Ansteckende PC-Monster

Sie treiben Unfug und hinterlassen grauenhafte Zerstörungen. Gemeint sind nicht Ausserirdische, sondern Computerviren, die den PC via Diskette, Internet und Word-Dokument bedrohen.

von Kurt Haupt

Ausserirdische und Computerviren haben eines gemeinsam: Es gibt unzählige Geschichten über sie. Ein Teil dieser Geschichten sind allerdings Schauermärchen oder Wunschträume: Während die einen Entführungen durch Ausserirdische für den morgendlichen Kater verantwortlich machen, geben andere vorsichtshalber mal einem Computervirus die Schuld, wenn sich ein Dokument auf der unorganisierten Festplatte nicht mehr finden lässt.

Mehrere tausend Viren – je nach Zählart sind es 3000 oder über 10'000 – sind heute bekannt. Von diesem Virenvolk sind aber nur rund 200 häufig in «freier Wildbahn» anzutreffen, die restlichen sind selten oder gar nur als Forschungsobjekte in Computerlabors bekannt. Die «Freien» gehörten bisher glücklicherweise sogar meist zu den harmloseren Gattungen. Doch dank Internet und vernetzten PCs ist die Virenverbreitung einfacher und schneller geworden. Vorsicht ist also angebracht, vor allem, weil in letzter Zeit häufig Makroviren mit grossem Schadenpotential auftauchen.

Die grösste Gefahr droht zurzeit denn auch durch diese Dateiviren, die sich in Dokumenten von Microsoft-Programmen einnisten. Es genügt bereits, ein simples Word-Dokument oder eine Excel-Tabelle zu öffnen, um den PC zu infizieren oder Daten auf Nimmerwiedersehen verschwinden zu lassen. Ein Makro ist üblicherweise ein kleines Hilfsprogramm, das erlaubt, häufig wiederkehrende Aufgaben in der Textverarbeitung Word oder der Tabellenkalkulation Excel zu automatisieren. Makros können in jedes Word-Dokument eingebettet werden, spezielle Makros laufen beim Öffnen eines Dokumentes sogar automatisch ab. Leider hat es der Softwarehersteller Microsoft unterlassen, die Makrosprache von Word und Excel mit der nötigen Sicherheit zu versehen. Makroviren nutzen diesen Schlupfwinkel: Ehe Sie merken, dass Sie beim Laden des infizierten Word-Dokuments den Programmcode des Virus ausführen, hat dieser im schlimmsten Fall bereits Ihre Festplatte formatiert. Selbst in der neuesten Version von Office 97 haben die Programmierer keine wirksamen Schutzmechanismen eingebaut. Microsoft hat sich im vergangenen Jahr sogar selber unbeabsichtigt als Verbreiter von Makroviren betätigt, als ein solcher auf eine CD-ROM gepresst wurde, die der Softwareriese an der Computermesse Orbit in Basel gratis verteilte.

Einen Schutz gegen Viren bieten zahlreiche Hersteller von Antiviren-Paketen, die meistens die Programmteile Virenschutzschild, -scanner und -entferner umfassen. In der täglichen Anwendung ist vor allem der Virenschutzschild praktisch. Er überprüft beim Öffnen jeder Datei, ob sich darin ein Virus befindet. Kontrolliert werden nicht nur Programme, sondern auch Dateien, die Makroviren enthalten können. Hundertprozentig ist dieser Schutz allerdings nicht, denn die Schilde können nur Viren identifizieren, die ihnen bekannt sind. Leider tauchen heute jedoch täglich neue Makroviren auf, so dass ein wirksamer Schutz nur gewährleistet ist, wenn Sie Ihren Schutzschild monatlich mit den neuesten Vireninformationen aktualisieren.

Leider verursachen die Virenschilde im täglichen Betrieb eine Verlangsamung des Systems, die vor allem beim Starten von Programmen oder beim Laden von Dokumenten spürbar ist. Die meisten Schilde lassen sich aber einfach per Knopfdruck ein- und ausschalten. Vor allem beim Surfen im Internet oder beim Einlegen fremder Disketten sollte der Virenschild aber unbedingt aktiviert sein.

