Profi-Tips zur Virenabwehr

KEINE ANGST VOR VIREN

Seien Sie vorsichtig! Dann läßt sich die Gefahr einer Infektion nämlich wesentlich reduzieren. Und auch im Fall des Falles verhindert besonnenes Verhalten meist größere Schäden

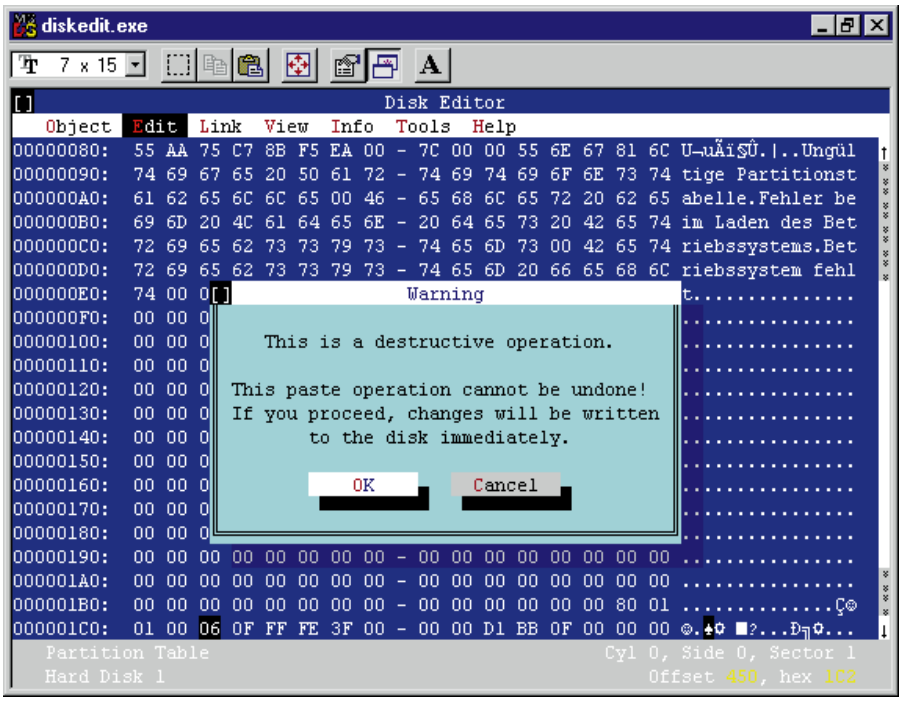
ILLUSTRATION: JOHNNY HÖRMANNSDORFER

Erwiesenermaßen resultieren massive Datenverluste nach einem Virenbefall meist nicht direkt aus der Schadensfunktion (dem „Payload“) des Virus, sondern aus panikartigen Überreaktionen der Betroffenen. Da wird wegen eines eher harmlosen Virus schon mal die Festplatte neu formatiert, nur weil der erste Säuberungsversuch gescheitert ist.

Bevor Sie derart drastische Maßnahmen einleiten, sollten Sie immer eines bedenken: Das primäre Ziel eines Virus ist die Fortpflanzung; die Schadensfunktion – sofern vorhanden – steht immer erst an zweiter Stelle. Das heißt vor allem, daß Sie Zeit haben: Zeit, Daten und nicht infizierte Programme zu sichern, Zeit, sachlich über die besten Desinfektionsmethoden nachzudenken, und Zeit, sich die erforderlichen Werkzeuge notfalls nachträglich zu besorgen. Unser Beitrag zeigt, daß in vielen Fällen sogar der – richtige – Einsatz von DOS-Bordmitteln ausreicht.

Am besten ist es freilich, wenn Sie über die korrekte Virenentsorgung erst gar nicht nachdenken müssen. Den Schwerpunkt dieses Beitrags bilden daher Verhaltensregeln zur Vorbeugung. Durch deren Einhaltung können Sie einen Virenbefall von vornherein vermeiden oder diese Gefahr zumindest entscheidend vermindern. In diesem Zusammenhang soll allerdings auch klar zur Sprache kommen, was jeder PC-Anwender unbesorgt tun darf: Einige Mythen hinsichtlich der Allmacht von PC-Viren verunsichern die Anwender unnötig und sollten daher vom Tisch.

Rainer Bumke / ha



Zurückschreiben des gesicherten Master Boot Record: Der Diskeditor warnt vor der Aktion, aber sie ist bisweilen der letzte Rettungsanker (Tip 5)

1. Infektionssymptome

Was sind typische und gut verifizierbare Anzeichen für aktive Viren?

PC-Viren können die unterschiedlichsten Schadenswirkungen hervorrufen: Schwierigkeiten beim Booten, Festplattenprobleme, verminderte Rechnerleistung, Fehlermeldungen und Abstürze. Die Auswirkungen der Vireninfektionen sind in der Regel viel zu heterogen und auch zu unspezifisch, als daß Sie gleich aus bestimmten Indizien sicher auf einen aktiven Virus schließen können – wenngleich im Zweifelsfall ein Virus-Scan natürlich stets angesagt ist.

Spezifischer und gut nachzuprüfen sind folgende Symptome:

1. Jeder aktive Virus benötigt etwas Speicher: Verringert sich der DOS-Arbeitsspeicher, ohne daß Sie die Konfiguration geändert haben, dann ist das ein deutliches Indiz für einen Befall mit Datei- oder Bootsektorviren. Auf einen Bootsektorvirus deutet hin, wenn der DOS-Speicher generell weniger als 640 KB umfaßt (ein Wert von exakt 639 KB kann allerdings auch auf Bios-Einstellungen zurückgehen).

2. Viele Viren überschreiben keinen Wirtscode, sondern hängen sich an das Wirtsprogramm an. Veränderte Dateigrößen von COM- und EXE-Programmen sind daher ein äußerst verdächtiges Anzeichen für Viren.

3. Diverse Viren markieren bereits infizierte Dateien durch eine Änderung der Zeitangaben. Da es in der Gruppe der Standard-Software jedoch nur sehr wenige selbstmodifizierende Programme gibt, verweisen solche Änderungen ebenfalls deutlich auf Virenaktivität.

4. Die Schadenswirkung vieler Viren besteht im Löschen von Dateien. Solche Löschaktionen lassen sich wie die vorher genannten Änderungen im Dateisystem anhand von vergleichenden DIR-Listen relativ leicht nachvollziehen.

