AntiVir®

für Windows 9x
Windows NT Workstation
Personal Edition

Benutzerhandbuch

Ausgabe Juni 2001
Herausgeber:
H+BEDV Datentechnik GmbH
D-88069 Tettnang, Lindauer Strasse 21

Internet: http://www.free-av.com

Über dieses Handbuch

Das kleine Viren–Einmaleins

AntiVir benutzen

1 Aufbau des Handbuches

Im vorliegenden Benutzerhandbuch, das Ihnen als PDF-Datei vorliegt, wird die Installation der Programmpakete der kostenfreien AntiVir Personal Edition beschrieben.

In den folgenden Kapiteln des Handbuches geht es um die Handhabung des Programmes. Dabei gehen wir von Standardsituationen aus, in denen Sie AntiVir verwenden können. Die Handhabung ist so beschrieben, daß auch Einsteiger AntiVir ohne Mühe benutzen können.

Wer es genauer wissen will, bekommt dort aber auch jede Funktion und Einstellmöglichkeit des Programmes erklärt. Nach deren Lektüre gilt vermutlich der Satz: *We're still puzzled, but on a much higher level*.

Als Orientierungshilfe finden Sie am Ende dieses Handbuches ein Index. Bei Schwierigkeiten rund um die AntiVir Personal Edition soll Ihnen die Rubrik 'Häufig gestellte Fragen' weiterhelfen.

Können Sie Ihr Betriebssystem nicht starten, weil ein Virus seine Schadensroutine „ erfolgreich" beendet hat, werden in dieser Anleitung unter 'Trouble Shooting' Wege beschrieben, wie Sie Ihr Rechnersystem mit Hilfe von AntiVir meistens wieder in den Griff bekommen können.

Sonst halten wir es wie Brian Eno, der sich als einer der ersten Anwender von Computersystemen in der Kunst- und Musikszene über Computer und deren Handbücher folgendermaßen geäußert hat:

> *Herzlichen Glückwunsch zu Ihrem neuen Computer. Wir danken Ihnen, daß Sie Ihre besten Jahre opfern wollen, um eine unterentwickelte Technologie zu verstehen. Das erste Kapitel des Handbuches erklärt, wie Sie mit dem Kapitel des Handbuches umgehen müssen, das erklärt, wie Sie mit dem Rest des Handbuches umgehen müssen. Bevor Sie dieses Kapitel lesen, machen Sie sich bitte mit dem nächsten Kapitel vertraut, das klarstellt, warum das erste Kapitel wichtig war. Wenn Sie das Handbuch gelesen haben, sind Sie zwar nicht in der Lage, Ihren Computer zu verstehen, aber erheblich älter.*
>
> ;-)

2 Konventionen

Symbolerklärung

➔ Dieser Pfeil zu Beginn eines Absatzes weist auf eine Handlung hin, die Sie durchführen sollen.

Voraussetzung

macht auf bestimmte Voraussetzungen aufmerksam, die für einen sinnvollen Einsatz von AntiVir erfüllt sein müssen.

Hinweis

informiert über Tips und Tricks, die Ihnen beim Umgang mit AntiVir unter Ihrem Betriebssystem weiterhelfen.

Achtung

weist auf knifflige Arbeitsschritte oder heimtückische Fallstricke hin.

Gefahr

warnt vor schwerwiegenden Gefahren, die in Zusammenhang mit Viren auftreten können.

“Saubere” Software einsetzen

Empfehlung, die 'bekanntermaßen gute DOS- oder Betriebssystem-Diskette' zur Hand zu nehmen. Mit diesem Symbol wird auch auf den Einsatz von Backups hingewiesen.

Zusatzinformationen

verweist auf weiterführende Stellen in unseren Handbüchern, in der READ.ME-Datei von AntiVir, in der Online-Hilfe von AntiVir oder in der Betriebssystem-Dokumentation.

Betriebssystem

hier abgekürzt als **O**perating **S**ystem. Dieses Piktogramm weist auf wesentliche Unterschiede zwischen den AntiVir-Paketen für verschiedene Betriebssysteme hin.

Die Screenshots in diesem Handbuch stammen in der Regel von AntiVir/Me.

Schriftarten

In diesem Handbuch werden folgende Schriftarten verwendet:

Keyboard	Kennzeichnet eine Taste auf der Tastatur
LW:\Pfad\>	Stellt den angewählten Laufwerksbuchstaben, den Pfad und den Prompt (>) unter DOS dar. Diese Zeichen dürfen in einer Befehlszeile nicht eingegeben werden!
`text eingabe`	Kennzeichnet Eingaben an ein Programm bzw. System
DATEI.ERW	Dateibezeichner (Dateiname und Erweiterung)
'Menü/Punkt'	Verweist auf einen Menüpunkt im entsprechenden Menü
Button	Schaltfläche in einem Dialogfenster

Tastaturbezeichnungen

Im Handbuch werden, soweit möglich, die deutschen Begriffe für die handelsüblichen Industrietastaturen verwendet.

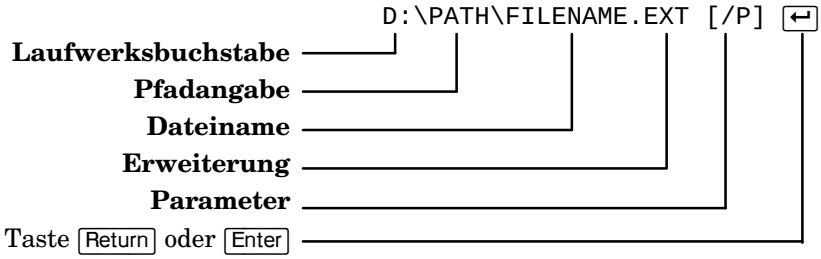
Bei Tastenkombinationen gilt für die Zeichen + und / diese Regel:

Alt+F4 beide Tasten werden gleichzeitig gedrückt.

Einfg / ↵ die Tasten werden nacheinander gedrückt.

DOS-Konventionen

Im gesamten Handbuch zu AntiVir werden dieselben Schreibweisen wie in den bekannten DOS-Handbüchern verwendet.
Die vollständigen Angaben zum Verweisen auf eine Datei bestehen aus:

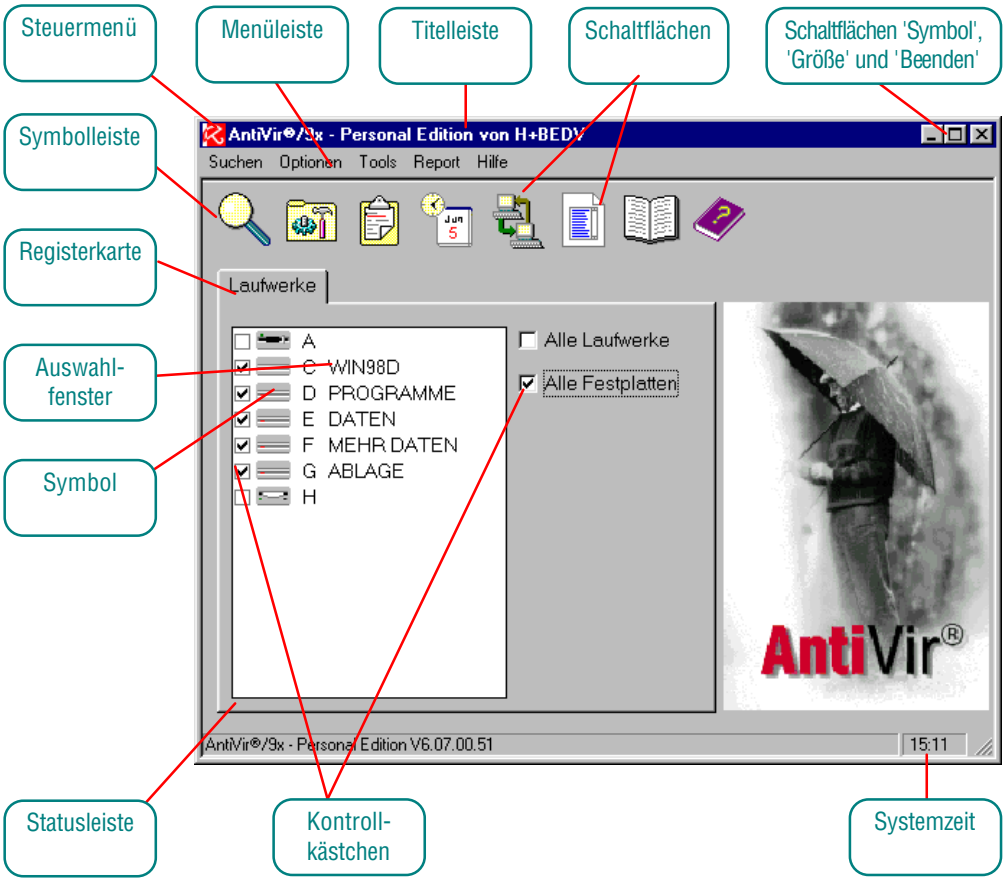


AntiVir unterstützt teilweise die Universal Naming Conventions – das sind die Datei- bzw. Pfadnamen, die mit einem doppelten umgekehrten Schrägstrich '\\' beginnen – nicht aber die übliche Schreibweise der Server- und Volumenamen. Hier können '\' und '/' gemischt werden. Workstationseitig kann je nach verwendeter Shell-Version ein Vergessen des '\' bei einem Volume-Bezeichner den Verlust des Mappings zur Folge haben!

Windows-Konventionen

Sicherlich verfügen Sie über Windows-Grundkenntnisse. Mit Begriffen wie Verzeichnis/Ordner, Laufwerk oder Datei sowie mit Vorgängen wie Kopieren, Löschen, Verzeichnis wechseln oder erstellen sind Sie vertraut.

Für die Bedienelemente der AntiVir® Personal Edition (hier Windows 98) werden die unter Windows gebräuchlichen Bezeichnungen verwendet:



Zu den hier aufgezählten Begriffen kommen noch die Bildlaufleiste (mit Bildlaufpfeil und Bildlaufmarke zum Navigieren innerhalb eines Fensters) und das Dialogfenster (dort werden Einträge gemacht oder Informationen angezeigt) hinzu.

Die meisten Funktionen lassen sich auf verschiedenen Wegen aufrufen:

- Auswahl mit der Maus in der Menüleiste
- Auswahl in der Symbolleiste
- Auswahl durch Tastenkombinationen

Kopfzeilen und Überschriften

In der Kopfzeile auf der linken Seite sehen Sie, in welchem Teil des Handbuches Sie sich gerade befinden, beispielsweise 'Über dieses Handbuch' oder 'AntiVir benutzen'. In der Kopfzeile rechts wird die Überschrift des Hauptkapitels wiederholt, z.B. 'Konventionen' oder 'AntiVir starten'. Auch die Überschriften der Unterkapitel und der Abschnitte unterscheiden sich in der Schriftgröße und sind nach links eingerückt.

3 Über die AntiVir Personal Edition

AntiVir® erkennt und repariert die uns bis dato bekannten Viren – und das sind derzeit über 56.000. Dazu zählen Bootsektorviren, verschiedene Arten von Dateiviren einschließlich der Makroviren sowie auch Trojaner. AntiVir® kann auch aktive Viren im Speicher erkennen und gibt eine entsprechende Meldung am Bildschirm aus.

Das **Such- und Reparaturmodul** (die Engine) ist das Herzstück von AntiVir. Hier findet sich alles, was mit dem Aufspüren von Viren und der Reparatur infizierter Dateien und Bootsektoren zusammenhängt.

Eine Datenbank mit den **Virenkennungen** (ANTIVIR.VDF) enthält alle notwendigen Angaben zu den Viren, die von der Engine abgefragt werden.

Vom der **Benutzeroberfläche** des Hauptfensters aus läßt sich steuern, was die Engine machen soll. Von dieser Schaltzentrale aus können Laufwerke ausgewählt, Suchläufe gestartet, der Scheduler, die Reportdatei und die Vireninformationen aufgerufen sowie die Einstellungen den eigenen Bedürfnissen angepaßt werden.

Der residente Virenwächter **AntiVirGuard** dient zur automatischen Überwachung von Dateibewegungen (Öffnen, Verschieben, Kopieren, Umbenennen). Dieser Wächter ist unter Windows 95/98/Me als VxD-Datei (= Virtual Extended Driver), unter Windows NT/2000 als Dienst aufgebaut. Der Virenwächter sollte beim Start des Betriebssystems möglichst früh aktiviert werden und dann ständig im Hintergrund aktiv bleiben.

Sowohl Engine als auch die Virenkennungen müssen so aktuell wie möglich sein. Nur dann erhalten die Anwender einen relativ sicheren Schutz vor Viren, die sich auf den Wegen der modernen Datenübertragung sehr schnell verbreiten können. Nutzen Sie deshalb die Möglichkeit, AntiVir in ca. zweimonatlichen Abständen durch eine neue Version zu aktualisieren.

Nebenbei bemerkt haben Sie das beste Mittel gegen Schäden, die durch Viren verursacht werden, selbst in der Hand: vollständige Backups in ausreichenden Zeitabständen.

3.1 Systemvoraussetzungen

Die hier aufgeführten Daten beziehen sich auf den Zeitpunkt der Fertigstellung dieses Handbuches. Auf grundlegende Änderungen wird in der entsprechenden Datei LISMICH.WRI hingewiesen.

AntiVir®/Me Personal Edition

- ✘ Windows 95, Windows 98 oder Windows Me
- ✘ CPU 80486, besser Pentium ab CPU 80586
- ✘ ca. 8 MB freier Speicherplatz auf der Festplatte
- ✘ 8 MB freier Hauptspeicher (bei aktiviertem Guard besser 16 MB)
- ✘ 4 MB temporärer Speicher auf dem Datenträger

AntiVir®/2000 Personal Edition

- ✘ Windows NT 4.0 Workstation, Windows 2000 Workstation
- ✘ CPU 80486, besser Pentium ab CPU 80586
- ✘ ca. 10 MB freier Speicherplatz auf der Festplatte
- ✘ 8 MB freier Hauptspeicher (bei aktiviertem Guard besser 16 MB)
- ✘ 4 MB temporärer Speicher auf dem Datenträger

Je nach Größe der Verzeichnisstruktur des verwendeten Datenträgers kommen bei allen Windows-Versionen noch mehrere KB Speicher hinzu. Sollen komprimierte Dateien, wie etwa PKLite-Dateien, dekomprimiert werden, wird zusätzlicher Hauptspeicher benötigt. Sollen auch Archivdateien entpackt werden, müssen sowohl ausreichend Platz in einem temporären Pfad zur Aufnahme der entpackten Dateien vor einer Untersuchung verfügbar als auch gegebenenfalls die Entpacker greifbar sein.

Alle Programme aus den AntiVir-Paketen dürfen nicht mit EXE-Packern wie etwa PKLite oder LZExe komprimiert werden, da alle Programme mit einer Selbstüberprüfung ausgestattet sind.

3.2 Inhalt der Programmpakete

AntiVir® für Windows ist der Oberbegriff für ein Schutzpaket, das aus dem Hauptprogramm, dem Virenwächter AntiVir Guard und verschiedenen Hilfsdateien besteht.

Auf diese Dateien möchten wir Sie besonders hinweisen: aktuelle Informationen erhalten Sie in den zu den Programmpaketen gehörenden LIESMICH.WRI-Dateien. Dort finden Sie alle Informationen, die zum Zeitpunkt der Fertigstellung des Handbuches noch nicht bekannt waren. Werfen Sie bitte vor der Installation einen aufmerksamen Blick in diese Datei oder drucken Sie diese aus.

3.3 Nutzungsvertrag

Bitte lesen Sie den folgenden Vertrag sorgfältig durch. Mit der Installation der Software erklären Sie Ihr ausdrückliches Einverständnis, an die Bestimmungen dieses Vertrages gebunden zu sein. Wenn Sie mit den Bestimmungen dieses Vertrages nicht einverstanden sind, dürfen Sie die Software nicht verwenden .

Diese kostenfreie AntiVir© Personal Edition ist ausschließlich für den privaten Einsatz auf einem Einzelplatz-PC (Workstation) vorgesehen. Das Kopieren des vollständigen Programmpaketes und die Weitergabe für eine ausschließlich private Nutzung ist erlaubt.

Der kommerzielle oder berufliche Einsatz der kostenfreien AntiVir© Personal Edition ist nicht gestattet.

§1 Vertragsgegenstand

1) Gegenstand des Vertrages sind die Computerprogramme (im Folgenden 'Software'), die Programmbeschreibungen und Bedienungsanleitungen.

2) Dem Anwender werden an der Software unentgeltlich Nutzungsrechte eingeräumt.

3) Das in der Bedienungsanleitung dargestellte Computerprogramm entspricht dem heutigen Stand der Technik. Die H+BEDV Datentechnik GmbH (im folgenden Lizenzgeber genannt) macht jedoch darauf aufmerksam, daß es nach dem heutigen Stand der Technik nicht möglich ist, Software so herzustellen, daß sie in allen Anwendungen und Kombinationen fehlerfrei arbeitet.

4) H+BEDV stellt diese Software auf ihrem Server lediglich zum Download bereit. H+BEDV bietet nicht die Übertragung dieser Software auf den Computer des Anwenders an.

§2 Umfang der Benutzung

Der Lizenzgeber gewährt dem Anwender der Software (im folgenden "Lizenznehmer" genannt) das einfache, nicht ausschließliche und persönliche Recht, die Software ausschließlich für den privaten Gebrauch auf einem einzelnen Computersystem und nur an einem Ort zu benutzen (im folgenden "Lizenz" genannt), so wie dies im folgenden beschrieben wird:

1) Der Lizenznehmer darf die Software auf einem privaten Personal Computer installieren, in den Arbeitsspeicher laden und abspielen.

2) Der Lizenznehmer darf die Software nur zu rein privaten Zwecken nutzen. Bildungseinrichtungen und gemeinnützige Einrichtungen werden wie kommerzielle oder geschäftliche Einrichtungen behandelt. Auch die Nutzung in einem Heimbüro für kommerzielle oder geschäftliche Zwecke ist nicht zugelassen.

3) Der Lizenznehmer darf die vollständige Software kopieren, um sie unentgeltlich und unter Beibehaltung der Marke, des Logos und des Copyright-Vermerks sowie unter Hinweis auf diese Nutzungsbedingungen an Dritte weitergeben.

4) Der Lizenznehmer darf eine Sicherheitskopie der Software anfertigen.

§3 Besondere Beschränkungen

Dem Lizenznehmer ist es insbesondere untersagt,

1) über den in §2 genannten Rahmen hinaus Kopien der Software, ganz oder auszugsweise, auf gleichen oder anderen Trägern zu fertigen.

2) die Komponenten der Software zu trennen, um sie an mehr als einen Computer zu nutzen.

3) die Software abzuändern, zu übersetzen, zurückzuentwickeln, zu entkompilieren oder zu disassemblieren, von der Software abgeleitete Werke zu erstellen oder das schriftliche Material zu vervielfältigen, es zu übersetzen oder abzuändern oder vom schriftlichen Material abgeleitete Werke zu erstellen;

4) die Software für eine geschäftliche Nutzung an Dritte weiterzugeben, zu vermieten, zu verleasen oder in irgendeiner anderen Form kommerziell zu verwerten. Dies gilt auch für Kopien der Software.

5) die Software oder Kopien davon entgeltlich an Dritte weiterzugeben. Dieses Softwarepaket darf nicht ohne Erlaubnis der H+BEDV Datentechnik GmbH auf kommerziellen Datenträgern (beispielsweise Sampler-CD, Shareware-CD, als OEM-Versionen) verbreitet werden.

§4 Inhaber von Rechten

1) Diese Software ist urheberrechtlich geschützt. Alle aus dem Urheberrecht resultierenden Rechte stehen dem Lizenzgeber zu. Das Urheberrecht umfaßt insbesondere den Programmcode, die Dokumentation, das Erscheinungsbild, die Struktur und Organisation der Programmdateien, den Programmnamen, Logos und andere Darstellungsformen innerhalb der Software.

2) Der Lizenznehmer erhält nur das individuelle, private Nutzungsrecht an der Software. Ein Erwerb von Rechten an der Software selbst ist damit nicht verbunden. Der Lizenzgeber behält sich alle Veröffentlichungs-, Vervielfältigungs-, Bearbeitungs- und Verwertungsrechte an der Software vor.

§5 Dauer des Vertrages

1) Der Vertrag läuft auf unbestimmte Zeit. Das Recht des Lizenznehmers zur Benutzung der Software erlischt automatisch ohne Kündigung, wenn er eine Bedingung dieses Vertrages verletzt.

2) Erlischt das Nutzungsrecht, ist der Lizenznehmer verpflichtet, die Software auf seinem Computersystemen zu deinstallieren. Er verpflichtet sich ebenso, alle Kopien der Software, das vollständige schriftliche Material sowie alle Kopien desselben, einschließlich etwaiger abgeänderter Exemplare zu vernichten.

§6 Gewährleistung

Die Nutzungsrechte an dieser Software werden dem Lizenznehmer unentgeltlich eingeräumt. Es findet daher weder kaufrechtliches noch sonstiges Gewährleistungsrecht Anwendung. Der Lizenznehmer akzeptiert dieses Programm in der Form, wie es derzeit vorliegt. Dem Lizenznehmer stehen somit keinerlei Gewährleistungsansprüche zu.

§7 Haftung

1) Der Lizenzgeber stellt die Möglichkeit eines bestimmungsgemäßen Gebrauches der Software in Übereinstimmung mit der Programmbeschreibung sicher. Es wird keine Haftung dafür übernommen, daß die Software für die Zwecke des Anwenders geeignet ist und mit beim Anwender vorhandener Software zusammenarbeitet. Es obliegt dem Lizenznehmer zu prüfen, ob das Produkt seinen Anforderungen genügt.

2) Schadensersatzansprüche gegen H+BEDV sind unabhängig vom Rechtsgrund, insbesondere aufgrund Verzug oder Unmöglichkeit, der Verletzung Beratungs- und vertraglichen Nebenpflichten, vorvertraglichen Pflichten, positiver Vertragsverletzung, der Verletzung gewerblicher Schutzrechte Dritter und unerlaubter Handlung ausgeschlossen, es sei denn, H+BEDV hat vorsätzlich oder grob fahrlässig gehandelt oder die Schadensersatzansprüche resultieren aus der Verletzung einer zugesicherten Eigenschaft.

3) Soweit H+BEDV dem Grunde nach haftet, wird der Schadensersatzanspruch auf den vorhersehbaren Schaden begrenzt. In jedem Fall ist der Ersatz für Folgeschäden wie entgangener Gewinn ausgeschlossen. Diese Schadensbegrenzung gilt nicht wenn das schadensauslösende Ereignis durch einen ihrer gesetzlichen Vertreter oder leitenden Angestellten grob fahrlässig oder vorsätzlich ausgelöst wurde.

4) Alle Schadensersatzansprüche gegen H+BEDV verjähren in sechs Monaten nach Erhalt der Software. Dies gilt nicht für Ansprüche aus unerlaubter Handlung.

5) Auf Ansprüche nach dem Produkthaftungsgesetz sind diese Bestimmungen nicht anwendbar.

§8 Schadensminderungsobliegenheit

1) Der Lizenznehmer wird ausdrücklich darauf hingewiesen, daß er von den auf seinem Computer befindlichen Daten regelmäßig in ausreichenden Zeitabständen (in der Regel wöchentlich) Sicherungskopien anzufertigen hat. Tut er dies nicht, verstößt er gegen seine Schadensminderungsobligenheit. H+BEDV haftet nicht für infolge dieses Verstoßes entstandene Schäden.

2) Der Lizenznehmer wird ausdrücklich darauf hingewiesen, daß er die Software nicht in gefährlicher Umgebung einsetzen darf, die fehlerfreien Betrieb voraussetzt (Hoch-Risiko-Aktivitäten wie beispielsweise Betrieb von Kernkraft-Einrichtungen, Waffensysteme, Luftfahrtnavigations- oder Kommunikationssysteme oder lebenserhaltende Maschinen). Tut er dies dennoch, verstößt er gegen seine Schadensmiderungsobliegenheit. H+BEDV haftet nicht für infolge dieses Verstoßes entstehende Schäden.

§9 Vertragsänderungen und Abwehrklausel

1) Diese Nutzungsbedingungen gelten in ihrer jeweils gültigen, auf der Webseite [www.free-av.com] veröffentlichten Form.

2) Diese Allgemeinen Nutzungsbedingungen werden auch dann Vertragsinhalt, wenn der Lizenznehmer anderslautende Vertragsbedingungen hat, auch wenn H+BEDV im Einzelfall nicht widerspricht.

§10 Rechtswahl

Auf sämtliche Rechtsbeziehungen zwischen den Parteien, einschließlich des Deliktsrechts, findet das Recht der Bundesrepublik Deutschland Anwendung. Der Gerichtsstand ist Tettnang.

§11 Schlußbestimmungen

1) Ergänzungen dieses Vertrages einschließlich dieser Klausel bedürfen der Schriftform.

2) Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, wird dadurch die Rechtswirksamkeit der übrigen Bestimmungen nicht berührt. Die unwirksame oder nicht durchführbare Bestimmung ist nach Möglichkeit durch eine zulässige, im wirtschaftlichen ihr gleichkommende zu ersetzen.

3) Auf diesen Vertrag findet das Recht der Bundesrepublik Deutschland Anwendung. Gerichtsstand ist Sitz des Lizenzgebers. Alle Fragen bezüglich der Gültigkeit, der Auslegung sowie der Erfüllung der Vertragsinhalte sollen am Gerichtsstand des Lizenzgebers in der Bundesrepublik Deutschland geklärt werden.

Wenn Sie Fragen zu diesem Lizenzvertrag haben, finden Sie weitere Informationen unter www.free-av.com.

Möchten Sie sich aus einem anderen Grund mit dem Lizenzgeber in Verbindung setzen, senden Sie bitte eine Mail an vertrieb@antivir.de oder schreiben Sie an: H+BEDV Datentechnik GmbH, Lindauer Straße 21, 88069 Tettnang.

4 Viren – der Versuch einer Definition

Bei Computerviren handelt es sich um kleine Programme, die von ihrem Programmierer in ein beliebiges Wirtsprogramm eingesetzt wurden. Bei jedem Aufruf dieses Wirtes (das kann eine Textverarbeitung oder jede andere beliebige Software sein) sucht sich der Virus ein anderes Programm, das er noch nicht infiziert hat und kopiert sich dort hinein. Viren sind zumeist selbstreproduzierend, irgendwann sind alle Programme infiziert.

Bei Bootsektorviren ist es ähnlich: Ihr „Wirtsprogramm" ist der Bootsektor, den alle Disketten – auch Datendisketten und sogar einige CD-ROMs – enthalten. Sollen Daten (physisch) ausgetauscht werden, bietet sich eine Diskette geradezu an – mit großem Infektionsrisiko. Jede nicht schreibgeschützte Diskette ist gefährdet und ein möglicher Virenträger.

Die Verbreitung allein wäre ja nicht allzu schlimm, sieht man von verbratenen Rechnerressourcen wie Prozessorzeit und Festplattenplatz ab. Doch fast alle Viren haben neben dem Vervielfältigungsteil noch einen weiteren Programmteil, der nach bestimmten Kriterien ausgelöst wird und Böses im Schilde führen kann. Kriterien sind z.B. ein bestimmtes Datum, ein bestimmter Wochentag, die Sättigung des Systems mit Viren, besondere Eingaben an der Tastatur etc., diese Viren werden zu Zeitbomben.

Die Gegenwart eines Virus wird oft erst bemerkt, wenn der Auslösezeitpunkt erreicht ist und der Virus mit bestimmten Aktionen beginnt. Das kann von mehr oder weniger „lustigen" Störungen der Bildschirmausgabe bis zum totalen Löschen oder der Verschlüsselung aller Daten reichen.

Vorsicht ist die Mutter der Siliziumkiste. Wer einen Virus während der Ausbreitung übersieht, hat ein ernstes Problem. Viele Viren haben ein Auslösedatum (=Trigger), das dem Virus viele Monate Zeit zur Verbreitung geben kann. Ein prominentes Beispiel hierzu ist der wohl allseits bekannte Michelangelo-Virus: Er überschreibt an jedem 6. März – dem Geburtstag des nach dem Künstler benannten Virus – wichtige Systemteile einer Festplatte. Oder nehmen wir den Jerusalem-Virus, der an jedem Freitag den 13. alle an diesem Tag aufgerufenen Programme löscht. Und wenn sich ein Virus über Monate auf Ihrem System breit macht, helfen oft auch keine Backups mehr. Ähnlich schlimm ist dies bei Viren, die eine schleichende Datenveränderung vornehmen, wie beispielsweise der Jack the Ripper-Virus. Dieser Bootsektorvirus vertauscht bei einem aus 1024 Schreibzugriffen auf die Festplatte wahllos in dem zu schreibenden Sektor zwei Worte miteinander. Bei einem simplen COMPRESS oder DEFRAG einer Festplatte kommen mehrere tausend solcher Schreibzugriffe vor.

Und dieses Problem macht Vireninfektionen besonders unangenehm: Sie müssen davon ausgehen, daß die Infektion an alle verschleppt wurde, mit denen Sie in der fraglichen Zeit Daten ausgetauscht haben.

4.1 Kleines Viren-Glossar

Bootsektor Dies ist der logisch erste Sektor einer Partition und enthält Angaben über die Struktur des Datenträgers, sowohl bei Festplatten als auch bei Disketten.

Bootsektorvirus Schmerzhafte Bazille im Bootsektor. Diese Spezies infiziert in der Regel nur den Bootsektor von Disketten; bei Festplatten wird normalerweise der Master-Bootsektor infiziert. Bootsektorviren lassen sich nur auf zwei Arten aktivieren: Booten mit einer infizierten Diskette im Laufwerk A: oder Starten eines Droppers bzw. eines mit einem Multipartite-Virus infizierten Programmes.

Bootsektorviren werden nicht durch 'DIR A:' aktiviert! Ist der Virus allerdings aktiv, wird bei 'DIR A:' (oder B:) jede eingelegte nicht schreibgeschützte Diskette infiziert! Bootsektorviren fallen häufig durch Reduzierung des Hauptspeichers auf (Ausnahme: Stealth-Viren, die gaukeln dem System die richtigen Werte vor). Der Rechner besitzt dann angeblich nur noch 638 KB oder 639 KB DOS-Speicher anstelle von 640 KB (655.360 Bytes).

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

Companion Virus Nutzt die Eigenart des DOS-Betriebssystemes aus, wonach beim Aufruf eines Programmes ohne Erweiterung eine bestimmte Suchreihenfolge eingehalten wird. Dieser Virus trägt den gleichen Namen wie eine EXE-Datei, aber mit der Erweiterung .COM. Deshalb wird diese Datei vor einer EXE-Datei gleichen Namens ausgeführt. Companions sind in der Regel stets gleich lang und meistens durch Setzen des Hidden- oder System-Dateiattributes versteckt. Werden alle erzeugten COM-Programme gelöscht, ist auch der Virus weg.

Dateivirus Diese Viren können sich an eine Wirtsdatei anhängen und modifizieren den Anfang einer ausführbaren Datei derart, daß zuerst die Viren die Kontrolle erhalten. Der Viruscode wird dann mit denselben Privilegien wie das Originalprogramm ausgeführt.

Dropper Eine Datei, die selbst nicht infiziert ist, aber einen Bootsektor- oder Dateivirus enthält, der beim Aufruf des Programmes auf der Festplatte bzw. Diskette installiert wird. Der Virus wird in der Regel erst beim nächsten Neustart aktiv.

Hoaxes Hoaxes sind Meldungen über angeblich zerstörerische Dateien, die mit Vorliebe per Email verbreitet werden. Diese Hoaxes lassen sich am besten mit Zeitungsenten vergleichen: Einmal in der Welt, lassen sie sich nicht mehr ausrotten. Besonders beliebt: 'Dieser Virus ist besonders hinterhältig: Während Sie diese Zeilen lesen, wird die Festplatte überschrieben, die Stereoanlage zerstört und Ihr Kühlschrank neu konfiguriert!'

Link-Viren Diese seltene Spezies modifiziert den Verweis auf den ersten zu dieser Datei gehörenden Cluster im Directory und lassen ihn auf den Virus selbst zeigen.

Logische Bombe Programmteile, die in nützlichen Code eingebettet sind und aus einem Auslöser (trigger) und einer Nutzlast (payload) bestehen, werden als logische Bombe bezeichnet. Ihre Nutzlast wird eine gewisse Zeit lang überhaupt nicht aufgerufen. Wird später eine Auslösebedingung erfüllt (wenn beispielsweise ein bestimmtes Datum erreicht oder das Programm fünfzig mal aufgerufen wurde), 'explodiert' die Bombe und ihre Zerstörungsfunktion beginnt. Ein Spezialfall ist die sogenannte ANSI-Bombe, welche die Tastaturbelegung mittels ANSI.SYS-Treiber neu definiert.

Makrovirus Ein Makro faßt eine Folge von Tastatureingaben bzw. Befehlen zu einem Komplex zusammen, der wiederum mit dem Aufruf des Makros abgearbeitet wird. Bei MS-Word werden diese Makros in Formatvorlagen (z.B. NORMAL.DOT) abgelegt, die wiederum die Grundlage der Textdateien (.DOC-Dateien) bilden.

Das Gefahrenpotential dieser Makros liegt hauptsächlich in der Möglichkeit, vielfältige Dateioperationen und DOS-Kommandos auszuführen. Beispielsweise ist das Formatieren von Festplatten, das Löschen von Dateien oder ein Zugriff auf die Windows-Systemumgebung (WIN-API) mit Hilfe eines Makros möglich.

Master-Bootsektor Dieser Sektor existiert ausschließlich auf Festplatten. Der Master-Bootsektor ist immer der physikalisch erste Sektor: Zylinder 0, Kopf 0, Sektor 1.

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

Multipartite Viren Diese Viren können neben Dateien auch Boot- bzw. Master-Bootsektoren infizieren. Beim Entfernen muß darauf geachtet werden, daß nicht nur eine Komponente des Virus gelöscht wird.

Partitions-tabelle 64 Byte lange Tabelle am Ende des Master-Bootsektors. Enthält die Tabelle über die Aufteilung der Festplatte und Angaben, wie groß jede Partition ist.

Polymorphe Viren Diese Viren sind verschlüsselt und ändern bei jedem infizierten Programm den Aufbau der Entschlüsselungsroutine. Damit ist eine Suche mittels Suchstrings unmöglich. Die 'Mutation Engine' erzeugt mehrere Millionen Arten von Verschlüsselungen. Polymorphe Viren können durch algorithmische Suche oder Codeemulation gefunden werden.

Signatur Mehrere aufeinanderfolgende Kombinationen von Bytefolgen zum Erkennen eines Virus.

Stealth-Virus Diese Viren können ihre Anwesenheit wie ein Tarnkappen-Bomber verstecken und versuchen damit alle Virenscanner zu täuschen. Veränderungen durch diese Viren lassen sich nicht ohne weiteres sichtbar machen. Sie verbergen die Tatsache, daß infizierte Dateien oder Sektoren verändert werden. Man unterscheidet zwischen Semi- und Vollstealth, wobei Semistealth-Viren nur die Dateiverlängerung verbergen, nicht aber die Dateiveränderung. Zum erfolgreichen Entfernen von Stealth-Viren muß der Rechner von einer sauberen Bootdiskette aus gestartet werden, da sonst der Virus noch aktiv im Hauptspeicher ist. Datei-Stealthviren fallen oft durch 'Fehlermeldungen' des Programmes CHKDSK auf, die durch den Unterschied zwischen FAT und Verzeichnis entstehen (bei dem CHKDSK-Befehl *nicht* den Parameter /F angeben! Hierbei droht Datenverlust!).

Systemvirus Virus, der weder Dateien noch MBR bzw. Bootsektor infiziert, sondern das Betriebssystem selbst. Beispielsweise infiziert der DIR-Virus keine Sektoren oder Dateien, sondern manipuliert direkt die Verzeichnisse von DOS. DIR-Viren breiten sich sehr schnell aus, da schon ein DIR aller Dateien in dem Verzeichnis ausreicht, diese zu infizieren.

Trojanisches Pferd (Trojaner) Ein Trojaner täuscht eine nützliche Funktion vor. Nach dem Aufruf zeigt solch ein Programm jedoch sein wahres Gesicht und beginnt sein meist zerstörerisches Werk. Trojaner können sich nicht selber verbreiten. Viele Trojaner tragen unscheinbare oder interessante Namen (STARTME.EXE oder SEX.EXE), die gleich nach Programmstart aktiv werden und beispielsweise die Festplatte formatieren oder Daten durcheinanderbringen.

Verschlüsselt Einige Viren versuchen sich vor Antiviren-Programmen zu verbergen, indem sie ihren Programmcode verschlüsselt abspeichern und erst während des Programmablaufs entschlüsseln.

Virus Ein Programm mit der Fähigkeit, sich nach seinem Aufruf selbsttätig an andere ausführbare Codefragmente 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 (Wirtscode), dessen Ablauf der Virus durch das Infizieren verändert. Die Wirte dienen lediglich als Transportmittel, deshalb wird der Ablauf des Wirtscodes nicht geändert.

Witzprogramme 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 Witzprogrammes irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für solche 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 sogar selbst tatsächlichen Schaden an.

Würmer Digitale Lebewesen, die sich verstärkt per Internet verbreiten. Die erste Definition lautet: “Programm, welches sich innerhalb von Netzwerken selbst vervielfältigt und Rechenzeit stiehlt”. Dies geschieht beispielsweise auf vernetzten Mainframes durch Prozeßgabelung.
Die zweite Erklärung lautet: ein Wurm ist ein Programm, welches sich selbst vervielfältigt, dabei jedoch keinerlei Wirtscode infiziert. Ein Beispiel dazu 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 selber aktivieren können. Sonst muß immer der Mensch an der Verbreitung eines Wurmes beteiligt sein, indem er ihn startet.

4.2 Vorsorgemaßnahmen

- Erstellen Sie eine 'bekanntermaßen gute DOS-Diskette'.
- Denken Sie auch an Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkserver und die einzelnen Workstations. Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- Starten Sie Ihr Rechnersystem von einer Diskette, verwenden Sie bitte die schreibgeschützte 'bekanntermaßen gute DOS- Diskette' oder die schreibgeschützte Original-Systemdiskette.
- Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Datendisketten enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an. Backups sind der Unterschied zwischen einem halben Tag Arbeit und einem Desaster. Und was passiert, wenn es kein Backup gibt?

  Dann müssen Sie sich bei der Suche nach Ihren Daten genauso anstrengen wie beim Lesen dieser Schrift, wenn es überhaupt noch geht.
- Begrenzen Sie den Programmaustausch: das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- Prüfen Sie neue Programme vor **und** nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, läßt sich ein Virus in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu 'Ihrem' Rechner, sollten Sie gewisse Spielregeln zum Schutz vor Viren beachten:

- Mustern Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerk-Medien) sowie auch von Downloads aus. Trennen Sie diesen Rechner aber vom Netzwerk!
- Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus notwendigen Schritte.
- Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/Veränderungen vermindern helfen. Programme und Massenspeicher lassen sich ersetzen, Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- Ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird, ist ein guter Schutz gegen Viren.

5 Installation

Das sollten Sie vor der Installation beachten:

Die Installation unter Windows Me/98/95 und Windows 2000/NT verläuft grundsätzlich gleich. Einzig die Namen einiger Pfade, Dateien und Hilfsprogramme weichen voneinander ab.

Ihr Rechnersystem sollte vor der Installation virenfrei sein. Wenn Sie sich dessen nicht sicher sind, starten Sie Ihren Rechner von der Notfall- bzw. Startdiskette Ihres Betriebssystemes.
Hinweise dazu finden Sie in diesem Handbuch unter dem entsprechenden Kapitel ab Seite 138.

Befindet sich während der Installation ein Virus im Speicher, könnte jede installierte Datei infiziert werden. Beachten Sie, daß auch bereits Windows-Dateien infiziert sein können! Daher ist ***vor* der Installation** ein Neustart von einer ‘sauberen’ DOS-Diskette bzw. Windows Startdiskette anzuraten.

