ILLUSTRATION JAMES YANG

Wie viel ist sicher?

Viren und Würmer machen Schlagzeilen. Das Bedürfnis nach mehr Sicherheit wächst bei Heimanwendern und KMUs. Doch was ist wirklich nötig?

von Bruno Habegger

Plötzlich war der Wurm drin. Erich E., der IT-Verantwortliche eines kleinen Unternehmens aus der Werbebranche, schlug die Hände über dem Kopf zusammen: Jetzt stand ihm eine Nachtschicht bevor. Halb so schlimm, wären das die einzigen schlimmen Folgen von Viren und Würmern. Kürzlich musste die Schweizerische Post ihre ganze Infrastruktur herunterfahren, weil sich ein alter Bekannter, der SQLSlammer, in ihre Systeme eingeschlichen hatte. Für Stunden ging nichts mehr – kein Telebanking, die Website blieb unerreichbar, Zahlungen am Schalter und am Postomaten konnten nur eingeschränkt abgewickelt werden. Der Übeltäter ist inzwischen beseitigt, doch die bohrende Frage bleibt: Welche Sicherheitsmassnahmen braucht der Anwender?

Das Maximum, wenn es nach den Herstellern und Vertreibern von Sicherheitslösungen geht. Entsprechend optimistisch schauen sie in die Zukunft: Allein der weltweite Markt für Antiviren-Lösungen soll von knapp zwei Milliarden US-Dollar im letzten Jahr bis 2007 auf das Doppelte wachsen. Firmen wie Symantec oder Network Associates profitieren von der Angst. Ihre Antiviren-Software für Heimanwender lässt sich nur für eine beschränkte Zeit mit aktualisierten Virensignaturen für die Erkennung neuer Schädlinge bestücken – derzeit ein Jahr. Danach wird der Preis für ein Jahresabo oder für eine neue Software-Version fällig.

Das Sicherheitsbewusstsein der Anwender wächst zwar, ist aber trotz aller Schreckensmeldungen noch immer ungenügend. Eine von PSINet Europe und Pan Security International (PanSec) durchgeführte Studie belegt, dass das Risiko durch Hacker-Angriffe auf ungeschützte Websites und Firmennetzwerke hoch ist. Jede zweite Firma sei ungenügend gesichert, so das Fazit der europäischen Untersuchung, für die acht Wochen lang ein ungeschützter sowie ein per Firewall gesicherter Server ins Internet gestellt wurde. Die Folge: Auf den geschützten Server erfolgten 1672 unbefugte Zugriffe, während der ungeschützte Server mit 19 128 Angriffen mehr als zehn Mal häufiger attackiert wurde.

Laut einer Untersuchung von Symantec wird die Bedrohungslage auch immer komplexer. Die Zahl der Würmer und Viren, die gleichzeitig mit unterschiedlichen Technologien zuschlagen können, nimmt ständig zu. Im ersten Halbjahr 2003 verzeichneten die von Symantec untersuchten Firmen weltweit im Durchschnitt 38 Angriffe pro Woche. Im selben Zeitraum dokumentiert die Studie 994 neue Viren und Würmer – doppelt so viele wie im ersten Halbjahr 2002.

Fazit beider Studien: Bereits minimale Schutzmassnahmen reduzieren das Risiko erheblich, Opfer einer Attacke zu werden.

Doch was wäre für einen optimalen Schutz wirklich nötig?

Heimanwender: Zur Grundausrüstung gehören zwingend eine aktuelle Antiviren-Software sowie eine einfach zu bedienende Desktop-Firewall. Im PCtipp wurde beides bereits getestet: Die entsprechenden Artikel finden Sie in der Orbit-Sonderausgabe 2003 und im PCtipp 9/2003. (www.pctipp.ch/archiv).

