Spione im Browser

Add-on fungiert als Datenwanze für seinen Hersteller

Eine vermeintlich nützliche Browser-Erweiterung für Firefox übermittelt jede aufgerufene URL an ihren Hersteller, der mit den so gewonnenen Surf-Profilen handelt. Der Fall zeigt, dass von Browser-Add-ons bislang unterschätzte Gefahren ausgehen – und dass Nutzer vorsichtiger sein sollten.

Von Uli Ries

Eine gemeinsame Recherche der NDR-Redaktionen von Panorama und Zapp sowie mobilsicher.de sorgte jüngst für Unsicherheit bei Internet-Nutzern. Den Journalisten gelang es, bei einem Datenhändler Zugang zu kompletten Surf-Historien von mehreren Millionen deutschen Nutzern zu erhalten. Vereinzelt konnten sie ohne großen Aufwand die Historien Nutzern zuordnen und damit personalisierte Web-Bewegungsprofile erstellen.

Bei der Suche nach der Quelle für diese Daten stießen sie auf Web-Browser-Erweiterungen, insbesondere das populäre „Web of Trust“ (WOT). Dieses Add-on soll Websurfern auf Basis von Community-Feedback Hinweise zur Vertrauenswürdigkeit angesurfter Websites geben. Wegen dieser Schutzfunktion war es sehr beliebt und wurde 2013 auch von c’t empfohlen. Ausgerechnet diese Erweiterung überträgt laut NDR hinter dem Rücken der Nutzer sämtliche im Browser abgerufenen URLs an den finnischen WOT-Hersteller, der sie dann verkaufe.

Den Beweis führte der von mobilsicher.de beauftragte Sicherheitsfachmann Mike Kuketz. Er generierte eine nur ihm bekannte Subdomain für seine eigene Domain. Diese Subdomain besuchte er mit einem lediglich mit WOT erweiterten Browser. Eine Woche später fanden sich genau diese Domain-Besuche in den vom NDR abrufbaren Daten.

Insgesamt spürte der NDR in den als „Probelieferung“ bezeichneten Daten 50 Klarnamen von deutschen Websurfern auf. Unter den identifizierten Personen fanden sich beispielsweise ein Manager, ein Richter und Journalisten. Der Richter etwa habe zwischendurch SM-Pornos abgerufen, während er in Shops nach einer neuen Robe Ausschau hielt. Ein Geschäftsmann aus Hamburg speicherte Hausbau-Unterlagen und Gehaltsabrechnungen ohne Passwortschutz in einem Cloud-Speicher, der über die aufgefundene URL einsehbar war.

Identifikation möglich

WOT versichert in seinen Datenschutzbestimmungen, dass alle Daten anonymisiert vom Add-on zum Dienst übertragen würden. Offensichtlich macht das Unternehmen dabei Fehler. Die NDR-Daten enthielten übergebene URLs inklusive aller Parameter sowie Datum, Uhrzeit und die abrufende IP-Adresse. Gerade anhand per Web-Formular abgefragter und in der URL übergebenen Daten lässt sich bisweilen auf Personen schließen – beispielsweise bei zum Seiten-Login verwendeten E-Mail-Adressen, die Vor- und Zuname des Anwenders enthalten.

Die in der URL übergebenen Daten sorgen für De-Anonymisierung.

Gegenüber der Frankfurter Allgemeinen Zeitung erklärte das finnische Unternehmen, dass es die Datenschutzbestimmungen im Juli 2016 aktualisiert habe. Seither sei darin zu lesen, dass angesurfte URLs erhoben und vermarktet würden. Man habe jedoch „übersehen“, auch das für Firefox-Nutzer bestimmte Dokument zu erneuern.

Demgegenüber steht die Aussage von Sami Tolvanen. Der finnische Programmierer hat WOT erfunden und entwickelt, ist aber 2014 aus dem Projekt ausgestiegen. Er behauptete, dass die Datensammeloption bereits im April 2015 zur Firefox-Version des Add-ons hinzugefügt worden sei. Entweder habe sie mehr als ein Jahr geruht, oder WOT habe bis Juli 2016 ohne Hinweis Surf-Historien übermittelt. Die Mozilla Foundation sowie Google haben das WOT-Add-on aus ihren Download-Portalen für Firefox beziehungsweise Chrome entfernt, als sie von den NDR-Recherchen hörten. Laut Mozilla dürfte WOT dennoch in mindestens 900.000 Firefox-Installationen aktiv sein.