5. Bootsektorviren verhindern häufig den 32-Bit-Dateizugriff unter Windows 3.11 oder 95. Kommt es beim Start von Windows unvermittelt und ohne Konfigurationsänderung zu einer entsprechenden Fehlermeldung, ist häufig ein Bootsektorvirus die Ursache.

2. Warmstart

Entfernt <Strg>-<Alt>-<Entf> jeden Virus aus dem Speicher?

Eigentlich ja. Ein Warmstart löscht den Arbeitsspeicher und damit auch jeden speicherresidenten Virus. Das Problem ist nur, daß Sie nach einer Vireninfektion nicht sicher sein können, daß das, was Sie als Warmstart erleben, tatsächlich ein Warmstart ist!

Einige Viren kontrollieren den Tastatur-Interrupt und simulieren bei <Strg>-<Alt>-<Entf> einen Warmstart, der sie am Leben läßt. Wählen Sie also besser gleich einen Weg, bei dem einem resi-

Virenvermeidung und Virenbekämpfung

Profi-Tips zur Virenabwehr

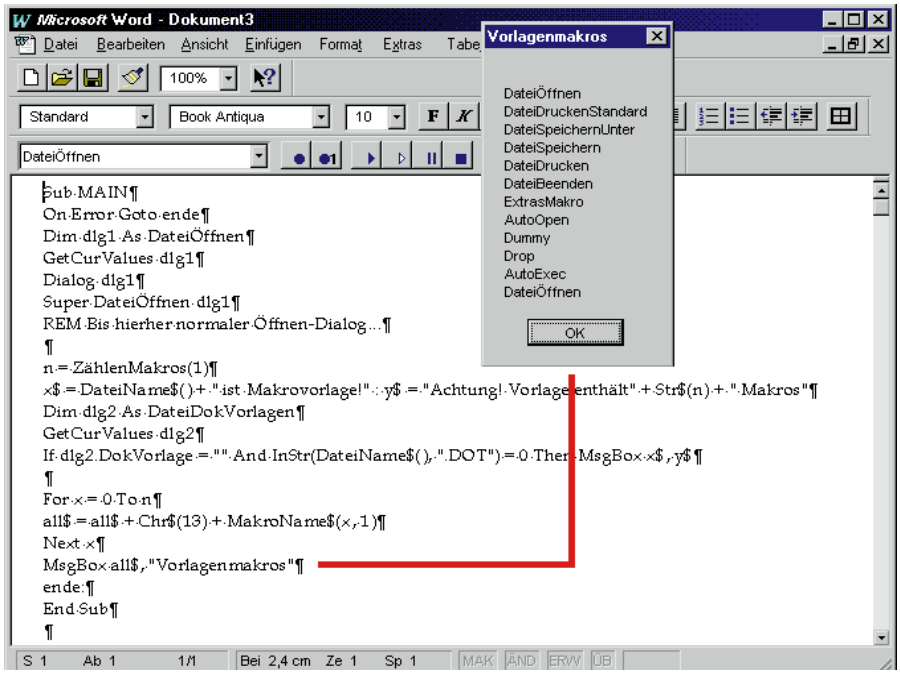
denten Virus keine Abwehrmöglichkeit bleibt: Drücken Sie auf den Reset-Knopf, oder schalten Sie den PC ganz aus.

3. Rettungsanker

Welche Programme sollte eine sinnvolle Bootdiskette enthalten?

Diese Frage ist vor allem für DOS- und Windows-3.1x-Anwender relevant. Was der SYS-Befehl leistet oder das noch dürftigere „Systemdatenträger erstellen“ im Datei-Manager, ist völlig unzureichend. Mit solchen Bootdisketten können Sie zwar das System starten, aber nichts reparieren. Die Programme Sys, Fdisk, Format, Scandisk, Mem, Undelete, Attrib, Xcopy (eventuell zusätzlich ein Packer-Utilitiy) sollten Sie noch per Hand auf die Diskette kopieren.

Windows-95-Anwender sind ganz gut beraten, wenn sie sich über „Systemsteuerung, Software“ eine Startdiskette erstellen lassen: Hier ist an alles Lebensnotwendige gedacht. Was dann aber noch fehlt, ist der obligate Virenscanner. Wenn der Platz der Bootdiskette dafür ausreicht, sollten Sie ihn dorthin kopieren – oder Sie erstellen eine zweite saubere Diskette mit dem Antiviren-Programm und versehen diese dann ebenfalls mit Schreibschutz.



Text mit Nemesis-Virus: Der abgebildete Code für „DateiÖffnen“ warnt Sie vor getarnten Makrovorlagen und zeigt die Makros an (Tip 7)

4. Bios-Schutz

Was nützt Ihnen die Bios-Option „Bootsector Virus Protection“?

Manche Bios-Versionen enthalten die vielversprechende Option „Bootsector Virus Protection“. Diese Option überwacht jeden Schreibzugriff auf den Bootsektor und stoppt gegebenenfalls das System. Sie erhalten dann eine englischsprachige Warnung vor einem Virenbefall. Diese Option schützt daher gegen Bootsektorviren – aber natürlich nicht gegen Dateiviren.

Schutz gegen Bootsektorviren – das klingt gut, hat aber auch seine Schattenseiten: Die genannte Bios-Funktion ist wirksam, aber primitiv und unflexibel; sie geht rigoros davon aus, daß ein Bootsektor unveränderlich zu sein hat. Folglich führt auch schon ein harmloser Label-Befehl („label c:“) zu einer irritierenden Virenmeldung. Je nach Betriebssystem ist daher mit häufigeren Fehlalarmen zu rechnen, die vor allem unerfahrene Anwender nicht richtig zu interpretieren wissen. Hinzu kommt, daß dieser Bios-Schutz gut dokumentiert ist. Inzwischen gibt es einige Viren, die ihn deaktivieren können.

5. Bootsektoren sichern

Von Ihren Daten besitzen Sie Backups – doch wie kommen Sie an Sicherheitskopien der beiden Bootsektoren?

Die meisten Antiviren-Programme enthalten eine entsprechende Option. Er-

Verwenden Sie ein Antiviren-Programm!

