PEARSON Education

Markt+Technik

Leichter Einstieg für Senioren

Sicherheit für Windows XP

GÜNTER BORN

Markt+Technik

Virenschutz von A bis Z

Viren und Trojaner gehören mit zu den größten Bedrohungen für Computerbenutzer. Schnell hat man sich einen solchen Schädling beim Surfen im Internet, im Anhang einer E-Mail oder von CD/Diskette über ein infiziertes Programm geholt. Schutz bieten Virenscanner, also Programme, die den Computer überwachen und Alarm schlagen, wenn ein Virus auf dem Rechner erkannt wird. Zudem können diese Virenschutzprogramme oft auch einen virenbefallenen PC von diesen Schädlingen säubern. In diesem Kapitel erwerben Sie das Wissen rund um das Thema Viren, Trojaner, Würmer etc. und erfahren, wie Virenschutzprogramme konkret eingesetzt werden.

Das lernen Sie in diesem Kapitel

- Grundwissen zu Viren & Co.
- Das Vexira-Notfallset
- Arbeiten mit AntiVir

3

Grundwissen zu Viren & Co.

In Kapitel 1 finden Sie einen kurzen Überblick über die Gefahren, die durch Viren, Würmer und Trojaner drohen. Als Computerbenutzer sollte es also Ihr Ziel sein, keinen dieser Schädlinge ins System einzuschleppen. Der folgende Abschnitt vermittelt Ihnen nützliches Zusatzwissen über Varianten von Viren, Infektionswege und mehr.

Wie kann ich Viren einschleppen?

Wer mit Grippe seinen Computer anhustet, verteilt vielleicht viele Grippeviren. Der Rechner wird davon aber natürlich nicht infiziert. Wenn hier die Rede von Viren (oder Würmern bzw. Trojanern) ist, sind Computerprogramme gemeint, die Schäden an Ihrem Rechner anrichten können. Das Tückische an diesen Schädlingen ist, dass sie sich hinter anderen Funktionen (z. B. in sinnvollen Programmen, in Dokumenten, Webseiten etc.) verstecken können und die schädigenden Funktionen eventuell erst an einem ganz bestimmten Datum wirksam werden. Computerviren (und andere Schädlinge) lassen sich auf unterschiedlichem Weg realisieren:

- **Programmviren** können in Programmdateien (*.exe*, *.com*) sowie in Dateien mit Erweiterungen wie *.pif* (Konfigurationsdatei für DOS-Anwendungen) oder *.scr* (Bildschirmschoner) enthalten sein bzw. über diese aktiviert werden.
- **Bootviren** sind eine besondere Form von Programmviren, die sich in den Startbereich von Festplatten oder Disketten einnisten. In diesem Bereich befinden sich normalerweise die Startroutinen des Betriebssystems, mit denen der Computer hochgefahren wird. Befindet sich dort ein Virus, übernimmt dieses bereits vor dem Start des Betriebssystems die Kontrolle über den Computer und kann z. B. Virenschutzprogramme abschalten oder (bei Disketten) weitere Laufwerke infizieren.
- **Makroviren** stecken in Dokumentdateien und werden beim Laden dieses Dokuments über den Makrocode ausgeführt. Solche Makro-

viren können in Dokumenten von Microsoft Office (Word: *.doc*-Dateien, Excel: *.xls*-Dateien etc.), von OpenOffice.org bzw. StarOffice (Writer: *.swx*-Dateien, Calc: *.scx*-Dateien etc.) verborgen sein. Aber auch in Dokumenten im *.pdf*-Format (Adobe Acrobat) oder im Macromedia Flash-Format (*.swf*) lassen sich Viren unterbringen.

- **Scriptviren** benutzen Scriptprogramme (*.vbs*, *.vbe*, *.js*, *.jse*, *.wsf*, *.php* etc.), Stapelverarbeitungsprogramme (*.bat*, *.cmd*) oder simple HTML-Dokumente (*.hta*, *.htm*, *.html*), um den Computer anzugreifen. Es reicht dann ggf., eine Internetseite aufzurufen oder eine im HTML-Format empfangene E-Mail zu öffnen, um das Virus zu aktivieren.

  Es reicht also, wenn Sie eine dieser Dateien öffnen. Das infizierte Programm oder die schädlichen Makros werden ohne entsprechende Schutzvorkehrungen sofort beim Öffnen der Datei ausgeführt. Anschließend wird das Schadprogramm im Hintergrund wirksam und beginnt im günstigsten Fall mit dem Löschen oder Verändern von Dateien. Viren kopieren ihren Programmcode zusätzlich in nicht befallene Dateien (so verbreitet sich das Virus über viele Programmdateien). Geben Sie eine solche Datei (z. B. per E-Mail-Anhang, auf Diskette oder auch auf einer selbstgebrannten CD) weiter, kann das Virus andere Computer infizieren.

  Manche Viren, Trojaner oder andere Schädlinge lesen das Adressbuch des lokalen Benutzers aus und versuchen sich als E-Mail-Anhang an möglichst viele andere Benutzer zu verschicken. Dies ist auch der Grund, warum Sie plötzlich virenverseuchte E-Mails von guten Bekannten bekommen können.

HINWEIS

Wenn in diesem Kapitel vorzugsweise von Viren die Rede ist, gilt das Gesagte natürlich auch für Trojaner und teilweise auch für Würmer. Diese Schädlinge nutzen ähnliche Mechanismen zur Verbreitung und haben das Bestreben, sich möglichst weit zu verbreiten. Die **Unterscheidung** in **Viren**, **Trojaner** und **Würmer** ist üblich, **um** deren **Wirkungsweise klassifizieren zu können**. Ein Virus hat primär das Ziel, Schäden (z. B. durch Löschen von Dateien) auf dem infizierten Compu-

ter anzurichten. Ein Trojaner versucht dagegen unbemerkt zu bleiben, um das System heimlich auszuspionieren oder als Tor für andere Schadprogramme zu dienen. Würmer haben typischerweise keine Schadroutinen und spionieren auch nicht den Wirtsrechner aus. Würmer nutzen häufig Sicherheitslücken in Windows zur Verbreitung aus. Ein Ziel von Würmern ist es, so genannte Hintertüren (Backdoors) auf dem befallenen Rechner einzurichten, über die Dritte dann Zugriff auf das System erhalten. Das Hauptziel von Würmern ist es aber, Internetserver durch ständige Nachrichtenanfragen anzugreifen. Erfolgt dies durch viele Millionen infizierte Rechner, wird der Internetserver durch diese Anfragen für normale Benutzer quasi blockiert (dies wird auch als Denial of Service oder kurz DoS-Attacke bezeichnet). Mittlerweile gibt es auch Würmer, die zusätzliche Schadroutinen wie Viren enthalten. Wenn also nachfolgend Virenschutzprogramme vorgestellt werden, können diese auch die meisten Trojaner, Würmer und sogar Dialer erkennen bzw. beseitigen. Die nachfolgend beschriebenen Schutzmaßnahmen beziehen sich daher auf alle diese Schädlinge.

Neben den klassischen Viren gibt es noch so genannte Trojanische Pferde (Trojaner), die sich unbemerkt irgendwo im System einnisten und den Inhalt der Festplatte, die Surfgewohnheiten, Kennwörter, Bank- bzw. Kreditkartendaten etc. ausspionieren oder die Tastatur auf Eingaben überwachen und per Internet an ihre Urheber melden.

Eingenistete Trojaner verursachen häufig zusätzliche Sicherheitslücken im System, über die sich weitere Schadprogramme einschleusen lassen. So wird ein Großteil des Werbemülls im Internet über infizierte Computer normaler Benutzer verschickt. Der ahnungslose Benutzer stellt also seinen Rechner für solchen Missbrauch zur Verfügung, zahlt nebenbei auch noch für die Internetkosten und bekommt im schlimmsten Fall noch Ärger, wenn sein PC als Quelle dieser Massen-E-Mails identifiziert wird.

TIPP

Die Internetseite *www.trojaner-info.de* enthält eine gute Übersicht über bekannte Trojaner, deren Beseitigung und mehr.

Zudem benutzen manche Webseiten aktive Module (so genannte Java-Applets oder ActiveX-Controls). Beim ersten Aufruf der Seite werden diese Zusatzmodule auf den lokalen Computer heruntergeladen. Ruft der Benutzer die betreffende Webseite später erneut auf, kann diese auf den Programmcode in den Java-Applets oder in den ActiveX-Controls zugreifen. Eigentlich ist dies eine tolle Sache, die Windows-Update-Funktion ist beispielsweise als ActiveX realisiert. Allerdings könnten auf obskuren Webseiten auch Java-Applets oder ActiveX-Controls lauern, die Viren oder Trojaner enthalten. Wie Sie auf so etwas reagieren, wird in Kapitel 4 beschrieben.

FACHWORT

Was sind Hoaxes?

Zu allem Überfluss gibt es neben Viren, Würmern und Trojanern noch Hoaxes, die von mehr oder weniger wohlmeinenden Zeitgenossen verbreitet werden. Ein Hoax ist eine Falschmeldung über ein angebliches Virus, die von irgendeiner Person in die Welt gesetzt wird. Oft wird ein Sachverhalt beschrieben, der auf den ersten Blick zutrifft. Man erfährt, dass eine Datei mit dem Namen *xyz* im Verzeichnis *abc* bei einer Vireninfektion zu finden sei. Die Datei ist natürlich vorhanden, enthält aber kein Virus, sondern kann sogar für den korrekten Betrieb des Systems wichtig sein. Im Hoax wird dann vor der angeblichen Gefahr gewarnt. Man findet ggf. Hinweise, wie die befallene Datei zu löschen ist, und wird gebeten, die betreffende Meldung mit der Warnung an möglichst viele Bekannte weiterzugeben. Nach dem Prinzip eines Kettenbriefs verbreitet sich so eine Meldung oft millionenfach per E-Mail und löst ziemliche Verwirrung aus. Wichtig ist also, nicht auf einen derartigen Schwindel hereinzufallen. Die Seite *www.hoax-info.de* enthält eine sehr gute Übersicht über das Thema Hoax-Meldungen und Kettenbriefe. Falls Sie also eine Virenwarnung erhalten, schauen Sie ggf. dort nach, ob diese als Hoax bekannt ist.

Wo kann ich Viren einschleppen?

Fragen Sie sich, wie Sie an solche »gefährlichen« Sachen wie Viren, Würmer und Trojaner geraten? Hier einige der Möglichkeiten zum Angriff auf Ihren Computer:

- Viren und Trojaner können Sie sich z. B. per Internet einfangen, wenn Sie Programme herunterladen und dann auf dem Rechner ausführen. Das Gleiche gilt bei der Übernahme ungeprüfter Dateien von Disketten/Datenträgern, die Sie von Dritten erhalten.
- Die zweite Quelle für solche »Schädlinge« sind E-Mails mit angehängten Dateien und Programmen. Öffnet der Benutzer einen solchen Anhang, wird das Programm samt Virus ausgeführt.

  Ähnliches gilt auch für Dokumentdateien, die Makro- oder Scriptviren enthalten können. Bei Webseiten genügt es bereits, diese im Browser aufzurufen, damit das Virus eventuell aktiv werden kann.

  Würmer oder andere Schädlinge können auch über Sicherheitslücken im Betriebssystem eingeschleust werden, wenn der Computer online ist. Abhilfe schaffen die regelmäßige Aktualisierung von Windows XP (siehe Kapitel 2) sowie der Einsatz von Sperrfunktionen (wie Firewalls, siehe Kapitel 6).

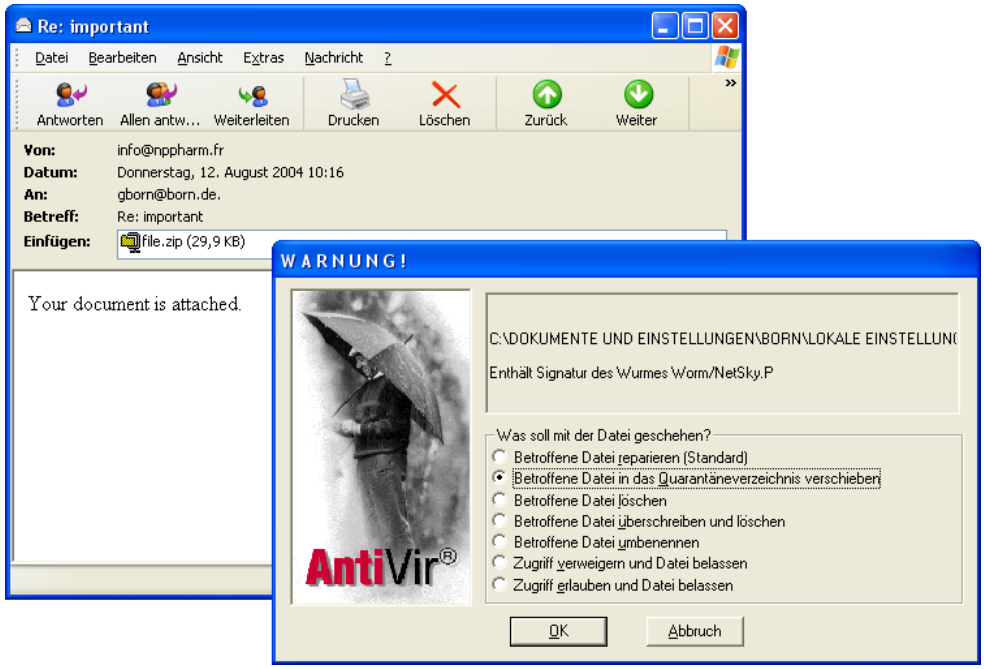
  Nun die gute Nachricht: Die Virengefahr ist begrenzt, Schäden werden in der Regel nur durch allzu große Sorglosigkeit oder Fahrlässigkeit der Benutzer verursacht. Mit ein paar Verhaltensregeln lässt sich die Gefahr fast auf null reduzieren:

- Melden Sie sich zum **Arbeiten mit** Windows über **ein normales Benutzerkonto** mit eingeschränkten Rechten an (siehe Kapitel 2). Fangen Sie sich dann trotz der nachfolgenden Vorsichtsmaßnahmen ein Virus oder einen Trojaner ein, bleibt der Schaden auf den Ordner *Eigene Dateien* begrenzt (sofern das Schadprogramm nicht eine Sicherheitslücke ausnutzen kann, um die Benutzerprivilegien für Administratoren zu erhalten).
- **Installieren Sie** ein **Virenschutzprogramm** auf dem Computer **und halten Sie dieses auf dem aktuellen Stand** (siehe die folgen-

den Seiten). Das Programm schlägt Alarm, sobald ein Virus erkannt wird. Lassen Sie zudem sporadisch eine Virenprüfung durchführen und testen Sie neu auf den Computer übertragene Programme auf Virenbefall.

