. die Registry unter Windows NT. Durch die Modifikation der INI-Datei, bzw. der Registry erreicht der Virus, daß er bei jedem Hochfahren des Systemes erneut gestartet wird. Hierdurch hat er die Möglichkeit, auch neue Posteingänge entsprechend zu beantworten.

In seiner Schadensroutine ist der Virus multi-threading-fähig: Er erzeugt zwei "Killer-Threads". Einer der Threads sorgt für die "E-Mail-Behandlung", ein anderer Thread ist für das "Leeren" der Dateien zuständig. Der erste Thread überwacht via MAPI neue Posteingänge. Durch das Überwachen neuer Posteingänge "beantwortet" der Virus eingegangene E-Mails sofort wieder mit sich selbst. Bestehende, bisher ungelesene Nachrichten werden ebenfalls sofort beantwortet.

Ein zweiter Thread "leert" Dateien mit folgenden Extensions ".doc, .c, .cpp, .h, .asm, .xls und .ppt". Das "Leeren" ist ein Kürzen der Dateien über die Windows-Funktion "CreateFile" auf 0 Byte! Durch diesen Vorgang werden Dateien nicht gelöscht und stehen auch nicht für eine Wiederherstellung über den Papierkorb zur Verfügung. Die gekürzten Dateien können nicht wiederhergestellt werden, da der Inhalt verlorengegangen ist.

Das Leeren von Dateien läßt sich auch an einer verstärkten Festplattenaktivität feststellen. Doch der Virus leert auch solche Dateien, die über "gemappte" Laufwerke bis hin zum Laufwerksbuchstaben "Z:" als Netzwerklaufwerke zur Verfügung stehen (WnetEnumResource).

Die Schadensroutine des Virus ist solange aktiv, wie auch der Virus selbst im Speicher ist.

Der Virus kann jedoch recht einfach durch Löschen der infektiösen Dateien und Modifizieren der WIN.INI bzw. Registry entfernt werden.

#### **Entfernen der Autostart-Einträge unter Windows 9x:**

Entfernen aus der WIN.INI (mittels SysEdit) durch Löschen folgender Zeile:

```
run=C:\WINDOWS\SYSTEM\Explore.exe
```

```
(run=%windir%\SYSTEM\Explore.exe)
```

oder

```
run=C:\WINDOWS\SYSTEM\_setup.exe
```

```
(run=%windir%\SYSTEM\_setup.exe)
```

#### **Entfernen der Autostart-Einträge unter Windows NT:**

Entfernen eines Keys aus folgendem Registry-Pfad (mittels RegEdit):

```
HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows
```

Hier muß unter \Run folgender Eintrag gelöscht werden:

```
run=C:\WINNT\SYSTEM32\Explore.exe
```

```
(run=%windir%\SYSTEM32\Explore.exe)
```

bzw.

```
run=C:\WINNT\SYSTEM32\_setup.exe
```

```
(run=%windir%\SYSTEM32\_setup.exe)
```

#### **Entfernen der infizierten Datei unter Windows 9x:**

Nach einem Neustart oder einem "Abschießen" des Virus über den Taskmanager sollte der Virus selbst gelöscht werden. Die Datei befindet sich unter dem Namen "Explore.exe" oder "\_setup.exe" unter:

```
c:\windows\system\Explore.exe
```

bzw.

```
c:\windows\system\_setup.exe
```

#### **Entfernen der infizierten Datei unter Windows NT:**

Die Pfade für Windows NT sind (nach Neustart oder "Abschießen"):

```
c:\winnt\system32\Explore.exe
```

bzw.

```
c:\winnt\system32\_setup.exe
```

Es kann daher nicht oft genug vor E-Mails mit unbekanntem Dateianhängen gewarnt werden. Es ist auch eher unüblich, daß Dokumente als selbstextrahierende .EXE-Dateien versandt werden. Anwender sollten mit geeigneten Antivirenprogrammen - auch zur Vorsorge - einmal alle Dateien eines Rechnersystems untersuchen. Es werden dann auch die temporären Dateien der diversen E-Mailprogramme untersucht und die darin gespeicherten Viren ggf. entdeckt.