Nach einer Erstinstallation empfehlen wir, unverzüglich alle Dateien auf allen erreichbaren Laufwerken nach Viren zu überprüfen. Wählen Sie bitte dazu im Menü 'Optionen' unter dem Menüpunkt 'Suchen/Dateien' die Option 'Alle Dateien' aus. Die Virensuche dauert bei dieser Einstellung länger, da wesentlich mehr Dateien geprüft werden. Deshalb sollte die Einstellung 'Alle Dateien' nicht als Standard übernommen werden.

Funktionen der allgemeinen Schaltflächen des Setup-Programmes

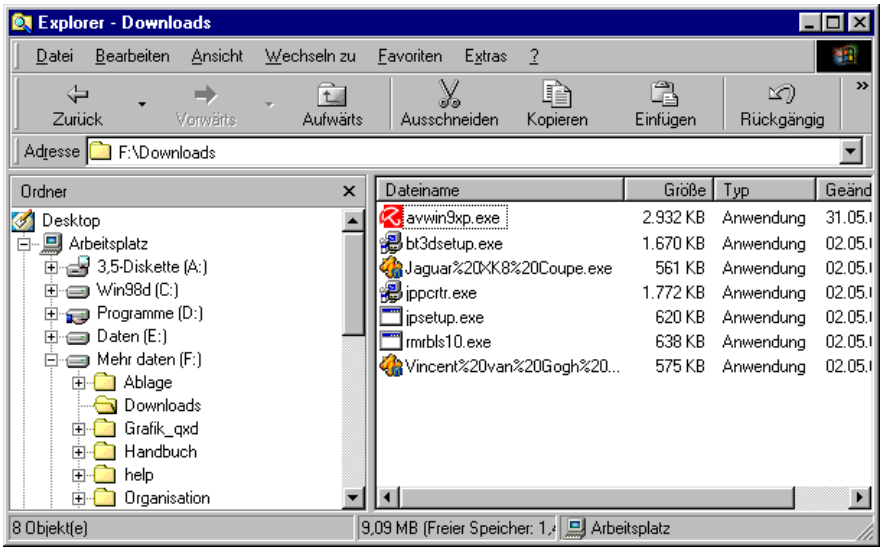
Im gesamten Setup-Programm führt Sie die Schaltfläche Weiter > zum nächsten Schritt. Die Installation kann mit der Schaltfläche Abbrechen beendet werden. Mit der Schaltfläche < Zurück gelangen Sie zum vorherigen Fenster des Setups, mit der Schaltfläche Hilfe läßt sie die Hilfe zum Setup-Programm aufrufen.

5.1 AntiVir® Personal Edition installieren

Download aus dem Internet

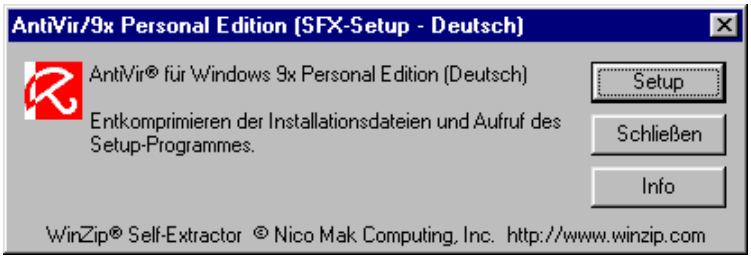
➔ Starten Sie den Download der AntiVir Personal Edition und kopieren Sie die gepackte Datei in einen (temporären) Ordner auf einer lokalen Festplatte (beispielsweise C:\HELP).

➔ Öffnen Sie den Windows-Explorer und wechseln Sie auf diesen Ordner:



➔ Klicken Sie im Fenster 'Inhalt von ...' des Windows-Explorers auf den Dateinamen AVWIN9XP.EXE bzw. AVWINNTP.EXE.

Nun erscheint das Fenster des SFX-Setup:



➔ Bestätigen Sie diese Meldung mit der Schaltfläche **Setup**, wird die Aktualisierung gestartet. Mit **Schließen** gelangen Sie unverrichteter Dinge zum Windows-Explorer zurück.

Wird die Aktualisierung mit Setup gestartet, werden zuerst die Programmdateien der entsprechenden Version von AntiVir (in diesem Beispiel die deutschsprachige Version der Personal Edition für Windows Me) dekomprimiert:

Ist dieser Vorgang abgeschlossen, wird sofort das Setup-Programm der AntiVir Personal Edition gestartet. Sie brauchen ab jetzt nur noch der Benutzerführung zu folgen.

Und hier ist die Beschreibung der Installationsschritte im Einzelnen:

Das Setup-Programm

Es erscheint zuerst die Meldung, daß InstallShield vorbereitet wird:

Danach durchsucht AntiVir den Hauptspeicher nach residenten Viren.

Wird bei der Suche ein aktiver Virus im Hauptspeicher gefunden (das geschieht zwar selten, ist jedoch nicht ausgeschlossen), wird die Installation der AntiVir Personal Edition sofort abgebrochen. Befindet sich während der Installation ein Virus im Speicher, könnte jede geprüfte bzw. installierte Datei infiziert werden.

Keine Panik! Schalten Sie Ihr Rechnersystem nicht sofort aus!

➔ Machen Sie ein Backup der fraglichen Datenträger, falls kein aktuelles Backup existiert – besser ein Backup mit Virus als gar keines.

➔ Unternehmen Sie jetzt einen zweiten Installationsversuch:

Booten Sie von einer 'bekanntermaßen guten DOS-Diskette' bzw. Ihrer 'bekanntermaßen guten Windows Systemdiskette'.
Versuchen Sie nun erneut, die AntiVir Personal Edition wie vorher beschrieben zu installieren.

Schlägt dies erneut fehl, sind möglicherweise Systemdateien infiziert (und es herrscht big trouble in little China: Es könnte eine Windows-Datei infiziert sein. Wird diese beim Start von Windows ausgeführt, ist der entsprechende Virus wieder im Speicher aktiv und AntiVir kann nicht installiert werden.). Hier können die Hinweise im Kapitel 'Erste Hilfe' ab Seite 138 weiterhelfen.

Ist dieser Vorgang beendet, heißt Sie das nächste Fenster des Setup-Programmes willkommen:

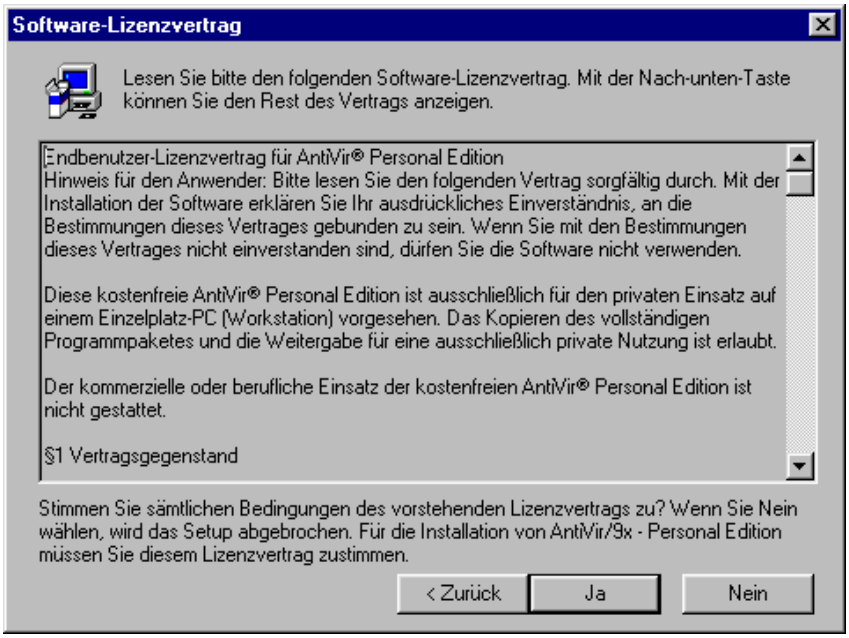
Hier empfiehlt Setup, alle Anwendungen zu schließen. Das ist besonders wichtig, wenn Sie ein Update durchführen wollen und noch eine Anwendung aus dem AntiVir-Programmpaket geöffnet ist.

➔ Mit Strg+Esc gelangen Sie in die Task-Leiste, dort können Sie noch geöffnete Programme schließen.

Bevor Sie ein Update der AntiVir Personal Edition durchführen, schließen Sie bitte auch den AntiVir Guard. Dieser wird in der Titelzeile mit dem Befehl 'Schießen' Alt+F4 oder im Menü 'Steuerung/Steuerprogramm beenden' geschlossen (*nicht* mit der Schaltfläche X oder dem Befehl 'Deaktivieren'!).

➔ Bestätigen Sie diese Meldung mit Weiter >, wenn alle Anwendungen geschlossen und alle Daten gesichert sind.

Jetzt werden Sie auf die Lizenzbedingungen aufmerksam gemacht:



Lesen Sie solche Texte gerne in etwas größerer Schrift oder schwarz auf weiß, finden Sie diese Lizenzbedingungen auch in diesem Handbuch ab Seite 10.

➔ Um die Installation fortsetzen zu können, müssen Sie diesen Bestimmungen durch Betätigen der Schaltfläche Ja zustimmen. Mit der Schaltfläche Nein wird die Installation abgebrochen.

Haben sie die Lizenzbedingungen akzeptiert, erscheint dieses Fenster:

Komponenten

In diesem Listenfeld wählen Sie aus, welche Programmteile und Hilfsprogramme auf Ihrem Computer installiert werden sollen. Dabei können Sie auswählen zwischen:

Programmdateien	alle vom Hauptprogramm benötigten Programm- und Hilfsdateien.
FAQ	eine Auflistung der häufig gestellten Fragen und deren Antworten. Bei der Lösung von Problemen ist dies die erste Informationsquelle.
Scheduler	kann zu festgelegten Zeiten einen Suchlauf mit AntiVir starten, andere Programme aufrufen oder Meldungen anzeigen.
Shell Erweiterung	im Explorer läßt sich ein Suchlauf in der Liste 'Alle Ordner' (linke Seite) über die rechte Maustaste mit dem Befehl 'Virensuche mit AntiVir' starten.
Supportkollektor	für eine schnelle Bearbeitung einer Supportanfrage via E-Mail benötigen wir eine Datei mit wichtigen Systemdaten, die mit Hilfe des Supportkollektors erstellt wird.

AVGuard ist der Virenwächter, der bei jedem Start von Windows aufgerufen wird und Dateien automatisch auf Virenbefall untersucht.

Zielordner

Gemäß der Voreinstellung legt das Setup-Programm automatisch einen Ordner namens AVPERSONAL an, und zwar im Ordner PROGRAMME desjenigen Laufwerkes, auf dem Windows installiert wurde (in der Regel Laufwerk C:). Dort werden alle Dateien installiert, die AntiVir benötigt. Beachten Sie, daß auf dem ausgewählten Datenträger mindestens 6 MB freier Speicherplatz vorhanden sein muß.

Wenn Sie in der Anzeigegruppe 'Zielordner' auf die Schaltfläche Durchsuchen . . . rechts neben der Eingabezeile klicken, erscheint ein Fenster, in dem Sie ein Laufwerk und einen Ordner auswählen können. Sie können auch direkt einen neuen Ordnernamen in die Eingabezeile eingeben, dieser Ordner wird bei der Installation automatisch erstellt.

Unter der Anzeigegruppe 'Zielordner' wird der von AntiVir benötigte Speicherplatz sowie der freie Speicherplatz auf dem Laufwerk des Zielordners angezeigt. Mit Hilfe der Schaltfläche Speicherplatz . . . läßt sich überprüfen, wie viel Platz auf den übrigen erreichbaren Laufwerken vorhanden ist.

➔ Entspricht die Auswahl der Komponenten und des Zielordners Ihren Wünschen, bestätigen Sie die Einträge mit Weiter >.

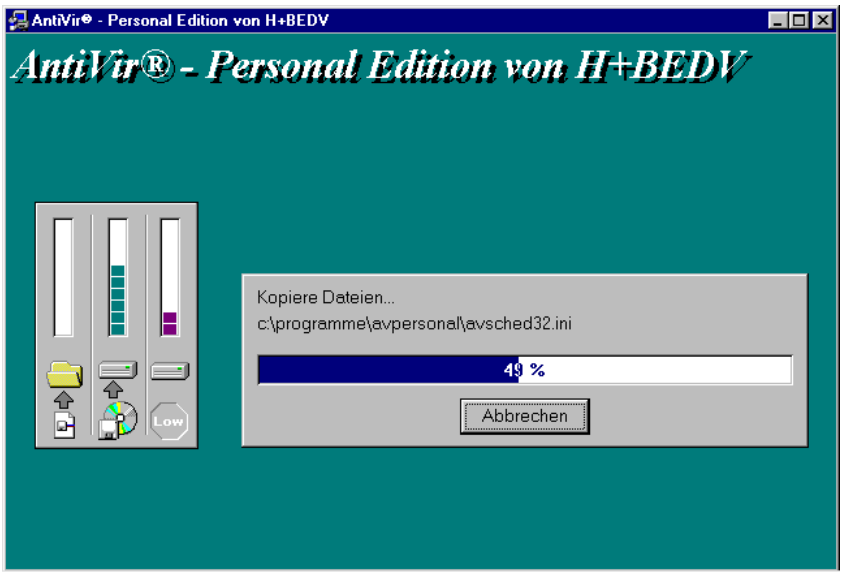
Das Setup-Programm legt automatisch Programmsymbole und einen Programmordner für AntiVir an. Gemäß der Voreinstellung wird der Programmordner 'AntiVir – Personal Edition von H+BEDV' vorgeschlagen. Sie können die Programmdateien aber auch in einen bereits vorhandenen Programmordner einfügen.

Wird im gleichen Ordner ein Update durchgeführt, wird keine neue Programmgruppe benötigt.

➔ Soll der voreingestellte Programmordner erstellt werden, bestätigen Sie den Eintrag 'AntiVir 9x – Personal Edition von H+BEDV' im Eingabefeld 'Programmordner' mit Weiter >.

➔ Soll AntiVir einem bereits vorhandenen Programmordner hinzugefügt werden, klicken Sie den Namen dieses Programmordners im Feld 'Vorhandene Ordner' an. Dieser Name wird daraufhin in das Feld 'Programmordner' übernommen. Bestätigen Sie anschließend Ihre Auswahl mit Weiter >.

Im nächsten Fenster können Sie beobachten, wie Setup alle notwendigen Dateien des AntiVir-Programmpaketes im Zielverzeichnis installiert:



Sobald der Kopiervorgang abgeschlossen ist, erscheint dieses Fenster:

➔ Bestätigen Sie die Voreinstellung 'Ja, jetzt nach Viren suchen' mit der Taste ↵ oder der Schaltfläche Weiter>, startet AntiVir einen Suchlauf.

Wenn Sie in diesem Fenster den Eintrag 'Nein, nicht durchsuchen' markieren, überspringt das Setup-Programm die Virensuche. Wir empfehlen, zumindest bei der Erstinstallation unbedingt einen Suchlauf durchzuführen, sonst handeln Sie sich Ärger ein, wenn sich doch ein Virus auf dem Rechner befindet und aktiviert wird.

Im nächsten Fenster entscheiden sie, ob Ihr Rechner jetzt neu gestartet werden soll:

➔ Bestätigen Sie die Voreinstellung 'Ja, Computer jetzt neu starten' mit der Taste ↵ oder der Schaltfläche Beenden, startet Windows neu.

Die AntiVir Personal Edition und der Guard sowie alle weiteren Hilfsprogramme stehen Ihnen nach dem Neustart vollständig zur Verfügung.

Wollen Sie den Computer jetzt nicht neu starten, klicken Sie das Optionsfeld 'Nein, Computer wird später neu gestartet' an. Betätigen Sie zur Bestätigung die Schaltfläche Beenden, gelangen Sie wieder zur Windows-Oberfläche. Die AntiVir Personal Edition und der AntiVir Guard werden dann erst nach dem nächsten Start von Windows vollständig konfiguriert sein.

Nach einer Erstinstallation empfehlen wir, alle Dateien auf allen erreichbaren Laufwerken nach Viren zu überprüfen. Wählen Sie bitte dazu im Menü 'Optionen' unter dem Menüpunkt 'Suchen/Dateien' die Option 'Alle Dateien' aus. Die Virensuche dauert bei dieser Einstellung länger als im Modus 'Programmdateien', da wesentlich mehr Dateien geprüft werden. Deshalb sollte die Einstellung 'Alle Dateien' nicht als Standard übernommen werden.

➔ Rufen Sie das Hauptfenster von AntiVir durch Anklicken des Icons 'AntiVir Personal Edition' in der AntiVir-Programmgruppe oder auf dem Desktop auf.

➔ Öffnen Sie nach Aufruf des Hauptprogrammes das Dialogfenster 'Optionen' mit der Schaltfläche Optionen oder der Tastenkombination Alt+O / S die Registerkarte 'Suchen'.

➔ Klicken Sie in der Gruppe 'Dateien' das Optionsfeld 'Alle Dateien' an.

➔ Bestätigen Sie diese Auswahl mit OK. Das Dialogfenster 'Optionen' wird geschlossen.

➔ Aktivieren Sie im Hauptfenster von AntiVir das Kontrollfeld 'Alle Laufwerke wählen'. Vor sämtlichen Laufwerkssymbolen in der Laufwerksliste muß nun ein Kontrollhäkchen sichtbar sein.

➔ Starten Sie einen Suchlauf mit der Schaltfläche Suche starten oder der Funktionstaste F2.

Spürt AntiVir während des Suchlaufs Viren auf und stellt Sie vor die Frage, was mit diesen geschehen soll, finden Sie im Kapitel 'Infizierte Dateien reparieren' ab Seite 51 weitere Informationen.

➔ Wurden keine Viren gemeldet oder alle Viren entfernt, öffnen Sie bitte das Fenster 'Optionen' erneut mit der Schaltfläche Optionen oder der Tastenkombination Alt+O / S die Registerkarte 'Suchen'.

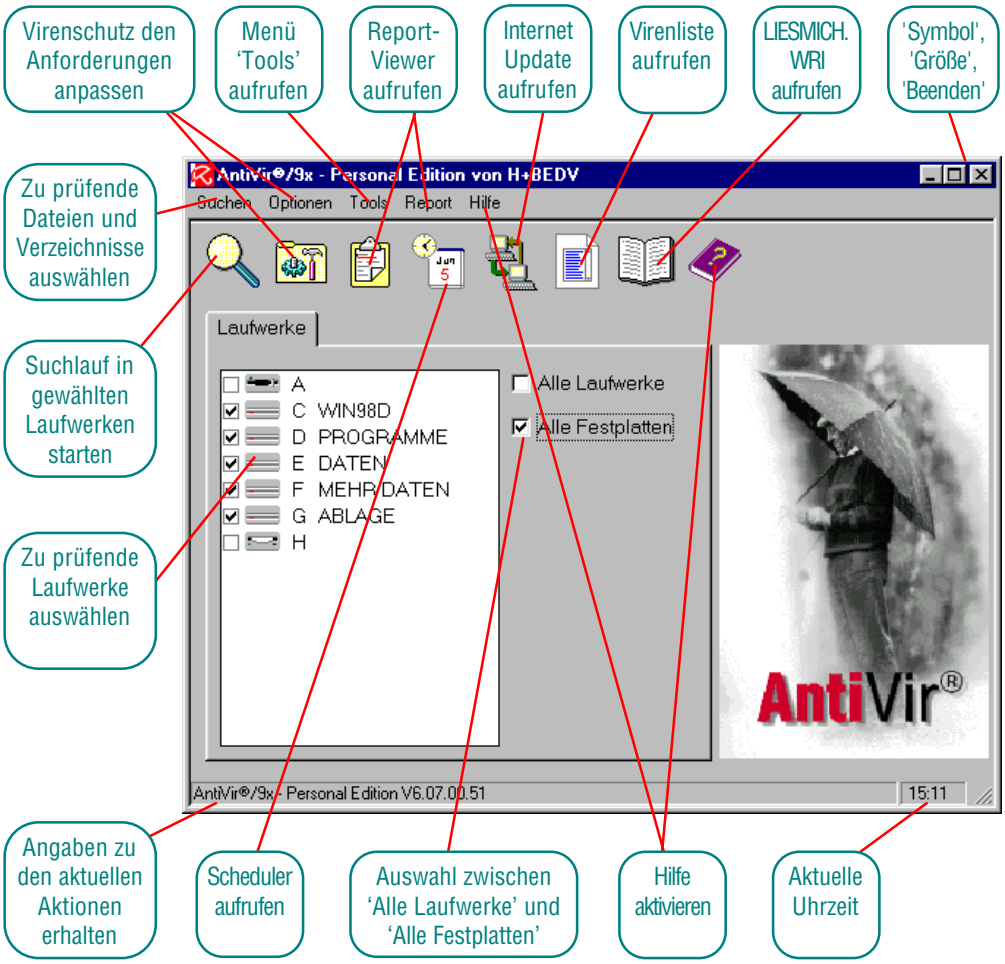
➔ Klicken Sie in der Gruppe 'Dateien' das Optionsfeld 'Alle Dateien' an.

➔ Bestätigen Sie diese Auswahl mit OK. Das Fenster 'Optionen' wird geschlossen.

6 Was bietet die Bedienoberfläche?

In den folgenden Kapiteln beschreiben wir die Vorgehensweise bei den Standard-Anwendungen von AntiVir. Sie finden hier die meisten Beispiele, wie Sie AntiVir nutzen können. Wenn Sie Fragen zu bestimmten Stichworten haben, hilft Ihnen sicherlich der Index im Anhang dieses Handbuches ab Seite 154 weiter.

Und das läßt sich mit den einzelnen Menüs und Schaltflächen anstellen:



Standard-Schaltflächen

Bei AntiVir werden die Standard-Schaltflächen von Windows verwendet, die entsprechenden Befehle lassen sich auch mit den folgenden Tastenkombinationen aufrufen. Um deren Funktion nicht immer zu wiederholen, präsentieren wir die Erklärungen vorneweg:

OK	Alt+O	bestätigt die letzte Aktion
Abbruch	Alt+A	bricht die letzte Aktion ab
Hilfe	Alt+H	zeigt die Hilfe zum aktivierten Fenster an

Wird die Funktion einer Standard-Schaltfläche erweitert oder weicht eine Funktion von den hier genannten Definitionen ab, wird die Erklärung unter dem entsprechenden Menü gegeben.

Standard-Tastenkombinationen

Mit folgenden Tastenkombinationen werden die entsprechenden Funktionen von AntiVir aktiviert:

F1	Hilfe wird aufgerufen
F2	Suche starten
ESC	Dialogfenster wird geschlossen
Alt+F4	Die Programme von AntiVir für Windows bzw. das aktive Fenster eines Programmes werden beendet

Schaltflächen der Symbolleiste im Hauptfenster

Und das passiert, wenn Sie die entsprechende Schaltfläche anklicken:


Ein Suchlauf wird gestartet


Das Internet-Update wird gestartet


Die Registerkarten mit den Optionen werden aufgerufen


Die Virenliste wird aufgerufen


AntiVir Report wird aufgerufen


Die Datei LIESMICH.WRI wird aufgerufen

Der Scheduler von AntiVir wird aufgerufen


Die kontextsensitive Hilfe wird aufgerufen

7 AntiVir starten

Die Programmgruppe AntiVir

Wurde beim Setup der vorgeschlagene Programmordner beibehalten, erscheint nach der Installation die Gruppe 'AntiVir/Me Personal Edition' bzw. 'AntiVir/2000 Personal Edition' auf dem Windows Desktop.

➔ Starten Sie ein hier aufgeführtes Programm oder eine Informationsdatei durch Doppelklicken auf das entsprechende Icon.

Verknüpfung auf dem Desktop

➔ Ist eine Verknüpfung mit AntiVir auf dem Desktop eingerichtet, läßt sich AntiVir durch Doppelklick auf das Icon der Verknüpfung aufrufen.

Wurde bei der Installation keine Verknüpfung eingerichtet, können Sie das jederzeit mit folgenden Schritten nachholen:

➔ Öffnen Sie den Windows-Arbeitsplatz oder den Windows Explorer.

➔ Suchen Sie im Arbeitsplatz oder im Explorer die Datei AVWIN9x.EXE AVWINNT.EXE.

➔ Klicken Sie auf das Icon dieser Datei, halten die Maustaste gedrückt und ziehen das Symbol auf das Desktop.

Das Icon erscheint auf dem Desktop, Sie können es dort an eine beliebige Stelle verschieben.

➔ Starten Sie AntiVir durch Doppelklick auf das AntiVir Schirm-Icon.

Auch die anderen Module, beispielsweise AntiVir® Report oder der AntiVir® Scheduler, lassen sich durch eine Verknüpfung auf dem Desktop starten. Das gilt sogar für die Virenliste, die AntiVir Hilfe und die Datei LIESMICH.WRI.

Die Schaltfläche Start in der Task-Leiste

Beim Setup wird im Startmenü von Windows im Ordner 'Programme' die Gruppe 'AntiVir Personal Edition' angelegt.

➔ Klicken Sie auf die Schaltfläche Start in der Task-Leiste und bewegen Sie den Mauszeiger auf 'Programme'.

Ein Pop-Up-Menü mit weiteren Programmordnern und ausführbaren Programmen erscheint.

➔ Bewegen Sie den Mauszeiger auf den Ordner 'AntiVir Personal Edition'.

Eine Liste mit den Namen 'AntiVir Hilfe', 'AntiVir Liesmich', 'AntiVir', 'AntiVir Report', 'AntiVir Scheduler', 'AntiVir Support Collector', 'AntiVir Virusinformation', 'Deinstallieren von AntiVir' und 'FAQ' wird aufgerufen.

➔ Klicken Sie auf den Namen der Datei, die Sie öffnen möchten. Diese Anwendung wird aufgerufen.

Ein wesentlich einfacherer Weg um AntiVir aufzurufen führt an dieser Stelle über die rechte Maustaste:

➔ Klicken Sie mit der auf die Schaltfläche Start in der Task-Leiste, erscheint ein Popup-Menü.

➔ Klicken Sie auf die Zeile 'Virensuche mit AntiVir', wird AntiVir aufgerufen und in den vorgegebenen Laufwerken ein Suchlauf gestartet.

Dann gibt es mit Hilfe der Schaltfläche Start in der Task-Leiste noch einen Weg über das Menü 'Ausführen':

➔ Klicken Sie auf die Schaltfläche Start in der Task-Leiste.

➔ Bewegen Sie den Mauszeiger auf 'Ausführen' und klicken Sie auf diesen Menüpunkt. Es erscheint das gleichnamige Fenster.

➔ Geben Sie in das Feld 'Öffnen' den Programmnamen AVWIN9X.EXE (AVWINNT.EXE) mit dem korrekten Pfad ein, bei der Standard-Installation wäre dies:

```
C:\PROGRAMME\AVPERSONAL\AVWIN9X.EXE   bzw.
C:\PROGRAMME\AVPERSONAL\AVWINNT.EXE
```

Erscheint eine Meldung, das Programm könne nicht gefunden werden, klicken Sie auf die Schaltfläche Durchsuchen und fahnden in diesem Dialogfenster nach der Datei.

Das Menü 'Suchen nach'

Wissen Sie nicht genau, auf welchem Pfad AntiVir installiert wurde (der Standard-Ordner ist C:\PROGRAMME\AVPERSONAL), führt ein Weg über die Funktion 'Suchen nach':

➔ Öffnen Sie das Dialogfenster 'Suchen nach' entweder im Menü 'Start' unter 'Suchen > Dateien/Ordner' oder im Explorer mit Hilfe der Menüleiste 'Extras/Suchen' mit der Auswahl 'Dateien/Ordner'.

➔ Geben Sie in das Feld 'Name:' den Dateinamen AVWIN9X.EXE bzw. AVWINNT.EXE ein.

➔ Wählen Sie über das Listenfeld 'Suchen in' das Laufwerk aus, auf dem sich der Ordner 'AVWIN9x' ('AVWINNT') befindet oder lassen Sie den gesamten Arbeitsplatz durchsuchen. Das Kontrollkästchen 'Untergeordnete Ordner einbeziehen' muß aktiviert sein.

➔ Betätigen Sie die Schaltfläche Durchsuchen, um die Suche zu beginnen.

War die Suche erfolgreich, erscheint der Dateiname in der Liste unter dem Fenster 'Suchen nach: ... '.

➔ Öffnen Sie AntiVir durch Doppelklicken auf das AntiVir Schirm-Icon unter dem Feld 'Name'.

Der Windows-Explorer

Dieser Weg macht die Virensuche im Explorers kinderleicht:

➔ Rufen Sie den Windows-Explorer auf.

➔ Markieren Sie eine Datei, ein Verzeichnis oder ein Laufwerk und klikken Sie auf die rechte Maustaste.

➔ Starten Sie im markierten Bereich eine Direktsuche: entweder durch Anklicken der Zeile 'Virensuche mit AntiVir' oder durch die Tastenfolge V / ↵.

AntiVir beginnt sofort mit der Suche und gibt nach dem Suchlauf im Statusfenster an, welche Daten durchsucht und ob Viren gefunden wurden.

Das Hauptprogramm sowie alle übrigen Programme der AntiVir Personal Edition lassen sich auch manuell im Explorer starten: öffnen Sie den Ordner, in dem sich AntiVir befindet (standardmäßig C:\PROGRAMME\AVPERSONAL) über das Listenfeld 'Alle Ordner'. Rufen Sie dort AntiVir (oder eine andere ausführbare Datei) in der Liste 'Inhalt von ...' durch Doppelklicken auf den Dateinamen AVWIN9X.EXE bzw. AVWINNT.EXE auf.

Start mit der Shell-Erweiterung

Jedes markierte Laufwerk, jeder markierter Ordner sowie jede markierte Datei kann auf dem Desktop, auf dem Windows-Arbeitsplatz und im Explorer, ja sogar im Fenster 'Öffnen' von vielen Windows-Programmen mit Hilfe der Shell-Erweiterung direkt auf die digitalen Plagegeister untersucht werden.

➔ Markieren Sie eine Datei, ein Verzeichnis oder ein Laufwerk und klikken Sie dort auf die rechte Maustaste.

➔ Starten Sie im markierten Bereich eine Direktsuche: entweder durch Anklicken der Zeile 'Virensuche mit AntiVir' oder durch die Tastenfolge V / ↵.

Es wird nun das Hauptprogramm der AntiVir Personal Edition aufgerufen und die markierten Objekte werden – abhängig von der Konfiguration von AntiVir – überprüft. Nach Beendigung der Suche wird das Fenster 'Status' (Notizblock) angezeigt. Wird dieses Fenster mit OK geschlossen, wird auch das Hauptprogramm beendet.

Automatischer Start von AntiVir

Mit der Autostart-Funktion von Windows läßt sich AntiVir bei jedem Start von Windows aufrufen:

➔ Klicken Sie auf die Schaltfläche Start in der Task-Leiste.

➔ Bewegen Sie den Mauszeiger auf 'Einstellungen' und klicken Sie im Pop-Up-Menü auf 'Task-Leiste'. Es erscheint das Fenster 'Eigenschaften von Task-Leiste'.

- Klicken Sie dort auf die Registerkarte 'Programme im Menü Start' und betätigen dort die Schaltfläche Hinzufügen. Es erscheint das Fenster 'Verknüpfung erstellen'.

- Geben Sie in dieses Fenster entweder den vollständigen Pfad ein (ggf. auch mit einem Kommandozeilenparameter) oder wählen Sie den Pfad mit Hilfe der Option Durchsuchen.

- Mit der Schaltfläche Weiter > gelangen Sie in ein Fenster, in dem eine Liste mit verschiedenen Programmgruppen angezeigt werden.

- Klicken Sie dort auf die Programmgruppe 'Autostart' und bestätigen Sie die Auswahl mit Weiter >.

- Es erscheint ein weiteres Fenster, in dem Sie den Namen für die Verknüpfung ändern können. Bestätigen Sie die Auswahl mit Weiter >.

- Schließen Sie das Fenster 'Eigenschaften von Task-Leiste' mit OK, werden die Einstellungen übernommen

Das AntiVir Hauptprogramm wird nun im Ordner 'Autostart' angezeigt und bei jedem Start von Windows automatisch aufgerufen.

Diese Funktion bietet sich besonders beim AntiVir Scheduler an: Das Programm wird sofort nach dem Start von Windows aufgerufen und der Scheduler kann, solange Windows läuft, keinen Termin „vergessen". Wie Sie den Scheduler einrichten können, damit er nur als Symbol gestartet wird, erfahren Sie in der Online-Hilfe von Windows unter dem Stichwort 'Minimiertes Fenster / Programm starten als'.

Beim Start von AntiVir werden automatisch ein Speicher-, ein System- und ein Selbsttest durchgeführt sowie die Master-Bootsektoren aller erreichbaren Festplatten und die Bootsektoren aller erreichbaren Laufwerke geprüft. Eine Virensuche können Sie anschließend manuell starten.

Wenn Sie Ihren Computer täglich zu festen Zeiten nutzen, bietet sich an, den Scheduler von AntiVir mit Autostart zu aktivieren. So können Sie sowohl AntiVir als auch Meldungen oder andere Programme zu den im Scheduler eingegebenen Zeiten starten.

Was sich mit dem Scheduler anstellen läßt, erfahren Sie im Kapitel 'AntiVir zum festgelegten Zeitpunkt starten' ab Seite 103.

8 Bestimmte Datenträger untersuchen

Sie bekommen ein neues Programm oder Daten und wollen diese Dateien auf Viren untersuchen. Oder Sie möchten Ihr Computersystem einfach nur routinemäßig durchchecken. AntiVir bietet Ihnen viele Auswahlmöglichkeiten, um den Kreis der zu durchsuchenden Dateien genau einzugrenzen. Doch was ist dabei zu tun?

Es wurde beim Start von AntiVir kein Virus im Hauptspeicher gemeldet (bzw. ein digitaler Schädling wurde erfolgreich beseitigt) und Sie haben sowieso für alle Fälle ein aktuelles Backup.

Es gibt nun mehrere Wege, Laufwerke, Ordner und Dateien gezielt zu untersuchen, die wir Ihnen in diesem Kapitel vorstellen:

8.1 Laufwerke, Ordner und Dateien auswählen

➔ Starten Sie AntiVir.

Direktauswahl in der Laufwerk-Liste des Hauptfensters

➔ Markieren Sie in der Laufwerk-Liste die Laufwerke, die durchsucht werden sollen. Dabei stehen Ihnen auch die Tasten Umschalt und Strg zur Verfügung, wenn Sie mehrere Laufwerke markieren wollen.

➔ Markierte Laufwerke können Sie abwählen, indem Sie erneut auf diese Zeile klicken. Die Markierung wird dann aufgehoben.

AntiVir verwendet folgende Symbole für Laufwerke:

 Diskettenlaufwerk

 Festplattenlaufwerk

 CD Rom

 RAM Disk

Unbekannter Laufwerkstyp

Auswahl in der Laufwerksliste des Hauptfensters

Alle Laufwerke wählen Alt+L**:** Ist dieses Kontrollkästchen aktiviert, werden alle vorhandenen lokalen Laufwerke (Diskettenlaufwerke, CD-Laufwerke, auswechselbare Speichermedien und Festplatten, aber *keine* Netzlaufwerke) angewählt bzw. abgewählt.

Alle Festplatten wählen Alt+F**:** Mit dieser Schaltfläche werden alle vorhandenen lokalen Festplatten angewählt bzw. abgewählt Die übrigen Laufwerkstypen sowie Netzlaufwerke bleiben außen vor. Das Feld ist nur aktiv, wenn auch Festplatten erkannt werden.

Bei diesen Einstellungen ist eine Umkehr möglich: Ist beispielsweise 'Alle Festplatten' markiert und Sie betätigen die Schaltfläche 'Alle Festplatten' erneut, werden sämtliche Markierungen der Festplatten in der Laufwerksliste aufgehoben.

Datei oder Ordner mit Drag & Drop auswählen

- Öffnen Sie den Windows Explorer sowie AntiVir. Ordnen Sie die Fenster beider Programme so auf dem Desktop an, daß ein Teil des Hauptfensters von AntiVir sichtbar ist.
- Markieren Sie im Explorer eine oder mehrere Dateien bzw. einen oder mehrere Ordner und halten dabei die linke Maustaste gedrückt.
- Ziehen Sie die markierten Dateien oder Ordner auf das Hauptfenster von AntiVir.

Diese Dateien oder Ordner werden sofort nach Loslassen der Maustaste nach Viren durchsucht.

Bootsektoren lokaler Laufwerke auswählen

Sie können auch gezielt Bootsektoren auswählen, die auf Virenbefall überprüft werden sollen.

Öffnen Sie die folgende Liste im Menü 'Suchen' den Menüpunkt 'Bootsektoren' oder verwenden Sie dazu die Tastenkombination Alt+S / B:

- Markieren Sie in der Laufwerk-Liste die Laufwerke, die durchsucht werden sollen.
- Markierte Laufwerke können Sie abwählen, indem Sie erneut auf die entsprechende Zeile klicken. Die Markierung wird dann aufgehoben.
- Starten Sie die Suche mit der Schaltfläche Suchen oder der Tastenkombination Alt+S.

8.2 Einen Suchlauf starten

➔ Sie können einen Suchlauf auf verschiedenen Wegen starten:

- Durch Anklicken der Schaltfläche Suchen
- über die Menüleiste 'Suchen/Suche Starten'
- die Tastenkombination Alt+S / S
- die Funktionstaste F2
- mit Hilfe der Drag & Drop-Funktion
- mit der Shell-Erweiterung

Luke Filewalker – der Computer-Kollege von Luke Skywalker aus den Star Wars-Filmen – wird gestartet und überprüft die Dateien in den ausgewählten Bereichen. In diesem Beispiel hat er bereits einen Virus gefunden, die Datei WW_256.DOC im Hauptverzeichnis von Laufwerk A:\ wird gerade untersucht:

Außerdem erhalten Sie Informationen über die Anzahl der bisher durchsuchten Dateien, die benötigte Zeit, die Anzahl der Viren 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' mit einem ✔ aktiviert, können Sie den Suchlauf mit der Schaltfläche Stop unterbrechen. Das spart viel Zeit, wenn Sie aus Versehen eine randvolle Gigabyte-Festplatte scannen, auf der all Ihre Programme untergebracht sind.

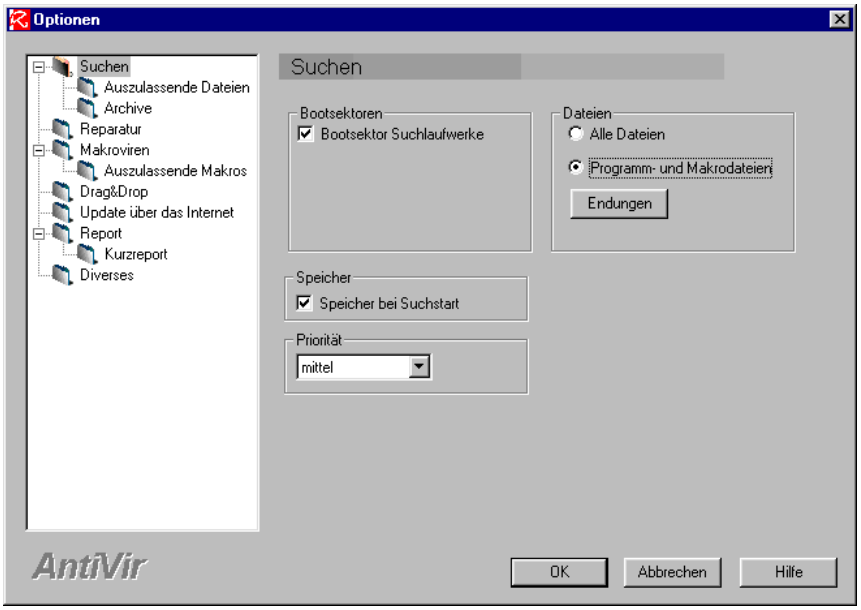
Der Notizblock im Fenster 'Status' zeigt an, ob ein bekannter Virus vorhanden ist. Das Ausrufezeichen über den Schaltflächen weist auf einen Virenfund hin. Fehlt es, gibt's zum Glück auch keinen bekannten Virus. In diesem Beispiel wurde die Suche normal beendet. Von den acht entdeckten Viren ließen sich sieben entfernen, eine infizierte Datei wurde gelöscht:

Mit der Schaltfläche Report wird der Dateibetrachter AntiVir Report aufgerufen, der einen ausführlichen Bericht über die Konfiguration von AntiVir und die Ergebnisse des letzten Suchlaufes anzeigt.

