Wer traut dem Web of Trust?

Vom Browser verraten: Der Skandal um die schnüffelnde Chrome- und Firefox-Erweiterung Web of Trust zeigt: Im Internet gibt es kein Entrinnen vor den Datenkapitalisten

VON FELIX KNOKE

Angeblich 140 Millionen Internetnutzer vertrauen der Browsererweiterung Web of Trust (WOT), um sich im Netz vor Datenkraken, Hackerfallen und Abzockern zu schützen. Doch dann wurde der Hersteller myWOT dabei ertappt, wie er hochbrisante Userdaten auf dem Datenmarkt anbot: Listen aller Webadressen, die Millionen von WOT-Nutzer innerhalb eines Monats aufgerufen haben – allein im Probedatensatz, den NDR-Reporter erwarben, waren die detaillierten Surfverläufe von drei Millionen deutschen WOT-Usern gespeichert. Alles nur ein Versehen, sagt der Hersteller in einer anonymen Stellungnahme und verspricht Besserung.

Wolfie Christl ist da weniger optimistisch. Für ihn ist der Vorgang ein Super-GAU: „Es ist absurd, dass eine Erweiterung, die Sicherheit verspricht, in Wirklichkeit für Unsicherheit sorgt, indem sie in extrem fahrlässiger Weise Daten weitergibt." Der Wiener Experte für Datenhandel weiß, wie Unternehmen Daten sammeln, auswerten und verkaufen – und was mit sochen Daten wie aus der WOT-Erweiterung passiert. Er hat zusammen mit der Forscherin Sarah Spiekermann ein Buch darüber geschrieben: Es ist eine äußerst präzise Studie darüber, wie im Verborgenen Nutzungsdaten zu Geld gemacht werden – oft im ethischen und rechtlichen Graubereich, aber garantiert immer zum Nachteil der Nutzer.

Geld aus Daten

Browser-Daten wie sie myWOT offenbar verkauft hat, sind besonders wertvoll im Datenkapitalismus, sagt Christl: „Aus ihnen werden Persönlichkeitsprofile für gezielte Werbung, aber auch ganz andere Zwecke erstellt." Anhand der Websites und Webdienste, die ein Mensch besucht, kann viel über dessen Gewohnheiten und Bedürfnisse abgeleitet werden. Das, für sich genommen, ist schon problematisch – aber leider auch längst Normalität. Zumindest in Deutschland bewegen sich Unternehmen, die so beschaffene Daten verwenden wollen, allerdings in einem relativ engen gesetzlichen Rahmen.

Nur: Das reicht nicht. Denn entscheidend ist, dass die erhobenen Daten so stark verfremdet werden, dass sie nicht auf eine konkrete Person zurückführbar sind. Und hier schlampte myWOT offenbar – ob aus Vorsatz oder Unvermögen, ist

derzeit noch unbekannt. „Es sieht so aus," sagt Christl, „als ob myWOT nicht nur die besuchte Webadresse plus Unterseite mitgeloggt und weiterverkauft hat, sondern die komplette URL samt Parameter." Das Erste sei üblich und werde auf großer Basis von der digitalen Werbewirtschaft betrieben. „Der zweite Fall ist aber ganz klar ein hochgradiges Sicherheitsrisiko". Komplette URLs beinhalten neben der Webadresse oft auch Daten, anhand derer auf den jeweiligen Nutzer geschlossen werden kann, etwa dessen E-Mail-Adresse, Links auf private Cloudspeicher oder Profilnamen in sozialen Netzwerken und Foren. Jeder kann das sofort in seinem persönlichen Browserverlauf nachvollziehen. MyWOT hat somit besonders schützenswerte Daten verkauft, die mit wenig Aufwand deanonymisiert werden können – und auch gegen die WOT-Datenschutzbestimmungen verstoßen.

Umfassende Profile

Datenhandelsexperte Christl überrascht der Skandal nicht: Browsererweiterungen gelten schon lange als Sicherheitsrisiko. Aber er sieht in myWOT auch nur einen vergleichsweise kleinen Knoten im Netz der Datenhändler. „Es gibt sehr viele Firmen, die unser Surfverhalten tracken." Es geht dabei um Milliarden von Internetnutzern und Millionen von Websites und Internetdiensten. Denn um Nutzerdaten ist längst ein Datenkapitalismus entstanden: Je mehr einer davon sammelt und verwertet, desto wertvoller werden sie. Umso detaillierter die echtzeitaktualisierten Dossiers über Vorlieben, Persönlichkeitseigenschaften und Verhaltensmuster sind, desto besser gelingt die gezielte Ansprache und Manipulation einzelner User. Dabei geht es längst nicht nur um Werbung, sondern auch um Kreditwürdigkeit oder das Ausreizen von Zahlungsbereitschaft.