Mozilla wurde kritisiert, weil die Foundation eigentlich Add-ons prüft, bevor sie sie zur Installation freigibt. Einer Sprecherin zufolge ließen die Prüfer die Neuerung durch, weil WOT in seiner Datenschutzrichtlinie falsche Angaben machte. Dies sei nun auch der Grund für den Rauswurf aus der Extension-Sammlung gewesen, nicht die Sammelei selbst.

Bei den Prüfern handele es sich um eine Gruppe von Entwicklern, die sich für Mozilla ehrenamtlich die Add-ons ansehen, erläuterte die Sprecherin. Sie nähmen an sich jedes neue Add-on genauso unter die Lupe wie dessen Updates – insgesamt gebe es bis zu 300 Einsendungen täglich. Dabei seien sie aber auf die Mithilfe der Add-on-Entwickler angewiesen: Täuschen diese, rutschen fragwürdige Erweiterungen durch.

Trau, schau, wem

Dies macht ein grundsätzliches Problem deutlich: Die Prüfer und die Anwender

haben kaum eine Chance, betrügerische Extensions zu erkennen – und davon dürfte es noch einige mehr geben. Der Journalist Dirk von Gehlen, den die NDR-Journalisten anhand der Datensammlung identifizierten, versicherte beispielsweise, WOT nicht installiert zu haben. Auch das (nur per Opt-in) datensammelnde Privacy-Add-on Ghostery verwende er nicht. In seinem Fall hat sehr wahrscheinlich eine andere Erweiterung Daten aus dem Browser ausgeleitet, die dann in der NDR-Stichprobe gelandet sind.

Dass Browser-Erweiterungen Datenschleudern sein können, hat Michael Weissbacher schon vor einigen Monaten belegt. Der Österreicher ist Doktorand am Security Lab der Northeastern University in Boston und hat die Bibliothek von upalytics.com untersucht, die von insgesamt 42 Chrome-Extensions verwendet und meist ohne Wissen der Nutzer installiert wird – bislang über acht Millionen Mal. Sie ist also mehr als achtmal so oft im Einsatz wie die Firefox-Version von WOT.

Die Bibliothek analysiert das Nutzerverhalten im Browser und leitet ähnlich wie WOT abgerufene URLs aus. Viele Erweiterungen, die auf upalytics zurückgriffen, hatten jedoch ganz andere Zwecke, etwa den Download von Videos aus Facebook oder Werbung in Web-Videos zu blockieren. In 23 Nutzungsbedingungen solcher Add-ons fand Weissbacher keinerlei Hinweis auf die Tracking-Funktion. Nachdem Weissbacher seine Erkenntnisse veröffentlichte, löschte Google die Erweiterungen aus dem Chrome Web Store.

Weissbacher hält es im Fall von WOT für wahrscheinlich, dass zuerst die eigentliche Idee „Sicherheitshinweise für Web-Nutzer“ geboren und die Analyse-Vermarktung erst später angeflanscht wurde. Er könne sich aus seiner Erfahrung heraus jedoch auch gut vorstellen, dass es umgekehrt war.

