

# Nur von Hackern empfohlen

Fast jeder zweite Internetsurfer benutzt eine veraltete Browser-Version. Das macht anfällig für Angriffe aus dem Umfeld der organisierten Kriminalität. *Von Andreas Hirstein*

Über 600 Millionen Internetnutzer verwenden eine veraltete Programmversion ihres Browsers – ein Anteil von über 45 Prozent aller Surfer. Das geht aus einer Studie hervor, die Forscher der ETH Zürich, von Google und IBM in der letzten Woche publiziert haben (techzoom.net/insecurityiceberg). Damit verzichten viele Internetnutzer nicht nur auf nützliche Funktionen und die grössere Geschwindigkeit der neuen Browser-Generation. Sie riskieren auch, zu Opfern einer neuen Form von Hackerangriffen zu werden, gegen die nur die neuesten Programmversionen zuverlässig schützen.

Schon der Besuch einer manipulierten Website kann genügen, um Hackern ein Einfallstor zu öffnen. Sie installieren Computerschädlinge (Trojaner) auf dem PC, die eine fast vollständige Kontrolle des Computers ermöglichen. So werden laut Schätzungen jedes Jahr Millionen von gekaperten PC zu virtuellen Netzen verbunden. Diese Botnets nutzen die Hacker, um Spam- und Phishing-Mails oder um Schutzgeld von grossen Websites zu erpressen. Wer nicht zahlt, erlebt den Blackout seiner Webserver, die unter der Last einer vom Botnet lancierten Anfragen-Lawine in die Knie gehen (Denial-of-Service-Angriffe). Im Mai 2007 zum Beispiel wurden Server von estnischen Regierungsstellen und Banken von einem russischen Botnet angegriffen. Damit sollte die Verlegung eines russischen Soldatendenkmals aus dem Zentrum an den Rand der Hauptstadt Tallinn verhindert werden.

## Das grosse Geld

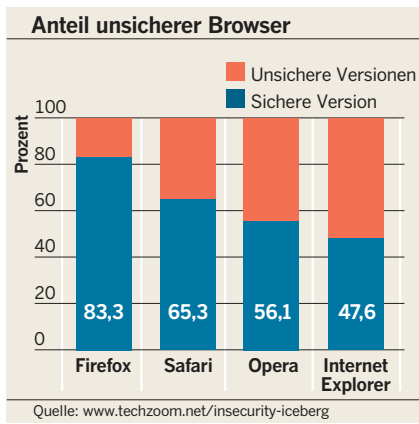
«Hinter solchen Angriffen verbirgt sich die organisierte Kriminalität», sagt Stefan Frei von der ETH Zürich, der Hauptautor der neuen Studie. Den Hackern geht es dabei zumeist nicht um politischen Druck, sondern um «das grosse Geld», sagt Frei.

Einer der Gründe für diese Masche sind veraltete Browser. Unter den Nutzern von Microsofts Internet Explorer (IE) zum Beispiel verwendet heute noch fast jeder zweite die Version 6, obwohl die Version 7 schon seit Oktober 2006 erhältlich ist. Dabei rät Microsoft schon längst zum Umstieg, weil im Internet heute Gefahren lauern, die bei der Lancierung des IE 6 noch gar nicht existierten.

Angriffsflächen bieten dabei nicht nur alte Programmversionen, sondern auch neue, deren Sicherheits-Updates



Vier aktuelle Browser. Unter dem Menü «Hilfe» erhält man – wie hier gezeigt – Auskunft über die verwendete Programmversion.



nicht auf dem letzten Stand sind. Um solche PC anzugreifen, manipulieren die Hacker im ersten Schritt populäre und daher unverdächtig erscheinende Internetseiten. Eine Angriffstechnik richtet sich gezielt gegen Seiten mit Eingabefeldern, zum Beispiel zum Durchsuchen einer Datenbank.

Die Angriffe erfolgen vollautomatisch von entsprechend programmierten Computern. Statt eines gewöhnlichen Suchbegriffs schreibt der angreifende Computer eine Befehlsfolge in das Eingabefeld, die den Inhalt der abgefragten Datenbank aktiv verändert. Statt eines Lesezugriffs erfolgt also ein

Schreibzugriff auf die Datenbank. «Solche Angriffe sind in der Praxis schwer zu verhindern», erklärt Stefan Frei. Bleibt der Hacker unentdeckt, kann er jeden einzelnen Datenbankeintrag gezielt verändern. Wer danach die manipulierte Website besucht, wird über die manipulierten Datenbankeinträge direkt auf eine mit Trojanern infizierte Hacker-Site geleitet. Je älter die Software, desto grösser das Risiko, dass der Schädling erfolgreich seinen Code ausführt. Dadurch wird der PC automatisch zu einem Mitglied im Botnet des Hackers. Solche Netze können aus Millionen von PC bestehen.