- **Beziehen Sie Programmdateien nur aus vertrauenswürdigen Quellen** (z. B. Webseiten renommierter Anbieter, CDs aus Büchern oder Zeitschriften) und lassen Sie diese vor dem Öffnen durch ein Virenschutzprogramm prüfen. Wer sich illegale Programme aus obskuren Quellen beschafft und ungeprüft ausprobiert, darf sich über einen eventuellen Virenbefall nicht wundern.
- **E-Mail-Anhänge** sollten Sie zunächst **speichern und** vor dem Öffnen **auf** einen möglichen **Virenbefall testen**. Ist ein Virenschutzprogramm installiert, wird dieses bereits beim Versuch eines Zugriffs auf die betreffende Datei (wie hier gezeigt) Alarm schlagen.

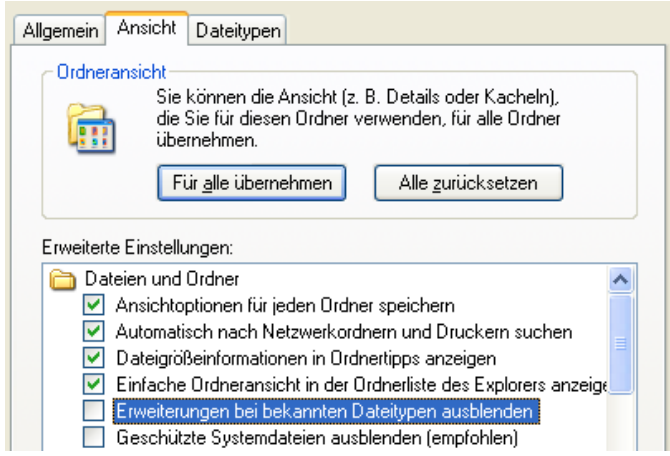
  Hier sehen Sie einen Warndialog, den ein Virenschutzprogramm beim Zugriff auf den virenverseuchten E-Mail-Anhang *File.zip* ausgelöst hat.



Über Optionen kann der Benutzer dann steuern, wie mit dem Schädling zu verfahren ist (hier wird die Datei in einen Quarantänebereich verschoben). Neben der Prüfung von Dateien auf Virenbefall können Sie zudem noch einige Verhaltensregeln und Maßnahmen zur Verbesserung der Sicherheit verwenden:

- **E-Mails von unbekannten Personen** sollten Sie **ungelesen löschen** (es sei denn, Sie erwarten gelegentlich E-Mails von unbekannten Absendern). Das Löschen empfiehlt sich insbesondere, wenn Sie mit dem Betrefftext wenig anfangen können (z. B. englischer Text) oder wenn Sie plötzlich zehn E-Mails von bekannten Absendern mit gleichlautendem Betreff erhalten (dann hat vermutlich ein Virus bei diesen Personen zugeschlagen).
- **Seien Sie auf der Hut**, wenn eine freundliche Mail von Microsoft oder anderen mit einem angeblichen Windows-Update, mit Sicherheitspatches oder einem Virenscanner im Anhang eintrifft. Firmen verschicken so etwas grundsätzlich nicht. Vielmehr muss man sich Updates von den betreffenden Firmenseiten herunterladen. Mit diesem Trick wurden aber bereits einige Viren verbreitet.
- Erhalten Sie eine E-Mail, in deren Text ein Link auf eine Webseite mit einem angeblichen Update enthalten ist? Dann sollten Sie sehr vorsichtig sein. Diese Links können gefälscht sein, statt des Updates wird ein Schädling auf Ihren Computer eingeschleust. Tippen Sie die Ihnen bekannten Adressen der Update-Seiten von Microsoft oder anderer Programmhersteller immer manuell ein. Nur so lässt sich sicherstellen, dass Sie nicht auf gefälschte Links hereinfallen.
- Auch als E-Mail-Anhänge verschickte **Grußkarten** (*.exe*-Dateien) oder **Bildschirmschoner** (*.scr*-Dateien) **sind** häufig **Virenverstecke**. Selbst in E-Mail-Anhängen von Bekannten könnte ein Virus enthalten sein (falls deren PC befallen ist oder ein Virus deren System zur Verbreitung benutzt hat). Bearbeiten Sie Ihre E-Mails nach Möglichkeit immer offline (also ohne aktive Internetverbindung), um die automatische Verbreitung von Viren zu verhindern (dann lässt sich der Postausgang vor der nächsten Online-Sitzung auf obskure Mails kontrollieren).

- Schalten Sie daher die **Anzeige der Dateinamenerweiterung** für bekannte Dateitypen unter Windows ein. Öffnen Sie hierzu ein Ordnerfenster (z. B. *Arbeitsplatz*) und wählen Sie im Menü *Extras* den Befehl *Ordneroptionen*. Auf der Registerkarte *Ansicht* löschen Sie die Markierung des Kontrollkästchens der Option *Erweiterungen bei bekannten Dateitypen ausblenden* (einfach die Option anklicken, damit das Häkchen verschwindet). Sobald Sie die Registerkarte über die *OK*-Schaltfläche schließen, werden die Erweiterungen sichtbar und Sie können auch bei heruntergeladenen Dateien oder E-Mail-Anhängen den Dateityp erkennen.

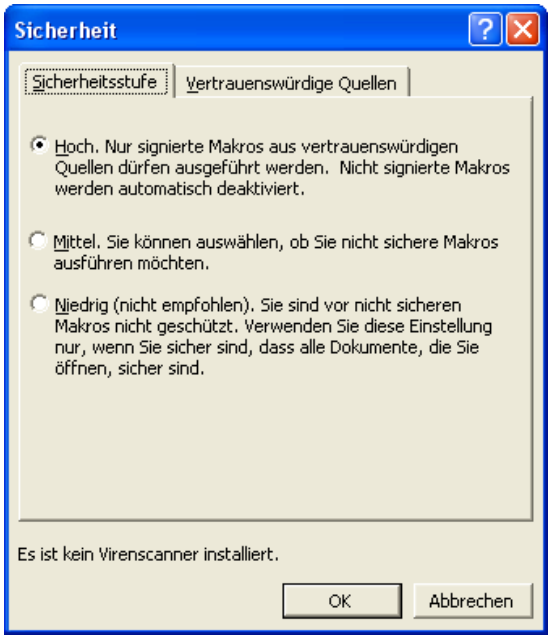


HINWEIS

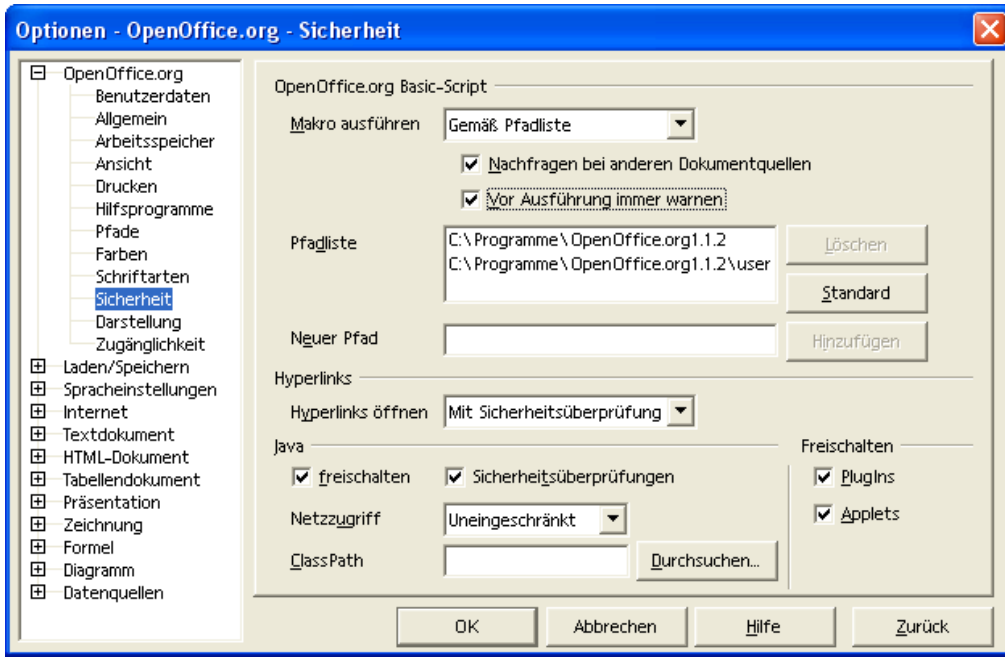
Gerade die ausgeblendeten Dateinamenerweiterungen sind eine Falle, die von Virenautoren genutzt wurde. Sie benannten Virendateien mit Namen wie *Liesmich.txt.exe*. Werden Dateinamenerweiterungen von Windows unterdrückt, sieht der Benutzer nur den Namen *Liesmich.txt* und erwartet eine Textdatei, die keine Viren enthalten kann. Beim Öffnen der vermeintlichen Textdatei wird dann das Virusprogramm ausgeführt.

- **Verhindern Sie** die **ungewollte Ausführung von Makros** in Microsoft Office-Dokumenten. Starten Sie eine der Microsoft Office-Anwendungen und wählen Sie (z. B. in Word) im Menü *Extras*

den Befehl *Makros/Sicherheit*. Im dann angezeigten Dialogfeld markieren Sie das Optionsfeld *Hoch* oder *Mittel* und schließen Sie das Dialogfeld über die *OK*-Schaltfläche.



- Bei StarOffice bzw. OpenOffice.org gilt es ebenfalls die **ungewollte Ausführung von Makros zu verhindern**. Wählen Sie (z. B. im Writer) im Menü *Extras* den Befehl *Optionen*. Im angezeigten Dialogfeld wählen Sie den Zweig *OpenOffice.org* bzw. *StarOffice* und klicken dann auf den Eintrag *Sicherheit*. Markieren Sie die Optionen *Nachfragen bei anderen Dokumentquellen* und *Vor Ausführung immer warnen*. Versucht der Benutzer ein Dokument, welches Makros enthält, zu laden, zeigt das Office-Programm eine Warnung an oder sperrt die Makroausführung (falls in Microsoft Office die Option *Hoch* oder in StarOffice der Wert des Listenfelds *Makro ausführen* auf »Niemals« gesetzt ist).



- **Verwenden Sie** auch die in diesem Buch erwähnten **Sicherheitseinstellungen für Internet Explorer** und **Outlook Express** (siehe das folgende Kapitel 4), um Scriptviren an der Ausführung zu hindern. Bei älteren Outlook- oder Outlook Express-Versionen reichte bereits die Vorschau einer E-Mail, um ein Virus zu aktivieren (ist dem Autor vor vielen Jahren passiert). Aber mit ein paar Einstellungen lässt sich dies verhindern.

  Es gilt das Sprichwort »Vorsicht ist die Mutter der Porzellankiste«. Einige Viren konnten sich nur verbreiten, weil unvorsichtige Benutzer entsprechende E-Mail-Anhänge sofort per Doppelklick geöffnet haben und kein Virenschutzprogramm installiert war. Speichern Sie niemals wichtige Informationen (z. B. Kennwörter) auf dem Computer und fertigen Sie Sicherheitskopien von wichtigen Dateien an (für den Fall, dass doch mal ein Virus auf den Rechner gelangt und die infizierten Dateien gelöscht werden müssen).

Wie kann ich Viren entfernen?

Ist es trotz aller Vorsicht doch passiert und Sie haben sich ein Virus, einen Trojaner, einen Wurm etc. eingefangen, gilt es das System schleunigst von diesem Schädling zu säubern. Hierzu benötigen Sie ein Virenschutzprogramm mit aktueller Virensignaturdatei. In der Virensignaturdatei speichert der Hersteller Informationen für den Virenscanner, damit das Virenschutzprogramm die Viren auch erkennen kann. Sobald neue Viren, Würmer oder Trojaner auftreten, ergänzen die Hersteller die Signaturdatei. Dies erklärt auch, warum es so immens wichtig ist, mit aktuellen Virenscannern bzw. Signaturdateien zu arbeiten.

Ist ein aktuelles Virenschutzprogramm auf dem Computer vorhanden, lassen Sie dieses durchlaufen. Es erkennt in aller Regel den Befall und meldet diesen. Dann gibt es mehrere Möglichkeiten:

- Es ist nur eine Datei durch das Schadprogramm befallen. Wurde die Datei gerade aus dem Internet oder von einem Datenträger übernommen, kann das Virenschutzprogramm diese Datei löschen und alles ist gut.
- Manche erkannten Schädlinge können durch das Virenschutzprogramm auch aus den befallenen Dateien entfernt werden. Dann lassen Sie das Virenschutzprogramm durchlaufen und erlauben diesem das Entfernen des Virencodes.
- Die befallene Datei darf nicht gelöscht werden und das Virus lässt sich auch nicht aus der Datei entfernen. Dann kann der Virenscanner die Datei in den so genannten Quarantänebereich verschieben. Dies eröffnet die Möglichkeit, der infizierten Datei ggf. mit weiteren Werkzeugen zu Leibe zu rücken.

  Solange nur die Datei mit dem Virus gelöscht wird, haben die Schutzmechanismen gewirkt. Falls mehrere Dateien infiziert wurden und das Virenschutzprogramm diese löschen musste oder den Virencode entfernt hat, besteht die Gefahr, dass Daten verloren gehen oder Windows bzw. einzelne Programme nicht mehr korrekt funktionieren. In diesem Fall hilft nur das Wiederherstellen der Daten aus einer Sicherungskopie. Ist Windows XP beschädigt,

können Sie versuchsweise die Systemwiederherstellung verwenden, um einen früheren (hoffentlich virenfreien) Zustand wiederherzustellen. Die notwendigen Schritte sind in Kapitel 2 im Abschnitt »Wie kriege ich Updates wieder weg?« beschrieben. Falls dies nicht hilft (was vorkommt), bleibt nur noch, die Festplatte zu formatieren und Windows sowie die vorhandenen Programme komplett neu zu installieren. Alle Daten sind dann natürlich weg – eine äußerst aufwändige und missliche Angelegenheit.

