COMPUTERVIREN

Viren und Würmer im Netz

Die Gefährdung durch Hackerangriffe, Computerviren und andere Bedrohungen im weltweiten Datennetz nimmt zu. Viele Unternehmen haben keine oder nicht ausreichende IT-Sicherheitskonzepte.

Viren und Würmer belasten das weltweite Datennetz. Jedes Monat werden von Hackern und Saboteuren etwa 400 neue Computer-Parasiten geschaffen. Sie legen im schlimmsten Fall Rechner lahm und richten Chaos und enorme Schäden an. Der jüngste große Schädling war der Wurm "Sobig.F", der erstmals am 19. August 2003 in Österreich gesichtet worden war. Dieses Programm unterschied sich von anderen Würmern vor allem durch seine Geschwindigkeit – nach Einschätzung von Experten übertraf er bis dahin bekannte Schädlinge um das Zehnfache.

"Größte Epidemie"

Laut dem Moskauer IT-Sicherheitsunternehmen "Kaspersky Lab" handelte es sich beim Sobig.F-Wurm um die "größte Epidemie" in den vergangenen eineinhalb Jahren. Allein der Virenschutz des E-Mail-Dienstes GMX filterte innerhalb von drei Tagen mehr als 420.000 mit diesem Wurm infizierte E-Mails heraus. Sobig.F suchte nicht nur im Adressbuch, sondern auf allen Daten der Festplatten der Opfer nach E-Mail-Adressen, über die er sich mit gefälschter Adresse verbreitete – und zwar hundertfach gleichzeitig statt hintereinander. Allein in Österreich wurden in den ersten Tagen durch Sobig.F hunderttausende PCs angesteckt.

Nie zuvor schlug ein Virus derart massiv in Österreich zu. Eine echte Schadensfunktion enthielt der Wurm nicht, berichtete Josef Pichlmayr, Chef des österreichischen Softwareunternehmens Ikarus. Sobig.F behinderte aber den E-Mail-Verkehr und sorgte für erhebliche Mehrarbeit bei den Usern. Sobig.F ist die sechste Version des Sobig-Virus, der im Januar 2003 aufgetaucht ist. Wie seine Vorgänger trug Sobig.F einen Selbstzerstörungsmechanismus in sich – ein Ablaufdatum. Nach dem 10. September verschwand der Wurm. Nach Erkenntnissen des US-Bundeskriminalamtes FBI (Federal Bureau of Investigaten) dürfte Sobig.F über eine pornografische Internet-Newsgroup in Umlauf gebracht worden sein. Thomas Fischer vom Antivirensoftware-Hersteller "Sophos" vermutet, dass Sobig.F von professionellen Spammern versendet wurde, die an Techniken arbeiten, um ihre unerwünschten Botschaften mit Würmern zu verbreiten. Auf diese Weise sind die Urheber nicht mehr ermittelbar.

Fast täglich landen neue Viren und Würmer in den E-Mail-Boxen. Sie nutzen Lücken in den Betriebssystemen und die Unachtsamkeit oder Neugier der Benutzer. Schätzungsweise 80.000 verschiedene Viren sind seit 1983 aufgetaucht; nur wenige hundert von ihnen führten zu größeren Schäden. Der erste spektakuläre Parasit war der "Jerusalem-Virus"; er verbreitete sich ab 1987 über Disketten und andere Datenträger. Ein Jahr später registrierten die Virenjäger den ersten Internet-Wurm.

Viele Würmer täuschen durch falsche Adressen eine seriöse Herkunft vor. So ist der seit Mitte Oktober 2003 verbreitete Wurm W32/Swen @MM mit einer Microsoft-Absendeadresse versehen und verschickt Attachments. Die Programme haben Namen wie installer777.exe

und patch433.exe. Der Wurm, auch Gibe.F genannt, ist leicht zu erkennen: Die Dateigröße der Mails liegt zwischen 130 und 160 Kbyte; Microsoft verschickt niemals unaufgefordert Security-Updates und aus dem Mailheader ist nicht Microsoft, sondern eine andere Absenderadresse ersichtlich.

Die Zahl der Würmer werde weiterhin drastisch steigen, vermutet "Arge Daten"-Chef Dr. Hans G. Zeger und empfiehlt gute, individuell zusammengestellte Mailfilter: "Das sind bessere Frühwarnsysteme, als schlecht konfigurierbare Antivirenprogramme."