Darüber hinaus zeigt dieser Virus mit seinem aggressiven Schadensteil wieder einmal deutlich, wie durch sinnvolle Rechtevergabe in Netzwerken die Schäden hätten begrenzt werden können.

#### **Allgemeine Informationen über den W95/CIH Virus:**

Name: W95/CIH  
 Alias: PE\_CIH, CIH  
 Merkmale: Resident, PE-Infector (Windows-EXE)  
 Textstring: Version 1.2 CIH v1.2 TTIT  
               Version 1.3 CIH v1.3 TTIT  
               Version 1.4 CIH v1.4 TATUNG  
 Länge: Version 1.2 1003 Bytes  
           Version 1.3 1010 Bytes  
           Version 1.4 1019 Bytes  
 Plattform: Windows 95/Windows 98

W95/CIH ist ein residenter Virus, der Windows-Programme (PE-Dateien) befällt. Er infiziert PE-Dateien derart, daß die Länge infizierter Dateien nicht verändert wird. Anhand der Kenntnisse über unbenutzte Bereiche innerhalb dieser PE-Dateien kann er sich in mehrere Teile aufteilen. W95/CIH enthält destruktive Schadensroutinen: Überschreiben des BIOS im Flash-ROM und Überschreiben aller Festplatten.

Dieser Virus ist in der letzten Zeit verstärkt auch in Deutschland aufgetreten. Die H+BEDV Datentechnik GmbH stellte bereits mit der Version 5.13.1 eine wirksame und leistungsfähige Sucherkennung zu Verfügung. Seit der Version 5.13.2 ist nun auch die Reparatur dieses Virus möglich. AntiVir geht hier den nicht sonst üblichen Weg, nur den Ladeteil des Virus zu deaktivieren ("Metzgermesser-methode"), sondern es erfolgt eine Reparatur nach der "Skalpelmethode". Da sich W95/CIH bei der Infektion einer Datei selbst in verschiedene Teile aufteilt und über verschiedene Sektionen in der zu infizierenden Datei verstreut, müssen bei einer Reparatur alle vom Virus veränderten Sektionen gesondert behandelt werden. Dadurch läuft AntiVir nicht Gefahr, Teile des Virus intakt zu lassen.

Viele andere Antivirenprogramme überschreiben nur die Installationsroutine des Virus oder "reparieren" allein durch Berichtigen des Programmeinsprunges. So verbleiben andere Teile des Virus in der eigentlich immer noch infizierten Datei in ausführbarer Form. Dies bedeutet, daß auch die Schadensroutinen noch in der Datei vorhanden sind und ggf. auch unkontrolliert (z.B. durch Programmabsturz, Fehler im Wirtsprogramm, Doppelinfektion etc.) ausgeführt werden können.

Da AntiVir genaue Kenntnisse sowohl über den Aufbau des Virus als auch den Aufbau der PE-Dateien besitzt, ist es AntiVir möglich, eine Qualitätsreparatur durchzuführen. AntiVir entfernt die einzelnen Teile des Virus in den unterschiedlichen Sektionen und stellt die internen Verwaltungsinformationen der Sektionen wieder her. Hierdurch sind diese Programme nach Reparatur durch AntiVir wieder gefahrlos einsetzbar.

Die Schadensroutinen des Virus variieren je nach Version. Die Version 1.2 versucht am 26. April und die Version 1.3 am 26. Juni eines jeden Jahres das BIOS im Flash-ROM zu überschreiben. Die Version 1.4 - sie ist momentan die am häufigsten festgestellte Version - scheint eine Weiterentwicklung zu sein: Sie versucht das Überschreiben des BIOS im Flash-ROM am 26. eines jeden Monats durchzuführen. Allen Versionen ist gemeinsam, daß auch noch alle Festplatten am jeweiligen Auslösedatum durch direkte Zugriffe überschrieben werden. Damit dürften die meisten Notfalldisketten wertlos sein, wenn nicht zusätzlich ein komplettes Backup vorliegt!

