

COMPUTERKRIMINALITÄT

Ihr Rechner ist besetzt!

Cyberkriminelle kapern fremde Computer und schließen sie zusammen. Über diese Schattennetze versenden sie Spam-Mails, manipulieren Internetseiten und plündern Bankkonten

VON LARS REPPESGAARD

Das Wochenende im Januar, an dem der Computerwurm zuschlug, war für Rainer Harpf, den Chief Information Officer der **Kärntner Landeskrankenanstalten** (Kabeg), ein Albtraum. Blitzschnell hatte der Schädling, den Sicherheitsfachleute Conficker getauft haben, am Samstagmorgen seine Arbeit aufgenommen, nachdem er irgendwo auf einen Rechner des Klinikverbunds geschlüpft war. Das Hackerprogramm sammelte die Passwörter, die auf dem Rechner zu finden waren, es kopierte Daten und versuchte, all diese Informationen an eine Adresse im Internet zu schicken. Conficker infizierte alle Computer, die er über das Netzwerk des Krankenhauses erreichen konnte. »In unsere medizinischen Systeme, in denen die Patienteninformationen und Röntgenbilder abgelegt sind, konnte der Wurm nicht eindringen«, sagt Harpf. »Aber er hat all unsere Computerarbeitsplätze lahmgelegt.«

Am Ende fand sich der Schädlingscode auf 3000 Computern wieder. E-Mails zu verschicken, im Internet zu surfen, ja sich überhaupt nur an ihrem Rechner anzumelden war für die Kabeg-Mitarbeiter unmöglich. Conficker versuchte, ihre Benutzerkonten aufzubrechen, indem er wahllos Millionen von Passwörtern ausprobierte. Bis zu 200 Mal pro Sekunde setzte er dazu an, über das Internet Computer irgendwo auf der Welt anzugreifen. Um den Schädling aufzuhalten, kappte Harpf die Netzwerkverbindungen aller Arbeitsplatzrechner. Dann begann das Aufräumen: Von Samstagmorgen um sieben Uhr bis Sonntagabend um elf neutralisierten er und seine Mitarbeiter den Hackercode auf jedem einzelnen Computer. Das Wochenende über arbeiteten die Ärzte notgedrungen wieder wie in der Vergangenheit: mit Fieberkurven und Krankenberichten auf Papier.

Nicht nur in Kärnten machten Computerfachleute in den vergangenen Wochen unliebsame Bekanntschaft mit dem verheerendsten Internetwurm seit Jahren. In Hamburg schlug er im **Albertinen-Krankenhaus** und im dazugehörigen Schulungszentrum für Pflegekräfte zu. In mehr als 4300 Unternehmen und Organisationen in Deutschland und weltweit auf mehr als sieben Millionen Rechner ist der Wurm nach Schätzungen des finnischen Antivirensoftware-Herstellers F-Secure eingedrungen. Bei der **Bundeswehr** hat der Computerschädling mehrere Hundert Rechner lahmgelegt. Die **französische Marine** musste Teile ihres Netzwerks abschalten; die Kampffjets der Luftstreitkräfte blieben zwei Tage auf dem Boden. Auch Computer des **bulgarischen Innenministeriums** und der **finnischen Regierung** sind von dem Superwurmgangriff betroffen. »Was genau hinter der Attacke steckt und wo der Wurm herkommt, ist unbekannt«, sagt

Thomas Hungenberg, Computersicherheitsexperte beim Bundesamt für Sicherheit in der Informationstechnik (BSI). »Aber er hat sich massiv ausgebreitet. Auch wir gehen davon aus, dass es weltweit mehrere Millionen betroffene Computer gibt.«