Für einen sicheren Mailverkehr sei es notwendig, "die Schnittstelle zwischen externer IT-Welt und internem Computersystem neu zu definieren". Dem Endbenutzer sollte am Bildschirm seines Computers eine sichere Umgebung bereitgestellt werden, die von seinem sonstigen Arbeitsbereich abgeschottet ist. Innerhalb dieser Umgebung kann er hereinkommende Dateien, Mails oder Webseiten übernehmen, testen und danach erst freigeben. Die Grundlagen derartiger Lösungen ("virtuelle Maschinen") gebe es laut Zeger seit Jahrzehnten, sie seien aber noch nicht in die gängigen Business-Betriebssysteme eingebaut.

Wurm-Mutationen

Manche Hacker verändern die Originalversionen von Würmern. Die Wurm-Mutationen können noch gefährlicher sein als ihre Ahnen. Nach Einschätzung des Stuttgarter IT-Unternehmens "NextiraOne" sind die Informationssysteme bei mehr als der Hälfte der Klein- und mittelständischen Unternehmen gegen Attacken von Internet-Würmern mangelhaft gesichert. Vielen Firmen mangle es an Ressourcen und dem erforderlichen Wissen. "In der Unternehmensspitze hat man sich oft nicht ausreichend mit dem Thema Datensicherheit auseinander gesetzt", warnt Massimiliano Mandato von "NextiraOne". So lange nichts passiert, werde kein Geld investiert, um die Verwundbarkeit der Informationssysteme zu beseitigen.

Schwachstellen bei den Sicherheitskonzepten gebe es nach Aussagen des Düsseldorfer Unternehmensberaters Ralf Sürtenich vielfach bei Notebooks und kleinen Firmen-Niederlassungen: "Das beste Sicherheitskonzept ist nicht stärker als die schwächste Stelle. Ein Notebook, das gesicherte Firmenzugänge benutzt und für normale Einwahlzugänge zum Internet eingerichtet ist, macht das beste Firewall-Konzept durchlässig." Ein weiteres Gefahrenpotenzial ergebe sich durch die zunehmende Verbreitung von drahtlosen Inhouse-Netzen (W-LAN). Sürtenich: "Das Sicherheitsproblem muss in alle Prozesse des Unternehmens einbezogen werden. Die Technik kann nur leisten, was durch Konzepte vorgegeben wird." Die Experten der US-Institution "Message Labs" schätzen, dass jede 166. E-Mail Viren enthält.

Laut dem deutschen Branchenverband Bitkom nimmt die Gefährdung durch Computerviren, Hackerangriffe und andere Bedrohungen in der digitalen Welt rasant zu. Im Schnitt beträgt der Schaden pro Virenbefall und Unternehmen 5.800 Euro. Bitkom schätzt die Zahl der "IT-Sicherheitsvorfälle" im ersten Quartal 2003 weltweit auf 160 Millionen, mit stark steigender Tendenz: Für das gesamte Jahr 2003 werden 700 Millionen Schadensfälle in der Informationstechnik erwartet. Der Branchenverband hat einen Leitfaden herausgegeben, in dem unter anderem Schritte für ein IT-Sicherheitskonzept beschrieben werden, das Grundlage der IT-Sicherheitsstrategie von Unternehmen sein sollte. Es wird erläutert, wodurch Arbeitsplatzrechner, Server, Netzwerke und Telekommunikationseinrichtungen bedroht werden und wie sich Unternehmen vor diesen Bedrohungen schützen können.

25 Prozent der großen österreichischen Unternehmen sind Opfer von Viren, Hackern und anderer Formen von Computer- und Netzkriminalität geworden. Das Bundesministerium für Inneres hat im September 2002 gemeinsam mit der Wirtschaftskammer Österreich (WKÖ) eine Kampagne gestartet, um das IT-Sicherheitsbewusstsein in der Wirtschaft zu verbessern. Laut WKÖ haben nur 36 Prozent der österreichischen Wirtschaftsunternehmen eine niedergeschriebene IT-Sicherheitspolitik. "Viele Unternehmen, vor allem kleinere und mittlere, vernachlässigen leider die Sicherheit in der Informationstechnik", erläutert Innenminister Dr. Ernst Strasser. "Wir wollen hier das Bewusstsein noch mehr schärfen, um Schäden zu vermeiden".

http://www.bmi.gv.at/

Deutsches Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi.de/

Bitkom-Leitfaden "Sicherheit für Systeme und Netze in Unternehmen": http://www.bitkom.org/

Microsoft: www.microsoft.com/security/antivirus/swen.asp

TU Wien: www.zid.tuwien.ac.at/security/links.php

Sophos-Vireninformation: http://www.sophos.com/virusinfo/

WÜRMER UND VIREN

Von "Melissa" bis "Sobig.F"

März 1999: Der Wurm "Melissa" verbreitet sich weltweit mit hoher Geschwindigkeit und befällt bereits am Tag Zehntausende Computer. Er pflanzt sich per elektronischer Post im Schneeballsystem fort und lässt die befallenen Rechner unter der Last eingehender E-Mails zusammenbrechen. Betroffene Unternehmen sind unter anderen Microsoft und Boeing.

