VIREN

Brutale Würmer vernichten Ihre Daten! I LOVE YOU & Co. Kleine Programme aus dem Internet. Angehängt an Mails. Tückisch getarnt. Hier kommt Hilfe:

Wer in den vergangenen Wochen eine E-Mail mit der Überschrift »I LOVE YOU« bekam, hatte es in den allermeisten Fällen nicht mit einer neuen Flamme, sondern mit einem der gefährlichsten Viren seit langem zu tun. Der so genannte Loveletter-Virus gehört wie seine Verwandten Melissa oder Muttertag zu den gefährlichen Wurmviren (worms).

Wie eine weltweite Seuche

Die Programmierer dieser fiesen Spezies haben einen Weg gefunden, wie sich ihre Viren mit Hilfe des Internets beinahe selbständig verbreiten. Der beliebteste Trick: Das Wurmvirus nutzt den Versand von Dateianlagen per E-Mail, um sich als Trojanisches Pferd in das Computersystem der Opfer einzuschleusen. Dort angekommen, breitet es sich auf andere Computer im Internet oder im Firmennetz aus, indem es Kopien von sich selbst an Freunde und Geschäftspartner schickt, die es im Adressbuch des E-Mail-Programms findet.

Tricks gegen die Mailwürmer

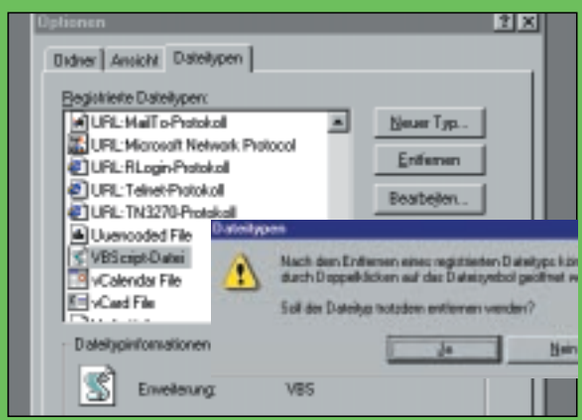
Schon allein dieser unfassbare Digitalmüll reicht bei einer größeren Viruswelle aus, um viele Server, die im Internet speziell die Mails verteilen, in die Knie zu zwingen. Was sie sonst noch für Schäden anrichten, hängt von der Kreativität des Virenprogrammierers ab – von Blödelmeldungen bis zum Löschen wichtiger Daten oder dem Formatieren der Festplatte ist alles drin. Und »I LOVE YOU« war nur einer von vielen. Nachfolger sind unterwegs. Aber keine Angst: Mit unseren Tricks verwandeln sich die gefährlichen Würmer in harmlose Blindschleichen.

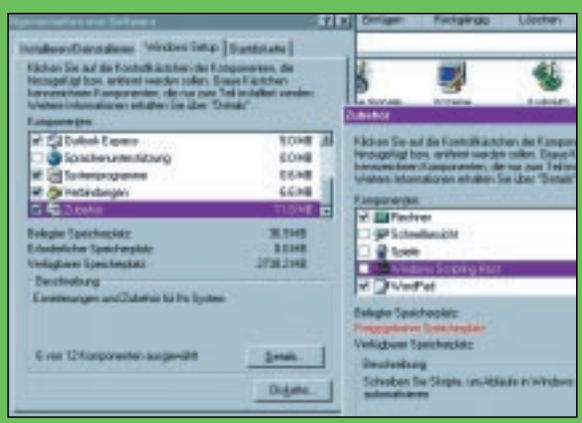
@ CHRISTIAN JUST

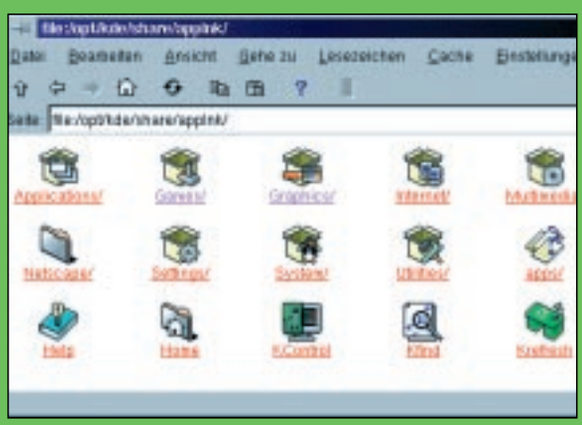
Wen können Viren per E-Mail am schlimmsten treffen?