AVP

Anbieter: Shareware-Versender, etwa SMM, Budenheim, Tel. 06139/916916
Preis: Registrierung inklusive Updates für ein Jahr 59 Mark

DR. SOLOMON'S ANTIVIRUS-TOOLKIT

Anbieter: S&S Deutschland, Hamburg, Tel. 040/2519540, Fax 040/25195450
Preis: ab 69 Mark (Emergency-Toolkit)

F-PROT FÜR DOS

Anbieter: Shareware-Versender, etwa SMM, Budenheim, Tel. 06139/916916
Preis: für Privatnutzung kostenlos

MCAFEE SCAN

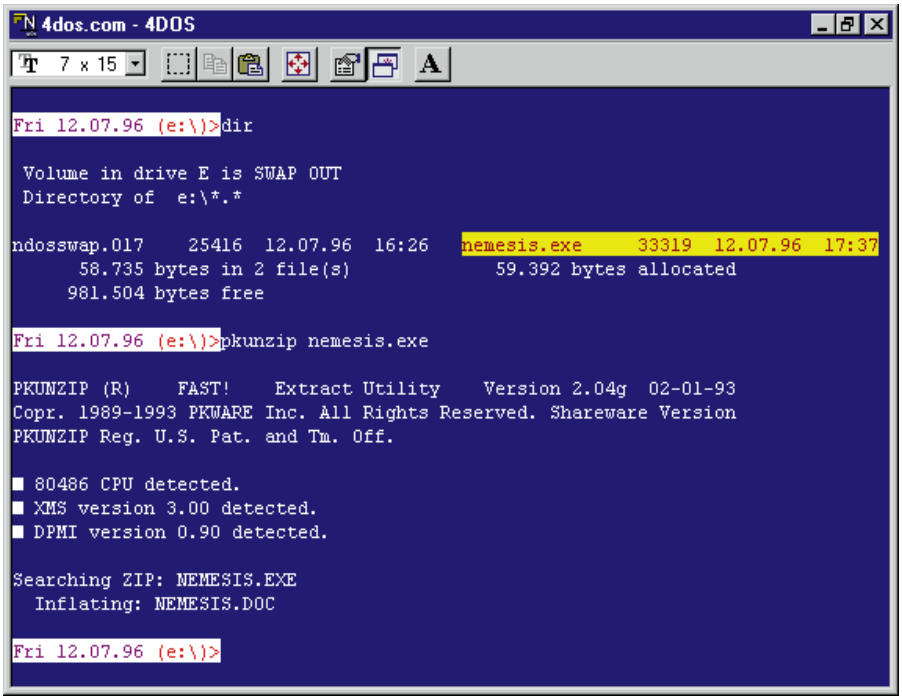
Anbieter: McAfee, Germering, Tel. 089/8943560, Fax 089/89435699
Preis: 123 Mark inklusive Updates für zwei Jahre (Mailbox/Internet); Demoversionen kostenlos im Internet

TBAV

Anbieter: Shareware-Versender, etwa SMM, Budenheim, Tel. 06139/916916
Preis: Registrierung 99 Mark

Demo- und Shareware-Versionen aller Scanner finden Sie auch im Internet unter http://www.valleynet.com/~joe/

fahrene Anwender können dafür aber auch einen Diskeditor wie Nortons Diskedit nutzen.
So setzen Sie Nortons Diskedit ein: Wählen Sie unter „Objekt, Laufwerk“ das Bootlaufwerk C: und dann „Objekt, Partitionstabelle“. Mit <F2> wechseln Sie in die HEX-Darstellung. Markieren Sie nun zunächst mit „Bearbeiten, Markieren“ den kompletten Sektor, um ihn dann mit „Bearbeiten, Kopieren“ abzubilden.
Unter „Werkzeuge, Schreibe Objekt auf“ geben Sie anschließend eine Zieldatei an. Am besten ist es, diese kleine Datei ebenfalls auf der Bootdiskette abzulegen, etwa als MBR.SEC.
Die gleiche Prozedur sollten Sie danach mit dem „Objekt“ Bootsektor wiederholen. Wenn Sie nun diese Sicherungsdaten mit DIR ansehen, müssen sie genau 512 Bytes groß sein.
Sollte das Zurückschreiben dieser beiden Sektoren notwendig werden, laden Sie zuerst das jeweilige Dateiobjekt, kopieren die HEX-Ansicht, laden dann den benötigten Sektor und wählen „Bearbeiten, Überschreiben“.



Selbstentpackendes EXE-Archiv: Sie können auch die normale Entpack-Routine verwenden, um die Virengefahr zu reduzieren (Tip 8)

6. Datei-Schreibschutz
Sind per Attribut schreibgeschützte Dateien sicher vor Vireninfektionen?

Der Glaube, mit „attrib +r ...“ oder gar mit „attrib +r +s +h ...“ geschützte Dateien seien sicher vor Viren, ist weit verbreitet. Tatsache ist, daß Virenprogrammierer sich genau der gleichen Software-Funktionen bedienen können wie Sie. Folglich kann ein Virus sowohl die Funktionen eines Standarddienstprogramms wie Attrib nutzen als auch selbst in das Dateisystem eingreifen. Attrib & Co. sind kein wirksamer Schutz vor Infektionen!
Andererseits beziehen die wenigsten Virenprogrammierer tatsächlich alle Eventualitäten der Systemkonfiguration mit ein, die ihr Virus später möglicherweise einmal antreffen könnte. Ein Software-Schreibschutz wird daher eine Vielzahl von Viren abhalten, weil in ihrem Programmcode diese Möglichkeit jeweils nicht berücksichtigt ist.
Haben Sie allerdings umfangreiche Schreibschutz-Maßnahmen vorgesehen, müssen Sie selbst mit diversen Problemen und Fehlermeldungen rechnen.