# Virus gefunden

## AntiVir hat einen Virus bzw. sonstige Malware gefunden.

Sie brauchen sich in der Regel keine Sorgen zu machen, wenn AntiVir oder der AntiVir Guard im Alltagsbetrieb einen Virus findet: die Viren werden entsprechend der AntiVir-Konfiguration entweder mit oder ohne Rückfrage entfernt (auf welche Art und Weise AntiVir infizierte Dateien behandeln kann, finden Sie in der Beschreibung der Optionen).

Trifft AntiVir während der Installation oder beim Programmstart auf einen **aktiven Virus im Speicher**, wird in einer nicht zu übersehenden Meldung darauf hingewiesen.

In diesem Fall werden Sie gebeten, von einer schreibgeschützten Systemdiskette (entweder der "bekanntermaßen guten DOS-Diskette", einer bootfähigen Windows-Startdiskette oder der bootfähigen AntiVir CD-ROM) zu booten.

Und wenn Ihnen dieser konkrete Virenverdacht gemeldet wurde: **Führen Sie keinen Warmstart, beispielsweise mit der "finalen Geierkralle" (Strg)+(Alt)+(Entf) oder einem Boot-Programm aus, einige residente Viren können dies überleben.** Stellen Sie sicher, dass Sie nur Programme von den Notfall- bzw. Systemdisketten starten. Die Programme auf den Festplatten - also auch die Windows-Systemdateien - können bereits infiziert sein.

## Wenn AntiVir für Windows nicht installiert oder gestartet werden kann:

Der einfachste (und meistens auch erfolgreiche) Weg ist die Virenbeseitigung mit dem Programm AVE32.EXE (Windows NT: AVNT.EXE):

1. Machen Sie ein Backup der fraglichen Datenträger - besser ein Backup mit Virus als gar keines.
2. Starten Sie Ihren Rechner unter **Windows 95/98** von der bekanntermaßen guten DOS-Diskette. Besitzen Sie keine "bekanntermaßen gute DOS-Diskette", können Sie auch - soweit vorhanden - die Original-DOS-Installationsdiskette verwenden. Es fehlen Ihnen dann einige Systemdateien und Hilfsprogramme, die Ihnen das Leben leichter machen können. Ein Start von der Windows Startdiskette ist ebenfalls möglich.

Unter **Windows XP (XP&2000&NT)** starten Sie bitte Ihren Rechner von der "bekanntermaßen guten Windows-Startdiskette".

Greifen Sie während des Systemstarts **nicht** auf die Festplatte zu, alle dort gespeicherten \*.COM-, \*.EXE- sowie die übrigen ausführbaren Dateien können bereits infiziert sein.

3. Legen Sie nach dem Neustart, falls nicht bereits geschehen, die AntiVir CD-ROM in das CD-Laufwerk und Ihre Lizenzdiskette mit der Datei HBEDV.KEY in das 3 1/2" Laufwerk ein. Für den Fall, dass Sie die Lizenzdatei (HBEDV.KEY) per Email erhalten haben, sollten Sie sich diese für "den Notfall" auf eine Diskette kopieren.
4. Die Treiber für Ihr CD-Laufwerk. (meistens ein \*.SYS-Treiber des Herstellers für die CONFIG.SYS und die MSCDEX.EXE Ihrer DOS-Version für die AUTOEXEC.BAT) müssen vorhanden und aktiviert sein. Gegebenenfalls müssen diese Treiber installiert werden.

