

Sicherheit im Internet: Verwenden Sie den sichersten Web-Browser?

Mit der immer wichtigeren Rolle des Internet in der heutigen Gesellschaft hat sich das Netz von einem nützlichen, aber doch eigentlich entbehrlichen Instrument zu einer Infrastruktur entwickelt, deren Verfügbarkeit und korrektes Funktionieren für praktisch alle unsere Tätigkeiten kritisch ist – sei dies für unsere geschäftlichen Bedürfnisse, für private Information und Kommunikation oder für die öffentlichen Dienste, die wir täglich nutzen. Das korrekte Funktionieren des Internet wird heute aber stark von dessen Sicherheit bestimmt.

von Stefan Frei und Bernhard Plattner

Die «Sicherheitslandschaft» des Internet hat sich in den vergangenen zwei Dekaden stark verändert. Während das Thema Sicherheit in der Anfangszeit kaum von Bedeutung war, kam es auf gelegentlich spektakuläre Art auf die Frontseiten der Presse (z. B. mit dem «Microsoft Blaster» Wurm, 2003). Würmer, Viren und andere Schadsoftware werden verbreitet, indem sicherheitsrelevante Fehler in der Betriebs- oder Anwendersoftware (sog. Schwachstellen) auf geeignete Weise genutzt werden. Heute sind wir daran gewöhnt, dass Schwachstellen in den von uns

benutzten Betriebssystemen regelmässig behoben werden (durch sog. Patches, die via Updates eingespielt werden). Weniger bekannt ist, dass die Nutzniesser der Schwachstellen heute bestens organisiert sind und in einer arbeitsteiligen, professionellen Art und Weise solche Schwachstellen nutzen, um privat oder beruflich genutzte Computer zu infiltrieren, mit dem Ziel, diese fernsteuern zu können und um an sensitive persönliche Daten heranzukommen. Letztere wiederum ermöglichen Angriffe auf die Nutzer von Diensten wie Telebanking oder e-Shopping [1].

Webbrowser sind ein lukratives Angriffsziel

Während in der Vergangenheit die Schwachstellen von Betriebssystemen wie Windows oder Mac OS die hauptsächlichen Einfallstore der Angreifer waren, sind heute die allgemein genutzten Web-Browser (Internet Explorer, Firefox, Safari etc.) im Visier der organisierten Kriminellen. Web-Browser sind komplexe Programme, die ebenfalls kritische Schwachstellen aufweisen. Dazu kommt, dass eine ganze Reihe von allgemein verwendeten Erweiterungen oder Plug-Ins (wie z. B. der Acrobat Reader, Adobe Flash oder Apple's Quicktime) die Komplexität vergrössern und ihre eigenen Schwachstellen beisteuern. Die Grafik in Fig. 1 zeigt, dass die Zahl der (entdeckten) Schwachstellen in Webbrowsern seit 2003 rasant angestiegen ist. Sie werden auch rege genutzt. Eine verbreitete Form eines Angriffs ist der «Drive-by Download». Dieser Angriff wird beim einfachen Betrachten einer entsprechend präparierten Webseite ausgeführt. Die schädliche Software wird dabei im Hintergrund auf den Computer des Opfers heruntergeladen, unter Ausnutzung einer Schwachstelle im verwendeten Webbrowser oder einer zugehörigen Erweiterung. Die besuchte Webseite kann von den Cyber-Kriminellen selbst bereitgestellt sein (z. B. auf einem Portal mit pornografischen Inhalten) oder ist eine vielbesuchte Webseite, die vorgängig von den Angreifern manipuliert wurde. Beispiele dafür gibt es genug: Im Jahr 2008 war die Webpräsenz der Vereinten Nationen, www.un.org, zeitweise manipu-

