COMPUTER

Verseuchter Seuchenschutz

Eine neue Bedrohung verbreitet sich im Internet: Nun sind es die Schutzprogramme selbst, die zum Einfallstor für Computerviren werden.

Seit „Witty“ unterwegs ist, steht die Welt Kopf: Wer Angst hat vor einem Einbruch und auf teure Überwachungstechnik setzt, macht sich gerade dadurch angreifbar.

Mit diesem Paradoxon schlägt sich die Software-Branche herum, seit der Computerwurm Witty sein Unwesen treibt. Das Dilemma begann damit, dass in der Computerschutz-Software „Black Ice“ der amerikanischen Firma ISS eine Sicherheitslücke gefunden wurde. Um die Lücke zu stopfen, bot die Firma ihren Kunden ein Reparaturprogramm an. Doch damit wurde die Lücke öffentlich bekannt, und noch bevor alle Kunden ihre digitale Rüstung flicken konnten, schlug der Feind erneut zu.

Mitten in der Nacht von Freitag auf Sonnabend, als die meisten Computernutzer in den USA schliefen, schlich sich Witty von Rechner zu Rechner und infizierte mehrere 10 000 Geräte durch die Schwachstelle in der löchrigen Schutzsoftware.

Nach wenigen Stunden flaute die Epidemie wieder ab. Zur Beruhigung der Lage kam es nicht etwa, weil die Lücke geschlossen worden wäre. Vielmehr agierte Witty zu aggressiv: Der Wurm brachte Tausende seiner Wirtsrechner zum Absturz, indem er Teile der Festplatte überschrieb.

Diese Episode ereignete sich bereits am 20. März 2004. Die Presse nahm davon kaum Notiz; verglichen mit Computerschädlingen wie „I Love You“, der im Jahr 2000 mehrere Millionen Rechner befallen hatte, schien Witty kaum der Erwähnung wert.

Es hätte schlimmer kommen können, dachten viele Experten. Und tatsächlich: Es kam schlimmer.

Denn Wittys Nachkommen könnten noch gefährlicher sein. Der Computerwurm war nur der Auftakt einer Flutwelle neuartiger Schadprogramme, die gezielt jene Programme missbrauchen, die doch eigentlich Schutz bieten sollen. Sogar Backup-Programme, die eigentlich dem Datenverlust vorbeugen sollen, sind ins Visier der Angreifer geraten.

Erst vorige Woche wurde bekannt, dass auch Software der Firma Panda offenbar eine Sicherheitslücke enthält – ein Eindringling könnte diese ausnutzen und fremde Rechner zum Absturz bringen. Das wäre noch vergleichsweise harmlos. Am gefährlichsten sind Schädlinge, die sich unbemerkt einnisten, um dann etwa unbemerkt jede Tastatureingabe mitzuprotokollieren und nach Passwörtern zu durchforsten.

Computer Associates, F-Secure, Kaspersky, Symantec – viele namhafte Hersteller von Sicherheitssoftware mussten inzwischen eingestehen, dass ihre Programme Schwachstellen enthalten. Unauffällig flickten die betroffenen Firmen jeweils ihre Löcher. Und wiegeln ab: „Die meisten dieser Bedrohungen sind doch rein hypothetisch“, sagt etwa Mikko Hyppönen, Virenspezialist der finnischen Sicherheitsfirma F-Secure. Doch in Insiderkreisen wird das Versagen der Branche kontrovers diskutiert.

Schutzprogramme üben einen besonderen Reiz auf zwielichtige Bastler aus: „Wer sich in der Szene einen Namen machen will, sucht nicht mehr nach der 1000. Lücke in Windows“, sagt Andrew Jaquith, Analyst bei der Bostoner Beratungsfirma Yankee Group. „Es gilt als viel cooler, einen Virenscanner direkt zu attackieren.“

Indirekt ist Witty auch der erhöhten Sicherheit von Microsoft-Produkten zu verdanken. „Windows-Produkte führen zwar immer noch die Risikostatistiken an“, so der Analyst, „aber der Missbrauch ist doch etwas schwieriger geworden.“

Neuerdings besteht die Gefahr, dass sich die Witty-Welle verselbständigt, warnt Rohit Dhamankar von der Sicherheitsfirma Tipping Point: „Jeder Anfänger kann mit frei erhältlichen Bausätzen einen neuen Eindringling zusammenklicken.“ Der Programmcode des Witty-Wurms dient sich geradezu für die Weiterverwendung an. Der Name Witty bezieht sich auf eine Botschaft, die im Programmcode versteckt ist: „insert witty message here“ – eine Aufforderung an Trittbrettfahrer, einfach den Code weiterzuverwenden und an diese Stelle eine „geistreiche Botschaft“ einzubetten, als wäre der Killerwurm nur eine Art elektronische Postkarte.

