Scharfe Wächter

Die Internet-Würmer Blaster und Sobig.F zwingen Microsoft zum Umdenken. Auch Private brauchen zuverlässige Netz-Wächter.

von Bruno Habegger

Die Jura-Studentin Andrea F. weiss nicht weiter: «Muss ich auf Linux umsteigen?» Sie sichere zwar regelmässig ihre Daten, fürchte sich aber dennoch vor einer neuen Attacke, die ihre wertvolle, mehrere hundert Seiten starke Abschlussarbeit vernichten könnte. Obwohl Sie sich mit einem Virenscanner und der Personal Firewall ZoneAlarm (www.zonelabs.com) schütze, habe sie seit dem Virenmonat August, in dem W32/Blaster (MS Blaster, Lovsan) und Sobig.F für Aufsehen sorgten, ein mulmiges Gefühl in der Magengrube.

Ihre Angst scheint berechtigt. Der Blaster-Wurm, der mittlerweile in verschiedenen Varianten auftritt, ist besonders heimtückisch, weil er sich nicht via E-Mail verbreitet, sondern gnadenlos eine Sicherheitslücke in Windows ausnutzt, gegen die Microsoft seit längerem ein Korrekturprogramm anbietet. Er trifft vor allem Heimanwender, weil Firmen ihre Systeme meist sofort abdichten. Warum die wenigsten den Patch bemerkt haben, zeigt ein Blick in die Dateiliste von www.windowsupdate.com: Zwar wird auf der ersten Seite ausführlich über Blaster informiert, doch der direkte Link auf das Korrekturprogramm fehlt. Wer nur selten Updates installiert, findet das Programm nur mit Mühe in der langen Liste der zu installierenden Patches. Ohne den Patch gestaltet sich aber das Entfernen von Blaster gemäss PCtipp-Anleitung in WEBCODE **24884** als schwierig. Kaum entfernt, sitzt der Wurm im schlimmsten Fall nach wenigen Minuten wieder drin, begünstigt durch den Umstand, dass die in Windows XP integrierte Firewall standardmässig ausgeschaltet ist. Erst die Firewall rein, dann den Wurm entfernen und zum Schluss den Patch installieren – so lautet die Reihenfolge.

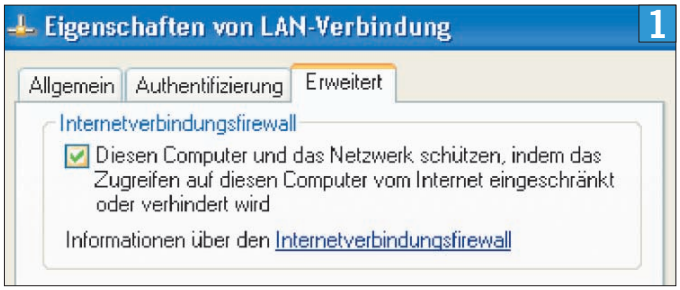
Die XP-Firewall finden Sie unter START/SYSTEMSTEUERUNG/NETZWERKVERBINDUNGEN. Klicken Sie die Netzwerkverbindung mit der rechten Maustaste an und wählen Sie EIGENSCHAFTEN. Die Firewall finden Sie im Reiter ERWEITERT ganz oben – setzen Sie ein Häkchen, und schon belästigt Sie Blaster nicht länger, **Screen 1**.

Die Vorfälle des Augusts haben Microsoft zu denken gegeben. Künftige Versionen von Windows XP sollen mit der bereits eingeschalteten Firewall ausgeliefert werden. Zudem plant Microsoft, die oft abgeschaltete Auto-Update-Funktion von Windows XP auszubauen und wichtige Updates ohne Zustimmung der Anwender automatisch zu installieren (siehe «Zwang zur Sicherheit?», S. 17).

Die Sicherheit, kein einziges Update zu verpassen, können Sie schon heute haben. Sie finden die Funktion in START/SYSTEMSTEUERUNG/SYSTEM. Klicken Sie hier auf den Reiter AUTOMATISCHE UPDATES. Wenn Sie vor dem Download informiert werden wollen, klicken Sie die mittlere Option an. Andernfalls lädt Windows die Updates ganz herunter, bevor Sie etwas davon mitbekommen. Das wiederum ist nur sinnvoll, wenn Sie an einem Breitbandanschluss hängen. Mit ISDN oder einem analogen 56K-Modem blockieren die oft mehrere MB umfassenden Updates Ihre Telefonleitung. Anwender älterer Windows-Versionen müssen sich gegenwärtig noch manuell auf www.windowsupdate.com bedienen.