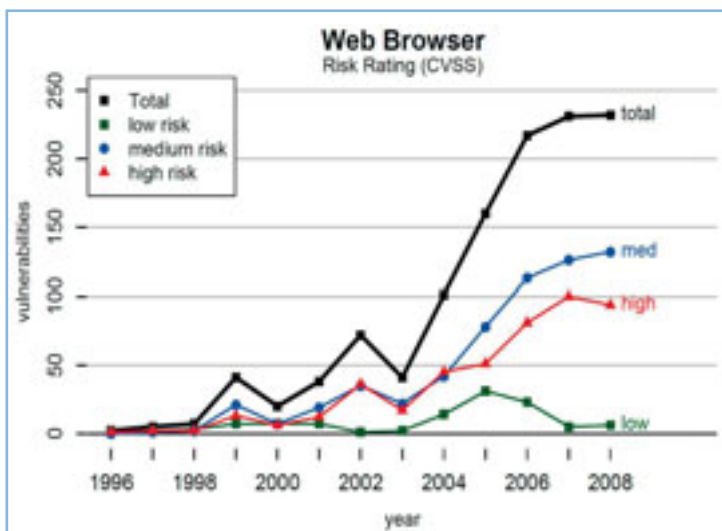


Fig. 1: Entwicklung der Anzahl gefundener Schwachstellen in Browsern seit 1996

liert; kürzlich war die Webseite der *New York Times* gleichermaßen betroffen.

Daraus folgt, dass auch Webbrowser regelmässig nachgeführt werden müssen und nur dann einigermaßen sicher sind, wenn tatsächlich alle zur Zeit verfügbaren Updates auch installiert sind. Damit stellt sich die Frage, wie schnell jeweils die von den Herstellern bereitgestellten Updates in den Browsern der Nutzer installiert werden. Eine gross angelegte Untersuchung, die an der ETH Zürich in Zusammenarbeit mit Google durchgeführt wurde, zeigt ein erschreckendes Bild. Untersucht wurden die von Benutzern der Google-Dienste verwendeten Browser auf ihren Zustand betreffend die Installation von Patches. Die Resultate zeigen, dass zwischen Januar 2007 und Juni 2008 weltweit durchschnittlich 637 Millionen Surfer (oder 45 % der Internet-Nutzer) einen Webbrowser verwendeten, der nicht auf den neuesten Stand nachgeführt war. Dies bedeutet, dass die Cyberkriminellen genügend Angriffsflächen vorfinden, weitgehend unabhängig davon, wie schnell die Hersteller erkannte Probleme beseitigen.

Wie schnell werden Patches installiert?

Es stellt sich nun die Frage, warum vorhandene Patches von einem Grossteil der Benutzer nur mit grosser Verzögerung eingespielt werden und welche Faktoren diesen Prozess beeinflussen. Dazu untersuchen wir die Update-Mechanismen, die von den Herstellern be-

kannter Browser eingesetzt werden, und messen deren Effektivität. Ein Update-Prozess kann grundsätzlich in drei aufeinanderfolgende Phasen aufgeteilt werden:

1. Vorhandensein von neuen Updates feststellen
2. Download der Updates
3. Installation der Updates

Die einzelnen Schritte erscheinen trivial, deren Umsetzung jedoch ist unterschiedlich, abhängig vom Hersteller des Browsers, was letztlich die Effektivität des gesamten Update-Prozesses bestimmt. Im Folgenden untersuchen wir die bekanntesten Browser: *Internet Explorer*, *Firefox*, *Apple Safari*, *Google Chrome* und *Opera*.

Browser erkennen neue Updates, indem sie regelmässig den Server des Herstellers danach abfragen. Die Frequenz, mit der diese Abfragen durchgeführt werden, variiert von fünf Stunden bis zu einer Woche. Im Extremfall verstreichen also 7 Tage, bis der Browser nur schon vom Vorhandensein eines Update erfährt. Der Download des Update geschieht dann entweder automatisch oder manuell. Dabei wird entweder das Update ohne Rückfrage an den Benutzer im Hintergrund heruntergeladen, oder der Download des Updates muss durch den Benutzer manuell gestartet werden, z. B. durch einen Mausklick oder sogar über einen Besuch der Download-Seite des Herstellers. Ist das Update lokal vorhanden, muss es installiert werden. Dies kann wiederum automatisch geschehen oder manuell durch einen Mausklick. Im Extremfall

Browser	Marktanteil	Update erkennen (Voreinstellung)	Download	Installation
Internet Explorer	68.8 %	täglich durch Betriebssystem	automatisch	automatisch
Mozilla Firefox 3.x	22.9 %	beim Start, kann ausgeschaltet werden	automatisch	manuell durch einen Mausklick
Apple Safari 3.x	3.6 %	wöchentlich, durch Betriebssystem	manuell, durch Betriebssystem Updater	manuell
Opera 9.x	2.1 %	wöchentlich	manuell, Download von Opera Website	manuell, Neuinstallation des Browsers
Google Chrome	1.6 %	alle 5 Std.	automatisch	automatisch, keine Benutzerintervention möglich

Tabelle 1: Update-Mechanismen von Google Chrome 1.x, Mozilla Firefox 3.x, Apple Safari 3.x und Opera 9.x. (Marktanteile vom April 2009 von hitlink.com)

bedeutet die Installation eines Updates eine Neuinstallation des Browsers. Tabelle 1 fasst die voreingestellten Parameter der Update-Mechanismen der untersuchten Browser zusammen.

