ILLUSTRATION MICHAEL KLEIN

# Wurmstichig

## PC-Schädlinge wie der Sasser-Wurm sind äusserst erfolgreich. Anwender könnten aber die Gefahr auf ein Minimum reduzieren.

**von Bruno Habegger**

Das nigelnagelneue Notebook von Buchhalter K.W. gab bereits nach wenigen Tagen den Geist auf: Virenbefall! Dabei war das Notebook bloss eine Stunde ans Internet angeschlossen gewesen – allerdings mit einem vom Hersteller vorinstallierten Antiviren-Programm, das seine letzte Aktualisierung vor über einem Jahr gesehen hatte.

**Hersteller und Anwender,** die Windows und die Virenjäger von Norton, Kaspersky, Norman & Co. derart veralten lassen, handeln fahrlässig. Um sich einigermassen wirkungsvoll zu schützen, genügt es nicht länger, auf das Öffnen von Anhängen in E-Mails zu verzichten. Moderne Schädlinge, so genannte Würmer, benötigen den Anwender nicht länger als Steigbügelhalter zum «Aufsteigen» auf ein fremdes System. Sie schmuggeln sich dank Sicherheitslücken in Windows hinein und machen sich in System, Netzwerk und damit auch im Internet breit.

Beispiel Sasser: Der kürzlich aufgetretene, sich massenhaft verbreitende Wurm nutzt eine Lücke in einem Bereich von Windows 2000 und XP aus, der zur Authentifizierung in Netzwerken dient. Bei Befall bringt der PC eine Meldung wie in Screen 1 und fährt selbstständig mehrfach hintereinander herunter. Sasser nimmt ausserdem nach dem Zufallsprinzip Kontakt mit beliebigen anderen PCs im Internet auf. Gemein: Hat er ein offenes System gefunden, sorgt er dafür, dass der eigentliche Wurm nachgeladen wird – von einem anderen infizierten PC. Und noch gemeiner: Per E-Mail werden Links angeboten, die den Sasser-Wurm angeblich entfernen. Dahinter könnte sich allerdings auch eine Variante des E-Mail-Wurms Netsky verstecken... Dessen jüngste Vertreter haben kürzlich mehrere Bildungs-Webseiten mit sinnlosen Anfragen (DOS-Angriff) in die Knie gezwungen. Viel schlimmer: Nach Angaben von Trend Micro führen 60 Prozent der kursierenden Würmer weitere Programme mit sich, die den befallenen Rechner für Hacker sperrangelweit öffnen.

**Die neuen Würmer dringen** immer schneller durch die Sicherheitslücken in Windows: Nur 16 Tage nach Bekanntwerden der Lücke verbreitete sich Sasser. Noch im letzten Jahr brauchten die Virenschreiber Monate. Ein schwacher Trost, dass auch der Zeitraum, bis Netzverseucher dingfest gemacht werden, immer kürzer wird. Eine Woche dauerte es beim Sasser-Autor. Der 18-Jährige scheint verpfiffen worden zu sein. Bei dem von Microsoft ausgesetzten Kopfgeld in der Höhe von 250000 Dollar kein Wunder.

Anwender von Windows XP können sich gegen Sasser wehren. Sobald eine Meldung erscheint, der Rechner müsse heruntergefahren werden, Screen 1, klicken Sie im START-MENÜ auf «Ausführen» und tippen Sie «shutdown -a» in die Befehlszeile. So wird der Restart-Vorgang unterbrochen und Sie können mit Hilfe der Anleitung auf www.pctipp.ch (WEBCODE 27279) den Wurm entfernen. Oder von einem der Antiviren-Hersteller ein Entfernungs-Tool herunterladen.

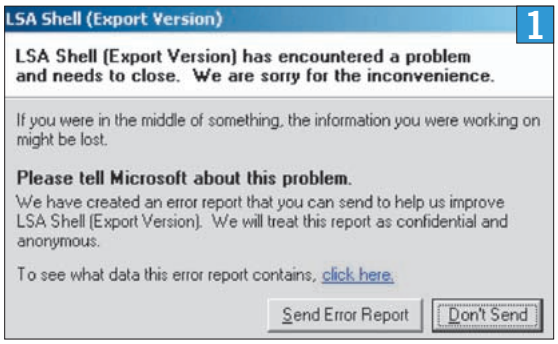
**Mit jeder neu entdeckten** Sicherheitslücke verschärft sich die Situation in der Mailbox. Beachten Sie deshalb folgende, allgemeine Sicherheitsregeln:

- Halten Sie Ihren Virenscanner stets aktuell.
- Installieren Sie eine Software-Firewall. In Windows XP finden Sie diese mit einem Rechtsklick auf die Netzwerk- oder DFÜ-Verbindung und einem Klick auf EIGENSCHAFTEN.
- Installieren Sie immer sofort alle Korrektur-Programme von Microsoft. Besuchen Sie dazu die Windows Update Site (http://windowsupdate.microsoft.com) und schalten Sie das automatische Update in Windows XP mit SYSTEMSTEUERUNG/SYSTEM/AUTOMATISCHE UPDATES ein. Setzen Sie ein Häkchen hinter die Option «Den Computer auf dem neuesten Stand...».
- Öffnen Sie niemals Anhänge, ohne sie vorher geprüft zu haben. Auch E-Mails von Bekannten können virenverseuchte Anhänge enthalten.
- Benützen Sie E-Mail-Programme, die HTML-E-Mails standardmässig als Text anzeigen. Outlook 2003 kann dies im Gegensatz zu den Vorgängerversionen.