Die Conficker-Welle ruft in Erinnerung, dass ein Wirtschaftszweig trotz der weltweiten Krise weiter blüht: die Cyberkriminalität. Viele Jahre lang trieben vor allem Neugier und Nervenkitzel die Programmierer von Viren und Netzwerkwürmern an. Doch seit der Jahrtausendwende werden die Hobbyhacker von einer neuen Generation von Virenautoren abgelöst: professionellen Programmierern, die ihre Kenntnisse an den Meistbietenden verkaufen. Das Schreiben von Programmen, die sich auf fremde Rechner schleichen und dort die Kontrolle übernehmen, ist zu einem einträglichen Geschäft geworden. Denn insgeheim gekaperte Computer lassen sich hervorragend zu riesigen Netzen zusammenschließen. Diese sogenannten Botnetze, die oft eine Million und mehr Computer umfassen, sind die Infrastruktur der Cyberkriminellen. Sie werden vermietet, um zum Beispiel Spammails zu verschicken. Oder sie legen als Rechnerverbund mit pausenlosen Anfragen Internetseiten lahm.

Doch die Schattenwirtschaft im Cyberuntergrund handelt in ihren anonymen Kommunikationsforen nicht nur mit Botnetz-Kapazitäten. Verkauft werden Kreditkartendaten, Informationen über Bankkunden, Zugangsdaten für E-Mail- oder eBay-Konten. »In der Untergrundwirtschaft lässt sich viel Geld verdienen«, sagt BSI-Experte Hungenberg. Mitarbeiter des Sicherheitssoftwareunternehmens Symantec beobachteten im vergangenen Jahr, wie binnen zwölf Monaten über geheime Internetforen Waren wie Botnetz-Kapazitäten, Hackersoftware oder Kontoinformationen für insgesamt 276 Millionen Dollar verkauft wurden. Allein mit den dort gehandelten Kreditkarteninformationen könnten bis zu 1,7 Milliarden Dollar unrechtmäßig abgehoben werden.

Auch das Geschäft mit den Spammails ist nach wie vor lukrativ, obwohl nicht einmal ein Promille der Empfänger dieser unerwünschten Werbemails die dort offerierten Produkte kauft. Seriöse Onlineunternehmen bieten den milliardenfachen Versand des E-Mail-Mülls gar nicht erst an – wohl aber die Betreiber von Botnetzen. Neun von zehn Spamnachrichten werden mit deren Hilfe verschickt. Die beiden größten dieser Verbände haben Sicherheitsexperten Storm-Netz und Srizbi getauft.

Die Botnetz-Betreiber mussten aber 2008 zwei Rückschläge verdauen. Die Zentralrechner, mit denen sie ihre Netze verwalten, stehen oft zur Miete in Rechenzentren von Providern, die nicht genau wissen wollen, was ihre Kunden so treiben. Im August kappten die übrigen Internetprovider alle Leitungen zu einem schwarzen Schaf der Zunft, dem kalifornischen Unternehmen Atrivo. Schon das führte dazu, dass im Oktober weniger Spam als in den Vormonaten verschickt wurde. Im November schaltete die Zunft alle Leitungen zu den Rechnern von McColo ab, einer Einmannfirma in San Jose am südlichen Ende des Silicon Valley, nachdem bekannt geworden war, dass das Unternehmen Botnetz-Betreibern,

Anbietern von Kinderpornografie und Profihackern auf seinen Festplatten Unterschlupf gewährt hatte.

Nach dem Abschalten von McColo beobachteten die Internetprovider Ende 2008 einen starken Rückgang der Spamflut. Alte Botnetze wie Srizbi funktionierten kaum noch, weil die Befehlszentrale fehlte. Doch die Spammerszene organisiert sich stets neu. Schon wenige Tage nach dem Ende von McColo beobachteten Sicherheitsfachleute, wie der Hydra neue Köpfe wuchsen: Sie bemerkten, dass so viele Computerviren wie schon lange nicht mehr in Umlauf gebracht wurden, um neue Rechner mit Hackersoftware zu infizieren. Derzeit entstehen neue Botnetze, die die Rolle der alten Netzwerke einnehmen. Eines, das Softwareexperten Cutwail nennen, umfasst bereits wieder eine Million einzelner automatischer Programme (Bots). Das neue Netz Donbot ist beinahe genauso groß. Heute hat sich die Menge der Spammails wieder auf dem Niveau vom Sommer 2008 eingependelt. Der Trend, dass Kriminelle mithilfe fremder Computer Geld verdienen, dürfte sich 2009 noch verstärken. Denn die Wirtschaftskrise heizt viele Formen der Kriminalität an, auch die Cyberkriminalität. Rik Ferguson, Sicherheitsberater beim Softwareunternehmen Trend Micro, hält jeden arbeitslosen Computerfachmann für einen potenziellen Kandidaten, um von Gangstern rekrutiert zu werden.