Mit der Schaltfläche Kurzreport gelangen Sie in ein Fenster, in dem Sie Informationen über die Ergebnisse der letzten Suchläufe erhalten.

8.3 Voreinstellungen zur Suche ändern

➔ Rufen Sie das Konfigurationsfenster zur Suche mit der Schaltfläche Optionen auf. Es erscheint zuerst das Fenster 'Suchen':



In der Anzeigegruppe **'Bootsektoren'** können Sie wählen zwischen:

- **Bootsektor Suchlaufwerke** Alt+B

Ist diese Funktion aktiviert – das erkennen Sie am ✔ – wird beim Start der Virensuche der Bootsektor der zu durchsuchenden Laufwerke auf Viren geprüft.

In der Anzeigegruppe **'Dateien'** können Sie wählen zwischen:

- **Alle Dateien** Alt+D

Per Voreinstellung untersucht AntiVir ausschließlich Programmdateien. Ist der Menüpunkt 'Alle Dateien' angewählt, werden sämtliche Dateien auf den entsprechenden Laufwerken nach Viren durchsucht, auch nicht ausführbare Dateien werden gescannt.

Diese Einstellung sollte nur nach einem Virenfund aktiviert werden, um einmal alle Dateien zu überprüfen. Sollen alle Dateien durchsucht werden, dauert die Virensuche länger, da wesentlich mehr Dateien geprüft werden müssen. Ist 'Alle Dateien' aktiv, läßt sich die Schaltfläche Endungen nicht anwählen.

- **Programmdateien** Alt+G

Mit dieser Funktion werden nur Dateien mit einer vorgegebenen Endung durchsucht (z.B. *.COM, *.EXE, *.DO? usw.). Bei den Endungen sind in der Default-Einstellung von AntiVir bereits Standardwerte vorgegebenen. Wenn Sie die Schaltfläche Endungen betätigen, lassen sich diese Einträge in dem neu aufgerufenen Fenster ändern.

Im Fenster **'Dateiendungen'** sind alle Endungen in der Liste angezeigt, die bei einem Suchlauf berücksichtigt werden. Voreingestellt sind die gebräuchlichsten Endungen von Programmdateien und solchen Dokumenten, in denen auch Makros gespeichert sein können:

In die Liste der Programm- und Dokumentendateien werden – soweit erforderlich – immer wieder neue Dateitypen aufgenommen. Im Fenster 'Dateierweiterungen' können Sie mit der Bildlaufleiste in der Liste blättern und nachsehen, welche Dateiendungen geprüft werden

Haben Sie Programmdateien mit anderen Endungen auf Ihrem Rechner, können Sie diese Endungen in die Liste mit Dateiendungen einfügen.

Im Fenster 'Dateiendungen' wird mit der Schaltfläche Einfügen oder der Tastenkombination Alt+E ein Dialogfenster geöffnet, in dem Sie Dateiendungen direkt eingeben können. Es werden maximal 3 Zeichen akzeptiert, der führende Punkt darf nicht mit eingegeben werden. Ein ungültiges Zeichen wird nicht akzeptiert, Wildcards (* und ?) sind als Stellvertre-

ter erlaubt. Nach Bestätigung mit OK werden ab dem nächsten Suchlauf Dateien mit dieser Endung ebenfalls geprüft.

Geben Sie bitte keine Endungen nicht ausführbarer Dateien ein, dies kann den Zeitbedarf für einen Suchlauf beträchtlich erhöhen.

Wird im Fenster 'Dateiendungen' die Schaltfläche Standard oder die Tastenkombination Alt+S betätigt, werden die vorhandenen Endungen gelöscht und die voreingestellten Dateinamenserweiterungen in die Liste übernommen.

Die Anzeigegruppe **'Speicher'**:

- **Speicher bei Suchstart** Alt+S

Ist diese Schaltfläche markiert, wird der Hauptspeicher Ihres Computers bei jedem Suchlauf nach Viren durchsucht. Diese Funktion sollte immer aktiv sein, um einen größtmöglichen Schutz vor Viren zu erhalten. Ist ein Virus im Speicher aktiv, können alle Dateien, die durchsucht werden, unter Umständen infiziert werden. Starten Sie in diesem Fall Ihr System von einer virenfreien, schreibgeschützten Systemdiskette neu.

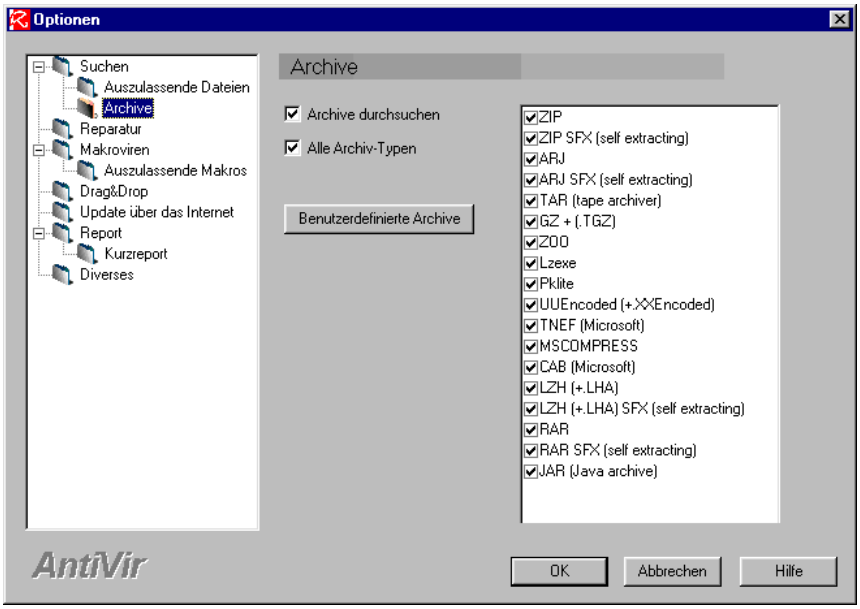
Die Anzeigegruppe **'Priorität'**:

In dem Listenfeld dieser Gruppe können Sie die Priorität des Suchvorganges 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.

Wollen Sie mit einem anderen Programm weiterarbeiten, während AntiVir nach Viren sucht, empfehlen wir, die niedrige Priorität zu wählen. Der Prozessor wird dann für die andere Anwendung weitaus häufiger freigegeben. Soll AntiVir nach Viren suchen, ohne daß andere Programme aktiv sind, wählen Sie die hohe Priorität; der Suchvorgang wird dann schneller beendet.

Der Ordner 'Archive'

In diesem Ordner können Sie die Einstellungen zu den Archiven vornehmen, die von AntiVir durchsucht werden sollen:



- **Archive durchsuchen**

➔ Ist das Kontrollkästchen 'Archive durchsuchen' mit einem Häkchen markiert, untersucht AntiVir bei einem Suchlauf auch alle Archive der Archiv-Typen, die im nebenstehenden Fenster markiert sind. Ist dieser Eintrag nicht markiert, werden alle Daten in Archiven von einem Suchlauf ausgenommen.

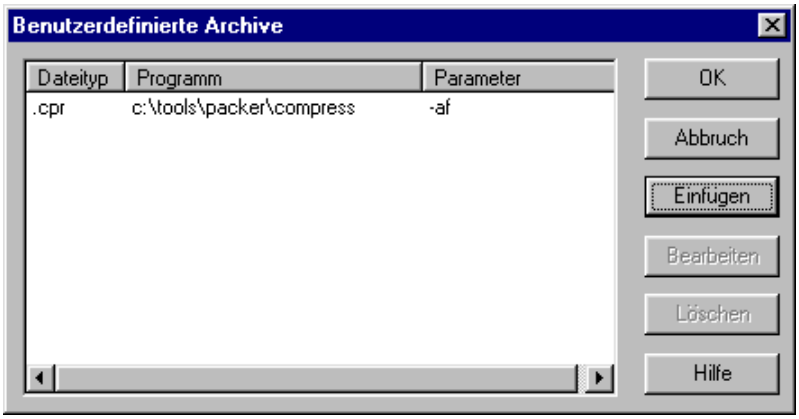
- **Archive durchsuchen**

➔ Mit dem Kontrollkästchen 'Alle Archiv-Typen' werden alle Einträge im rechten Fenster markiert bzw. die markierten Einträge aufgehoben.

- **Listenfeld Archiv-Typen**

➔ Im Fenster mit den Archiv-Typen können Sie durch Anklicken eines Kontrollkästchens den entsprechenden Archiv-Typ einzeln markieren bzw. von der Suche ausnehmen.

➔ Mit der Schaltfläche Benutzerdefinierte Archive wird ein Fenster geöffnet, in dem benutzerdefinierte Archive eingetragen sind. Hier lassen sich weitere Programme hinzufügen oder bereits vorhandene Einträge löschen:



➔ Soll ein neues Archiv eingefügt werden oder ein vorhandener Eintrag bearbeitet werden (der Pfad zum Packprogramm hat sich geändert oder es soll ein anderer Parameter verwendet werden), wird durch Anklicken der Schaltfläche Einfügen bzw. Bearbeiten ein weiteres Fenster geöffnet:

➔ Mit der Schaltfläche OK wird der Eintrag in das Listenfeld des Fensters 'Benutzerdefinierte Archive' übernommen, mit Abbruch kehren Sie unverrichteter Dinge zu diesem Fenster zurück.

➔ Mit der Schaltfläche Löschen wird ein markierter Eintrag im Listenfeld des Fensters 'Benutzerdefinierte Archive' gelöscht.

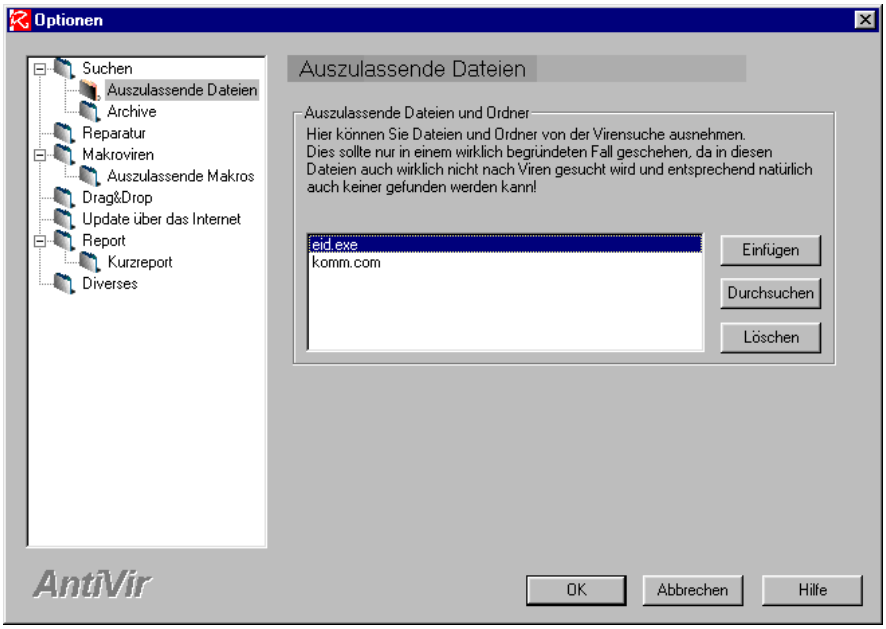
Bei den benutzerdefinierten Archivprogrammen benötigen Sie das Entpackprogramm, mit dem das entsprechende Archiv erstellt wurde. Außerdem muß ein Pfad auf denjenigen Ordner gelegt sein, in dem sich das ent-

sprechende Packprogramm befindet (z.B. in der AUTOEXEC.BAT ein Eintrag PATH=C:\PACKER;C:\REST; ...). Sie können auch in das Feld unter dem jeweiligen Packprogramm den Pfad direkt eingeben oder mit Hilfe der Ordner-Schaltfläche suchen. Sind diese Voraussetzungen erfüllt und ist dieser Punkt aktiviert, entpackt AntiVir die Dateien aus den Archiven, durchsucht die entpackten Dateien in einem temporären Ordner und löscht diese entpackten Dateien anschließend wieder.

Ist ein Packprogramm infiziert – das wird beim Start der Suche geprüft – wird die entsprechende Option automatisch abgewählt. Wird der Packer nicht gefunden, wird die entsprechende Option ebenfalls abgewählt.

Der Ordner ' Auszulassende Dateien'

➔ In diesem Fenster sind alle Dateien aufgelistet, die bei einem Suchlauf ausgenommen werden sollen:



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

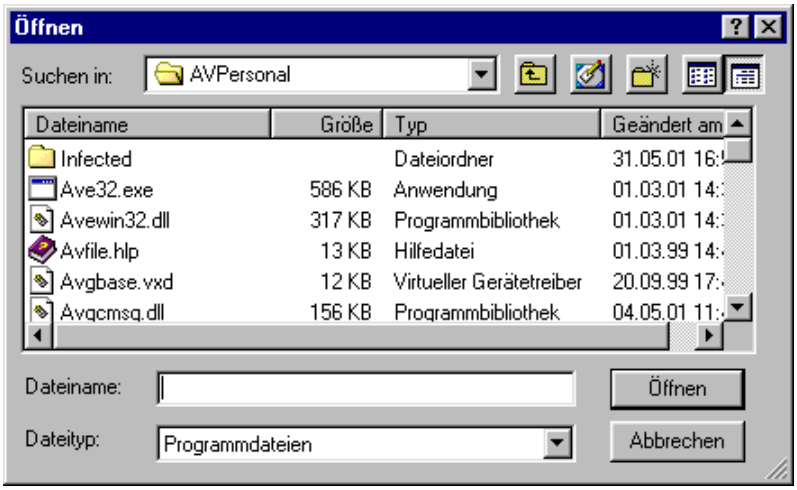
➔ Um der Liste einen Eintrag hinzuzufügen, klicken Sie auf die Schaltfläche Einfügen oder benutzen Sie die Tastenkombination Alt+E. Es erscheint ein Dialogfenster, in dem Sie einen Dateinamen für eine auszulassende Datei eingeben können:

➔ Tragen Sie den Namen und gegebenenfalls den Pfad der auszulassenden Datei in das Feld 'Auszulassende Datei' ein.

Geben Sie hier nur einen Dateinamen an, wird jede Datei mit diesem Namen auf jedem angewählten Laufwerk bei einem Suchlauf übergangen. Soll nur eine bestimmte Datei mit genau diesem Namen (Dateiname und Extension) nicht berücksichtigt werden, müssen Sie den kompletten Pfad und Namen eingeben. Bestätigen Sie den Eintrag mit der Taste ↵ oder OK.

➔ Bestätigen Sie den Eintrag mit der Taste ↵ oder OK.

Durchsuchen Alt+D: Wenn Sie den Pfad oder den Dateinamen der auszulassenden Datei nicht genau wissen, können Sie im Fenster 'Auszulassende Dateien' mit der Schaltfläche Durchsuchen ein Dialogfenster zur Suche auf einem Datenträger öffnen.



Im Feld 'Suchen in' wählen Sie das Laufwerk und den Ordner aus, in dem sich die auszulassende Datei befindet. Markieren Sie in der Auswahlliste einen Dateinamen, wird dieser automatisch in das Feld 'Dateiname' übernommen. Mit der Schaltfläche Öffnen gelangen Sie wieder zurück zum Fenster 'Auszulassende Dateien'. Der ausgewählte Dateiname wird in der Liste aufgeführt.

Löschen Alt+L: Um einen Eintrag zu löschen, markieren Sie in der Liste die Datei, die gelöscht werden soll. Klicken Sie anschließend auf die Schaltfläche Löschen.oder benutzen Sie die Tastenkombination Alt+L.

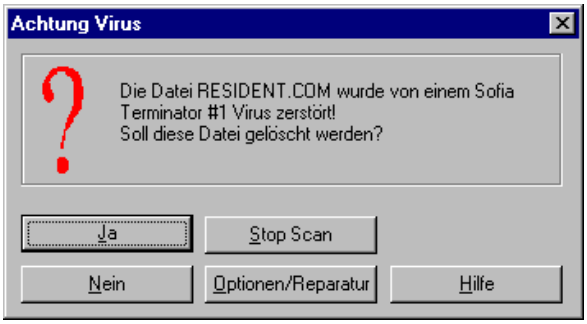
Die Schaltfläche Löschen ist nicht aktiv, wenn kein Eintrag vorhanden oder markiert ist.

➔ Bestätigen Sie alle Änderungen im Fenster Auszulassende Dateien mit der Taste ↵ oder der Schaltfläche OK, sonst werden die Änderungen nicht übernommen.

9 Infizierte Dateien reparieren

9.1 AntiVir meldet: Virus gefunden

Sie führen einen Suchlauf auf einem Datenträger durch, auf dem sich infizierte oder zerstörte Dateien befinden. Sofern Sie nichts an den Voreinstellungen verändert oder AntiVir mit bestimmten Kommandozeilenparametern gestartet haben, meldet AntiVir einen Virus in dieser Form:



Ob eine Meldung ausgegeben, eine infizierte Datei mit oder ohne Rückfrage repariert, gelöscht oder infizierte Dateien nur in der Reportdatei genannt werden, hängt von den Voreinstellungen unter 'Optionen/Reparatur' ab.

Egal wie Sie sich entscheiden, anschließend erscheint eine Meldung, was mit den Viren geschah. In unserem Beispiel wurden acht Viren erkannt, sieben infizierte Dateien repariert und eine infizierte Datei gelöscht:

Wollen Sie genau wissen, welche Dateien infiziert waren und ob auch alles korrekt über die Bühne gegangen ist, können Sie jetzt mit der Schaltfläche Report die Reportdatei aufrufen. Mit der Schaltfläche Kurzreport läßt sich eine Statistik der letzten Suchläufe aufrufen.

In der Regel läuft alles glatt und die erkannten Viren werden von Ihrem Computer entfernt. Stellen Sie in der Statusanzeige oder der Reportdatei jedoch fest, daß nicht alle Dateien repariert wurden – auch AntiVir ist nicht unfehlbar, ja manchmal birgt eine Reparatur sogar Gefahren und es wird absichtlich nicht repariert, so etwa bei dem Bootsektorvirus 'Form' oder bei Viren mit Stealth-Techniken – gilt als wichtigste Regel:

* * * **Keine Panik!** * * *

Bewahren Sie einen kühlen Kopf und beachten Sie folgende Punkte:

➔ Schalten Sie Ihr Rechnersystem noch nicht sofort aus.

➔ Machen Sie, wenn Ihr Rechnersystem noch reagiert, ein Backup der fraglichen Datenträger – besser ein Backup mit Virus als gar keines.

Wenn Ihr Rechner jetzt nicht mehr reagiert, haben Sie ein ernsthaftes Problem, vor allem, falls Ihnen keine aktuellen Backups zur Verfügung stehen.

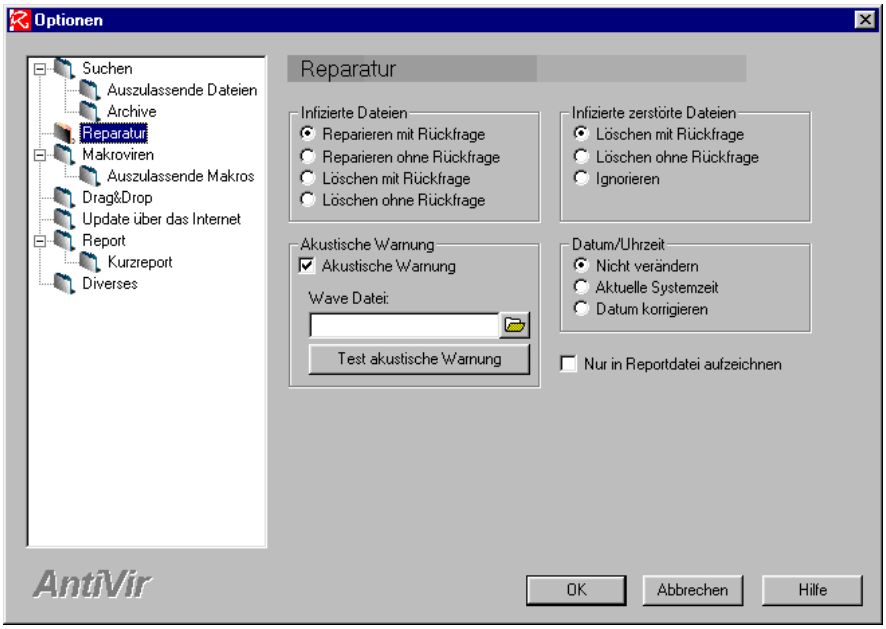
Doch auch dann möchten wir Ihnen Mut zusprechen und verweisen auf das Kapitel 'Erste Hilfe' ab Seite 138 dieses Handbuchs. Dort wird beschrieben, wie Sie den Viren mit Hilfe der 'bekanntermaßen guten Systemdiskette' und AntiVir zu Leibe rücken können.

9.2 Voreinstellungen zur Reparatur ändern

Im Menü 'Optionen/Reparatur' legen Sie fest, wie AntiVir reagieren soll, wenn ein Virus gefunden wurde. Die Bandbreite der Aktionen reicht vom Aufzeichnen der Ereignisse bis hin zur Reparatur der infizierten Dateien.

➔ Rufen Sie das Konfigurationsfenster mit der Schaltfläche Optionen auf und klicken im Auswahlfenster auf den Ordner 'Reparatur'.

Die meisten Einstellungen in diesem Menüpunkt lassen sich nur anwählen und sind auch nur wirksam, wenn der Punkt 'Nur in Reportdatei aufzeichnen' *nicht* aktiviert ist.



In der Anzeigegruppe **'Infizierte Dateien'** können Sie wählen zwischen:

- **Reparieren mit Rückfrage** Alt+M

AntiVir fragt nach Auffinden einer infizierten reparablen Datei zuerst zurück, ob die entsprechende Datei repariert werden soll (Voreinstellung).

- **Reparieren ohne Rückfrage** Alt+K

Infizierte reparable Dateien werden sofort ohne Rückfrage repariert.

- **Löschen mit Rückfrage** Alt+F

Infizierte Dateien werden nach Rückfrage gelöscht. Wollen Sie sichergehen, daß sich die infizierte Datei nicht wieder herstellen läßt (z.B. mit UNFORMAT), markieren Sie zusätzlich unter 'Optionen/Diverses' den Punkt 'Zu löschende Dateien überschreiben'. Ist 'Zu löschende Dateien überschreiben' aktiviert, werden auch infizierte Dateien gelöscht, die vielleicht reparabel sind.

- **Löschen ohne Rückfrage** Alt+R:

Infizierte Dateien werden ohne Rückfrage gelöscht. Wollen Sie sicher gehen, daß sich die infizierte Datei nicht wieder herstellen läßt (z.B. mit UNFORMAT), markieren Sie zusätzlich unter 'Optionen/Diverses' den Punkt 'Zu löschende Dateien überschreiben'.

In der Anzeigegruppe **'Infizierte zerstörte Dateien'** können Sie wählen:

- **Löschen mit Rückfrage** Alt+C

Konnte eine infizierte Datei nicht repariert werden, weil sie z.B. durch einen Virus zerstört wurde, wird diese Datei nach Rückfrage gelöscht, wenn diese Einstellung aktiv ist (Voreinstellung). Wollen Sie sicher gehen, daß sich die infizierte Datei nicht wieder herstellen läßt (z.B. mit UNFORMAT), aktivieren Sie unter '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 'Löschen ohne Rückfrage' aktiviert, wird die entsprechende Datei ohne Rückfrage gelöscht. Wollen Sie sicher gehen, daß sich die infizierte Datei nicht wieder herstellen läßt (z.B. mit UNFORMAT), aktivieren Sie unter 'Optionen/Diverses' den Punkt 'Zu löschende Dateien überschreiben'.

- **Ignorieren** Alt+I

Ist diese Einstellung aktiv, wird eine nicht reparable Datei nicht gelöscht.

Verbleibt eine defekte Datei auf Ihrem System, ist diese Datei zwar wahrscheinlich nicht mehr lauffähig, aber sie enthält immer noch virulenten Code, der gegebenenfalls Schaden anrichten kann.

In der Anzeigegruppe **'Akustische Warnung'** können Sie ändern:

- **Akustische Warnung** Alt+W

Ist diese Einstellung aktiviert, meldet sich Ihr Rechnersystem laut und deutlich, wenn ein Virus aufgestöbert wird – vorausgesetzt, ein Lautsprecher ist angeschlossen. Im Normalbetrieb ist diese Einstellung anzuraten, sind jedoch viele Dateien infiziert, kann das Piepen einige Nerven kosten.

- **Wave Datei** Alt+E

In diesem Feld können Sie den Pfad und den Namen einer Wave-Datei angeben, die Sie bei einem Virenfund warnen soll. Der Button mit dem Ordner-Symbol öffnet ein Fenster, in dem Sie nach einer vorhandenen oder selbst erstellten Wave-Datei suchen können.

Die Schaltfläche Test akustische Warnung bzw. die Tastenkombination Alt+T dienen zum Ausprobieren der ausgewählten Wave-Datei. Voraussetzung dafür sind eine Soundkarte und eingeschaltete Brüllwürfel (Lautsprecher wäre meist eine Beleidigung für jede anständige HiFi-Anlage).

In der Anzeigegruppe **'Datum/Uhrzeit'** können Sie einstellen:

- **Nicht verändern** Alt+V

Das Datum und die Uhrzeit einer infizierten Datei wird bei einer Reparatur normalerweise auf das aktuelle Systemdatum gesetzt (Voreinstellung). Dabei erfolgt ein schreibender Zugriff auf diese Datei (der Virencode muß ja entfernt werden). Sollen die originalen Datums- und Zeitangaben der Datei beibehalten werden, aktivieren Sie diese Einstellung.

- **Aktuelle Systemzeit** Alt+S

Das Datum und die Zeit 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 ist der Vienna-Virus, der den Sekundeneintrag der infizierten Datei auf 62 setzt. Mit 'Datum korrigieren' setzt AntiVir die Datums- und Zeitangaben nach einer Reparatur wieder auf einen gültigen Wert.

Haben Sie Spiele von der Firma Sierra auf Ihrem Rechner installiert, sollten Sie diese Einstellung nicht wählen. Sierra erhöht die Jahreszahl um 100. Ein Tremor-Virus macht das ebenfalls, um infizierte Dateien erkennen zu können. Und woher soll AntiVir nun wissen, ob es sich um Ihr Spiel oder einen Virus handelt?

- **Nur in Reportdatei aufzeichnen** Alt+V

Ist diese Einstellung aktiviert, werden weder Reparaturen vorgenommen noch infizierte Dateien gelöscht! Wird in der Reportdatei ein Virus gemeldet, müssen Sie selbst entscheiden, was mit den infizierten Dateien geschehen soll. Damit auch immer eine Reportdatei erstellt wird, sollten Sie im Menü 'Optionen/Report' den Punkt 'Kein Report erstellen' *nicht* ausschalten.

9.3 AntiVir meldet: Makrovirus gefunden

Die Makroviren erobern einen immer größer werdenden „ Marktanteil“ in der Welt der Viren. AntiVir sucht in Formatvorlagen, beispielsweise von MS-Word, nach dieser speziellen Art von Viren.

Oft werden die Makroviren als Dokumentviren bezeichnet, was allerdings so nicht ganz richtig ist. Bei Word-Dateien basiert jedes Dokument auf einer Formatvorlage (unter Word 6/7 im Normalfall der NORMAL.DOT), von der eine Kopie in der Dokumenten-Datei (=.DOC) angelegt wird. Diese Formatvorlagen können gegenüber den Dokumenten jedoch zusätzliche Daten enthalten. Öffnet beispielsweise Word 6/7 eine Formatvorlage (.DOT oder .WIZ-Dateien), dann sucht es nach solchen Daten. Unter Word 8 werden je nach Voreinstellung diese Formatvorlagen im Dokument mit gespeichert. Eine Formatvorlage (engl.: Template) kann neben Menüs, speziellen Shortcuts usw. auch Makros enthalten.

Nun zum zweiten wichtigen Begriff: Ein Makro hat die Aufgabe, eine Folge von Tastatureingaben bzw. Befehlen zu einem Komplex zusammenzufassen, der wiederum mit dem Aufruf des Makros abgearbeitet wird. Auf diese Weise lassen sich häufig anfallende Arbeitsschritte automatisieren. Die von MS-Word verwendeten Makros sind in der Scriptsprache WordBasic (ab Office 97: Visual Basic for Applications) geschrieben und werden bei deren Aufruf von Word abgearbeitet. Makros können vom Benutzer manuell aufgerufen werden. Bestimmte Makros wie z.B. „ AutoOpen“ oder „ AutoClose“ werden aber von Word automatisch aufgerufen, wenn eine Formatvorlage geöffnet wird, das diese Makros enthält.

Das Gefahrenpotential dieser Makros liegt hauptsächlich in der Möglichkeit, vielfältige Dateioperationen und DOS-Kommandos auszuführen. So ist z.B. das Formatieren von Festplatten oder das Löschen von Dateien unter DOS oder Windows NT oder ein Zugriff auf die Windows-Systemumgebung (API) mit Hilfe eines Makros möglich. Auch beim Netzwerkbetrieb unter Windows NT wird der Benutzer auf einige – wenn nicht gleich alle – Dateien Schreibrechte besitzen und könnte somit Opfer einer Virenattacke werden. Makros benutzen bestimmte Methoden, um Dokumente zu infizieren. AntiVir sucht auch nach diesen Methoden und erkennt daran einen möglichen Virenbefall.

Findet AntiVir in einer Datei den Suchstring eines bekannten Makrovirus, wird dieser wie ein „ normaler“ Virus behandelt. Hier gelten die Voreinstellungen, die unter 'Optionen/Reparatur' eingestellt sind. Wurde dort in der Anzeigegruppe 'Infizierte Dateien' oder 'Infizierte zerstörte Dateien' die Auswahl 'Reparieren mit Rückfrage' oder 'Löschen mit Rückfrage' getroffen, erscheint eine entsprechende Virenmeldung:

In diesem Fenster wählen Sie aus, ob Sie mit Ja den Befehl geben, diese Datei zu reparieren oder mit Nein die Datei unangetastet zu lassen.

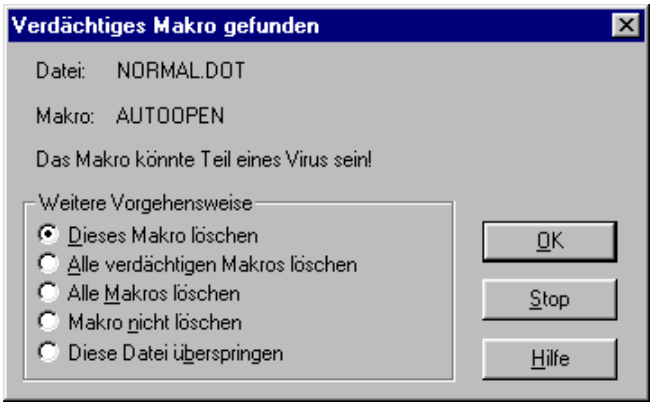
Wird eine große Zahl von Viren gemeldet, können Sie in diesem Fenster mit der Schaltfläche Stop Scan den Suchlauf abbrechen, ohne daß die zuletzt gefundene infizierte Datei repariert wird. Mit der Schaltfläche Optionen / Makroviren können Sie das Fenster mit den Voreinstellungen aufrufen und beispielsweise ändern, so daß die Virenmeldung nicht mehr erscheint und infizierte Dateien ohne Rückfragen repariert werden.

Ist in den Optionen zu den Makroviren in der Anzeigegruppe 'Formatvorlagen konvertieren' die Einstellung 'Nachfragen' aktiviert, erscheint ein Dialogfenster, wenn sich kein Makro mehr in der betreffenden Datei befindet. In diesem Fenster können Sie auswählen, ob Sie mit der Schaltfläche Ja den Befehl geben, diese Datei in ein Dokument umzuwandeln (dabei werden alle Makros in dieser Formatvorlage gelöscht) oder mit Nein die Formatvorlage unangetastet zu lassen.

AntiVir verwendet ein heuristisches Verfahren bei der Suche nach Makroviren. Dabei können wir – trotz der sehr hohen Zuverlässigkeit dieses Verfahrens, auch bis dato unbekannte Makroviren zu entdecken – Fehlmeldungen nicht ausschließen. Diese Fehlinterpretationen können auftreten bei:

- Antiviren-Makros
- Makros, die sich ähnlich wie Viren verhalten
- Makros, die Systemanalysen betreiben.

Ist in den Optionen zu den Makroviren die Einstellung 'Aktion nachfragen' in der Anzeigegruppe 'Verdächtige Makros' aktiviert und es wird bei einem Suchlauf von AntiVir ein verdächtiges Makro mit dem heuristischen Verfahren entdeckt, erscheint dieses Dialogfenster:



Dieses Makro löschen Alt+D: Bei dieser Einstellung wird das verdächtige Makro aus der Datei gelöscht.

Alle verdächtigen Makros löschen Alt+A: Es werden nur die Makros gelöscht, die Bestandteil eines Makrovirus sein könnten.

Alle Makros löschen Alt+M: Bei dieser Einstellung werden alle Makros aus der Datei gelöscht.

Makro nicht löschen Alt+N: Sind Sie sicher, daß dieses Makro kein Bestandteil eines Makrovirus ist, bleibt Ihnen dieses Makro erhalten und der Rest der Datei wird weiter nach verdächtigen Makros untersucht.

Diese Datei überspringen Alt+B: Die Datei bleibt vom Zeitpunkt der Auswahl dieser Option unverändert. Der Suchlauf wird bei der nächsten Datei fortgesetzt.

Alle Auswahlmöglichkeiten beziehen sich nur auf das Dokument, die gerade überprüft wird. Wird ein verdächtiges Makro ebenfalls von einem anderen Dokument verwendet, erscheint die Meldung 'Verdächtiges Makro gefunden' erneut.

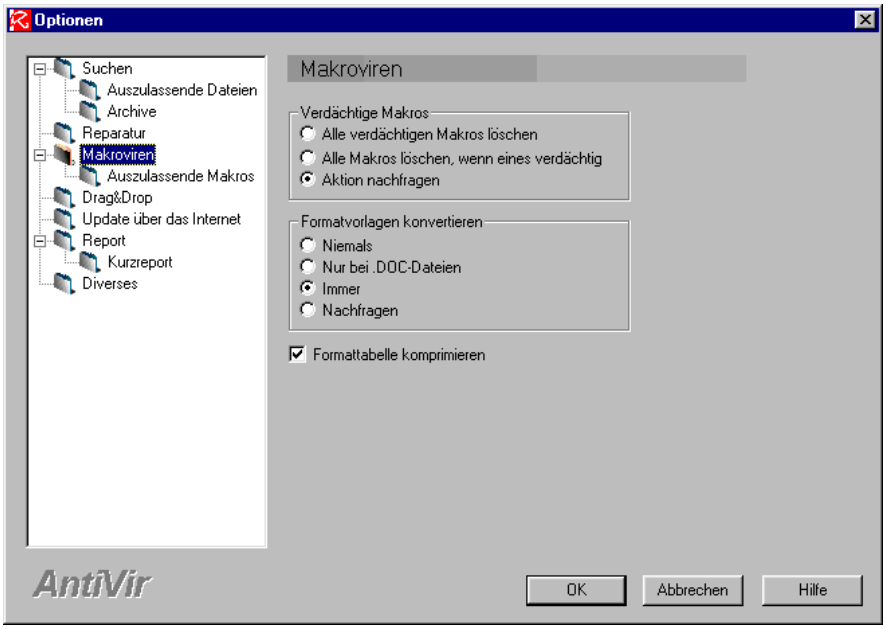
Sie können in diesem Fenster mit der Schaltfläche Stop den Suchlauf abbrechen. Doch Vorsicht: es können sich immer noch infizierte Dateien an Bord Ihres Computers befinden.

Ist in den Optionen zu den Makroviren in der Gruppe 'Formatvorlagen konvertieren' die Einstellung 'Nachfragen' aktiviert, erscheint ein weiteres Fenster, wenn kein Makro mehr in der betreffenden Datei vorhanden ist. Dort informiert Sie AntiVir darüber, daß die Datei '*.DOC eine Formatvorlage ist und fragt nach, ob diese Datei konvertiert werden soll:

➔ In diesem Fenster können Sie auswählen, ob Sie mit der Schaltfläche Ja den Befehl geben, diese Datei in ein Dokument umzuwandeln (dabei werden alle Makros in dieser Formatvorlage gelöscht) oder mit Nein die Formatvorlage unangetastet zu lassen.

9.4 Voreinstellungen zu Makroviren ändern

➔ Rufen Sie das Konfigurationsfenster mit der Schaltfläche Optionen auf und klicken im Auswahlfenster auf den Ordner 'Makroviren':



In der Anzeigegruppe **'Verdächtige Makros'** wählen Sie zwischen:

- **Alle verdächtigen Makros löschen** Alt+V

Ist dieses Optionsfeld markiert, werden alle verdächtigen Makroviren aus der gerade überprüften Formatvorlage gelöscht. Nicht verdächtige Makros bleiben in dieser Formatvorlage erhalten.

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

Finden andere Antiviren-Programme, die nur nach den Namen der Makros suchen, dieses übriggebliebene Makro, melden sie unter Umständen auch dann einen Virus, wenn die übrigen zu diesem Virus gehörenden Makros entfernt wurden.

- **Alle Makros löschen, wenn eines verdächtig** Alt+M

Ist diese Einstellung aktiviert (Voreinstellung), entfernt AntiVir ausnahmslos alle Makros aus der Formatvorlage, die gerade überprüft wird. Diese „ Radikalkur“ ist die sicherste Methode, sich der 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.

Wenn Sie häufig Makros selbst programmieren, sollten Sie besser 'Aktion nachfragen' auswählen, um nicht um den Lohn Ihrer Arbeit gebracht zu 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.

Diese Einstellung gewährleistet die größtmögliche Kontrolle über die Formattabelle – vorausgesetzt, Sie wissen, welche Makros von Ihren Vorlagen verwendet werden. Dabei hilft übrigens, sich den Inhalt der Formattabelle der wichtigsten Dokumente zu notieren.

Wollen Sie infizierte Makros nicht löschen, können Sie im Menü 'Optionen/Reparatur' den Punkt 'Nur in Reportdatei aufzeichnen' anwählen. Dann werden auch die Makroviren und möglicherweise infizierte Dateien nur in der Reportdatei aufgezeichnet.

In der Anzeigegruppe **'Formatvorlage konvertieren'** wählen Sie zwischen:

- **Niemals** Alt+L

Ist dieses Optionsfeld markiert, werden Formatvorlagen nicht umgewandelt, wenn ein Makrovirus gefunden und beseitigt wurde.

- **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 markiert, wartet AntiVir auf Ihre Bestätigung, ob die angezeigte Datei konvertiert werden soll. Dieses Feld ist in der Voreinstellung von AntiVir markiert.