5. Rufen Sie unter DOS auf der CD-ROM unter [sprache]\PRODUCTS\CMDPROGS\ das Programm AVE32 im Verzeichnis AVE32\SETUP mit dem Parameter /ALLHARD auf. Das Programm AVNT finden Sie unter [sprache]\PRODUCTS\CMDPROGS\AVNT\SETUP

Die Befehlszeile sollte folgendermaßen aussehen:

```
X:\...\ANTIVIR\AVE32.EXE /ALLHARD bzw.
```

```
X:\...\ANTIVIR\AVNT.EXE /ALLHARD
```

Das "X:" steht für den Laufwerksbuchstaben des CD-Laufwerks, in dem sich die AntiVir CD-ROM

befindet.

6. Bestätigen Sie diese DOS-Befehlszeile mit der Taste "Return".  
AVE32 (AVNT) wird nun ohne weitere Eingaben alle Dateien in allen Unterverzeichnissen auf allen erreichbaren Laufwerken sowie alle Bootsektoren ab Laufwerk A: testen. **Eventuell gefundene Viren werden in diesem Modus nicht gelöscht. Besondere Vorkommnisse, beispielsweise eine zerstörte Datei oder ein Virus, werden im Reportfenster von AVE32 (AVNT) vermerkt.**
7. Werden infizierte Dateien gemeldet, sollten Sie mit AVE32 (AVNT) einen Reparaturlauf mit dem Parameter /e durchführen. **Beachten Sie hier, dass nicht reparable Dateien bei diesem Durchgang gelöscht werden.** Hier sollten Sie sicherstellen, dass Sie diese infizierten Dateien nicht mehr benötigen. Ist Ihnen ein Programm mit Menüsteuerung und Mausbedienung sympathischer, können Sie auch AntiVir für DOS installieren und die infizierten Dateien mit diesem Programm reparieren.  
Haben Sie diese Prozedur erfolgreich abgeschlossen, lässt sich AntiVir in der Regel problemlos installieren bzw. starten.
8. Starten Sie sofort nach der Installation von AntiVir einen Suchlauf in allen erreichbaren Laufwerken durch Anklicken der Schaltfläche "Suchen".  
Wurde kein Virus im Speicher mehr gefunden, jedoch immer noch infizierte Dateien gemeldet, empfehlen wir, alle Programmdateien *aller* vorhandenen Laufwerke und Datenträger auf Virenbefall zu überprüfen. Denn einige Viren verbreiten sich nicht nur auf dem aktuellen Laufwerk, sondern gelangen auch auf andere Datenträger, mit Vorliebe auf Disketten und andere beschreibbare Datenträger (CD-R, CD-RW, ZIP, MO, ...) sowie auf Netzlaufwerke.
9. Sehen Sie in der Reportdatei nach, ob virulente Dateien entfernt wurden oder ob sich einige Dateien nicht reparieren ließen.
10. Wurden alle Dateien erfolgreich wiederhergestellt und die zerstörten Dateien gelöscht, ist Ihr Rechner virenfrei.  
Haben Sie zerstörte Dateien nicht gelöscht, kann der Virus beim Aufruf dieser Datei - wenn diese noch lauffähig ist - aktiviert werden und sich erneut verbreiten. Behandeln Sie diese Dateien mit äußerster Vorsicht. Wir empfehlen, diese Dateien auf jeden Fall zu löschen und die Dateien von den Originaldisketten oder einem virenfreien Backup neu auf die Festplatte zu kopieren bzw. zu installieren.

Bricht AntiVir für Windows die Installation auch nach der Virenbeseitigung mit AVE32.EXE (AVNT) immer noch ab bzw. lässt sich AntiVir nicht starten, führt ein zweiter, zeitintensiver Weg zur Lösung eines Virenproblems über eine temporäre Windows-Version:

