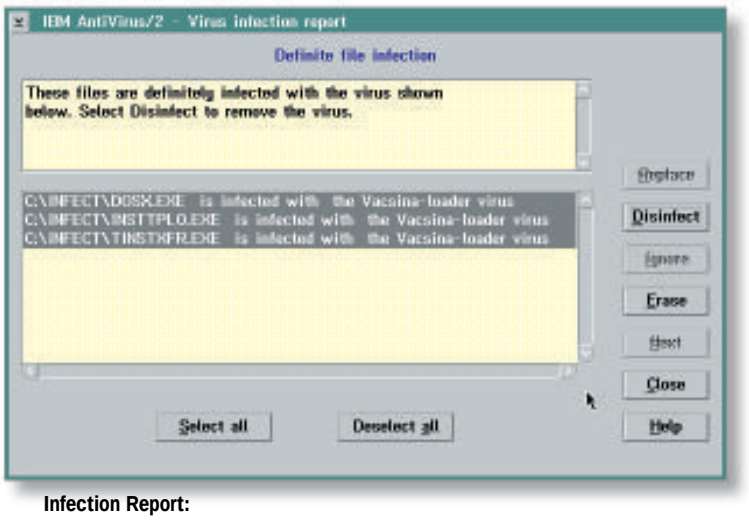
IBM Antivirus im Test

Virenwächter

Hätten wir uns an den Verpackungsaufdruck von IBM Antivirus gehalten, so wäre dieser Artikel nicht erschienen: „Install-and-forget“ empfiehlt einem IBM dort. Wir sind diesem Rat nicht gefolgt und haben uns das IBM-eigene Antiviren-Programm genauer angesehen.

THOMAS BINZINGER

Gleich drei Versionen seines Antiviren-Programms hat IBM in eine Packung gesteckt: je eine Version für DOS, Windows und OS/2 sowie Warp Connect. Vier Disketten, eine Anleitung und ein kleiner Papierstapel – die Lizenzbestimmungen – enthält die englische Version 2.2 (Mai 1995) von Antivirus. Die Anleitung gibt sich IBM-typisch nüchtern. Statt einer Aufzählung über die Bedeutung jeder einzelnen Programmdatei wäre ein Kapitel über Viren – das heißt



Infection Report: Die hier angezeigten infizierten Dateien können mit Antivirus „gesäubert“ werden

ein paar Hintergrundinformationen – sicherlich nützlicher gewesen. Leider gibt es hierzu nur den lapidaren Satz: „You do not need do develop a detailed understanding of viruses or anti-virus-technology...“ Vielen Dank, IBM. Endlich sagt uns jemand, was wir verstehen müssen und was nicht. Davon abgesehen ist die Dokumentation jedoch ausführlich gehalten und verständlich geschrieben.

Hinsichtlich der Bedienung der einzelnen Versionen gibt es keine Unterschiede. Eine gute Idee ist der „Push-here“-Button: Ein Mausklick genügt, und die Virensuche beginnt. Ebenfalls positiv ist die zeitgesteuerte Suche, die man unter DOS aktivieren kann.

Ein wenig unübersichtlich hingegen ist die Berichtsfunktion geraten: Mit Hilfe des „Next“-Buttons muß man sich von Prüfbericht zu Prüfbericht hangeln – es gibt keine Übersicht, in der die Suchergebnisse in einer Headline zusammengefaßt werden. Und auch eine Virendatenbank, in der man nachschlagen kann, was ein einzelner „Schädling“ so treibt, fehlt bei IBM Antivirus nicht, ist jedoch etwas dürftig ausgefallen. Hier kann man zwischen einer Auflistung aller dem Programm bekannten Viren wählen – jedoch ohne jede Erklärung – oder einer kleineren Auswahl von „wichtigen“ Viren, die dann etwas ausführlicher beschrieben sind.

Sieben Monate soll diese Version – laut Readme-Datei – aktuell sein. Viele Hersteller von Antiviren-Programmen propagieren eine sehr viel schnellere Update-Politik, und auch uns erschien dieser Zeitraum ein wenig lang. In Compuserve konnten wir uns zwar ein Update auf die Version 2.3 (von September 95) laden, aber auch ein (zum Testzeitpunkt) zwei Monate altes Update ist nicht gerade als hochaktuell zu bezeichnen und machte uns neugierig, wie es um die Erkennungsrate neuer Viren bestellt ist.

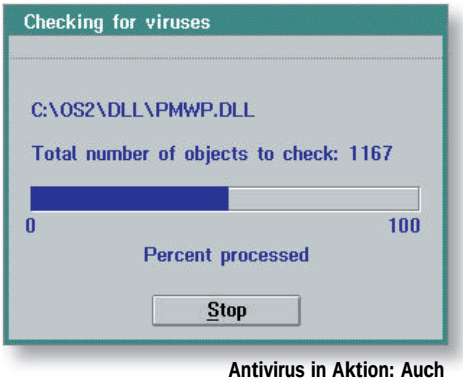
Test. Tests in bezug auf die Erkennungsrate sind mit extremer Vorsicht zu genießen: Ein Programm, das in einem Vergleichstest 90 Prozent der Viren erkennt, kann manchmal weniger nützen als eines, das nur 80 Prozent erkennt. Denn viele Viren sind Laborviren, die in freier Wildbahn nicht existieren. Auch ist die Virenpopulation in Europa und den USA unterschiedlich – daher kann es vorkommen, daß ein europäisches Produkt in einem Test schlechter abschneidet als ein amerikanisches – aber trotzdem die hier grassierenden Viren besser erkennt.