Trotz der Gefahr verwenden aber über 45 Prozent aller Surfer eine veraltete Programmversion. Oder sie nutzen zwar die neueste Fassung, haben es aber versäumt, alle verfügbaren Sicherheits-Updates einzuspielen. Herausgefunden haben die Forscher dies, indem sie zwischen Januar 2007 und Juni 2008 die Suchanfragen bei Google analysiert haben. Neben dem Suchbegriff übermittelt jeder Browser nämlich immer auch seine Versionsnummer an die aufgerufene Website, in diesem Fall an Google. Der Suchmaschinenbetreiber hat diese Daten gespeichert und für die Studie anonymisiert zur Verfügung gestellt. «Google hat weltweit einen Marktanteil von 75 Prozent», sagt Frei. «Somit stand uns eine riesige Stichprobe zur Verfügung, die einen repräsentativen Querschnitt aller Internetnutzer bildet.»

## Vorbild Firefox

Vorbildlich verhalten sich offenbar die Nutzer des Firefox-Browsers: Über 83 Prozent hatten im Juni 2008 alle Updates eingespielt. Weniger als 50 Prozent waren es dagegen beim Marktführer Internet Explorer von Microsoft, etwas besser sieht es bei Apple Safari und dem Opera-Browser aus.

«Firefox sucht bei jedem Programmstart automatisch nach Updates», erklärt Frei. Falls vorhanden, werden sie sofort installiert. Auch der Opera-Browser kontrolliert seine Aktualität automatisch. «Updates müssen hier aber manuell heruntergeladen und der Browser muss anschliessend komplett neu installiert werden.» Der Internet Explorer wird von Microsoft alle 30 Tage automatisch aktualisiert. Sein schlechtes Abschneiden in der Studie geht daher auf das Konto von Internet-surfern, die immer noch die Version 6 statt der neuesten Version 7 nutzen.

«Unsere Studie zeigt, dass Computersicherheit auch ein Problem der Ergonomie ist. Updates dürfen keinen Aufwand verursachen, um von den Kunden akzeptiert zu werden», sagt Frei. Häufig fehle bei den Anwendern auch das Bewusstsein, dass Software ein «verderbliches Gut wie ein Nahrungsmittel» sei, kritisiert Frei. Die Wissenschaftler fordern daher eine Art Haltbarkeitsdatum für Browser: «Dem Nutzer sollte stets angezeigt werden, wann sein Programm zuletzt nach Aktualisierungen gesucht hat und wie viele inzwischen verfügbare Updates noch nicht installiert wurden.»

## Notebook



### Flachbildschirme und Klima

Die Produktion von Flachbildschirmen könnte zu einer wachsenden Emission des Treibhausgases Stickstofftrifluorid (NF<sub>3</sub>) führen, vermutet der amerikanische Forscher Michael Prather von der Universität Kalifornien in Irvine. NF<sub>3</sub> sei als Treibhausgas 17 000-mal schädlicher als Kohlendioxid und verbleibe 550 Jahre lang in der Atmosphäre. Sein Produktionsvolumen dürfte sich wegen des Booms bei LCD-Fernsehern derzeit jährlich verdoppeln. Im Unterschied zu anderen, weniger potenten Treibhausgasen ist NF<sub>3</sub> aber in keinem internationalen Umwelt- und Klimaschutzabkommen erfasst. Allerdings ist unklar, wie die Elektronikindustrie mit dem Stoff umgeht. Ein grosser Hersteller des Gases sagte dem Wissenschaftsmagazin «New Scientist», dass nur wenig in die Atmosphäre gelange, und der japanische Elektronikkonzern Matsushita verzichtet bereits auf die Chemikalie. (hir.)

### Steve Jobs' Tagebücher

Zwei Jahre lang haben «Die geheimen Tagebücher von Steve Jobs» die Techno-

logiebranche beschäftigt. Jetzt beendet der als «fälscher Steve Jobs» (FSJ) bekannt gewordene Autor sein populäres Blog, berichtet die «New York Times». Der richtige Name des Autors war lange Zeit unbekannt, bis die englische «Times» letzten Sommer das Geheimnis lüftete und berichtete, dass Daniel Lyons, ein früherer Journalist des Magazins «Forbes», der Verfasser war. Nun hat Lyons offenbar das Interesse an der von ihm geschaffenen Figur FSJ verloren. Lyons wird in Zukunft als Technik-Kolumnist beim Nachrichtenmagazin «Newsweek» tätig sein. (hir.)