ACHTUNG

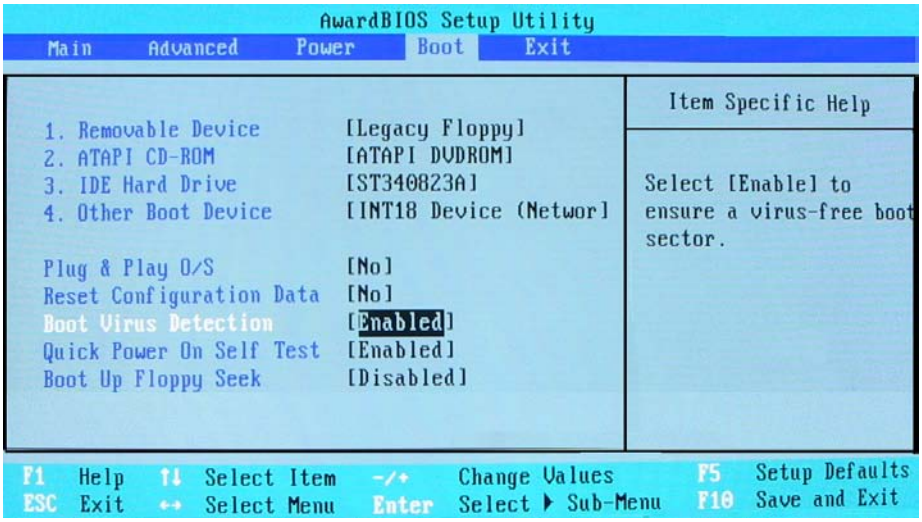
Denken Sie aber daran, dass bei der Verwendung der Systemwiederherstellung alle Änderungen, die Sie zwischenzeitlich am System ausgeführt haben, ggf. zurückgesetzt werden. Falls Sie im Hinblick auf den Virenschutz geschludert haben und die Sicherung ebenfalls virenverseucht ist, treiben Sie den »Teufel mit dem Belzebub« aus. Sie müssen also nach einer Systemwiederherstellung oder nach dem Einspielen von Sicherungsdateien sofort eine erneute Virenprüfung durchführen, um sicherzustellen, dass das System nicht erneut durch Viren verseucht wurde! Versuchen Sie auch die Ursache für den Virenbefall zu erkennen und diese Schwachstelle zu beseitigen!

Achtung bei Befall durch Bootviren

Besondere Aufmerksamkeit erfordern so genannte Bootviren. Diese Schädlinge nisten sich direkt auf der Festplatte in einem besonderen als Master Boot Record bezeichneten Bereich ein. Bootviren können auch Wechselmedien wie Disketten oder ZIP-Medien befallen. Wird eine solche mit einem Bootvirus infizierte Diskette in einem Laufwerk vergessen, versucht der Rechner beim nächsten Einschalten das Betriebssystem von Diskette zu laden. Da die Diskette aber statt des Betriebssystems das Bootvirus enthält, wird dieses gestartet. Anschließend kann sich das Virus in den Bootbereich der Festplatte kopieren und der Rechner ist infiziert.

HINWEIS

Moderne Rechner besitzen eine Möglichkeit, das Beschreiben des Bootbereichs einer Festplatte zu verhindern. Erfahrene Benutzer können diesen Schutz im so genannten BIOS einschalten. BIOS steht für Basic Input Output System, ein Bereich mit Basisprogrammen für den Computer. Wenn Sie den Computer einschalten, werden auch bestimmte Testroutinen des BIOS ausgeführt. Das BIOS zeigt für einige Sekunden einen Textbildschirm mit Statusinformationen an. Drücken Sie während dieser Zeit eine bestimmte Taste (Entf, F1 oder Esc, welche Taste dies ist, steht in den Statusinformationen auf dem Bildschirm), gelangen Sie in das BIOS-Setup. Dort finden Sie in der Regel auch eine Option, um die Überwachung auf Bootviren einzuschalten.



Konsultieren Sie ggf. die Unterlagen zu Ihrem Rechner bezüglich dieser Information. Allerdings sollten nur erfahrene Benutzer, die wissen, was sie tun, die BIOS-Einstellungen verändern (andernfalls kann es sein, dass der Rechner nicht mehr funktioniert).

Ist ein System durch ein Bootvirus befallen, müssen Sie besondere Sorgfalt beim Entfernen walten lassen. Bootviren haben teilweise die Möglichkeit, Virenschutzprogramme abzuschalten oder zu

löschen. Hier einige **Punkte**, die **beim Befall durch Bootviren** zu **befolgen** sind:

- Wenn der Verdacht auf eine Infektion mit einem Bootvirus besteht, müssen Sie den Rechner sofort vom Internet (und – falls vorhanden – von einem lokalen Netzwerk) trennen. Am besten ziehen Sie die entsprechenden Stecker für die Verbindungsleitungen zum Netzwerk/Internet.
- Läuft der Rechner und ist ein Virenscanner (z. B. AntiVir) installiert, können Sie diesen ausführen und nach dem Bootvirus suchen lassen. Das Programm sollte einen Befall melden (siehe auch den nachfolgenden Abschnitt zu AntiVir). Dieser Ansatz eignet sich vor allem zur Suche nach Bootviren auf Datenträgern (Disketten, CDs, ZIP-Medien). Kritisch wird es bei Bootviren, die sich auf der Festplatte des Rechners eingenistet haben. Dies deutet entweder darauf hin, dass kein Virenschutzprogramm installiert ist oder dass dieses das Virus nicht erkennt bzw. durch das Virus deaktiviert wurde (andernfalls wäre ja der Befall verhindert worden). In diesem Fall können Sie die nachfolgenden Ausführungen zu Rate ziehen.
- Da das Bootvirus sofort beim Starten des Rechners aktiv wird, kann es ggf. einen vorhandenen Virenscanner deaktivieren oder gleich beim Start des Computers Schäden verursachen. Haben Sie den Verdacht auf einen Befall durch ein Bootvirus und ist kein Virenscanner installiert oder ist der Rechner abgeschaltet, sollten Sie i. d. R. einen erneuten Start des Rechners vermeiden. Sie benötigen daher eine Notfall-CD oder einen entsprechenden Diskettensatz, über die bzw. den Sie den Rechner starten müssen. Das Notfallsystem sollte über einen Virenscanner verfügen, mit dem Sie das Bootvirus sicher erkennen können. Starten Sie den Rechner mit der Notfall-CD oder dem betreffenden Diskettensatz und stellen Sie fest, ob der Rechner wirklich durch ein Bootvirus befallen ist. Trifft dies zu, muss der Bootsektor der Festplatte manuell bereinigt werden (siehe unten).
- Ist das System wieder unter Windows XP lauffähig, sollten Sie es erneut mit einem Virenscanner (mit aktueller Signaturdatei) überprüfen lassen. Nach der Bereinigung müssen Sie auch sicherstellen,

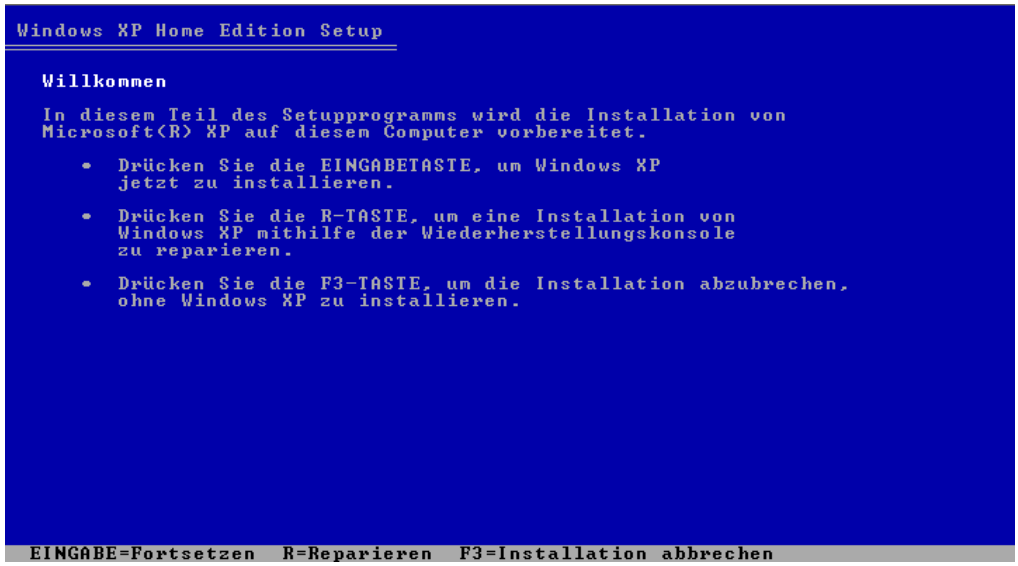
dass keinerlei Speichermedien (Disketten, ZIP-Speichermedien, USB-Speichersticks) noch mit dem Bootvirus behaftet sind. Wenn Sie dies nicht beachten, kommt es zu einer so genannten Rückinfektion. Dies bedeutet, Teile des Virus befinden sich noch auf der Festplatte oder auf Datenträgern (z. B. in Dateien) und infizieren den Bootsektor beim Betrieb des Computers erneut.

Das Problem bei Bootviren besteht darin, dass ein normaler Anwender weder über eine Notfall-CD mit integriertem Virenscanner noch über die notwendigen Kenntnisse zum Überschreiben des Bootsektors mit den Originaldateien verfügt. Als **Einsteiger sollten** Sie daher die Finger davon lassen und **das Entfernen** des **Virus** einem **Profi überlassen**. Für **erfahrene Nutzer** möchte ich kurz **zwei Möglichkeiten skizzieren**. In beiden Fällen benötigen Sie die Windows XP-Installations-CD.

1 Legen Sie die Windows XP-Installations-CD in das CD-Laufwerk ein und schalten Sie den Computer ein.

2 Falls der Rechner nicht über die CD-ROM bootet, müssen Sie einen Neustart ausführen, ins BIOS-Setup wechseln und das CD-Laufwerk als Bootmedium einstellen.

3 Warten Sie, bis der Computer ein Mini-Windows von der Installations-CD geladen hat und das Setup-Menü anzeigt.



4 Die **Radikalkur** besteht darin, die ↵-Taste zu drücken, um eine Neuinstallation auszuführen. In den Folgeschritten müssen Sie die Option zum Formatieren der Festplatte wählen und anschließend Windows XP neu installieren lassen.

Das Formatieren der Festplatte samt Neuinstallation entfernt aber nicht nur das Virus, sondern auch alle installierten Programme, die Windows-Einstellungen und die gespeicherten Daten – gelegentlich ist dies aber die letzte Rettung für virenbefallene Rechner.

5 Eine **Alternative** besteht darin, im Installationsmenü die so genannte Wiederherstellungskonsole über die Taste R aufzurufen.

6 Nach der Anmeldung an der Wiederherstellungskonsole können Sie über den Befehl *FIXMBR /device/harddisk0* den so genannten Master Boot Record der Festplatte neu schreiben lassen.

Befand sich das Bootvirus im Master Boot Record, wird dessen Code überschrieben. Anschließend empfiehlt es sich, den Rechner mit einer Notfall-CD oder einem Diskettensatz erneut zu starten und durch einen Virenscanner auf weitere Viren prüfen zu lassen. Erst wenn dieser Schritt ein virenfreies System ergibt, können Sie Windows XP erneut starten lassen. Im Anschluss ist eine erneute Virenprüfung mit aktueller Virensignatur unter Windows XP auszuführen. Dabei dürfen Sie, wie oben erwähnt, auch die Datenträger nicht von der Prüfung ausnehmen.

ACHTUNG

Eine einfache MS-DOS-Diskette mit einem DOS-Virenscanner wie F-Prot (*www.f-prot.com*) ist übrigens bei Windows XP zur Virenbeseitigung meist weitgehend nutzlos (auch wenn dieser Tipp in Webseiten häufiger auftaucht)! Meist wird Windows XP auf Laufwerken mit dem so genannten NTFS-Dateisystem installiert. Ein MS-DOS-Virenscanner kann dann zwar noch Bootviren erkennen, vermag aber nicht auf dieses NTFS-Dateisystem (d. h. auf die betreffenden Festplattenlaufwerke) zuzugreifen. Nur die oben erwähnte manuelle Vorgehensweise ermöglicht das Beseitigen von Bootviren. Da der Ablauf zum Überschreiben des Master Boot Records oder zur Windows-Installation recht komplex ist und entsprechendes Vorwissen erfordert, sprengt eine Beschreibung der Details das Ziel dieses Buches. Interessierte Leser und Leserinnen, die über die betreffende Erfahrung verfügen, werden in dem von mir bei Markt+Technik publizierten Titel »Windows XP Home Tricks« fündig. Dort wird auch beschrieben, wie man sich eine Windows XP-Notfall-CD mit integriertem Virenscanner mittels des Programms PE-Builder erstellen kann. Diese Notfall-CD erlaubt ein recht komfortables Arbeiten unter einer Windows-Oberfläche. Falls Sie sich unsicher bezüglich der Schritte zum Entfernen eines Virus sind, überlassen Sie die Sache lieber Fachleuten. Niemand kommt auf die Idee, ohne entsprechendes Wissen und Spezialwerkzeuge die Kolbenringe eines Motors auszuwechseln. Also halten Sie sich auch bei Windows an diese Regel.

Auch Fehlalarme sind möglich

Virenscanner identifizieren Viren oder andere Schädlinge anhand so genannter Signaturen. Dies sind meist Anweisungsfolgen im Programmcode des Virus. Zusätzlich prüfen die Scanner Dokumente auf Makro- und Scriptviren. Dabei wird häufig nur nachgesehen, ob im betreffenden Programmcode verdächtige oder gefährliche Anweisungen gefunden werden. Ein Befehl zum Löschen von Dateien gehört zum Beispiel in diese Kategorie. Ob dieser Befehl eventuell doch eine sinnvolle Funktion hat, kann der Virenscanner nicht beurteilen und schlägt Alarm (ohne dass ein Virus dahinter stecken muss).

Für Sie bedeutet dies aber, erhöhte Vorsicht und Wachsamkeit walten zu lassen. Meldet der Scanner eine infizierte Datei, sollten Sie diese in den Quarantänebereich verschieben lassen. Nur wenn Sie absolut sicher sind, dass es sich um einen Fehlalarm des Virenscanners handelt (beispielsweise haben Sie die Makrodatei selbst erstellt oder aus einer vertrauenswürdigen Quelle mit einer Garantie hinsichtlich Virenfreiheit erhalten), sollten Sie die Dateien verwenden.

Das Vexira-Notfallset

Die US-Firma Vexira bietet ein Notfall-Virenset für Privatanwender an, das sich kostenlos aus dem Internet herunterladen und dann entweder als Notfall-CD-ROM brennen oder auf einen Notfall-Diskettenset kopieren lässt. Das so genannte Vexira Antivirus Rescue-Kit setzt dabei auf dem Betriebssystem Linux auf und benötigt kein funktionierendes Windows-System. Das Notfallset lässt sich neben Linux-Computern auch für alle Windows-Versionen und deren Dateisysteme (auch NTFS) einsetzen. Nachfolgend möchte ich diese Lösung, die sich insbesondere zum Erkennen von Bootviren eignet, kurz vorstellen.

So erstellen Sie einen Notfall-Diskettensatz

Wer keinen CD-Brenner besitzt oder sich mit dem Brennen von CDs nicht besonders gut auskennt, kann sich mit den folgenden Schritten einen Notfall-Diskettensatz mit Virenscanner erstellen.

