

Heimtückischer Sektierer

Der 22. August und der 22. September sind die Tage der Wahrheit, wenn *Hare.7610* auf dem PC ist. Der auch Krsna oder HDEuthanasia genannte Virus überschreibt alle Festplatten, während er die Meldung „Hare Krsna, hare, hare...“ anzeigt.

Der in den USA und Europa mehrfach gesichtete Virus verlängert Programmdateien um gut 7 Kilobyte. Er befällt aber auch den Partitionssektor (MBR).

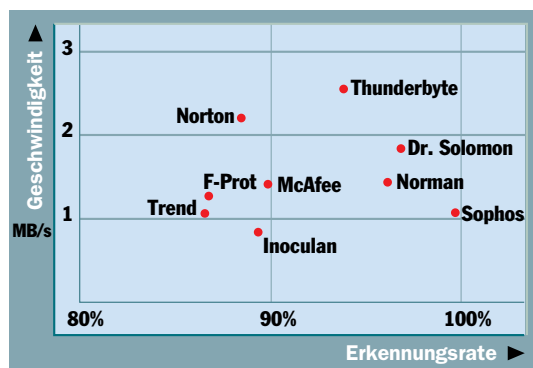
Vorsicht bei der Entfernung: Von einer sauberen Systemdiskette gebootet ist die Festplatte nicht mehr zugänglich. Es ist deshalb ratsam, ein Anti-Viren-Programm zu verwenden.

Beim Test über Michelangelo gestolpert

Neue Versionen – neue Fehler. Diese leidvolle Erfahrung mußten die Tester des englischen Fachmagazins „Virus Bulletin“ (Juni 1996) machen, als sie Scanner für Windows 95 unter die Lupe nahmen. Fast die Hälfte

Zoll-Disketten unlesbar für DOS. Während die Anti-Virus-Programmierer der DOS-Versionen dieses Problem umschifften, scheiterten ihre Kollegen aus der Windows-95-Abteilung teilweise daran.

Scanner für Windows 95



Quelle: Virus Bulletin

CHIP

der bewerteten Produkte übersah den Michelangelo-Virus auf Disketten mit 1,44 Megabyte Kapazität.

Der Grund: Der bekannteste aller Viren macht 3,5-

Den für den deutschen Markt relevanten Auszug der Testergebnisse zeigt die Grafik im Überblick. Getestet wurden unter anderem folgende Programme:

Anti-Viren-Software für Windows 95

Programm	Anbieter
Inoculan	Cheyenne, 81737 München
F-Prot	Percomp-Verlag 22041 Hamburg
McAfee Scan	McAfee Network Security & Management, 81677 München
Norman Virus Control	Norman Data Defense Systems, 42697 Solingen
Norton Antivirus	Symantec, 40237 Düsseldorf
Sophos Sweep	Novir Data, 23569 Lübeck
Dr. Solomon's AVTK	S&S International, 20537 Hamburg
Trend PC-Cillin	GSP, 85238 Petershausen
Thunderbyte	Promus Conception, 45468 Mülheim

Winword-Viren in Schach halten

Makroviren gefährden jetzt auch die Anwender von deutschem Winword. Die Schädlinge verstecken sich in Textdokumenten und verbreiten sich, wenn solche Dateien – auf Diskette oder via E-Mail – weitergegeben werden. Absoluten Schutz gibt es nicht. Die folgenden Maßnahmen verhindern jedoch das Schlimmste:

1. Von der Vorlagendatei NORMAL.DOT eine Sicherheitskopie anlegen, weil sich Makroviren meist dort einnischen.

Tip	Das können Sie tun	anwendbar?	erledigt
1	NORMAL.DOT sichern	✓	
2	Automakro-Start deaktivieren	?	
3	Dokumente scannen	✓	regelmäßig
4	Schutzmakros nutzen	✓	
5	Schäden vorbeugen	?	

sten. Das Original mit Schreibschutz versehen, falls keine Änderungen geplant sind.

2. Winword mit dem Zusatz „/m“ beim Start an der Ausführung der Autoexec-Makros hindern, falls keine eigenen Makros ablaufen müssen. Dazu in Windows 3.x im Programm-Manager einmal auf das Winword-Symbol klicken, im Menü »Datei« den Befehl »Eigenschaften« wählen und dort die Option ergänzen. In Windows 95 siehe Hilfetema „Startoptionen von Microsoft Word“.

3. Mit den üblichen Scannern bekannte Makroviren aufspüren. Der heuristische Shareware-Scanner F/WIN entdeckt mit großer Wahrscheinlichkeit auch unbekannte Makroviren.

4. Schutzmakros wie die der Anti-Viren-Programme AVP oder F-Prot installieren. Sie melden dubiose Vorgänge.

5. Kritische Programme wie FORMAT und DEBUG (unter Win 95 im Verzeichnis WINDOWS\COMMAND) entweder löschen, umbenennen oder archivieren – wenn man sie nicht benötigt. Denn manche Makroviren treiben mit Hilfe solcher DOS-Kommandos Unfug.

F/WIN: Download von <http://www.chip.de> möglich.

Harmloser Patriot

Sollte am 19. August bei Ihnen auf dem Bildschirm eine russische Flagge sichtbar werden, ist vermutlich „Russian_Flag“ aktiv. Er versteckt sich im Boot-Sektor und bringt die Nationalfarben beim Start in drei Bändern auf den Monitor.

Nach einem Tastendruck geht es zum Glück problemlos weiter: Der Virus ist anscheinend nicht bösartig, sondern will nur an den miß-



lungenen Militärcoup vor fünf Jahren erinnern. Entfernen läßt er sich mit dem DOS-Kommando FDISK /MBR.