sueddeutsche.de Computer

09.01.2006 15:23 Uhr

An der Daten-Front

Unwissenheit schützt vor Viren nicht

Beim Thema Internet-Sicherheit ist nur eines sicher: Hundertprozentige Sicherheit existiert nicht. Dennoch gibt es die ein oder andere Maßnahme, mit der man seinen Computer gegen Virus- und Spamattacken wappnen kann – zumindest für den Moment.
Von Katharina Böhringer

Besonders fieses Subjekt: der Spammer. Foto: www.sicher-im-netz.de

Gerhard Forster kämpft mit Leib und Seele gegen einen unsichtbaren Feind. Sie heißen Viren, Trojaner, Spam, Würmer - und das sind nur einige der fiesen Elemente, die Computer befallen können. „Der Rechner kann blitzschnell zum ferngesteuerten Zombie werden“, warnt Forster, Geschäftsführer der IT-Sicherheitsfirma Supratec.

Seine Zuhörer lauschen gebannt. Es sind gewiss nicht Computercracks, die Forster erreichen will. Es sind Nutzer wie du und ich, die den PC in der Freizeit oder bei der Arbeit verwenden. Vor allem aber ist es die Generation, die bei dem Begriff Trojaner noch zuerst an Homers Ilias denkt.

Auch an diesem Morgen sind vor allem ältere Teilnehmer zum kostenlosen Vortrag im Rahmen der Initiative „Deutschland sicher im Netz“ nach Gröbenzell bei München gekommen. Aber auch der Jungmeister eines Handwerkbetriebs will sich darüber informieren, wie sich sein Unternehmen absichern kann. Schließlich würden laut Forster rund 75 Prozent der kleinen und mittelständischen Unternehmen durch mangelhafte IT-Sicherheit Schaden erleiden.

Immer wieder updaten

Grimmig blicken die Gesellen von der Leinwand, vor denen sich jeder besonders in Acht nehmen sollte: der Hacker, der Schmutzfink, der Online-Betrüger und der Spammer. Letzterer nervt vor allem, der Schmutzfink nutzt das Netz als Halde für seinen geistigen Müll, meist gewaltverherrlichender oder rechtsradikaler Art.

Richtig bedrohlich für den PC können vor allem der Hacker, korrekt müsste er eigentlich Cracker heißen und der Online-Betrüger genannt werden.

„Es geht hier nicht um die Technik", sagt Forster weiter, "sondern darum zu erkennen, dass man etwas tun muss, um sich vor Angreifern zu schützen.“ Forsters goldene und wichtigste Regel: Updaten, updaten, updaten.

So lästig es auch sein mag, nichts schütze besser als immer wieder die neuesten Versionen von Virenscanner und Betriebssystem herunterzuladen. „Und selbst dann kann ich nur sagen: Sie sind *jetzt* sicher, was nachher ist, weiß ich nicht“, räumt Forster ein.

Misstrauen gegenüber Anhängen

Die häufigen Updates sind deshalb so wichtig, weil der Rechner nur so

gegen die neuesten Virenattacken geschützt ist. Auch Betriebssystem und Anwendungen müssen regelmäßig aktualisiert werden.

Entdecken die Hersteller nämlich eine Schwachstelle in ihrer Software, wird ein so genanntes „Patch“ veröffentlicht, damit Hacker jene Schwachstelle nicht ausnutzen können. Außerdem sollte der „digitale Türsteher“, unter Fachleuten Firewall genannt, nicht fehlen.

Ein weiterer Ratschlag: unbekannte Anhänge nicht öffnen. Gerade wenn die Freundin Helga eine blinkende E-Mail mit tanzendem Bärchen schickt und die Aufforderung, das Dokument zu öffnen, noch so lustig ist, sollte man widerstehen. Das heißt: Helgas Bekannte sollte die Datei sofort löschen. Andernfalls droht sich ein Trojaner einzuschleichen. Dieser hat es vor allem auf Passwörter, Pins und Tans abgesehen.

Sofort vernichten sollte der Internet-Anwender auch Anhänge mit der Endung .exe. Da diese sich auch hinter 25 Leerzeichen verstecken kann, ist immer Vorsicht geboten. Immerhin: Über den Acrobat Reader lesbare Anhänge mit der Endung .pdf sind meist sicher.

Misstrauen sollte sich hingegen bei den Microsoft-Produkten Word, Excel und Powerpoint regen. Jene Anhänge könne verseucht sein, etwa wenn Helga einen Virus auf dem PC hat. Öffnet sich ein Fenster, das abfragt, ob ein Makro geöffnet werden soll – löschen.

„Viele öffnen infizierte Dokumente, weil Sie denken: ‚Das hat ja die Helga geschickt, der kann ich vertrauen’. Dabei vergessen sie, dass Helga vielleicht ohne ihr Wissen einen Schädling auf ihrem PC eingefangen hat“, gibt Forster zu bedenken.

