Ist Ihr Webbrowser sicher?

Wer Sicherheitsupdates für seinen Webbrowser nicht sofort installiert, kann leicht Opfer eines Drive-by-Downloads werden. Unsere weltweiten Messungen belegen, dass der verwendete Updatemechanismus die Internetsicherheit wesentlich mitbestimmt. Thomas Dübendorfer

Dr. Thomas Dübendorfer ist Präsident der Information Security Society Switzerland (ISSS), www.isss.ch, und Senior Software Engineer Tech Lead bei Google Switzerland GmbH.
thomas@duebendorfer.ch

Im März 2010 wurden die Betreiber des Botnetzwerks «Mariposa» in Spanien verhaftet. Diese kontrollierten bis Ende 2009 ein Botnetzwerk aus gegen 13 Millionen Computern in 190 Ländern. Diese Computer waren mit Schadsoftware infiziert, die Passwörter und Kreditkartendaten heimlich ausspionierte und zu den Hackern ins Internet schickte. Wie konnte es dazu kommen, dass eine kleine Hackergruppe Zugang zu derart vielen Computern erlangen konnte? Die eingesetzte Schadsoftware verbreitete sich unter anderem via Drive-by-Download: Beim Besuch einer für Mariposa präparierten Webseite wurde die Schadsoftware in älteren Browserversionen mit bekannten Sicherheitsschwachstellen automatisch im Hintergrund installiert. Ansonsten wurde dem Benutzer der Download der Schadsoftware als angebliches Update für Adobe Acrobat Reader angeboten.

Schwachstellen in Webbrowsern

Die zahlreichen Webbrowser überbieten sich gegenseitig mit immer neuen Funktionalitäten (auch «Features» genannt), um die Gunst der Internetnutzer für sich zu gewinnen. Sicherheit, die nicht direkt sichtbar oder messbar ist, scheint beim «Featuritis»-Wettbewerb nebensächlich zu sein. Abbildung 1 zeigt die Anzahl neu entdeckter Schwachstellen in Webbrowsern (ohne Plug-ins) pro Jahr, aufgeteilt nach Risikostufe. Diese Schwachstellen werden in der öffentlichen National Vulnerability Database (NVD) zusammen mit den betroffenen Softwareversionen publiziert.

Seit 2003 wurden jedes Jahr noch mehr neue Schwachstellen gefunden. Der Anteil von Schwachstellen mit hohem Risiko lag oft über 30 Prozent. Im Jahr 2008 und ebenso im Jahr 2009 wurde in jedem der fünf populärsten Webbrowser Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera und Apple Safari mindestens eine gravierende

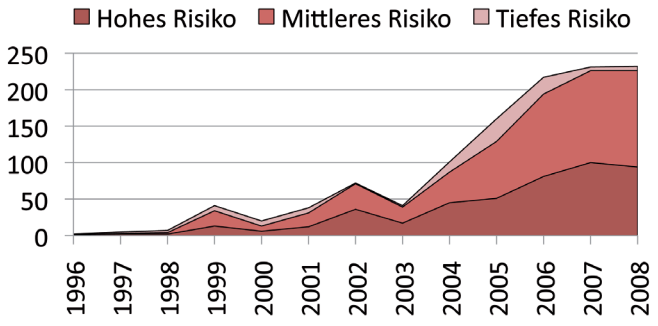

Abbildung 1: Anzahl neu entdeckter Schwachstellen in Webbrowsern (ohne Plug-ins) nach Risikostufe pro Jahr. Quelle: National Vulnerability Database (NVD)

Schwachstelle entdeckt, die es erlaubte, über einen Drive-by-Download Software auf den Computer des Benutzers unbemerkt herunterzuladen und zur Ausführung zu bringen. Bei den Browser-Plug-ins sieht die Softwaresicherheit leider auch nicht besser aus. Die weit verbreitete Videoabspielsoftware «Apple Quicktime» enthielt 125 Schwachstellen in der Zeit von 1996 bis 2008 und der «Adobe Acrobat» wies 59 Schwachstellen in dieser Zeit auf. Abbildung 1 zeigt klar, dass die heutigen funktionsreicheren Webbrowser von wesentlich mehr Sicherheitsschwachstellen betroffen sind als frühere Browserversionen, die weniger «Features» vorzuweisen hatten. Deshalb aber eine alte Webbrowserversion einzusetzen in der Hoffnung, diese sei sicherer, ist aber oftmals ein Irrweg; später gefundene Schwachstellen werden in älteren Browserversionen oftmals gar nicht mehr behoben, da der Support längst dafür eingestellt wurde. Es bleibt dem Internetnutzer mit einem Bedürfnis nach Sicherheit also nichts anderes übrig, als möglichst schnell neu verfügbare Sicherheitsupdates für den verwendeten Webbrowser einzuspielen.