1 Rufen Sie die englischsprachige Internetseite des Antivirenherstellers Vexira unter *www.centralcommand.com/downloads.html* auf und suchen Sie ggf. die Rubrik »Vexira Antivirus Free Software«.

2 Klicken Sie auf den Hyperlink *Creation of a bootable 4 diskette set* und laden Sie die gut 5 Megabyte große Windows-Programmdatei *rescuedisk.exe* in einen lokalen Ordner auf der Festplatte des Rechners herunter. Anschließend blättern Sie auf der Webseite nach unten zur Rubrik »Miscellanous Downloads«, laden zusätzlich die beiden aktuellen Virensignaturdateien (ca. 1 Megabyte und 800 Kilobyte) unter »Vexira Antivirus Split VDF (for use with the Rescue Disk System)« herunter und speichern diese auf der Festplatte des Rechners.

Anschließend können Sie die Internetverbindung wieder trennen und den Browser schließen. Sie benötigen jetzt insgesamt sechs leere Disketten für den Notfall-Diskettenset.

1 Öffnen Sie das Ordnerfenster, in dem die heruntergeladenen Dateien gespeichert wurden, und starten Sie das Programm *rescuedisk.exe*. Dieses zeigt kurz ein Dialogfeld an und öffnet dann das Fenster der Eingabeaufforderung.

2 Befolgen Sie jetzt die Anweisungen des Programms, welches Sie auffordert, eine leere Diskette einzulegen, und betätigen Sie dann die ↵-Taste.

3 Das Programm schreibt daraufhin die benötigten Daten auf die betreffende Diskette. Ist dieser Schritt ausgeführt (wird vom Programm gemeldet), entnehmen Sie die Diskette und beschriften diese mit einer fortlaufenden Nummer (z. B. »Vexira Disk 1«).

Sie müssen die Schritte 2 und 3 für insgesamt vier Disketten durchführen. Mit diesen Disketten lässt sich später ein System starten. Um immer eine aktuelle Virensignatur verwenden zu können, sollten Sie nun noch zwei Disketten mit den aktuellen Virensignaturdateien erzeugen.

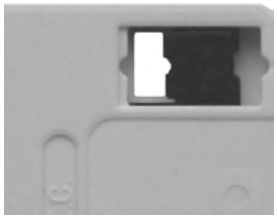
1 Öffnen Sie das Ordnerfenster, in dem die heruntergeladenen Signaturdateien gespeichert wurden, und legen Sie eine leere Diskette ein.

2 Kopieren Sie nun die erste Signaturdatei auf die erste Diskette. Anschließend entnehmen Sie die Diskette und beschriften diese entsprechend.

3 Legen Sie die zweite leere Diskette in das Laufwerk ein und kopieren Sie dann die zweite Signaturdatei auf diese Diskette. Anschließend ist auch diese Diskette zu entnehmen und zu beschriften.

Wenn alles geklappt hat, verfügen Sie über vier Notfalldisketten und zwei Disketten mit den aktuellen Virensignaturen. Zukünftig sollten Sie in regelmäßigen Abständen (z. B. alle vier Wochen) die Dateien mit den aktuellen Virensignaturen von der Vexira-Webseite herunterladen und dann auf die beiden Disketten kopieren. Dies ermöglicht Ihnen, die Virenprüfung mit aktuellen Signaturen durchzuführen.

TIPP



Denken Sie daran, den Schreibschutz auf den so erstellten Notfalldisketten zu aktivieren (einfach den Schreibschutzschieber der Diskette so verschieben, dass das Schreibschutzloch geöffnet ist).

Zudem empfiehlt sich anschließend ein Test, ob der Notfall-Diskettensatz auch funktioniert. Fahren Sie Windows XP herunter und starten Sie den Rechner gemäß den Anweisungen im nachfolgenden Abschnitt zum Einsatz des Virenscanners.

So erstellen Sie eine Notfall-CD

Falls Sie einen CD-Brenner besitzen, können Sie auch eine Notfall-CD mit dem Vexira-Notfallset brennen.

1 Rufen Sie die englischsprachige Internetseite des Antivirenherstellers Vexira unter *www.centralcommand.com/downloads.html* auf und blättern Sie zur die Rubrik »Vexira Antivirus Free Software«.

2 Klicken Sie auf den Hyperlink *Creation of a bootable CD-Rom* und laden Sie die gut 12 Megabyte große ISO-Datei *rescuedisk.iso* in einen lokalen Ordner auf der Festplatte des Rechners herunter.

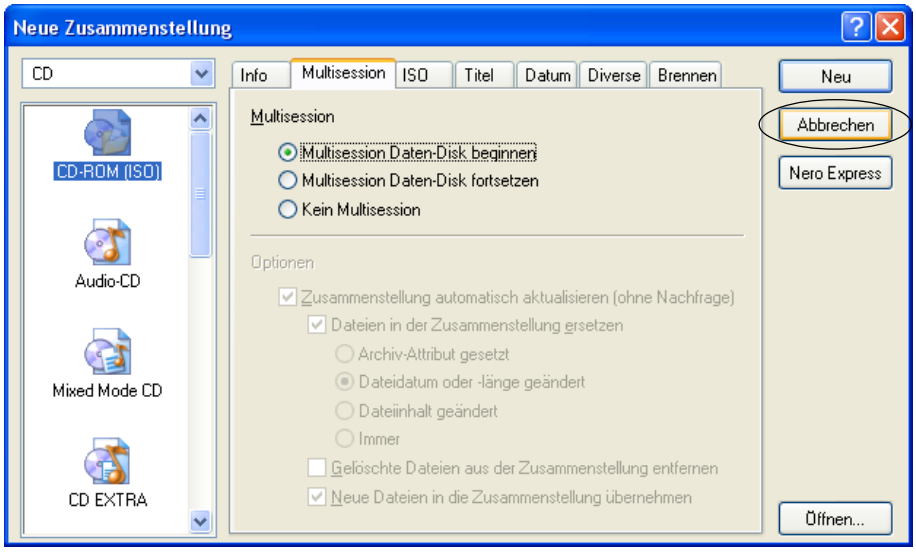
3 Anschließend blättern Sie auf der Webseite nach unten zur Rubrik »Miscellanous Downloads«, laden zusätzlich die beiden aktuellen Virensignaturdateien (ca. 1 Megabyte und 800 Kilobyte) unter »Vexira Antivirus Split VDF (for use with the Rescue Disk System)« herunter und speichern diese auf der Festplatte des Rechners.

4 Kopieren Sie die zwei Signaturdisketten gemäß den Erläuterungen im vorherigen Abschnitt auf zwei beschriftete Disketten und legen Sie diese Medien beiseite.

5 Nach diesen Vorbereitungen müssen Sie die heruntergeladene *.iso*-Datei auf eine CD brennen.

Sie können dabei verschiedene Brennprogramme verwenden, um die heruntergeladene *.iso*-Datei auf eine CD zu bringen. Nachfolgend wird davon ausgegangen, dass Sie hierzu das weit verbreitete Programm Nero Burning Rom 6 verwenden.

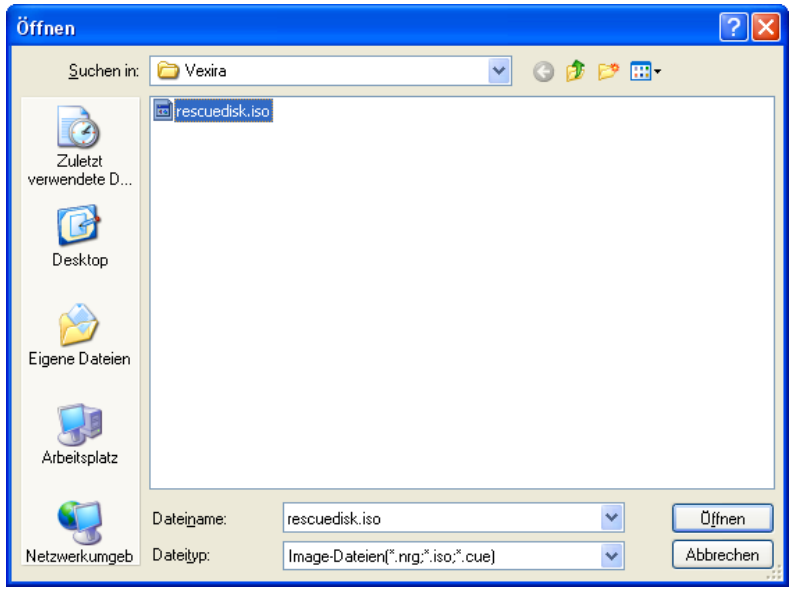
1 Starten Sie das Brennprogramm Nero Burning Rom 6. Den dann angezeigten Dialog *Neue Zusammenstellung* zur Auswahl des CD-Typs beenden Sie über die *Abbrechen*-Schaltfläche.



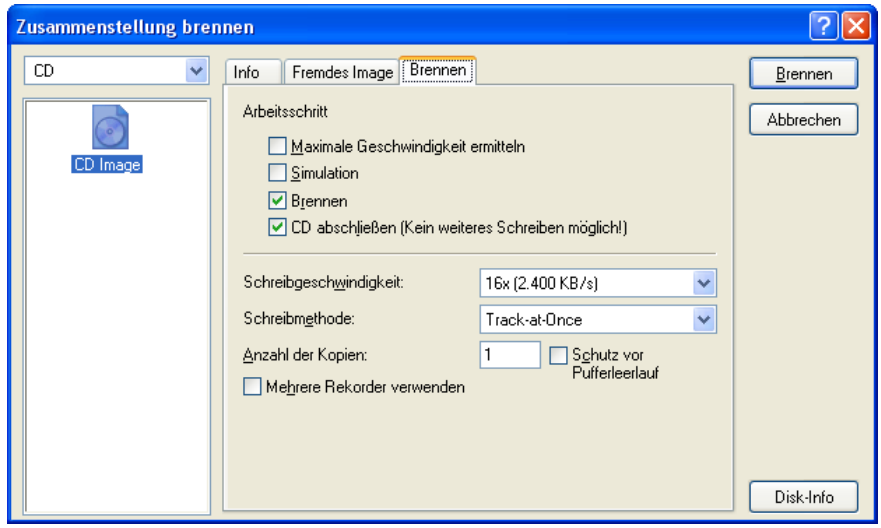
2 Wählen Sie den Befehl *Öffnen* (z. B. über den gleichnamigen Befehl im Menü *Datei* des Nero Burning Rom-Fensters oder durch Drücken der Tastenkombination Strg+O).

3 Wählen Sie im Dialogfeld *Öffnen* den Ordner, in den Sie die *.iso*-Datei von der Vexira-Webseite heruntergeladen haben.

4 Klicken Sie auf das Listenfeld *Dateityp* des Dialogfelds *Öffnen* und stellen Sie den Dateityp auf den Wert »Image-Dateien(*.nrg; *.iso; *.cue)« ein.



5 Markieren Sie dann im Dialogfeld *Öffnen* die angezeigte Datei *rescuedisk.iso* und klicken Sie auf die *Öffnen*-Schaltfläche.



6 In dem anschließend angezeigten Dialogfeld *Zusammenstellung brennen* markieren Sie auf der Registerkarte *Brennen* die hier gezeigten Kontrollkästchen *Brennen* sowie *CD abschließen* und klicken dann auf die Schaltfläche *Brennen*.

7 Befolgen Sie anschließend die Dialoge, die Sie zum Einlegen eines CD-R-Rohlings auffordern, warten Sie, bis der Brennvorgang abgeschlossen ist, schließen Sie das Dialogfeld mit den Statusinformationen zum Brennen, entnehmen Sie den gebrannten Rohling und beenden Sie das Brennprogramm.

Nach diesem Vorgang sollten Sie die neu erstellte CD-ROM entsprechend beschriften. Anschließend legen Sie diese CD in das CD-Laufwerk ein und führen einen Test aus, indem Sie Windows XP herunterfahren und den Rechner neu starten lassen. Wenn das CD-Laufwerk im BIOS als Bootmedium zugelassen ist (siehe auch weiter oben im Abschnitt »Achtung bei Befall durch Bootviren«), sollte das Not-Betriebssystem von der CD geladen und der Virenscanner gestartet werden.

TIPP

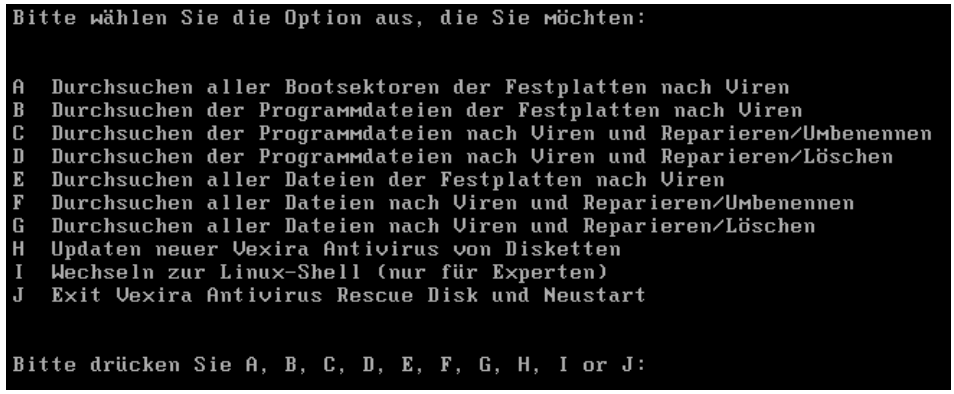
Falls Sie anstelle eines CD-R-Rohlings lieber einen wiederbeschreibbaren CD-RW-Rohling verwenden, muss dieser vor dem Brennen komplett gelöscht werden. Dies lässt sich in Nero Burning Rom 6 über den Befehl *Rewritable-Disk löschen* des Menüs *Rekorder* durchführen. Wichtig ist dabei, dass Sie im dann angezeigten Dialogfeld *Rewritable-Disk löschen* als Löschmethode »RW-Disk vollständig löschen« wählen. Falls Sie dies ignorieren, wird die so gebrannte CD nutzlos. Die Dateien befinden sich dann zwar auf der CD, Sie können den Rechner aber nicht über das Medium starten!

So nutzen Sie das Vexira-Notfallset

Möchten Sie den Rechner mit dem Vexira-Notfallset auf Virenbefall untersuchen, gehen Sie in folgenden Schritten vor:

1 Legen Sie die Vexira-Notfall-CD oder die erste Diskette des Diskettensatzes in das Laufwerk ein und fahren Sie den Rechner ggf. herunter. Falls der Rechner nicht auf die Diskette oder CD-ROM zugreift, sondern direkt auf die Festplatte, schalten Sie diesen sofort aus, starten neu und stellen die so genannte Bootreihenfolge in den BIOS-Optionen entsprechend um. Falls Sie dies nicht selbst können, lassen Sie sich von einem erfahrenen Benutzer helfen.