Virenscanner sind Programme, die sporadisch Ihre gesamte Festplatte oder verdächtige Disketten durchkämmen. Einige Produkte bieten als Zusatz auch eine Impffunktion an. Dabei wird die Originallänge vorhandener Dateien abgespeichert und die Dateien mit einem «Prüfsiegel» versehen. Nistet sich ein Virus ein, wird das Prüfsiegel verletzt, woran der Scanner oder der Virenschutzschild die Manipulation erkennt und einen Alarm auslöst. Aber auch Virenscanner sind ohne regelmässige Aktualisierung schnell veraltet. Deshalb sollten Sie beim Kauf eines Antiviren-Programms darauf achten, welche Update-Möglichkeiten angeboten werden, siehe dazu unsere Vergleichstabelle auf Seite 34.

Der Virenentferner letztlich sorgt dafür, dass ein Virus möglichst ohne grösseren Schaden wieder vom System entfernt werden kann.

Dank Internet lassen sich führende Virenschutzprogramme beinahe automatisch aktualisieren. Vorbildlich ist hier das Programm «Norton AntiVirus für Windows 95» von Symantec. Ein Knopfdruck genügt um die Internet-Verbindung zum Symantec-Servicerechner aufzubauen, von dort die neuesten Vireninformationen zu beziehen und das Programm auf dem PC auch gleich zu aktualisieren. So ist das Norton-Programm innert Minuten wieder gegen die neuesten Virentypen gewappnet.

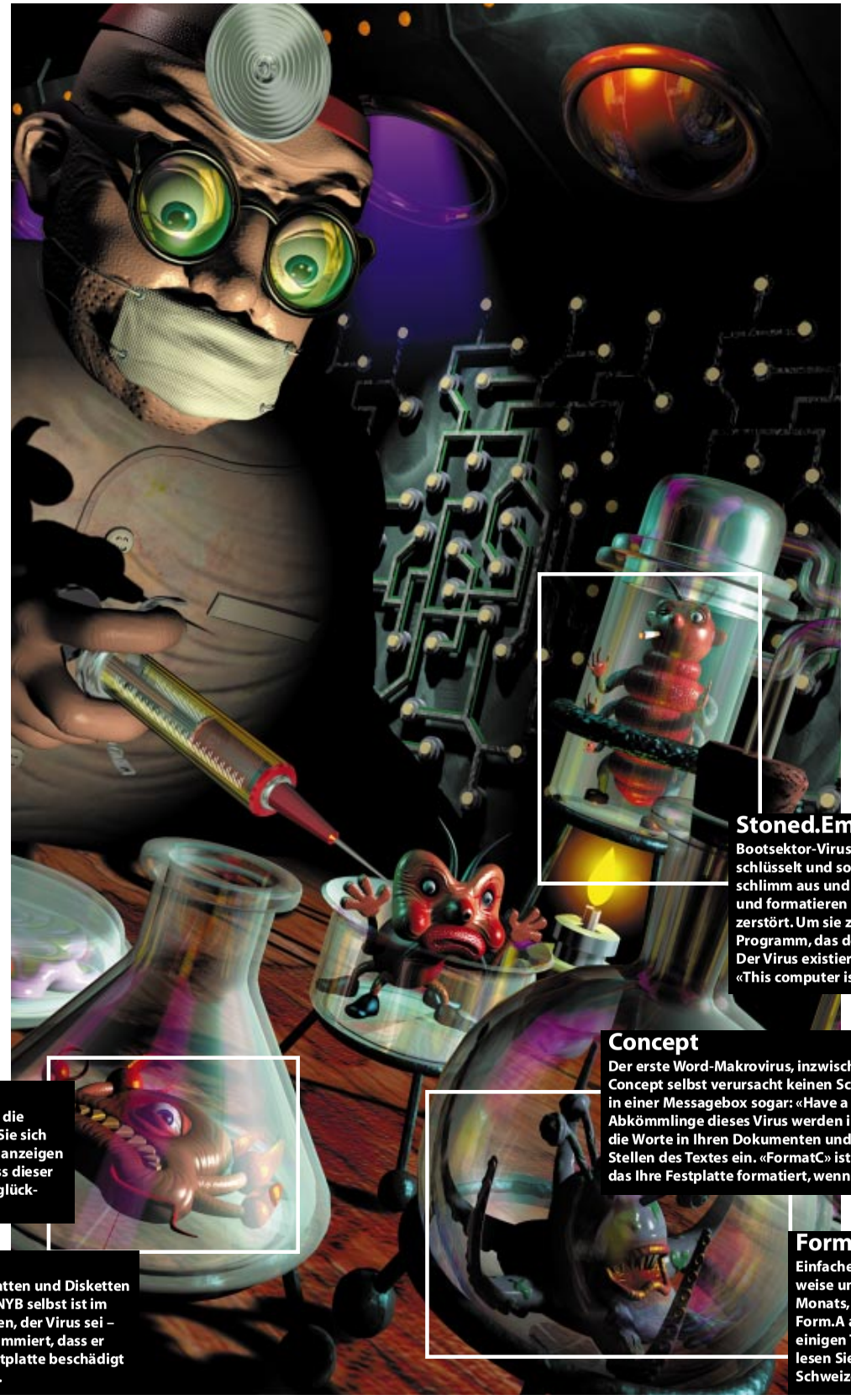
Aktuelle Virenscanner lassen sich übrigens bei zahlreichen Herstellern zu Testzwecken gratis via Internet beziehen. Auch im PCtip-Online-Dienst finden Sie einige dieser Testversionen. Sie können meist während 30 Tagen kostenlos eingesetzt werden.

