

KNOW-HOW: TIPPS GEGEN FIESE VIREN

Aus PC Direkt, Ausgabe 8/2004

Würmer wohnen im Systemverzeichnis

Haben Sie den Verdacht, dass ihr PC infiziert ist, obwohl der Virens Scanner nichts findet? Bevor Sie sich einen zweiten Scanner kaufen, können Sie sich selbst auf Virenjagd begeben. Drei Stellen sind für die Suche lohnenswert: in den Systemordnern, bei den aktiven Programmen und bei den Programmen, die beim Booten starten.

Die meisten aktuellen Würmer nisten sich im Windows- oder im Systemordner ein (bei Windows 2000/XP: System32). Deshalb schadet es nicht, alle paar Wochen den Inhalt dieser Ordner im Explorer auf verdächtige Dateien hin zu durchforsten. Voraussetzung ist, dass im Explorer-Menü Extras/Ordneroptionen/Ansicht folgende Optionen ausgeschaltet sind: Erweiterungen bei bekannten Dateitypen ausblenden und Geschützte Systemdateien ausblenden (empfohlen). Umgekehrt sollten die Optionen Inhalte von Systemordnern anzeigen und Versteckte Dateien und Ordner: Alle Dateien und Ordner anzeigen aktiv sein. Sinnvoll ist es außerdem, die genannten Ordner nach Datum zu sortieren: Meist sind die Würmer neuer als die Windows-Systemdateien.

Fallen bei der Kontrolle ausführbare Dateien mit ungewöhnlichen Namen auf, informiert eine Suchmaschine wie Google, ob ein bekannter Wurm oder Dialer diesen Dateinamen benutzt. Auch spezialisierte Datenbanken wie www.sysinfo.org und eine Suche in Newsgroups (groups.google.de) helfen weiter. Gibt es keinerlei Infos zu dem betreffenden Dateinamen, so kann auch das eventuell auf einen Virus hindeuten, denn die Biester verstecken sich gerne hinter zufällig generierten Namen wie 12345_up.exe.

Danach ist zu prüfen, welche Infos die Datei selbst über ihre Herkunft bereithält. Aber Achtung: Ein einziger unbedachter Mausklick könnte den potenziellen Virus starten! Fehlt im Eigenschaften-Fenster (rechte Maustaste: Eigenschaften und dann Version) die Versionsseite oder enthält sie merkwürdige Einträge, ist das ein weiteres Verdachtsmoment. Löschen Sie die Datei jedoch nicht leichtfertig, sie könnte sich immer auch als harmlose System- oder Anwendungssoftware entpuppen.