April 1999: Der aus Taiwan stammende CHI-Virus (auch "Tschernobyl" genannt) verbreitet sich vor allem in Asien und richtet Millionenschäden an. Allein in China sind mehr als 200.000 PCs betroffen. Auch der Computerriese IBM ist Opfer der Attacke.

Mai 2000: Mit rasanter Geschwindigkeit verbreitet sich der virtuelle Wurm "I-love-you" über das E-Mail-Programm Outlook und richtet vor allem in großen Unternehmens-Netzwerken einen enormen Schaden an. Das Virus mit der Betreff-Zeile "I love you" hatte die Postfächer von Millionen Internet-Nutzern heimgesucht und die Netzwerke völlig überlastet. Schöpfer ist ein philippinischer Student. Er verursacht den bis dahin größten Schaden.

Juli/August 2001: "Code Red" infiziert weltweit Hunderttausende Internet-Rechner. Die erste Attacke des Wurms richtet sich gegen das Web-Angebot der US-Regierung. Er soll sich in den Computern einnisten, vermehren und dann zu einem bestimmten Zeitpunkt von dort aus die Webseiten des Weißen Hauses unter einer Datenflut zusammenbrechen lassen. Techniker können den Angriff verhindern.

September 2001: "Nimda", eine gefährliche Mischung aus Computervirus und Internet-Wurm, greift größere Server und Personal Computer an, die mit "Outlook Express" und dem "Internet Explorer" von Microsoft arbeiten. "Nimda" reißt etwa Lücken in das

Sicherheitssystem und macht den PC so von außen zugänglich. Sowohl Microsoft selbst als auch die Deutsche Bank sollen zu den Opfern des Virus zählen.

2003: Der Computer-Virus "LovSan" bringt weltweit Millionen Rechner mit dem Betriebssystem Windows zum Absturz. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet von einer "sehr hohen Verbreitung" des Virus in Deutschland und ruft die höchste Warnstufe aus. Der Virus enthält die Botschaft: "Billy Gates, warum lässt du das zu? Hör auf Geld zu verdienen und repariere deine Software!" ("billy gates why do you make this possible? Stop making money and fix your software!!")

August 2003: "Sobig.F", vom Software-Unternehmen "Ikarus" als "König der Viren" bezeichnet, rast durchs weltweite Datennetz. Der fünfte Abkömmling des Sobig-Virus verursacht enormen Ärger und Schaden.

ANTIVIRUS-SOFTWARE

Gesunde Geschäfte

Der Weltmarkt mit Antivirus-Software wird sich bis 2007 verdoppeln und ein Volumen von vier Milliarden Dollar erreichen. Den Hauptanteil am Wachstum tragen nach einer Analyse der Unternehmensberatung Frost & Sullivan mehrschichtige Sicherheitslösungen.

Mit Abstand die wichtigste Region im Weltmarkt für Antivirus-Software ist mit einem Umsatzanteil von 45 Prozent Nordamerika. Die Region EMEA (Europa, Naher Osten, Afrika) kommt auf 30 Prozent.

SOFTWARE

Schutz gegen Schädlinge

Computerviren befallen andere Programme und können bei jedem Start entweder sofort oder verzögert Schaden anrichten. Viren brauchen für ihre Verbreitung "Trojanische Pferde": Lädt sich ein Internet-Surfer etwa ein Gratisprogramm auf seinen PC, kann sich dahinter ein Virus verbergen. Würmer sind Viren, die sich eigenständig vermehren, meist über E-Mail, Internet oder Chat-Programme. Sie nutzen Sicherheitslücken in Programmen, um sich zu starten bzw. weiterzuverbreiten.

Was für die Autos die Bremsen sind, sollten für den vernetzten Computer Firewalls und Virenschutzprogramme sein. Wer sich nicht schützt, ist auch eine Gefahr für andere. Eine Firewall ist ein Programm, das den Datenverkehr zwischen Internet und eigenem Netz oder eigenem Rechner überwacht und verdächtige Daten nicht durchlässt.

Antivirenprogramme schützen nicht vor neuen Würmern und Viren, daher sollte die Software regelmäßig aktualisiert werden. Für Unternehmen ist eine IT-Sicherheitspolitik erforderlich.

Im E-Mail-Verkehr gilt: Unverlangte Attachments nicht öffnen; Programme nur von vertrauenswürdigen Websites downloaden.

Anbieter von Virenschutz-Programmen:

http://www.ikarus-software.at/

http://www.mcafee.com/

http://www.symantec.com/

http://www.sophos.com/

www.kaspersky.com/de