### Altes iPhone nicht updaten

Seit Freitag ist nicht nur das neue iPhone in Schweizer Shops zu kaufen. Apple hat gleichentags auch die neue Software-Version 2.0 für das iPhone der ersten und der neuen Generation veröffentlicht. Wer in der Schweiz ein solches Gerät benutzt und die SIM-Sperre entfernt hat, sollte vorläufig nicht auf die neue Programmversion updaten, weil das Handy dann erneut gesperrt und somit in Schweizer Netzen unbrauchbar werden könnte. Auch von einem Update der iTunes-Software, die zum Synchronisieren des iPhone mit dem Computer verwendet wird, ist abzuraten, solange im Internet noch keine neue Software zum Brechen der aktualisierten iPhone-Sperre verfügbar ist. (hir.)

### Google-Handy im Oktober

Gemäss Gerüchten im Internet wird T-Mobile USA schon am 1. Oktober ein Handy mit dem offenen Google-Betriebssystem Android auf den Markt bringen. An diesem Stichtag lanciert T-Mobile in den USA

auch sein Mobilfunknetz der dritten Generation. Das Google-Handy würde diesen Start öffentlichkeitswirksam unterstützen. Die Hardware soll der taiwanische Hersteller HTC liefern, berichtet «The Register». Auch für Google handelt es sich um ein Prestigeprojekt, denn der Suchmaschinenbetreiber hatte versprochen, das erste Android-Handy werde noch dieses Jahr auf den Markt kommen. Bisher war das Projekt aber von verschiedenen Verzögerungen geplagt. So erwies sich die Anpassung von Handy-Applikationen als schwierig, die ursprünglich für andere Betriebssysteme geschrieben wurden. Laut «Register» könnte das T-Mobile-Handy daher zunächst mit einer geringeren Anzahl von zugänglichen mobilen Diensten ausgeliefert werden. (hir.)



## Wie geht das?



## Klimageräte

Im Prinzip arbeiten sie wie ein Kühlschrank. Eine kühlende Fläche nimmt Wärmeenergie aus dem Innenraum auf und leitet sie über einen Kältemittel-Kreislauf an einer wärmeableitenden Fläche ins Freie. Beim Kühlschrank befindet sich Letztere auf der Geräte-rückseite. Bei einem Klimagerät unterscheidet man zwei unterschiedliche Bau-Typen: Monogeräte, bei denen beide Flächen in einem Gehäuse stecken, und Splitgeräte, bei denen die wärmeableitende Fläche im Freien steht.

Im Übrigen funktioniert die Kühlung genau gleich: Innerhalb eines geschlossenen Kreislaufs zirkuliert ein Kältemittel. Ein Kompressor saugt das Kältemittel an und komprimiert es. Dabei erwärmt sich das Gas – der gleiche Effekt, den man von einer Velopumpe her kennt. Das heisse Gas wird anschliessend durch einen Wärmetauscher (die erwähnte wärmeableitende Fläche) geleitet. Dabei kühlt sich das Gas ab und kondensiert. Jetzt durchströmt die unter Druck stehende Flüssigkeit ein Ventil, hinter dem ein niedriger Druck herrscht. Deshalb wechselt das Kältemittel erneut seinen Aggregatzustand und wird gasförmig. Die zum Verdampfen erforderliche Energie entzieht das Kältemittel der Raumwärme. Deshalb sinkt dort die Temperatur. Anschliessend gelangt das Kältemittel wieder zum Kompressor, und der Kreislauf beginnt von neuem.

Ein Splitgerät benötigt Rohrleitungen, durch die das Kältemittel zwischen dem inneren und äusseren Geräteteil zirkulieren kann. Ein Monogerät kommt ohne diesen Installationsaufwand aus. Dafür muss aber ein Fenster geöffnet bleiben, durch das die warme Luft nach draussen geblasen wird. Dies hat zur Folge, dass Luft von draussen in den Raum nachströmt, was die Kühlwirkung je nach den im Freien herrschenden Temperaturen begrenzt und den Energieverbrauch in die Höhe treibt. (hir.)

Ihre Fragen: wie-geht-das@nzz.ch