7. Dokumentviren in Textprogrammen
Wie schützen Sie sich am besten vor Winword-Makroviren?

Wollen Sie ganz sicher gehen, lesen Sie Textdateien unbekannter Herkunft einfach mit Viewer oder Editor ohne Makrofunktionen. Wenn Sie nur wissen wollen, was eine Datei im Netz enthält, reicht diese wenig elegante, aber absolut wirksame Methode völlig aus.
Anders steht es, wenn Sie fremde Texte auswerten oder weiterbearbeiten wollen. Dann benötigen Sie ein vollwertiges Textprogramm, das aber für den Fall des Falles präpariert sein sollte. Den automatischen Start von Winword-Autoopen-Makros können Sie verhindern, indem Sie ein Makro „Autoexec“ in der Standard-Dokumentvorlage „Normal“ eintragen, das den folgenden einschlägigen Makrobefehl enthält (Winword 6/7):

```
Sub Main
AutoMakroUnterdrücken 1
End Sub
```

Es ist allerdings längst nachgewiesen, daß sich damit kein kompletter Schutz erreichen läßt:
Einige Makroviren benutzen keine Autoopen-Makros, sondern besetzen einfach bestimmte Standardbefehle, die der Anwender höchstwahrscheinlich ausführen wird (etwa „DateiSchließen“), mit ihren Instruktionen. Sie brauchen also beides – sowohl den Schutz gegen selbststartende Makros als auch eine Warnung vor weiteren enthaltenen Makros. Diese Warnung erhalten Sie, wenn Sie den in der Abbildung wiedergegebenen Code als „DateiÖffnen“-Makro in alle häufig benutzten Dokumentvorlagen ablegen. Eine Ablage in der Dokumentvorlage NORMAL.DOT genügt lediglich dann, wenn Sie Dateien nur über das entsprechende Menü öffnen, nicht aber per Doppelklick im Programm-Manager beziehungsweise im Explorer.
Das „DateiÖffnen“-Makro interpretiert jede Makrovorlage, die nicht die dafür vorgesehene Endung DOT hat, als Virenträger und informiert auch gleich über die enthaltenen Makros. Beim Öffnen normaler Texte werden Sie nicht

Virenvermeidung und Virenbekämpfung

Profi-Tips zur Virenabwehr

belästigt. Die meisten Makroviren, etwa der bekannte Word.Concept, werden übrigens von den gängigen DOS-Antiviren-Programmen erkannt. Und diese Antiviren-Programme können die Makroviren auch entfernen.

8. Komprimierte Dateien

Welche Regeln gelten für gepackte Archive und selbstentpackende EXE-Dateien?

Da kein Virenscanner zuverlässig alle Arten gepackter Archive auf Virenbefall untersuchen kann, empfiehlt sich grundsätzlich folgende Vorgehensweise: ZIP, ARJ & Co.: Scannen Sie nicht das Archiv, sondern entpacken Sie zunächst das Archiv in ein leeres Verzeichnis, und scannen Sie dann die entpackten Dateien. Vergessen Sie nicht, neben den entpackten Daten auch das Ursprungsarchiv umgehend zu löschen, sofern sich eine der entpackten Dateien als virenverseucht erweist!

Selbstentpackende EXE-Archive unbekannter Herkunft sind doppelt gefährlich: Zum einen kann die EXE-Datei selbst einen Virus enthalten, zum anderen können die komprimierten Dateien infiziert sein. Solche EXE-Archive sollten Sie immer – wie übrigens jede fremde ausführbare Datei – vor dem Aufruf scannen, und nach dem Entpacken ist ein weiterer Suchlauf über die entpackten Dateien angesagt. Auch hier gilt wieder: Ist eine der Archivdateien infiziert, entfernen Sie diese zusammen mit dem EXE-Archiv.

Ganz Vorsichtige können übrigens auf die Dienste des EXE-Headers ganz verzichten: Ein mit Zip2Exe als EXE-Datei abgelegtes ZIP-Archiv läßt sich jederzeit auch mit Pkunzip entpacken. Das einzige kleine Problem besteht darin, zunächst den verantwortlichen Packer des EXE-Archivs festzustellen. Wenn Sie ein mit ARJ gepacktes EXE-Archiv mit Pkunzip behandeln wollen, erhalten Sie natürlich eine Fehlermeldung.

9. Ansi-Bomben

Wie können Sie sich vor Ansi-Bomben schützen?

Ansi-Bomben besitzen zwar nicht die Fähigkeit, sich zu vermehren, können aber durch Umbelegen von Standardtasten erheblichen Schaden anrichten. Wer nicht recht weiß, wozu der Treiber ANSI.SYS in der CONFIG.SYS gut ist, sollte ihn dort einfach löschen oder mit Semikolon auskommentieren.

Anwendern, die ANSI.SYS wirklich brauchen, wird folgende knappe Anweisung genügen: Laden Sie ANSI.SYS in einen Diskeditor, zum Beispiel in den Norton Diskeditor:

```
diskedit c:\dos\ansi.sys
```

Suchen Sie dort das Byte 61h. Dort steht „70“, also dezimal „112“ – der Ascii-Wert für „p“. „p“ ist das Standardzeichen von ANSI.SYS für Tastaturumbelegungen. Tragen Sie dort einen anderen Wert ein. Wenn Sie „70“ etwa durch „74“ ersetzen, wird statt „p“ nun das „t“ zum Umbelegungszeichen. Nach diesem Patch des Ansi-Treibers haben Ansi-Bomben keine Chance mehr.

10. Infektionsgefahr durchs Kopieren?

Können Sie bereits durch das bloße Kopieren von Daten einen Virus in Ihr System einschleusen?

Nein. Weder ein Kopiervorgang mit Copy, Xcopy, Backup, Pkzip noch eine Download-Aktion innerhalb einer DFÜ-Verbindung aktiviert direkt einen Virus – selbst dann nicht, wenn der sendende Datenträger infiziert ist. Haben Sie jedoch eine infizierte Datei kopiert oder auf Ihren PC übertragen und rufen Sie sie auf, dann wird der Virus aktiv.

11. Mit Viren infizierte CD-ROMs

Kann es passieren, daß Sie beim Einlesen von CDs einen Virus aktivieren?