Nach erfolgter Installation ist in jedem Fall ein Neustart des Browsers notwendig, um die zuvor installierte neueste Version zu aktivieren.

Messmethode

Beim Besuch einer Webseite gibt ein Browser seinen Namen und die Versionsnummer bekannt. Alle Browser, ausgenommen der Internet Explorer, geben die Major- und die Minor-Version bekannt (z. B. bezeichnet in «Firefox/3.0.8» die Zahl 3 die Major-Version und «0.8» die Minor-Version). Die Minor-Version erlaubt den Rückschluss auf den letzten installierten Patch. Diese Angaben finden sich in den Logdaten von Webservern. Aus anonymisierten Logs der Dienste von Google der ersten neun Monate im Jahr 2009 können wir die Versionsangaben (Major/Minor) und damit den Patch-Zustand der Browser eines beträchtlichen Teils der weltweiten Internet-Benutzer bestimmen. Leider ist eine genaue Analyse für den Internet Explorer nicht möglich, da dieser einem Web-Server seine «Minor Version» nicht mitteilt.

Resultate

In einem ersten Schritt messen wir während 21 Tagen nach der ersten Verfügbarkeit eines Patches den Anteil derjenigen Benutzer, welche den Patch installiert haben. Fig. 2 zeigt die Adoption der aktuellsten Patches für verschiedene Browser im April 2009 [3]. Die Unterschiede sind frappant. Google Chrome und Firefox führen mit über 80 %, während bei den anderen Browsern nach 21 Tagen maximal 53 % der Benutzer den Patch installierten. Der hohe Anteil von Google Chrome und Firefox kann mit der hohen Automatisierung des Update-Prozesses erklärt werden. Bei Google Chrome ist keine Benutzerinteraktion nötig, der Prozess ist vollständig automatisiert und der Benutzer hat auch keine Möglichkeit einzugreifen – beim nächsten Start des Browsers wird die aktualisierte Version automatisch verwendet (dies wird als «silent update» bezeichnet). Bei Firefox kann der Benutzer, nachdem ein Update im Hintergrund heruntergeladen wurde, mit einem Mausklick entweder der sofortigen Installati-

on zustimmen oder diese auf später verschieben. Die Nachfrage von Firefox führt offenbar dazu, dass dieser in den ersten fünf Tagen besser abschneidet als Google Chrome. Firefox-Benutzer werden auf ein anstehendes Update aufmerksam gemacht und wählen bei der Anfrage die Installation, während Benutzer von Google Chrome nichts von einem bereitstehenden Update erfahren; der erforderliche Neustart des Browsers erfolgt daher mit einer gewissen Verzögerung.

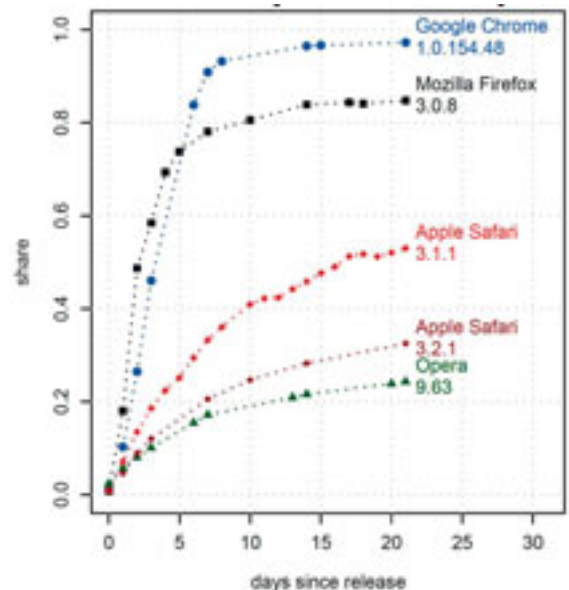


Fig. 2: Anteil der Benutzer, die den aktuellsten Patch in den ersten 21 Tagen nach seiner Bereitstellung installierten