Und der Conficker-Wurm? Ist auch er das Werk von Profis, die in der Cybercrime-Branche ihr Geld verdienen? Hat auch er die Aufgabe, neue Rechner für die Schattenwirtschaft zu kapern? Einiges deutet darauf hin – etwa die Art und Weise, wie er programmiert wurde. »Wir beobachten, was der Wurm tut, wenn er erfolgreich in ein System eingedrungen ist«, sagt Kevin Hogan, Leiter der Antivirenabteilung bei Symantec in Dublin. »Er sucht dann über das Internet den Kontakt zu anderen Rechnern, um weitere Software herunterzuladen.« Auf ihnen liegt oft eine Ladung Codes, die auf die befallenen Computer gesaugt wird. Danach sind auch sie Zombierechner, die von den heimlichen Herren der Botnetze unbeobachtet aus der Ferne gesteuert werden können.

Rätsel gibt den Sicherheitsfachleuten auf, dass die Conficker-Programmierer den zweiten Schritt – ihren Wurm mit neuer Software zu versorgen – noch nicht getan haben. Eine Panne ist kaum daran schuld. »Conficker ist ein technisches Meisterstück«, sagt Hogan. Möglich ist, dass der Erfolg von Conficker den Autoren über den Kopf gewachsen ist. »Ich denke, hier hat jemand ausprobiert, was technisch möglich ist. Erschreckend, sich vorzustellen, wie viele Rechner ein Hacker nun kontrollieren kann«, sagt Sean Sullivan, Antivirenexperte bei F-Secure. »Wir hoffen, dass der Erfolg des Wurms seine Absender so erschreckt hat, dass sie nicht wagen, aktiv zu werden.« Tatsächlich haben professionelle Computerkaperer bei ihren Attacken stets darauf geachtet, nicht zu viele Geräte zu infizieren. »Sie operieren unterhalb der Radarschirme; zu viel öffentliche Aufmerksamkeit kann für sie gefährlich werden«, sagt Sullivan.

Wenn ein Wurm wie Conficker auf spektakuläre Weise Millionen Systeme niederwalzt, fällt das nicht nur den Ermittlungsbehörden auf. Es wird auch deutlich, auf welch tönernem Fundament die Informationsgesellschaft steht.

Dass Computersysteme schlampig aufgestellt und betreut werden, sei nicht die Ausnahme, sondern die Regel, sagt der Sicherheitsexperte Hartmut Pohl von der Hochschule Bonn-Rhein-Sieg. »Mindestens 50, vielleicht aber sogar 95 Prozent aller Server sind nach unserer Erfahrung nicht ausreichend abgesichert.« Einen Softwareflicken gegen die Schwachstelle im Betriebssystem Windows, die Conficker ausnutzte, hatte Hersteller Microsoft schon im Oktober veröffentlicht – einen Monat bevor die erste Version des Superwurms durch das Netz geisterte. Viele Systemadministratoren haben diese Warnung nicht ernst genommen.

Bei Kabeg liegt der Fall anders. Harpf und seine Kollegen haben alle Systeme auf dem neusten Stand gehalten. Doch Conficker wurde von seinen Erschaffern permanent weiterentwickelt. Nur die erste Version des Wurms nutzte allein die alte Windows-Lücke aus. Die Variante B, die sich jetzt weltweit auf die Rechner schleicht, ist trickreicher: Sie verbreitet sich auch über USB-Sticks, die Mitarbeiter in die Firma mitbringen, um die Kollegen mit Weihnachtsfotos zu erfreuen. Oder die Patienten in die Praxis tragen, um dem Arzt die digitalen Röntgenbilder zu zeigen.

ZEIT ONLINE 2009