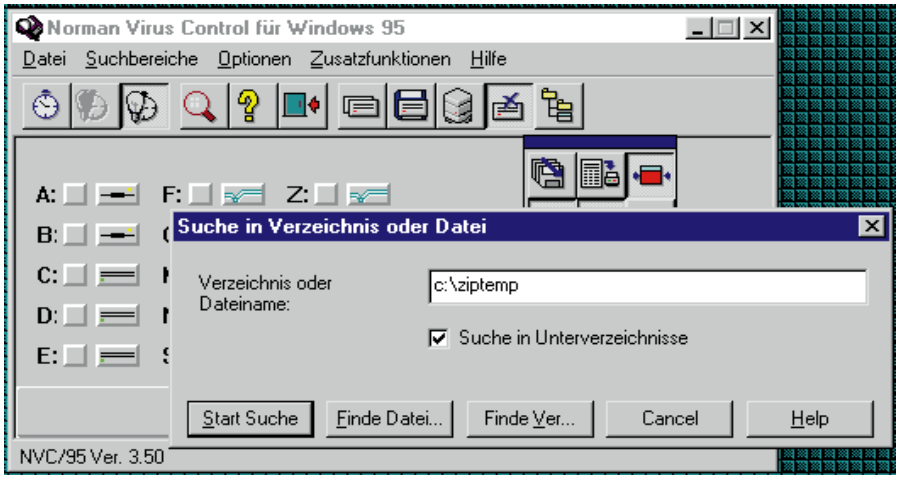
An sich nein. Unter Windows 95 gilt jedoch: ja, wenn auch auf indirektem Weg. Windows 95 kommt mit der sogenannten „Autoplay“-Funktion – einer Spielerei, die beim Anklicken des CD-Icons automatisch ein beliebiges, in der AUTORUN.INF definiertes Programm startet. Wenn das aufgerufene Programm ein DOS-Programm ist und einen Dateivirus enthält, droht eine Infektion.

Bei Installations-CDs von Standard-Software ist dieser Fall auszuschließen. Was heute theoretisch erscheint, könnte aber bei zunehmender Verbreitung der inzwischen erschwinglichen CD-Brenner zu einer massiven Bedrohung führen. Näheres zu „Autoplay“ und zur Gegenmaßnahme siehe Windows-Tips, Nummer 43–45 in dieser PC-WELT auf Seite 64.

12. Virenscanner – wie häufig?

Wie oft sollten Sie Ihren Virenscanner einsetzen, und mit welchen Optionen?

Auf einem Netzwerk-Server, der jederzeit und von beliebigen Usern Daten



Schnelles Scannen von neu erhaltenen Dateien: Alle Scanner unterstützen die Auswahl von bestimmten Verzeichnissen (Tip 12)

Virenvermeidung und Virenbekämpfung

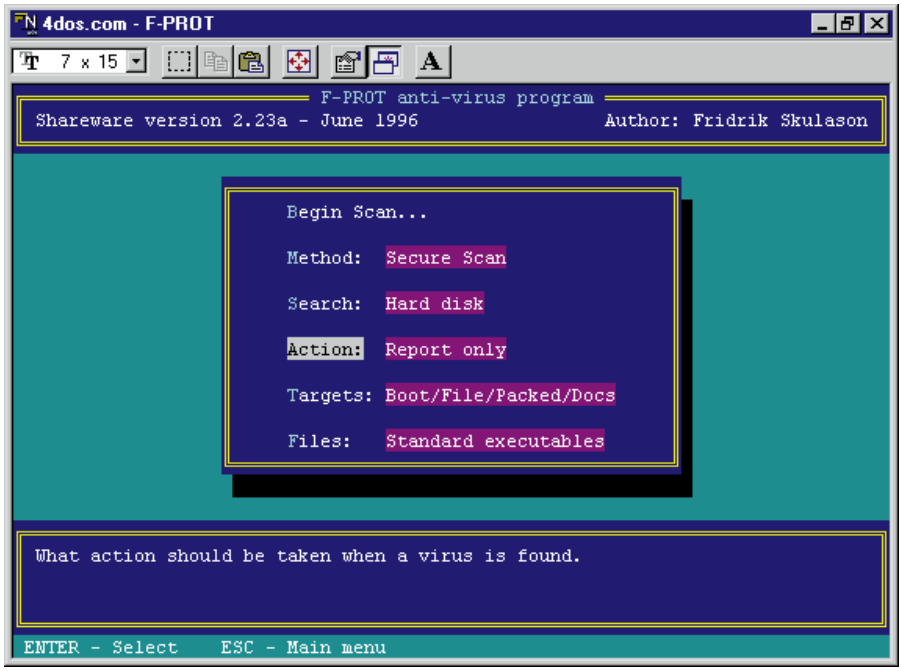
Profi-Tips zur Virenabwehr

aufnehmen muß, ist eine regelmäßige Prüfung sicher sinnvoll, etwa bei jedem Start. Auf einem Arbeitsplatzrechner oder Home-PC sieht das hingegen ganz anders aus:

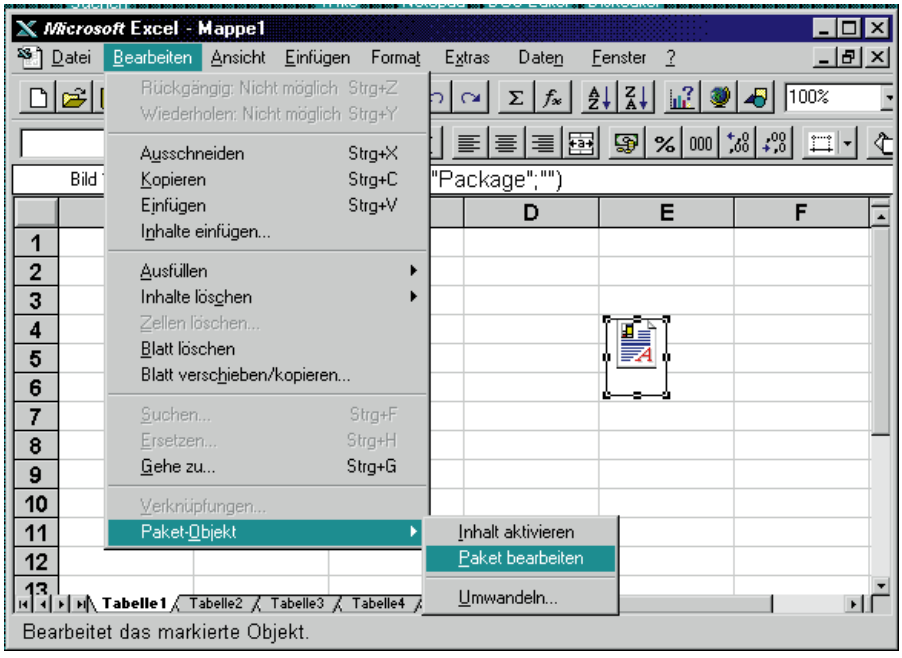
Warum sollten Sie jeden Tag oder jede Woche scannen, wenn Sie nur ein paar neue Benutzerdateien angelegt haben? Hier empfiehlt sich vielmehr ein sehr bewußtes Scannen ad hoc (aber konsequent – also immer!), sobald Sie neue Programmdateien von Diskette oder vom Netz kopiert (oder entpackt) oder online auf die Platte geladen haben. Das gleiche gilt, wenn Sie unbekannte Anwendungs-Programme direkt aus dem lokalen Netz oder von Diskette ausgeführt haben.