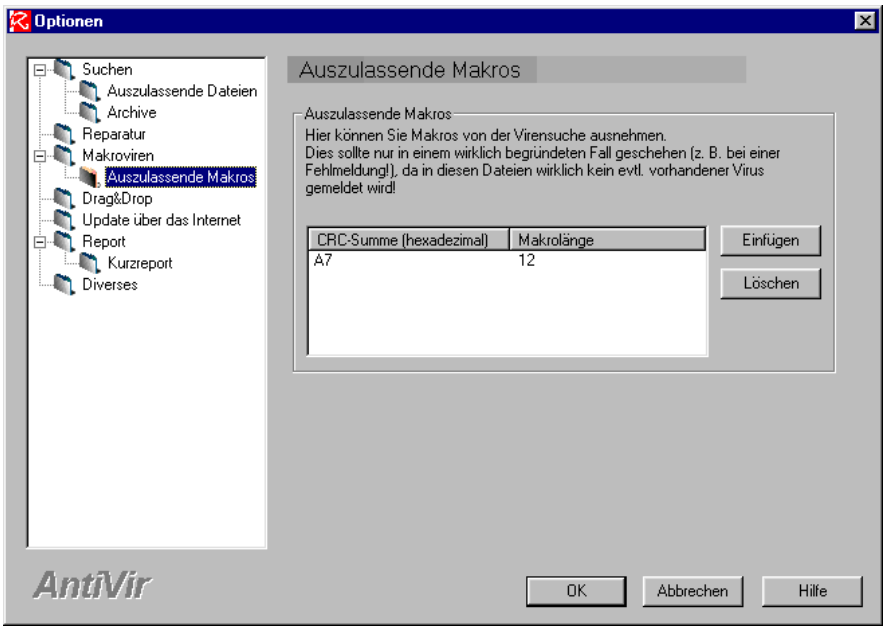
Formattabelle komprimieren Alt+K

Legen Sie hier fest, ob AntiVir auch die Referenzen auf gelöschte Makros und deren Namen aus der Tabelle der Formatvorlagen entfernen soll.

Haben Sie 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 Antiviren-Programme suchen jedoch nicht nach dem Inhalt eines Makros sondern nur nach deren Namen und melden Viren, wo keine mehr sind.

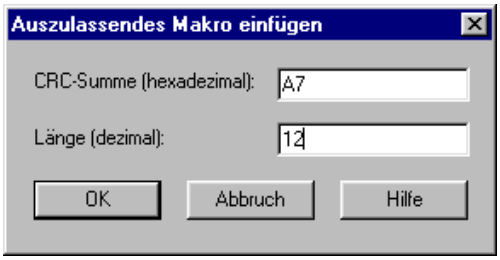
Der Ordner ' Auszulassende Makros'

➔ In diesem Fenster sind alle Makros aufgelistet, die bei einer Suche ausgenommen werden sollen:



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 normalen Suchlauf nicht kontrolliert werden sollen. Wir empfehlen, diese Makros auf jeden Fall auf Viren zu untersuchen, bevor sie in diese Liste aufgenommen werden!

Einfügen Alt+E: Um der Liste einen Eintrag hinzuzufügen, klicken Sie auf die Schaltfläche Einfügen oder benutzen Sie die Tastenkombination Alt+E. Es erscheint ein Dialogfenster, in dem Sie die CRC-Summe und die Länge des Makros für eine auszulassende Datei eingeben können:



➔ Tragen Sie die CRC-Summe des auszulassenden Makros mit ihrem hexadezimalen Wert und die Länge in Dezimalzahlen in die entsprechenden Felder ein. Die Werte für die CRC-Summe und die Länge erfahren Sie beispielsweise in der Reportdatei.

Jedes Makro mit diesen Werten wird bei einem Suchlauf übergangen. Es spielt keine Rolle, auf welchem Laufwerk sich diese Datei befindet. Wenn Sie den Eintrag mit der Taste ↵ oder OK bestätigen, erscheint nochmals eine Warnmeldung, die auf die Gefahren hinweist, wenn ein Makro von der Suche ausgeschlossen wird.

Löschen Alt+L: Um einen Eintrag zu löschen, markieren Sie in der Liste unter 'CRC-Summe (hexadezimal)' das Makro, welches aus der Liste entfernt werden soll. Klicken Sie danach auf die Schaltfläche Löschen,oder benutzen Sie die Tastenkombination Alt+L.

Die Schaltfläche Löschen ist nicht aktiv, wenn kein Eintrag vorhanden oder markiert ist.

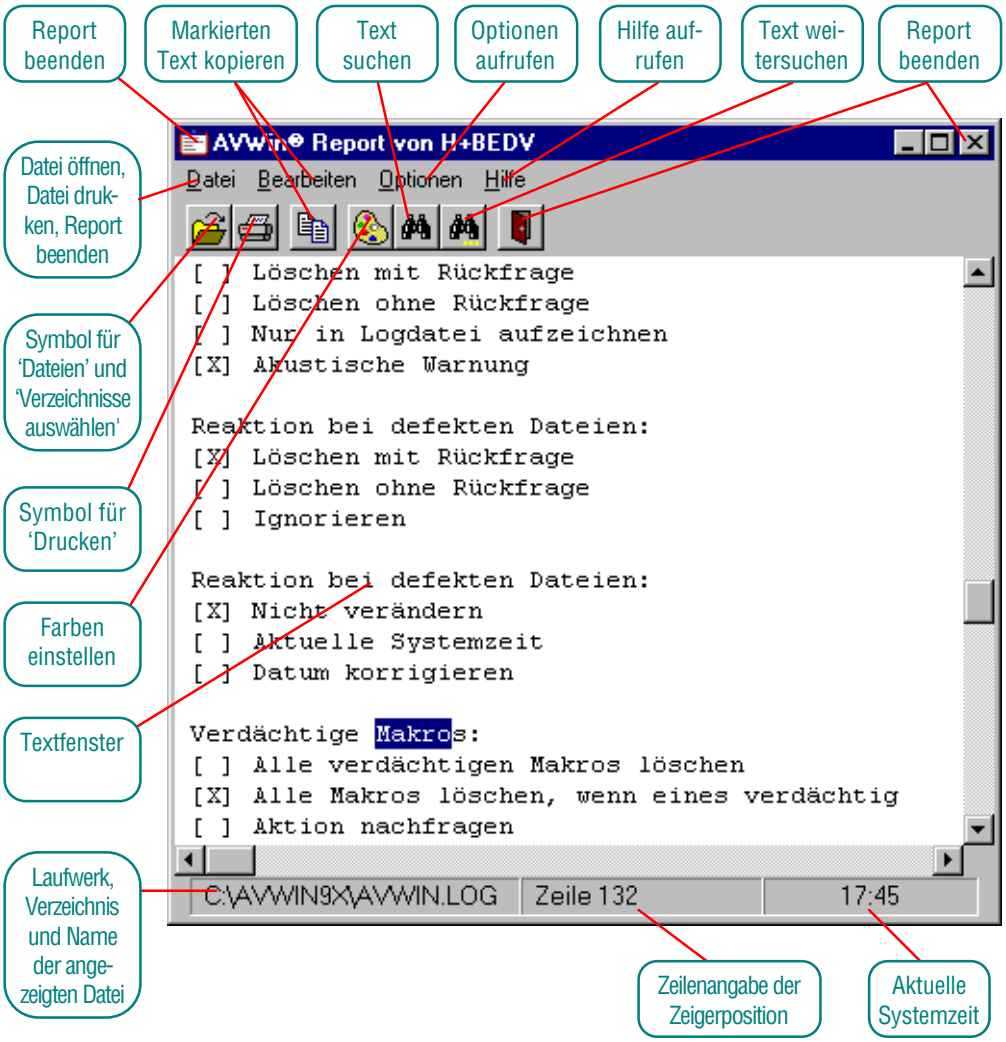
➔ Bestätigen Sie alle Änderungen im Fenster Auszulassende Dateien mit der Taste ↵ oder der Schaltfläche OK, sonst werden die Änderungen nicht übernommen.

10 Reportdatei nutzen

AntiVir Report ist ein Dateibetrachter, mit dem Sie auf einfache und bequeme Art Report- und Textdateien ansehen können. Mit AntiVir Report wird im Normalfall die Reportdatei von AntiVir geladen und angezeigt.

Besonders wichtig ist die Reportdatei, wenn Sie sich im Falle einer Virusinfektion an eine andere Stelle – beispielsweise Ihrem Systembetreuer oder unsere Hotline – wenden müssen.

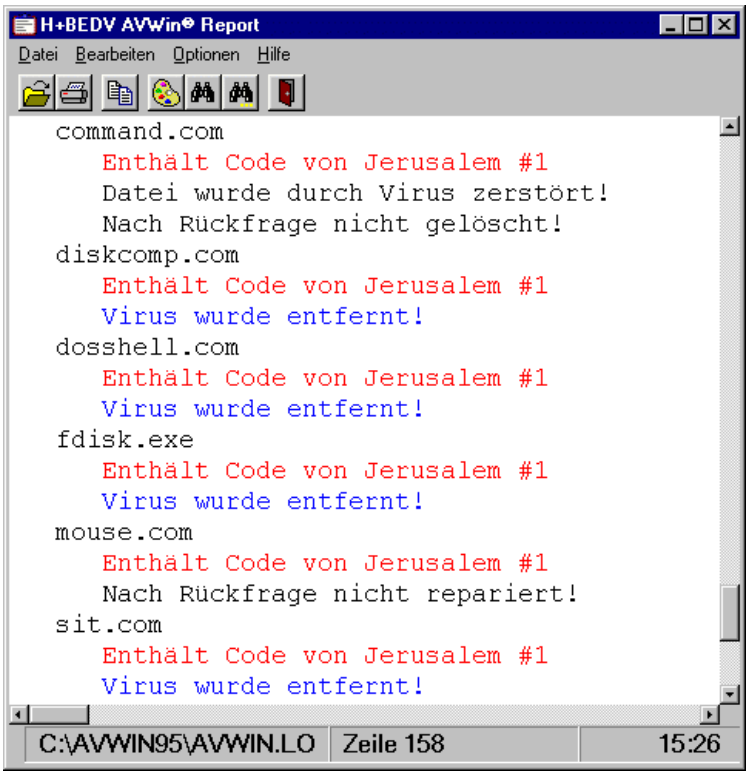
➔ Rufen Sie AntiVir Report mit der Schaltfläche Report, mit 'Report/Anzeigen' oder Alt+R / A von AntiVir aus auf.



10.1 Reportdatei vom Status-Fenster aus aufrufen

Wollen Sie genau wissen, welche Dateien infiziert waren und ob alles korrekt über die Bühne gegangen ist, rufen Sie nach einem Suchlauf die Reportdatei im Statusfenster (Notizblock) mit der Schaltfläche Report auf.

AntiVir Report präsentiert sich beim Herunterblättern nach einem umfangreichem Virenfund beispielsweise in diesem Bild:



Es werden der Name der infizierten Datei sowie in roter Schrift – sofern Sie die voreingestellte Farbe nicht geändert haben – der Name des gefundenen Virus angegeben. Eine erfolgreiche Reparatur wird in blauer Schrift, Warnungen werden „ pretty in pink“ dargestellt.

In diesem Beispiel wurde nach Rückfrage bei der Reparatur die Datei MOUSE.COM nicht repariert, der Virus befindet sich also immer noch auf Ihrem Datenträger. COMMAND.COM ist zerstört und wurde nicht gelöscht. Bei den übrigen Dateien wurde der Virus entfernt (das erkennen Sie an den blau geschriebenen Erfolgsmeldungen).

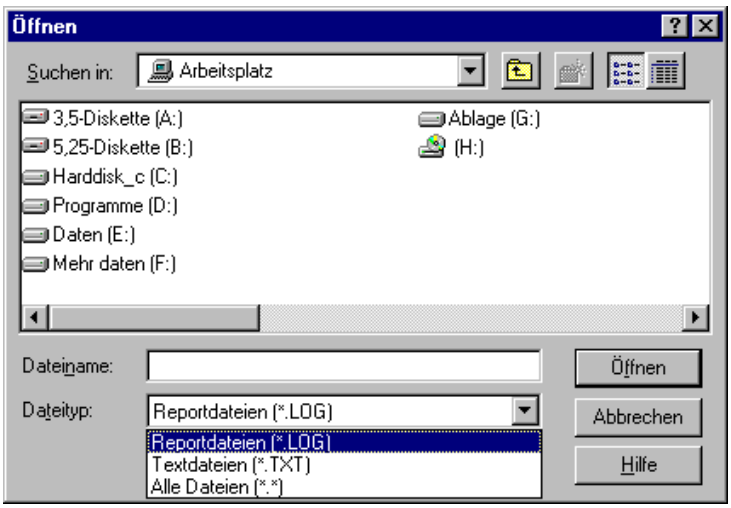
10.2 Eine Report- oder Textdatei öffnen

➔ Rufen Sie AntiVir Report vom Hauptprogramm aus mit der Schaltfläche Report, mit 'Report/Anzeigen' oder Alt+R / A auf. Oder öffnen Sie AntiVir Report über die Programmgruppe 'AntiVir/NT' aus dem Startmenü heraus. Sie können auch den Windows-Explorer bemühen. Wurde auf dem Desktop eine Verknüpfung mit AntiVir Report angelegt, öffnen Sie den Report durch Doppelklicken auf das Icon.

Es erscheint das Programmfenster mit der Reportdatei zum Protokoll des letzten Suchlaufes.

➔ Wollen Sie eine andere .LOG- oder .TXT-Datei mit AntiVir Report betrachten, betätigen Sie die Schaltfläche Ordner oder wählen Sie in der Menüleiste von AntiVir Report den Punkt 'Datei/Öffnen' aus.

Es erscheint ein Dialogfenster, in dem Sie eine Datei auswählen können, die von AntiVir Report angezeigt werden soll:



➔ Geben Sie im Feld 'Dateiname' den Namen und den Pfad derjenigen Datei an, die Sie ansehen möchten.

Der Dateiname kann auch aus dem Auswahlfenster über diesem Feld gewählt werden. In dieser Liste werden alle Dateien mit der im Feld 'Dateityp' gewählten Dateinamenserweiterung (*.LOG oder *.TXT oder *.*) angezeigt.

➔ Wählen Sie unter 'Suchen in' das Laufwerk und den Ordner aus, in dem sich die zu öffnende Datei befindet.

➔ Wählen Sie unter 'Dateityp' die Endung aus, die im Feld 'Dateiname' angezeigt werden soll:

'Reportdateien (*.LOG)'	listet alle Dateien im aktuellen Ordner mit der Dateinamenserweiterung .LOG auf.
'Textdateien (*.TXT)'	listet alle Dateien im aktuellen Ordner mit der Dateinamenserweiterung .TXT auf.
'Alle Dateien (*.*)'	listet alle Dateien im aktuellen Ordner auf.

Wurde vor dem Öffnen der neuen Datei schon eine Datei angezeigt (gewöhnlich die Reportdatei von AntiVir), wird diese geschlossen.

Report- oder Textdatei mit Drag & Drop öffnen

➔ Markieren Sie im Explorer eine *.LOG oder *.TXT-Datei, halten dabei die linke Maustaste gedrückt und ziehen die Datei mit der Maus auf das aktive AntiVir Report.

Der Inhalt dieser Datei wird dann angezeigt. Sie können bei diesen Dateien alle Funktionen nutzen, die Ihnen AntiVir Report bietet.

Läßt sich eine Datei nicht von AntiVir Report öffnen, erscheint eine Meldung in der Art 'LW:\PFAD\PROGNAME.EXE konnte nicht geladen werden'. Sind mehrere Dateien markiert, wird nur die erste Datei mit einem gültigen Format geladen. Ordner lassen sich nicht aufrufen.

Angezeigte Datei drucken

➔ Mit der Schaltfläche Drucken oder dem Menüpunkt 'Datei/Drucken' starten Sie den Ausdruck der gerade angezeigten Datei. (im Normalfall die Reportdatei von AntiVir). Treten dabei Probleme auf, überprüfen Sie den Drucker oder richten gegebenenfalls den Druckertreiber ein.

Mit der Schaltfläche Eigenschaften wird ein Dialogfenster geöffnet, in dem Sie Einstellungen für Ihren Drucker ändern.

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

Eine Textpassage suchen

Mit dem Befehl 'Suchen' können Sie nach einem Wort oder einer Textpassage in der angezeigten Datei suchen.

➔ Klicken Sie auf die Schaltfläche Suchen oder rufen Sie den Befehl 'Optionen/Suchen' auf.

Es erscheint ein Fenster mit mehreren Einstellmöglichkeiten:

➔ Geben Sie in das Feld 'Suchen nach' das Wort oder den Text ein, nach dem Sie suchen wollen.

➔ Wenn Sie das Optionsfeld 'Als Wort' markieren, wird der angegebene Text als selbständiges Wort gesucht, nicht aber als Teil eines Wortes.

➔ Wenn Sie 'Groß/Kleinschreibung' markieren, wird die Groß- und Kleinschreibung des angegebenen Textes berücksichtigt.

➔ Legen Sie mit 'Suchrichtung' die Richtung der Suche ausgehend von der aktuellen Cursorposition fest. Mit 'Aufwärts' wird von der Cursorposition bis zum Dateianfang gesucht, mit 'Abwärts' von der Cursorposition bis zum Dateiende.

Die letzten Eingaben in die Dialogbox 'Suchen' bleiben gespeichert, solange AntiVir Report aktiviert ist.

Haben Sie mit dem Befehl 'Suchen' nicht die richtige Stelle gefunden, weil z.B. der angegebene Text mehrfach im Dokument vorkommt oder in falscher Richtung gesucht wurde, können Sie mit dem Menüpunkt 'Weitersuchen' erneut nach dem zuletzt angegebenen Text suchen.

➔ Mit der Schaltfläche Weitersuchen, der Taste F3 oder durch Aufrufen des Menüpunktes 'Optionen/Weitersuchen' wiederholen Sie das letzte Suchen-Kommando.

Mit dieser Schaltfläche oder dem Menüpunkt 'Bearbeiten/Kopieren' läßt sich im Textfenster markierter Text in die Zwischenablage kopieren.

Farben der Meldungstexte auswählen

Damit Sie sich in der Reportdatei gut orientieren können, zeigt AntiVir Report einen Virenfund, Warnungen oder das Entfernen eines Virus farbig an. Mit dem Menüpunkt 'Optionen/Farben' oder durch Betätigen der Schaltfläche mit der Farbpalette wird ein Auswahlfenster geöffnet:

Per Voreinstellung wird ein gefundener Virus rot, ein entfernter Virus blau und eine Warnmeldung pink angezeigt. Um eine Farbe zu ändern, wählen Sie die entsprechende Schaltfläche **Wechseln** und es erscheint der Standarddialog zum Ändern von Farben. Sie können hier eine der angezeigten Farben auswählen und mit **OK** übernehmen.

Mit der Schaltfläche **Farben definieren** (Alt+D) wird das Dialogfenster erweitert. Hier lassen sich weitere Farben aus dem RGB-Farbspektrum auswählen und mit **Farbe hinzufügen** für die Nachwelt erhalten. Die gewünschte Farbe wird mit der Schaltfläche **OK** übernommen.

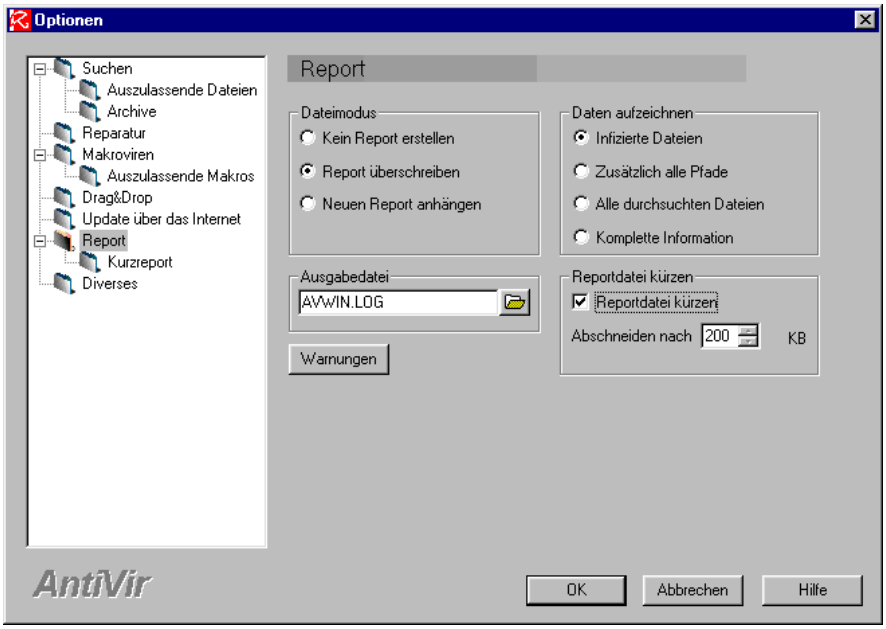
AntiVir Report beenden

Mit diesem Symbol, dem Menüpunkt 'Datei/Ende' oder der Tastenkombination Alt+F4 oder Alt+D / E sowie mit der Schaltfläche **X** rechts oben in der Titelleiste läßt sich AntiVir Report beenden.

10.3 Voreinstellungen zur Reportdatei ändern

In dieser Registerkarte können Sie Einstellungen für die Reportdatei von AntiVir vornehmen. Als Voraussetzung muß ein gültiger Dateiname für die Ausgabedatei vorhanden sein. Werden die Voreinstellungen beibehalten, wird die Reportdatei unter dem Namen AVWIN.LOG im Installationsordner von AntiVir abgelegt.

➔ Rufen Sie das Fenster 'Optionen' mit der Schaltfläche Optionen auf und klicken im Auswahlfenster auf den Ordner 'Report'. Sie können auch im Menü 'Report' direkt den Menüpunkt 'Einstellungen' anwählen.



In der Anzeigegruppe **'Dateimodus'** können Sie wählen zwischen:

- **Kein Report erstellen** Alt+K

Im normalen Betrieb sollten Sie immer eine Reportdatei erstellen lassen.

- **Report überschreiben** Alt+E

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

- **Neuen Report anhängen** Alt+N

AntiVir hängt die neue Reportdatei an eine bestehende Reportdatei an. Wenn Sie mit dieser Einstellung arbeiten, sollten Sie Ihre Reportdatei von Zeit zu Zeit wieder löschen, damit die Reportdatei durch das Anhängen nicht zuviel Platz auf Ihrer Festplatte verbrät.

Bei den folgenden Einstellungen gilt: Ist der Report ausgeschaltet, kann auch keine Reportdatei angelegt bzw. nichts in die Reportdatei geschrieben werden.

Die Anzeigegruppe **'Ausgabedatei'**:

Sie können in das Feld in dieser Anzeigegruppe den Namen und den Pfad für eine Log-Datei direkt eingeben. Mit der Ordner-Schaltfläche wird ein Fenster geöffnet, in dem Sie ein Laufwerk und einen Ordner auswählen können, in dem die Reportdatei abgelegt werden soll.

Es muß ein gültiger Dateiname für die Ausgabedatei vorhanden sein, sonst wird die Reportdatei nicht gespeichert. Wollen Sie eine Reportdatei für die Nachwelt erhalten, muß im Modus 'Reportdatei überschreiben' der Name dieser Datei für jeden Suchlauf geändert werden.

In der Anzeigegruppe **'Daten aufzeichnen'** können Sie wählen zwischen:

- **Infizierte Dateien** Alt+I

Es werden nur die Namen der infizierten Dateien mit Pfad aufgenommen.

- **Zusätzlich alle Pfade** Alt+P

Zusätzlich werden alle durchsuchten Pfade aufgenommen.

- **Alle durchsuchten Dateien** Alt+D

In die Reportdatei werden alle Dateinamen und Pfade, die durchsucht wurden, sowie die Namen der infizierten Dateien aufgenommen.

- **Komplette Information** Alt+M

Es werden neben den gleichen Informationen wie unter 'Alle durchsuchten Dateien' auch der Inhalt der Dateien AUTOEXEC.BAT, CONFIG.SYS, WIN.INI und SYSTEM.INI aufgenommen. Wenn Sie uns zur Fehlersuche eine Reportdatei zusenden, erstellen Sie diese bitte in diesem Modus.

In der Anzeigegruppe **'Reportdatei kürzen'** können Sie einstellen:

- **Reportdatei kürzen** Alt+R

Aktivieren Sie diese Funktion, läßt sich mit 'Abschneiden nach ... KB' die gewünschte Dateilänge bestimmen.

- **Abschneiden nach ... KB** Alt+S

Diese Einstellung begrenzt die Reportdatei auf eine maximale Größe. Ist 'Reportdatei kürzen' aktiviert, können Sie in diesem Feld die gewünschte Größe eingeben (nach unseren Erfahrungen reicht ein Wert zwischen 100 und 200 KB aus). So behalten Sie noch etwas freien Platz auf Ihrer Festplatte, wenn Sie im anhängenden Modus arbeiten und die Reportdatei im Modus 'komplette Informationen' erstellen.

Warnungen Alt+W

Wird diese Schaltfläche betätigt, gelangen Sie in ein Dialogfenster, in dem Sie auswählen können, welche Warnungen in der Reportdatei aufgenommen werden sollen.

Bei diesen Einstellungen handelt es sich ausschließlich um Warnungen, nicht um Virenfunde oder CRC-Änderungen.

➔ Sie können diese Warnungen, die in die Reportdatei geschrieben werden, durch Anklicken der Schaltfläche vor dem entsprechenden Eintrag ein- bzw. ausschalten.

Tritt ein Ereignis auf, dessen Optionsfeld hier aktiviert ist, erscheint eine entsprechende Warnmeldung in der Reportdatei.

Zugriffsfehler/Datei ist gesperrt Alt+Z

Auf diese Datei kann nicht zugegriffen werden, sie wurde daher auch nicht nach Viren durchsucht. Diese Meldung tritt z.B. bei der Swap-Datei von Windows (Auslagerungsdatei) auf. Die Swap-Datei bleibt permanent geöffnet, solange Windows läuft und läßt sich daher nicht überprüfen.

Falsche Dateigröße im Verzeichnis Alt+F

Die für ein Verzeichnis vermerkte 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 beispielsweise 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. Der Spielehersteller Sierra ist seiner Zeit voraus und erhöht die Jahreszahl bei einigen seiner Programme ebenfalls um 100.

COM-Datei zu groß Alt+C

Eine COM-Datei darf maximal 65535 Bytes groß sein, damit sie noch ausgeführt werden kann. 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 (Code Segment Instruction Point) abgelegt. Diese Warnung wird ausgegeben, wenn hier eine falsche Adresse gefunden wurde.

Ungültiger EXE-Header Alt+G

Wird im EXE-Header eine Veränderung festgestellt (beispielsweise in der Länge der EXE-Datei), wird diese Warnung ausgegeben.

Möglicherweise von Viren beschädigt Alt+M

Diese Datei könnte von Viren beschädigt worden sein. Treten beim Umgang mit dieser Datei Probleme auf, ersetzten Sie diese Datei sicherheitshalber durch die Originaldatei.

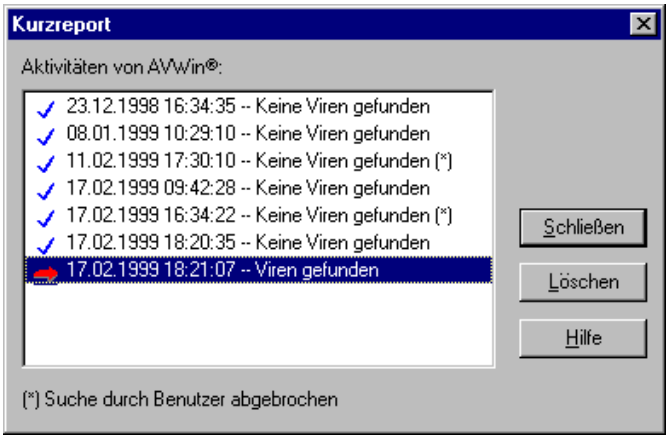
OLE-Datei ist beschädigt oder geschützt Alt+L**:**

Diese Datei kann von Viren beschädigt worden sein oder diese Datei ist geschützt. Treten beim Umgang mit dieser Datei Probleme auf, ersetzten Sie diese Datei durch die Originaldatei.

10.4 Das Wichtigste auf einen Blick: der Kurzreport

In den Kurzreport werden Eckdaten für jeden Suchlauf von AntiVir geschrieben, mit denen Sie die Aktivitäten von AntiVir über längere Zeit hinweg verfolgen können. So läßt sich immer nachvollziehen, was sich in Sachen Viren auf Ihrem System in letzter Zeit getan hat.

Nach einem Suchlauf wird der Kurzreport im Statusfenster mit der Schaltfläche Kurzreport aufgerufen. Sie können ihn aber auch über die Menüleiste des Hauptfensters über 'Report/Kurzreport anzeigen' öffnen. Er präsentiert sich in dieser Form:



Wurde eine Virensuche vom Benutzer abgebrochen, ist dies am Ende der Zeile mit (*) markiert. Ist ein Eintrag mit einem blauen ✔ markiert, wurde bei diesem Suchlauf kein Virus von AntiVir gefunden. Ist allerdings ein Eintrag mit einem roten ➦ markiert, wurde ein Virus gefunden.

Unter 'Optionen/Kurzreport' läßt sich die Zahl der Einträge festlegen. Wird die Anzahl der maximalen Einträge überschritten, werden entsprechend viele Einträge am Anfang der Liste gelöscht.

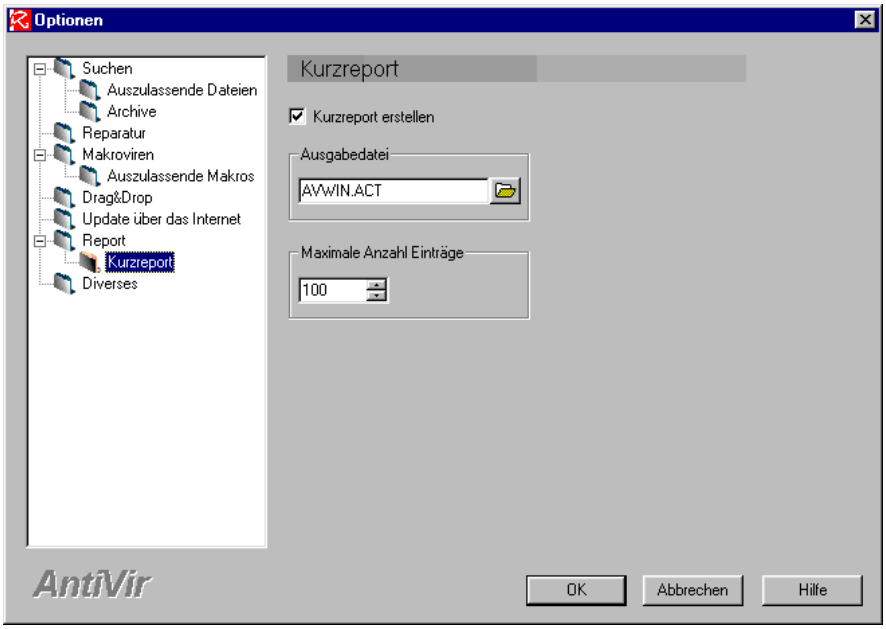
➔ Mit Löschen wird der gesamte Kurzreport ohne Nachfragen entfernt.

Wenn Sie auf einen Eintrag doppelklicken, erhalten Sie zusätzliche Informationen über den entsprechenden Eintrag (dazu gehören unter anderem: Datum; Uhrzeit; durchsuchte Verzeichnisse und Dateien; Anzahl der Warnungen, der gefundenen Viren, der gelöschten Dateien und entfernter Viren).

10.5 Voreinstellungen zum Kurzreport ändern

In dieser Registerkarte geht's um die Einstellungen für den Kurzreport.

➔ Rufen Sie das Konfigurationsfenster mit der Schaltfläche Optionen auf und klicken im Auswahlfenster auf den Ordner 'Kurzreport'. Sie können auch im Menü 'Report' direkt den Menüpunkt 'Kurzreport Einstellungen' anwählen:



- **Kurzreport erstellen** Alt+K

Ist dieses Feld markiert, wird der Kurzreport automatisch geschrieben.

- **Ausgabedatei** Alt+D

Geben Sie hier einen Dateinamen ein, unter dem die Daten des Kurzreports gespeichert werden sollen. AntiVir schlägt 'AVWIN.ACT' vor und speichert diese Datei im Installationsordner.

- **Maximale Anzahl Einträge** Alt+M

Mit dieser Funktion 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 Pfeile rechts vom Eingabefeld verändern. Bei diesen Schaltflächen wird der angezeigte Wert um 1 oder bei gleichzeitigem Drücken der Taste Strg um 10 verändert.

11 Den Virenwächter AntiVir Guard einsetzen

Dieses Modul prüft Dateien, testet Bootsektoren, kann online reparieren, erkennt Makroviren durch eine heuristisch arbeitende Engine und verfügt über die gleiche Such- und Reparaturleistung wie auch das Hauptprogramm der AntiVir Personal Edition.

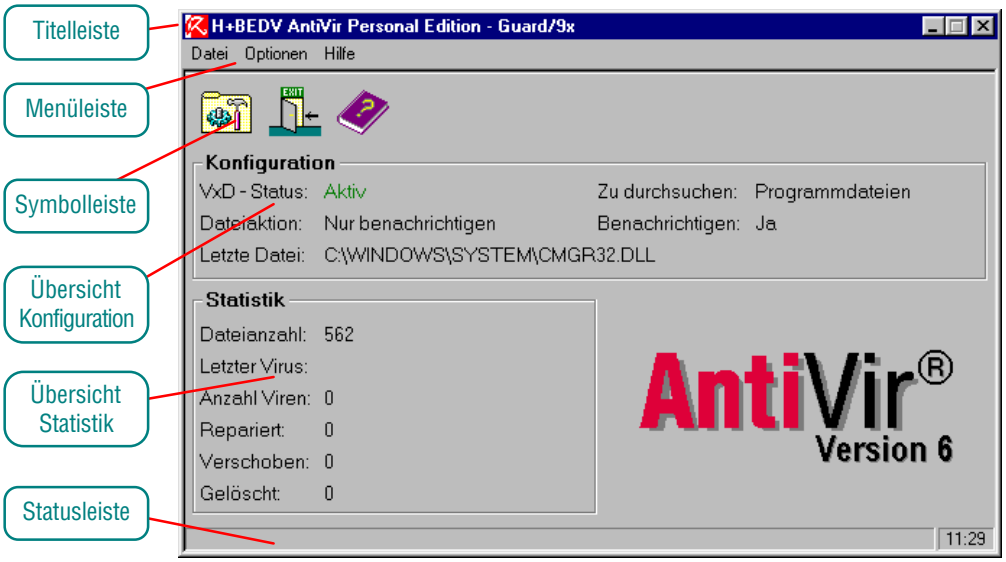
Der AntiVir Guard wird automatisch beim Start Ihres Computers aufgerufen, und zwar *bevor* andere Anwendungen gestartet werden. Bei aktiviertem Guard ist rechts im Anzeigebereich der Task-Leiste ein Icon sichtbar, das einen Schirm darstellt.

Der AntiVir Guard für Windows Me/98/95 weist einige Unterschiede zu dem AntiVir Guard für Windows 2000/NT auf. Daher werden beide Virenwächter getrennt beschrieben.

11.1 Der AntiVir/Me Guard

➔ Rufen Sie das Menüfenster des Virenwächters durch einen Doppelklick auf das Icon mit dem Schirm rechts unten in der Task-Leiste auf.

Es erscheint bei Windows Me/98/95 dieses Fenster:



In der **Titelleiste** können Sie mit Hilfe des Programm-Icons das Steuerprogramm des AntiVir Guard schließen.

In der **Menüleiste** lassen sich unter 'Datei', 'Optionen' und 'Hilfe' die einzelnen Menüpunkte zum Anpassen des Virenwächters aufrufen.

In der **Symbolleiste** befinden sich die Schaltflächen für die Konfiguration, zum minimieren des Kontrollprogrammes sowie zum Aufruf der Hilfe.

In der Anzeigegruppe **Konfiguration** wird angezeigt, ob der Guard aktiviert oder deaktiviert ist und welche Einstellungen zur Zeit aktuell sind.

'Status: Aktiv' bedeutet, daß dieser Dienst entsprechend der Voreinstellungen arbeitet. Auch in diesem Modus sucht der Guard nicht zwangsläufig nach Viren, da der Gerätetreiber, die zu überwachenden Laufwerke oder anderes eventuell deaktiviert sind.

'Status: Deakiv' bedeutet, daß das Steuerprogramm des AntiVir Guard entweder absichtlich vom Anwender beendet wurde oder daß ein Dienst nicht gefunden wurde bzw. dieser nicht antwortet. Eventuell ist der Name des Zielcomputers falsch oder es besteht ein Kommunikationsproblem. Beachten Sie ggf. das Eventlog auf dem Zielrechner.

In der Anzeigegruppe **Statistik** können Sie nachvollziehen, wieviel Dateien durchsucht, welcher Virus zuletzt gefunden, wie viele Viren gefunden und wie viele Dateien repariert, verschoben oder gelöscht wurden.

Die Statistik wird aus Performancegründen nur zweimal pro Sekunde aktualisiert. Die angezeigten Werte lassen sich mit der Funktion 'Statistik löschen' wieder auf Null zurücksetzen.

In der **Statusleiste** wird Ihnen angezeigt, welche Auswirkungen die einzelnen Bedienelemente der Oberfläche des Kontrollprogrammes haben.

Menü: Datei Alt+D

- **AVGuard aktivieren** Alt+D / A

Dieser Menüpunkt läßt sich nur anwählen, wenn der AntiVir Guard deaktiviert ist. Wird auf 'AVGuard aktivieren' geklickt, untersucht der Virenwächter ab diesem Zeitpunkt alle Dateien, die kopiert, geöffnet oder umbenannt werden.

- **AVGuard deaktivieren** Alt+D / D

Dieser Menüpunkt läßt sich nur anwählen, wenn der AntiVir/9x Guard aktiviert ist. Wird auf 'AVGuard deaktivieren' geklickt, stellt der Virenwächter ab diesem Zeitpunkt seine Arbeit ein bis zum nächsten Neustart oder bis der Menüpunkt 'AVGuard aktivieren' angewählt wird.

Wählen Sie diese Einstellung nur in einem wirklich begründeten Fall, da der deaktivierte Guard keine Dateien und Bootsektoren mehr durchsucht und auch keine Viren mehr finden kann.

- **Hauptprogramm starten** Alt+D / A

Das Hauptprogramm wird aufgerufen.

- **Ende und minimieren** Alt+D / M

Mit diesem Menüpunkt wird das Steuerprogramm des Guard nicht geschlossen sondern verkleinert (minimiert). Um das Steuerprogramm wieder zu vergrößern, doppelklicken Sie einfach einen auf das Programm-Icon rechts unten im Anzeigebereich der Task-Leiste. In diesem Modus benötigt das Steuerprogramm keine Rechenzeit.

Ist das Steuerprogramm im Hintergrund aktiviert (also nicht beendet), zeigt das Icon mit dem Schirm rechts unten im Anzeigebereich der Task-Leiste an, ob der Guard aktiviert oder deaktiviert ist:

 Guard ist aktiviert

 Guard ist deaktiviert

- **Ende und schließen** Alt+D / S

Mit diesem Menüpunkt verlassen Sie das Steuerprogramm des AntiVir Guard, das Programm wird vollständig beendet. Das Steuerprogramm kann anschließend nur noch über das entsprechende Icon im Installationsverzeichnis von AntiVir oder durch einen Neustart der Workstation aufgerufen werden.

Wählen Sie diese Einstellung nur in einem wirklich begründeten Fall, da der deaktivierte Guard keine Dateien und Bootsektoren mehr durchsucht und auch keine Viren mehr finden kann.

Das Steuerprogramm läßt sich auch im AntiVir Programmordner, also standardmäßig aus C:\PROGRAMME\AVPERSONAL, mit dem Namen AVGCTRL.EXE aufrufen.

Menü: Optionen Alt+O

- **Konfigurieren** Alt+O / K

Mit dem Menüpunkt 'Einstellungen ändern' gelangen Sie in das Fenster 'AVGuard – Einstellungen'.

In diesem Fenster können Sie den Virenwächter konfigurieren. Wie das geht, erfahren Sie ab Seite 79.

Menü: Hilfe Alt+H

- **Hilfe F1; Alt+H / H**

Wird dieser Menüpunkt aufgerufen, der Button in der Symbolleiste oder die obligatorische Hilfetaste F1 betätigt, erscheint die ebenfalls obligatorische Windows-Hilfe zu dem jeweils aktuellen Fenster des AVGuard.