Trotzdem wollten wir auf einen Test nicht verzichten und setzten vier Antiviren-Programmen (nämlich F-Prot 2.20, McAfee Scan 2.2.7, Turbo Anti Virus 9.75, IBM Antivirus mit Virensignaturen 9/95) ein Testpaket aus 98 Dateien vor, von denen 92 tatsächlich infiziert waren – jeweils mit unterschiedlichen Viren und teilweise mit Mehrfachinfektionen. Alle Dateien sind echte Infektionen, die auf Computern – bei Privatleuten oder Firmen in Deutschland – aufgetreten sind. Vorweg gesagt: Spitzenreiter in diesem Test war Turbo Anti Virus 9.75 mit

Praktisch: Mit nur einem Mausklick checkt man sein System

90 erkannten Dateien, das Schlußlicht bildete McAfee Scan mit 80 Dateien. IBMs Produkt schlug sich mit 85 erkannten Infektionen recht ordentlich.

Ein übler Ausrutscher passiert IBM Antivirus jedoch beim Säubern der Dateien: Aus nur elf (!) Dateien ist es gewillt, die Viren zu entfernen, die anderen Dateien können bestenfalls gelöscht werden. Zum Vergleich die Werte der anderen Kandidaten: Turbo Anti Virus 84, F-Prot 80, Scan 35. Zwar wurde nicht geprüft, ob diese Programme „sauber“ gesäubert haben, ob also die Dateien anschließend in Ordnung waren. Trotzdem scheint der Wert des IBM-Programms inakzeptabel niedrig. Und: Das „DOS-Shield“ erkennt nur einen Bruchteil der dem Scanner bekannten Viren. Dafür konnte Antivirus den Winword.Nuclear Virus erkennen – ein Pluspunkt, da dieser Virentyp (er befällt keine Programme, sondern mit Microsoft Word erstellte Texte) erst kürzlich auftauchte.



Antivirus in Aktion: Auch die Suche im Hintergrund ist hier möglich

Fazit. Für den Preis (zirka 90 Mark) von einem Programm bekommt man gleich drei, nämlich die DOS-, Windows- und OS/2-Variante. Auch sehr praktisch: Alle haben die gleiche Benutzeroberfläche, so gibt es keine Umstellungsprobleme. Natürlich haben sie auch die gleichen Such-Engines, und so bringt dem Privatanwender diese Vielfalt eigentlich – nichts. In Unternehmen jedoch mag dies anders aussehen.

Das Update-Intervall erscheint uns ein wenig zu lang, andererseits sind Updates in Compuserve erhältlich – sofern man darauf Zugriff hat. Positiv zudem die Möglichkeit, eine Notfall-Diskette zu erzeugen. Unverständlich allerdings, warum das DOS-Shield sich auf eine Teilauswahl der Viren beschränkt. Auffällig zudem: die schlechte Quote beim Säubern unserer Testdateien.

Wie arbeiten Viren?

Computerviren sind kleine Programme, die in der Regel über eine besondere Fähigkeit verfügen: Sie können ihren eigenen Progammcode an die Datei, die den Programmcode anderer Programme enthält, anhängen. Zudem modifizieren sie die Originaldatei so, daß erst das Virenprogramm und dann die „infizierte“ Datei ausgeführt wird.

Startet der Anwender unwissentlich das Virenprogramm, so kann dieses – vom Anwender unbemerkt – weitere Programme infizieren oder jede programmtechnisch mögliche Aktion durchführen, also etwa eine Meldung anzeigen, eine Melodie spielen, Teile der Festplatte formatieren etc. Es kann allerdings nicht die Computerhardware beschädigen. Klar, daß ein Virusprogramm sich erst einmal verbreiten wird, bevor es auf sich aufmerksam macht, andernfalls hätte der Anwender zu schnell Gelegenheit, Gegenmaßnahmen zu ergreifen.

Auch bei Computerviren lassen sich spezielle Typen unterscheiden: Ein *Bootsektor-Virus* befällt entweder den Partitionslader oder den Betriebssystemlader auf Festplatten. Er tritt damit schon vor Aktivierung des Betriebssystems in Kraft und ist somit unabhängig von diesem. Im Gegensatz dazu infizieren *Dateiviren* Programmdateien bestimmter Betriebssysteme und sind daher auf das jeweilige Betriebssystem angewiesen. Beide Typen sind CPU-spezifisch, arbeiten also zum Beispiel nur dann, wenn eine (Intel-) 80x86-CPU vorhanden ist – genauer gesagt: nur auf einem PC.

Dies trifft für *Macro-Viren* nicht zu. Diese benutzen die Makrosprache von Textverarbeitungen, Tabellenkalkulationen etc. als Basis und arbeiten daher auf jedem Computertyp, auf dem diese Makrosprache zur Verfügung steht. So kann etwa der WinWord.Nuclear-Virus sowohl auf PC als auch auf Macs auftreten, da auf beiden Systemen Winword läuft. Alle drei genannten Virentypen können natürlich auch kombiniert werden.

Viele Viren verändern bei jeder Infektion ihren Programmcode ein wenig oder verschlüsseln jede neue Infektion. Dadurch wird es für Anwender (und Antiviren-Programme) schwieriger, eine Infektion zu erkennen. Zudem sind fast alle modernen Viren speicherresident, das heißt der Virus wird nicht nur aktiv, wenn das infizierte Programm gestartet wird, sondern er klinkt sich in das Betriebssystem ein und bleibt, wurde erst einmal ein infiziertes Programm gestartet, die ganze Zeit aktiv. Der Vorteil (oder Nachteil, je nachdem aus welcher Position man es betrachtet) ist, daß der Virus Aktionen unabhängig vom Programmstart durchführen kann.