2 Sobald der Rechner vom Vexira-Notfallset startet, befolgen Sie die angezeigten Schritte. Sie müssen den Start über die [↵]-Taste einleiten und verschiedene Lizenzbedingungen über diverse Tasten (z. B. [ ]-Taste) bestätigen. Anschließend lässt sich über eine weitere Taste die Menüsprache (Englisch oder Deutsch) wählen. Beim Diskettensatz werden dann die verschiedenen Disketten angefordert.



3 Nach dem Start erscheint ein Menü, dessen Bedeutung selbsterklärend ist. Sie müssen lediglich den Buchstaben vor dem Menüpunkt eintippen, um die Funktion abzurufen.

Zum Prüfen auf Bootviren geben Sie den Buchstaben A ein. Beachten Sie aber, dass das Notfallset Bootviren nur erkennen, nicht aber entfernen kann. Zum Entfernen müssen Sie die im vorherigen Abschnitt beschriebenen manuellen Schritte ausführen. Mit den restlichen Buchstaben können Sie die Festplatten auf Viren prüfen und ggf. eine Bereinigung infizierter Dateien durchführen lassen. Mit dem Buchstaben H lässt sich die Virensignatur aktualisieren. Sie werden dann aufgefordert, die betreffenden Signaturdisketten einzulegen. Zum Beenden der Virenprüfung entfernen Sie die Diskette bzw. CD aus dem Laufwerk und starten dann den Rechner durch Drücken der Taste J neu.

Arbeiten mit AntiVir

Arbeiten mit dem Computer ohne aktuelles Virenschutzprogramm ist wie russisches Roulette – man weiß nie, wann es einen erwischt. Sie sollten daher auf jeden Fall ein solches Programm unter Windows XP installiert haben. Die Firma H+BEDV bietet ein für Privatanwender kostenloses Virenschutzprogramm AntiVir zum Download aus dem Internet an. Mit AntiVir lassen sich Windows-Systeme zuverlässig gegen Viren schützen. Nachfolgend erfahren Sie, wie Sie das Programm aus dem Internet herunterladen, aktualisieren und einsetzen.

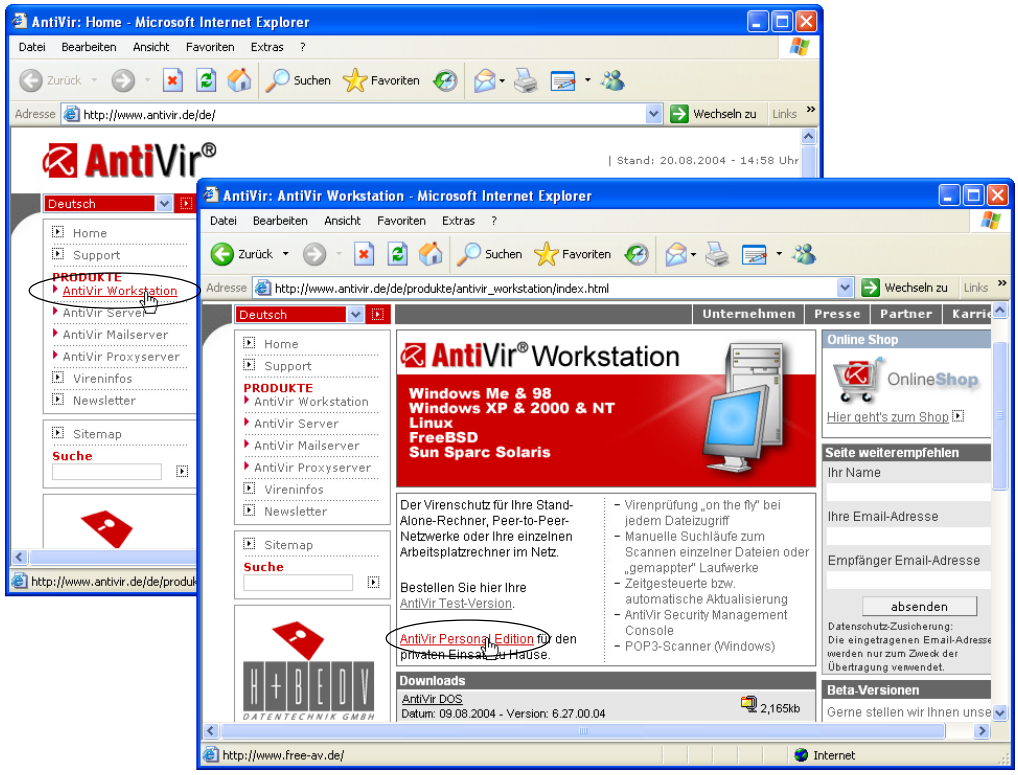
Wo gibt es AntiVir?

Das Virenschutzprogramm AntiVir der Firma H+BEDV findet sich häufig auf Begleit-CD-ROMs von Computerzeitschriften. Problem ist allerdings, dass diese Fassungen häufig veraltet sind. Die aktuelle Fassung ist nur per Internet erhältlich. Um sich eine aktuelle Version von AntiVir für Windows XP herunterzuladen, gehen Sie in folgenden Schritten vor:

1 Stellen Sie über Ihren Computer eine Internetverbindung her und starten Sie den Internet Explorer oder einen anderen Browser. ------►

2 Rufen Sie die Webseite *www.antivir.de* im betreffenden Browser auf. Die AntiVir-Webseite wird so ähnlich wie hier gezeigt aussehen (wobei die Seite aber von Zeit zu Zeit vom Anbieter neu gestaltet wird).

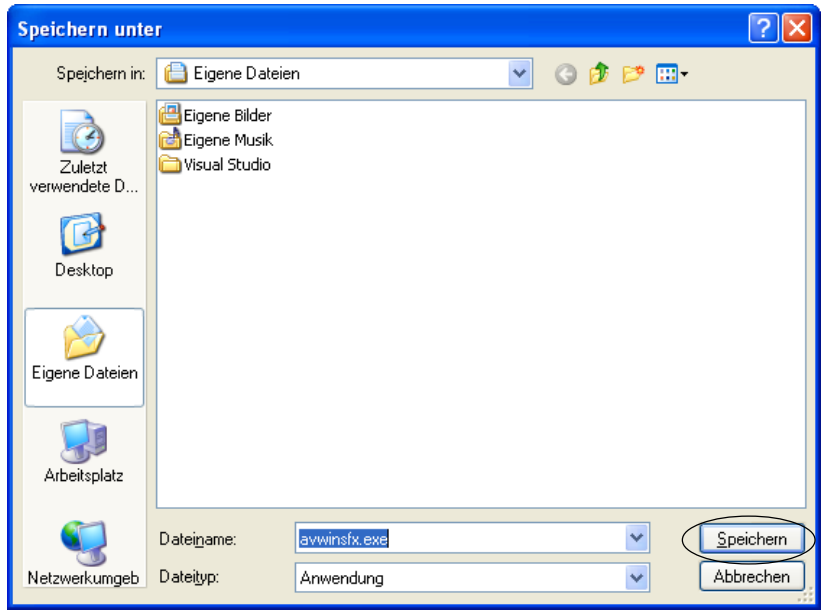
3 Suchen Sie nun auf der AntiVir-Webseite den Hyperlink der kostenlosen AntiVir-Version für Privatanwender. In der hier gezeigten Version der Webseite müssen Sie in der linken Spalte der Eingangsseite den Hyperlink *AntiVir Workstation* wählen. Die Folgeseite listet dann die verfügbaren AntiVir Workstation-Produkte auf. Dort gilt es auf den Hyperlink *AntiVir Personal Edition für den privaten Einsatz zu Hause* zu klicken.



4 Auf der Download-Seite zur AntiVir Personal Edition klicken Sie in der linken Spalte auf die Schaltfläche *Download*. Anschließend können Sie in der mittleren Spalte einen der Download-Links (*Server 1* oder die Seite der Zeitschrift *Chip*) anklicken.

Windows XP startet nun eine Download-Anforderung an den betreffenden Server. Je nach dessen Auslastung dauert es dann einige Sekunden, bis der Download-Dialog erscheint. Falls dieser Dialog nach einer Minute nicht sichtbar wird, ist der betreffende Server ausgefallen oder überlastet. Dann schließen Sie das Browserfenster und wiederholen die obigen Schritte erneut, wählen aber für den Download einen alternativen Server.

5 Klappt die Download-Anfrage, zeigt Windows XP mit installiertem Service Pack 2 das Dialogfeld *Dateidownload – Sicherheitswarnung*. Klicken Sie auf die Schaltfläche *Speichern*.



6 Wählen Sie im Dialogfeld *Speichern unter* den Zielordner, in dem die AntiVir-Installationsdatei zu hinterlegen ist. Der Dateiname wird automatisch vorgegeben. Klicken Sie erneut auf die Schaltfläche *Speichern*.

Nun beginnt der Download der Programmdatei von der AntiVir-Webseite. Ist der Download abgeschlossen, können Sie die Internetverbindung wieder trennen und den Browser mit der AntiVir-Webseite schließen.

HINWEIS

Je nach Auslastung des Internets bzw. der AntiVir-Webseite und in Abhängigkeit von der Übertragungsgeschwindigkeit Ihrer Internetverbindung (Modem, ISDN oder DSL) kann der Download des mittlerweile über 4 Megabyte umfassenden Programmpakets bis zu 15 Minuten dauern. Bei einer Modem- oder einer ISDN-Verbindung empfiehlt sich daher der Download zu Tageszeiten mit verbilligtem Tarif.

Neben der kostenlosen AntiVir Personal Edition für den privaten Einsatz bietet die Firma H+BEDV die kostenpflichtige Fassung AntiVir Workstation. Diese kann auch wegen verschiedener Zusatzfunktionen (Support, Option zum Erzeugen einer Notfall-CD etc.) für Privatanwender interessant werden. Preisinformationen sowie Benutzerhandbücher zu den jeweiligen Varianten finden Sie auf der AntiVir-Download-Seite im so genannten PDF-Format. Um solche PDF-Dateien ansehen zu können, benötigen Sie den Adobe Reader, den Sie von der Webseite *www.adobe.de* kostenlos herunterladen können.

So installieren Sie AntiVir

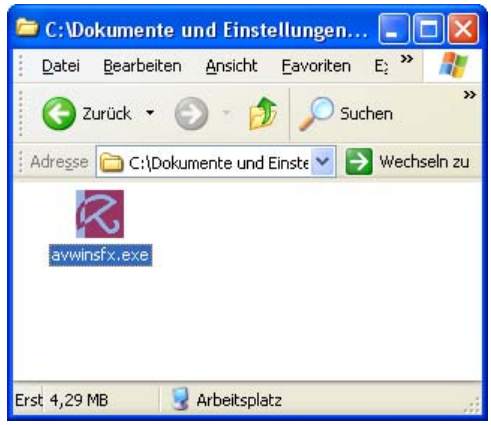
Sobald die Installationsdatei der AntiVir Personal Edition aus dem Internet heruntergeladen wurde, müssen Sie das Programm installieren.

HINWEIS

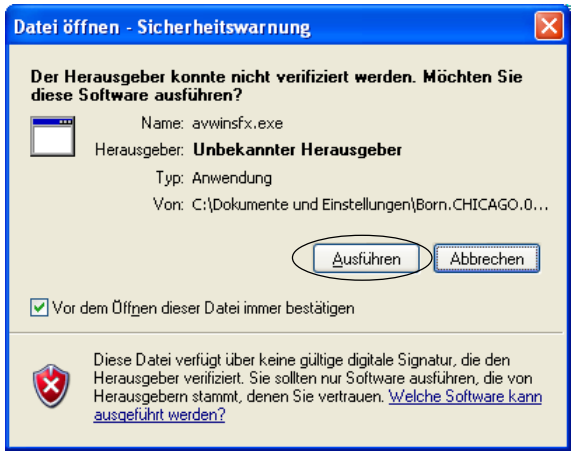
Wenn Sie aus Sicherheitsgründen meinen Empfehlungen aus Kapitel 2 gefolgt sind, arbeiten Sie standardmäßig unter einem eingeschränkten Benutzerkonto. Zur Installation von AntiVir müssen Sie sich am Administratorenkonto des Benutzers anmelden. Erst dann lassen sich die nachfolgenden Schritte fehlerfrei ausführen.

1 Beenden Sie alle laufenden Anwendungen unter Windows XP. Dies soll verhindern, dass diese ggf. den Installationsvorgang beeinflussen.

2 Öffnen Sie (z. B. über das Startmenüsymbol *Arbeitsplatz*) ein Ordnerfenster und suchen Sie den Ordner, in den Sie die AntiVir-Installationsdatei heruntergeladen haben.



3 Starten Sie das Installationsprogramm, indem Sie die betreffende Datei (*avwinsfx.exe*) per Doppelklick anwählen.

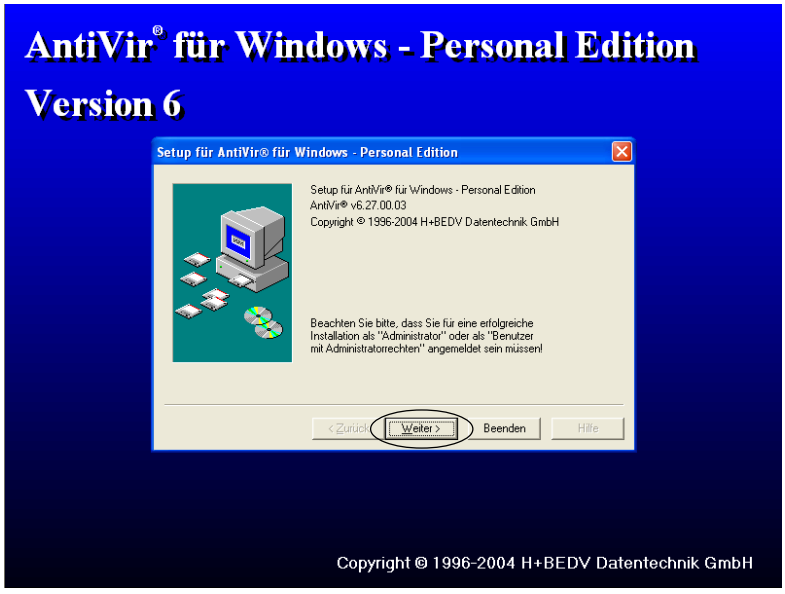


Bei installiertem Windows XP Service Pack 2 erscheint ggf. der nebenstehende Warndialog.