Gefährlich werden Wurmviren wie Loveletter lediglich auf PCs mit Windows 98 oder Windows 2000 sowie auf PCs mit Windows 95 oder Windows NT 4, auf denen gleichzeitig Internet Explorer 5 installiert ist. Nur auf diesen Systemen kann der eigentlich gefährliche Teil des Virus, das als E-Mail-Anhang versandte VBScript »LOVE-LETTER-FOR-YOU.TXT.vbs« (Name variiert je nach Virus), automatisch bzw. durch Doppelklick ausgeführt werden. Die Details lesen Sie rechts.

So säubern Sie Ihren







KILLER

Rechner:

1 Win 95, NT, 2000 Unter Win 95 (und vergleichbar NT) mit installiertem Internet Explorer 5 muss man die automatische Dateiverknüpfung von vbs-Dateien mit einem ausführenden Programm entfernen. Öffnen Sie »Arbeitsplatz«, im Menü »Ansicht« den Eintrag »Optionen/Dateitypen«: Dort scrollen Sie nach unten bis zum Eintrag »VBScript-Datei«, klicken auf »Entfernen« und bestätigen die Nachfrage mit »Ja«. Bei Win 2000 klicken Sie dazu im Arbeitsplatz in den Ordner »Optionen«.

2 Windows 98 und 98/zweite Ausgabe Unter Windows 98 lässt sich die automatische Ausführung der potenziell gefährlichen VBScripts recht einfach in der Systemsteuerung ausschalten. Klicken Sie dazu auf den »Start«-Button, wählen »Systemsteuerung« und klicken dann dort auf »Software«: Nun markieren Sie hier im Menü »Windows Setup« in der Rubrik »Zubehör« den Windows Scripting Host – und deinstallieren ihn mit einem Mausklick auf den entsprechenden Button.

3 Linux, MacOS, BeOS, OS/2 VBScript gibt es nur für Windows – daher bleiben die populären VBS-Viren auf anderen Betriebssystemen wie Linux (Bild links), Mac, BeOS oder OS/2 ohne Wirkung. Wer allerdings eine infizierte Mail samt Anlage an einen Windows-PC weiterreicht, kann den Virus zumindest weitergeben. Für den Eudora-Internet-Mailserver ist unterwww.mactcp.org.nz/eims/eimsfilters.html ein Filter erhältlich, der den Loveletter-Virus schon unterwegs abfängt.

Illustration: Thomas di Paolo

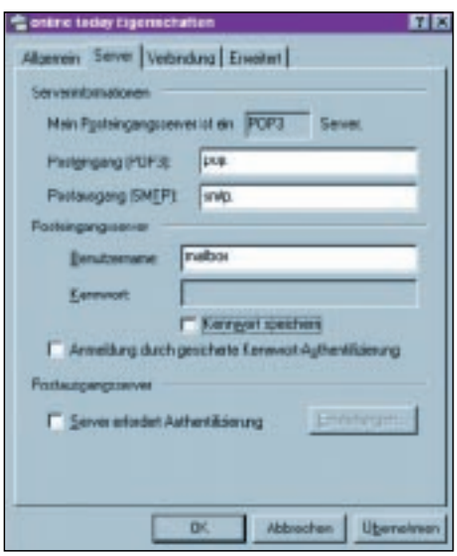
Schützen Sie Ihre Mail-Software

Am schnellsten verbreiten sich die berüchtigten Viren per E-Mail. Für einen Virus ist nichts einfacher, als sich einzunisten und über das Adressbuch weiterzuverteilen.

Achtung: Eine Mail allein bringt noch keinen Virus – der Anhang ist's! Öffnen Sie nie einen Dateianhang (Attachment), ohne ihn vorher geprüft zu haben (Software siehe S. 14):

Misstrauisch sein!

1 Ob Ihr Mailprogramm nun im Browser steckt (Outlook Express im Internet Explorer oder Netscape Messenger), Sie Eudora, Pegasus oder PostMe nutzen: Kein Mailprogramm lässt automatische Zugriffe auf angehängte Daten zu. Mit Viren verseuchte Dateianhänge werden erst durch Doppelklick gestartet. Wer fragwürdige Mails mit unangeforderten Dateianlagen sofort löscht, hat nichts zu befürchten! Seien Sie misstrauisch, auch wenn die Mail scheinbar von einem guten Bekannten kommt – dessen Mailprogramm könnte ja auch verseucht sein.

