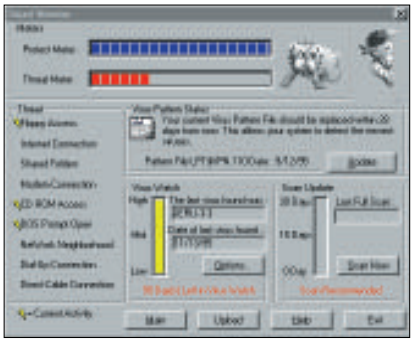
VIREN

Internet-Bewußtsein

Neue Gefahren rufen nach neuen Schutzmechanismen. Viren können etwa aus dem Internet leicht als Mail-Anhängsel eingeschleppt werden. *PC-Cillin* von Trend Micro Devices untersucht daher in der Profi-Pack-Ausstattung unter Windows 95 solche Dateien und macht dabei auch vor der gebräuchlichen UUE-Codierung nicht halt. Je nach Aktivitäten des Windows-95-Benutzers paßt die Software ihr Überwachungsniveau dynamisch an.



Ein kostenloses Update der Virensteckbriefe ist aus dem Programm heraus über das Internet oder eine Mailbox möglich.

Firmen können das Übel direkt an der Wurzel bekämpfen, indem sie einen anderen Aufpasser am Tor zum Internet postieren: Das für verschiedene Unix-Varianten erhältliche *Interscan* überprüft Mail- und Ftp-Transfers auf mitreisende Viren. Die Kontrolle einer Datei soll nur etwa 16 Millisekunden dauern.

Anbieter: GSP, 85238 Petershausen, Telefon (08137) 1318, Fax 3865

Berühmter Virenjäger im Umbruch

Mit Antivirensoftware ist die Firma groß geworden, doch hat sie auch in anderen Bereichen investiert: McAfee betrachtet heute Netzsoftware als Kerngeschäft. Durch den Zukauf von Unternehmen enthält das Sortiment nun die Programme von Brightworks und Saber, die die Netzverwaltung und die lokale sowie unternehmensweite Verteilung von Software erleichtern sollen. McAfee ist in Deutschland nun mit einer eigenen Niederlassung vertreten.

McAfee Network Security & Management, 81677 München, Tel. (089) 92404-214, Fax 92404-211

Wehrlos gegen Word-Viren?

Eine neue Bedrohungsdimension schafft der *Colors*-Virus. Konnte man die bisherigen Word-Viren entschärfen, indem man die Textverarbeitung ihrer Automakro-Fähigkeit beraubte, so läßt dies den neuesten Makrovirus kalt. Er infiziert zwar ähnlich wie seine Vorgänger beim Öffnen eines ansteckenden Dokuments die Formatvorlagen-Datei, doch legt er auch beim Speichern oder Schließen eines Dokuments oder beim Beenden des Programms los. Betroffen sind bislang nur die aktuellen englischen Word-Versionen unter allen Betriebssystemen.

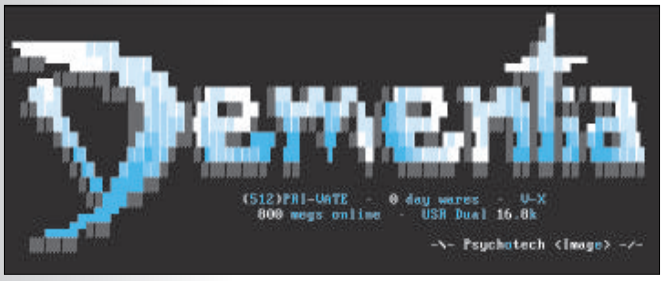
Der Virus ist der erste, der sich zu verstecken sucht: Er führt zwar neue Makros ein, doch beim Blick in die Makroliste erscheinen sie nicht. Wie *Word Nuclear* (CHIP 11/95, S. 14) liegt er verschlüsselt vor, kann also nicht so einfach analysiert oder verändert werden.

Den namengebenden Effekt löst er über einen Zähler mit dem Namen countersu in der Datei WIN.INI aus: Gelegentlich verändert er die Windows-Farben willkürlich, so daß beim nächsten Windows-Start die Fenster in schrägen Farbkombinationen erscheinen.

Ein bekloppter Dateischmuggler

Das Besondere am *Dementia*-Virus ist nicht nur, daß er ZIP-Dateien infizieren kann. Schlimmer noch: Er benutzt sie als Verpackung, in der sich heimlich Dateien aus Mailboxen schmuggeln lassen.

Dementia beginnt sein Unwesen zu treiben, wenn eine



Datei mit dem Namen CALL-FAST.COM aus einem ZIP-Archiv gestartet wird. Ab dann injiziert er diesen Virenträger in jede ZIP-Datei, wenn sie geöffnet wird. Befindet sich noch eine Datei namens REQUEST.IVA in dem Archiv, sammelt der Virus die dort bezeichneten Dateien von seinem Gastrechner ein und verstaut sie unter dem Namen RECEIPT.IVA ebenfalls in der ZIP-Datei.

Was das soll? Dementia benutzt eine Archivdatei wie einen Einkaufskorb, in dem ein Einkaufszettel liegt. Eine fatale Wirkung kann der Virus besonders in Mailboxen entfalten, wenn beispielsweise die Paßwortdateien oder ähnlich sicherheitsrelevante Daten auf seiner Wunschliste stehen. Falls der Betreiber den Schmuggel nicht durchschaut, könnten beim ersten Download Kopien wichtiger Dateien als blinde Passagiere mit auf die Reise gehen.

... in aller Kürze

Auch in RAR-gepackten Dateien kann das **Antiviral Toolkit Pro** nach Viren suchen. Howard Fuhs Elektronik (65203 Wiesbaden-Biebrich) liefert das Programm auch auf bootfähigen Disketten, um seinen Einsatz sicherer zu gestalten.

Eine verbesserte heuristische Suchfunktion sollen die **Thunderbyte-Anti-Virus-Utilities** ab der Version 6.50 haben. Promus Conception (45468 Mülheim a. d. Ruhr) bietet ab jetzt kostenlose Updates per DFÜ.