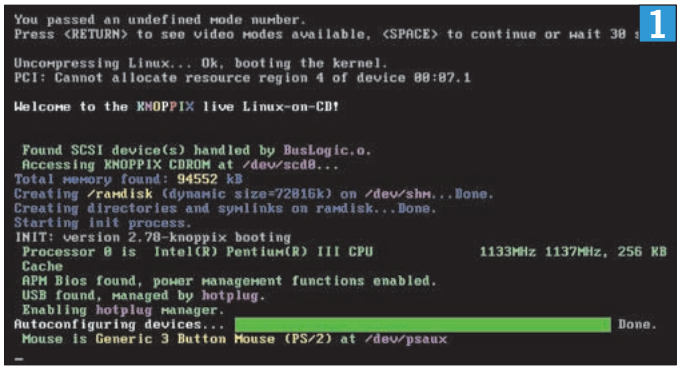
Desktop-Firewalls bieten nur dann einen gewissen Schutz, wenn sie richtig konfiguriert sind. Hängt an Ihrem PC ein eingeschaltetes Modem oder ein ISDN-Adapter, müssen Sie sich auch vor Web-Dialer-Programmen schützen. Informationen dazu finden Sie auf www.dialerschutz.de. Nützliche Programme gibts im Download-Bereich von www.pctipp.ch unter WEBCODE **20556** und WEBCODE **23008**.

Wer auf ADSL umsteigt, sollte statt eines billigen ADSL-Modems einen ADSL-Router wählen, auch wenn nur ein einziger PC daran hängt: Der Router verfügt bereits über grundlegende, das Risiko senkende Sicherheitsmechanismen.

Wer ganz sichergehen will, richtet zwei Betriebssysteme auf der Festplatte ein. Ein System verwenden Sie ausschliesslich für E-Mail und Internet, eines nur für allgemeine Arbeiten, die keinen Netzanschluss benötigen. Eine Anleitung, wie Sie dazu am besten vorgehen, lesen Sie unter WEBCODE **21083**.

Diese Sicherheit bedingt aber, dass Sie jedes Mal den PC neu starten müssen und ein Bootmanager (z. B. PartitionMagic, XFDisk, oder AcronisOS Selector) jeweils die Partition mit dem nicht benötigten Betriebssystem versteckt.

Am sichersten surfen und mailen Sie aber mit dem auf Linux basierenden CD-ROM-Betriebssystem Knoppix (www.knoppix.net), **Screen 1**. Es ist so einfach wie Windows zu bedienen und läuft direkt vom CD-Laufwerk – die lokale Festplatte wird dabei praktisch komplett für Zugriffe gesperrt.



Das Knoppix-Betriebssystem läuft direkt ab CD-ROM – sicherer gehts nicht

KMU: Kleine und mittlere Unternehmen benötigen im Prinzip dieselbe Ausrüstung wie Heimanwender. Zwischen ihrem Firmennetzwerk und dem Internetprovider sollte aber zusätzlich eine Hardware-Firewall ihren Dienst verrichten.

Aber auch diese muss gepflegt sein. Eine anspruchsvolle Arbeit, die viel Fachwissen verlangt, das KMUs selten haben. Mit dem Umstieg auf ADSL können KMUs aber von so genannten Managed Firewalls profitieren. Dabei nimmt der Anbieter (oft der ADSL-Provider selbst) die Konfiguration der Hardware-Firewall vor und pflegt sie per Fernbedienung. So können der Firewall – ähnlich wie Antiviren-Programmen – feste Angriffs-Erkennungsmuster beigebracht («Intrusion Detection») oder ganze IP-Adressbereiche gesperrt werden, aus denen ständig Attacken erfolgen. Zu guter Letzt sollten alle wichtigen Daten ständig gesichert werden – für den Fall der Fälle.

LINKS

Mehr Infos

PanSec: www.pansec.com
Astalavista: www.astalavista.ch
iFrame: www.iframe.ch
CERT: www.cert.org
BSI: www.bsi.de
Virusoffice: www.virusoffice.com
Sicherheit Online:
www.sicherheit-online.net

Die Sicherheitsexperten sind sich einig: Die Basis für einen optimalen Schutz legen die Anwender mit ihrem umsichtigen Verhalten. «Mitarbeiter müssen durch Schulung sensibilisiert werden», sagt Michael Jäger, Geschäftsführer der Netzwerk- und Unternehmensberatung iFrame. «Es ist nicht der bösartige Cracker oder der Wirtschaftsspion aus dem Ostblock, der KMU-Netzwerke bedroht und Kosten verursacht – es sind in erster Linie Viren.»

Pascal Mittner vom Sicherheitsspezialisten Astalavista bemerkt im täglichen Umgang mit Sicherheitsproblemen von KMUs immer wieder dieselben Fehler: Verwendung von nicht aktueller Antiviren-Software, laienhaft konfigurierte Systeme, an einzelnen PCs installierte Modems zur Umgehung der Firmen-Firewall und veraltete Betriebssysteme, für die keine Sicherheits-Updates mehr erhältlich sind. ■

MEINUNG

Wo bleiben die Urteile?

