KRIMINALITÄT IM INTERNET

Geist aus der Flasche

Der weltweite Schaden durch den Loveletter-Virus wird auf rund 600 Milliarden Schilling geschätzt. Der verhängnisvolle Liebesbrief ist einer von rund 70.000 verschiedenen Virenarten.

In wenigen Stunden um die Welt: Der Loveletter-Virus machte am 4. Mai 2000 auf drastische Weise klar, wie gefährlich Computerviren sind und wie schnell sie verbreitet werden. Ein Doppelklick aktiviert den Makro-Virus; wie der Geist aus der Flasche beginnt er das Zerstörungswerk. Er arbeitet rastlos und zerstört zunächst Dateien mit der Endung *.jpg, *.jpeg, *.mp3 und *.mp2, also Bild-, Ton- und Videodateien. Dann verschickt sich der Virus als Kopie an alle, die im Adressbuch für E-Mails aufscheinen.

Sein Vorgänger Melissa hatte sich noch mit den ersten 50 E-Mail-Adressen begnügt. Auf den Philippinen in die Welt gesetzt, tourte der heimtückische Liebesbrief über Hongkong nach Großbritannien, von dort aus nach Deutschland und Österreich, in die USA und weiter nach Japan – innerhalb weniger Stunden.

Die Verbreitung erfolgte nicht nur über die Adresslisten, sondern auch über alle Teilnehmer, die am Internet Relay Chat (IRC) angeschlossen sind, in dem sich ein Infizierter eingeklinkt hatte. Der Virus überschrieb auch die Registry (früher: win.ini) des am meis-ten verwendeten Betriebssystems und füllte sie mit sinnlosen Befehlen an. Die Registry ist eine Konfigurationsdatei, die das Zusammenspiel der einzelnen Komponenten eines Computers steuert. Der Virus wirkt, als wären in einen Motor wahllos Schraubenschlüssel hineingeworfen worden. Beim Neustart des Computers funktioniert fast nichts mehr. Die Schäden durch den Loveletter werden auf 600 Milliarden Schilling (43 Milliarden Euro) geschätzt.

Gesundes Misstrauen ist jedem Anwender gegenüber allem anzuraten, was unter Liebe und Sex angeboten wird. Beim vorliegenden Infekt waren Bild-, Ton- und Videodateien verloren, und nicht mehr oder nur mit großem Aufwand wiederherstellbar. Es ist ratsam, Notfalldisketten anzulegen, von denen aus man den Computer starten kann. Das Anlegen von Notfalldisketten, die auch ein Abbild der Registry enthalten, wird bei jeder Neuinstallation des Betriebssystems empfohlen. Zumindest wöchentlich sollte eine Ergänzung erfolgen, um Änderungen einbeziehen zu können. Beim Start über die Notfalldiskette wären die Eintragungen in der Registry wieder hergestellt worden und die Programme hätten normal betrieben werden können. Danach hätte man den zerstörerischen Loveletter löschen können. Da sich der Virus in das System mit den Dateinamen MSKernel32.vbs, Win32DLL.vbs und LOVE-LETTER-FOR-YOU.TXT.vbs hineinkopiert hat, lässt mit der Suchfunktion nach Dateien mit der Endung *.vbs suchen, sodass man die Virusdateien entfernen kann. Nach dem Auftreten des Liebesbriefs wurden innerhalb von Stunden Anti-Viren-Programme entwickelt und auf den Markt gebracht, mit denen der Virus entdeckt und entfernt werden konnte. Inzwischen gibt es zahlreiche Varianten des Loveletter-Virus, die eine laufende Anpassung der Schutzprogramme erfordern.

Kurt Hickisch/Christian Schmid

Öffentliche Sicherheit, Ausgabe 07-08/2000