- a) Starten Sie von einer nicht infizierten Windows-Startdiskette.  
Besitzen Sie keine "bekanntermaßen gute Windows-Diskette", empfehlen wir, Windows von den schreibgeschützten Originaldatenträgern in einem temporären Verzeichnis neu zu installieren - auch wenn das eine Menge Arbeit bedeutet.  
**Starten Sie Windows auf keinen Fall von der Festplatte aus**, es sind vielleicht schon einige Windows-Dateien infiziert.
- b) Benennen Sie die Datei `SYSTEM.INI` im Ordner `WINDOWS` um, beispielsweise in `SYSTEM.VIR` (verwenden Sie dabei bitte keine gängigen Extensions von Programmen oder Dokumenten und schreiben Sie sich den neuen Namen sicherheitshalber auf). Sonst startet Windows zuerst die alte, infizierte Version. Damit der alte Windows-Ordner nicht von der neuen Windows-Version gefunden wird, können Sie den auch umbenennen, beispielsweise in `WINOLD`.
- c) Legen Sie ein temporäres Verzeichnis an (beispielsweise `TEMPWIN`) (dieser Schritt ist hier nicht



zwingend erforderlich; Sie müssen sonst dem Ordner, in den das temporäre Windows installiert werden soll, bei der Installation einen anderen Namen geben)

- d) Installieren Sie eine minimierte Windows-Version von der Original Windows-CD-ROM in den temporären Ordner (Sie werden irgendwann von Windows gefragt, in welchen Ordner Windows kopiert werden soll, und hier müssen Sie den Laufwerksbuchstaben und den Namen des temporären Ordners korrekt eintragen).
- e) Starten Sie Windows aus diesem Verzeichnis heraus.  
Stellen Sie **sicher, dass sie nur die Programme und Hilfsprogramme aus diesem Verzeichnis** heraus starten. Alle übrigen Programme auf dem Laufwerk könnten bereits infiziert sein.
- f) Installieren Sie AntiVir von der AntiVir CD-ROM neu.
- g) Bestätigen Sie die Nachfrage, ob Ihre Festplatte nach Viren durchsucht werden soll, mit "Ja".
- h) Rufen Sie nach erfolgreich abgeschlossener Installation AntiVir auf.
- i) Unter dem Menüpunkt Optionen/Reparatur können Sie auswählen, ob Sie sich die Reparatur jeder infizierten Datei bestätigen oder nicht bestätigen lassen wollen.
- k) Starten Sie einen Suchlauf durch Anklicken der Schaltfläche "Suchen"  
Wurde kein Virus im Speicher gefunden, jedoch infizierte Dateien gemeldet, empfehlen wir, alle Programmdateien *aller* vorhandenen Laufwerke und Datenträger auf Virenbefall überprüfen. Denn einige Viren verbreiten sich nicht nur auf dem aktuellen Laufwerk, sondern gelangen auch auf andere Datenträger, mit Vorliebe auf Disketten und andere wiederbeschreibbare Datenträger sowie auf Netzlaufwerke.
- l) Sehen Sie in der Reportdatei nach, ob alle Viren repariert wurden oder ob sich einige Dateien nicht reparieren ließen.  
  
Wurden alle Dateien erfolgreich repariert und die zerstörten Dateien gelöscht, ist Ihr Rechner virenfrei. Haben Sie zerstörte Dateien nicht gelöscht, kann der Virus beim Aufruf dieser Datei - wenn diese noch lauffähig ist - aktiviert werden und sich erneut verbreiten. Behandeln Sie diese Dateien mit äußerster Vorsicht. Wir empfehlen, diese Dateien auf jeden Fall zu löschen und die Dateien von den Originaldisketten oder einem virenfreien Backup neu auf die Festplatte zu kopieren bzw. zu installieren.
- m) Sind Sie sicher, dass kein Virus mehr auf Ihrem Rechner sein Unwesen treibt, können Sie den alten Windows-Ordner wieder zurückbenennen und ebenfalls die SYSTEM.INI auf ihren alten Namen umbenennen. Beim nächsten Neustart wird Windows zuerst in diesem Ordner nachsehen, ob sich dort eine SYSTEM.INI befindet. Ist dies der Fall, startet die alte, mit AntiVir reparierte Windows-Version mit dem von Ihnen mühsam eingerichteten Desktop. Zum Schluss müssen Sie nur noch die temporäre Windows-Version von Ihrem Rechner entfernen - den Speicherplatz können Sie sicher besser verwenden.

