



04.05.2009 13:56

## Studie: Stille Updates erhöhen Sicherheit

Die Aktualisierung des Browsers ohne Nachfrage beim Anwender ist offenbar die erfolgreichste Methode, um für eine hohe Verbreitung der jeweils aktuellen Version zu sorgen – und damit für eine geringe Zahl verwundbarer Browser. In einer gemeinsamen Studie von Google Switzerland und der ETH Zürich kommen die Autoren zu dem Schluss, dass zuviel Interaktion oder Aufwand bei einem Update dazu führe, dass Anwender den Vorgang abbrechen oder gar nicht erst starten.

Bei Opera ist für eine Aktualisierung der manuelle Download und die Installation über mehrere Dialoge erforderlich, was dazu führe, dass von den beobachteten Anwendern nur 24 Prozent die neueste Version installiert hätten. Genau andersherum stellt es sich bei Googles Chrome dar: Ein verfügbares Update wird ohne Benachrichtigung des Anwenders heruntergeladen und installiert (Silent Update). 21 Tage nach Bereitstellung eines Updates hätten 97 Prozent der beobachteten Chrome-Anwender die aktuelle Version benutzt. Bei Googles Browser Chrome ist es ohnehin nicht möglich, das automatische Update zu deaktivieren.

Bei Firefox surfen 21 Tage nach einem Release 85 Prozent mit der neuesten Version, bei Safari waren es immerhin noch 53 Prozent. Für den Internet Explorer konnten die Forscher nach eigenen Angaben keine Messungen mit ihren Webservern machen, da dieser nur unzureichende Informationen seines Patchstandes überträgt.

Die Autoren der Studie empfehlen aufgrund der Ergebnisse den Browserherstellern, Silent Updates zu implementieren, da die Vorteile auf der Hand lägen. Opera plant für die kommende Version 10 immerhin ein automatisches Update einzuführen, allerdings wird auch dies vermutlich nicht ohne Zutun des Anwenders starten.

Darüber hinaus regen die Autoren auch veränderte Patch-Strategien und -Zyklen an. So sei der starre monatliche Patchday von Microsoft ist erster Linie den Geschäftskunden geschuldet, die für die Aktualisierung ihrer Infrastrukturen feste Zeitpunkte bräuchten. Bei kritischen Lücken im Internet Explorer sei aber etwa nicht einzusehen, warum Millionen anderer Anwender längere Zeit ungeschützt blieben und bis zum nächsten Patchday warten müssten. Bereits im Februar **kritisierte[1]** der Sicherheitsdienstleister Qualys, dass die Verteilung von IE-Patches von den restlichen Sicherheits-Updates nicht getrennt sei, womit das Stopfen von Löchern mehrere Wochen dauere.

Zwar bieten aus Sicherheitssicht Silent Updates für viele Anwender enorme Vorteile, allerdings geht damit auch ein Kontrollverlust einher. Nicht jeder Anwender möchte nach seiner erstmaligen, gewollten Installation ungefragt neue Versionen auf die Platte geschoben bekommen. Zudem muss klar geregelt sein, ob sich stille Updates nur auf Sicherheitsmaßnahmen beschränken oder ob auch neue Funktionen so heimlich den Weg in das System finden können.

Die vollständige Studie ist online verfügbar: [http://www.techzoom.net/publications/silent-updates/\[2\]](http://www.techzoom.net/publications/silent-updates/[2]),

([dab\[3\]](#)/c't)

**URL dieses Artikels:**

<http://www.heise.de/newsticker/meldung/137192>

**Links in diesem Artikel:**

[1] <http://www.heise.de/security/Neuer-Exploit-nutzt-Luecke-im-Internet-Explorer--/news/meldung/132779>

[2] <http://www.techzoom.net/publications/silent-updates/>

[3] <mailto:dab@ct.heise.de>