- **Hilfe verwenden Alt+H / V**

Mit diesem Menüpunkt öffnet Windows Me/98/95 seine Hilfe zur Hilfe. Dort erfahren Sie, wie Sie mit der Windows-Hilfe umgehen können.

- **Index Alt+H / I**

Mit diesem Menüpunkt wird die Windows-Hilfe aufgerufen. Dort finden Sie eine Liste mit verschiedenen Stichworten vor, zu denen Sie Hilfe bekommen.

- **Produktinformationen Alt+H / P**

Mit diesem Menüpunkt wird ein Informationsfenster geöffnet:

Hier gelangen Sie durch Anklicken der blauen Internetadressen automatisch zu den dort angegebenen Stellen.

Die Voreinstellungen des AntiVir/Me Guard ändern

➔ Rufen Sie das Steuerprogramm des Virenwächters durch Doppelklick auf das Icon mit dem Schirm rechts unten im Anzeigebereich der Task-Leiste auf.

➔ Rufen Sie in der Menüzeile im Menü 'Einstellungen' (den Menüpunkt 'Einstellungen ändern' auf oder benutzen Sie dazu die Tastenkombination Alt+E / E.

➔ Es erscheint das Fenster 'Konfiguration', in dem Sie die Einstellungen zum Virenwächter anpassen können:

➔ Bestätigen Sie die Änderungen mit der Schaltfläche OK, mit Abbruch bleiben die Einstellungen unverändert. Wenn Sie das Fenster 'Optionen' mit der Schaltfläche X rechts oben in der Titelleiste oder mit Alt+F4 schließen, werden die Einstellungen nicht übernommen.

Doch nun zu den einzelnen Registerkarten in diesem Fenster:

Die Registerkarte 'Suchen'

In der Anzeigegruppe **'Durchsuchen'** legen Sie fest, welche Dateiarten durchsucht werden:

- **Alle Dateien**

Per Voreinstellung untersucht der AntiVir/Me Guard ausschließlich Programmdateien und Dokumente. Ist dieser Menüpunkt angewählt, werden sämtliche Dateien nach Viren durchsucht, auch nicht ausführbare Dateien werden gescannt. Sollen alle Dateien durchsucht werden, dauert die Virensuche länger, da wesentlich mehr Dateien geprüft werden müssen.

- **Programmdateien und Dokumente**

Mit dieser Funktion werden nur Dateien mit einer vorgegebenen Endung durchsucht (z.B. ∗.COM, ∗.EXE, usw. sowie auch Dokumente, die vorzugsweise von Makroviren heimgesucht werden, also beispielsweise ∗.DOC und ∗.DOT). Bei den Endungen sind in der Default-Einstellung Standardwerte vorgegeben.

In die Liste der Programm- und Dokumentendateien werden – soweit erforderlich – immer wieder neue Dateitypen aufgenommen. Im Fenster 'Dateierweiterungen' können Sie mit der Bildlaufleiste in der Liste blättern und nachsehen, welche Dateiendungen geprüft werden

Haben Sie Programmdateien mit anderen Endungen auf Ihrem Rechner, können Sie diese Endungen wie bei dem Hauptprogramm in die Liste mit Dateiendungen einfügen. Wie das geht, wird ab Seite 43 beschrieben.

Die Anzeigegruppe **'Infizierte Dateien'**

- **Reparatur aktivieren**

Hier wählen Sie aus, ob eine infizierte Datei automatisch repariert werden soll oder nicht. Ist diese Option nicht aktiviert oder die betreffende Datei nicht reparabel, werden die Einstellungen der Anzeigegruppe 'Wenn Datei nicht repariert' wirksam.

Die Anzeigegruppe **'System herunterfahren'**

- **Warnung, wenn Diskette in Laufwerk A:**

Ist diese Einstellung aktiviert, erscheint eine Warnmeldung, wenn beim Beenden von Windows eine Diskette im Bootlaufwerk befindet.

Diese Einstellung sollten Sie immer aktiviert lassen, da dies der einfachste Schutz vor Bootsektorviren ist: Bootsektorviren können nur aktiv werden, wenn von einer infizierten Diskette gebootet wird. Dies geschieht in den meisten Fällen unbeabsichtigt indem vergessen wird, die Diskette vor dem Abschalten des Rechners aus dem Laufwerk zu entfernen. Wird der Rechner das nächste mal gestartet, ist es soweit: Der Rechner lädt den Bootsektor (= Virus) von der Diskette und startet diesen. Auf dem Bildschirm erscheint nur ein Text wie „Kein Betriebssystem“ oder ähnliches. Oder gar nichts, weil der Rechner vom Virus angehalten wurde. Der Virus hat sich jetzt aber schon auf ihre Festplatte begeben und wird – nachdem Sie die Diskette entfernt und den Rechner neu gestartet haben – von dort geladen. Und das alles nur, weil eine Diskette im Laufwerk A: vergessen wurde.

Die Registerkarte 'Aktion'

In der Anzeigegruppe **Aktion falls Datei nicht repariert'** legen Sie fest, was passiert, wenn eine infizierte Datei nicht repariert wird:

- Infizierte Datei löschen

Ist dieses Optionsfeld markiert, wird eine infizierte Datei gelöscht. Diese Option ist zwar brutal, dafür aber auch sehr sicher.

- Infizierte Datei verschieben

Ist dieses Optionsfeld markiert, werden infizierte Dateien in das unter 'Quarantäneverzeichnis' angegebene Verzeichnis verschoben.

- Datei umbenennen nach *.VIR

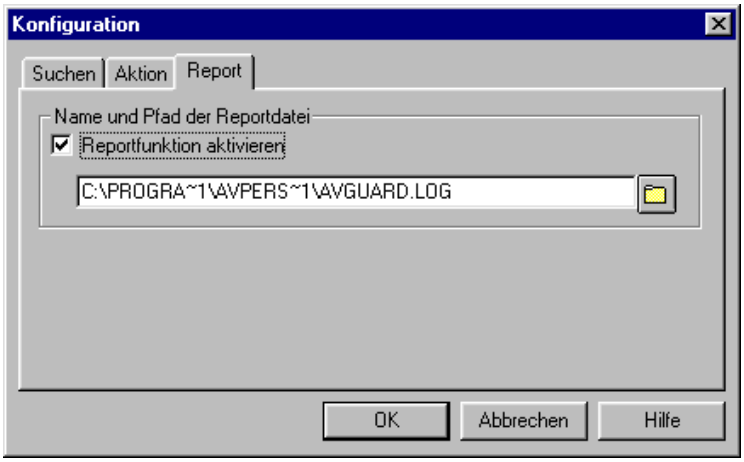
Soll die Datei umbenannt werden, hängt der Guard die Endung '.VIR' an den kompletten Dateinamen an. Eine Datei DOCUMENT.DOC würde also nach DOCUMENT.DOC.VIR umbenannt. Der Pfad zu dieser umbenannten Datei bleibt unverändert.

- Datei ignorieren

Die Infektion wird lediglich in der Reportdatei eingetragen, sofern diese aktiviert ist.

Ist diese Einstellung aktiviert und die Option 'Reparatur aktivieren' ausgeschaltet, werden weder Reparaturen vorgenommen noch infizierte Dateien gelöscht! Wird in der Reportdatei ein Virus gemeldet, müssen Sie selbst entscheiden, was mit den infizierten Dateien geschehen soll. Damit auch immer eine Reportdatei erstellt wird, sollten Sie im Menü 'Optionen/Report' den Punkt 'Kein Report erstellen' *nicht* ausschalten.

Die Registerkarte 'Report'



Die Anzeigegruppe **'Name und Pfad der Reportdatei'**

- Kontrollkästchen 'Reportfunktion aktivieren'

Wollen Sie die Meldungen des Guard für die Nachwelt erhalten, können Sie in diesem Listenfeld einen gültigen und vollständigen Dateinamen für eine Reportdatei (beispielsweise AVGUARD.LOG) eintragen. Diese Reportdatei wird in diesem Beispiel dann im Installationsverzeichnis von AntiVir angelegt. Die Datei wird vom AntiVir/9x Guard für lesende Zugriffe freigegeben, für schreibenden Zugriff jedoch gesperrt. Um die Reportdatei löschen zu können, müssen Sie den Guard deaktivieren.

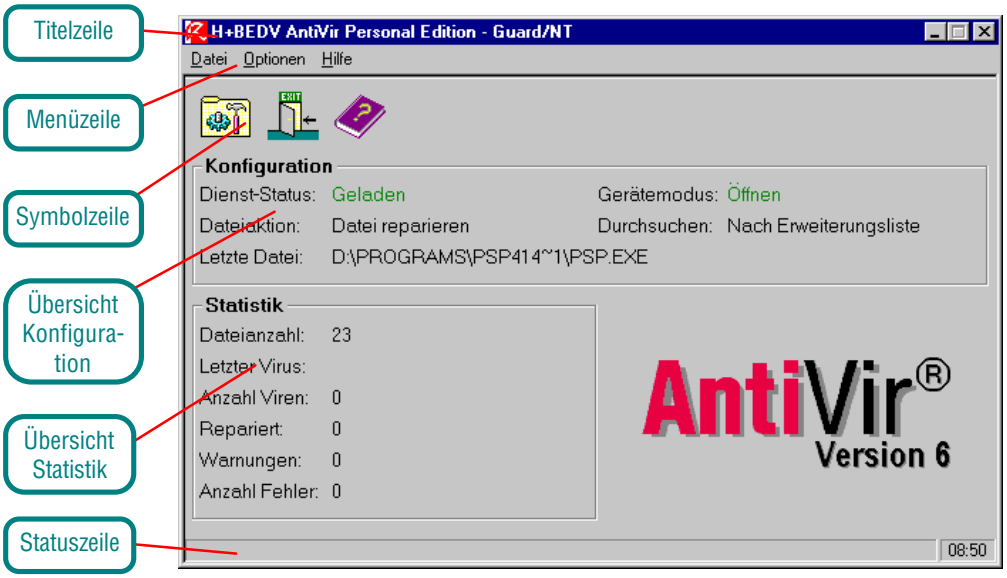
- Listenfeld 'Name und Pfad der Reportdatei'

Dieses Feld enthält die Voreinstellung des Pfades und Dateinamens der zu erstellenden Reportdatei. Alle Einträge werden an das Ende dieser Datei angefügt.

Sie können hier auch einen anderen Pfad und Dateinamen eintragen. Mit der Schaltfläche 'Durchsuchen' (das ist das Ordner-Symbol hinter dem Eingabefeld) können Sie sich in der Verzeichnisstruktur Ihres Computersystems bewegen.

11.2 Der AntiVir/2000 Guard

➔ Rufen Sie das Menüfenster des Virenwächters durch einen Doppelklick auf das Icon mit dem Schirm rechts unten im Anzeigebereich der Task-Leiste auf. Es erscheint dieses Fenster:



In der **Titelzeile** befinden sich allgemeine Angaben über den Guard.

In der **Menüzeile** lassen sich unter 'Datei', 'Optionen' und 'Hilfe' weitere Menüpunkte zum Anpassen des Virenwächters aufrufen.

In der **Symbolzeile** befinden sich die Buttons 'Konfigurieren', 'Statistik löschen' 'Konfiguration speichern', 'Schließen und minimieren' und 'Hilfe'.

In der Anzeigegruppe **Konfiguration** wird angezeigt, ob der AntiVir/NT Guard aktiviert ist und welche Einstellungen aktuell sind.

Status: Zeigt den aktuellen Status des Guard-Dienstes an (aktiviert / deaktiviert).

Aktiv bedeutet, daß der Dienst entsprechend den Einstellungen arbeitet. Beachten Sie aber bitte, daß Guard nicht zwangsläufig auch nach Viren sucht, da der Gerätetreiber, die zu überwachenden Laufwerke oder anderes eventuell deaktiviert sind.

Deakiv bedeutet, daß das Kontrollprogramm des Guard/NT den Dienst nicht finden konnte oder dieser nicht antwortet. Eventuell ist der Name des Zielcomputers falsch, der Dienst wurde manuell

beendet oder es existiert ein Kommunikationsproblem. Beachten Sie ggf. das Eventlog auf dem Zielrechner.

Dateiaktion:	Dieses Feld zeigt die auszuführende Aktion an, wenn die Benutzerwarnungen deaktiviert sind.
Gerätemodus:	gibt an, wann der Guard die Dateien untersuchen soll.
Zu durchsuchen:	Was ist zu durchsuchen: Alle Dateien oder nur Dateien mit speziellen Dateierweiterungen. (Programmdateien)

In der Übersicht **Statistik** stehen aktuellen Informationen zum Guard:

Letzte Datei:	Name der zuletzt vom Guard/NT durchsuchten Datei
Dateianzahl:	Anzahl der durchsuchten Dateien
Letzter Virus:	Name des letzten gefundenen Virus
Anzahl Viren:	Anzahl der gefundenen Viren
Repariert:	Anzahl der erfolgreich reparierten Dateien

Beachten Sie bitte, daß diese aus Performancegründen nur 2 mal pro Sekunde aktualisiert wird. Diese Statistik läßt sich mit der Option 'Statistik löschen' wieder auf Null zurücksetzen.

In der **Statuszeile** werden weitere Informationen zum Guard angezeigt.

Menü: Datei Alt+D

- **Ende und minimieren** Alt+D / M

Wählen Sie diesen Eintrag, wenn Sie das AntiVir/NT Guard Kontrollprogramm verlassen wollen, es jedoch nicht vollständig geschlossen werden soll. Es wird verkleinert (minimiert) und Sie können anschließend das Programm-Icon rechts unten im Anzeigebereich der Task-Leiste sehen. Um es wieder zu vergrößern, machen Sie einfach einen Doppelklick auf das kleine Icon. Im minimierten Zustand benötigt das Steuerprogramm keine Rechenzeit.

- **Ende und schließen** Alt+D / S

Mit dieser Funktion verlassen Sie das Kontrollprogramm des AntiVir/2000 Guard, das Programm wird vollständig beendet.

Wählen Sie diese Einstellung nur in einem wirklich begründeten Fall, da der deaktivierte Guard keine Dateien und Bootsektoren mehr durchsucht und auch keine Viren mehr finden kann.

Das Steuerprogramm kann anschließend nur noch über das entsprechende Icon im Installationsverzeichnis von AntiVir/2000 gestartet werden.

Ist das Steuerprogramm im Hintergrund aktiviert (also nicht beendet), zeigt das Icon mit dem Schirm rechts unten in der Task-Leiste an, ob der Guard aktiviert oder deaktiviert ist:

 Guard ist aktiviert

 Guard ist deaktiviert

Menü: Optionen Alt+O

- **Konfigurieren** Alt+O / K

Mit dem Menüpunkt 'Konfigurieren' oder dem Button in der Symbolleiste gelangen Sie in das gleichnamige Fenster, in dem Sie die Voreinstellungen des Guard ändern können.

Welche Einstellungen Sie in welcher Weise ändern können, erfahren Sie ab Seite 79.

- **Statistik löschen** Alt+O / K

Mit dieser Option oder dem Button in der Symbolleiste können Sie die interne Statistik des AntiVir/NT Guard löschen. Alle numerischen Werte werden auf Null gesetzt, alle Textfelder auf eine Leerzeile.

- **Konfiguration speichern** Alt+O / K

Mit diesem Befehl oder dem Button in der Symbolleiste wird ein Kommando an den AntiVir/NT Guard gesendet, um die aktuelle Konfiguration sofort zu speichern. Der AntiVir/2000 Guard führt dies allerdings auch beim Beenden des Dienstes automatisch aus.

Menü: Hilfe Alt+H

- **Hilfe** F1

Wird dieser Menüpunkt aufgerufen, der Button in der Symbolleiste oder die obligatorische Hilfetaste F1 betätigt, erscheint die Hilfe zum jeweils aktuellen Fenster des Guard.

- **Hilfe verwenden** Alt+H / V

Mit diesem Menüpunkt öffnet Windows seine Hilfe zur Hilfe. Dort erfahren Sie, wie Sie mit der Windows-Hilfe umgehen können.

- **Index** Alt+H / I

Mit diesem Menüpunkt wird die Windows-Hilfe aufgerufen. Es erscheint eine Liste mit verschiedenen Stichworten, zu denen Sie Hilfe bekommen.

- **Produktinformation** Alt+H / P

Mit diesem Menüpunkt wird ein Informationsfenster geöffnet. In der Anzeigegruppe **'Versionsinformationen'** werden die Version und das Erstellungsdatum des AntiVir/2000 Guard Kontrollprogrammes, die Versionsnummer der verwendeten AntiVir-Suchengine sowie die Version, das Erstellungsdatum und der Typ der aktuell verwendeten Virendefinitionsdatei angegeben.

In der Anzeigegruppe **'Lizenzinformationen'** finden Sie den Namen des lizensierten Benutzers, seine Seriennummer sowie die Gültigkeitsdauer der in der vorhandenen Lizenzdatei befindlichen Lizenz.

Benötigen Sie technischen Support, Produktinformationen oder sonstige Auskünfte, können Sie uns unter einer der in der Anzeigegruppe 'Hotline/ Weitere Produktinformationen' angegebenen Adressen erreichen.

Die Voreinstellungen des AntiVir/NT Guard ändern

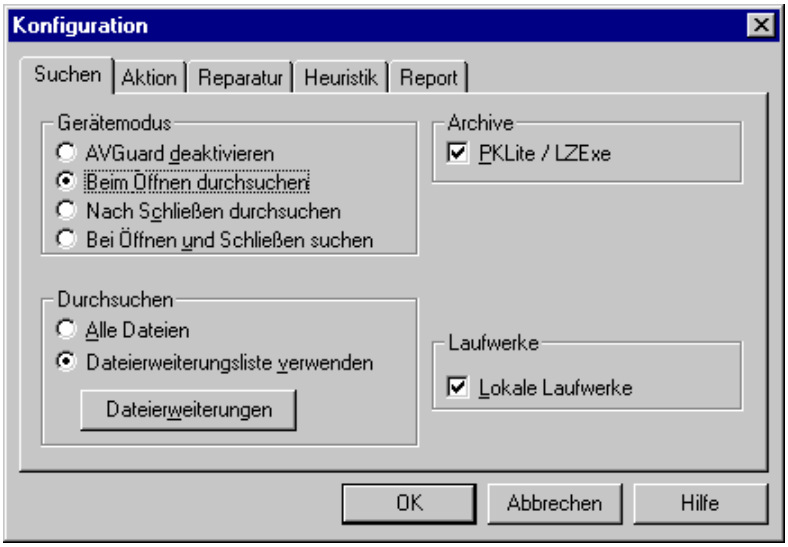
➔ Rufen Sie das Steuerprogramm des Virenwächters durch Doppelklick auf das Icon mit dem Schirm rechts unten in der Task-Leiste auf.

➔ Klicken Sie auf das Symbol 'Konfiguration' oder benutzen Sie die Tastenkombination Alt+O.

Es erscheint das Fenster 'Konfiguration', in dem Sie den Virenwächter konfigurieren können.

➔ Bestätigen Sie Änderungen in diesem Fenster mit der Schaltfläche OK, mit Abbruch bleiben die Einstellungen unverändert. Schließen Sie das Fenster 'Optionen' mit der Schaltfläche X rechts oben in der Titelleiste oder mit Alt+F4, werden die Einstellungen nicht übernommen.

Die Registerkarte 'Suchen'



In der Anzeigegruppe **'Gerätemodus'** wird der Zeitpunkt für das Durchsuchen einer Datei beim Zugriff festgelegt:

- AVGuard deaktivieren

Ist dieses Feld aktiviert, wird der AntiVir Guard minimiert. **Achtung: Der Guard überprüft in diesem Modus keine Dateien auf Viren!** Das Programm läßt sich durch Anklicken des geschlossenen Schirm-Icons im Anzeigebereich der Task-Leiste aufrufen und aktivieren.

- Beim Öffnen durchsuchen

Ist dieses Feld aktiviert, werden die entsprechenden Dateien durchsucht, bevor Sie von der Anwendung oder dem Betriebssystem gelesen werden können. Dies ist die Defaulteinstellung, da der Guard aufgrund seines internen Dateinamens-Cache die meisten Dateien nur einmal durchsucht.

- Nach Schließen durchsuchen

Wenn diese Option aktiviert ist, werden nur Dateien durchsucht, die auf einem Volume neu erstellt oder verändert wurden.

In der Anzeigegruppe **'Archive'** legen Sie fest, ob der AntiVir/NT Guard komprimierte Dateien zu dekomprimieren und diese entpackten Dateien dann zu durchsuchen.

- PKLite/LZExe

Ist diese Option gewählt, werden von PKLite und LZExe gepackte Dateien vor der Suche dekomprimiert und erst dann durchsucht. Hierdurch können eventuelle Viren, die sich möglicherweise in diesen komprimierten Dateien verbergen, ebenfalls gefunden werden. Sind viele komprimierte Dateien zu überprüfen, macht sich allerdings ein Performanceverlust bemerkbar.

Die Anzeigegruppe **'Durchsuchen'** kann wie ein Filter verwendet werden, um die Anzahl der zu durchsuchenden Dateien einzuschränken, die Suche läßt sich auf Dateien mit einer bestimmten Erweiterung einschränkt.

- Alle Dateien

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

- Dateierweiterungsliste verwenden

Per Voreinstellung werden nur Dateien nach Viren durchsucht, deren Erweiterung in der Liste 'Dateierweiterung' aufgenommen ist. Beachten Sie, daß sich die Standardeinträge von Version zu Version ändern können.

Mit der Schaltfläche Dateierweiterung wird ein Fenster geöffnet, in dem eine Liste mit den Dateierweiterungen angezeigt wird.

Diese Liste läßt sich ähnlich wie im Hauptprogramm editieren. Wie das geht, wird ab Seite 43 beschrieben.

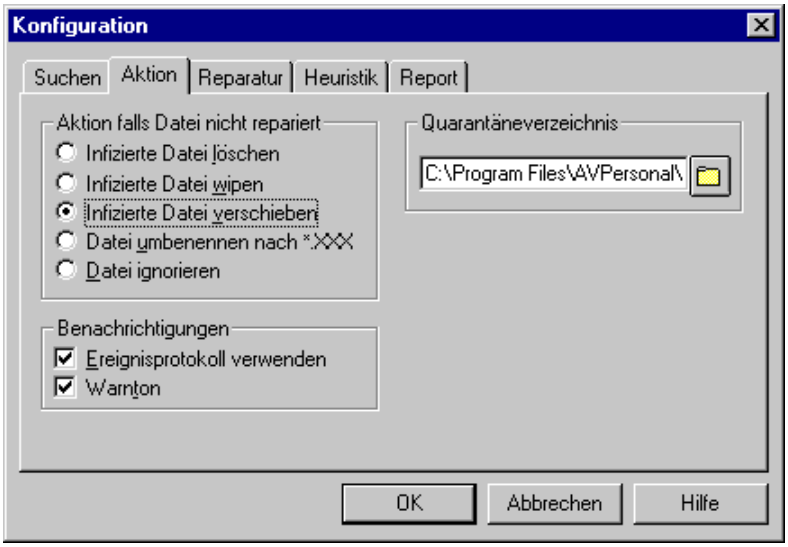
Bestätigen Sie in diesem Fenster die Änderungen mit der Schaltfläche OK, mit Abbruch bleiben die Einstellungen unverändert. Wenn Sie das Fenster 'Optionen' mit der Schaltfläche X rechts oben in der Titelleiste oder mit Alt+F4 schließen, werden die Einstellungen nicht übernommen.

In der Anzeigegruppe **'Laufwerke'** legen Sie fest, welche Laufwerke vom Guard überwacht werden sollen.

- Lokale Laufwerke

Ist diese Funktion aktiviert, werden Dateien von lokalen Laufwerken wie Diskettenlaufwerke, Festplatten, CDs, ZIP-Drives, etc. durchsucht.

Die Registerkarte 'Aktion'



In dieser Registerkarte werden die Aktionen konfiguriert, die der Guard ausführen soll, wenn ein Virus gefunden wurde.

Wenn der Guard einen Virus findet, hängt es zuerst von Einstellung in der Registerkarte 'Reparatur' unter 'Infizierte Dateien' ab, was nun passieren wird:

Ist dieser Schalter aktiviert, wird AntiVir zuerst versuchen, die infizierte Datei zu reparieren. Schlägt dieser Versuch – aus welchen Gründen auch immer – fehl, reagiert AntiVir entsprechend der Einstellungen in der Registerkarte 'Aktion'.

Ist die automatische Reparatur nicht aktiviert, kommt automatisch die Voreinstellung in der Registerkarte 'Aktion' zum Zug.

Die Anzeigegruppe **'Aktion falls Datei nicht repariert'**

- Infizierte Datei löschen

Die infizierte Datei wird gelöscht, kann jedoch mit einem entsprechenden Programm wiederhergestellt werden.

- Infizierte Datei wipen

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

- Infizierte Datei verschieben

Die infizierte Datei wird in das Quarantäneverzeichnis verschoben, ein direkter Zugriff ist nicht mehr möglich. Bitte beachten Sie: In einem Netzwerk sollte nur der Administrator Zugriff auf dieses Verzeichnis haben.

- Datei umbenennen nach *XXX

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

- Datei ignorieren

Die Infektion wird lediglich in der Reportdatei eingetragen, sofern diese aktiviert ist.

In der Anzeigegruppe **'Benachrichtigungen'** werden verschiedene Möglichkeiten angeboten, auf welche Weise sich der AntiVir/NT Guard nach einem Virenfund bemerkbar machen soll:

- Ereignisprotokoll verwenden

Bei jeder Infektion wird ein Eintrag in das Ereignisprotokoll geschrieben. Der Administrator kann Infektionen erkennen und entsprechen reagieren.

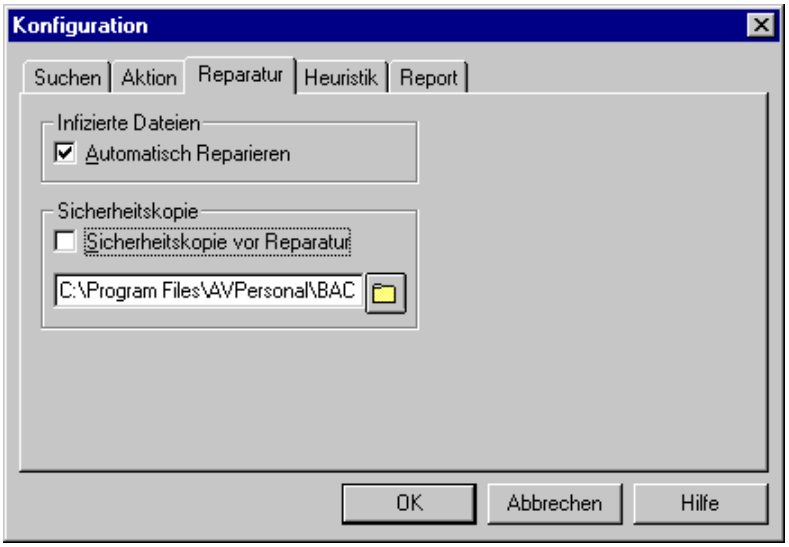
- Warnton

Der AntiVir Guard wird bei einer Infektion die kurze Tonfolge 'Virus gefunden' abspielen.

Die Anzeigegruppe **'Quarantäneverzeichnis'**

Geben Sie in dieser Anzeigegruppe einen Ordner an, in welches infizierte – und nicht reparierte – Dateien verschoben werden sollen. Die verschobenen Dateien bekommen neue Namen, damit keine Konflikte bei Duplikaten auftreten. Per Voreinstellung ist hier der Ordner '\INFECTED' im Installationsverzeichnis von AntiVir eingetragen. Mit Hilfe des Ordnersymbols können Sie einen anderen Pfad für das Quarantäneverzeichnis in der Verzeichnisstruktur Ihres Rechners auswählen.

Die Registerkarte 'Reparatur'



Diese Registerkarte enthält die Einstellungen für die Reparatur infizierter Dateien.

Die Anzeigegruppe **'Infizierte Dateien'**

- Automatisch reparieren

Ist dieses Kontrollkästchen aktiviert, wird der AntiVir/NT Guard infizierte Dateien soweit möglich automatisch reparieren. Diese Option muß auch dann aktiviert sein, wenn der Benutzer in den Warnmeldungen die Reparatur auswählen können soll (oder so ...).

Die Anzeigegruppe **'Sicherheitskopie'**

Der AntiVir/NT Guard kann von infizierten Dateien vor der Reparatur eine Sicherheitskopie (Backup) erstellen.

Diese Funktion kann in mehreren Fällen hilfreich sein: Zum einen zu Dokumentationszwecken, falls bei Ihnen Virenbefall dokumentiert und protokolliert wird, und zum anderen, wenn bei eingeschalteter automatischer Reparatur ein Makrovirus 'nur' von der Heuristik erkannt und entfernt wird. Wir würden uns freuen, wenn Sie uns dann die erstellt Sicherheitskopie zusenden, damit die Signatur dieses Makrovirus in das nächste Update mit aufgenommen werden kann.

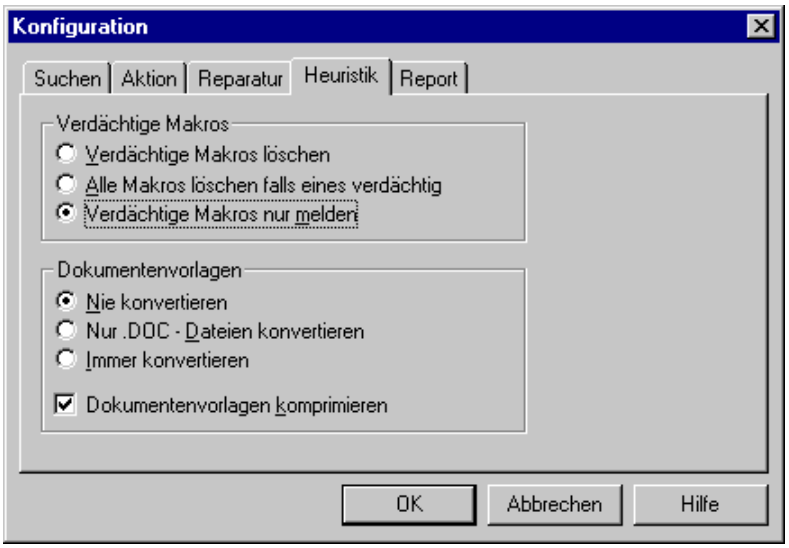
- Sicherheitskopie vor Reparatur

Ist dieses Kontrollkästchen aktiviert, kopiert der AntiVir/NT Guard jede zu reparierende Datei vor der eigentlichen Reparatur in das angegebene Verzeichnis, d.h. es wird ein Backup erstellt.

- Verzeichnis für Sicherheitskopien

In diesem Verzeichnis werden die Sicherheitskopien vor der Reparatur erstellt. Per Voreinstellung ist hier der Ordner '\BACKUP' im Installationsverzeichnis des AntiVir/2000 Guard eingetragen. Mit Hilfe des Ordnersymbols können Sie einen anderen Pfad für den Ordner der Sicherheitskopien in der Verzeichnisstruktur Ihres Rechners auswählen.

Die Registerkarte 'Heuristik'



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

Der AntiVir/2000 Guard enthält eine Makrovirenheuristik, die auch unbekannte (neue) Makroviren entdecken kann. Dies geschieht durch eine aufwendige Analyse und Untersuchung der Makros nach typischen Merkmalen von Makroviren. Solche Makros werden dann als verdächtig gemeldet. Verdächtige Makros können gelöscht oder nur gemeldet werden. Da aber ein Virus normalerweise aus mehr als einem Makro besteht, stellt sich die Frage, was mit den restlichen, möglicherweise nützlichen Makros geschehen soll.

Die Anzeigegruppe **'Verdächtige Makros'**

- Verdächtige Makros löschen

Alle als verdächtig gemeldete Makros werden gelöscht. Mit dieser Einstellung werden nützliche Makros dann nicht versehentlich gelöscht. Der Nachteil hierbei liegt darin, daß die restlichen zum Virus gehörenden Makros im Dokument verbleiben und von Antiviren-Programmen anderer Hersteller gemeldet werden könnten.

- Alle Makros löschen falls eines verdächtig

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

- Verdächtige Makros nur melden

Keine sehr gute Einstellung. Hiermit könnte der Verbreitung von Makroviren Tür und Tor geöffnet werden. Um sicher zu gehen, daß ein als verdächtig gemeldetes Dokument keinen Virus enthält, sollten Sie uns die Datei zur Überprüfung zusenden. Wir benachrichtigen Sie umgehend, falls es sich wirklich um einen Virus handelt.

Die Anzeigegruppe **'Dokumentenvorlagen'**

Mit der Textverarbeitung Word 6/7 erstellte Dokumentvorlagen (zu erkennen an der Endung *.DOT) bestehen wie normale Dokumente (= *.DOC) aus Text, zusätzlich können Sie jedoch andere Daten wie beispielsweise Makros enthalten. Wenn Word 6/7 solch eine Dokumentvorlage öffnet, sucht es nach diesen Daten und wertet Sie aus. Ein Makrovirus kann nur Dokumentvorlagen (= *.DOT) infizieren, deshalb werden Dokumente bei einer Infektion immer zuerst in dieses Vorlagen-Format gewandelt. Der AntiVir Guard kann nun solche Dokumentvorlagen wieder zurück in das ursprüngliche Dokumentformat (= *.DOC) wandelt, wenn keine zusätzlichen Daten vorhanden sind. Alle Makros müssen gelöscht sein, es sind keinerlei Menüs oder Shortcuts erlaubt.

- Nie konvertieren

Dokumentvorlagen werden in keinem Fall in das Dokumentformat gewandelt.

- Nur .DOC Dateien konvertieren

Dokumentvorlagen haben meist die Dateierweiterung *.DOT oder *.WIZ. Dokumente sind an der Dateierweiterung *.DOC zu erkennen. Aktivieren Sie diese Option, wenn der Guard reparierte Dokumentvorlagen mit der Dateierweiterung *.DOC zurück in das Dokumentformat wandeln soll.

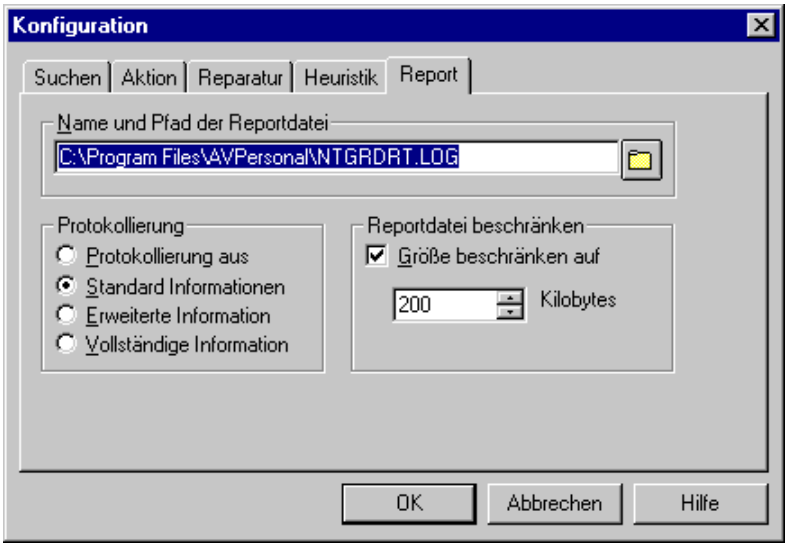
- Immer konvertieren

Ist diese Option aktiviert, konvertiert der AntiVir/2000 Guard alle Word 6/7 Dokumentvorlagen in das Dokumentformat, sofern möglich.

- Dokumentenvorlagen komprimieren

Wenn ein Makro gelöscht wird, verbleibt sein Name immer noch im Dokument. Das Makro selber wurde überschrieben und als gelöscht markiert. Da einige Antiviren-Programme nur nach solchen Makronamen suchen, könnten Sie einen Virus melden wo keiner mehr ist. Der AntiVir/NT Guard kann nun mit dieser Option auch alle Referenzen auf gelöschte Makros und Ihre Namen aus der Dokumentvorlage löschen.

Die Registerkarte 'Report'



Der AntiVir Guard/2000 besitzt umfangreiche Protokollfunktionen, die exakte Hinweise über eine Virusinfektion geben können.

Die Anzeigegruppe **'Name und Pfad der Reportdatei'** enthält Pfad und Dateinamen der zu erstellenden Reportdatei. Alle Einträge werden an das Ende dieser Datei angefügt. Mit der Schaltfläche 'Durchsuchen' (das ist das Ordner-Symbol hinter dem Eingabefeld) können Sie sich in der Verzeichnisstruktur Ihres Computersystems bewegen.

In der Anzeigegruppe **'Protokollierung'** wird der Umfang der Reportdatei festgelegt:

- Protokollierung aus

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

- Standard Informationen

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

- Erweiterte Informationen

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

- Vollständige Informationen

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

Den AntiVir Guard beenden

Dieser Absatz gilt wieder für Windows Me/98/95 und Windows 2000/NT. Wurde der AntiVir Guard installiert, bleibt dieser auch dann noch aktiv, wenn das Hauptprogramm geschlossen wird.

Wurde der AntiVir Guard mit dem Icon rechts unten im Anzeigebereich der Task-Leiste aufgerufen und in diesem Steuermenü die Schaltfläche Deaktivieren betätigt, wird der Virenwächter *nicht* beendet.

Auch durch gewohnten Doppelklick auf das Icon im Steuermenü (in der linken oberen Ecke des Hauptfensters) bzw. Anklicken dieses Icons und scrollen auf den Befehl 'Schließen' wird der AV Guard *nicht* beendet. Das gilt auch für die Schaltfläche X rechts oben in der Titelleiste oder die Tastenkombination Alt+F4.

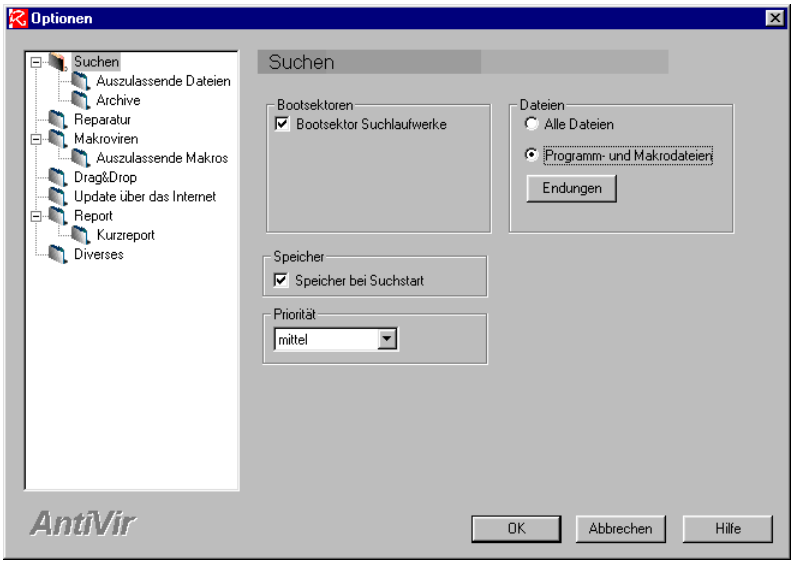
➔ Um den Virenwächter zu beenden, klicken Sie im Menü 'Datei' auf den Punkt 'Ende und schließen'. Es erscheint eine Meldung, ob Sie tatsächlich den Virenwächter verlassen wollen.

➔ Bestätigen Sie diese Meldung mit Ja, verschwindet das Icon aus der Task-Leiste. Mit den Schaltflächen Nein und Abbrechen wird der Vorgang ohne Änderung abgebrochen.

12 Voreinstellungen ändern

Unter diesem Menüpunkt können Sie die Einstellungen für AntiVir und die Reportdatei ändern.