Der Updatemechanismus ist zentral für sicheres Surfen

Es ist lobenswert, dass die Hersteller der Webbrowser in der Regel binnen weniger Wochen eine gemeldete Sicherheitsschwachstelle beheben, die neue Version aufwendig testen und den Nutzern kostenlos ein Update zur Verfügung stellen. Wenn die Benutzer das Update nicht oder erst sehr spät installieren, wird der mögliche Sicherheitsgewinn beim Benutzer allerdings stark reduziert, trotz der schnellen Reaktion der Hersteller. Für die Maximierung des Sicherheitsgewinns ist ein gut funktionierender Updatemechanismus, der jede Installation der fehlerhaften Software binnen kurzer Frist auf den neuesten Stand bringen kann, absolut zentral. Genau daran scheitern aber auch heute noch mehrere Browserhersteller. Ein konkretes Beispiel ist der Mix von Opera-9.x-Webbrowserversionen im täglichen Einsatz drei Wochen nach der Verfügbarkeit von Opera 9.63 (siehe Abbildung 2a). Diese Version behob gleich drei schwerwiegende Schwachstellen, wobei jede die Ausführung von beliebigem Code durch einen Angreifer im Internet ermöglichte. Gemäss unseren Messungen auf den weltweit verteilten Webservern von Google kamen die Anwender der Aufforderung von Opera zur Installation des Updates allerdings nur zu 24 Prozent nach. Die restlichen 76 Prozent surften unbekümmert weiterhin mit einer älteren verwundbaren Version des Opera-9.x-Webbrowsers auch nach öffentlicher Bekanntgabe der gravierenden Sicherheitsschwachstellen durch den Hersteller.

Beim Webbrowser Apple Safari wurden in Version 3.2 mehrere gravierende Schwachstellen behoben, darunter eine, die auf Windows und Mac OS X die Ausführung von beliebigem Code beim Besuch einer speziell präparierten Webseite erlaubte. Version 3.2 hatte allerdings Stabilitätsprobleme, welche die Version 3.2.1 behob. Wie in Abbildung 2b ersichtlich, hatten drei Wochen nach Verfügbarkeit von Version

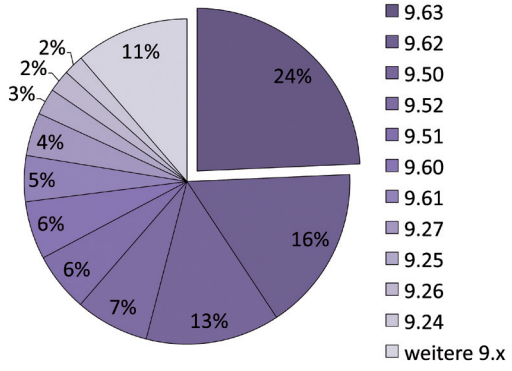

Abbildung 2a: Verwendete Versionen von Opera 9.x drei Wochen nach Verfügbarkeit des Sicherheitsupdates 9.6.3. Quelle: Google

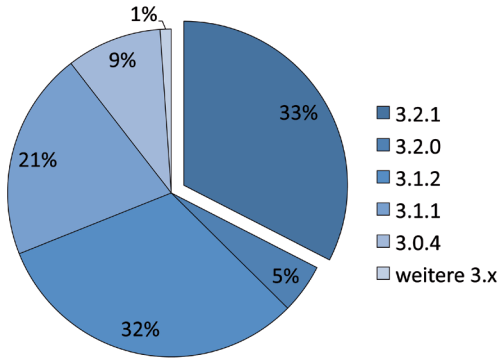

Abbildung 2b: Verwendete Versionen von Apple Safari 3.x drei Wochen nach Verfügbarkeit des Sicherheitsupdates 3.2.1. Quelle: Google

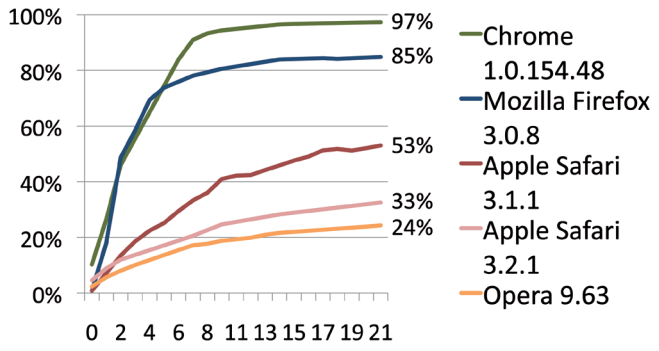

Abbildung 3: Anteil aktualisierter Webbrowser (innerhalb der gleichen Hauptversion) über den Zeitraum von 21 Tagen nach Updateverfügbarkeit. Quelle: Studie «Web Browser Security Update Effectiveness», Dübendorfer, T. (Google), Frei, S. (ETH), CRITIS 2009

