Computersicherheit

Franz Marty

Die Computersicherheit ein immer wieder brisantes Thema – wir möchten hier deshalb wiederum auf Sicherheitsaspekte hinweisen.
Anfang Februar zwang ein sich rasant ausbreitender Virus verschiedene Mailserver in die Knie. Der Schaden hielt sich allerdings in Grenzen, die Verbindungen waren innerhalb von Stunden wieder hergestellt. Der Schädling belastete zwar den Internet-Verkehr, er zerstörte aber keine Dateien.

Neue Varianten

Unangenehmer sind neue Varianten von Würmern, welche ohne eigenes Zutun auf den Computer gelangen können. Der Eintritt erfolgt über Sicherheitslücken in der Software (vor allem Webbrowser und Netzwerksoftware des Betriebssystems) oder über offene Ports (Verbindungen des Betriebssystems nach aussen). Es werden praktisch täglich neue Viren entdeckt und Gegenmassnahmen ergriffen. Eine gute Übersicht und nähere Information findet sich z.B. auf http://www.sophos.com/downloads/ide/.
Augenfällig lehnt sich die Terminologie der Computerpiraterie stark an diejenige von biologischen, infektiösen Systemen. Wir sprechen von Monokultur, Virenbefall, Würmern und infizierten Systemen, neuerdings auch von «Polyvalenz» und «Polymorphismus». Die (Informations-) Konzepte der biologischen und elektronischen Welt scheinen eigenartigerweise verwandt, oder zumindest mit analoger Terminologie beschreibbar. Die Computerviren

- agieren oft auf mehreren Ebenen (Polyvalenz);
- nisten sich in eine System-Startdatei ein (Phagen);
- verbreiten sich über E-Mail an die auf dem Computer gespeicherten Adressen (Replikation);
- beenden antivirus- und andere sicherheitsrelevante Prozesse im Computer (Resistenz);
- verhindern Verbindungen zu Antivirus-Websites (Resistenz);
- können sich während der eigenen Installation verändern um einer Entdeckung zu entgehen (Polymorphismus).

Das Scrollen durch die Charakterisierung des «W32/Agobot-JI»-Virus (http://www.sophos.com/virusinfo/analyses/w32agobotji.html) gibt einen Eindruck über die Fähigkeiten dieser elektronischen Schädlinge.

«Trusted computing»?

Die Polyvalenz der Viren, der immer häufiger festgestellte Polymorphismus sowie die Resistenz gegen Abwehrmassnahmen stellen die Spezialisten vor immer grössere Probleme. Für uns Benutzer und die Antivirensoftware-Hersteller bedeutet diese Entwicklung einen immer grösseren Aufwand. «Trusted computing», eine vor zwei Jahren angekündigte Initiative von Intel, Microsoft und andern grossen IT-Frmen, möchte die Sicherheitstechnologie auf Ebene der Hardware (Sicherheits-Chip) einführen. Die Entwicklung einer solchen Technologie ohne Einschränkung der Daten- und Anwender-Autonomie des Benutzers scheint schwierig, eine Einführung ist nicht in Sicht.
Befolgt man einige wichtige Regeln, kann man sich auch heute schon gut vor Viren schützen.

- Mit einem Schlag von allen Problemen befreit ist man durch einen Wechsel auf ein Unix-System (Linux oder MacOSX). Für Linux sind einige Viren bekannt, allerdings ohne Relevanz für den täglichen Einsatz. Für MacOSX ist seit Einführung des Systems 2001 kein Virus von Bedeutung bekannt geworden.

Windows-Benutzer müssen weiterhin wachsam sein, einige einfache Massnahmen halten aber schon den allergrössten Teil der Viren zurück.

- In E-Mails keine dubiosen, unbekannten Dateien anklicken oder öffnen.
- Keine unbekannten Disketten/CD's einlesen. Vor allem auf seinem PC oder Laptop nicht die eigenen Kinder Software oder Spiele installieren lassen.
- Outlook und IE-Browsr möglichst sicher einstellen, oder besser auf alternative Software wechseln: «Firefox» als Browser und «Thunderbird» als E-Mail-Programm oder Mozilla bzw. Opera als integrierte Pakete. Alles sehr stabile, schnelle und einfach zu installierende Software.

http://www.mozilla.org/products/firefox/
http://www.mozilla.org/products/thunderbird/
http://www.opera.com/

- Bei einem ADSL-Anschluss: Der Computer ist, sofern nicht abgestellt, permanent vom Internet her erreichbar. Deshalb empfiehlt sich die Einrichtung einer Firewall. Eine solche ist in einem ADSL-

Modem oft schon integriert. Auf jeden Fall sollte in regelmässigen Abständen eine Kontrolle von aussen durchgeführt werden.

- Einsatz und regelmässiges Update einer Antiviren-Software.

Website: zur Sicherheitsüberprüfung

Studerus stellt auf einer Website Werkzeuge zur Überprüfung der Sicherheit des eigenen Computers zur Verfügung:
http://www.security-check.ch
Im «Security-Check-Test» kann durch das Anklicken eines Links ein «Browsercheck», ein «Quick Scan» und ein «Full scan» aktiviert werden. Der Server von Studerus überprüft in der Folge mit Angriffen von aussen den eigenen Computer, unsichere Sofware und offene Ports werden in einem Bericht fein säuberlich aufgelistet zurückgesendet.
Des weiteren findet sich auf der Website ein gut verständlicher Sicherheitsratgeber und ein Glossar.

Dr. med. Franz Marty
Erlenweg 8
CH-7000 Chur
franz.marty@primary-care.ch