➔ Rufen Sie das Konfigurationsfenster mit der Schaltfläche Optionen oder der Tastenkombination Alt+O / K auf und klicken auf den Ordner, in dem Sie Änderungen vornehmen wollen. Sie können auch im Menü 'Optionen' den Menüpunkt 'Konfigurationsmenü' anwählen:



➔ Klicken Sie im linken Anzeigefeld auf den Ordner zu dem Bereich, in dem Sie die Einstellungen ändern möchten.

Steht in der folgenden Übersicht hinter einer Option (Beschreibung ab Seite **), wird auf die entsprechende Seite in diesem Handbuch verwiesen. Fehlt eine Seitenangabe, folgt die Beschreibung nach der Übersicht in diesem Kapitel.

Suchen: Unter diesem Menüpunkt legen Sie fest, wo und wie AntiVir nach Viren suchen soll. Hier finden Sie auch die Einstellungen zu 'Auszulassende Dateien' und 'Archive'
(Beschreibung ab Seite 40).

Reparatur: Hier lassen sich Einstellungen für die Reparatur infizierter Dateien vornehmen
(Beschreibung ab Seite 52).

Makroviren: Hier werden alle Voreinstellungen zur Suche und Beseitigung von Makroviren ausgewählt. Hier finden Sie auch die Einstellungen zu 'Auszulassende Makros'
(Beschreibung ab Seite 58).

Drag & Drop: Hier können Sie festlegen, ob bei Drag & Drop auch Unterverzeichnisse durchsucht und welche Dateiarten berücksichtigt werden sollen.

Update über das Internet: In diesem Ordner ändern Sie die Einstellungen, die das Update über das Internet betreffen.
(Beschreibung ab Seite 129).

Report: Entscheiden Sie, welche Informationen in der Reportdatei aufgenommen werden sollen. Hier finden Sie auch die Einstellungen zum 'Kurzreport'
(Beschreibung ab Seite 70).

Diverses: Stellen Sie hier ein: Den Start eines Bildschirmschoners (Leerlaufzeit), den temporären Pfad, ob sich die Virenprüfung abbrechen läßt und ob zu löschende Dateien überschrieben werden sollen.

Bestätigen Sie die Änderungen mit OK, mit Abbruch bleiben die Einstellungen unverändert. Schließen Sie das Fenster 'Optionen' mit der Tastenkombination Alt+F4 oder mit der Schaltfläche X in der Titelleiste, werden die Änderungen nicht übernommen.

Diese beiden Funktionen lassen sich über das Menü 'Optionen' aufrufen:

Einstellungen sichern: Alle aktuellen Einstellungen werden einmalig in der Datei AVWIN95.INI bzw. AVWINNT.INI gespeichert.

Einstellungen beim Beenden speichern: Alle aktuellen Einstellungen werden beim Verlassen des Hauptprogrammes in der Datei AVWIN95.INI bzw. AVWINNT.INI gespeichert.

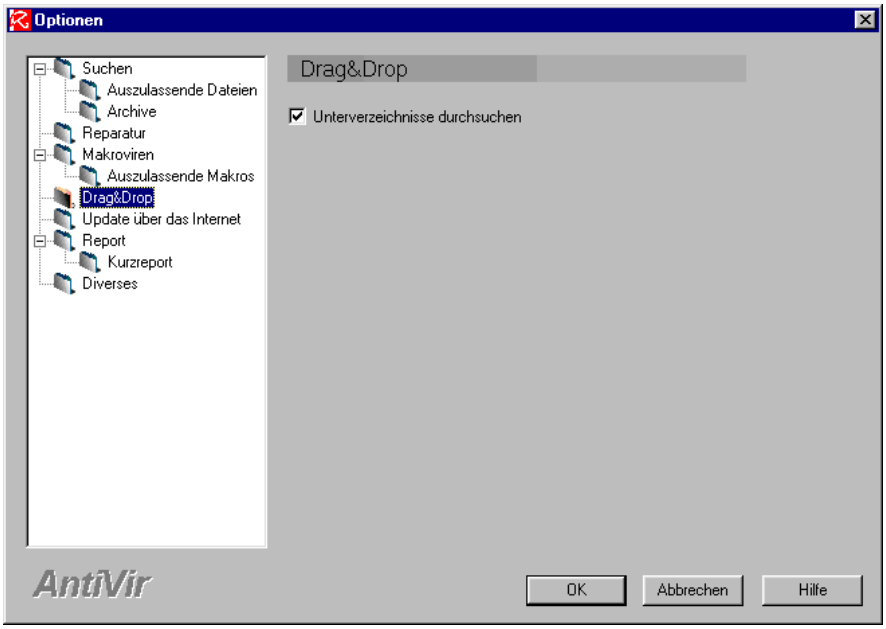
Kommandozeilenparameter

AntiVir läßt sich mit verschiedenen Kommandozeilenparametern starten, die in bestimmten Situationen sowohl bei der Anpassung an Ihre Rechnerumgebung als auch bei Problemen mit besonders hartnäckigen Viren nützlich für Sie sein können. Eine ausführliche Beschreibung finden Sie im Kapitel 'Kommandozeilenparameter' ab Seite 121.

Optionen/Drag & Drop

Mit Drag & Drop lassen sich Verzeichnisse oder Dateien auf das Hauptfenster von AntiVir ziehen. Diese werden dann nach Viren durchsucht.

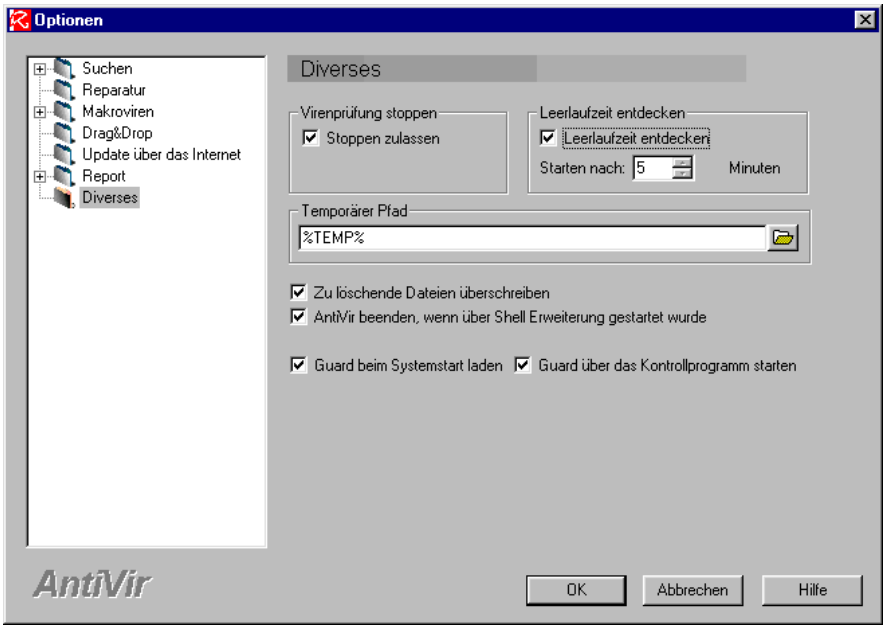
In diesem Ordner werden Einstellungen zu Drag & Drop festgelegt:



Unterverzeichnisse durchsuchen

Ist diese Funktion markiert, werden im Modus Drag & Drop alle Unterverzeichnisse bei der Virensuche berücksichtigt.

Optionen/Diverses



Anzeigegruppe 'Virenprüfung stoppen' Alt+S

Ist das Kontrollfeld 'Stoppen zulassen' aktiviert, läßt sich eine Virensuche im Fenster 'Luke Filewalker' jederzeit mit der roten Schaltfläche Stop beenden. Ist diese Einstellung deaktiviert, wird diese Schaltfläche grau unterlegt. Sie können die Virensuche nicht vorzeitig beenden und müssen brav warten, bis AntiVir sein Werk vollendet hat.

Anzeigegruppe 'Leerlaufzeit entdecken' Alt+L

Ist diese Einstellung aktiviert, arbeitet AntiVir wie ein Bildschirmschoner. AntiVir prüft permanent, ob Sie mit Ihrem Rechner gerade arbeiten. Ist dies nicht der Fall, startet AntiVir nach einer angegebenen Zeitspanne automatisch eine Virensuche auf allen nicht wechselbaren Laufwerken. Zu Beginn der Virensuche aktiviert AntiVir den von Ihnen eingestellten Bildschirmschoner, falls es sich um den von Windows oder After Dark handelt.

Starten nach ... Minuten Alt+N: Sie geben in diesem Feld die Zeit ein, nach der AntiVir starten soll.

Bei After Dark ist es möglich, daß AntiVir zwar den Bildschirmschoner startet, selbst aber keine Dateien untersuchen kann. Einige Bildschirmschoner von After Dark geben den Prozessor nicht mehr frei und die Virensuche von AntiVir kommt nicht zum Zug.

Anzeigegruppe 'Temporärer Pfad' Alt+T

Der temporäre Pfad für AntiVir wird verwendet, um Reparaturen durchzuführen, Archive zu entpacken und gepackte ausführbare Dateien zu entpacken und zu durchsuchen.

Mit dem Symbol Ordner können Sie auf gewohnte Weise durch das Ordnersystem blättern und Ihren Zielordner auswählen.

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 können deshalb die Umgebungsvariable 'TEMP' oder 'TMP' in Ihrer AUTOEXEC.BAT setzen (SET TMP=C:\RAMDISK).

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

Zu löschende Dateien überschreiben Alt+Z

Ist dieses Optionsfeld aktiviert, werden die Daten einer zu löschenden Datei zuerst überschrieben und anschließend gelöscht. Diese Einstellung sollte immer aktiv sein, da auf diese Weise das Wiederherstellen einer infizierten Datei (z.B. mit UNFORMAT) nicht mehr möglich ist.

AntiVir beenden, wenn über Shell Erweiterung gestartet Alt+A

Wurde AntiVir über die Shell-Erweiterung gestartet, wird das Programm nach einem Suchlauf wieder beendet. Ist AntiVir aktiv und es wird mit Hilfe der Shell-Erweiterung eine Suche gestartet, hat diese Option keine Wirkung.

Guard beim Systemstart laden Alt+G

Soll der Guard beim Start von Windows aktiviert werden, muß diese Default-Einstellung aktiviert sein.

Guard über das Kontrollprogramm starten Alt+K

Wird diese Einstellung aktiviert, läßt sich der Guard vom Kontrollprogramm aus aktivieren.

Optionen/Einstellungen sichern Alt+O / E

Wenn Sie diesen Menüpunkt wählen, werden alle aktuellen Einstellungen von AntiVir einmalig in der Datei AVWIN95.INI bzw. AVWINNT.INI gespeichert.

Optionen/Einstellungen beim Beenden speichern Alt+O / I

Ist diese Funktion aktiv (gekennzeichnet durch einen Haken am Anfang des Textes), werden alle Einstellungen von AntiVir beim Verlassen des Programms automatisch in der Datei AVWIN95.INI bzw. AVWINNT.INI gespeichert.

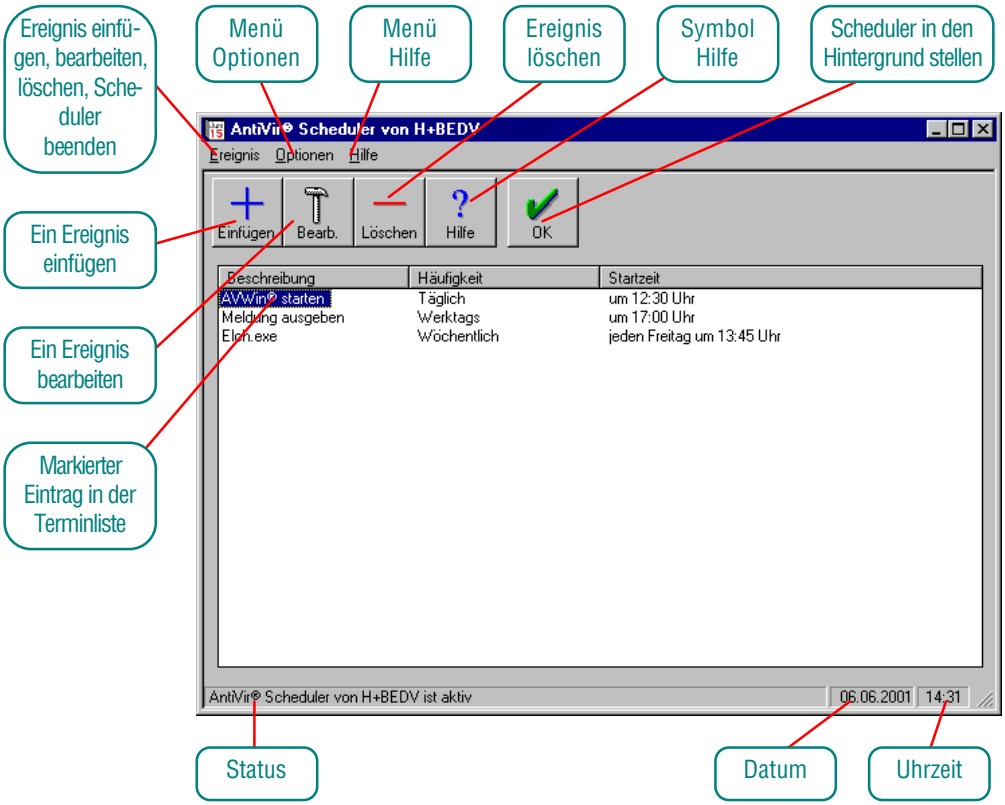
Wurden Änderungen vorgenommen, als diese Funktion nicht aktiv war, wird vor Beenden von AntiVir nachgefragt, ob diese Änderungen gespeichert werden sollen. Bestätigen Sie diese Abfrage mit Ja, werden die Änderungen gespeichert, mit Nein schließen Sie AntiVir ohne Speichern der Änderungen, mit Abbruch kehrt AntiVir zum Hauptmenü zurück, als ob nichts geschehen wäre.

13 AntiVir zu festgelegten Zeitpunkten starten

Sie wollen routinemäßig Ihre Programme und Daten auf Viren untersuchen und dazu nicht immer extra AntiVir manuell starten. Für diesen Fall bietet Ihnen der Scheduler die Möglichkeit, AntiVir zu festgelegten Zeiten zu aktivieren. Dabei können Sie auswählen zwischen den Zeitpunkten einmalig, täglich, werktags oder wöchentlich.

Ihr Rechnersystem muß zu dem Zeitpunkt in Betrieb sein.

Der Scheduler von AntiVir muß entweder manuell oder automatisch aktiviert worden sein.



Bestimmen Sie den Zeitpunkt, an dem der Scheduler AntiVir starten soll:

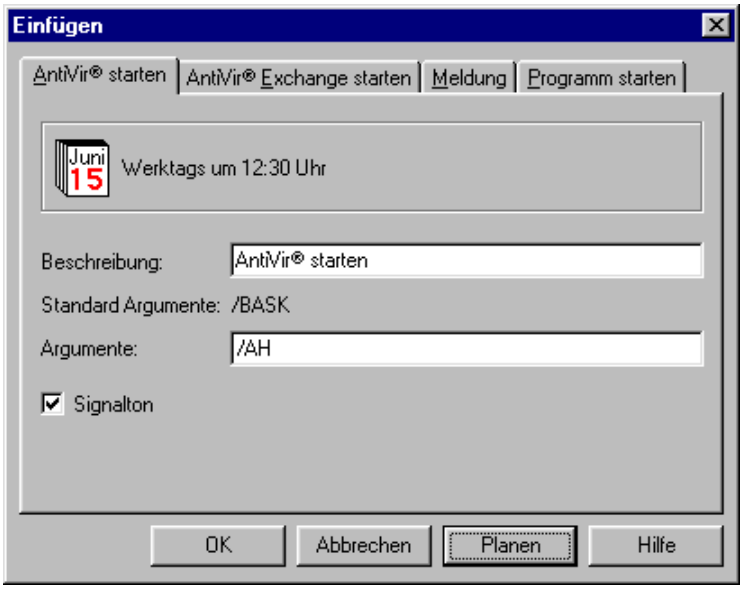
➔ Rufen Sie Ihre AntiVir-Version auf.

➔ Öffnen Sie den Scheduler mit der Schaltfläche **Scheduler**, über die Menüleiste 'Tools/Scheduler' oder die Tastenkombination Alt+T / S. Vom Desktop aus läßt sich der Scheduler aus der Programmgruppe 'AntiVir' oder – soweit angelegt – durch eine Verknüpfung starten.

Ereignis einfügen

➔ Wählen Sie im Hauptfenster durch ein Mausklick auf die Schaltfläche Einfügen oder durch die Taste + den Menüpunkt 'Ereignis/Einfügen'.

Es erscheint die Registerkarte 'AntiVir starten':



Im Feld 'Beschreibung' ist bereits der Befehl 'AntiVir starten' eingetragen. Dieser Eintrag wird später im Listenfeld des Schedulers angezeigt.

➔ In das Feld 'Laufwerk' gelangen Sie durch Mausklick auf das entsprechende Eingabefeld oder durch die Tastenkombination Alt+L.

➔ Geben Sie in diesem Feld den Laufwerksbuchstaben des Laufwerkes ein, das nach Viren durchsucht werden soll.

Sie können auch Kommandozeilenparameter, beispielsweise /AH (all harddisks) oder /AF (all floppies) eingeben. Es lassen sich bis zu 26 Laufwerksbuchstaben eintragen.

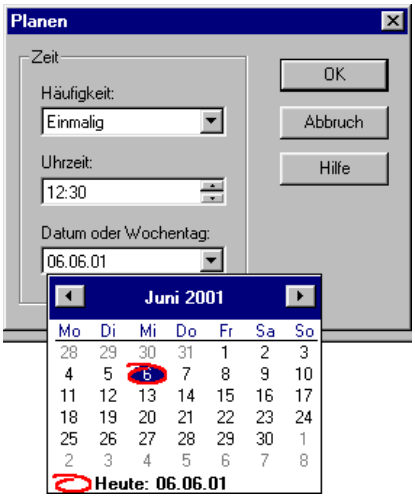
➔ In das Feld 'Signalton' gelangen Sie durch Mausklick auf das Eingabefeld oder durch die Tastenkombination Alt+S.

Ist dieses Feld markiert, gibt AntiVir beim Aufruf durch den Scheduler einen Signalton aus.

➔ Klicken Sie die Schaltfläche Planen an oder verwenden Sie die Tastenkombination Alt+P, um das Fenster 'Planen' aufzurufen.

➔ Klicken Sie auf das Listenfeld 'Häufigkeit', in diesem Feld bestimmen Sie, wann AntiVir ausgeführt werden soll.

Die Anzeigen in den Feldern Uhrzeit, Datum und Wochentag hängen von der Auswahl der Optionen im Listenfeld 'Häufigkeit' ab:



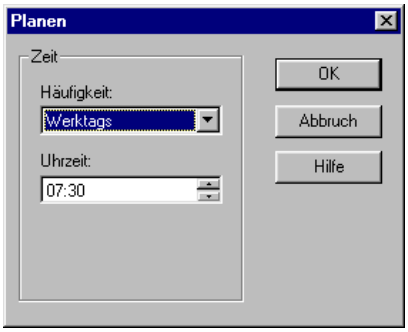
Einmalig: AntiVir wird nur einmal am festgelegten Tag zur festgelegten Zeit ausgeführt. Nach dem Start wird der Aufruf aus der Ereignisliste gelöscht.

Im Feld 'Uhrzeit' ist die aktuelle Systemzeit voreingestellt. Klicken Sie auf dieses Feld, läßt sich eine andere Uhrzeit eingeben (zum Beispiel 15:09).

Im Feld 'Datum' läßt sich der gewünschte Termin direkt eingeben. Klicken Sie auf den Pfeil rechts von diesem Feld, erscheint ein Kalender mit dem aktuellen Systemdatum, dort läßt sich ebenfalls ein anderes Datum einstellen.

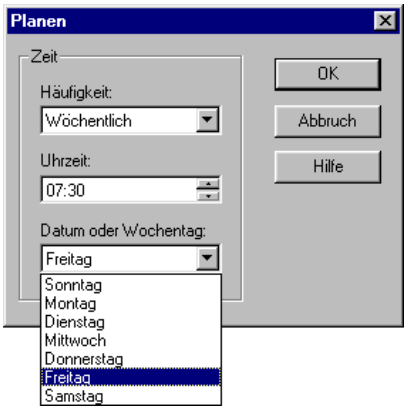
Täglich: Das Ereignis tritt täglich zur festgelegten Zeit auf.

Im Feld 'Uhrzeit' ist die aktuelle Systemzeit voreingestellt. Klicken Sie auf dieses Feld, läßt sich eine andere Uhrzeit eingeben (beispielsweise 12:30).



Werktags: Das Ereignis wird an jedem Werktag (Montag bis Freitag) zur festgelegten Uhrzeit ausgeführt.

Im Feld 'Uhrzeit' ist die aktuelle Systemzeit voreingestellt. Klicken Sie auf dieses Feld, läßt sich eine andere Uhrzeit eingeben (z.B. 17:00).



Wöchentlich: AntiVir wird an dem ausgewählten Wochentag zur festgelegten Uhrzeit ausgeführt.

Im Feld 'Uhrzeit' ist die aktuelle Systemzeit voreingestellt. Klicken Sie auf das Feld, läßt sich eine andere Uhrzeit eingeben (z.B. 13:45).

Im Feld 'Wochentag' wird der Tag ausgewählt, an dem AntiVir gestartet werden soll. Voreingestellt ist der aktuelle Wochentag.

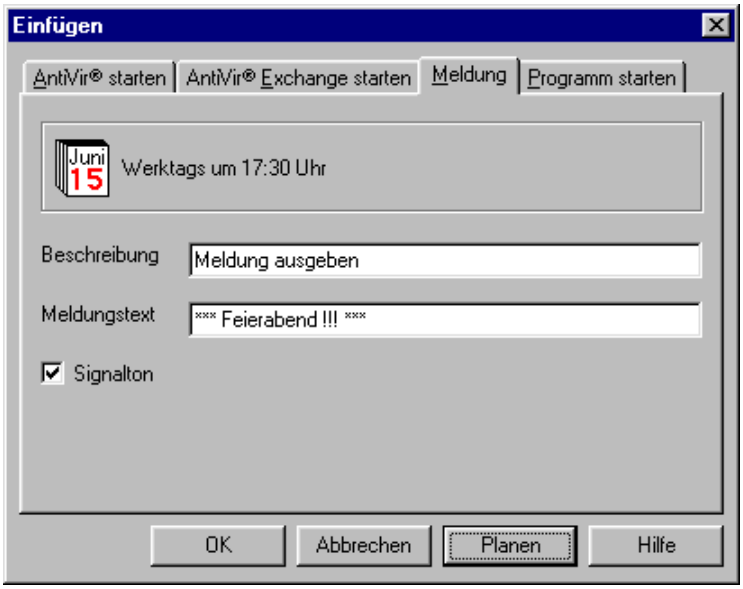
➔ Tragen Sie in diesem Fenster 'Planen' alle notwendigen Angaben für die gewünschte Einstellung ein.

➔ Bestätigen Sie diese Einträge mit der Taste ↵ oder klicken auf OK.

Im Fenster 'Einfügen' ist jetzt die Schaltfläche OK aktiv.

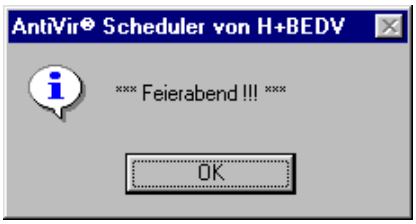
➔ Bestätigen Sie den Zeitpunkt für den automatischen Programmstart von AntiVir mit der Taste ↵ oder klicken Sie auf OK, damit dieses Ereignis in die Ereignisliste aufgenommen wird.

Sie können den Scheduler auch für die automatische Anzeige von Meldungen nutzen. Rufen Sie dazu unter 'Ereignis/Einfügen' die Registerkarte 'Meldung' auf und geben einen Meldungstext ein:

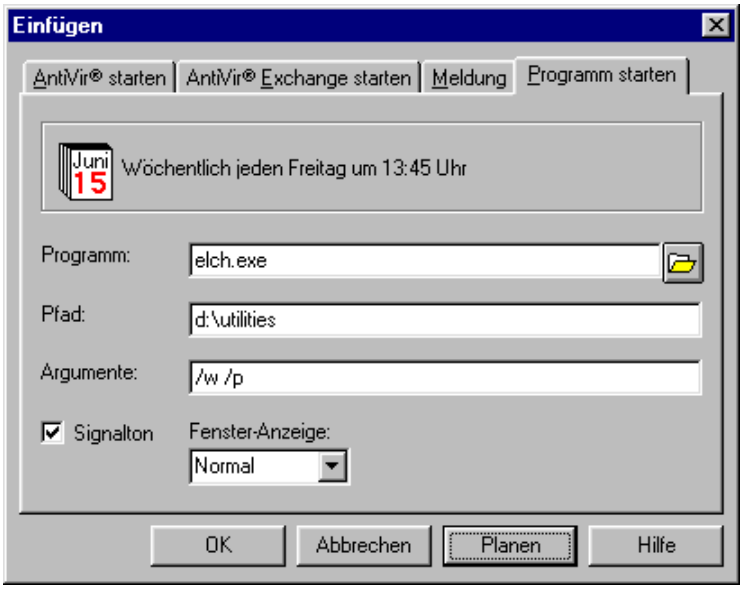


Mit der Schaltfläche **'Planen'** wird ein Fenster aufgerufen, mit dem sich, der Termin bestimmen läßt, an dem die Meldung angezeigt werden soll. Das funktioniert genau wie im Abschnitt zur Registerkarte 'AntiVir starten' beschrieben.

Ist zum ausgewählten Zeitpunkt sowohl das Rechnersystem in Betrieb als auch der Scheduler aktiviert, erscheint die Meldung am ausgewählten Termin zur festgelegten Uhrzeit, beispielsweise:



Sie können den Scheduler auch zum Starten anderer Programme nutzen. Geben Sie dazu in der Registerkarte 'Programm starten' in den entsprechenden Feldern den Startbefehl und den Pfad des zu startenden Programmes an:



Geben Sie in das Textfeld **'Programm'** den Namen des Programms ein, das Sie starten möchten oder öffnen Sie mit der Schaltfläche Durchsuchen das Dialogfenster 'Zu startende Programme' und wählen dort das gewünschte Programm aus. Bei der Auswahl mit Durchsuchen wird der markierte Dateiname automatisch in das Textfeld übernommen.

In das Textfeld **'Pfad'** wird der Pfad eingegeben, in dem sich das zu startende Programm befindet. Wurde das Programm im Dialogfenster 'Zu startende Programme' ausgewählt, wird der im Dialogfenster angegebene Pfad automatisch in das Textfeld übernommen.

Im Textfeld **'Argumente'** lassen sich Kommandozeilenparameter für das zu startenden Programm angeben.

Im Listenfeld **'Fensteranzeige'** können Sie den Modus wählen, in dem das Programm ausgeführt wird. Sie haben die Wahl zwischen 'Normal', 'Symbol' und 'Vollbild'. Voreingestellt ist der Modus Normal.

Mit der Schaltfläche **'Planen'** wird ein Fenster aufgerufen, mit dem sich, der Termin bestimmen läßt, an dem die Meldung angezeigt werden soll. Das funktioniert genau wie im Abschnitt zur Registerkarte ' AntiVir starten' beschrieben.

Ereignis bearbeiten

➔ Um ein Ereignis aus dem Terminplan des Schedulers zu bearbeiten, beispielsweise um die Uhrzeit oder ein Datum zu ändern, markieren Sie diesen Eintrag im Listenfeld des Schedulers.

➔ Aktivieren Sie diesen Modus über die Schaltfläche Bearbeiten, die Menüleiste mit 'Ereignis/Bearbeiten', die Tastenkombination Alt+E / B, oder betätigen Sie einfach die Taste ↵.

➔ Wenn Sie einen Doppelklick auf einen Eintrag ausführen, wird ebenfalls das Menü 'Bearbeiten' aufgerufen.

Die Einträge lassen sich mit den gleichen Parametern bearbeiten wie unter dem Menü 'Ereignis/Einfügen' beschrieben.

➔ Haben Sie alle gewünschten Änderungen eingetragen, bestätigen Sie diese mit ↵ oder Anklicken von OK.

Das Ereignis wird mit den geänderten Einstellungen wieder in die Ereignisliste aufgenommen.

Löschen eines Ereignisses - oder Alt+E / L

Mit diesem Menüpunkt können Sie ein Ereignis aus dem Terminplan des Scheduler-Fensters entfernen.

Achtung: Ein Ereignis wird sofort gelöscht, ohne daß nach einer Bestätigung gefragt wird! Das gelöschte Ereignis kann nicht wiederhergestellt werden.

➔ Markieren Sie den Eintrag, der gelöscht werden soll, im Listenfeld des Schedulers.

➔ Wählen Sie nun den Menüpunkt 'Löschen' oder klicken Sie auf die Schaltfläche Löschen.

Das Ereignis wird sofort aus dem Terminplan gelöscht.

Hilfe aufrufen Alt+F1

➔ Rufen Sie die Hilfe für den AntiVir Scheduler über die Schaltfläche Hilfe, die Menüleiste mit 'Hilfe/Inhalt' oder die Tastenkombination Alt+F1 bzw. Alt+H / H auf.

Sie finden hier für den AntiVir Scheduler die Stichworte 'Ereignis', 'Hilfe' und 'Kommandozeile'.

In den Hintergrund stellen

Mit dieser Schaltfläche OK läßt sich der AntiVir Scheduler in den Hintergrund stellen, das Programm wird also *nicht* geschlossen sondern bleibt aktiviert, solange Windows nicht beendet wird. Der Scheduler verkrümelt sich in den Hintergrund.

Auch mit einem Doppelklick auf das Icon H+BEDV im Steuermenü (in der linken oberen Ecke des Hauptfensters) bzw. Anklicken dieses Icons und scrollen auf den Befehl 'Schließen' wird der Scheduler in den Hintergrund gestellt. Das gilt auch für die Schaltfläche X rechts oben in der Titelleiste.

➔ Der Scheduler kann per Doppelklick auf das kleine rot-weiße Kalender-Icon in der Task-Leiste unten rechts wieder in den Vordergrund geholt werden.

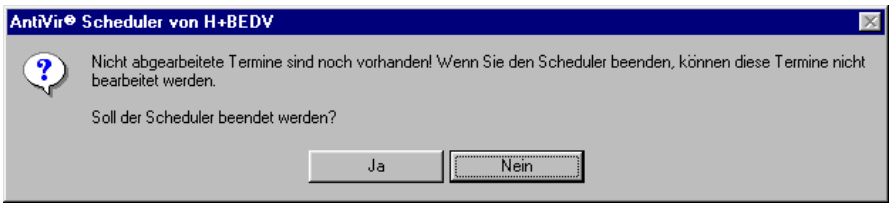
Scheduler beenden Alt+F4

➔ Schließen Sie den Scheduler entweder im Menü 'Ereignis / Ende'

➔ oder mit der üblichen Tastenkombination Alt+F4 'Schließen'.

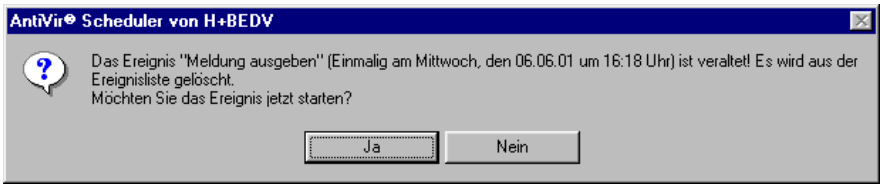
Einmal aufgerufen, läßt sich der Scheduler *nicht* durch gewohnten Doppelklick auf das Icon H+BEDV im Steuermenü (in der linken oberen Ecke des Hauptfensters) bzw. Anklicken dieses Icons und scrollen auf den Befehl 'Schließen' beenden. Auch mit der Schaltfläche X rechts oben in der Titelleiste geht das nicht. Statt dessen verschwindet das Programm wieder in den Hintergrund und bleibt aktiv. Der Scheduler läßt sich per Doppelklick auf das kleine rot-weiße Kalender-Icon in der Task-Leiste unten rechts wieder in den Vordergrund holen.

Es können nur dann Ereignisse vom AntiVir Scheduler aufgerufen werden, wenn dieser – zumindest im Hintergrund – aktiviert ist. Wird der Scheduler geschlossen, wenn einige Ereignisse noch nicht abgearbeitet sind, erscheint ein entsprechender Hinweis, beispielsweise:



➔ Quittieren Sie die Meldung nach Wunsch mit Ja oder Nein.

Konnte ein einmaliges Ereignis nicht abgearbeitet werden, weil beispielsweise der Scheduler nicht aktiv war, erscheint bei einem Neustart des Schedulers ein entsprechender Hinweis:



➔ Bestätigen Sie diese Meldung mit Ja, wird das im AntiVir Scheduler eingetragene Ereignis trotz der 'Verspätung' ausgeführt. Nach Quittieren mit Nein wird der Eintrag gelöscht.

Kommandozeilenparameter

Wollen Sie alle auftretenden Ereignisse für die Nachwelt erhalten und in einer Datei aufzeichnen, müssen Sie den Scheduler mit dem Kommandozeilenparameter '/LOG' starten. Die Datei AVSCHED.LOG wird im Installationsordner von AntiVir angelegt.

Beim Start mit dem Parameter /NoOldEvent prüft AVSched32 bei einem Neustart nicht, ob sich in der Ereignisliste veraltete Einträge befinden.

Soll beim Öffnen des Schedulers kein Startbild angezeigt werden, müssen Sie den Scheduler mit dem Kommandozeilenparameter '/NS' (steht für 'no screen') starten.

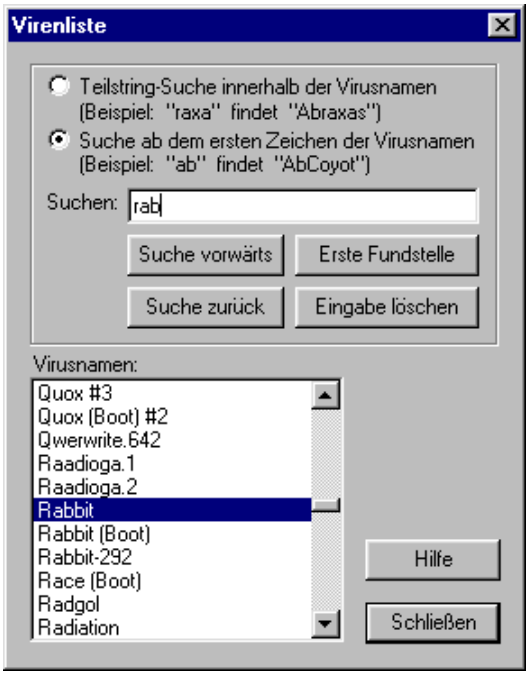
14 Informationen über bestimmte Viren erhalten

14.1 Virenliste aufrufen

Wollen Sie erfahren, welche Viren von AntiVir erkannt werden, hilft Ihnen die Virenliste weiter. Rufen Sie die Virenliste im Hauptfenster mit der Schaltfläche Virenliste, in der Menüleiste über den Punkt 'Tools/Virenliste' oder die Tastenkombination Alt+T / L auf.

AntiVir® für Windows erkennt mehr Viren, als in dieser Liste aufgeführt sind. Es werden manchmal nur die Namen von Viren oder eine Zeile eines Viruscodes verändert und diese modifizierten Viren als neue Viren in Umlauf gebracht. Die charakteristischen Merkmale eines Virus ändern sich dabei nicht, diese modifizierten Viren werden trotzdem von AntiVir erkannt.

Unter 'Virusnamen' befindet sich eine Liste mit denjenigen Virusnamen, die AntiVir bekannt sind. Die meisten Viren dieser Liste lassen sich auch mit AntiVir entfernen. Die Virennamen sind alphabetisch geordnet.



➔ Benutzen Sie die Bildlaufleiste, um in der Liste weiter nach unten oder zurück nach oben zu gelangen.

➔ Sie können auch im Feld 'Suchen' einen Buchstaben oder ein Zeichen auf der Tastatur eingeben, die Markierung springt auf die entsprechende Stelle der Namensliste.

Das Suchergebnis hängt von der Einstellung der Optionsfelder ab: hier ist 'Suche ab dem ersten Zeichen' ideal, wenn Sie den Namen genau wissen. Wenn Sie nicht genau wissen, wie der Virusname geschrieben wird, können Sie es mit der Einstellung 'Teilstring-Suche innerhalb des Virusnamen' versuchen. Wird die Zeichenfolge nicht gefunden, erscheint eine entsprechende Meldung links neben dem Feld mit den Virusnamen.

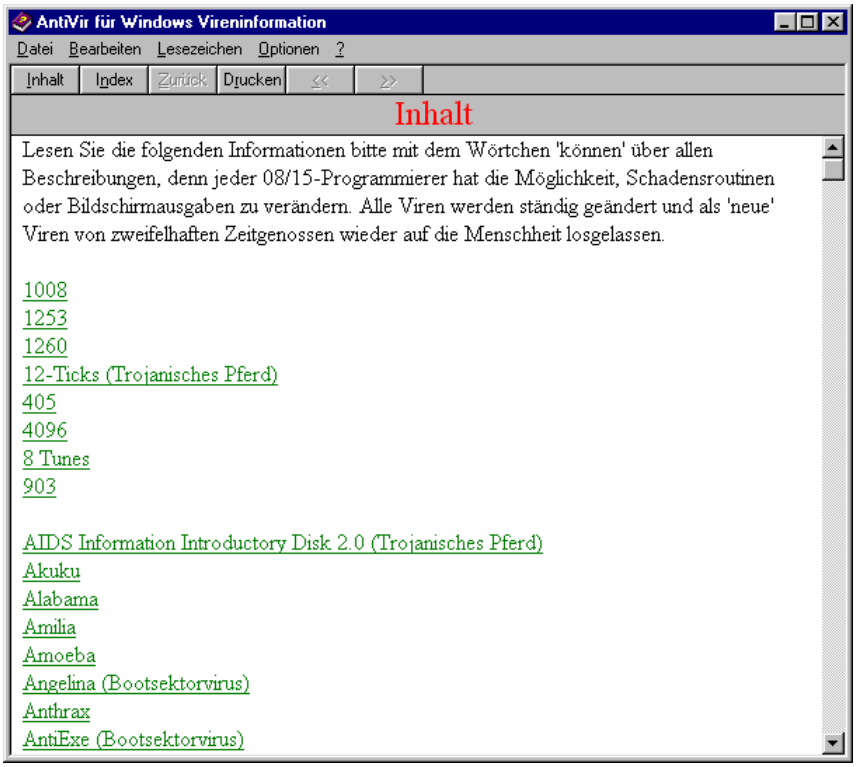
In diesem Fenster helfen die Schaltflächen Suche vorwärts, Suche zurück, Erste Fundstelle und Eingabe löschen beim Navigieren durch die Virenliste.

➔ Wollen Sie dieses Fenster verlassen, klicken Sie auf die Schaltfläche Schließen oder betätigen die Taste ↵.

14.2 Vireninformationen

Wenn Sie mehr über einen Virus wissen wollen, steht Ihnen in der Menüleiste 'Tools/Vireninformationen' eine Hilfedatei zur Verfügung, in der Informationen zu den meisten häufiger auftretenden Viren zu finden sind.

➔ Rufen Sie diese Hilfedatei über die Menüleiste mit 'Tools/Vireninformationen' Alt+T / V auf.



Die Bedienung entspricht der Handhabung der Windows-Hilfedateien.

Auswählen eines Virusnamens

- Benutzen Sie im Fenster 'Inhalt' die Bildlaufleiste, um in der Liste weiter nach unten oder zurück nach oben zu gelangen.
- Sie können auch die Schaltflächen im alphabetischen Register nutzen: Wenn Sie auf einen Buchstaben klicken, springt das Inhaltsverzeichnis auf den ersten Namen mit diesem Anfangsbuchstaben.
- Bewegen Sie dem Mauszeiger auf einen grün geschriebenen Namen. Der Mauszeiger verwandelt sich in eine Hand.
- Rufen Sie den Virusnamen, auf den der Zeigefinger weist, durch einen Mausklick auf. Es erscheint ein Fenster mit Informationen über den ausgewählten Virus.