3.2.1 erst 33 Prozent der Apple-Safari-Benutzer dieses Update installiert. Weitere 5 Prozent der Benutzer hatten immerhin auf Version 3.2.0 gewechselt. Die restlichen 62 Prozent der Apple-Safari-Benutzer surften weiterhin unbekümmert mit einem verwundbaren Webbrowser im Internet. Mit ein Grund, warum das Update 3.2.1 nur von 33 Prozent der Apple-Safari-Benutzer binnen dreier Wochen eingespielt wurde, war sicher auch, dass dieses Browserupdate auf Mac OS X nur dann installiert werden konnte, wenn man über Mac OS X Tiger ab 10.4.11 oder Mac OS X Leopard ab 10.5.5 verfügte und zudem vorerst das neueste Mac-OS-X-Sicherheitsupdate 2008-007 eingespielt hatte. Diese Abhängigkeit führte paradoxerweise gar dazu, dass Windows-Benutzer von Safari wesentlich schneller Apple Safari 3.2.1 installierten und dadurch früher geschützt waren als die Apple-Safari-Benutzer auf Mac OS X. Der Vorgänger Apple Safari 3.1.1 hatte diese Abhängigkeit vom Patchlevel des Betriebssystems nicht und wurde von immerhin 53 Prozent der Apple-Safari-Benutzer binnen dreier Wochen ab Verfügbarkeit installiert. Je mehr technische Voraussetzungen ein Update verlangt, umso weniger Endsysteme erreicht man damit.

In meiner ersten Studie, basierend auf anonymisierten Besucherstatistiken der Webserver von Google, die zusammen mit der Communication Systems Group (CSG) der ETH Zürich erstellt wurde, konnte nachgewiesen werden, dass im Jahr 2008 gut 45 Prozent der Websurfer weltweit nicht die neueste verfügbare Browserversion verwendeten.

Faktoren für die Effektivität eines Updates

Damit ein Update den Endbenutzer erreicht, müssen die vier Schritte Entdeckung, Download, Installation und Aktivierung durchlaufen werden. In jedem Schritt kann wertvolle Zeit verloren gehen, sodass der Benutzer mit einem unsicheren Webbrowser im Internet surft, trotz Vorliegen eines Sicherheitsupdates beim Hersteller. In welchem Schritt wie viel Zeit verloren geht, hängt direkt mit dem verwendeten Updatemechanismus und dessen Einstellungen ab. Einzig Google Chrome automatisiert standardmässig die Entdeckung, den Download und die Installation des Updates ohne einen einzigen Benutzereingriff zu erfordern.

Zudem werden bei laufendem Computer Updates alle 5 Stunden durch den vom Browser unabhängigen Updatedienst gesucht. Die Updateprüfung der anderen Webbrowser erfolgt maximal einmal täglich beziehungsweise nur bei Benutzung des Browsers. Bei Opera wurde bis Version 9 maximal einmal pro Woche nach (Sicherheits-) Updates gesucht und die Updateinstallation war gleich aufwendig wie eine manuelle Erstinstallation. Im September 2009 erhielt Opera in Version 10 endlich eine Auto-Update-Funktion. Mozilla Firefox testet bei jedem Start oder auf Wunsch seltener nach Updates und fragt beim Benutzer aufdringlich nach, ob denn nun das verfügbare Update installiert werden darf. Dieses Verhalten führt dazu, dass viele Benutzer dem Update bald zustimmen.

Wie gut funktioniert die Updateverteilung nun aber im Internet wirklich? Dazu haben Stefan Frei von der ETH Zürich und ich im Jahr 2009 in einer zweiten Webbrowserstudie die anonymisierten Besucherlogs der weltweit verteilten Google-Webserver ausgewertet.

Updatemechanismen im Feldtest

Wenn ein Webbrowser von einen Webserver eine Webseite anfordert, schickt dieser nicht nur seinen Namen wie zum Beispiel «Mozilla Firefox», sondern auch gleich noch das verwendete Betriebssystem und die Versionsnummer des Webbrowsers mit. Dies ermöglicht dem Webserver, die Webseite optimal für die Anzeige im Webbrowser aufzubereiten. Die Versionsnummer kann zudem verwendet werden, um festzustellen, welches Update eingespielt wurde. Einzig Microsoft Internet Explorer beschränkt sich auf die Hauptversionsnummer (z.B. «8» statt «8.0.6001.18702»), weshalb er in der zweiten Studie nicht berücksichtigt werden konnte. Um doppelte Zählungen bei Mehrfachbesuchen des gleichen Webbrowsers zu eliminieren, wurden die bereits vorhandenen Cookies benutzt, die jedem installierten Browser eine eindeutige temporäre Kennung zuordnen. Die Messresultate in Abbildung 3 zeigen eindrücklich, wie unterschiedlich stark der Anteil der Benutzer mit dem neuesten Update innerhalb der gleichen Browserfamilie und Hauptversion wächst über den Zeitraum von 21 Tagen nach Updateverfügbarkeit. Je schneller der Anstieg, desto grösserer der Anteil der Benutzer, der optimal geschützt ist.

Das Rennen um mehr Features in den Webbrowsern wird wohl ungebremst weitergehen. Es bleibt zu hoffen, dass die Sicherheit des Endbenutzers in Zukunft vermehrt als wichtiges Kriterium für den besten Browser mitgewertet wird. Wann haben Sie das letzte Mal überprüft, ob Sie mit dem neuesten Webbrowser surfen?