Spam-Mails nerven; und einige davon verstossen gegen geltendes Recht. Warum warten die Gerichte mit der Behandlung der anstehenden Fälle?


Gaby Salvisberg, Redaktorin

Etwa die Hälfte des gesamten Mailverkehrs besteht aus Spam. Inzwischen empfinden 70 Prozent der Benutzer den Umgang mit E-Mail als nervenaufreibend, 50 Prozent trauen dieser Kommunikationsform weniger als früher (siehe auch Seite 19), da befürchtet wird, dass wichtige Post in der Spam-Flut untergeht.

Zwar schimmert am Horizont die Morgenröte durch: Sowohl in der Schweiz als auch in der EU sind Gesetze am entstehen, die Spam verbieten sollen. Vor dem Jahr 2005 ist jedoch nicht damit zu rechnen, dass diese – zumindest in der Schweiz – in Kraft treten. Und bis dahin werden wir alle endgültig im Spam ertrinken.

Aber ganz so machtlos wären wir in der Schweiz nicht, wenn wir nur wollten! Schliesslich verstossen Spammer gerne gegen Gesetze, die schon längst in Kraft sind, so zum Beispiel das Datenschutz-, das Pornografiegesetz oder jenes gegen unlauteren Wettbewerb (UWG). Doch was tun die Gerichte, wenn ihnen solche Verstösse angezeigt werden? Sie wimmeln die Spam-Opfer ab oder schieben die Fälle so lange auf ihren Pulten hin und her, bis sie verjährt sind. Den Grund für diese Tatenlosigkeit vermuten viele Spam-Gegner in der mangelnden Sachkenntnis der Behörden.

Liebe Richter, so wird das nichts! Gibt es denn unter Ihnen keine spamgeplagten E-Mail-Benutzer? Sind es Ihre Sekretärinnen, die für Sie den Spam ausfiltern? Nehmen Sie sich doch endlich jener Fälle an, die seit Monaten oder Jahren auf Ihren Pulten liegen. Und geben Sie den Datenschutzbeauftragten mehr Handlungsspielraum. Ein Aussitzen dieser Fälle bis zum Sankt-Nimmerleins-Tag (oder bis 2005) löst das Problem nämlich nicht.

KURZINFOS

KONKURS

In der Orbit-Ausgabe stellte der PCtipp auch Sicherheits-Software der Firma F-Secure vor. Deren bisheriger Schweizer Vertreiber Netstuff ging leider im Oktober Konkurs. F-Secure-Produkte sind hier zu Lande aber weiterhin über die Firma Schnidrig Informatik (www.schnidrig.com) verfügbar.

1. UPDATE

Microsoft warnt vor einem Problem mit Office 2003: Werden Dokumente in Office 2000 bearbeitet und gespeichert, können beim Öffnen mit Word 2003, Excel 2003 und PowerPoint 2003 die Grafikinhalte verloren gehen. Ein Patch steht unter http://office.microsoft.com/OfficeUpdate bereit.

ÜBERTEUERT

Swisscom hat in den letzten vier Jahren für verschiedene Interkonnektionsdienste um bis zu 35 Prozent zu viel verlangt und muss deshalb die Tarife für TDC Switzerland (Sunrise) und MCI WorldCom nachträglich senken. So lautet ein Entscheid der Eidgenössischen Kommunikationskommission. Swisscom hat beim Bundesgericht Beschwerde eingereicht.

SCHNELLER

Intel steigert die Geschwindigkeit der günstigen Celeron-Prozessoren. Neu sind sie mit einer maximalen Taktfrequenz von 2,8 GHz erhältlich. Weitere Eckdaten sind 400 MHz System-Bus, 128 KB L2-Cache und Unterstützung der Multimediatechnologie MMX.

KOPFGELD

Microsoft hat mit einer Startsumme von fünf Millionen US-Dollar das so genannte «Anti-Virus Reward Program» gegründet. Es soll Strafverfolgungsbehörden helfen, Virenautoren vor Gericht zu bringen. Das Software-Haus will dabei Hinweise, die zur Verhaftung der Cyber-Täter führen, finanziell belohnen.