4 Klicken Sie auf die Schaltfläche *Ausführen*, um das Installationsprogramm zu starten.

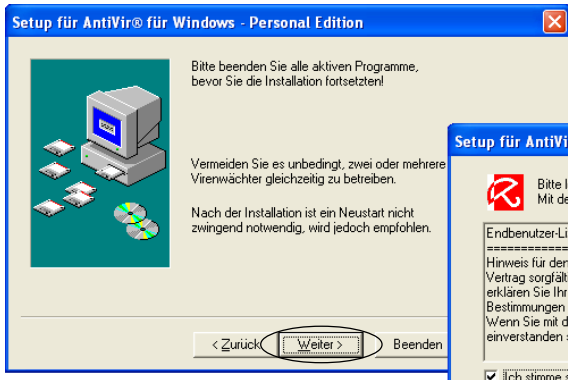
5 Sobald dieses Dialogfeld erscheint, klicken Sie auf die mit *Setup* beschriftete Schaltfläche.

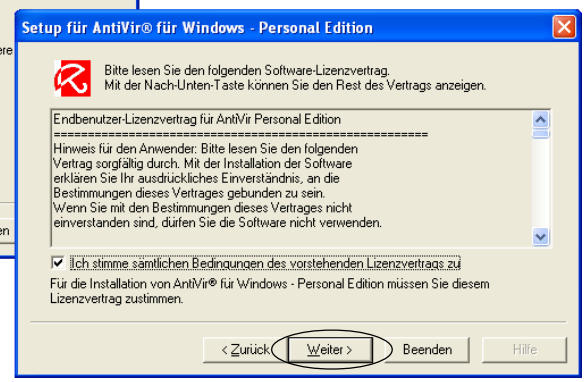
Um das Paket für den Download per Internet möglichst kompakt zu halten, hat der Hersteller alle Dateien in einer Archivdatei komprimiert. Das Installationsprogramm beginnt daher zuerst mit dem Entpacken der jeweiligen Dateien in einen lokalen Ordner der Festplatte. Sie werden über eine Fortschrittsanzeige des Dialogfelds *WinZip Self-Extractor* über diesen Schritt informiert. Erst wenn alle Dateien entpackt sind, startet der eigentliche Installationsvorgang automatisch. Der Windows-Desktop verschwindet und wird durch den blauen Installationshintergrund sowie den Dialog des Installationsassistenten ersetzt.



6 Klicken Sie im Dialogfeld des Setup-Assistenten auf die Schaltfläche *Weiter*.

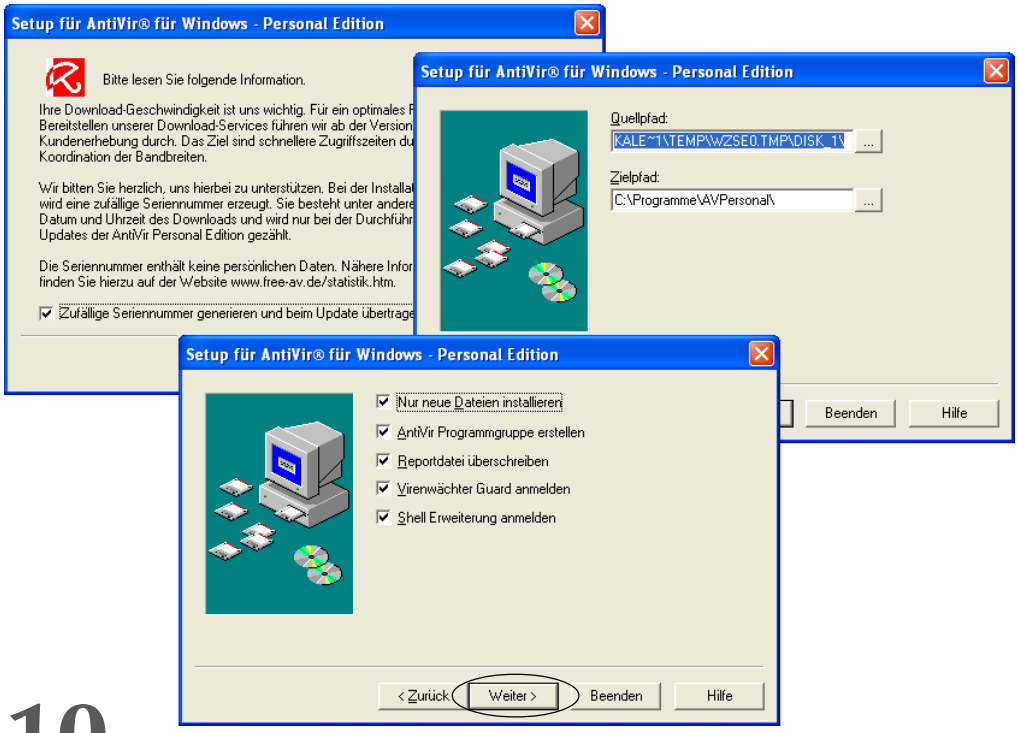
7 Lesen Sie die Hinweise im Folgedialog. Falls noch nicht alle Programme beendet oder andere Virenscanner installiert sind, sollten Sie die Installation über die Schaltfläche *Beenden* abbrechen. Andernfalls klicken Sie im Dialogfeld des Setup-Assistenten erneut auf die Schaltfläche *Weiter*.





8 Lesen Sie nun den im Dialogfeld eingeblendeten Endbenutzervertrag. Anschließend markieren Sie das Kontrollkästchen *Ich stimme sämtlichen Bedingungen des vorstehenden Lizenzvertrags zu* und klicken Sie erneut auf die Schaltfläche *Weiter* des Setup-Assistenten.

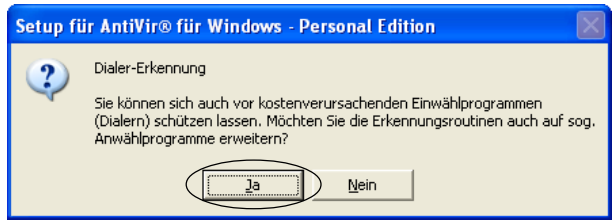
9 Im Folgedialog belassen Sie die Markierung des Kontrollkästchens *Zufällige Seriennummer generieren und beim Update übertragen* und klicken lediglich auf die *Weiter*-Schaltfläche.



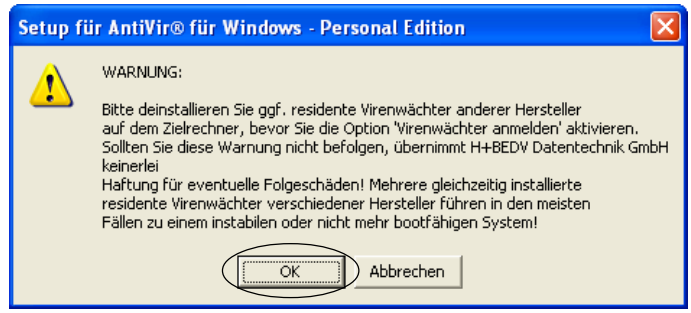
10 Im Dialog mit der Angabe des Zielpfads können Sie die Vorgaben des Assistenten belassen und die Schaltfläche *Weiter* des Setup-Assistenten wählen.

11 Der Assistent gibt Ihnen über mehrere Kontrollkästchen im Dialogfeld die Möglichkeit, die zu installierenden Komponenten zu wählen. Falls Sie unsicher sind, was installiert werden soll, belassen Sie die Vorgaben des Assistenten und klicken wiederum auf die Schaltfläche *Weiter*.

Eine hilfreiche Zugabe von AntiVir ist die Möglichkeit zum Erkennen von Dialern. Einige dieser Dialer leiten die Internetverbindung ungewollt auf sehr teure Anbieter (2 Euro pro Minute oder mehrere Euro pro Einwahl). Der Setup-Assistent fragt Sie während der Installation in einem Dialogfeld, ob die Dialererkennung mit eingerichtet werden soll.



12 Sobald dieses Dialogfeld erscheint, klicken Sie ggf. auf die *Ja*-Schaltfläche.

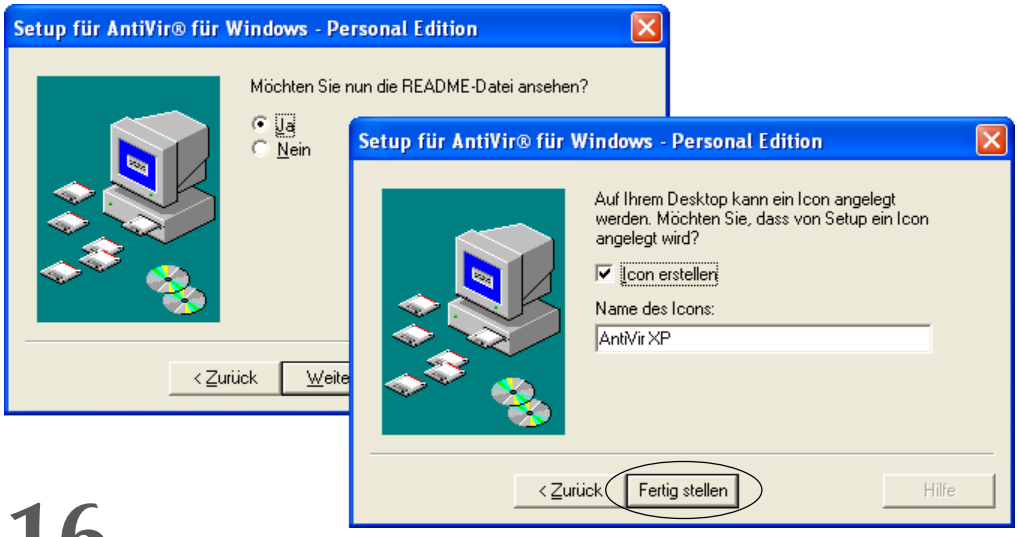


13 Die Warnung des Herstellers in diesem Dialogfeld quittieren Sie über die *OK*-Schaltfläche.

Nun besitzt das Installationsprogramm alle benötigten Informationen und beginnt mit dem Einrichten von AntiVir. Sie werden durch eine Fortschrittsanzeige über den Ablauf informiert.

14 Wenn dieses Dialogfeld erscheint, ist die Installation abgeschlossen und Sie müssen auf die *Weiter*-Schaltfläche klicken.

15 In einem weiteren Dialog bietet Ihnen der Assistent die Möglichkeit, eine so genannte Readme-Datei im Windows-Editor anzusehen. Belassen Sie die Markierung des Optionsfelds auf *Ja* und klicken Sie auf die Schaltfläche *Weiter*. Anschließend können Sie die Hinweise im Fenster des Editors lesen und danach das Fenster schließen.



16 Belassen Sie im nächsten Dialogfeld die Markierung des Kontrollkästchens *Icon erstellen* sowie den Namen des Icons und schließen Sie die Installation mittels der *Fertig stellen*-Schaltfläche ab.

Das Setup-Programm wird dann neben einem Eintrag im Startmenü auch ein AntiVir-Symbol auf dem Windows-Desktop ablegen. Um sicherzugehen, dass der Computer nicht infiziert ist, wird ein Programm mit dem Namen *Luke Filewalker* gestartet.

Das Programm führt dann einen Virenscan über die Laufwerke des Computers aus. Sie werden in einem entsprechenden Fenster über den Fortschritt informiert.

Aus Sicherheitsgründen sollten Sie diese Prüfung durchlaufen lassen und keinesfalls über die im unteren Bereich des Fensters angezeigte *Stop*-Schaltfläche abbrechen. Nur wenn Luke Filewalker alle Dateien geprüft und keine Viren gemeldet hat, sind Sie auf der sicheren Seite. Nach der Überprüfung auf Viren werden die Installationsfenster automatisch geschlossen.

Wenn alles geklappt hat, sollte ein AntiVir-Symbol auf dem Desktop zu sehen sein. Zudem finden Sie im Infobereich der Taskleiste ein AntiVir-Symbol.

Öffnen Sie das Windows-Sicherheitscenter (z. B. über die Systemsteuerung), sollte beim Thema Virenschutz ein grüner Punkt mit dem Text »Aktiv« erscheinen.

Damit ist der Computer vor Viren und sonstigen Schädlingen durch den Virenwächter von AntiVir geschützt. Wie Sie mit dem Programm umgehen, wird in den folgenden Abschnitten skizziert.

Ist ein aktuelles AntiVir installiert und auch alles andere in Ordnung, verschwindet das im Infobereich der Taskleiste eingeblendete Symbol des Windows-Sicherheitscenters. Erst wenn potentielle Sicherheitsprobleme erkannt werden (z. B. veraltete Signaturdatei des Virenscanners), blendet Windows das Symbol erneut ein. Nach der Installation sollten Sie vorsichtshalber Windows neu starten, um ggf. Aktualisierungsprobleme zu vermeiden.

So halten Sie AntiVir aktuell

Die Installation eines Virenschutzpakets ist der erste Schritt zu mehr Sicherheit. Aber so, wie ein schlecht gewartetes Auto irgendwann zum Sicherheitsrisiko wird, ist es auch wichtig, dass

das Antivirenprogramm immer auf dem aktuellen Stand gehalten wird. Ständig tauchen neue Viren auf, die von älteren Antivirenprogrammen eventuell nicht mehr erkannt werden. Die Hersteller der Antivirenprogramme stellen daher regelmäßig aktualisierte Signaturen für neue Viren oder Programmupdates im Internet bereit. Auch AntiVir kann den Computer nur schützen, wenn eine aktuelle Version vorliegt.

AntiVir überprüft bei jedem Start, ob die Virensignatur jünger als 14 Tage ist. Erscheint beim Anmelden an Windows XP dieses Dialogfeld auf dem Desktop, ist dies ein deutlicher Hinweis darauf, dass Sie nicht mit einer aktuellen Version arbeiten.

Falls Sie nicht sofort ins Internet gehen können, lässt sich das Dialogfeld über die *OK*-Schaltfläche schließen. Sie sollten dann aber daran denken, AntiVir bei nächster Gelegenheit zu aktualisieren.

Auch wenn das 14-tägige Aktualisierungsintervall noch nicht abgelaufen ist, kann es sein, dass H+BEDV bereits auf neue Viren reagiert und aktualisierte Signaturdateien bereitgestellt hat. Bei installiertem Windows XP Service Pack 2 überprüft AntiVir automatisch bei jeder Internetsitzung, ob Updates vorhanden sind. Trifft dies zu, meldet das Programm dies an das Windows-Sicherheitscenter. Öffnen Sie anschließend das Windows-Sicherheitscenter (z. B. über das Symbol im Infobereich der Taskleiste oder über die Systemsteuerung), sollte in der Kategorie »Virenprüfung« eine entsprechende Meldung eingeblendet werden.

