MEDIEN

SURFEN HINTERLÄSST SPUREN

Komfort oder Privatsphäre?

Andreas Lorenz-Meyer

FOTO: RAYMOND KLEIN

Spanner gibts nicht nur am stillen Örtchen. Auch im Internet bewegen wir uns unter den Blicken von Google und Co. Ein Schelm, wer Böses dabei denkt.

Sich frei und bequem im WWW bewegen, ist für viele ein Stück Lebensqualität. Doch was tun gegen die virtuellen „Spanner", die unsere Daten ausspähen und sammeln?

„To browse" bedeutet so viel wie stöbern oder sich umsehen. Ein zutreffender Name, denn Browser sind genau dafür da. Mit den Programmen lassen sich Seiten im World Wide Web darstellen. Sie dienen sozusagen als Fenster zum Internet. Zwar herrscht Browser-Wahlfreiheit, aber die großen Vier - Microsofts Internet Explorer, Googles Chrome, Apples Safari und Mozillas Firefox – teilen sich den Markt weitgehend untereinander auf.

Wie sieht es mit der Geschwindigkeit aus? Schnell muss der Browser sein, schließlich nervt das Surfen auf Seiten, die sich nur langsam aufbauen. Es gibt verschiedene Geschwindigkeitstests, welche vor allem die Java-Script-Leistung des Browsers überprüfen. Diese Programmiersprache ist auf vielen Seiten eingebunden und bestimmt neben anderen Faktoren die Geschwindigkeit. Laut Peacekeeper scheint Firefox am besten mit Java klarzukommen. Der Browser bekommt bei diesem Test die meisten Punkte. Der Internet Explorer ist mit Abstand der langsamste. Jedoch kommen andere Tester zu anderen Ergebnissen. Bei JS Bench steht Safari an der Spitze, dicht gefolgt von Chrome. Deutlich abgeschlagen ist Firefox. Der Sunspider-Test bringt auch keine klareren Verhältnisse. Hier gewinnt der sonst auf den letzten Platz abonnierte Explorer.

Offene Türen

Welcher Browser ist also am schnellsten? Markus Limacher von InfoGuard, einem Unternehmen für Informationssicherheit, schätzt die Tests so ein: „Die Ergebnisse sind eine Momentaufnahme und werden auch durch die Messung selbst beeinflusst. Somit sind solche Tests nur bedingt aussagekräftig und mit der nötigen Vorsicht zu genießen. Unseres Erachtens sind die aktuellen Versionen der bekannten Browser über alle Einsatzgebiete hinweg ungefähr gleich schnell."

Der Browser ist leider auch ein Einfallstor für Viren. Sogar ein ziemlich großes, wenn der Browser nicht ausreichend geschützt ist. Darum nehmen die Anbieter mehr oder weniger regelmäßig Aktualisierungen vor. Bei den Neuversionen sind bestenfalls alle bekannten Sicherheitslücken gestopft. Der Nutzer sollte das Update sofort auf den Rechner laden, denn ältere Versionen bieten weniger Schutz gegen Virenangriffe.

Beim Update kann jedoch auch mal was schief gehen. Firefox hatte bei Version 37 anfangs eine so genannte opportunistische Verschlüsselung eingebaut, welche das Surfen sicherer machen soll. Doch die Verschlüsselung musste wegen eines Programmierfehlers wieder entfernt werden. Mozilla veröffentlichte flugs Version 37.1, diesmal ohne opportunistische Verschlüsselung.

Aktualisierungen sind aber nur ein Sicherheitsfaktor von vielen, erklärt Limacher. Nutzer sollten auch Malware-Scanner und Web-Filter-Funktionen installiert haben. Gefährlich kann es sein, alle möglichen Zusatzmodule zu installieren, fügt der Sicherheitsexperte hinzu. Er meint Add-ons und Plug-ins, die Erweiterungsprogramme. Da sei Vorsicht geboten, gerade bei den Nutzungsbestimmungen. Die regeln unter anderem, welche Daten für welche Zwecke gesammelt oder weitergegeben werden dürfen. Limacher: „Dem wird häufig bedenkenlos zugestimmt. Und selbst wenn man die Nutzungsbestimmungen bei Erstinstallation gelesen hat, ist man nicht auf der sicheren Seite. Der Hersteller behält sich oft vor, Änderungen an den Bestimmungen anzubringen. Diese werden dann - wenn überhaupt - nur über die jeweilige Webseite publiziert."

Über den Browser kommen nicht nur Viren herein, es gehen auch persönliche Daten hinaus. Jeder hinterlässt digitale Spuren: unter anderem die Seiten, die man anklickt, und wie lange man auf den Seiten verweilt. Limacher drückt es so aus: „Der Browser selbst ist eine Informations-Quelle, auf die nicht nur die Hersteller zugreifen, sondern auch Dritte. Viele der Funktionen, die wir alle aus Komfortgründen schätzen und vielfach nicht mehr missen wollen, fördern die Möglichkeit der Informationssammlung."

Epic schützt Privatsphäre

Zu den „Helferlein" zählen: automatische Vervollständigung von Eingaben, interaktive Browserbedienung, Spracherkennung, Formularausfüllung, Browser Cookies, Suchempfehlungen und so weiter. Wer auf ihre Dienste verzichten will, sollte zum Beispiel bei Chrome die Datenschutz-Voreinstellungen überprüfen. Bei „Rechtschreibfehler korrigieren", „Vervollständigung von Suchanfragen und URLs" oder „Nutzungsstatistiken automatisch an Google senden" muss das Häkchen weg. Anderenfalls gehen unaufhörlich Daten an Google.

Neben den großen gibt es eine Menge von unbekannten Browsern. Für sie spricht allein schon, dass sie seltener von Hackern angegriffen werden. Es gibt auch solche, die den Datenschutz schon implantiert haben. Epic gehört dazu. Sämtliche Trackingversuche, auch die von Drittanbietern, werden blockiert, lautet das Versprechen. Epic gibt bemerkenswerte Einblicke in die Prozesse, die während des Surfens im Hintergrund ablaufen. Öffnet man eine beliebige Seite, erscheint rechts unten auf dem Bildschirm für ein paar Sekunden ein kleines Fenster. In dem sind alle Dienstleister aufgelistet, zumeist solche aus dem Werbebereich, die auf den Rechner zugreifen wollten. Was ihnen Epic aber nicht gestattet hat.

Zudem ist bei diesem Browser die Suchhistorie, also die Liste aller zuvor besuchten Seiten, nicht aufrufbar. Eine Adresse muss man bei erneutem Besuch der Seite also neu eingeben. Limacher meint zu Datenschutz-Browsern wie Epic: „Diese Form der Nutzung bietet einen höheren Schutz der Privatsphäre, hat aber einen negativen Einfluss auf den Komfort. Man könnte rhetorisch fragen: Ist jeder bereit, diese Beeinträchtigung zu tragen? Da muss man abwägen, was einem wichtiger ist: Komfort oder Privatsphäre."