MONITOR 6/00 – Computerkolumne der Südost copyright: Rolf Monitor

Windows: I love you
Viren fressen sich durchs Netz

Donnerstag 15.30 Uhr, I. Mehl (Name von der Redaktion geändert), Mitarbeiter des Internetproviders Telda.Net, bekommt eine Mail von einem Kollegen mit dem Betreff ILOVEYOU. Herr Mehls erster Gedanke dabei ist nicht für die Öffentlichkeit bestimmt (Man könnte ihn kurz zusammenfassen mit: Ist der jetzt völlig durchgeknallt?). Er öffnet die Mail und damit nimmt das Schicksal seinen Lauf. Weltweit tun in den nächsten Stunden Millionen Menschen etwas ähnliches: bei der NASA, beim Geheimdienst CIA und BND, bei Regierungsstellen und Behörden. Betroffen sind nur Windows-Anwender. Aber das sind über 90 Prozent aller Computernutzer. Sobald der Anhang angeklickt wurde, vermehrt sich der Virus (da er sich über E-Mails verbreitet, bezeichnet man ihn eigentlich als Wurm) über System-, Bild und Sound-Dateien auf der Festplatte. Er bereitet seine Verbreitung über Chat und E-Mails vor und versendet sich an in der Email-Software Outlook gespeicherte Adressen. Einige Firmen – wie auch der oben erwähnte Provider - reagieren schnell und schützen die eigenen Kunden oder Mitarbeiter, indem sie alle mit dem Virus verseuchten Mails an den Absender zurückschicken oder löschen.

Bilanz nach einer Woche: Schaden 32 Mrd Mark (so der britische Versicherer Lloyds), 29 Loveletter Varianten (eine sogar mit dem Betreff „virus alert“, also „Virus Alarm“, normalerweise eine Information über einen neuen Virus), diverse unschuldig Verdächtigte durch die Philippinische Polizei, aber auch durch Interpol, möglicher Anspruch auf Schadensersatz, wenn Sie den Virus von einer Behörde bekommen haben, möglicher Anspruch auf Schadensersatz, weil Microsoft nicht rechtzeitig vor dem Virus gewarnt hat.

Des weiteren: Hektische Gesetzesaktivitäten: England will Einrichtungen schaffen, um jede Email „abhören“ zu können. In Deutschland fordert die Arbeitsgruppe „Informationstechnische Bedrohung für kritische Infrastrukturen“ (KRITIS), ein „Nationales Alarmzentrum“ nach Vorbild der USA in Deutschland.

Neben der spektakulären Suche nach dem Autor des Virus muss die Frage erlaubt sein, ob nicht jeder, der im Auto ohne Sicherheitsgurt fährt (sprich: keine Antivirus-Software installiert hat) oder gar Hersteller, die gar keine Sicherheitsgurte anbieten (die mangelnde Sicherheit von Windows ist seit Jahren sprichwörtlich) mitschuldig sind. Immerhin tauchten die ersten Viren schon vor zehn Jahren auf. Heute gibt es ca. 17.000 Viren (davon sind allerdings nur ca. 170 aktuell im Umlauf) und täglich kommen 15 neue dazu. Bereits 1996 gaben 98 Prozent der US-Unternehmen zu, Sie Virenprobleme zu haben.

Das eine ist der Schutz, das andere ist die Frage, was denn überhaupt die Motivation der Virenprogrammierer ist. In Interviews geben sie an, dass es ein Weg ist, das Programmieren und die Betriebssysteme besser kennenzulernen. Sie entwickeln den Ehrgeiz, Sicherungsmechanismen auszuhebeln oder es macht einfach Laune. Nur einer hat bisher gesagt, das ihm das Zerstören fremder Daten Spaß mache. Einige Autoren erzählen auch, dass sie wieder aufgehört haben, weil es zu einfach sei.

In den meisten Staaten gibt es mittlerweile eine gesetzliche Grundlage, Virenautoren zu bestrafen. In den übrigen geben die Programmierer Interviews und unterhalten sogar Mailboxen zum Tausch von Viren.

Der Ausblick ist düster: Experten warnen vor weit gefährlicheren Computer-Angriffen und kritisieren mangelnde Sicherheitsvorkehrungen. „Was wir gerade mit dem Liebes-Virus erleben, ist der Anschlag aus einem fahrenden Auto mit einer Wasserpistole""

Linx:

Was macht ILOVEYOU und wie wird man ihn los? www.symantec.de
Bundesamt für Sicherheit in der Informationstechnik www.bsi.bund.de
Für den privaten Gebrauch kostenfreie Schutzsoftware www.complex.is/f-prot oder www.free-av.de
Die Zeitschrift Chip 5/00 zu Viren inkl. Test von Antivirensoftware www.chip.de
Weitere Links zum Thema: www.heise.de/ct/antivirus/
International Publication on Computer Virus Prevention www.virusbtn.com
Ironische Nachlese zum letzten Monat (Anklage der Gruppe Metallica gegen MP3 Anbieter): www.angelfire.com/nc2/boycottmetallica und www.paylars.com

Welche Virengruppen gibt es?

Boot-Viren setzen sich in Bereiche der Datenträger, die für den Start des Betriebssystems sorgen. Bei der Diskette ist das der Boot-Sektor, bei der Festplatte der Partitions-Sektor (engl. Master Boot Record, MBR) oder der Boot-Sektor. Die Viren werden durch einen Kalt- oder Warmstart (bzw. bei Daten-Disketten auch erfolglosem Boot-Versuch) aktiviert. Abhilfe: Start des Computers von einer virenfreien und mit einem System versehenen Diskette und Ausführen von FDISK.EXE /MBR.

Datei-Viren verbreiten sich über ausführbare Dateien (.exe oder .com) und durch Weitergabe dieser Programme. Abhilfe: Antivirensoftware, keine unbekannte Software auf den eigenen Rechner lassen..

Makro-Viren befallen Datendateien (z.B. MS Office Dokumente), die ausführbaren Code (Makros) enthalten können. Durch den weltweiten Austausch von Dateien steigt Ihr Anteil sprunghaft. Abhilfe: Die Ausführung von Makros nur gestatten, wenn man weiß, was sie tun.

Trojanische Pferde geben sich als nützliches Programm aus, enthalten aber Spionage- oder Schadensfunktionen (versenden z.B. die eigenen auf der Platte gespeicherten Passwörter).

Würmer vermehren sich über Netzwerke. Sie sind eigenständige Programme.

Grundsätzlicher Schutz:
Installation von Antiviren Software mit monatlichen Updates,
regelmäßige Datensicherung auf unterschiedliche Datenträger,
gesunde Skepsis bei Übernahme fremder Programme oder Dokumente.