In diesem Fall empfiehlt sich die Aktualisierung des Virenschutzprogramms bzw. der Virensignatur gemäß den nachfolgenden Schritten.

HINWEIS

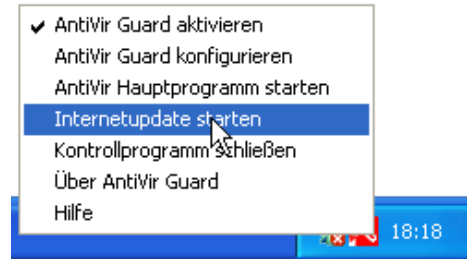
Beim Update der Virensignatur reduziert sich die Datenmenge auf ca. 1,8 Megabyte, weshalb die nachfolgend beschriebene Methode zu bevorzugen ist. In der Vergangenheit gab es gelegentlich Probleme mit dem Internetupdate. In diesem Fall können Sie die jeweils aktuelle Version von AntiVir von der H+BEDV-Webseite herunterladen und installieren. Leider sind dann aber immer über 4 Megabyte Daten zu laden.

1 Melden Sie sich unter einem Administratorenkonto unter Windows XP an, um Fehler während des Internetupdates wegen fehlender Benutzerrechte zu verhindern. ----------►

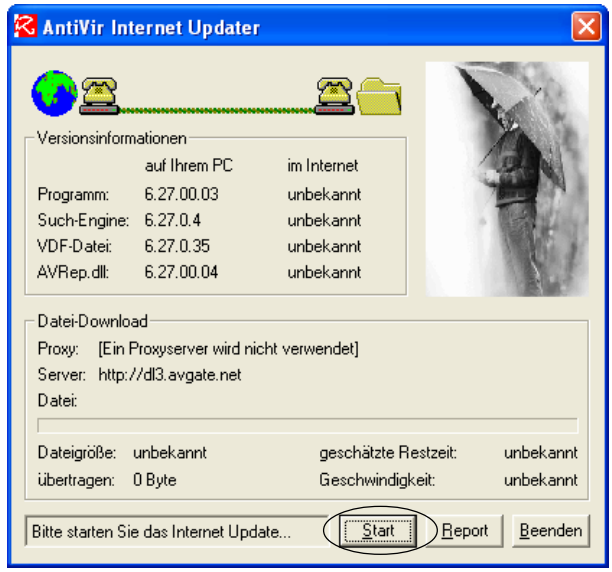
2 Stellen Sie anschließend eine Internetverbindung her und rufen Sie dann die Antivir-Funktion zum Internetupdate auf.

Das Internetupdate lässt sich in AntiVir sowohl über das Hauptprogramm also auch über den Virenwächter (AntiVir Guard) vornehmen.

Sie können daher mit der rechten Maustaste auf das AntiVir Guard-Symbol im Infobereich der Taskleiste klicken und dann im Kontextmenü den Befehl *Internetupdate starten* wählen.



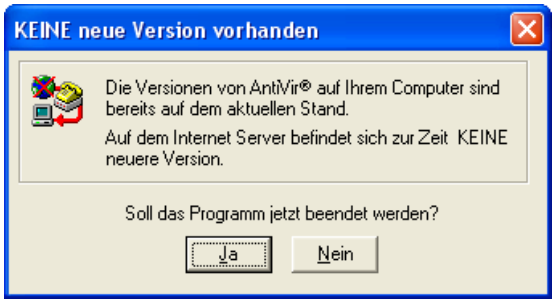
Oder Sie rufen alternativ das AntiVir-Hauptprogramm auf. In diesem Programm lässt sich die Schaltfläche *Internetupdate* in der Symbolleiste oder der Befehl *Internetupdate starten* im Menü *Tools* wählen.

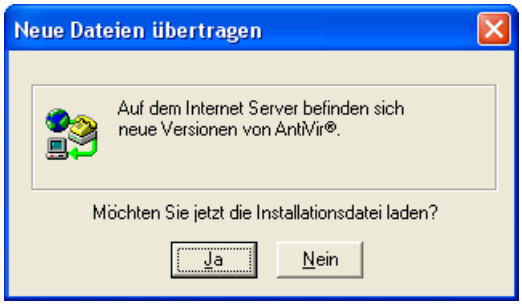


3 Klicken Sie im Dialogfeld *AntiVir Internet Updater* auf die Schaltfläche *Start*.

AntiVir nimmt Kontakt mit dem Internetserver der Firma H+BEDV auf und prüft, ob neue Updates vorliegen.

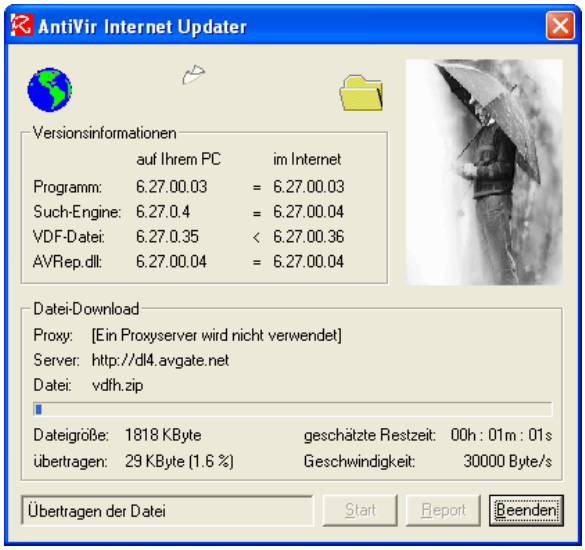
Sind keine Updates vorhanden, wird dieses Dialogfeld angezeigt. Sie können das Programm dann über die *Ja*-Schaltfläche schließen.

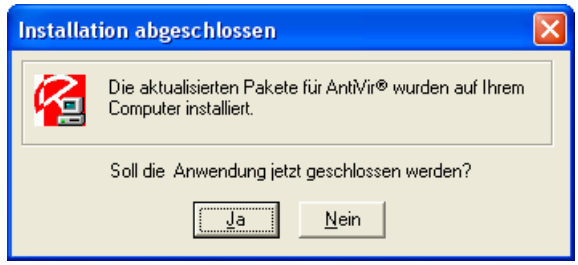




4 Wurde ein Update gefunden, erscheint dieses Dialogfeld und Sie können das Update über die *Ja*-Schaltfläche starten.

AntiVir beginnt dann mit dem Herunterladen der erforderlichen Daten. Je nach Übertragungsgeschwindigkeit kann dies einige Minuten dauern. Allerdings umfasst ein Update meist wesentlich weniger Daten als der Download der AntiVir-Installationsdatei. Eine Fortschrittsanzeige im Dialogfeld informiert Sie über den Ablauf.





5 Sobald dieses Dialogfeld erscheint, klicken Sie auf die *Ja*-Schaltfläche.

Mit diesem letzten Schritt wird das Dialogfeld geschlossen und das Update von AntiVir ist damit beendet. Spätestens nach dem nächsten Windows-Start sollte die AntiVir-Warnung vor veralteten Signaturdateien sowie die Warnung des Sicherheitscenters verschwunden sein.

So wird ein Virenbefall gemeldet

Wenn AntiVir korrekt installiert wurde, ist auch der Virenwächter AntiVir Guard aktiv. Sie erkennen dies an dem kleinen Symbol im Infobereich der Taskleiste. Dieses Programm überwacht alle Ihre Zugriffsversuche auf Dateien. Sobald Sie eine mit einem Virus, Wurm oder Trojaner infizierte Datei per Doppelklick öffnen bzw. ausführen, blockiert AntiVir dies und zeigt einen Warndialog. Im oberen Teil des Dialogfelds erhalten Sie einen Hinweis, welcher Schädling gefunden wurde. Zudem zeigt AntiVir Ihnen den Pfad zur Datei an. Allerdings wird diese Angabe bei längeren Pfadnamen meist abgeschnitten.

1 Wählen Sie nun eine der gewünschten Optionen, indem Sie auf das betreffende Optionsfeld der Gruppe *Was soll mit der Datei geschehen?* klicken.

2 Bestätigen Sie diese Auswahl durch Anklicken der *OK*-Schaltfläche.

Bezüglich der auszuwählenden Optionen im Dialogfeld können Sie sich an folgenden Empfehlungen orientieren:

- Haben Sie die infizierte Datei gerade aus dem Internet heruntergeladen, per E-Mail erhalten oder über einen Datenträger (Diskette) bekommen, sollten Sie die Option *Betroffene Datei löschen* wählen. Dann wird die Datei vom Rechner entfernt – sicher ist sicher.
- Meldet AntiVir oder der Virenwächter AntiVir Guard während des laufenden Betriebs ein Virus (ohne dass Sie eine Datei geöffnet haben) oder benötigen Sie eine infizierte Dokumentdatei dringend, können Sie die Option *Betroffene Datei reparieren (Standard)* anklicken. Mit etwas Glück kann AntiVir das Virus entfernen und die Datei retten.
- Die Option *Zugriff erlauben und Datei belassen* sollten Sie nur mit allergrößter Vorsicht verwenden. Nur wenn Sie sicher sind, dass

AntiVir einen Fehlalarm auslöst (z. B. bei einer Dokumentdatei mit integriertem Makro, welches mit Sicherheit kein Virus enthält), können Sie die Option wählen.

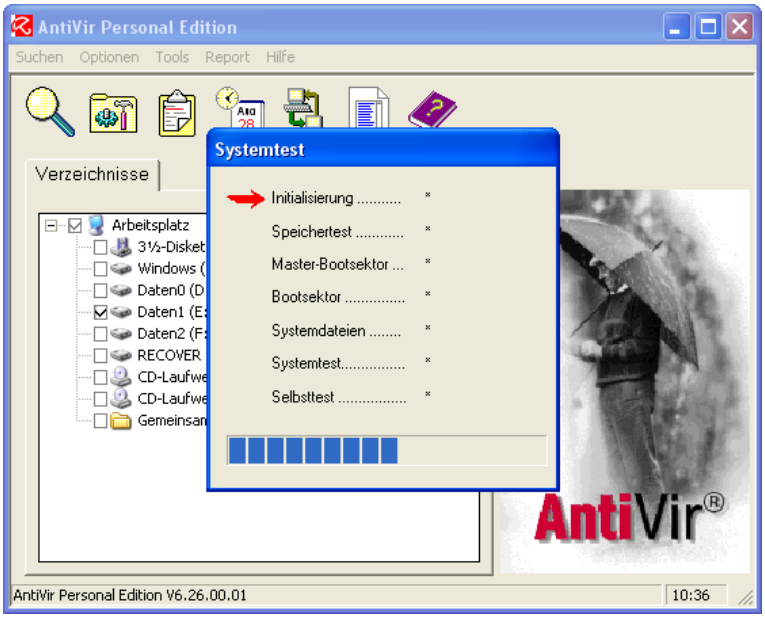
Auf die Option *Betroffene Datei in das Quarantäneverzeichnis verschieben* sollten Sie verzichten, da dann die infizierten Dateien im AntiVir-Programmordner gespeichert werden. Dies führt dazu, dass die infizierten Dateien weiter auf der Festplatte bleiben und dort Speicherplatz belegen. Ein Entfernen ist nur erfahrenen Benutzern, die unter einem Administratorenkonto angemeldet sind, möglich. Auch Optionen wie *Zugriff verweigern und Datei belassen* oder *Betroffene Datei umbenennen* sollten nur von wirklich erfahrenen Benutzern gewählt werden. Diese Optionen erlauben ggf., die befallene Datei weiter zu analysieren.

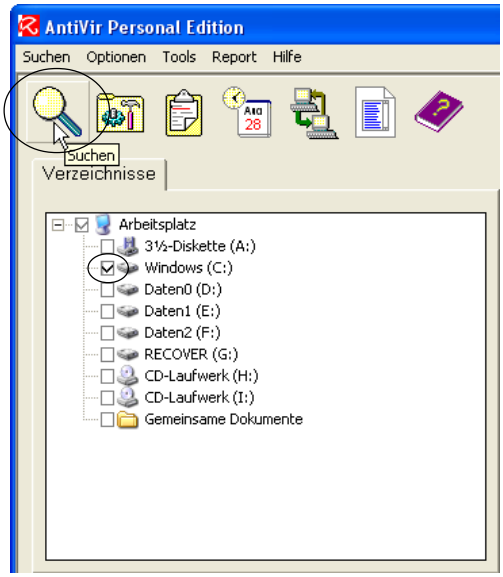
So überprüfen Sie ganze Laufwerke

Um einen Datenträger oder die Festplatten des Computers auf Schädlinge wie Viren, Trojaner etc. zu überprüfen, lässt sich das AntiVir-Hauptmodul verwenden.

1 Starten Sie das AntiVir-Hauptprogramm. Dies kann über das Desktop-Symbol, über den Eintrag im Startmenü oder über den Befehl *AntiVir Hauptprogramm starten* im Kontextmenü des AntiVir Guard-Moduls erfolgen.

2 Nachdem das AntiVir-Hauptfenster erscheint, wird ein Systemtest durchgeführt. Dieser Test soll sicherstellen, dass keine Viren im Arbeitsspeicher oder im Bootbereich vorhanden sind. Warten Sie, bis der Test abgeschlossen ist und das Dialogfeld *Systemtest* geschlossen wird.





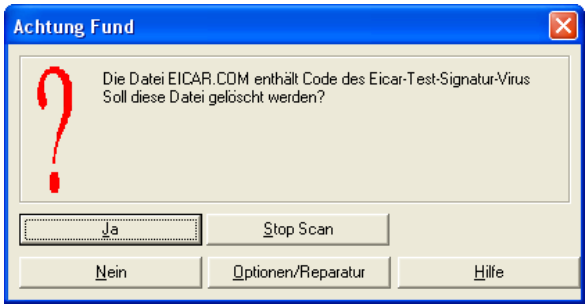
3 Markieren Sie nun im AntiVir-Fenster die Kontrollkästchen der Laufwerke, die auf Viren zu prüfen sind (die Kontrollkästchen anklicken, damit diese ein Häkchen aufweisen, ein zweiter Mausklick auf das Kontrollkästchen löscht das Häkchen wieder). - - - - ►

4 Klicken Sie in der Symbolleiste des AntiVir-Fensters auf die Schaltfläche *Suchen*.

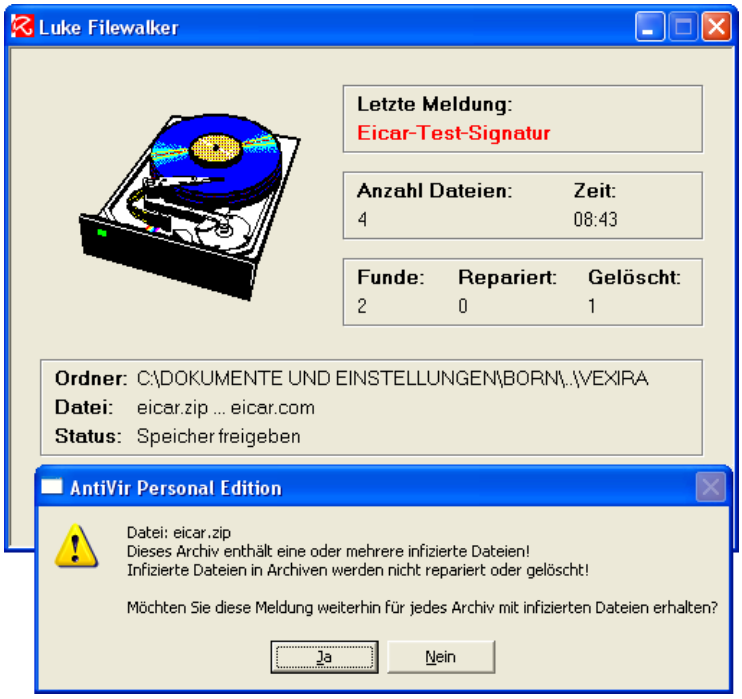
AntiVir startet den bereits bekannten Luke Filewalker, der die Dateien des angegebenen Laufwerks auf Viren und sonstige Schädlinge untersucht. Der Fortschritt wird in einem eigenen Dialogfeld angezeigt.