Abhilfe

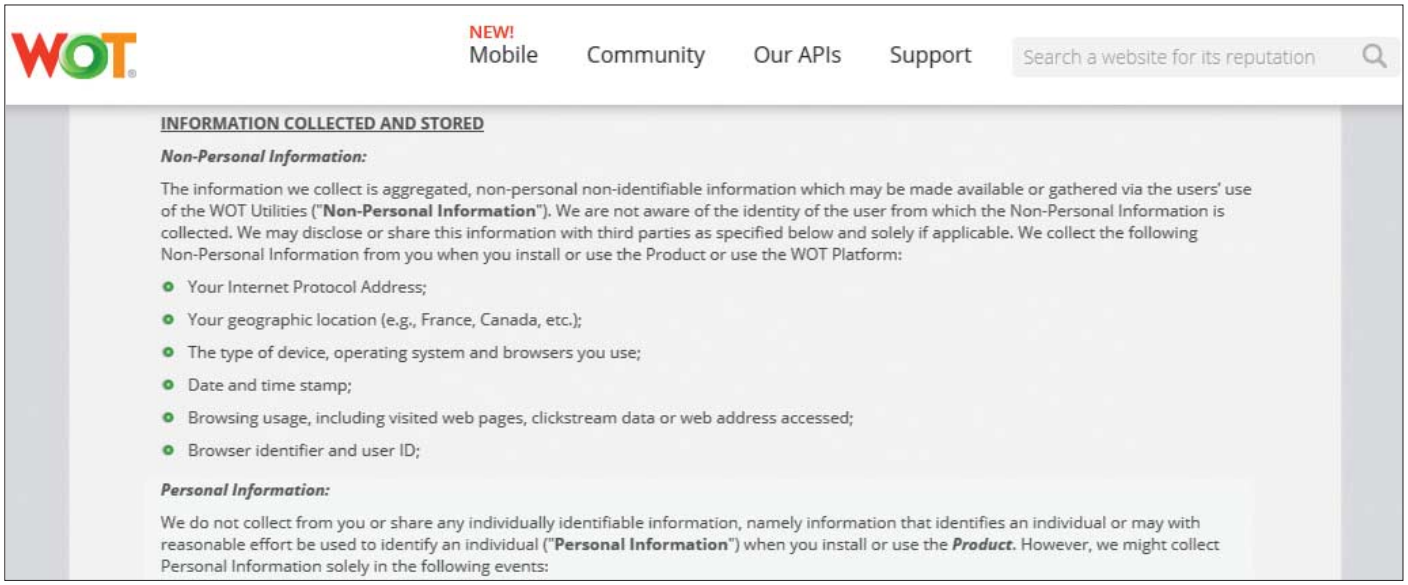
Mozilla gab gegenüber c’t zu bedenken, dass es angesichts der Architektur des Internet schwierig sei, sich gegen Tracking zu schützen und vollständig anonym zu surfen. Die Browser-Macher geben Anwendern zuallererst den Ratschlag, sich mit den Funktionsweisen des Web sowie den zum Surfen verwendeten Werkzeugen vertraut zu machen. Mozilla rät zudem, sich vor der Installation von Add-ons davon zu überzeugen, dass der Anbieter vertrauenswürdig ist. Angesichts der Diskussion um WOT, einem bis vor Kurzem unbescholtenen Anbieter, mutet dieser Tipp ein wenig skurril an.

Große Browser-Hersteller haben viel zu verlieren.

Nützlicher dürfte da schon ein Ratschlag von Michael Weissbacher sein: Anwender sollten in jedem Fall die Nutzungsbedingungen lesen. Verschweigt ein Add-on-Anbieter hier eventuelle Datensammlungen, riskiere er wenigstens den sofortigen Rauswurf aus der Sammlung. Auch die Bewertungen der Extension gäben oftmals Hinweise auf unerwünschte Schnüffelei.

Am besten reduziert man das Risiko, ausspioniert zu werden, indem man einen Browser der drei großen Hersteller Mozilla, Microsoft oder Google verwendet und keine Add-ons einsetzt. Zum einen haben diese Hersteller bereits gelernt, aufgerufene URLs zu prüfen, ohne dass sie auf den eigenen Servern eine Datenspur hinterlassen (etwa zum Schutz vor Malware-Seiten), und zum anderen können sie es sich nicht leisten, in den Mittelpunkt eines großen Datenschutzskandals zu geraten.

Das Grundproblem, dass sich aus den aufgerufenen URLs eines Nutzers mit genügend Recherche dessen Klarname und weitere Details herauslesen lassen, wird man auch auf diese Weise nicht aus der Welt schaffen können. Allerdings muss der, dem der Datensatz in die Hände fällt, gezielt forschen, um eine bestimmte Person aus der Datenmenge zu fischen. Nach allen vorliegenden Informationen sind die persönlichen Informationen im vom NDR beschafften Datensatz zu heterogen, um sie automatisch auswerten und Nutzer massenweise enttarnen zu können. *(hob@ct.de)*



In seinen Nutzungsbedingungen vom Juli 2016 informierte Web of Trust lediglich über anonymisierte Datensammelei.