Wenn Sie dieser Ad-hoc-Methode wirklich konsequent folgen, genügt es, den Scanner nur das Verzeichnis mit den neuen Dateien prüfen zu lassen und damit Zeit zu sparen.

Der herkömmliche Weg bei der Virenerkennung ist die Suche nach bekannten Virensignaturen. Handelt es sich jedoch um eine Infektion durch einen neuen Erreger, muß der Scanner passen. Bietet Ihr Scanner die Option einer heuristischen Suche, wie etwa F-Prot mit „/analyse“, sollten Sie deshalb einen zweiten Suchlauf mit dieser Option starten. Diese Methode erlaubt es, auch unbekannte Viren zu identifizieren, indem das Programm nach typischen Merkmalen eines Virus fahndet.



DOS-Virenscanner unter Windows 95? Anders als die residenten DOS-Antiviren-Schilder sind die DOS-Scanner voll im Fenster lauffähig (Tip 14)



Mißtrauen gegenüber OLE: Beim Objekttyp „Paket“ ist vor dem blind vertrauenden Doppelklick eine strenge Paketkontrolle angesagt (Tip 13)

Zeigt ein Programm eine gewisse Anzahl solcher verdächtigen Merkmale, ist es höchstwahrscheinlich infiziert. Mit einer gut programmierten Heuristik lassen sich bis zu 80 Prozent aller neuen Viren erkennen. Es gibt aber einen Nachteil: Nicht selten kommt es dabei zu Fehlalarmen – die Suchroutine meldet Ihnen ganz harmlose Programme als „wahrscheinlich infiziert“.

Die meisten Scanner der im Handel angebotenen Anti-Viren-Programme durchsuchen standardmäßig den gesamten DOS-Speicher bis 1 MB nach Viren. Sollte Ihr Scanner nur den Bereich bis 640 KB durchsuchen, gibt es sicher einen Schalter, der auch den UMB-Bereich mit berücksichtigt. Einige Viren belegen diesen Speicherbereich. XMS-Viren sind hingegen vorerst Theorie.

13. Unbekannte OLE-Flugobjekte

Stimmt es, daß der Aufruf von OLE-Objekten Viren aktivieren kann?

Das ist unwahrscheinlich, aber theoretisch möglich: OLE-Objekte können DOS-Programme aufrufen, die einen Virus aktivieren oder eine wichtige Sy-

stemdatei wie COMMAND.COM direkt infizieren. Im zweiten Fall ist es schwieriger dem Virus auf die Spur zu kommen, weil der in der DOS-Box aktive Virus mit dem Abschluß der Box aus dem Speicher verschwindet.
Wenn Sie OLE-Objekten in Dateien unbekannter Herkunft mißtrauen, sollten Sie das Objekt einmal anklicken, um es zu markieren, und zunächst im Menü „Bearbeiten“ nachsehen, ob hier der OLE-Typ „Paket Objekt“ erscheint. Dann handelt es sich wahrscheinlich um ein DOS-Programm, und Sie sollten das Objekt mit „Paket bearbeiten“ (in älteren Anwendungen „Paket Objekt“ ohne Untermenü) kontrollieren. Damit startet automatisch der Objekt-Manager, und unter „Bearbeiten, Befehlszeile“ erfahren Sie das Programm, das bei einem Doppelklick starten würde.
Sie werden diese Vorsichtsmaßnahme nicht bereuen, wenn Sie an dieser Stelle Vernichtungsbefehle vorfinden, die das Trojaner-Objekt abgerufen hätte. Darin liegt die wesentliche Gefahr solcher durch ein Icon getarnten DOS-Pakete. Einen Virus kann das OLE-Objekt nur dann starten, wenn mit dem Windows-Dokument zusätzliche infizierte EXE- oder COM-Dateien transportiert wurden (etwa auf Diskette).

14. PC-Viren in der DOS-Box

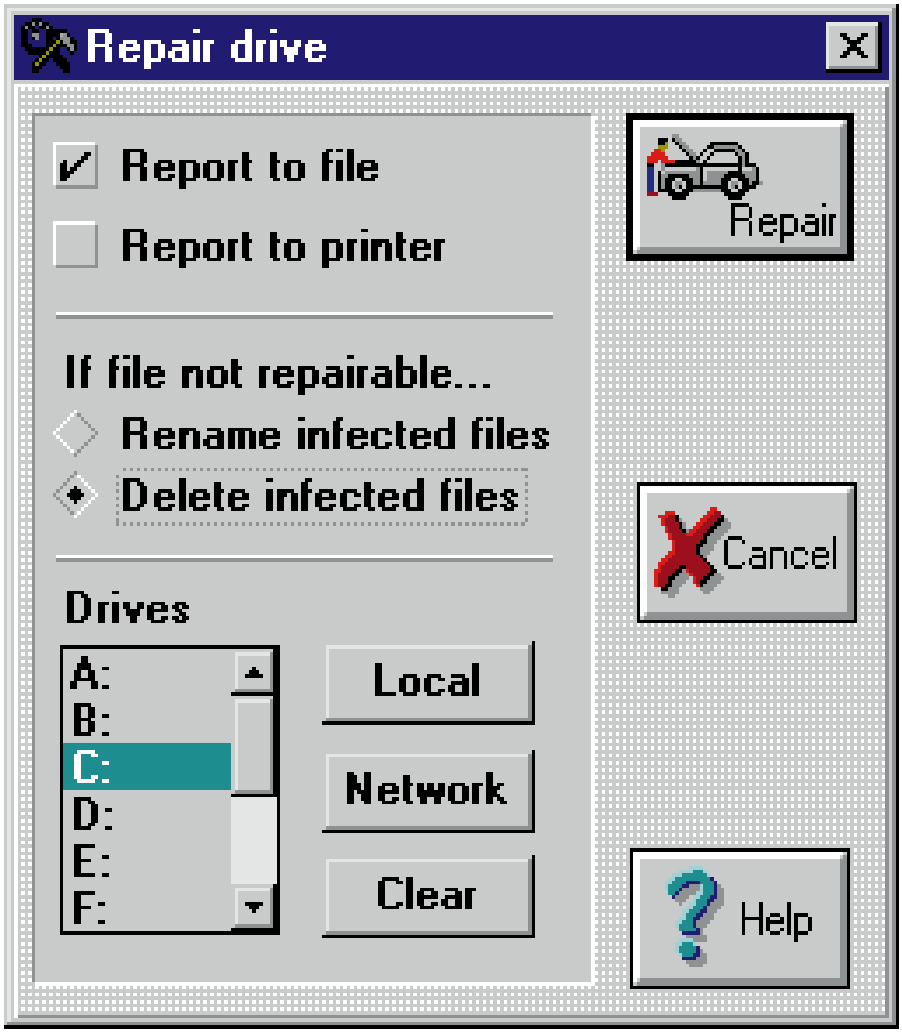
Kann ein Virus innerhalb einer DOS-Box unter Windows, OS/2, Linux aktiv werden?