Einige Teilnehmer runzeln die Stirn, murmeln etwas von „Hätt’ ich das gewusst“ und wenden ihre Aufmerksamkeit wieder dem Vortragenden zu. „Und was ist mit eigenen .docs?“ will eine Zuhörerin wissen. „Wenn sich ein Virus erst mal eingenistet hat, befällt er alles“, so die ernüchternde Antwort.

Noch ein übler Geselle: der Hacker.
Foto: www.sicher-im-netz.de

Spyware untergräbt den PC wie ein Maulwurf

Der Vortrag dreht sich vor allem um Microsoft-Produkte. Das hat laut Forster aber weniger damit zu tun, dass hinter „Sicher im Netz“ vor allem Microsoft steckt, sondern liege vor allem daran, dass Microsoft-Anwendungen auf nahezu jedem PC zu finden seien. „Die MS-Produkte sind wie ein Weizenfeld“, erklärt Forster, „hat sich erst ein Pilz an einen Stängel geheftet, befällt er alle anderen.“

Ob es sich denn lohne, auf Linux umzusteigen, will ein Teilnehmer wissen. „Haben Sie MS-Programme, auf die Sie keinesfalls verzichten können oder wollen?“ lautet Forsters Gegenfrage. Manche hätten beispielsweise Lieblingsspiele, die nur unter MS liefen. Ansonsten sei Linux aber ein gleichwertiges Betriebssystem. „Noch vor fünf Jahren war Linux nur etwas für Experten – heute ist es ein System für alle“, sagt Forster.

Dem 78-jährigen Schwiegervater hat Forster nicht ohne Grund Linux auf seinem PC installiert: „Noch ist Linux nämlich für Hacker uninteressant, weil der Nutzerkreis beschränkt ist.“ Mac-PCs seien für Hacker noch uninteressanter: Nur fünf Prozent setzen bisher auf Apple.

Unabhängig vom Betriebssystem kann Spyware für jeden Internet-Nutzer zum Problem werden. Spyware ist der Sammelbegriff für unerwünschte Software, die unter Umständen auf dem PC bestimmte Aufgaben ausführt,

ohne dass der Anwender dies beabsichtigt hätte.

Dabei kann es sich um Werbung handeln oder auch um das Ausspionieren von Nutzungsgewohnheiten. Deshalb sollten Sicherheitswarnungen, Lizenzvereinbarungen und Datenschutzbestimmungen vor dem Download von Software immer genau gelesen werden. Sollte das Anti-Viren-Programm nicht vor Spyware und Dialern schützen, so empfiehlt sich die Installation von Anti-Spyware-Programmen.

2006 werden voraussichtlich 60 Milliarden E-Mails verschickt

„Und wenn nun doch der Computer von Viren befallen ist? Kann ich dann noch an meine wichtigen Dokumente?“ sorgt sich ein älterer Herr. „Da kann ich Ihnen wenig Hoffnung machen. Aber hier sind wir schon bei einem weiteren wesentlichen Punkt: der Datensicherung“, antwortet Forster.

Damit im Fall unbeabsichtigten Datenverlusts wichtige Dokumente nicht verloren gehen, sollten sie regelmäßig gesichert werden. Am einfachsten brennt man jene Kontoauszüge, Fotos oder Schriftstücke auf CD oder DVD. Auch ein Zip-Laufwerk, externe Festplatten oder Mini-USB-Flash-Laufwerke sind sinnvolle Archivierungsträger.

Noch einen Tipp gibt Forster mit auf den Weg: Internet-Nutzer sollten mit kostenlosen Programmen ihre E-Mails verschlüsseln. An chiffrierten elektronischen Briefen beiße sich sogar der Geheimdienst die Zähne aus. „Die EU will uns überwachen, nicht Terroristen“, interpretiert er den neuen EU-Vorstoß, künftig E-Mails „auf Vorrat“ ohne Verdachtsmoment zu speichern. Die Provider müssten dafür ungerechterweise zahlen.

„Im Jahr 2006 werden voraussichtlich 60 Milliarden E-Mails verschickt. Der Terror ist nur das Aushängeschild für die Speicherung, aber es betrifft den Bürger“, mutmaßt Forster.

Bequem waren seine Tipps sicher nicht. Aber für jeden nachvollziehbar und umsetzbar. Und während die Teilnehmer am Ende schon gedanklich ihren Computer einer Revision unterziehen, wird ihnen klar, dass Sicherheit am PC kein einmaliger Akt sein kann, sondern ein Prozess ist. Forster: „Man hat nie seine Ruhe! Höchstens einen Zeitvorsprung. Ungeschützte PCs gefährden alle!“

(sueddeutsche.de)

im Netz

Kostenloser Vortrag Terminübersicht
Initiative "Deutschland sicher im Netz"

drucken

Fenster schließen