Für Mikko H. Hyppönen, Direktor der Antiviren-Forschung der finnischen F-Secure (www.f-secure.com), sind automatische Updates der einzig sinnvolle Weg, Würmern wie Blaster Einhalt zu gebieten. Und Microsoft muss weiter ernsthaft an der Sicherheit seiner Produkte arbeiten. Für Hyppönen liegt Microsofts Hauptproblem aber nicht in erster Linie in den vielen Fehlern im Betriebssystem, sondern in dessen Marktmacht. Microsoft ist deswegen unter den Virenautoren verhasst und das Hauptziel ihrer Angriffe. Auch Linux und andere Betriebssysteme enthalten Lücken, die aber viel weniger oft ausgenutzt werden.

ILLUSTRATION TAVIS COBURN



Sinnvoll: Aktivieren Sie in Windows XP die Firewall

Mit Slammer zu Jahresbeginn sowie Blaster und Sobig wurden Microsoft-Produkte dieses Jahr gleich von drei schweren Virenvorfällen getroffen. Jeder dieser Schädlinge war gefährlicher, als es Viren bisher für gewöhnlich waren. Slammer betraf Anwender der Profidatenbank Microsoft SQL und verbreitete sich wie Blaster ohne Zutun der Anwender. Er sorgte für zahlreiche Server-Zusammenbrüche.

Die von Blaster befallenen Rechner wiederum starteten einen kombinierten Angriff auf die Update-Seite von Microsoft. Sobig schliesslich war der schlimmste von allen: Er verbreitete sich rasant im Internet und in lokalen Netzwerken. Zudem taucht er in immer neuen Varianten auf, indem er sich neue Bestandteile von Internet-Servern nachlädt.

So kann er theoretisch sogar zu einem Superwurm mit beliebigen Schadensfunktionen mutieren und die ganze Internetkommunikation auf den Kopf stellen. «Sobig.F stellt E-Mail in seiner jetzigen Form in Frage», befürchtet Experte Mikko H. Hyppönen. «Microsoft muss jetzt unbedingt seine Mailtechnologie auf eine sicherere Grundlage stellen.»

Wie schnell sich der Koloss von Redmond bewegt, ist ungewiss. Trotzdem müssen Heimanwender nicht sofort auf ein anderes Betriebssystem umstellen, um sich sicherer zu fühlen. Schon mit etwas mehr Verantwortungsbewusstsein für die Sicherheit des eigenen PCs machen es Anwender Virenprogrammierern sehr schwer. Lesen Sie dazu den Kommentar von PCtipp-Redaktor Beat Rüdt, unten.

Der Virenmonat August führt zu drei wichtigen Einsichten: Erstens steigt das Risiko auch für Virenprogrammierer. Bereits sind zwei Programmierer von Blaster-Varianten verhaftet worden. Zweitens genügt es nicht mehr, bloss beim Öffnen von E-Mail-Anhängen Vorsicht walten zu lassen. Eine Firewall ist nach Blaster zum Muss geworden, ebenso eine ständig aktualisierte Antiviren-Software. Der PCtipp testete die gängigsten Sicherheitspakete in Ausgabe 9/2003 im Artikel «Doppelt schützt besser», S. 66.

Und drittens kann es noch viel schlimmer kommen. Gefährliche Wurm-Klone, die Elemente anderer Schädlinge integrieren, treten immer häufiger auf. Der Superwurm wäre eine Kombination aus dem sich schnell verbreitenden Slammer und einem Angriff à la Blaster auf die wichtigsten Router, Switches und Nameservers des Internets, also auf die Netz-Infrastruktur. Er könnte so unter Umständen das Internet für Stunden oder Tage lahm legen. ■

BLASTER

Optimierter Patch

Microsoft hat im Windows-Dienst (RPC/DCOM), der auch von Blaster ausgenutzt wird, drei weitere gefährliche Schwachstellen entdeckt. Zwei davon ermöglichen es einem Angreifer, beliebigen Code auf einem fremden System auszuführen. Microsoft empfiehlt, den unter http://windowsupdate.microsoft.com bereitgestellten Patch umgehend zu installieren. Er schliesst gleichzeitig die Lücke, die vom Blaster-Wurm ausgenutzt wird, und sollte deswegen an Stelle des bisherigen Blaster-Patches aufgespielt werden.