Findet Luke Filewalker ein Virus oder einen anderen Schädling, werden Sie gewarnt. Die Details des Warndialogs sowie die weiteren Reaktionen hängen von der Art der infizierten Datei und vom Schädling ab.

- **Wird** eine **befallene Datei gefunden**, erscheint das Dialogfeld *Achtung Fund*. AntiVir gibt Ihnen dann die Gelegenheit, die **infizierte Datei** zu **löschen** oder zu **reparieren**. Welche Option angeboten wird, hängt von der Art des gefundenen Schädlings ab. Bei Makroviren bietet AntiVir z. B. die Reparatur an. Sobald Sie auf die *Ja*-Schaltfläche klicken, wird die befallene Datei gelöscht bzw. repariert. Die *Nein*-Schaltfläche sollte nur von erfahrenen Benutzern gewählt werden, da die infizierte Datei auf dem Computer verbleibt. Eine solche Option ist z. B. sinnvoll, um die infizierten Dateien weiter zu analysieren. Bei einem Befall durch einen Wurm können sich erfahrene Anwender beispielsweise über einen separaten Rechner per Internet Programme zum Entfernen des Schädlings herunterladen.



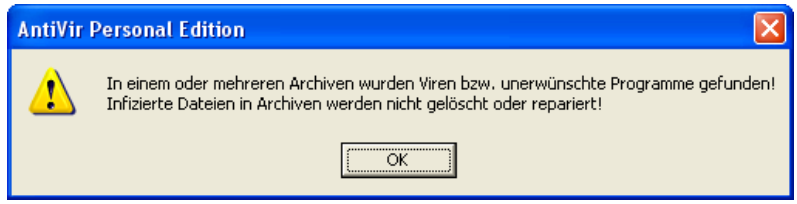
- AntiVir überprüft i. d. R. auch Dateien, die in komprimierten Archiven (ZIP-Archiven etc.) hinterlegt sind. Infizierte Dateien in diesen Archiven lassen sich aber nicht reparieren oder entfernen. Sie erhalten dann lediglich eine Warnung über ein Dialogfeld. Solange dieses Dialogfeld im Vordergrund geöffnet ist, können Sie im Luke Filewalker-Fenster den Ordner sowie den Namen der befallenen Datei sowie den Typ des Virus ablesen (hier sind beide Dialogfelder zu sehen). Wenn Sie die *Ja*-Schaltfläche betätigen, setzt der Virenscanner die Analyse weiterer Dateien fort.



HINWEIS

Auf der Vexira-Webseite *www.centralcommand.com/downloads.html* finden Sie übrigens eine Testdatei *Eicar.zip*. Dieses ZIP-Archiv enthält eine Test-Signatur, die von aktuellen Virenscannern erkannt werden sollte. In den hier gezeigten Dialogen wurde das betreffende Virus erkannt.

Sie sollten die Analyse des Datenträgers komplett durchlaufen lassen und Virenfunde über die *Ja*-Schaltfläche bestätigen. Konnte AntiVir die befallenen Dateien nicht reparieren oder löschen (z. B. bei ZIP-Archiven), erhalten Sie in einem Dialogfeld eine entsprechende Warnung angezeigt.



Sie sollten sich bereits während der Virenprüfung die Namen und die Ordner der befallenen Archive bzw. Dateien notieren. Anschließend müssen Sie die betreffenden Dateien nach der Virenprüfung manuell löschen.

Zum Abschluss eines Scans gibt AntiVir Ihnen im Dialogfeld *Status* noch einen Überblick über den Befall und die Zahl der reparierten bzw. gelöschten Dateien. Über die Schaltfläche *Report* können Sie eine genaue Übersicht über die Virenfunde abrufen. Mit der *OK*-Schaltfläche lässt sich das Dialogfeld schließen.

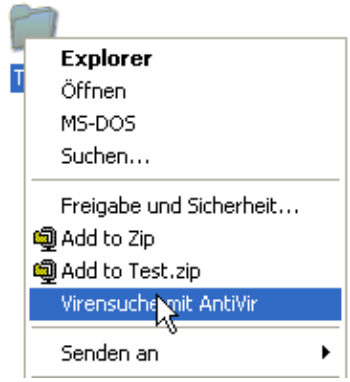
ACHTUNG

Falls ein Befall durch Viren, Trojaner, Würmer oder andere Schädlinge von AntiVir festgestellt wurde, können Sie die infizierten Dateien reparieren oder löschen lassen. Es empfiehlt sich, anschließend das System über eine Notfall-CD oder einen Notfall-Diskettensatz (siehe vorhergehende Seiten) zu starten und von einem separaten Virenscanner analysieren zu lassen. Dies stellt sicher, dass ein Virus durch einen blockierten Virenscanner nicht unerkannt bleibt. Weiterhin sollten Sie nach einem Befall Ihr System ausgiebig testen. Reparierte oder gelöschte Dateien können dazu führen, dass Windows XP selbst, Anwendungen oder Dokumentdateien nicht mehr korrekt funktionieren. Spätestens an dieser Stelle zahlt es sich aus, wenn Sie virenfreie Sicherungskopien der wichtigsten Dokumentdateien besitzen. Wurden Programme befallen, müssen Sie diese ggf. von den Original-CDs neu installieren oder reparieren lassen. Ist Windows XP beschädigt, müssen Sie das komplette Betriebssystem ggf. von der Installations-CD neu aufspielen. Falls Sie sich diese Aufgabe nicht zutrauen, lassen Sie sich von erfahrenen Benutzern oder Experten helfen.

So prüfen Sie Ordner oder Dateien

Möchten Sie lediglich eine einzelne Datei oder den Inhalt eines Ordners überprüfen, finden im AntiVir-Hauptmodul aber nur die Möglichkeit, komplette Laufwerke auszuwählen? Mit den folgenden Schritten geht es dennoch:

1 Um Ordner oder Einzeldateien zu prüfen, klicken Sie diese mit der rechten Maustaste im Ordnerfenster an.



2 Anschließend wählen Sie im Kontextmenü den Befehl *Virensuche mit AntiVir*.

Der weitere Ablauf entspricht der Beschreibung im vorhergehenden Abschnitt. Nachdem der Selbsttest abgeschlossen wurde, prüft AntiVir den Inhalt des angegebenen Ordners oder der Datei. Werden Viren gefunden, wird dies, wie oben beschrieben, gemeldet. Sie können dann die befallenen Dateien löschen oder reparieren lassen.

TIPP

Wenn Sie im AntiVir-Fenster das Menü *Tools* öffnen und den Befehl *Vireninformationen* wählen, öffnet das Programm eine Hilfeseite. Auf dieser Hilfeseite finden Sie zusätzliche Informationen über die Wirkungsweise der von AntiVir erkannten Schädlinge.

So überprüfen Sie Bootsektoren mit AntiVir

Haben Sie den Verdacht, dass das System von einem Bootvirus befallen ist? Oder möchten Sie Datenträger wie Disketten auf Bootviren prüfen?

1 Legen Sie ggf. den Datenträger in ein Laufwerk ein, starten Sie das AntiVir-Hauptprogramm (z. B. über das Desktop-Symbol) und warten Sie, bis AntiVir den Selbsttest durchgeführt hat.

2 Anschließend wählen Sie im AntiVir-Fenster im Menü *Suchen* den Befehl *Bootsektoren*.

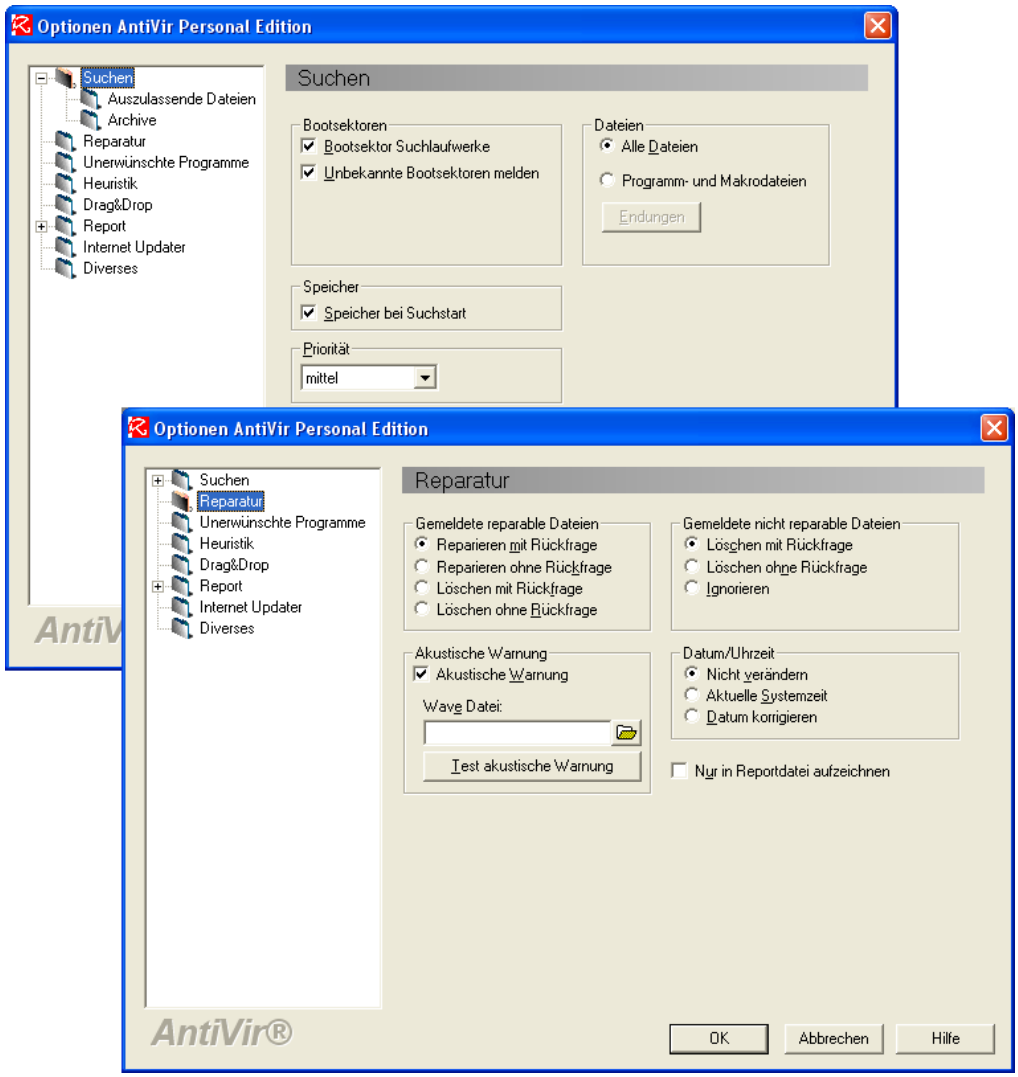
3 Markieren Sie das gewünschte Laufwerk und klicken Sie anschließend auf die *Suchen*-Schaltfläche.

AntiVir wird dann eine Prüfung des Laufwerks auf Bootviren durchführen. Gefundene Bootviren werden gemeldet und lassen sich, je nach Datenträger (z. B. von Disketten) auch entfernen. Ist aber der Master Boot Record des Systemlaufwerks befallen, müssen Sie den Bootsektor manuell wiederherstellen (siehe weiter oben im Abschnitt »Achtung bei Befall durch Bootviren«).

Hier passen Sie die AntiVir-Einstellungen an

Standardmäßig wird AntiVir so installiert und eingerichtet, dass Sie als normaler Benutzer damit arbeiten können. Sofern Sie nur über wenig Erfahrung verfügen, belassen Sie einfach diese Einstellungen. Erfahrenere Benutzer können aber im AntiVir-Fenster das Menü *Optionen* öffnen und dann den Befehl *Konfigurationsmenü* wählen. AntiVir öffnet das hier gezeigte Dialogfeld, in dem Sie die verfügbaren Optionen ansehen und anpassen können. Die Optionen sind dabei in verschiedene Kategorien unterteilt. Eine Kategorie erreichen Sie, indem Sie in der linken Spalte des Dialogfelds auf das betreffende Ordnersymbol klicken. Anschließend können Sie im rechten Teil des Dialogfelds die verfügbaren Optionen ansehen.

Benötigen Sie Informationen zu den angezeigten Optionen, klicken Sie auf die *Hilfe*-Schaltfläche des Dialogfelds. Das dann eingeblendete Hilfefenster enthält Informationen zu den einzelnen Optionen.



Zusammenfassung

Nun kennen Sie die Verbreitungswege von Viren und anderen Schädlingen. Sie haben zudem gelernt, wie Sie Antivirenprogramme einsetzen und wo Sie diese aus dem Internet herunterladen können. Neben den hier beschriebenen Virenscannern gibt es weitere Alternativen. In Kapitel 6 wird beispielsweise eine Sicherheitslösung von Symantec vorgestellt, die einen integrierten Virenscanner beinhaltet.

Testen Sie Ihr Wissen

Zur Überprüfung Ihrer Kenntnisse können Sie die folgenden Fragen beantworten:

- **Nennen Sie Virenarten.**
  (Programmviren, Bootviren, Makroviren, Scriptviren.)
- **Wie erkennt man Viren?**
  (Indem man den Rechner durch ein aktuelles Virenschutzprogramm prüfen lässt.)
- **Was ist bei Virenschutzprogrammen zu beachten?**
  (Diese sollten Windows XP mit Service Pack 2 unterstützen und aktuell sein.)