Rund ein halbes Dutzend Hersteller liefern komplette Lösungen, die Ihren PC schützen und nötigenfalls auch die Viren wieder entfernen. ▶

Fachchinesisch

Bootsektor
Winziges Programm in der äussersten Spur einer Systemdiskette, das den PC auffordert, sein Betriebssystem (DOS, Windows, etc.) zu laden.

Trojanisches Pferd
Ein Anwendungsprogramm, das neben seiner eigentlichen Funktion «unbemerkt» einen Virus transportiert.



Stoned.Empire.Monkey
Bootsektor-Virus, der die Partitionstabelle Ihrer Festplatte verschlüsselt und so deren Inhalt unzugänglich macht. Das sieht schlimm aus und Sie vermuten, dass all Ihre Dateien verloren sind und formatieren Ihre Platte neu. Der Virus hat aber die Daten nicht zerstört. Um sie zurück zu bekommen, benötigen Sie ein Antiviren-Programm, das den Virus erkennt und die Partitionstabelle repariert. Der Virus existiert in zahlreichen Varianten. Eine zeigt die Meldung «This computer is stoned»: Dieser PC befindet sich im Delirium...

AntiEXE
Bootsektor-Virus, der sich ausbreitet, wenn Sie auf die Systemtabelle einer Diskette zugreifen (z.B. wenn Sie sich deren Inhalt mit dem Explorer oder Dateimanager anzeigen lassen). Virenexperten haben herausgefunden, dass dieser Virus nur eine einzige Programmdatei befällt – unglücklicherweise wissen sie noch nicht welche.

Concept
Der erste Word-Makrovirus, inzwischen über das Internet weit verbreitet. Concept selbst verursacht keinen Schaden (eine neuere Variante wünscht in einer Messagebox sogar: «Have a nice day!»), aber zerstörerische Abkömmlinge dieses Virus werden immer häufiger. «Wazzu» z.B. vermixt die Worte in Ihren Dokumenten und fügt den eigenen Namen an zufälligen Stellen des Textes ein. «FormatC» ist ein sogenanntes Trojanisches Pferd, das Ihre Festplatte formatiert, wenn Sie die infizierte Datei öffnen.

NYB (New York Boot)
Bootsektor-Virus, der sich über infizierte Festplatten und Disketten verbreitet, wenn das System aufgestartet wird. NYB selbst ist im Grunde nicht schädlich, aber Virenexperten sagen, der Virus sei – wie viele andere Viren auch – so schlecht programmiert, dass er ungewollt den Bootsektor der Diskette oder Festplatte beschädigt und so verhindert, dass Ihr System starten kann.

Form.A
Einfacher und weit verbreiteter Bootsektor-Virus, normalerweise unschädlich. Starten Sie Ihren PC jedoch am 18. eines Monats, dann werden zufällige Sektoren der Festplatte von Form.A als zerstört markiert, Ihre Tastatur gibt plötzlich bei einigen Tasten Piepstöne von sich und auf dem Bildschirm lesen Sie eine Mitteilung, die wir in einem anständigen Schweizer Magazin nicht veröffentlichen können.