MEINUNG

Schuld ist immer Microsoft! Ach ja?

Jeder Wurm und jeder Virus hat einen Urheber, der belangt werden könnte. Viel einfacher ist es, die Schuld Microsoft zu geben.

Beat Rüdt, Redaktor

Autos weisen gravierende Sicherheitslücken auf: Ein Stich mit dem Messer in den Pneu genügt, um das Vehikel fahruntüchtig zu machen. Und obwohl diese Lücke bekannt ist, seit es Autos gibt, unternehmen die Hersteller nichts, um sie zu beheben. **Bei Betriebssystemen ist das anders.** Mit dem Auftreten der Würmer Blaster und Sobig.F hat Microsoft die Anwendergemeinschaft erzürnt. Von der linken WOZ («Nun ist hinlänglich bekannt, dass dessen [Microsofts] Produkte Lücken und Mängel aufweisen, die den Schädlingen als willkommene Einfallstore dienen») bis zur bürgerlichen NZZ («Es wäre schon viel gewonnen, wenn in der heutigen Generation Rechner so ausgeliefert würden, dass alle Schotten dicht sind») weisen alle Medien die Schuld dem Software-Riesen zu. **Diese populäre Polemik nutzt auch die Stiftung für Konsumentenschutz** («Microsoft lanciert immer wieder fehlerhafte Produkte, vor deren Sicherheitslücken der Konzern dann später oft selber warnt») und hat von der Wettbewerbskommission eine Untersuchung über die Marktmacht Microsofts verlangt. **Kaum jemand aber weist auf das tatsächliche Problem hin:** Tausende, meist jugendliche Cracker suchen gezielt nach Funktionen im Betriebssystem, die sich ausnutzen lassen. Microsoft reagiert auf die Angriffe: Automatische Updates wehren böse Programme (wie Blaster) ab. Bei Sobig.F sind es aber ausschliesslich leichtsinnige Anwender, die mit einem gezielten Mausklick den Virus aktivieren. **Warum man bei so viel krimineller Energie der Cracker und Fehlverhalten der Anwender von Sicherheitslücke spricht, ist mir schleierhaft.** Es sind mutwillig geschlagene Breschen. Und der Irrglaube, dass ein komplexes System wie ein Computer einfach funktioniert – ohne Wartung, wie sie beim Auto selbstverständlich ist.

KURZINFOS

GRATISEINTRITT

Vom 24. bis zum 27. September findet die diesjährige Orbit statt. Möchten Sie gerne an die Messe, haben aber noch kein Ticket? Kein Problem, der PCtipp offeriert Ihnen einen Gratiseintritt. Besuchen Sie die Website www.orbitcomdex.com/online-ticket und lösen Sie dort den Priority Code «257-DR99Y52T» ein.

USB-UPDATE

Unter www.microsoft.com/downloads findet sich ein neues Upgrade für die USB-Treiber von Windows XP. Es behebt verschiedene Probleme mit Peripheriegeräten. Um das Update herunterzuladen, geben Sie unter «Einen Download suchen» die Nummer «822603» ein.

SWISSCOM-SHOPS

Das grosse Echo über die Einführung von Beratungsgebühren in den Swisscom-Shops sorgte für einen Gesinnungswandel. Beratung und individuelles Einrichten von Diensten sind ab sofort gratis. Die Unterscheidung zwischen kostenlosen und kostenpflichtigen Diensten habe die Kunden verunsichert, so die Begründung der Swisscom.

ALLES LEGAL

Citydisc hat die erste legale Musikdownload-Plattform der Schweiz aufgeschaltet (www.directmedia.ch). Angeboten werden über 210 000 Songs von mehr als 8500 Interpreten. Grosses Gewicht wird auf Schweizer Künstler gelegt. Die Songs sind ab 99 Rappen zu haben.

MEHR OFFICE

Auf der Seite http://office.microsoft.com bietet Microsoft zahlreiche Vorlagen, Cliparts und Trainingskurse für Office-Programme wie Word oder Excel an. Die Homepage wird von über hundert Mitarbeitern betreut und täglich aktualisiert.

Office-Clipart