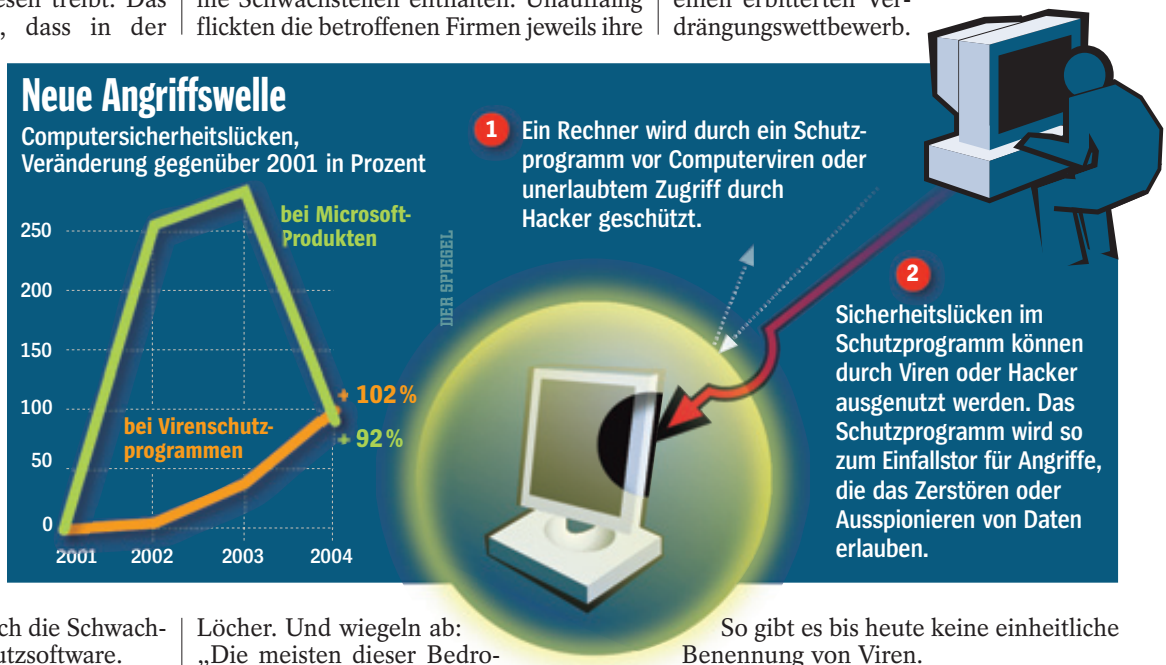
Doch die wichtigsten Gründe für die neue Verletzlichkeit liegen nicht bei den oft minderjährigen Angreifern, sondern bei einer Branche, die sich beharrlich weigert, erwachsen zu werden. Seit Jahren schon liefern sich über ein Dutzend Hersteller einen erbitterten Verdrängungswettbewerb. So gibt es bis heute keine einheitliche Benennung von Viren.

„Der Zeitdruck ist enorm gestiegen, fast alle Anbieter bringen fast jeden Tag ein neues Update, und oft bleibt kaum Zeit, die Software zu testen“, sagt Andreas Marx, Sicherheitsberater aus Magdeburg. Außerdem werden die Sicherheitspakete ständig um neue Funktionen erweitert, bisweilen mit mangelhaften Komponenten von Drittanbietern. Die vermeintlichen Flicken sind daher manchmal selbst löchrig.

Die meisten Computernutzer sind noch ahnungslos. Brav zahlen sie oft über 40 Euro für ihre Computerschutz-Programme – ohne zu ahnen, dass ihr Seuchenschutz selbst blitzartig hochinfektiös werden könnte.

Wie aber sollen sich die Kunden verhalten? „Das Allerdümmste wäre es, in Panik zu verfallen und auf den Virenschutz zu verzichten“, rät Andreas Marx, „Wo im Leben gibt es schon absolute Sicherheit?“

HILMAR SCHMUNDT



Virenforscher Marx
Risiko Zeitdruck