„All diese Firmen", sagt Christl, „versuchen unser Surfverhalten, unsere Einkäufe, unsere Verhaltensdaten über Geräte, Plattformen und Lebensbereiche hinweg zu verknüpfen." Statt eines Namens schreiben die Datenhändler über ihre so erstellten Dossiers ein Pseudoym, einen eindeutigen Buchstabencode, der per Hash-Funktion aus bekannten Mailadressen oder Telefonnummern abgeleitet wird – also relativ stabilen Personenmerkmalen. Dieser eindeutige Code wird nun immer wieder einer Person zugeordnet, sobald sie von einem Tracker erkannt wird, beim Surfen zu Hause, am Arbeitsplatz, am Internet-TV oder bei der Benutzung einer Kundenkarte.

Gefährliches Ausmaß

„Es werden umfassende Profile über unseren Alltag und unser Leben angelegt, die weit über das hinausgehen, was jemals irgendeine mächtige Instanz in der Geschichte der Menschheit über einzelne Menschen wusste. Das ist extrem problematisch!" Anonymität ist in so einem System nur noch eine Farce. Um jemandem etwas zu verkaufen, muss man seinen Namen nicht kennen. Um die Brisanz der von WOT geleakten Daten zu verstehen, muss man nicht nur den Informationsgehalt scheinbar harmloser (Browsing-)Daten kennen. Ebenso erschreckend ist das Ausmaß des Datenhandels – der weltweite Markt zur Anhäufung und Veredelung solcher Daten zu vorhersagefähigen Nutzerprofilen. Nur ein Beispiel aus Christls Buch: Oracle hat im Sommer das Tracker-Unternehmen AddThis gekauft. Nach eigenen Angaben überwacht es auf 15 Millionen Websites insgesamt drei Milliarden Nutzer. Für jeden hat es ein Dossier erstellt. Bei solchen Größenordnungen versagen herkömmliche Methoden der Anonymisierung komplett: Wenn es für jeden Surfer ein Dossier gibt, das ihm eindeutig zugeordnet werden kann, spielen Namen keine Rolle mehr. Der Identifikationscode ist dann sein neuer Name. Der Kern des Problems ist aber ein anderer: Der Wunsch der Datenfirmen nach einer besseren Steuerung der Nutzer.

Einzelnen Firmen den Datenhandel zu untersagen ist wirklichkeitsfremd. Wie ein realistischer Datenschutz unter solchen Bedingungen aussieht, muss noch herausgefunden werden. Aber zum Glück ist zumindest der Fall WOT einfacher gelagert. Denn dort mangelte es offenbar nicht nur am Programmiergeschick, sondern auch am guten Willen. Denn wäre es dem Unternehmen – wie es in seiner Stellungnahme sagt – jemals ernst mit der Anonymisierung gewesen, hätte es kurzen Prozess mit den eingesammelten Daten gemacht, glaubt Wolfie Christl. Um ihren Zweck zu erfüllen, hätte die WOT-Erweiterung auch nur Domains statt der verräterischen URL-Stränge speichern können. Diese Daten hätten noch immer einen Wert auf dem Datenmarkt – aber wären erheblich weniger riskang für die User.

trend@chip.de

Anonymität ist eine Illusion

Latanya Sweeney, Datenschutzexpertin an der Harvard University

2009 zeigte IT-Expertin Latanya Sweeney, dass 87 Prozent der US-Bevölkerung allein anhand ihres Geburtsdatums, Geschlechts und ihrer Postleitzahl eindeutig identifizierbar sind. Dieses Prinzip nutzen heute viele Datenfirmen, um über User anonyme, aber trotzdem **eindeutig zuschreibbare Nutzerprofile** zu erstellen. Es gibt allerdings Methoden, einzelne Daten mit geringerem Risiko für die Privatsphäre aus so einem Profil zu extrahieren. So wurde das Konzept der **Differenziellen Privatsphäre** (differential privacy) entwickelt. Demnach kann Anonymität zum Beispiel nicht ausschließlich durch Weglassen von Informationen, sondern eher durch Hinzufügen von Datenrauschen oder der Manipulation von Datenpunkten erreicht werden. Doch solche Methoden sind gesetzlich nicht vorgeschrieben. Für Datenschutzexperten muss deshalb eine neue Regelung her: Nicht die ordentliche Anonymisierung sollte Pflicht werden, sondern die **unfreiwillige De-Anonymisierung** bestraft werden.

Networks of Control

Wolfie Christl, Sarah Spiekermann: Networks of Control, erschienen 2016

Kostenloser Download **http://crackedlabs.org/en/networksofcontrol**
Die gedruckte Version ist bei Facultas erschienen **http://facultas.at/2016/networksofcontrol**