Finden Sie im Text wiederum ein grün geschriebenes Wort, können Sie diese Stelle erneut anklicken. Es erscheint ein weiteres Fenster zu dem neuen Stichwort.

- Sie können zur Auswahl eines Informationstextes auch die Schaltfläche Index anklicken oder die Tastenkombination Alt+N betätigen. Es erscheint folgendes Dialogfenster:

- Geben Sie im Textfeld, in dem sich der Cursor befindet, einen Namen ein. Sobald Sie einen Buchstaben oder ein Zeichen auf der Tastatur eingeben, springt die Markierung zur entsprechenden Stelle der Namensliste. Oder wählen Sie einen Namen direkt in der Namensliste aus und markieren diesen mit einem Mausklick.
- Mit den Bildlaufpfeilen oder der Bildlaufmarke blättern Sie in dieser Liste vorwärts und zurück.
- Nach Auswahl des gewünschten Namens betätigen Sie die Schaltfläche Anzeigen. Das Stichwort erscheint im Hilfe-Fenster.

Doch nun zurück zu den Funktionen des Fensters Vireninformation:

- Mit der Schaltfläche Zurück gelangen Sie in die Ebene, die vorher aktiv war. Wenn Sie mehrere Querverweise geöffnet hatten, bewegen Sie sich mit dieser Schaltfläche schrittweise zurück.
- Mit der Schaltfläche Inhalt gelangen Sie zurück in das Fenster 'Inhalt'.
- Mit der Schaltfläche Bisher rufen Sie ein Fenster auf, in dem alle seit dem Start der Vireninformation aufgerufenen Stichworte verzeichnet sind. Dort können Sie durch einen Doppelklick auf einen Namen diese Information erneut aufrufen.
- Mit den Schaltflächen << und >> wird in allen seit Start der Vireninformation aufgerufenen Stichworten zurück- bzw. vorgeblättert.

Informationen drucken

- Drucken Sie über die Menüleiste mit 'Datei/Thema drucken' den Inhalt des aktuellen Fensters aus.
- Um den Drucker einzurichten, rufen Sie zuerst das Menü 'Datei/Thema drucken' auf. Dort klicken Sie auf die Schaltfläche Eigenschaften und nehmen die gewünschten Einstellungen vor.

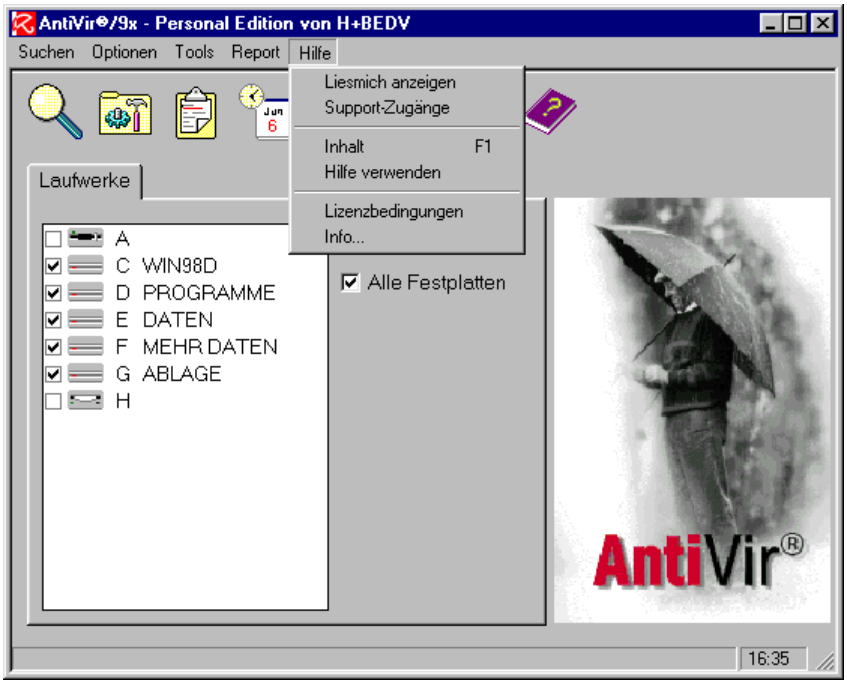
Vireninformation schließen

- Schließen Sie das Fenster Vireninformation mit der Schaltfläche X (Beenden) rechts oben in der Titelleiste, der Tastenkombination Alt+F4 oder über die Menüleiste mit 'Datei/Beenden'.

Weitere Informationen über die Funktionen von Hilfedateien erhalten Sie in der Windows-Dokumentation.

15 Hilfe zu AntiVir aufrufen

Rufen Sie die Hilfe mit der Schaltfläche Hilfe im Hauptfenster, über den Punkt 'Hilfe' in der Menüleiste oder die Taste F1 bzw. die Tastenkombination Alt+H auf.

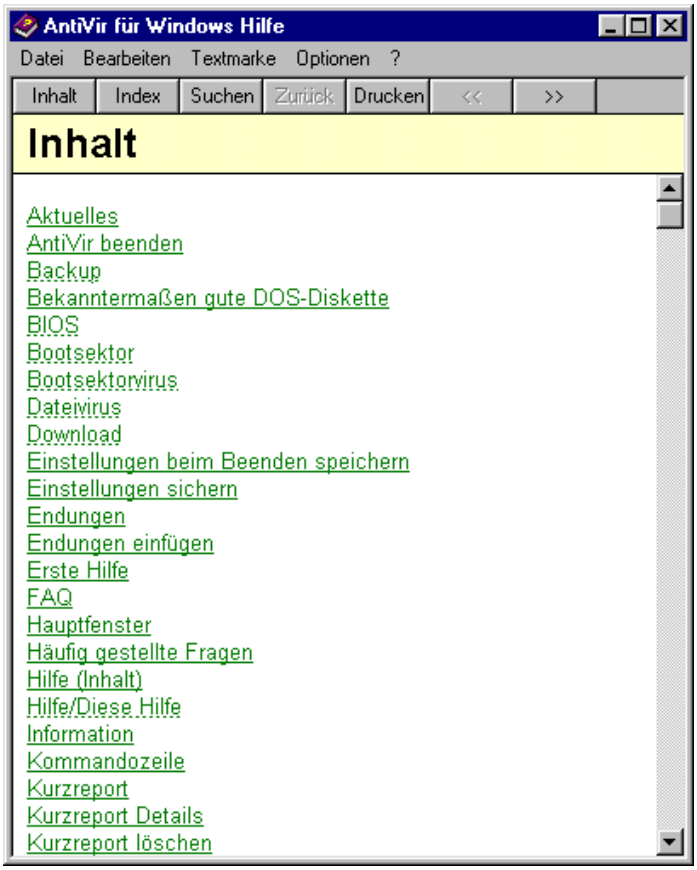


Liesmich Alt+H / M

In dieser Datei finden Sie wichtige Informationen zu jeder neuen Version von AntiVir. Durch die kurzen Zeiträume zwischen den Updates ist es uns nicht immer möglich, alle Neuerungen im Handbuch aufzunehmen; diese Neuerungen werden deshalb in der Datei LIESMICH.WRI beschrieben.

Inhalt Alt+H / I

Mit dem Menüpunkt 'Inhalt' wird das Inhaltsverzeichnis der Hilfe angezeigt. Dieselbe Funktion hat auch die Schaltfläche Hilfe. Der Aufbau der Hilfe von AntiVir entspricht der unter Windows üblichen Konvention. Sie können eines der aufgelisteten Themen aufrufen und sich anzeigen lassen.



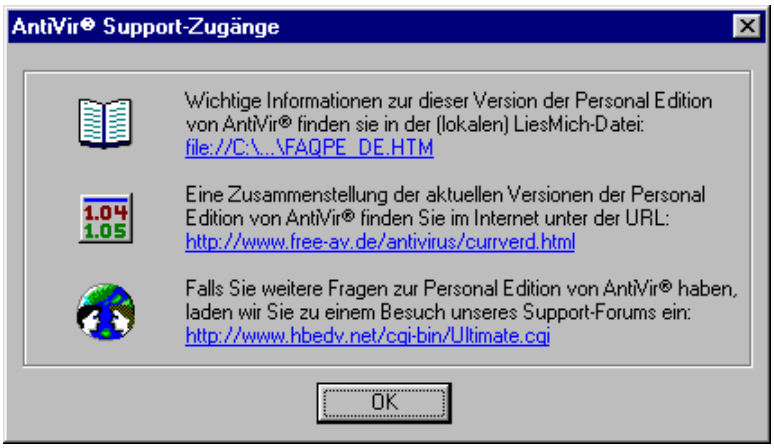
Hilfe verwenden Alt+H / H

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

Für eine genauere Beschreibung der Hilfefunktionen bleibt Ihnen der Blick in das Windows-Handbuch nicht erspart.

Support-Zugänge Alt+H / S

Mit diesem Menüpunkt wird ein Fenster geöffnet, in dem die wichtigsten Informationsquellen und Supportwege für die AntiVir Personal Edition aufgeführt sind:



Lizenzbedingungen Alt+H / L

Mit diesem Menüpunkt lassen sich die aktuellen Lizenzbedingungen im Windows Write-Editor anzeigen.

Lesen Sie solche Texte gerne in etwas größerer Schrift oder schwarz auf weiß, finden Sie diese Lizenzbedingungen auch in diesem Handbuch ab Seite 10.

Info Alt+H / N

Hier werden Informationen zu AntiVir angezeigt: das sind die Versionsnummern des Hauptprogrammes, der Suchengine und des AVGuard sowie Copyright, der Name des Lizenznehmers und die Seriennummer sowie die Telefonnummer der Hotline.

16 AntiVir beenden

- Schließen Sie AntiVir entweder unter dem Menü 'Suchen' mit 'AntiVir beenden',
- durch Anklicken des AntiVir-Symbols im Steuermenü (das Schirm-Icon in der linken oberen Ecke) und scrollen auf den Befehl 'Schließen',
- mit der üblichen Tastenkombination Alt+F4 'Schließen'
- oder mit Hilfe der Schaltfläche X rechts oben in der Titelleiste.

Ist der Menüpunkt 'Optionen/Einstellungen beim Beenden speichern' beim Schließen von AntiVir aktiv (gekennzeichnet durch einen ✔ am Anfang des Textes), werden automatisch alle Einstellungen in der Datei AVWIN.INI gespeichert. Ist dieser Punkt nicht aktiv und wurden Einstellungen geändert, fragt AntiVir nach, ob diese Änderungen gesichert werden sollen.

Um den **Virenwächter** zu beenden, klicken Sie im Menü 'Datei' auf den Punkt 'Ende und Schließen'. Das Icon verschwindet dann aus der Task-Leiste .

Wurde die Schaltfläche Deaktivieren im Steuermenü der AntiVir Guard betätigt, wird der Virenwächter *nicht* beendet. Auch durch gewohnten Doppelklick auf das Schirm-Icon im Steuermenü (in der linken oberen Ecke des Hauptfensters) bzw. Anklicken dieses Icons und scrollen auf den Befehl 'Schließen' wird der AV Guard *nicht* beendet. Das gilt auch für die Schaltfläche X rechts oben in der Titelleiste und die Tastenkombination Alt+F4.

17 Kommandozeilenparameter von AntiVir

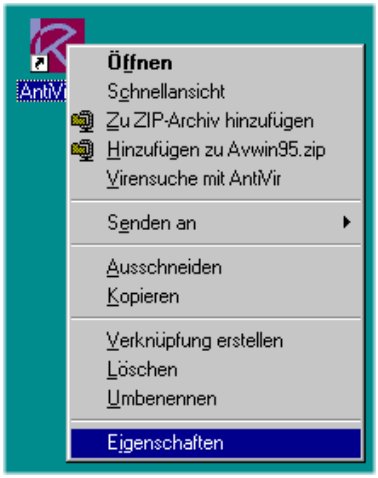
AntiVir stellt Ihnen mehrere Kommandozeilenparameter zur Verfügung, die in bestimmten Situationen sowohl bei der Anpassung an Ihre Rechnerumgebung als auch bei Problemen mit besonders hartnäckigen Viren nützlich sein können.

Geben Sie unter Windows Me/98/95 bzw. Windows 2000/NT Kommandozeilenparameter folgendermaßen ein:

Hier gibt es mal wieder Unterschiede zwischen den einzelnen Windows-Varianten, stellvertretend ist hier das Beispiel Windows 98 beschrieben.

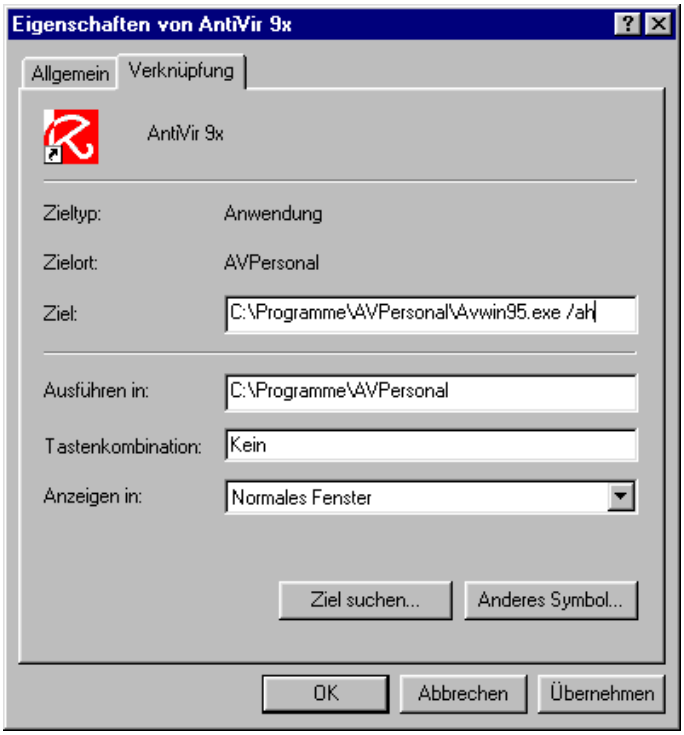
Verläuft die Angabe von Kommandozeilenparametern bei Ihnen irgendwie anders, müssen Sie die Hilfe Ihrer Windows-Version um Rat fragen.

➔ Klicken Sie mit der rechten Maustaste auf das AntiVir-Icon auf dem Desktop. Es erscheint dieses Menü:



➔ Klicken Sie dort den Punkt 'Eigenschaften' an.

Es erscheint ein Fenster mit mehreren Registerkarten:



➔ Klicken Sie in diesem Fenster die Registerkarte 'Verknüpfung' an.

➔ Tragen Sie im Feld 'Ziel' hinter dem Pfad und dem Dateinamen die gewünschten Parameter ein. Dabei muß zwischen einem Dateinamen und dem Schrägstrich vor einem folgenden Parameter ein Leerzeichen gesetzt sein.

Geben Sie mehrere Kommandozeilenparameter ein, müssen diese ebenfalls durch ein Leerzeichen voneinander getrennt sein. Welche Kombination für Ihre Zwecke sinnvoll ist, hängt von Ihrem Rechnersystem sowie auch von Ihrem Sicherheitsbedürfnis ab.

➔ Mit der Schaltfläche Übernehmen wird diese Einstellung in der .INI-Datei von Windows gespeichert. AntiVir wird dann nach einem Neustart von Windows mit diesem Parameter aufgerufen.

➔ Damit die Änderungen beim nächsten Start von AntiVir wirksam werden, müssen Sie Ihren Eintrag mit der Schaltfläche OK bestätigen.

Und dazu können Sie die Kommandozeilenparameter verwenden:

/AF Bedeutet 'All Floppies' und sorgt dafür, daß bei Start von AntiVir alle Diskettenlaufwerke markiert sind. In Zusammenhang mit dem Batchmodus werden beim Aufruf von AntiVir alle Diskettenlaufwerke durchsucht, die Einträge über Laufwerke der AVWIN.INI werden ignoriert.

/AH Bedeutet 'All Harddisks' und sorgt dafür, daß bei Start von AntiVir alle Festplatten markiert sind. In Zusammenhang mit dem Batchmodus werden beim Aufruf von AntiVir alle Festplatten durchsucht, die Einträge über Laufwerke der AVWIN.INI werden ignoriert.

/B Steht für Batchmodus und wird z.B. benötigt, wenn AntiVir mit der Autostart-Gruppe von Windows aufgerufen wird. Alle in der Datei AVWIN.INI aufgeführten Laufwerke oder Parameter werden überprüft. Der automatische Batchmodus wird nur vorzeitig beendet, wenn im Speicher Viren gefunden wurden oder wenn ein Bootsektor oder Master-Bootsektor infiziert ist. Eine Reportdatei sollte immer angelegt werden.

/BASK ist ein automatischer Batchmodus, bei dem die Einstellungen von AntiVir beachtet werden. Haben Sie die Voreinstellungen geändert, daß beispielsweise alle gefundenen Viren automatisch repariert werden, wird dies in diesem Modus auch gemacht. Sollten Sie diesen Parameter zusammen mit dem Parameter /B angeben, wird Parameter /B ignoriert.

/BASK+ Dieser Parameter ist identisch mit /BASK, bis auf den kleinen Unterschied, daß am Ende eines Suchlaufes die Statistik über diesen Suchlauf angezeigt wird.

/CLA Die Reportdatei wird nach jedem Schreibzugriff geschlossen. Verwenden Sie diesen Parameter nur nach Rücksprache mit dem Support von H+BEDV, da durch das permanente Öffnen und Schließen der Reportdatei die Performance sinkt.

/DY Dieser Parameter 'daily' ist nur im Batchmodus wirksam. Es muß also einer der folgenden Parameter zusätzlich gesetzt sein: /B, /BASK oder /BASK+. Sofern keine Viren gefunden wurden und die Suche normal beendet wurde (der Suchlauf nicht abgebrochen wurde), speichert AntiVir das aktuelle Datum in einer Datum-Log-Datei (AVWIN95.DLG bzw. AVWINNT.DLG). Wird AntiVir am gleichen Tag nochmals mit denselben Parametern gestartet, wird nur der Selbsttest durchgeführt. Am folgenden Tag wird beim ersten Aufruf von AntiVir wieder gemäß aller angegebenen Parameter gesucht.

/DYNoMsg Dieser Parameter 'daily/no message' ist identisch mit /DY bis auf den Unterschied, daß keine Meldung beim Beenden nach dem Selbsttest ausgegeben wird.

/FF Mit 'full file' werden die zu durchsuchenden Dateien vollständig überprüft (Voreinstellung: nur die ersten und die letzten 20 KB werden überprüft).

/GURU Wird der /Guru-Parameter verwendet, finden Sie unter dem Menü 'Suchen' zusätzlich die Funktion 'Diskedit', der Ihnen einen Diskeditor zur Verfügung stellt.

/IM Mit diesem Parameter 'infected move' können Sie unter 'Optionen / Diverses' einstellen, ob infizierte Dateien vor der Reparatur in den Ordner INFECTED verschoben werden sollen. Wurde AntiVir ohne '/IM' gestartet, ist diese Auswahl nicht möglich.

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

/NOESC Mit 'No Escape' gibt's keine Rettung, ein Suchlauf läßt sich nicht vom Anwender unterbrechen. Die Schaltfläche 'Stop' im Luke Filewalker ist deaktiviert.

/NOHMA Bedeutet 'No High Memory Area' und schaltet den Speichertest in der HMA (zwischen 1024K – 1088K) ab.

/NOUMB Bedeutet 'No Upper Memory Block' und schaltet den Speichertest in den UMB-Bereichen (zwischen 640K – 1MB) ab.

/NS Steht für 'No Screen' und unterdrückt die Anzeige des Startbildes beim Start von AntiVir.

/R0 Es wird keine Reportdatei erstellt. Dieser Parameter ist nur in Zusammenhang mit Parameter '/B' wirksam. Er dient ausschließlich zum Testen.

X: Steht für einen Laufwerksbuchstaben. Die Einstellungen für die Laufwerke aus der Datei AVWIN.INI werden ignoriert und nur diese ausgewählten Laufwerke werden überprüft. Hier sind maximal 26 Einträge möglich.

Die Kommandozeilenparameter lassen sich beliebig mischen, eine wichtige Ausnahme ist der Parameter /R0: Er läßt sich nur zusammen mit dem Parameter /B einsetzen (und ist auch nur dann sinnvoll; sonst befindet sich ein Virus auf dem Rechner und Sie merken nichts davon ...).

18 AntiVir aktualisieren

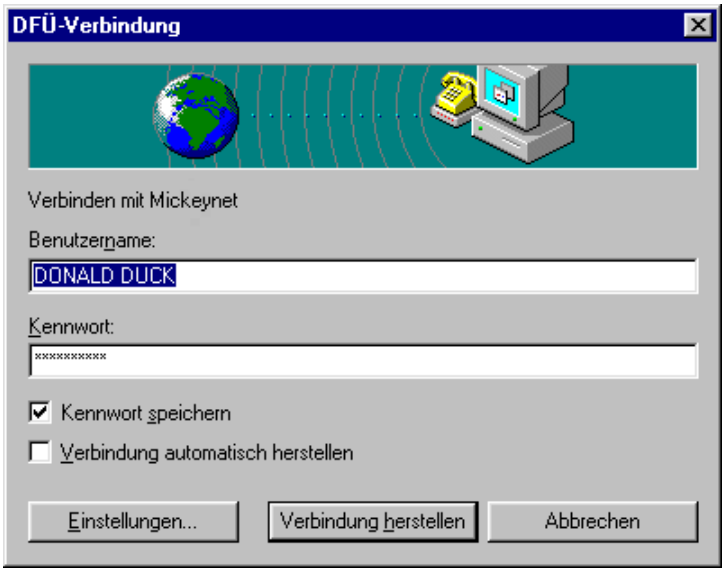
Da ständig neue Computerviren programmiert und auch in Umlauf gebracht werden, ist nichts älter als ein Antiviren-Programm von gestern. Ständige Weiterentwicklung sowie die Aufnahme neuer Viren sind deshalb unser Tagesgeschäft. Damit Sie immer über die aktuelle Version der AntiVir Personal Edition verfügen, haben wir Ihnen das Übertragen des Updates so einfach wie möglich gemacht.

18.1 Ein Update durchführen

Voraussetzung für ein Update ist, daß die AntiVir Personal Edition bereits einmal vollständig installiert wurde.

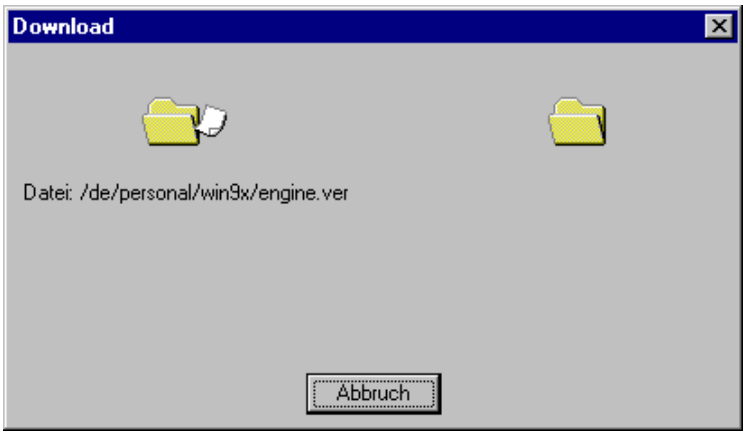
➔ Klicken Sie in der Symbolleiste des Hauptfensters der AntiVir Personal Edition auf die Schaltfläche 'Internet-Update'

Ist zu diesem Zeitpunkt keine DFÜ-Verbindung aktiviert, muß diese noch hergestellt werden. Dazu tragen Sie Ihren Benutzernamen und Ihr Kennwort an den entsprechenden Stellen ein und bestätigen diese Eingaben mit der Schaltfläche Verbindung herstellen:



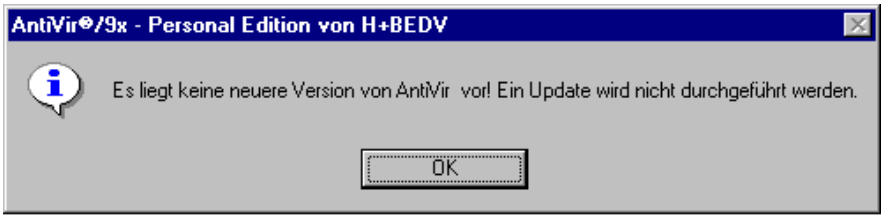
Ist die Verbindung hergestellt (oder waren Sie bereits online), erscheint in diesem Fenster die Meldung, daß Sie mit unserem Server (hier über ftp.free-av.com) verbunden sind:

War die Suche mit der Taschenlampe erfolgreich, wird dieses Fenster geschlossen und eine Datei mit dem Namen ENGINE.VER automatisch in einen temporären Ordner kopiert:



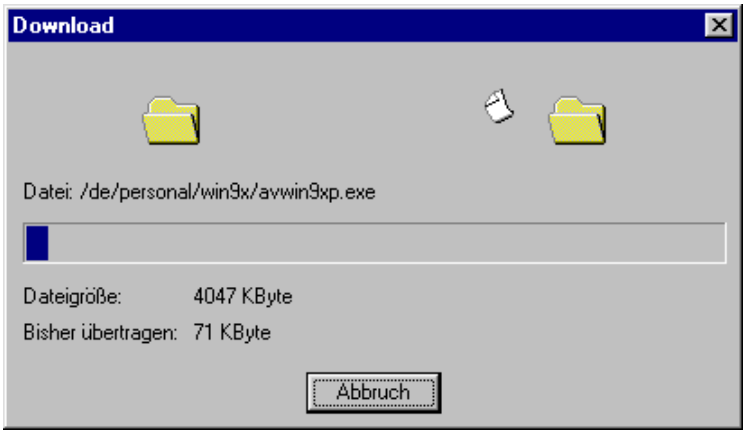
Mit Hilfe dieser Datei ENGINE.VER führt AntiVir automatisch ein Versionsabgleich durch.

Wird bei dem Versionsabgleich festgestellt, daß die Internet-Version unter ftp.free-av.com genauso aktuell wie die Dateien auf Ihrem Computersystem sind, erhalten Sie eine entsprechende Meldung:

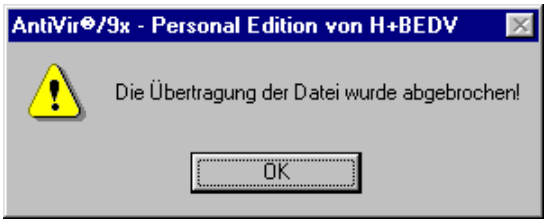


Bestätigen sie diese Meldung mit OK, wird die Datei ENGINE.VER aus dem temporären Ordner gelöscht und Sie haben nun die Gewißheit, mit der aktuellsten Version der AntiVir Personal Edition zu arbeiten.

Wird bei dem Versionsabgleich festgestellt, daß die AntiVir-Version im Internet aktueller als die auf Ihrer Festplatte installierten Version ist, wird die aktualisierte AntiVir-Programmdatei geladen:

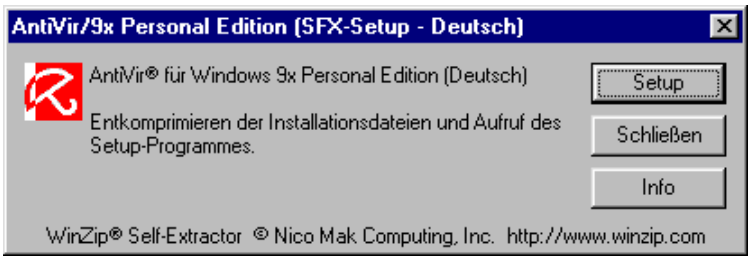


Wollen Sie zu diesem Zeitpunkt die aktuelle AntiVir-Version nicht laden, läßt sich der Download in diesem Fenster mit der Schaltfläche Abbruch beenden, die folgende Meldung muß dann mit OK bestätigt werden:



Brechen Sie an dieser Stelle ab, verbleibt eine alte Programmversion auf Ihrem Rechner, die Ihnen keinen zuverlässigen Schutz vor Computerviren bieten kann. Sie kehren dann unverrichteter Dinge zurück und die Datei ENGINE.VER im temporären Ordner wird gelöscht

Ist der Download-Vorgang erfolgreich abgeschlossen, erscheint automatisch das Fenster des SFX-Setup:



➔ Bestätigen Sie diese Meldung mit der Schaltfläche Setup, wird die Aktualisierung gestartet. Mit Schließen gelangen Sie unverrichteter Dinge zum Windows-Explorer zurück.

Wird die Aktualisierung mit Setup gestartet, werden zuerst die Programmdateien der entsprechenden Version von AntiVir (in diesem Beispiel die deutschsprachige Version der Personal Edition für Windows Me) entkomprimiert und in den Installationsordner der AntiVir Personal Edition kopiert:

Anschließend wird der InstallShield vorbereitet und das Setup-Programm gestartet. Sie brauchen ab jetzt nur noch der Benutzerführung zu folgen.

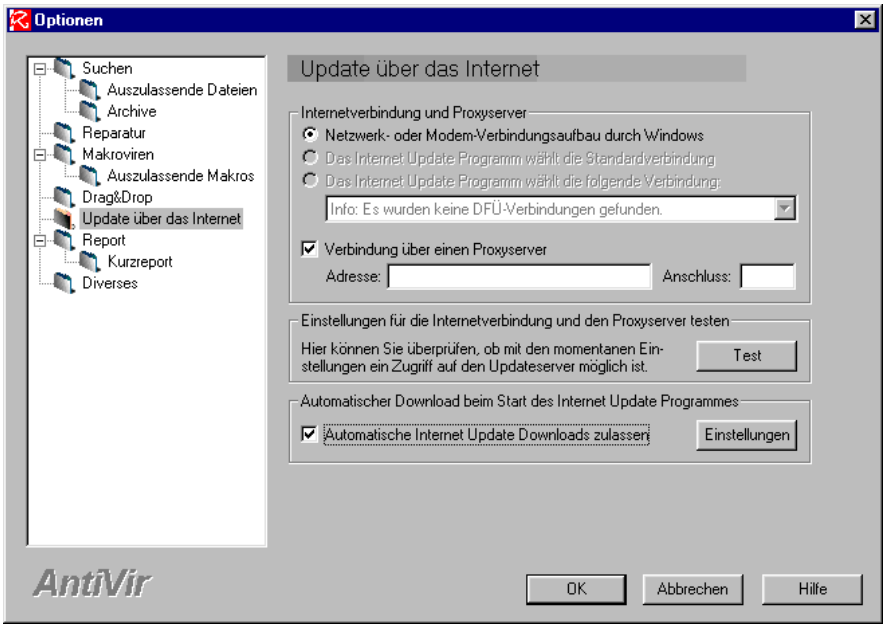
Oder Sie lesen die Einzelheiten zum Setup-Programm Schritt für Schritt im Kapitel 'AntiVir Personal Edition installieren' nach.

Beachten Sie, daß Ihnen die neue Version der AntiVir Personal Edition erst nach einem Neustart vollständig zur Verfügung steht (das betrifft in erster Linie den Virenwächter AVGuard).

18.2 Einstellungen für die Internetverbindung

Der Download kann auch über einen Proxy-Server abgewickelt werden, dies sorgt für eine wesentlich schnellere Übertragung beim Download.

➔ Rufen Sie das Fenster 'Optionen' mit der Schaltfläche Optionen auf und klicken im Auswahlfenster auf den Ordner ' Update über das Internet':



Die Anzeigegruppe '**Internetverbindung und Proxyserver**'

➔ Soll zum Datentransfer ein Proxy-Server verwendet werden, muß in den Optionen das entsprechende Kontrollkästchen markiert sein.

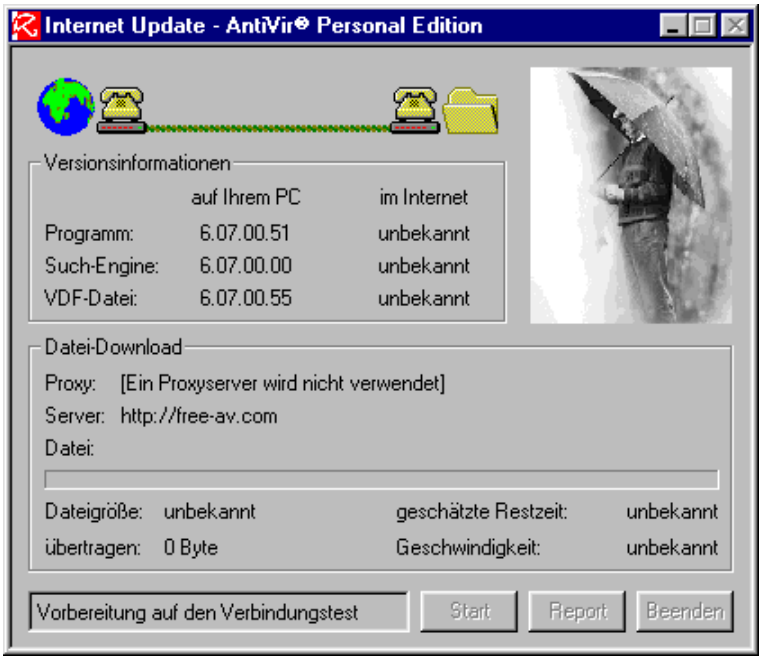
➔ Ist das Kontrollkästchen markiert, geben Sie im Feld 'Adresse' den vollständigen Namen desjenigen Proxy-Servers an, über den die Aktualisierung abgewickelt werden soll.

➔ Tragen Sie in das Feld 'Anschluß' die Anschlußnummer des verwendeten Proxy-Servers ein.

Haben Sie diese Informationen nicht zur Hand (z.B. in den Unterlagen, die Sie von Ihrem Internet-Provider erhalten haben), hilft Ihnen hier sicherlich der Provider Ihres Vertrauens weiter.

Die Anzeigegruppe '**Einstellungen für die Internetverbindung und den Proxyserver testen**'

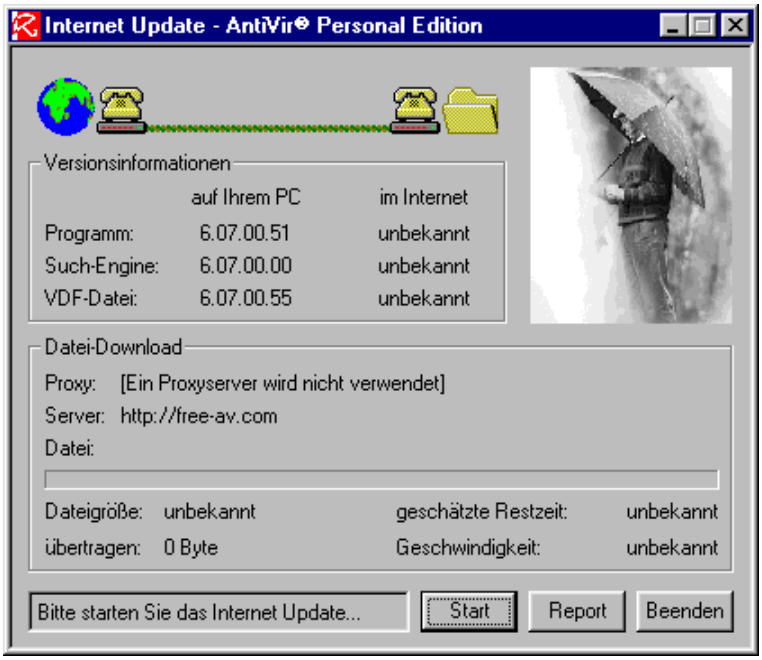
➔ Durch Anklicken der Schaltfläche Test können Sie prüfen, ob die Verbindung zum Server 'free-av' derzeit korrekt arbeitet. Es erscheint folgendes Fenster, in dem die wichtigsten Einstellungen dargestellt sind:



Kann eine Internetverbindung hergestellt werden, wird dies im nächsten Fenster gemeldet:

Lautet die Meldung, daß keine Verbindung hergestellt werden konnte, prüfen Sie bitte zuerst Ihre aktuelle Internetverbindung, vielleicht ist ja seit dem letzten Download von AntiVir etwas an der Verbindung verändert worden.

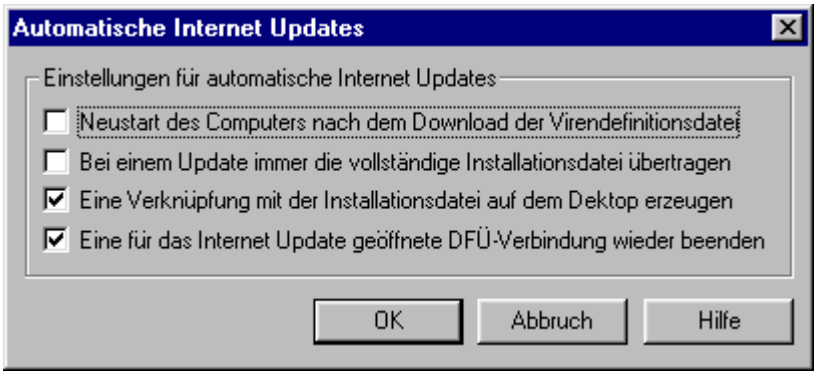
Ist das Kontrollfeld 'Automatische Internet-Update Downloads zulassen' aktiviert, wählt sich das AntiVir Internet Update automatisch ins Netz ein. Es wird das Fenster 'Internet Update – AntiVir® Personal Edition' aufgerufen:



➔ Wenn Sie überprüfen wollen, ob eine neue AntiVir-Version vorliegt, klicken Sie auf die Schaltfläche Start. Mit der Schaltfläche Beenden wird die Internetverbindung getrennt und Sie kehren unverrichteter Dinge wieder zurück zum Desktop.

Das automatische Internet Update funktioniert derzeit ausschließlich unter Standard-TCP/IP. Verwendet der Provider Ihrer Wahl ein anderes Protokoll, können beim automatischen Internet Update Probleme auftreten.

Ist das Kontrollfeld 'Automatische Internet-Update Downloads zulassen' markiert, gelangen Sie mit Hilfe der Schaltfläche Einstellungen in ein Fenster, in dem Sie die Voreinstellungen ändern können:



Behalten Sie die Voreinstellung bei, werden Sie über eine neue AntiVir-Version informiert und die DFÜ-Verbindung wird nach Übertragen der Informationen wieder geschlossen.

➔ Mit der Schaltfläche OK werden die Einstellungen übernommen, mit Abbruch kehren Sie wieder zurück zum Fenster 'Optionen/Update über das Internet'.

19 Der AntiVir Support Collector

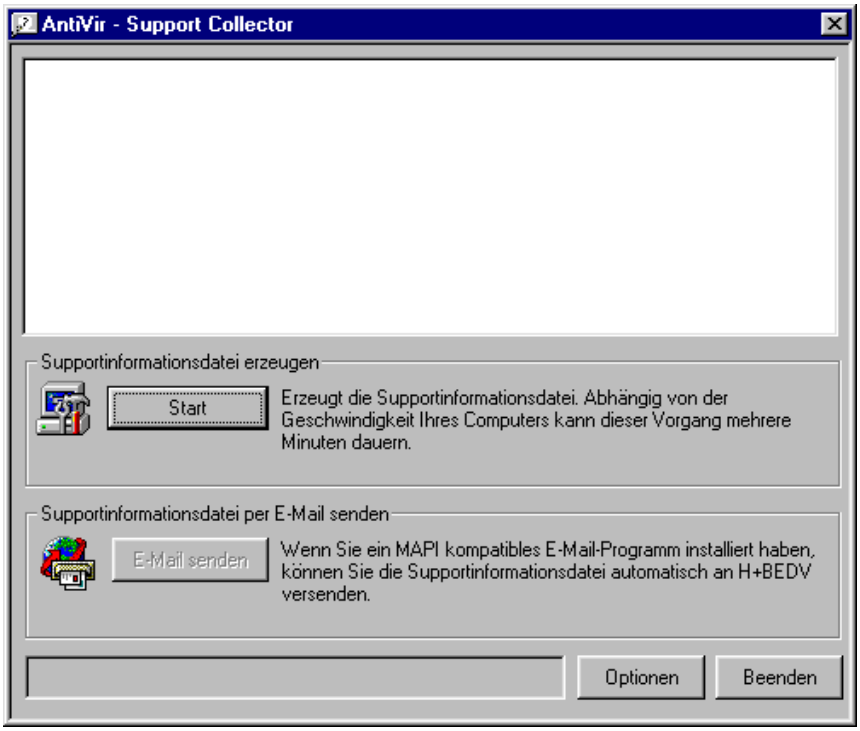
Getreu dem Motto "auch ein Sheriff braucht mal Hilfe" steht Ihnen für den Support der Weg über E-Mail zur Verfügung.