■ Prüfen Sie den Namen des Anhangs. Endet er auf .pif, .vbs, .exe oder ein anderes Ihnen vielleicht unbekanntes Format, könnte es sich um einen Virus handeln. Bitten Sie die Absender, Ihnen Anhänge immer als .zip-Datei zuzusenden.
■ Tipp: Bitten Sie Ihre Bekannten, Mails mit einem bestimmten Wort in der Betreffzeile zu versehen. So können Sie leicht den E-Mail-Filter oder den Regelassistenten einsetzen, um gefährliche Mails auszusortieren.

Bisher blockierten die Würmer lediglich Server oder dienten dazu, Software für andere Zwecke zu installieren, etwa zum Angriff auf fremde Server oder zum Versand von Spam. Mit Witty ist nun aber ein brandneuer Wurm aufgetaucht, der an Daten und Betriebssystem schwere Schäden anrichtet. Buchhalter K. W. hilft jetzt ebenfalls mit, das zu verhindern, und hat unverzüglich einen aktuellen Virenscanner und eine Firewall installiert.

Mehr zum Thema Sicherheit im Internet erfahren Sie im Artikel «Spionage-Gefahr», ab S. 28. ■




**So siehts aus, wenn Ihr PC vom Sasser-Wurm befallen ist**

MEINUNG

# 735 oder 710?

**Intel schafft die Taktfrequenz im Prozessornamen ab. An ihre Stelle tritt eine dreistellige Nummer. Damit wird der PC-Kauf nur noch komplizierter.**

**Sascha Zäch, Redaktor**

Soll es ein Notebook mit dem Prozessor-Modell Pentium M 735 oder doch lieber eines mit Pentium M 710 sein? Diese Frage werden sich Anwender künftig beim Kauf eines Rechners stellen müssen. Für Verwirrung ist gesorgt. Intel möchte dem Benutzer «die Gesamtheit der Funktionen» seiner Prozessoren besser vermitteln und führt deshalb demnächst ein neues Bezeichnungssystem ein. Die Angabe der Taktfrequenz entfällt, stattdessen ziert eine dreistellige Zahl den Prozessornamen. Sie berücksichtigt auch Merkmale wie Architektur, Cache und Frontside-Bus. Jahrelang pflegte Intel die Taktfrequenz als alleinigen Gradmesser für die Leistung eines Prozessors. Anwender wussten – oder glaubten es zumindest – dass ein Pentium 4 3,2 GHz mehr Leistung bringt als ein Pentium 4 2,8 GHz. Jetzt soll plötzlich alles anders sein. «Der Prozessor lässt sich mit der Taktfrequenz allein nur unzureichend beschreiben», so Intels neue Sicht der Dinge. Für Notebooks seien Merkmale wie längere Akkulaufzeit oder integrierte WLAN-Funktionalität auch wichtig. Klingt eigentlich logisch. Das Nachsehen für Intels späte Einsicht hat der Anwender. Ihm wird, entgegen der Darstellung von Intel, die Kaufentscheidung nicht erleichtert. Er muss sich mit einem komplizierteren System herumschlagen. Eine höhere Zahl im Prozessornamen bedeutet nicht wie bisher mehr Leistung. Wer Genaueres über die Spezifikationen eines Chips wissen will, muss sich selbst informieren. Ausserdem setzt Intel die Kenntnis von weiteren technischen Merkmalen wie Frontside-Bus und Cache voraus. Diese Begriffe sagen aber vielen Anwendern gar nichts.
Mehr zum neuen Namenssystem der Intel-Prozessoren erfahren Sie in «Generationenwechsel», Seite 74.

## KURZINFOS

**■ GOOGLE-BANNER**
Die Suchmaschine Google vermarktet neuerdings Online-Werbung mit Bildern, etwa Werbebanner. Allerdings nur für fremde Webseiten: Google selbst soll nach wie vor frei von Bannern bleiben.

**■ ANTI-SASSER**
Das Sasser Worm Removal Tool von Microsoft gibts seit kurzem in der neuen Version 4.0. Es erkennt neben den A- bis E-Varianten des Wurms auch die F-Variante (www.microsoft.com/downloads).

**■ EXCHANGE MIT LINUX**
Die Microsoft Outlook nachempfundene Linux-Mailsoftware Evolution kann jetzt gratis mit einem Exchange-2000-Server zusammenarbeiten. Novell hat die bisher kostenpflichtige Software Ximian Connector gratis zum Download freigegeben (www.ximian.com).

**■ OPENOFFICE 1.1.2**
Die Entwickler von OpenOffice.org haben in der Version 1.1.2 der Büro-Suite vor allem Fehler korrigiert. Gleichzeitig haben sie eine erste, allerdings noch nicht stabile Version von OpenOffice 2.0 zum Download bereitgestellt.

**■ WLAN LAHM LEGEN**
Australische Sicherheitsexperten haben eine Lücke im WLAN-Protokoll gefunden. Mit einem PDA und eingeschobener Wireless-Karte können in Reichweite befindliche drahtlose Netzwerke für die Dauer des Angriffs komplett lahm gelegt werden. Abhilfe soll es derzeit noch keine geben.