ILLUSTRATIONS: HM LUDTKE

PCtips

1. Sichern Sie Ihre Daten regelmässig und bewahren Sie mehrere Sicherungszyklen auf.
2. Entfernen Sie vor dem Ausschalten die Diskette aus dem Laufwerk.
3. Wechseln Sie im BIOS die sogenannte Boot-Up-Sequence von A:C: zu C:A:. Das verhindert, dass Ihr PC versucht ab Diskette aufzustarten und sich so einen Virus holt.
4. Beziehen Sie Dateien aus dem Internet von sicheren Quellen. Die Web-Seite eines Herstellers ist sicherer als eine Seite wie www.pirates.com. Scannen Sie E-Mails und Disketten von Fremden und Freunden mit einem aktuellen Virenscanner.
5. Verzichten Sie – wenn Sie können – auf den Einsatz von MS-Excel und MS-Word, bis der Softwarehersteller einen Schutz gegen Makroviren bietet. Bisher sind keine Makroviren bekannt, welche die Konkurrenzprodukte von Lotus, Corel oder StarOffice infizieren.

Virenschutz

▶ Die National Computer Security Association (NCSA) prüft und zertifiziert regelmässig Virenscanner. Eine Liste zertifizierter Antivirenprogramme finden Sie auf der Internet-Seite http://www.ncsa.com/virus/avpdmembers.html. Egal, welches dieser Virenprogramme Sie einsetzen, wichtig ist eine regelmässige Aktualisierung, denn Viren ändern sich ständig und täglich kommen neue hinzu.

Eine Liste der häufigsten Viren zeigt, dass die Makroviren auf dem Vormarsch sind. Auf Platz eins steht zwar noch immer der bejahrte Form-Virus, der nur wenig Schaden anrichtet. Auf Rang zwei folgt dann aber schon der Concept-Makrovirus. Auffällig ist auch, dass sich unter den zehn häufigsten Viren sechs Boot-Viren befinden. Infektionen durch Boot-Viren passieren meist, wenn sich beim Start des Systems eine infizierte Diskette im Laufwerk befindet.

Die beste Versicherung gegen die Folgen eines Virenbefalls ist eine regelmässige Datensicherung (siehe PCtip 04/97, Seite 27). Besitzen Sie zusätzlich eine schreibgeschützte Diskette, mit der sich Ihr Rechner starten lässt, ist die Desinfektion Ihres PCs ebenfalls um einiges einfacher. Wie Sie mit Windows 95 eine solche Systemdiskette erstellen, können Sie in dieser Ausgabe auf Seite 15 nachlesen. Übrigens: Zum Testen der Funktionen Ihres Virenschutzprogrammes können Sie einfach die Internet-Seite http://www.av.ibm.com/InsideTheLab/VirusInfo/EICAR/ besuchen. Wenn Ihr Scanner funktioniert, sollte er beim Herunterladen der Probe-Datei eicar.com sofort Alarm schlagen.

Falschalarme und Legenden machen in PC-Clubs und an Stammtischen immer wieder die Runde. Da gibt es beispielsweise eine E-Mail-Mitteilung mit dem Titel «Good News», die vor einem Virus warnt, der sich just in einer so betitelten E-Mail-Meldung verstecken soll. Da sich dann jedermann veranlasst sieht, diese Warnung weiter zu vermitteln entsteht tatsächlich eine Flut von «Good News»-Meldungen. Ins Reich der Legenden gehören auch Geschichten über Viren, welche die Monitoreinstellungen so verändern, dass schädliche Strahlungen verursacht werden. Ein gelungener Aprilscherz ist auch die Story einer deutschen Computerfachzeitschrift, wonach sich der Schreibschutzschieber von Disketten mittels spezieller Softwarebefehle umgehen lässt. Panik hat bei einigen Anwendern eine persönlich adressierte E-Mail ausgelöst, in der steht, ein Virus namens «NaughtyRobot» habe sämtliche vertraulichen Adressdaten des PCs ausspioniert. In Wirklichkeit wurde die E-Mail-Adresse nur aufgrund einer Beteiligung an einer Newsgroup oder durch die Registrierung auf einer Webseite in Erfahrung gebracht. Witzbolde verwenden diese Adressangaben dann für die elektronische Schreckensbotschaft. Ebenfalls verwirrend ist die Geschichte des AOL4FREE-Virus. Erst verbreiteten Witzbolde eine absolut unbegründete Panikmeldung. Dann schrieb ein Böswilliger tatsächlich ein Killerprogramm, das ebenfalls unter dem Name AOL4FREE verteilt wird und wirklich Schaden anrichtet.

