SZ 10.7.2004 Seite 18

Operation am digitalen Herzen

Computerexperten haben ein massives Sicherheitsleck im Internet gestopft

Computerexperten haben in einer konzertierten Aktion eine gewaltige Sicherheitslücke im Internet gesschlossen. Monatelang bestand für Hacker offenbar die Möglichkeit, das so genannte Domain Name System (DNS) zu manipulieren, eine Art Zentralnervensystem des Internets. Kenner hatten diese Stelle schon vor Jahren als einen Schwachpunkt des ansonsten robusten Netzes identifiziert. Jetzt haben 68 üblicherweise in Konkurrenz stehende Firmen sich unter der Leitung von Microsoft zusammengetan, um gemeinsam eine Lösung des Problems zu erarbeiten. Um es vollständig zu beseitigen, seien nach Ansicht von Experten aber weitergehende Maßnahmen nötig.

„Die Bedrohung ist real", sagt Jürgen Schmidt, Sicherheitsexperte beim Computermagazin *c't*. Es seien bereits mehrere Fälle bekannt geworden, in denen Kriminelle versucht haben, das DNS für ihre Machenschaften auszunutzen.

Getarnte Umleitung

Aber wie kommen Kriminelle überhaupt an dieses Herzstück des Internets heran? Das DNS muss man sich vorstellen wie ein digitales Telefonbuch. Computer kommunizieren untereinander über ein System von Ziffernkombinationen, die sich Menschen nur schwer merken können. Die Hauptfunktion des DNS ist es daher, Namen wie www.sueddeutsche.de in Zahlen zu übersetzen, in diesem Fall 213.221.91.5. In den Anfangszeiten des Internets mussten entsprechende Tabellen mit Namen und zugehörigen Ziffernfolgen noch auf jedem einzelnen Rechner gespeichert werden. Heute ist daraus ein hierarchisch gegliedertes System aus Tausenden von Computern geworden. Wer auf seinem PC eine WWW-Adresse, beispielsweise www.bundestag.de eingibt, erzeugt damit automatisch eine Anfrage an diese DNS-Rechner. Damit diese Computer die vielen an sie gerichteten Anfragen schnell beantworten können, legen sie ihre Daten im Arbeitsspeicher ab – und genau an dieser Stelle lauert die Gefahr.

Am späten Abend des 3. März 2005 war es soweit. Die technisch Veranwortlichen mehrerer Internetangebote berichteten beim SANS Internet Storm Center, einer nichtkommerziellen Genossenschaft mit dem Schwerpunkt Internetsicherheit, von seltsamen Attacken. Anwender, hieß es dabei, seien beim Versuch, auf eine Seite zu kommen, umgeleitet worden auf andere Seiten, die Schadsoftware enthielt. Doch das war erst der Anfang. Während die Experten noch dabei waren, den ersten Angriff zu ergründen, wurden schon neue gemeldet, und stets erprobten die Angreifer dabei neue Methoden. Erfolgreich attackieren konnten die Hacker damals aber nur fehlerhaft eingerichtete DNS-Rechner.

Doch im Frühjahr dieses Jahres entdeckte dann der in der Computerszene angesehene Sicherheitsexperte Dan Kaminsky nach eigener Darstellung eine Möglichkeit, wie man Speicher (Cache) mit den Nummern und den Namen auf einfache Weise manipulieren kann. Er setzte sich daraufhin mit betroffenen Herstellern in Verbindung, die – ein ziemlich ungewöhnlicher Vorgang – plötzlich zusammenarbeiteten, um das Problem wenn auch nicht vollständig zu lösen, so doch die Schwelle für potentielle Angreifer wieder zu erhöhen. An diesem Dienstagabend wurde dann weltweit eine Reparatursoftware verteilt, die beispielsweise die im Betriebssystem Windows betroffene Stelle absichert. Wie genau er das DNS austrickst, dazu will Kaminsky erst bei einer Konferenz zur Internetsicherheit im August mehr sagen. Einige Aufmerksamkeit dürfte dem eloquenten Ex-Hacker jedoch sicher sein.

Das Domain Name System ist deshalb so angreifbar, weil es schon Anfang der 1980er Jahre entwickelt wurde, zu einer Zeit also, in der niemand daran dachte, dass es einmal Gauner geben würde, die das Internet als Infrastruktur nutzen. „Dass das Internet überhaupt funktioniert, obwohl es so riesig geworden ist, ist an sich schon faszinierend", sagt Marc-Oliver Pahl vom Lehrstuhl für Netzarchitektur und Netzdienste der TU München. Das DNS sei dabei einer der Bereiche, von denen Experten schon seit langem wüssten, dass nicht alles zum besten stehe. Um gänzlich zu verhindern, dass Gauner arglose Internet-Nutzer auf gefälschte Web-Seiten umlenken, beispielsweise auf die vermeintliche Seite einer Bank, müsste „eigentlich das gesamte System verändert werden", sagt Pahl.

Ein enstprechendes Verfahren gibt es auch schon, doch ist es dabei wie mit dem Internetprotokoll, der Universalsprache des Internets: Alle Experten wissen, dass ein seit kurzem angebotenes, neues Protokoll erhebliche Vorteile bietet, unter anderem nahezu beliebig viele neue Adressen. Solange das alte aber noch so gut läuft, wollen sich nur wenige die Kosten aufbürden, es einzuführen.

„Noch funktioniert's ja"

„Es ist seit Jahren absehbar, dass das DNS die Achillesferse des Internets ist", sagt auch der *c't*-Sicherheitsexperte Schmidt, „aber seit vielen Jahren wird da nur Flickschusterei betrieben, nach dem Motto: noch funktioniert's ja." DNSSEC, so heißt das neue, bessere Verfahren, ist bei den Verwaltern von DNS-Computern deshalb unbeliebt, weil es mehr Arbeit macht. Um zu gewährleisten, dass die Übersetzung von Web-Adresse in die zugehörige Ziffernfolge stimmt, bietet es ein erheblich sichereres Verfahren, das aber mehr Pflege erfordert.

Auch wenn das neue, besser gesicherte DNS noch nicht so bald kommt, müssten sich normale Nutzer im Internet dennoch nicht mehr als bisher sorgen, so der Experte für Internetsicherheit von der Universität Passau, Joachim Posegga. Das grundsätzliche Problem sei ja schon lange bekannt. „Das DNS wurde halt nicht gemacht, um sicher zu sein", sagt der Informatiker. Nutzer sollten darauf achten, alle Sicherheitserweiterungen einzuspielen, die Hersteller zur Verfügung stellten und sich, wenn ihnen etwas sonderbar vorkomme, „wundern und mal nachfragen". HELMUT MARTIN-JUNG