Do not Track! - Tools für trackingfreies Browsen

CryptoParty Dresden

6. Dezember 2012

Hier gibt es eine kleine Übersicht über Tools und Mechanismen, die sich einfach benutzen lassen, um wieder mehr Kontrolle darüber zu erhalten, wer wieviel davon weiß, wie wir uns im Internet verhalten.

Cookies und Tracking - ein paar Grundlagen

https://www.verbraucher-sicher-online.de/media/cookiefilm

Cookies aus dem Internet krümeln nicht. Dafür können sie Informationen über den Nutzer einer Internetseite speichern. Das passiert, wenn die Seite, die den Cookie beim Benutzer speichern will, aufgerufen wird. Man ruft also nicht nur die Seite ab, sondern speichert unter Umständen auch gleichzeitig einen oder mehrere Cookies dazu ab.

Doch wozu dienen Cookies eigentlich? Cookies sind auf keinen Fall per se böse, denn sie erfüllen mitunter sinnvolle Aufgaben, ohne die der Besuch einer Webseite mitunter sehr unkomfortabel und mühselig wäre. Zum Beispiel speichern sie Benutzerdaten auf Seiten, bei denen man sich einloggen muss, wie sozialen Netzwerken. Oder sie enthalten den Inhalt des Warenkorbes bei Onlineshops. Ohne Cookies müsste man diese Informationen also ständig neu eingeben, weil der Browser selbst sie sich nicht merken kann. Auch Benutzereinstellungen, wie die Sprache oder das gewünschte Aussehen einer Seite, können in Cookies abgelegt werden.

Aber Cookies können auch dazu genutzt werden, das Surfverhalten von Nutzern zu verfolgen, den Nutzer also zu *tracken*. Das geschieht meist über sogenannte *Drittanbieter-Cookies*, also jene, die gar nicht vom eigenen Betreiber der Webseite kommen, sondern von Dritten, die beispielsweise einen Werbebanner auf der besuchten Seite platziert haben und so ihre Cookies an die Nutzer der Seite verteilen. Ist dieser Drittanbieter auf mehreren Seiten im Netz vertreten, merkt das Cookie, das den Nutzer bereits vom Besuch einer anderen Seite kennt, wenn dieser weitere Seiten betritt, auf denen der Drittanbieter vertreten ist. Das Cookie kann also dazu benutzt werden, die Wege des Nutzers im Netz nachzuverfolgen. Dann kann ermittelt werden, wofür er sich interessiert und vielleicht bekommt er schon bald ganz persönliche Werbung angezeigt, die auf magische Art und Weise zu wissen scheint, wonach er gerade sucht.

Kommt Dir das bekannt vor? Willst Du nicht, dass unbekannte

andere ausnutzen, wofür Du dich gerade interessierst oder was Du deiner Mutter zu Weihnachten schenkst bevor Du selbst es weißt? Im Folgenden sind ein paar Möglichkeiten beschrieben, wie man besser kontrollieren und nachvollziehen kann, welche Informationskrümel man für wen im Netz hinterlassen will.

Tools und Co.

Cookie-Einstellungen

Auch ohne zusätzliche Tools hat man bereits die Möglichkeit, sich einen Überblick über gespeicherte Cookies zu verschaffen. Im Firefox-Browser kann man über das Einstellungsmenü[1] die Registerkarte *Datenschutz* öffnen. Wählt man *Firefox wird eine Chronik:* ***nach benutzdefinierten Einstellungen anlegen***, kann man einstellen, dass beispielsweise Cookies von Drittanbietern nicht mehr akzeptiert werden. Über den *Cookies anzeigen...*-Button lassen sich alle gespeicherten Cookies auflisten und bei Bedarf einzeln löschen.

[1] *Linux*: Bearbeiten - Einstellungen
Windows/Mac: Firefox - Einstellungen

Do Not Track

Unter dem *Datenschutz*-Menüpunkt (s.o.) findet sich an erster Stelle die Option *Websites mitteilen, dass ich nicht verfolgt werden möchte*. Diese Option sollte auf jeden Fall aktiv sein. Es handelt sich beim sogenannten **Do Not Track** (nicht verfolgen) um ein Feld, das beim Anfordern einer Internetseite vom Browser gesendet wird und dem Server signalisiert, dass der Nutzer nicht verfolgt werden will. Da die Einhaltung dieser Bitte freiwillig ist, gibt es jedoch keine Garantie, dass der Betreiber sich daran hält oder überhaupt den Inhalt des *Do Not Track*-Feldes ermittelt.

Add-ons Im Folgenden werden einige Firefox-Addons aufgelistet, die beim Verhindern unerwünschter Cookies nützlich sind und andere positive Effekte auf die Privatsphäre beim Surfen im Internet haben. Bei der Installation der Plugins ist das Vorgehen immer das gleiche: Klickt man auf *Firefox - Addons* bzw. *Extras - Addons*, öffnet sich ein Fenster zur Add-On-Verwaltung. Im Reiter *Add-ons suchen* können nun Add-ons gesucht sowie Details über Add-ons angezeigt werden.

Mehr Details und Hilfe zur Add-on-Installation: https://support.mozilla.org/de/kb/addons-finden-und-installieren-und-firefox-anpassen

Will man direkt ein Add-on über den Namen finden, kann man diesen in das Suchfeld oben rechts eingeben. Die Installation erfolgt dann über den *Installieren*- bzw. *Zu Firefox hinzufügen*-Button.

Nach der Installation muss Firefox in der Regel neu gestartet werden - nun ist das Add-on verfügbar!

Ghostery

https://www.ghostery.com/

Ghostery deckt versteckte Trackingmechanismen auf Webseiten auf (zum Beispiel Zählpixel) und zeigt dem Nutzer eine Liste der aktiven Trackingmechanismen an. Er kann sich dann dazu entschließen, welche er blockieren oder erlauben möchte. Außerdem stellt Ghostery bei Auswahl eines dem Programm bekannten Trackers zusätzliche Informationen zu dessen Herkunft bereit, wie zum Beispiel Abgaben zur Herkunftsfirma und deren Datensammlung.

Better Privacy

https://addons.mozilla.org/de/firefox/addon/betterprivacy/

Sie werden auch Flash-Cookies genannt, da sie durch das Ausführen von Flash-Plugins gespeichert werden

Better Privacy hilft dem Nutzer, Langzeitcookies zu löschen. Das sind Cookies, die nicht wie klassische Cookies ein Verfallsdatum haben, nach dem sie automatisch vom Browser entfernt werden, sondern die unbegrenzte Lebensdauer haben, weil sie in einem anderen Verzeichnis des Rechners von der Löschung unbehelligt bleiben.

AdBlock Plus

http://adblockplus.org/de/

Neben dem Effekt, dass Werbung unangenehm ist und beim Betrachten einer Website stört, werden durch ebenjene oftmals Cookies und Zählpixel auf eine Seite eingeschleust – ein Werbeblocker bietet hier einfache Hilfe!

NoScript

https://addons.mozilla.org/de/firefox/addon/noscript/

NoScript blockiert die Ausführung von Skripten, denen nicht explizit vertraut wurde. Das schützt vor der unbemerkten Ausführung von Schadcode und beispielsweise auch Flash-Cookies.