Fachchinesisch

CMOS-Tabelle
Complementary Metal Oxide Semiconductor. Speicherbaustein, der mit Batterie die Langzeit-Speicherung der Grundinformationen des Systems übernimmt.

BIOS
Basic Input/Output System, ein Speicherchip, der wichtige Informationen über den PC und seine Komponenten enthält und die Kommunikation zwischen Prozessor, Arbeitsspeicher und Peripheriegeräten steuert.

Dass Viren einen gesamten Betrieb lahm legen können, beweist die Geschichte der Bank National City Corporation, bei der eine Virenifektion das gesamte Computer-Netzwerk mit über 10'000 Rechnern während Stunden ausser Betrieb setzte. Der Virus verbreitete sich rasend schnell im Rechnernetz. Die Spezialisten mussten letztlich rund 3000 Exemplare des lästigen Programmes killen, bevor das Netz gesäubert war. Details dieser Geschichte sind auf der Web-Seite http://www.av.ibm.com/current/Feature2/ nachzulesen.

One Half
Ein polymorpher Virus (d.h. er verändert seine Gestalt bei jeder Infektion), der Festplatten-Sektoren verschlüsselt – still und leise, nach und nach. Am Anfang bemerken Sie nichts, da der Virus bereits verschlüsselte Daten beim Zugriff wieder entschlüsselt. Ist die Hälfte Ihrer Platte infiziert, meldet er «This is one half». Der Zugriff auf Dateien und System wird zunehmend schwieriger. Antiviren-Programme können den Virus entfernen, aber Ihre Dateien nicht mehr retten.

Marktübersicht Virenkiller-Software

	Produkt	Preis* in Fr.	Updates inklusive	System	NCSA-Test**	VTC-Test***	Web	Info	Bemerkung
	Dr. Solomon Anti-Virus Toolkit	299.–	Vier im ersten Jahr	Win 3.x/95/NT, DOS, OS/2, Unix, Mac	100/89	100/97.9	http://www.drsolomon.com/	Sotec, Tel. 022/362 31 44	Pro: Beste Virenerkennungs- und Desinfektionsraten Contra: Teuer, Updates nur über Subskriptionsdisketten
	Norman ThunderByte Anti-Virus Utilities	139.–	Für Private lebenslang gratis, Diskette à Fr. 20.–	Win 3.x/ 95/NT, DOS, OS/2	95/60	96/72	http://www.thunderbyte.nl/ oder http://www.senndata.ch/	Senn Data Security, Tel. 01/786 26 00	Pro: Gute Konfiguration der Virenerkennung Contra: Desinfektion mässig und für Anfänger zu kompliziert
	Norton AntiVirus 2.0	149.–	Via Internet automatisch	Win 3.x/95/NT, DOS	100/77	98.6/84.6	http://www.symantec.com/avcenter/	Symantec, Tel. 071/626 20 40	Pro: Einfache Bedienung, automatisches Update über Internet Contra: Konnte im Test nur 77% der Vireninfektionen beseitigen.
	Touchstone PC-Cillin II	125.–	Ein Jahr via Internet	Win 3.x/95, DOS	100/80	nicht im Test	http://www.antivirus.com/	Markt & Technik, Tel. 041/747 47 47	Pro: Erkennung/Desinfektion sehr gut, einfaches Update via Internet Contra: Verwirrend viele Konfigurationsoptionen
	McAfee VirusScan 3.0	108.–	Vier (pro Quartal eine Diskette)	Win 3.x/95/NT, DOS, OS/2, Mac und andere	92/59	98.9/95.1	http://www.mcafee.com/	BW Digitronic, Tel. 01/940 44 10	Pro: Betriebssystem egal, preisgünstigstes Produkt Contra: Schlechteste Erkennung im NCSA-Test, wenige Updates

***Angegeben ist der Preis der Windows-95-Version.**
**** Erkennungs-/Desinfektionsrate in % im NCSA-Test. Gibt an, wieviel Prozent der getesteten Viren erkannt bzw. sogar desinfiziert werden konnten. Der NCSA-Test wurde im Auftrag der Zeitschrift PC World USA im Frühling 1997 durchgeführt.**
***** Erkennungsrate von «In the Wild»/Makroviren in % im VTC-Test. Gibt an wieviele herkömmliche bzw. Makroviren beim Test erkannt wurden. Der VTC-Test wurde durch das Virus-Test-Center der Uni Hamburg im Frühling 97 durchgeführt (http://www.informatik.uni-hamburg.de/AGN/).**