Interessant sind die unterschiedlichen Resultate für Safari 3.1.1 und 3.2.1. Der Anteil der neueren Version 3.2.1 steigt langsamer und erreicht einen geringeren Wert als derjenige der älteren Version 3.1.1. Der Grund dafür liegt darin, dass ein Update auf Safari 3.2.X die aktuellste Version des Apple-Betriebssystems Mac OS-X Tiger oder Leopard voraussetzt. Damit haben die Benutzer von älteren Versionen des Betriebssystems gar keine Möglichkeit, den Patch einzuspielen. Vor der Aktualisierung des Browsers muss daher zwingend das Betriebssystem aktualisiert werden – diese zusätzliche Restriktion bewirkt eine Reduktion des Anteils der neusten Version um ca. 20 %. Opera liegt weit abgeschlagen zurück, da ein Update einer kompletten Neuinstallation des Browser – inklusive eines manuellen Downloads – gleichkommt. Der gesamte Prozess erfordert durchschnittlich 11 Benutzerentscheide (Datei wählen, Installationsverzeichnis

wählen, Browser schliessen etc.); dies im Vergleich zu einem oder gar keinem Mausklick bei Firefox bzw. Chrome. Opera hat den Update-Mechanismus zwischenzeitlich in der seit Kurzem verfügbaren Version stark 10 verbessert.

Schlussfolgerungen

Welche Schlüsse können aus diesen Untersuchungen gezogen werden? Offensichtlich gibt es beträchtliche Unterschiede in der Dynamik der Installation von Patches. Innerhalb der ersten 10 Tage erreichen die am schnellsten nachgeführten Browser, Google Chrome und Firefox, einen Anteil der neuesten Version von zwischen 80 und 95 %. Der Grund liegt darin, dass die Durchführung eines Updates dem Benutzer so einfach wie möglich gemacht wird – ein Mausklick und 10 Sekunden Wartezeit bei Firefox, ohne Rückfrage und damit vollständig transparent für den Benutzer von Google Chrome. Apple Safari hingegen erreicht nach 10 Tagen einen Anteil von mageren 25 – 40 %, was mit grosser Wahrscheinlichkeit daran liegt, dass nur alle sieben Tage nach Updates gesucht wird, die Benutzer einen Click mehr absolvieren müssen und dass Apple ihren Browser nur gleichzeitig mit dem Betriebssystem mit Updates versieht. Am unteren Ende der Skala liegt der Browser Opera, der durch den für den Benutzer aufwändigen Update-Prozess behindert wird.

Die Ergonomie scheint ein wichtiger Faktor dafür zu sein, dass der Anwender seine Software auf dem neuesten Stand hält. Ansätze wie «silent update» von Google Chrome, der vom Anwender keine Intervention erwartet, erfüllen diese Anforderung zweifelsohne am besten. Allerdings erzeugt ein derartiger Ansatz Probleme beim Einsatz in Unternehmen, welche aus verschiedenen Gründen genau kontrollieren wollen, welche Software und -versionen von den Mitarbeitenden eingesetzt werden. Ein «silent update» würde in diesem Umfeld von den Verantwortlichen kaum akzeptiert. Dem könnte Rechnung getragen werden, indem der «silent update» per Voreinstellung zwar aktiviert ist (im Hinblick auf die grosse Masse privater Nutzer), aber beim Einsatz im Unternehmen von den Systemverantwortlichen deaktiviert werden kann.

Mehr Sicherheit im Internet erreichen wir nur mit einem interdisziplinären Ansatz, in welchem technische Massnahmen zwar eine wichtige, aber nicht die

einzigste Rolle spielen. Vielmehr müssen die gewählten Lösungen immer auf ihre Ergonomie und Akzeptanz durch die Anwender überprüft werden, ansonsten eine getroffene Massnahme ihre Wirkung verfehlen könnte. □

Referenzen

- [1] Cybercrime als Dienstleistung (2008), Digma, 8. Jahrgang, Heft 4, Dezember 2008, http://www.techzoom.net/papers/digma_cybercrime_als_dienstleistung_2008.pdf
- [2] Understanding the Web browser threat, «Insecurity Iceberg» (2008), White Paper, ETH Zürich, <http://www.techzoom.net/insecurity-iceberg>
- [3] Why silent updates boost security (2009), White Paper, ETH Zürich, <http://www.techzoom.net/silent-updates>



Dr. Stefan Frei ist IT-Security-Forscher mit Schwerpunkt Cybercrime und Dozent für Netzwerksicherheit an der ETH Zürich.



Dr. Bernhard Plattner ist Professor für Technische Informatik an der ETH Zürich. Er leitet eine Forschungsgruppe, die sich mit Computernetzen und Internet-Sicherheit beschäftigt.