Christiane Schulzki-Haddouti:

Würmer und Viren im Netz

Gefahren des Cyber-Terrors und seiner Bekämpfung

Internationale Politik, Jg. 59, Nr. 2 (Februar 2004), S. 41–48

Christiane Schulzki-Haddouti, Dozentin am Institut für Journalistik der Universität Dortmund, beschreibt die Risiken und Chancen des IT(Informationstechnologie)-Verbundes an praktischen Beispielen und bietet damit für „Nicht-IT-Spezialisten" einen über die Beschreibung der Gefährlichkeit von Computerviren hinausgehenden interessanten Artikel.

Die Ausbreitungsgeschwindigkeit der Computerviren wächst beinahe exponentiell: Brauchte im Frühjahr 2002 der Wurm CodeRed noch 37 Minuten für die Verdoppelung der infizierten Systeme, so benötigte der Wurm Slammer im Jänner 2003 nur mehr 8½ Sekunden dazu. Innerhalb von nur zehn Minuten waren mehr als 90 Prozent aller angreifbaren Systeme infiziert – und über 15 000 Bankomaten ausgefallen.

Das Schadenspotenzial erläutert sie an den IT-Folgen des 11. September 2001: Nicht nur in Lower Manhattan, ja in ganz New York City, Connecticut und Massachusetts wurden Festnetz- und Mobil-Telefone unterbrochen, es kam auch weltweit zu Ausfällen. Etliche transatlantische Netzverbindungen waren unterbrochen. Bis Rumänien fielen Netzwerke aus, das Forschungszentrum CERN in Genf war in Mitleidenschaft gezogen, und Südafrika verschwand mit seinen „.za"-Websites für einige Tage ganz aus dem Internet. In New Yorker Krankenhäusern konnten Ärzte nicht mehr auf die Datenbanken mit den für die Therapie benötigten Patientendaten zugreifen.

In Deutschland zeigte schon 2001 ein Planspiel die groben Sicherheitsmängel bei Firmen wie Bahn, Flugsicherung, Deutscher Bank, Lufthansa, Siemens oder Telekom auf. Generell gilt: Je komplexer die Informations- und Kommunikationssysteme werden, desto größer sind die Risiken. Wenn es brennt, brauchen nicht nur Unternehmen, sondern auch Behörden und Universitäten dringend Hilfe von so genannten Computer Emergency Response Teams (CERTs).

Schulzki-Haddouti geht auch der wiederum sehr aktuell gewordenen Frage nach, ob realistischerweise die Chance zur Früherkennung terroristischer Angriffsabsichten durch Datenvernetzung besteht, und kommt zu einem eher ernüchternden Schluss: Daten über die Terroristen von New York und Washington waren in Unmengen vorhanden. Aber erst nach dem 11. September konnten die Daten in einen sinnvollen Zusammenhang gebracht werden, vorher seien die Ermittler in den Datenmassen schier ertrunken. Rasterfahndungs-Programme sind für den Einsatz im Bereich der Wirtschaftsspionage wesentlich besser geeignet: Eine gezielte Abfrage der Flugpassagierdaten – wie sie die USA nunmehr von den Europäern einfordern – ermöglicht etwa Hinweise auf Geschäftsanbahnungen. Wenn man weiß, was man sucht, findet man es leichter.

Allerdings versucht die US-Regierung hier Abhilfe zu schaffen. 2003 zählte das General Accounting Office (GAO) des amerikanischen Kongresses noch zwölf verschiedene untereinander inkompatible Datenbanken zur Erfassung Terrorverdächtiger. Zwei Jahre nach dem 11. September 2001 beschloss die Bush-Regierung die Einrichtung einer zentralen Informationssammelstelle, des so genannten Terrorist Screening Center (TSC). Zeitgerecht warnen können wohl nur Experten, die die richtigen Puzzlestückchen schnell und flexibel zueinander legen.

Werner Lackner

Zur Erklärung: Als *Trojaner* wird ein Programm bezeichnet, das andere oder zusätzliche Funktionen ausführt als die Oberfläche erahnen lässt, z..B. heimliche Datensammlung, während Bilder (Bildschirmschoner, Pin-Ups etc.) angezeigt werden. Als *Virus* wird ein Code bezeichnet, der ohne Wirt nicht überleben kann und aus dem Grund in möglichst viele Dateien und insbesondere ausführbare Dateien eingefügt wird, damit er seine schädlichen Funktionen ausführen kann. Ein *Wurm* besitzt als bezeichnende Eigenschaft die eigenständige Fortpflanzungs- und Verbreitungsmöglichkeit sowie die Fähigkeit, Verbreitungswege zu anderen Rechnern zu finden, z.B. über Email-Adressen am infizierten Rechner.