Für eine schnelle Bearbeitung einer Supportanfrage via E-Mail benötigen wir von Ihnen eine Datei mit wichtigen Systemdaten, die mit Hilfe des Support Collectors erstellt wird.

➔ Sie können den AntiVir Support Collector auf folgende Arten aufrufen:

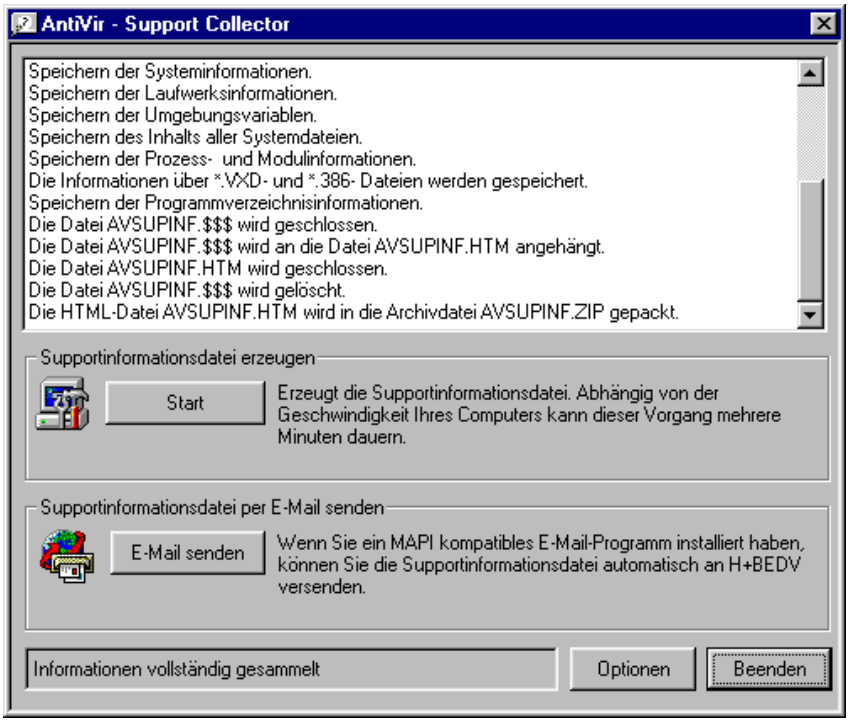
- in der Task-Leiste mit dem Button Start im Menü 'Programme' mit der Gruppe 'AntiVir/... – Personal Edition'
- in der Task-Leiste mit dem Button Start im Menü 'Ausführen'
- Per Windows-Explorer durch Aufruf des Programmes SUPPCOLL.EXE im AntiVir-Verzeichnis (per Default C:\PROGRAMME\AVPERSONAL)

Es erscheint dann dieses Fenster, mit dessen Hilfe Sie eine Datei mit allen notwendigen Supportinformationen erstellen können:

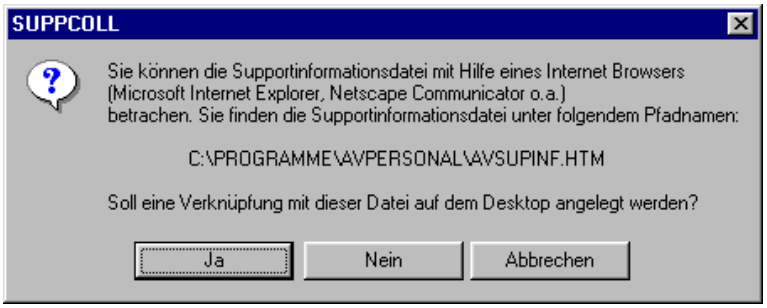


➔ Zum Erstellen einer Supportdatei klicken Sie auf die Schaltfläche Start.

Im Anzeigefeld können Sie sehen, welche Angaben gesammelt werden:



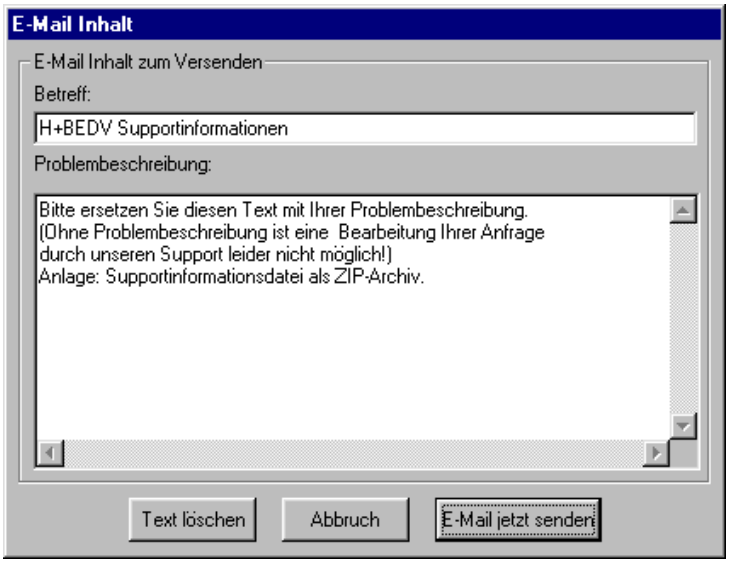
Ist dieser Vorgang abgeschlossen, erscheint dieses Fenster:



➔ Wenn Sie die Reportdatei sofort versenden möchten, benötigen Sie keine Verknüpfung mit dieser Datei auf dem Desktop. Schließen Sie dieses Fenster mit Nein.

➔ Soll die Protokolldatei erst später versandt werden oder wollen Sie den Inhalt der Datei in einem HTML-Browser lesen, läßt sich eine Verknüpfung mit dieser Datei auf dem Desktop anlegen. Sonst müssen Sie diese Datei erst wieder suchen (in der Regel wird sie unter dem Namen AVSUPINF.HTM im Programmverzeichnis von AntiVir abgelegt).

➔ Im Fenster 'AntiVir - Support Collector' können Sie mit Hilfe der Schaltfläche E-Mail versenden direkt eine E-Mail an H+BEDV schicken (Voraussetzung: MAPI-kompatibles E-Mail-Programm). Sie werden in diesem Fall im folgenden Fenster gebeten, den vorhandene Text durch einen eigenen Eintrag zu ersetzen:



Bitte tragen Sie hier soweit wie möglich Angaben zu folgenden Fragen ein:

- Welche Fehlermeldung wurde aufgerufen?
- Wurde eine Fehlernummer angezeigt?
- Beschreiben Sie bitte das Problem so exakt wie möglich!
- Welche Schritte bzw. Eingaben wurde vor dem Problem durchgeführt?
- Welche Schritte wurden bisher zur Problemlösung durchgeführt?
- Ist das Problem reproduzierbar? Wenn ja, wie?
- Weitere Informationen oder Besonderheiten.

➔ Haben Sie das Problem nach bestem Wissen und Gewissen beschrieben, senden Sie uns die E-Mail bitte durch Betätigen der Schaltfläche E-Mail jetzt senden zu.

20 Deinstallation

Für die Installation eines Updates brauchen Sie das "alte" AntiVir nicht deinstallieren.

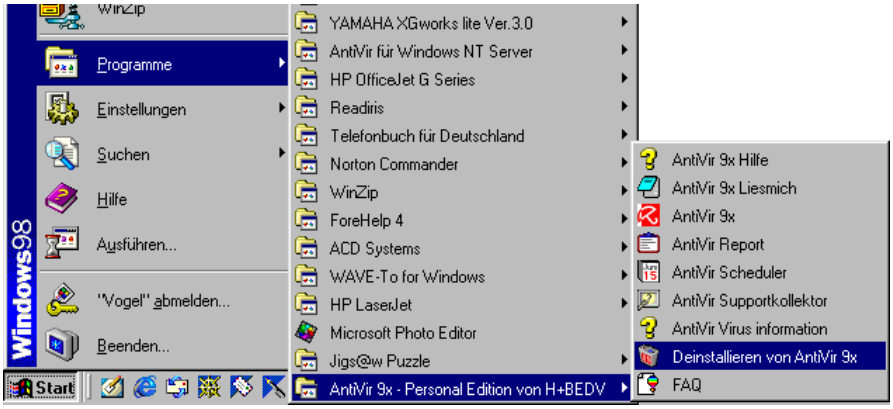
Verwenden Sie zum vollständigen Entfernen der AntiVir Personal Edition die AntiVir-Deinstallationsroutine, damit alle ausschließlich von AntiVir verwendeten .DLLs vollständig von Ihrem Rechner gelöscht werden.

➔ Beenden Sie AntiVir und alle dazugehörigen Anwendungen (besonders gerne werden der AntiVir Guard und der Scheduler vergessen ...).

➔ Klicken Sie auf die Schaltfläche Start in der Task-Leiste.

➔ Klicken Sie im Pop-Up-Menü auf die Zeile 'Programme'.

➔ Markieren Sie in dem Pop-Up-Menü mit den Programmordnern auf den Eintrag 'AntiVir** – Personal Edition von H+BEDV':



➔ Klicken Sie dort auf den Eintrag 'Deinstallieren von AntiVir **'.

Es erscheint ein Fenster, in dem folgende Gewissensfrage gestellt wird:

➔ Bestätigen Sie die Meldung mit Ja, wenn Sie AntiVir von Ihrer Festplatte löschen wollen. Mit Nein kehren Sie wieder unverrichteter Dinge zurück zum Desktop.

Wurde diese Meldung mit Ja bestätigt, gibt Ihnen das Informationsfenster des UninstallShield darüber Auskunft, was gerade geschieht:

Möglicherweise wird eine .DLL-Datei noch von anderen aktiven Anwendungen verwendet. In diesem Fall erhalten Sie bei der Deinstallation von AntiVir die Meldung, daß beispielsweise die Datei SYS_RW16.DLL nicht gelöscht werden konnte. Dies ist die sicherste Methode, auch diese Datei loszuwerden: Starten Sie Windows neu und löschen Sie mit Hilfe des Explorers das Verzeichnis AVWIN9X bzw. AVWINNT manuell.

21 Erste Hilfe

21.1 Bekanntermaßen gute DOS-Diskette erstellen

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 Ihr Rechnersystem 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 einmal 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 Betriebsystemprogramme und Treiber auf diese Diskette. z.B.:

FDISK.*	COMP.*	KEYB.*	FORMAT.*
LABEL.*	HIMEM.*	SYS.*	DISKCOPY.*
MSCDEX.*	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 zugehörendes Restore-Pendant und so etwas wie die Norton Utilities. Wenn nicht genügend Platz auf einer Diskette ist, können Sie diese Programme auf weiteren sauberen Hilfsmittel-Disketten unterbringen.

Zum guten Schluß schieben Sie bitte noch den Schreibschutzschieber auf 'schreibgeschützt' ('durchsichtig' bei einer 3 ½" Diskette) und bewahren Sie diese Diskette gut auf.

21.2 Bekanntermaßen gute Windows-Disketten

Mit dieser Diskette wird Windows wieder notdürftig zum Laufen gebracht. Der Aufwand zum Erstellen hat sich schon gelohnt, wenn Sie die Diskette nur ein mal nutzen müssen – Sie sparen gegebenenfalls eine Neuinstallation Ihrer Windows-Version und das Einrichten Ihrer Windows-Arbeitsumgebung.

Die Bedingung für die Erstellung einer bekanntermaßen guten Windows-Diskette ist ein absolut virenfreies System.

Sie können sich die 'bekanntermaßen gute DOS-Diskette' sogar sparen, wenn Sie die erste der Windows-Notfalldisketten als Systemdiskette anfertigen. Sie müssen aber wegen Platzmangel auf einige nette DOS-Befehle (z.B. XCOPY, KEYB) und Ihre liebgewonnenen Utilities (z.B. Norton Utilities) verzichten.

Haben Sie bei der Installation von Windows keine Startdiskette erstellt, können Sie dies auch nachträglich tun, dazu benötigen Sie Leerdisketten und die Windows-Originaldisketten bzw. die 'Windows CD-ROM'.

Doch Vorsicht: Voraussetzung für das Erstellen einer Startdiskette ist ein virenfreies System! Also nicht erst die Startdiskette erstellen, wenn das Kind schon in den Brunnen gefallen und Ihr System bereits infiziert ist.

➔ Rufen Sie unter 'Start/Einstellungen/Systemsteuerung' das Menü 'Software' auf.

➔ Wählen Sie dort die Registerkarte 'Startdisketten' aus und klicken auf die Schaltfläche Diskette erstellen.

➔ Befolgen Sie die Arbeitsschritte, die Ihnen das Installationsprogramm von Windows vorgibt.

➔ Zum guten Schluß schieben Sie bitte den Schreibschutzschieber auf 'schreibgeschützt' („ durchsichtig“ bei einer 3½" Diskette) und bewahren Sie diese Diskette gut auf.

Vorsicht ist geboten bei der SYSTEM.INI: Jeder Verweis auf eine Festplatte erhöht das Risiko, eine infizierte Datei aufzurufen, und in der SYSTEM.INI sind jede Menge davon enthalten. Sollte die Installation von AntiVir nach Start von der 'bekanntermaßen guten Windows-Diskette' fehlschlagen, läßt sich diese Datei auf das für ihre Systemkonfiguration richtige Maß zurechtstutzen (bitte erst nach Umbenennen der alten SYSTEM.INI). Diese Aktion ist recht aufwendig und sollte EDV-Spezialisten vorbehalten bleiben, da umfangreiche Eingriffe in die Windows-Umgebung stattfinden. Sie sollten in jedem Fall *vorher* versuchen, einen Virus mit dem Kommandozeilenscanner AVE32 bzw. AVNT oder mit AntiVir für DOS zu beseitigen.

➔ Booten Sie den Rechner von der 'bekanntermaßen guten Windows-Diskette',

Nun sollte Ihre Windows-Version mit allen notwendigen Hilfsprogrammen starten, die Sie zur Neuinstallation von AntiVir brauchen.

Wenn Sie AntiVir jetzt neu installieren, ist die Wahrscheinlichkeit gering (Ausnahme: residenter Bootsektorvirus ist aktiviert), daß die von AntiVir benötigten Hilfsprogramme (DLL-Dateien) infiziert sind. AntiVir kann seine Aufgabe ordnungsgemäß erfüllen.

22 Letzte Rettung

Sie haben einen Virus auf Ihrem Rechner und wollen diesen möglichst schnell wieder eliminieren. Im Normalfall gibt es nach einer gelungenen Installation Ihrer AntiVir-Version beim Erkennen und der Reparatur infizierter Dateien keine Probleme. Doch in wenigen Fällen, beispielsweise wenn sich ein Virus im Hauptspeicher eingenistet hat, kommen Sie nur noch auf den hier beschriebenen Wegen zu einem 'sauberen' Rechner. Beachten Sie in solch einem Fall unbedingt den folgenden Hinweis: Keine Panik! Denn ein zweibeiniger Virus richtet meist mehr Schaden an.

Führen Sie bitte keinen Warmstart, beispielsweise mit der 'finalen Geierkralle' (Strg+Alt+Entf) oder einem Boot-Programm aus, einige residente Viren können dies überleben. Stellen Sie auch sicher, daß sie nur Programme und Hilfsprogramme von den Notfall- bzw. Systemdisketten oder der bootfähigen AntiVir CD-ROM starten. Die Programme auf den Festplatten könnten bereits infiziert sein.

22.1 Start mit AntiVir® für DOS

Sie sollten das Computersystem nach dem Booten von der der 'bekanntermaßen guten DOS-Diskette' zuerst mit AVE32 bzw. AVNT überprüfen. Diese kommandozeilenorientierten Programme suchen nach Viren und können auch infizierte Dateien löschen oder reparieren – welche Aktionen diese Programme ausführen, hängt von den Kommandozeilenparametern ab, die Sie eingeben. Wollen Sie nur wissen, ob überhaupt Dateien mit einem Virus infiziert sind, ist dieses Programm die richtige Wahl. Zur Analyse des Computersystems reicht sogar eine Demoversion eines dieser Programme aus (Download unter www.antivir.de), diese können jedoch keine infizierten Dateien reparieren!

➔ Booten Sie von einer 'bekanntermaßen guten DOS-Diskette' oder von der AntiVir CD-ROM und bleiben bitte auch vorerst im DOS-Modus. Besitzen Sie keine Notfalldiskette, booten Sie bitte von der schreibgeschützten Original-DOS-Installationsdiskette (dann steht Ihnen nur die amerikanische Tastaturbelegung zur Verfügung. Beachten Sie bitte, daß sich dann der Backslash auf der Taste # befindet).

➔ Legen Sie – falls noch nicht geschehen – die AntiVir CD-ROM ein.

➔ Geben Sie den Laufwerksbuchstaben Ihres CD-ROM-Laufwerkes zusammen mit dem : ein.

Verweigert Ihr Computer den Zugriff auf das CD-ROM-Laufwerk Ihres Computers, müssen Sie den CD-ROM-Treiber von DOS und den Treiber des CD-ROM-Laufwerkes neu installieren: Starten Sie dazu die MSCDEX.EXE auf der 'bekanntermaßen guten DOS-Diskette' oder DOS-Originaldiskette und den Treiber von der zu Ihrem CD-ROM-Laufwerk gehörenden Diskette. Legen Sie dazu die Diskette mit den Treibern in das entsprechende Diskettenlaufwerk ein und rufen in dem Verzeichnis, auf dem sich der Treiber befindet, den Befehl 'MSCDEX.EXE' bzw. den zum CD-ROM-Laufwerk gehörenden Treiber mit dessen .EXE-Befehl auf.

➔ Rufen Sie die Datei AVE32.EXE (AVNT.EXE) mit folgender Befehlszeile auf (LW:\> steht für Ihr CD-ROM-Laufwerk):

LW:\> `[...]\PRODUCTS\CMDPROGS\AVE32\SETUP\AVE32.EXE -allhard` ↵

➔ Protokollieren Sie den Suchlauf: Notieren Sie, welche Dateien möglicherweise infiziert oder beschädigt sind. Benutzen Sie die Taste Pause, um den Suchlauf zu unterbrechen, mit ↵ wird die Suche fortgesetzt. Mit der Taste Esc brechen Sie den Suchlauf ab.

Wurden keine mit Viren infizierte Dateien gefunden, können Sie Ihre AntiVir-Version ohne Bedenken unter dem entsprechenden Betriebssystem installieren. Hat der Kommandozeilenscanner Viren gefunden, können diese infizierten Dateien in fast allen Fällen mit AntiVir® für DOS repariert werden. Setzen Sie dann die Virenentfernung wie im folgenden Abschnitt beschrieben fort:

➔ Wechseln Sie unter DOS auf Ihr CD-ROM-Laufwerk.

➔ Geben Sie anschließend bitte folgende Befehlszeile ein:

LW:\> `[...]\PRODUCTS\DOS\SETUP\INSTALL.EXE`

➔ Wollen Sie AntiVir® für DOS installieren, betätigen Sie eine beliebige Taste oder brechen Sie die Installation mit der Taste Esc ab.

➔ Wählen Sie mit den Tasten ↓ und ↑ aus, ob die Vollversion oder die Demoversion (ohne Lizenzdiskette) installiert werden soll. Achten Sie unbedingt auf die Auswahl des richtigen Laufwerksbuchstaben Ihres 3½" Diskettenlaufwerkes und bestätigen Sie Ihre Auswahl mit ↵.

➔ Wählen Sie mit den Tasten ↓ und ↑ das Laufwerk aus, auf dem AntiVir® für DOS installiert werden soll und bestätigen die Auswahl mit ↵. AntiVir schlägt die zuerst gefundene Festplatte vor, also meistens Laufwerk C:.

➔ In der Eingabezeile des anschließend erscheinenden Fensters können Sie ein Zielverzeichnis angeben, vorgeschlagen wird hier \ANTIVIR.

➔ Ist dieses Verzeichnis bereits angelegt und sind Dateien aus dem AntiVir Programmpaket vorhanden (z.B. bei einem Update), überschreibt AntiVir für DOS Dateien im Zielverzeichnis. Wollen Sie bestehende Dateien nicht überschreiben, brechen Sie die Installation hier mit der Taste [Esc] ab und wählen entweder ein anderes Zielverzeichnis oder kopieren die Dateien aus diesem Verzeichnis an eine andere Stelle.

Im nächsten Fenster können Sie beobachten, wie die Programmdateien in das Zielverzeichnis kopiert werden. Anschließend fragt AntiVir nach der Lizenzdiskette.

➔ Legen Sie Ihre Lizenzdiskette in Ihr 3½"-Diskettenlaufwerk ein und betätigen eine Taste. Wird keine Lizenzdatei gefunden, wird AntiVir als Demoversion installiert. Eine Reparatur ist dann nicht möglich!

➔ Abschließend erscheint ein Fenster mit Hinweisen auf Update-Angebote, das Sie durch Betätigen einer beliebigen Taste schließen können.

➔ Starten Sie einen Suchlauf in den Laufwerken bzw. Verzeichnissen, in denen AVE32 Virensignaturen entdeckt hat (oder nehmen Sie am besten gleich alles genau unter die Lupe).

➔ Wollen Sie ganz sicher gehen, daß auch wirklich alle Dateien durchsucht werden, können Sie noch einmal alle Dateien im erweiterten Modus überprüfen lassen. Rufen Sie dazu AntiVir® für DOS mit folgendem Kommandozeilenparameter auf:

```
[LW:\>]ANTIVIR /ALL
```

Sie können auch im Hauptfenster von AntiVir/DOS im Menü 'Einstellungen / Laufwerke' den Eintrag 'Alle Laufwerke' und unter 'Einstellungen / Suche' den Eintrag 'Alle Dateien' auswählen und mit [STRG]+[F2] eine Suche oder mit [STRG]+[F3] einen Reparaturlauf starten.

Es werden nun bei Programmstart der Hauptspeicher, alle Bootsektoren sowie alle Dateien in allen erreichbaren Laufwerken überprüft.

Wenn Sie unter DOS Probleme mit AntiVir haben: Versuchen Sie es mit der integrierten Hilfe (Aufruf: 'ANTIVIR /H' oder 'AVE32 /?'). Es werden alle Kommandozeilenparameter erklärt.

Eine Übersicht des Hauptfensters von AntiVir für DOS finden Sie in dieser Installationsanleitung, eine ausführlichere Erklärung finden Sie im entsprechenden PDF-Handbuch auf der CD-ROM.

22.2 Start mit temporärer Windows-Version und AntiVir

Dieses Kapitel wurde für den Fall geschrieben, daß AntiVir für Windows während der Installation wegen eines aktiven Virus streikt, sich also nicht vollständig installieren läßt. Wir schlagen die folgende Vorgehensweise vor (auch in der genannten Reihenfolge, zuerst mit weniger aufwendigen Versuchen, und wenn nichts mehr hilft, kommen Sie um eine Neuinstallation von Windows auf einem temporären Ordner nicht herum).

➔ Hat sich Ihr Computer bei dem Installationsversuch nicht vollständig aufgehängt (Sie können also noch unter der Windows-Oberfläche arbeiten), schalten Sie Ihren Rechner noch *nicht* aus!

➔ Schließen Sie alle Dateien und Programme (auch alle residenten Anwendungen wie beispielsweise einen aktivierten AntiVir Guard).

➔ Fertigen Sie ein *zusätzliches* Backup Ihrer Daten an (besser ein Backup mit Virus als gar keines oder eines mit museumsreifen Daten).

➔ Beenden Sie Windows und schalten Sie den Rechner für einige Sekunden aus.

Führen Sie bitte keinen Warmstart beispielsweise mit der 'finalen Geierkralle' Strg+Alt+Entf oder einem Boot-Programm aus, einige residente Viren können dies überleben.

Unter Windows Me,98 oder 95:

➔ Booten Sie Ihren Rechner von Ihrer 'bekanntermaßen guten DOS-Diskette', die Sie ja sicherlich angefertigt haben oder von der bootfähigen AntiVir CD-ROM.

➔ Versuchen Sie, den Virus mit AntiVir für DOS zu beseitigen (wie dies geht, steht im Kapitel 'Start mit AntiVir für DOS' ab Seite 141).

Unter Windows 2000 oder NT:

➔ Booten Sie Ihren Rechner von Ihrer 'bekanntermaßen guten Windows-Diskette' bzw. von der Windows-Startdiskette.

➔ Versuchen Sie jetzt, AntiVir/NT erneut zu installieren. Haben Sie dabei Erfolg, wurde beim Start von Windows vermutlich keine infizierte Datei aktiviert. Prüfen Sie anschließend noch einmal alle erreichbaren Festplatten mit der Funktion 'Alle Dateien' (im Menü 'Optionen/Suche' von AntiVir in der Anzeigegruppe 'Dateien').

Bricht AntiVir den zweiten Installationsversuch ebenfalls ab, ist sehr wahrscheinlich eine Windows-Systemdatei infiziert. In diesem Fall sollten Sie das Programm AVNT einsetzen (unter Windows NT das Gegenstück zum Kommandozeilenscanner AVE32). Eine Beschreibung des Programmes und der Parameter finden Sie ab Seite 32.

Sind Sie nach diesem Versuch die digitalen Plagegeister immer noch nicht losgeworden, kommen Sie um die Installation einer 'abgespeckten' Windows-Version in einem temporären Ordner nicht herum.

Jetzt fragen Sie sich, weshalb wird nicht das gesamte Windows-Paket neu installiert? Hier ist die Gegenfrage: wollen Sie Ihre Windows-Umgebung tatsächlich neu einrichten und gegebenenfalls Ihre Programme neu installieren? Denn mit einem Trick haben Sie die Chance, Ihre gewohnte Windows-Umgebung zu retten.

➔ Falls noch nicht geschehen, booten Sie den Rechner von Ihrer 'bekanntermaßen guten Windows-Diskette' bzw. Windows-Startdiskette.

➔ Benennen Sie die Datei SYSTEM.INI im Ordner WINDOWS um, beispielsweise in SYSTEM.VIR (verwenden Sie dabei bitte keine gängigen Erweiterungen von Programmen oder Dokumenten und schreiben Sie sich den neuen Namen sicherheitshalber auf). Sonst startet Windows zuerst die alte, infizierte Version – und das Theater hätte wir auch leichter haben können. Damit der alte Windows-Ordner nicht von der neuen Windows-Version gefunden wird, können Sie den auch umbenennen, beispielsweise in 'WINOLD'.

➔ Legen Sie einen temporären Ordner auf der Festplatte an, beispielsweise \TEMPWIN auf dem Laufwerk C: (dieser Schritt ist hier nicht zwingend erforderlich; Sie müssen sonst dem Ordner, in den das temporäre Windows installiert werden soll, einen anderen Namen geben).

➔ 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).

Sie benötigen nicht die Standardinstallation, die schleppt eine Menge für unseren Zweck überflüssige Programme mit. Sie müssen also beim Setup 'Benutzerdefiniert' angeben und in diesem Menü des Windows-Setup die Option 'Minimiert' auswählen oder selbst unnötige Teile abwählen.

➔ Starten Sie Windows neu, sobald Sie vom Setup-Programm dazu aufgefordert werden.

Hat alles funktioniert, sollte Windows mit einem neuen – nicht mit der gewohnten, von Ihnen eingerichteten – Desktop starten.

Stellen Sie sicher, daß Windows aus diesem Ordner heraus startet. Ihre Programme auf der Festplatte – und damit auch Ihre Windows-Version – könnten von einem Virus infiziert sein.

➔ Installieren Sie AntiVir für Windows von der aktuellen CD-ROM neu.

Nur wenn AntiVir für Windows neu installiert wird, haben Sie Gewißheit, daß die benötigten Hilfsprogramme (DLL-Dateien) nicht infiziert sind und AntiVir seine Aufgabe ordnungsgemäß erfüllen kann.

Verweigert Ihr Computer den Zugriff auf Ihr CD-ROM-Laufwerk, müssen Sie den CD-ROM-Treiber von Windows und ggf. den Treiber Ihres CD-ROM-Laufwerkes neu installieren.

➔ Folgen Sie bei der Installation der Benutzerführung und bestätigen Sie bei der Installation die Abfrage, ob ein Viren-Suchlauf gestartet werden soll, *auf jeden Fall* mit Ja.

Gelingt die Installation nicht, hilft nach einer Prüfung, ob Windows aus dem richtigen Verzeichnis heraus gestartet wurde, nur ein zweiter Versuch und wenn dieser scheitert, ein Anruf bei unserer Hotline.

Ist die Installation von AntiVir erfolgreich, empfehlen wir, auch alle Daten auf allen Laufwerken und Wechselmedien (sprich Disketten, Zip- oder MO-Laufwerke, CD-R, CD-RW, usw.) sowie auch auf dem aktuellen Backup zu prüfen. Dazu wählen Sie im Menü 'Optionen' unter 'Suchen' in der Anzeigegruppe 'Dateien' den Modus 'Alle Dateien' aus. Das kostet zwar Zeit, schützt aber vor Reinfektionen.

➔ Unter dem Menüpunkt 'Optionen/Reparatur' können Sie auswählen, ob Sie sich die Reparatur jeder infizierten Datei bestätigen lassen wollen (da quälen Sie manchmal die Maus durch die andauernde Klickerei) oder nicht bestätigen lassen wollen (geht schneller, aber manchmal will man direkt am Bildschirm sehen, was da so repariert wird).

➔ Starten Sie einen Suchlauf durch Anklicken der Schaltfläche Suchen.

➔ Rufen Sie nach dem Ende des Suchlaufes die Reportdatei entweder mit der Schaltfläche Report oder über 'Report/Anzeigen' auf.

➔ Sehen Sie in der Reportdatei nach, ob alle Viren entfernt wurden oder ob sich einige Dateien nicht reparieren ließen.

Wurden alle Dateien erfolgreich repariert und zerstörte Dateien gelöscht, befinden sich keine bekannten Viren auf Ihrem Rechner.

Haben Sie zerstörte Dateien nicht gelöscht, kann ein Virus beim Aufruf dieser Datei – wenn diese noch lauffähig ist – aktiviert werden und sich erneut verbreiten. Behandeln Sie diese Dateien mit äußerster Vorsicht. Löschen Sie diese Dateien auf jeden Fall und kopieren bzw. installieren Sie die Dateien von den Originaldisketten oder einem virenfreien Backup neu auf die Festplatte.

Jetzt hätten Sie sicherlich gerne Ihre alte Windows-Version zurück. Das verstehen wir gut, da Sie wahrscheinlich viel Schweiß und Tränen bei der Einrichtung der Windows-Umgebung aufgebracht haben (es heißt ja auch unter Systemadministratoren 'Plug & Pray').

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 umtaufen. 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 restlos entfernen oder während des Setups die Option 'Nur neue Dateien' im Konfigurationsfenster abwählen. Denken Sie auch daran, daß Sie in jedem Fall Ihre Lizenzdiskette benötigen).

23 Häufig gestellte Fragen

Die HTML-Datei 'FAQ'

Weitere aktuelle Fragen werden in der eigens dafür bereitgestellten **HTML-Datei 'FAQ'** beantwortet. Wir empfehlen, bei Schwierigkeiten mit der AntiVir Personal Edition zuerst einen Blick in diese Datei zu werfen, bei vielen Problemen ist die Lösung eines Problemes bereits hier beschrieben.

➔ Klicken Sie auf die Schaltfläche Start in der Task-Leiste.

➔ Klicken Sie im Pop-Up-Menü auf die Zeile 'Programme'.

➔ Markieren Sie in dem Pop-Up-Menü mit den Programmordnern auf den Eintrag 'AntiVir** - Personal Edition von H+BEDV'

➔ Klicken Sie dort auf den Eintrag 'FAQ'.

Jetzt wird Ihr HTML-Browser gestartet und die Datei mit den aktuellen 'häufig gestellten Fragen' angezeigt.

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 den Blinkern und dem Licht. Täglich ein Standard-Suchlauf über die Festplatte. Es werden auf der Festplatte ausführbare Programmdateien (.COM, .EXE etc.) untersucht. Dies ist in etwa dem Ölwechsel gleichzusetzen. Die Inspektion im wöchentlichen Rhythmus etwa könnte diese Prüfung sein: die ausführbaren Programmdateien werden komplett durchsucht. 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 ja schon von selbst. Und falls Sie immer den Licht- und Blinkertest vor dem Start machen, können Sie ja 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 berühmtberüchtigten 'bekanntermaßen guten DOS-Diskette'. Starten Sie Windows mit Hilfe der 'bekanntermaßen guten Windows-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, lassen Sie bitte die ganze Festplatte durch AntiVir mit seinen Standardoptionen (nur Programmdateien) durchsuchen und reparieren. Kontrollieren Sie den Datenträger anschließend im Suchmodus (nicht reparieren) mit 'Alle Dateien'. Falls AntiVir jetzt noch auf Viren stößt, können dies Viren sein, müssen es aber nicht.

Beim dritten Schritt werden Sie besonders gefordert: 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 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.

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 Einstellungen '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.

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 Antivi-

ren-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 Rechnersystemes 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' oder einer 'bekanntermaßen guten Windows-Startdiskette' gebootet 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 Startvorganges wurde während des Abarbeitens der Dateien CONFIG.SYS bzw. AUTOEXEC.BAT auf 'C:' zugegriffen. Dieser Zugriff kann ein DIR C: oder ein Laden eines Programmes 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 Startvorganges Ihres Rechnersystemes die linke Shift-Taste. Ein Laden der Kompressionstreiber unterbleibt dann ebenso wie ein Abarbeiten einer CONFIG.SYS bzw. AUTOEXEC.BAT.

24 Support

Wir weisen hier besonders gerne auf vier Hilfsmittel hin:

- Dieses **Handbuch** hat ein Stichwortverzeichnis, mit dessen Hilfe Sie sich leicht zurechtfinden können.
- Die Datei **LIESMICH.WRI** bietet aktuelle, wichtige Informationen, daher legen wir Ihnen diese Datei wärmstens ans Herz.
- Auch die **FAQ** werden ständig ergänzt, so daß Sie hier auch Antworten auf häufig gestellte Fragen erhalten.

  Klicken Sie auf die Schaltfläche Start in der Task-Leiste. Dort finden Sie im Pop-Up-Menü 'Programme / AntiVir - Personal Edition von H+BEDV ' auch den Eintrag 'FAQ'. Durch Anklikken dieses Eintrages wird Ihr HTML-Browser gestartet und die Datei mit den aktuellen 'häufig gestellten Fragen' angezeigt.
- Das **Support-Forum** steht allen Usern der Personal Edition zur Verfügung. Dort können Sie Fragen stellen oder auch anderen Menschen beim Umgang mit der Personal Edition zur Seite stehen. Selbstverständlich sehen wir auch regelmäßig dieses Forum durch, um Verbesserungsvorschläge in unsere Software einfließen zu lassen.

Der **Support** für die kostenfreie AntiVir Personal Edition wird **ausschließlich über E-Mail** abgewickelt.

Für eine schnelle Bearbeitung einer Supportanfrage via E-Mail benötigen wir von Ihnen eine Datei mit wichtigen Systemdaten, die mit Hilfe des Support Collectors erstellt wird. Näheres dazu erfahren Sie ab Seite 133.

Falls Sie mit AntiVir Probleme oder Schwierigkeiten haben, können Sie uns auch eine "formlose" E-Mail senden an:

support@free-av.com	Support für kostenfreie AntiVir Personal Edition
virus@antivir.de	an diese Adresse senden Sie bitte Viren, die ggf. nicht erkannt werden oder entfernen lassen, als gepacktes Attachment (z.B. ZIP, ARJ).

Bitte haben Sie Verständnis, falls es bei dieser kostenfreien Version von AntiVir etwas länger dauert, bis Ihre Anfragen beantwortet werden.

Wenn Sie den Support Collector nicht nutzen, benötigen wir auf jeden Fall folgende Informationen, um Ihrer Nachfrage bearbeiten zu können:

- ✘ Hersteller, Fabrikat und Ausstattung Ihres Rechnersystemes
- ✘ Die Windows-Version (bitte bis zur letzten Stelle hinter dem Komma)
- ✘ Die Versionsnummer und das Datum Ihres AntiVir-Programmes.
- ✘ So viele Informationen wie möglich über das aufgetretene Problem.

Bitte beantworten Sie auch folgende Fragen soweit wie möglich:

- Welche Fehlermeldung wurde aufgerufen?
- Wurde eine Fehlernummer angezeigt?
- Beschreiben Sie bitte das Problem so exakt wie möglich!
- Welche Schritte bzw. Eingaben wurde vor dem Problem durchgeführt?
- Welche Schritte wurden bisher zur Problemlösung durchgeführt?
- Ist das Problem reproduzierbar? Wenn ja, wie?
- Weitere Informationen oder Besonderheiten.

Die AntiVir Professional Edition

Für den kommerziellen und geschäftlichen Einsatz finden Sie in unserer AntiVir Professional Edition auch für Ihre Anforderungen ein zuverlässiges und flexibles Antiviren-Programm. Sie finden hier Workstation- und Server-Produkte für verschiedene Betriebssysteme (Workstations: DOS, Windows Me/98/95, Windows 2000/NT, OS/2; Server: Windows NT, Novell NetWare, Linux, FreeBSD und OpenBSD), und Virenscanner für Mail-Programme (MS Exchange, Outlook und Messaging, Eudora sowie Exchange Server). Und das alles von Einzelplatz-Versionen über Mehrfach-Lizenzen bis hin zu Company-Lizenzen.

Informationen zu dieser Produktpalette erhalten Sie auf der H+BEDV Homepage www.antivir.com oder www.hbedv.com oder fordern Sie unser Informationsmaterial unter folgender Adresse an:

H+BEDV Datentechnik GmbH	Tel.: 07542-93040
Lindauer Straße 21	Fax: 07542-52510
D-88069 Tettnang	E-Mail: info@antivir.de

Sicherheit durch den Fast Update-Service

Aufgrund der immer wieder neu in Umlauf gebrachten Viren wurde für die Programmpakete der AntiVir® Professional Edition der Fast Update-Service geschaffen, um AntiVir-Anwender regelmäßig bei der Virenerkennung auf dem Laufenden zu halten. Dieser Service garantiert, daß Sie immer ein Antiviren-Programm haben, das auch die Viren erkennen kann, die seit der vorherigen Programmversion aufgenommen wurden.

Aktualität heißt Sicherheit. Damit Sie immer die Gewißheit haben, mit einer aktuellen Version von AntiVir für Linux zu arbeiten, bieten wir Ihnen zwei unterschiedliche Aktualisierungsstufen an.

Je nach Sicherheitsstufe können Sie wählen zwischen dem zweimonatlichen Fast Update-Service (FUSE 6 = **F**ast **U**pdate-**Se**rvice mit **6** Updates für ein Jahr) und dem wöchentlichen Fast Update-Service (FUSE 6/wi = **F**ast **U**pdate-**Se**rvice mit **6** Updates plus **w**eiterer Updates per **I**nternet für ein Jahr). Die Zwischenupdates des FUSE 6/wi erscheinen in der Regel wöchentlich. Alle Updates können Sie über unsere Mailbox bzw. unseren Internet-Server abrufen. Als registriertem Anwender senden wir Ihnen zusätzlich die zweimonatlichen Updates während eines laufenden Update-Service automatisch per Post zu.

Fragen zum Vertrieb (Update-Service, Lizenzerweiterung, Informationen zu weiterer Antiviren-Software von H+BEDV) können Sie uns auch per E-Mail zusenden, und zwar einfach an:

– vertrieb@antivir.de

Index

/

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z