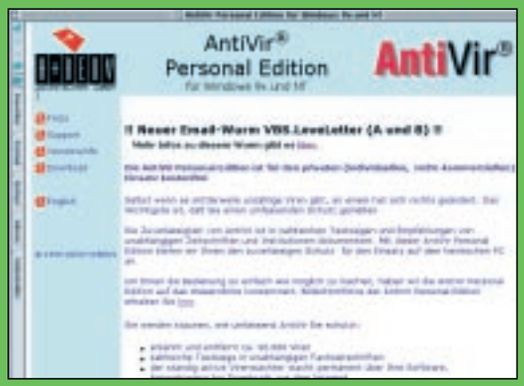


Gefahr bei Outlook

2 Das Mailprogramm Outlook ist bei Virenprogrammierern besonders beliebt, denn Viren können hier ohne weiteres auf das eingebaute Adressbuch zurückgreifen, um massenweise Kopien der verseuchten Mail zu versenden. Um den klammheimlichen Versand von Virusmails zu verhindern, sollten Outlook-Benutzer dem automatischen Versand einen Riegel vorschieben und den Datentransfer beobachten. Tipp: Das Passwort für den Mailzugriff unter dem Menü »Extras/Konten« bei »Eigenschaften/ Server« nicht speichern, sondern vor dem Mailversand stets manuell eingeben.

Anti-Viren-Programme

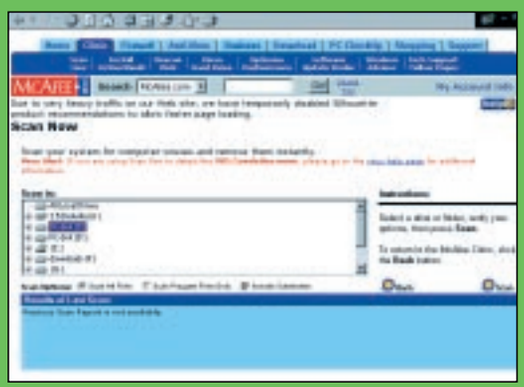
Sie können sich schützen und effektiv Viren aller Art abwehren. Da immer wieder neue Varianten des Loveletter-Virus und anderer Wurmviren erscheinen, ist der Einsatz eines Anti-Viren-Programms die beste Lösung. NIcht vergessen: Nur regelmäßige Updates dieser Programme sorgen für wirklichen Schutz! Wir stellen Ihnen die wichtigsten Angebote vor.



AntiVir

www.free-av.de

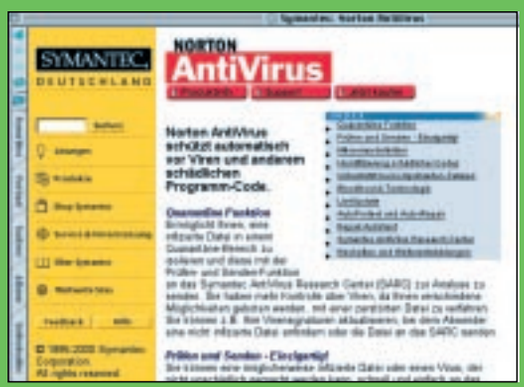
Speziell für Privatnutzer hat die Tettnanger Firma H+BEDV die kostenlose Personal Edition der sonst vor allem auf Netzwerke und Unternehmen zugeschnittenen Software AntiVir Professional zusammengestellt. AntiVir ist recht aktuell, erkennt diverse Varianten des Loveletter-Virus und beseitigt gefundene Virenschäden nach Möglichkeit sofort.



McAfee Clinic

clinic.mcafee.com

Virencheck einfach online – auf diese Weise ist garantiert, dass immer die neuesten Virenwarnungen berücksichtigt werden. Etwas Software wird auch hier installiert, doch dann erfolgt der Virenscan tatsächlich über den Browser selbst. 14 Tage kann man den Dienst kostenlos nutzen, sonst zahlt man 29,95 US-Dollar pro Jahr (Einführungspreis).



Norton AntiVirus

www.symantec.de

Norton AntiVirus ist ein Klassiker, den es für Windows und Mac gibt (69/149 Mark). Updates der Virendaten werden mindestens einmal im Monat auch automatisch installiert. Das Symantec AntiVirus Research Center sorgt für zuverlässigen Schutz. Tipp: Für den akuten Bedarf kann man sich die voll funktionsfähige 30-Tage-Testversion laden.

Trendmicro

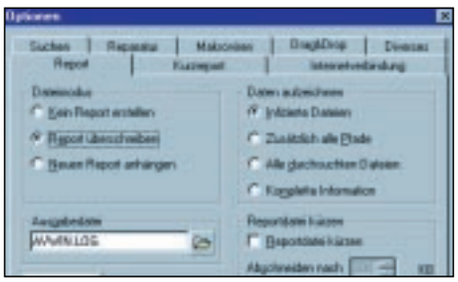
www.trendmicro.de

Trendmicro ScanMail-Virusscanner erkennen gefährliche Viren bereits auf dem Mailserver, bevor die Daten und die Empfänger weitergeleitet werden. Interscan VirusWall schützt das Unternehmensnetzwerk, und für den Einzelanwender gibt es OfficeScan. Unterstützt werden neben Windows NT und Novell Netware einige Unix-Betriebssysteme.

