PrimaryCare 2003;3:321

Trojaner, Dialer, Hoaxes, Viren und Würmer

Marcel Hanselmann

Mit dem Eingang der Informatik in den medizinischen Alltag müssen wir uns immer mehr auch um die Schattenseiten dieser Technologie kümmern. Waren es früher die Boot- und Dateiviren, die vor allem über die beliebten Floppy-Disketten verbreitet wurden, spielen heutzutage schadenstiftende Programme, die über das Internet ihren Weg zu unseren Maschinen finden, eine grosse Rolle. Diese Programme können sowohl unsere eigenen Computer wie auch die verschiedenen Server im Internet, die für den geregelten Datenverkehr zuständig sind, befallen und so indirekt unsere Verbindungen nach aussen stören.

Als Schutz davor wirken teils analoge Vorkehrungen, wie wir sie in der Medizin als Regeln der Asepsis kennen: den Kontakt mit potentiell infektiösen Daten meiden, schädliche Software entdecken und entfernen. Die Hersteller von Betriebssystemen müssen fortlaufend Sicherheitslöcher in ihren Programmen stopfen. Um von dieser Arbeit zu profitieren, müssen wir oft neuere Versionen von Programmen installieren (z.B. Internet-Browser), in denen die Sicherheitslücken geschlossen wurden.

http://www.trojaner-info.de/nachrichtendienst/index.html

Was sind Trojaner? Es handelt sich um schädliche Programme, die oft mit nützlichen Funktionen verbunden sind. Die Schadensfunktion, z.B. Übermitteln von Passwörtern, läuft im Hintergrund und für den Benutzer unbemerkt.

http://www.dialerschutz.de/home/International/international.html

Dialer sind Programme, die sich über kostenpflichtige, meist teure Verbindungen, ins Internet einwählen. Betroffen sind Benützer von analogen Modems und von ISDN-Verbindungen. ADSL- und Cable-Modems bauen keine Telefonverbindung auf und können deshalb auch keine entsprechenden Gebühren auflaufen lassen. Diese Dialer können z.B. als Zugangssoftware zu Bildern oder zu Musik installiert werden. Die normale Einwahlnummer des eigenen Internet-Providers wird durch eine andere Nummer ersetzt, das Resultat ist auf der nächsten Telefonrechnung sichtbar. Was dagegen unternommen werden kann, steht auf dieser deutschen Seite, die einen Abschnitt mit speziellen Informationen über die Situation in der Schweiz aufweist.

http://www.vhm.haitec.de/makro/

Makroviren heissen so, weil sie Anwendungsprogramme, die mit sogenannten Makro-Programmierungen ausgestattet sind, befallen. Es handelt sich dabei in erster Linie um Microsoft Word und Excel, auch für andere Office-Programme existieren Makroviren. Aus diesem Grund ist es auch gefährlich, Word- und Excel-Dateien als Mail-Attachment zu verbreiten. Der Absender ist dafür verantwortlich, dass die Attachments keine schädlichen Programme enthalten. Der Empfänger ist bei .doc- und .xls-Dateien immer im Ungewissen, ob er sich mit «malware» (*mal*icous soft*ware*) infiziert. Deshalb ist es ratsam, kurze Mitteilungen immer als reinen Text zu verschicken. Grössere Dokumente, bei denen die Formatierung wichtig ist, sollten sicherheitshalber als .pdf-Dateien verschickt werden und vom Empfänger mittels Acrobat Reader betrachtet werden.

Der Acrobat Reader ist gratis unter der Adresse http://www.adobe.com/products/acrobat/readstep2.html herabzuladen. Das Umwandeln von Dokumenten in .pdf-Dateien ist etwas aufwendiger; das entsprechende Programm von Adobe ist teuer. Die Firma Adobe stellt auf ihrer Website die Möglichkeit zur Verfügung, Dokumente via Internet in .pdf-Files umzuwandeln, was aber nach meiner Erfahrung eher eine Geduldsprobe darstellt.

Andere Hersteller stellen eigene Programme zur Verfügung, die ebenfalls dazu in der Lage sind. Ich habe diese nicht getestet. Für Linux-Benutzer existiert «tex2pdf», ein Tool, das aus dort verwendetem .lyx-Format .pdf-Dateien herstellt.

http://www.tu-berlin.de/www/software/hoax.shtml

Wer kennt sie nicht, die aufgeregte Mitteilung per E-Mail über gefährliche Viren mit hohem Schadenspotential; als Quelle wird oft eine öffentliche Autorität, wie z.B. die Kantonspolizei Zürich, im Betreff «Virus Warning» oder ähnliches aufgeführt, mit dem Hinweis, die Warnung an alle Bekannten und Freunde zu senden. Es handelt sich dabei um Computer-Viren, die keine sind: Hoaxes.

Als besonders gemeine Variante kann noch die Aufforderung enthalten sein, irgend eine für das System wichtige Datei zu löschen. Das Resultat ist ein nicht mehr laufendes Betriebssystem.

http://www.bsi.bund.de/av/

Wichtige Viren mit weiter Verbreitung und/oder grossem Schadenspotential sind ausführlich erklärt. Ebenso enthält die Seite viele Hinweise, wie man sich vor «malware» schützen kann.

Dr. med. Marcel Hanselmann
Hauptstrasse 52
CH-4528 Zuchwil
hanselmann.m@datacomm.ch