Ja, denn für die DOS-Box gelten praktisch die gleichen Spielregeln wie bei einem reinen DOS-System. Daß sich alle Speicheraktionen „eigentlich“ im für Viren unzugänglichen XMS abspielen, kann dem Virus egal sein – er bekommt das auch gar nicht mit. Der virtuelle PC namens DOS-Box bietet dem Virus praktisch die gleichen Voraussetzungen wie die primäre DOS-Instanz.
Und doch besteht ein ganz wesentlicher Unterschied, der DOS-Boxen als Virenbremse auszeichnet: Das Schließen der DOS-Box entfernt den Virus unverzüglich aus dem Speicher. Bereits erfolgte Dateiinfektionen bleiben danach allerdings bestehen. Übrigens: Da die überwiegende Zahl der Infektionen von DOS-Viren verursacht wird, genügen auch unter Windows, OS/2 oder Linux DOS-basierte Antiviren-Programme. Diese sind per Aufrufparameter und Batch oft sogar bequemer zu bedienen. Und sie bieten Profis meist mehr Möglichkeiten, genau auf ihre Erfordernisse abgestimmte Routinen zu stricken als ihre GUI-Kollegen.

15. Wie häufig sind Infektionen?

Gibt es Statistiken über die Wahrscheinlichkeit und Schadenswirkung von Virenifektionen?

Die Wahrscheinlichkeit einer Vireninfektion hängt vom Verhalten des Anwenders ab und davon, mit wie vielen Dateien fremder Herkunft er zu tun hat. Statistiken, denen zufolge jeder dritte PC-Anwender mindestens eine Vireninfektion seines Rechners erlebt hat oder in einem Unternehmen etwa alle 14 Monate ein Virus auftritt, sagen wenig aus. Ein normaler Anwender, der zu Hause arbeitet und nur Standard-Software installiert, wird nie einen Virus sehen; ein aktiver und zugleich leichtsinniger Online-Nutzer, der zudem viel Diskettenpost erhält, wird sich dagegen alle paar Monate mit einem Virus herumschlagen müssen.
Direkte und indirekte Schäden: Mehr als 70 Prozent aller Viren werden anhand typischer Symptome oder durch Scan-



Desinfizieren mit Rückversicherung: Lassen Sie das Antiviren-Programm immer eine Reportdatei anlegen, dann können Sie Dateien eventuell rückkopieren (Tip 17)

ner entdeckt und mit DOS-Mitteln oder Antiviren-Programmen entfernt, bevor sie irgendwelche Datenverluste verursachen. Ein Schaden entsteht aber dennoch durch den Zeitverlust, der bei der Desinfektion entsteht.

Zu Datenverlusten kommt es bei etwa 30 Prozent der PC-Infektionen. Dabei ist allerdings der Virus nur bei knapp einem Drittel der Fälle der direkte Verursacher des Schadens. Zwei Drittel der Datenverluste gehen auf panische, schlicht falsche Reaktionen des Benutzers zurück. Ein sehr geringer Anteil geht schließlich auf das Konto der Antiviren-Software – die Daten werden beim Desinfizieren beschädigt.

99 Prozent aller Vireninfektionen werden derzeit von etwa 25 sehr verbreiteten Viren verursacht (Word.Concept, Parity-Boot, Form, Tremor, Ripper, Junkie). Die Wahrscheinlichkeit, sich einen der übrigen rund 9000 Viren einzufangen, ist relativ gering.

16. Die Folgen einer Viren-Infektion

Welche Schäden an Daten (und Hardware?) können Viren anrichten?

Durch Viren verursachte Schäden an der Hardware sind bloße theoretische Spekulation: Es gibt keinen Virus, der Festplatte, Monitor oder Grafikkarte so belasten könnte, daß das Gerät zerstört würde.

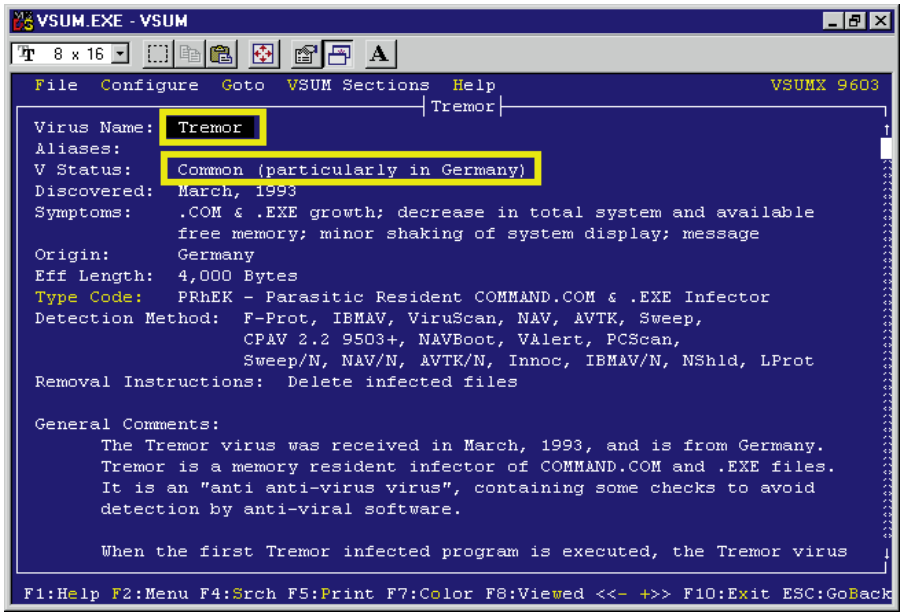
Die Einflußmöglichkeiten der Viren auf die Software – also auf Dateien, Dateisystem und Bootsequenz – sind hingegen theoretisch unbegrenzt. In der Praxis verzichten dennoch viele Virenprogrammierer auf drastische Vernichtungsfunktionen – aus dem einfachen Grund, daß sie damit auch den Lebensraum des Virus zerstören würden (manche vielleicht auch aus moralischen Gründen).