Nach dem nächsten Start von Windows kann es passieren, dass Sie AntiVir nicht mehr von Ihrer wiederhergestellten Windows-Version starten können. In diesem Fall müssen Sie die Konfiguration der restaurierten Windows-Version anpassen (neues Icon, AVShell nachinstallieren) oder am besten gleich AntiVir neu installieren (bitte vorher die alte Version mit UNINSTALL entfernen oder während des Setups die Option "Nur neue Dateien" im Konfigurationsfenster abwählen).

# Wichtige Hinweise



Erstellen Sie auf einem garantiert virenfreien Rechnersystem eine bekanntermaßen gute DOS-Diskette, indem Sie eine Diskette frisch mit "format a: /s /u" formatieren. Bitte kopieren Sie die wichtigen Programme, wie man sie von FORMAT.EXE bis zu KEYB.COM alle braucht. Versehen Sie die Diskette mit einem Schreibschutz und bewahren sie sie gut auf.



Seit Anfang 1999 ist die AntiVir CD-ROM bootfähig, die "bekanntermaßen gute DOS-Diskette" ist für einen Neustart in einer garantiert malwarefreien Umgebung in den meisten Fällen nicht mehr erforderlich. Und das hat es mit dieser bootfähigen CD-ROM auf sich:



Nach einer Virusinfektion der Boot- und Master-Bootsektoren auf FAT16- bzw. FAT32-Laufwerken ist möglicherweise das Betriebssystem nicht mehr startfähig. Mit dem AntiVir Rescue System auf der bootfähigen CD-ROM von der H+BEDV Datentechnik GmbH können diese infizierten Sektoren ohne Verwendung eines externen Betriebssystems repariert werden.



Zusätzlich zur Reparatur in den Bootbereichen lassen sich auch alle Dateibereiche auf FAT16- bzw. FAT32-Laufwerken unmittelbar nach dem Start von der AntiVir CD-ROM (Bestandteil des Komfortpaketes - Info: [www.antivir.de](http://www.antivir.de)) aus scannen.



Als Read-Only Medium stellt diese CD-ROM eine Überprüfung unter garantiert malwarefreier Umgebung sicher. Bisher war hierzu immer eine "bekanntermaßen gute DOS-Diskette" erforderlich. Doch entweder wurde diese vorher nicht auf einem garantiert malwarefreien System erstellt oder sie ist nicht auffindbar. Mit der von der H+BEDV Datentechnik GmbH entwickelten selbstbootenden AntiVir CD-ROM sind Sie dieser Sorge enthoben.



Da sich die AntiVir-Programme ebenfalls auf der CD-ROM befinden, lässt sich das infizierte Betriebssystem nun mit AntiVir reparieren. Das bisher zeitraubende Nachladen der Programme von Disketten entfällt.



Ein Bootmanager auf der CD-ROM ermöglicht es, auf Standardsystemen wahlweise von der CD-ROM oder wie gewohnt von der Festplatte zu starten, ohne dass hierzu die CD-ROM aus dem Laufwerk entfernt werden muss.

Weiter Informationen finden Sie auf der Seite [Häufig gestellte Fragen](#).

## Hilfe

Diese Hilfe wird angezeigt.

# Optionen/Unerwünschte Programme

{button ,AL('rtoAktion nach',0,',')} siehe auch

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 Meldungen 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.

**Folgende Schaltflächen sind in diesem Dialogfenster vorhanden:**

**{button OK,}**

Die Einträge aus dem Fenster "Unerwünschte Programme" werden übernommen und das Dialogfenster geschlossen.

**{button Abbrechen,}**

Das Dialogfenster wird geschlossen, ohne die neuen Einstellungen zu übernehmen.

**{button Hilfe,}**

Diese Hilfe wird angezeigt.