Gratis-Schutz: Installation von AntiVir Personal

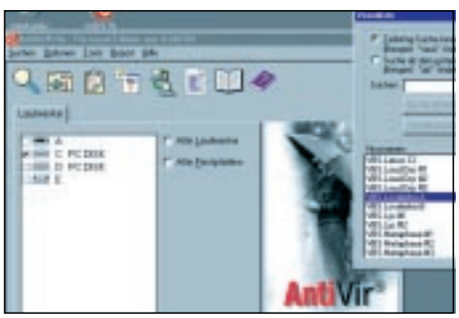
Installieren

1 Der Installer wird mit einem Doppelklick gestartet; der Rest läuft automatisch.



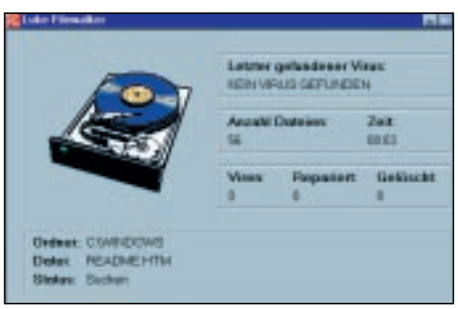
Starten

2 Nach einem Systemstart kann man alle Einstellungen der Software vornehmen.



Gezielte Suche

3 Bei konkretem Verdacht ist ein Blick in die Liste der bekannten Viren hilfreich.



Prüfergebnis

4 Glück gehabt – dieser PC ist virenfrei. Nicht vergessen: regelmäßig prüfen!

@ Weitere Anti-Viren-Infos in unserem Software-Guide www.online-today.de/software

Fünf Schritte zum sicheren PC

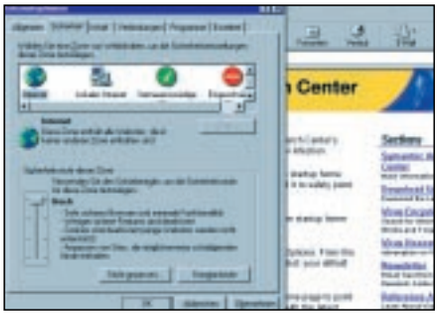
1 E-Mail-Anlagen nur öffnen, wenn Inhalt und Absender bekannt sind. Anlagen mit der Endung ».vbs« grundsätzlich löschen

2 Downloads von Software (Share- und Freeware) nur von vertrauenswürdigen Anbietern, die ihre Angebote auf Viren prüfen

3 Disketten und Wechselmedien (z. B. ZIP) vor Benutzung mit Anti-Virus-Software checken; speziell natürlich fremde Discs

4 Deaktivieren Sie VBScripts deinstallieren Sie Windows Scripting Hosts (Details Seite 15 »So säubern Sie Ihren Rechner«).

5 Browser: Sicherheitseinstellungen erhöhen, Script-Inhalte ausschalten, WinScripting Host nach der Installation von Internet Explorer 5 deinstallieren



Infiziert? So retten Sie Ihren PC!

Ein einfacher Test klärt, ob der Loveletter-Virus bei Ihnen zugeschlagen hat: Ist die Suche nach den Dateien »Win32DLL.vbs«, »MSKernel.vbs«, »LOVE-LETTER-FOR-YOU.txt« oder »LOVE-LETTER-FOR-YOU.HTM« im Windows-Systemverzeichnis erfolgreich, so war der Virus bereits aktiv!

Manuelle Beseitigung:

Zunächst müssen Sie die vier genannten Dateien sowie sämtliche veränderten Multimedia-Dateien mit neu angehängten Endungen ».vbs« löschen, also »vbs.vbs«, »vbe.vbs«, »mp3.vbs«, »jpeg.vbs« und Ähnliche. Dann müssen Sie die vom Virus veränderte Startseite im Internet Explorer wieder zurücksetzen und eine Reihe von Einträgen in der Windows-Registry entfernen. Anwender des Chat-Programms mIRC müssen die Datei »script.ini« löschen, um eine Weiterverbreitung des Virus im Chat zu verhindern.

Eine ausführliche Anleitung zur manuellen Entfernung des Virus finden Sie auf Deutsch unter www. heise.de/newsticker/data/nl-04.05.00-001/ sowie auf Englisch bei den Symantec-Experten ww.sarc.com/avcenter/venc/data/vbs.loveletter.a.html.