Um die Fortpflanzung der Erreger zu sichern, bevorzugen die Virenprogrammierer eher unbemerkt schleichende Veränderungen der Daten oder Zeitbomben, die dem Virus vor der Zerstörung der Daten und der Entdeckung der Infektion erst etwas Zeit zum Weiterverbreiten geben.

Wir haben im folgenden die in Deutschland derzeit am weitesten verbreiteten Viren zusammengestellt und mit einem Stichwort ihre Payload-Funktionen charakterisiert:

Virenvermeidung und Virenbekämpfung

Profi-Tips zur Virenabwehr



Ausführliche Viren-Infos: Indices wie VSUM.EXE informieren über Charakteristika, Verbreitung und Schadenswirkung bekannter Viren

Parity-Boot	→ Systemabstürze
Form	→ harmlos
Tai-Pan	→ harmlos
Antiexe	→ HD-Probleme
Tremor	→ Abstürze, HD-Probleme
Ripper	→ Speichern falscher Bytes
Quickie 1376	→ harmlos
Junkie	→ harmlos
Tequila	→ harmlos
Michelangelo	→ formatiert HD am 6. März
AntiCMOS	→ ändert Bios-Einstellungen
Delwin 1759	→ verhindert Windows-Start

17. Was tun im Ernstfall?

Wie sollten Sie reagieren, wenn Sie Symptome einer Vireninfektion bemerken?

Speichern Sie offene Dateien, und schalten Sie den Rechner dann umgehend aus. Starten Sie keinesfalls weitere Programme, auch keinen Viren-Scanner.

Wenn Ihr Rechner in einem Peer-to-Peer-Netz auch als Server auftritt, ziehen Sie am besten das Netzkabel ab. Starten Sie den Rechner dann mit der Bootdiskette neu. Dazu müssen Sie in der Regel erst die Bootreihenfolge im Bios auf „A:,C:“ umstellen. Nachdem das System von Diskette gebootet hat, starten Sie den Virenscanner entweder von der Bootdiskette oder einer anderen, garantiert virenfreien Diskette und durchsuchen damit alle Daten. Wenn der Scanner Ihren Verdacht tatsächlich durch einen Virenfund bestätigt, sollten Sie zunächst ein Backup Ihrer Daten auf einen neuen Datenträger machen. Hierfür verwenden Sie Xcopy oder einen Packer von der Bootdiskette.

Auch andere Dateien können lebensnotwendige Daten enthalten, die man in der verständlichen Hektik oft übersieht – etwa Dokumentvorlagen, Batchdateien, Konfigurationsdateien. Lassen Sie sich Zeit bei der Sicherung, aber kopieren Sie keine Programme (EXE, COM).

Die Aufgabe der Desinfektion können Sie nun entweder dem Antiviren-Programm übergeben oder selbst übernehmen. Lassen Sie sich die Reportdatei des Antiviren-Programms über die reparierten oder gelöschten Dateien auf jeden Fall auf dem Drucker oder in eine Datei ausgeben. Dann können Sie kaputtreparierte oder fehlende Programmdateien eventuell manuell zurückkopieren.

Wenn Sie ein komplettes Backup der Platte besitzen, sollten Sie das Löschen der infizierten Dateien stets der Desinfektion vorziehen. Das Desinfizieren ist nicht absolut sicher – und die gelöschten Dateien sind mit Hilfe des Backups schnell wiederhergestellt.

18. Unbestätigter Verdacht

Was sollten Sie tun, wenn der Scanner nichts findet und Sie dennoch eine Vireninfektion befürchten?

Sichern Sie vor allem alle wesentlichen Benutzerdateien einschließlich der Konfigurationsdateien – am besten alles außer den infizierbaren EXE- und COM-Dateien. Eventuell vorhandene Bootsektorviren können Sie nach den oben beschriebenen Regeln sozusagen aufs Geratewohl entfernen.

Anders steht es bei nicht erkannten, aber vermuteten Dateiviren: Leihen Sie sich zunächst ein, zwei weitere aktuelle Virenscanner aus, und durchsuchen Sie damit alle Dateien. Führt auch das zu keinem Ergebnis, sollten Sie die Prüfsummenmethode des Antiviren-Programms einsetzen, um alle Änderungen an ausführbaren Dateien gemeldet zu bekommen. Sie können aber auch mit DOS-Mitteln Speicher und Dateibestand protokollieren. Legen Sie mit

```
dir/s \*.exe > \files1
dir/s \*.com >> \files1
```

Dateilisten an, die Sie am nächsten Tag mit der neuen Liste vergleichen

```
fc files1 files2
```

Änderungen bestätigen Ihren Verdacht. Einige Viren, die bereits infizierte Dateien mit Hilfe des Dateidatums markieren, verrät der Xcopy-Test:

```
xcopy /p/d:1.1.2000/s
  c:\*.* a:\
```

Dateien, die Sie hier angezeigt bekommen, sind aus dem 21. Jahrhundert – und mit einiger Sicherheit infiziert.

Infizierte Programme sollten Sie an den Hersteller Ihrer Antiviren-Software senden und eine Analyse sowie Desinfektionshilfe anfordern. Wenn Sie Shareware einsetzen oder kein Antiviren-Programm besitzen, senden Sie die infizierte Wirtsdatei an die Mailbox VHM (Virus Help Munich, Tel. 08084/94071), die den Virus an Antiviren-Programm-Hersteller weiterleitet. Sie können dann entweder das Ergebnis abwarten oder die sicher infizierten Programme manuell löschen und neu installieren. ■