# Viren sowie sonstige Malware

## Malware

Malware (malicious software) ist die Sammelbezeichnung für alle Arten von Programmen mit Schadfunktionen. Charakteristisch für Malware ist, dass sie verdeckte Funktionen enthält, die durch Löschen, Überschreiben oder Manipulation unkontrollierbare Schäden in EDV-Systemen oder in Datenbeständen auslösen können. Malware verursacht zusätzlichen Arbeitsaufwand und Kosten, beeinflusst Vertraulichkeit und Verfügbarkeit von Programmen und Daten negativ und ist z. T. in der Lage, sich selbstständig weiterzuverbreiten.

Zur Kategorie der Malware gehören u. a. Viren (zum Beispiel Access-Viren, Active-X-Viren, AmiPro-Viren, Batchviren, Boot- und Master-Bootsektorviren, Companion-Viren, Dateiviren, DOC-Viren in RTF-Dateien, Dropper, Email-Viren, Excel-Makroviren, File-System-Viren, Gepackte Viren, HTML-Viren, Java-Viren, Linux-Viren, Macintosh-Viren, Multi-Partite-Viren, OS/2-Viren, PDA-Viren, polymorphe Dateiviren, polymorphe Makroviren, PowerPoint-Makroviren, Scriptviren, Stealth-Viren, TSR-Viren, Viren in Embedded OLE, Viren in laufzeitkomprimierten Dateien, Viren in Shell-Scrap-Dateien, Visio-Viren, Word-Makroviren), Trojaner (u. a. Logische Bomben) oder Würmer.

## Viren

Ein Computervirus ist ein Programm, welches die Fähigkeit besitzt, sich nach seinem Aufruf selbstständig an andere Programme auf irgendeine Weise "anzuhängen", diese also zu infizieren. Viren vervielfältigen sich selbst, was sie von Trojanern und Bomben unterscheidet. Dabei müssen sie nicht zwangsläufig zerstörerische Programmteile in sich tragen. Ein Computervirus benötigt grundsätzlich fremden Code (Wirtscodes), dessen Ablauf der Virus durch das Infizieren verändert. Die Wirte dienen lediglich als Transportmittel, der Ablauf des Wirtscodes wird nicht geändert.

Die hier vorgestellte Definition entspricht der der deutschen Viren-FAQ (Frequently Asked Questions) von Martin Rösler.

## Würmer

Der Begriff "Wurm" existiert in zwei Bedeutungen.

Die erste Definition lautet: "Programm, welches sich innerhalb von Netzwerken selbst vervielfältigt und Rechenzeit stiehlt". Dies geschieht beispielsweise auf vernetzten Mainframes durch Prozessgabelung.

Eine zweite Erklärung lautet: ein Wurm ist ein Programm, welches sich selbst vervielfältigt, dabei jedoch keinerlei Wirtscodes infiziert. Ein Beispiel wäre ein Programm WURM.COM, welches Befehle enthält, sich selbst auf alle vorhandenen Laufwerke in die aktiven Ordner zu kopieren. Würmer können somit nicht Bestandteil anderer Programmabläufe werden und sind nur dann eine Gefahr, wenn sie auf Multitasking-Systemen selber eine andere Task erzeugen und sich darin auch selber aktivieren können, da sonst immer der Mensch an der Verbreitung eines Wurmes beteiligt sein muss, indem er ihn startet.

Die hier vorgestellte Definition entspricht der der deutschen Viren-FAQ (Frequently Asked Questions) von Martin Rösler.

## Trojaner

Ein trojanisches Pferd oder Trojaner ist ein Programm, welches vorgibt, eine nützliche Funktion zu haben. Nach dem Aufruf zeigt es jedoch sein wahres Gesicht und beginnt sein meist zerstörerisches Werk.

Trojaner können sich nicht selber verbreiten, was sie von Viren und Würmern unterscheidet. Die meisten Trojaner sind Programme mit einem unscheinbaren oder sehr interessanten Namen (STARTME.EXE oder SEX.EXE), die unmittelbar nach der Ausführung aktiv werden und z.B. die Festplatte formatieren oder Daten durcheinanderbringen. Eine spezielle Art eines Trojaners ist ein Dropper, der Viren einpflanzt - also ein "Opfer" selbst, das beim Aufrufen des Trojaners den Computer infiziert und damit einen Schneeballeffekt auslöst.

Die hier vorgestellte Definition entspricht der der deutschen Viren-FAQ (Frequently Asked Questions) von Martin Rösler.

## **Logische Bomben**

Eine logische Bombe (kurz: Bombe) ist streng genommen eine Spezialart eines trojanischen Pferdes. Bomben sind Programmteile, die in nützlichen Code eingebettet sind und aus einem Auslöser (trigger) und einer Nutzlast (payload) bestehen. Ihre zerstörerischen Funktionen werden eine gewisse Zeit lang überhaupt nicht aufgerufen. Später, wenn eine Auslösebedingung erfüllt ist (beispielsweise ein bestimmtes Datum erreicht oder das Programm fünfzig mal aufgerufen wurde), "explodiert" die Bombe, und ihre Zerstörungsfunktion wird aufgerufen.

Ein Spezialfall einer logischen Bombe ist die sogenannte ANSI-Bombe, welche die Tastaturbelegung mittels ANSI.SYS-Treiber neu definiert.

Die hier vorgestellte Definition entspricht der der deutschen Viren-FAQ (Frequently Asked Questions) von Martin Rösler.

# Dialer gefunden

AntiVir hat einen Dialer gefunden

Im Unterschied zu Computerviren können Dialer normalerweise keine Dateien beschädigen oder verändern. In der Regel sind sie auch nicht in der Lage, Registry-Einträge vorzunehmen. Zumeist kopieren sie sich als .EXE-Datei nach C:\Windows, C:\Windows\System\ oder auf den Desktop, wobei (es gibt auch Ausnahmen) eine Verknüpfung ins Startmenü erfolgt. In einigen Fällen kann es zu Einträgen in das Startmenü (Start - Programme - Autostart) kommen.

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 Dialer einfach zu löschen.

# Spiel (Game) gefunden

AntiVir hat ein Spiel (Game) gefunden

Computerspiele dienen der Unterhaltung und des Zeitvertreibs. Sie haben weder einen schädlichen Einfluss auf Dateien, noch zielen sie darauf ab, die Funktionsfähigkeit von Rechnersystemen zu unterbinden. Dennoch ist ihre Anwesenheit nicht immer willkommen oder mitunter sogar unerwünscht, weil sie möglicherweise Arbeitszeit- und Rechnerressourcen in Anspruch nehmen.

AntiVir erkennt Computerspiele. 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.



# 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 erkennt Computerspiele. 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" aktiviert haben, erhalten Sie eine entsprechende Warnung, wenn AntiVir fündig geworden ist.

# Profile (Inhalt)

(Nur AntiVir Professional)

{button ,AL('rtoProfiles',0,'')} siehe auch

## AntiVir bietet in diesem Menü folgende Optionen:

### Profil als Standard sichern...

Mit dieser Menü Option oder mit der Schaltfläche "Als Standardprofil speichern" wird ein Fenster aufgerufen, in dem Sie ein neu erstelltes Profil als Standardprofil speichern können.

Wenn Sie AntiVir neu starten, wird dieses Standardprofil automatisch in die Registerkarte geladen.

### Profil sichern als...

Mit dieser Option oder mit der Schaltfläche "Profil speichern" wird ein Fenster aufgerufen, in dem Sie ein neu erstelltes oder bearbeitetes Profil speichern können.

Die Profildateien können Sie an der Endung \* .PRO erkennen.

### Profil laden...

Soll ein bereits erstelltes Profil nach Viren bzw. unerwünschten Programmen durchsucht werden, öffnen Sie die Liste der Profile mit Hilfe dieser Menü Option oder mit der Schaltfläche "Profil laden" und doppelklicken auf das entsprechende Profil in der Liste (Alternative: markieren und die Schaltfläche "Öffnen" betätigen).

### Neues Profil erstellen

Öffnet die Registerkarte Profile