Selbstschutz der Online-Privatsphäre

Kaum eine Woche vergeht, in der nicht weitere Entdeckungen aus den Snowden-Papieren in der Presse erscheinen. Kann man überhaupt seine Privatsphäre noch schützen? Wie kann man noch mit Kollegen halbwegs sicher kommunizieren? Eine besonders heimtückische Komponente ergibt sich aus der Datensammelwut der kommerziellen Dienste und dem Zugang zu diesen Daten für Behörden, oft ohne richterliche Anordnung oder jedwede Kontrolle. Vorsichtsmaßnahmen sind daher angebracht, um das Anwachsen persönlicher Daten zu verringern und einen persönlichen Schutz vor vollkommener Transparenz und Überwachung zu entwickeln.

Eine gute Übersicht zur Datenüberwachung sowie Gefahren und Abwehrmöglichkeiten bietet www.selbstdatenschutz.info/datenschutzprobleme

Polizei und BSI haben einen Kompass zur sicheren Internetnutzung erstellt. Dieser kann jedoch nur als absolute Basis verstanden werden. www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Kompass_zur_sicheren_Internetnutzung_26092013.html

Spuren reduzieren – Datenvermeidung

Der beste Schutz ist und war schon immer die Datenvermeidung. Daten, die nicht entstehen, können auch nicht gespeichert werden. Das beginnt bei der extrem zurückhaltenden Weitergabe des eigenen Namens und der E-Mail-Adresse und weiterer Angaben.

Für viele Dienste und Registrierungen kann sowohl ein Pseudonym als auch eine Einmal-E-Mail-Adresse verwendet werden. Für die eigene Mail sollte man sich eine eigene Domain bei einem deutschen Anbieter wert sein (mail@meinname.de). Kostenlose Anbieter leben vom Verkauf von Profilen, Werbung und anderen Geschäften. Einmal-E-Mail-Adressen gibt es bei:

- www.mailinator.com
- www.10minutemail.com/10MinuteMail/index.html
- www.trash-mail.com
- www.emailgo.de
- www.schafmail.de
- www.sofort-mail.de

Google und wahrscheinlich auch andere Suchmaschinen speichern jede Anfrage mit Zeitstempel und einer Art Fingerabdruck, der aus ca. 50(!) Parametern wie IP-Adresse, Betriebssystemversion, Browserversion, Schriften usw. erstellt wird. Damit ist fast jeder eindeutig gekennzeichnet. Spätestens beim Log-in in einen der Dienste des Google-Imperiums wird daraus auch eine persönliche Identifizierung.

Eine ausführlich Erläuterung zum Thema findet sich hier: https://panopticlick.eff.org/browser-uniqueness.pdf

Daraus folgt, dass man zumindest verschiedene Suchmaschinen abwechselnd verwenden sollte. Neben Google sind das vor allem:

- www.bing.com und
- www.yahoo.com

Eine weitgehende Anonymisierung verspricht dabei www.duckduckgo.com durch Nichtweitergabe der oben erwähnten Parameter.

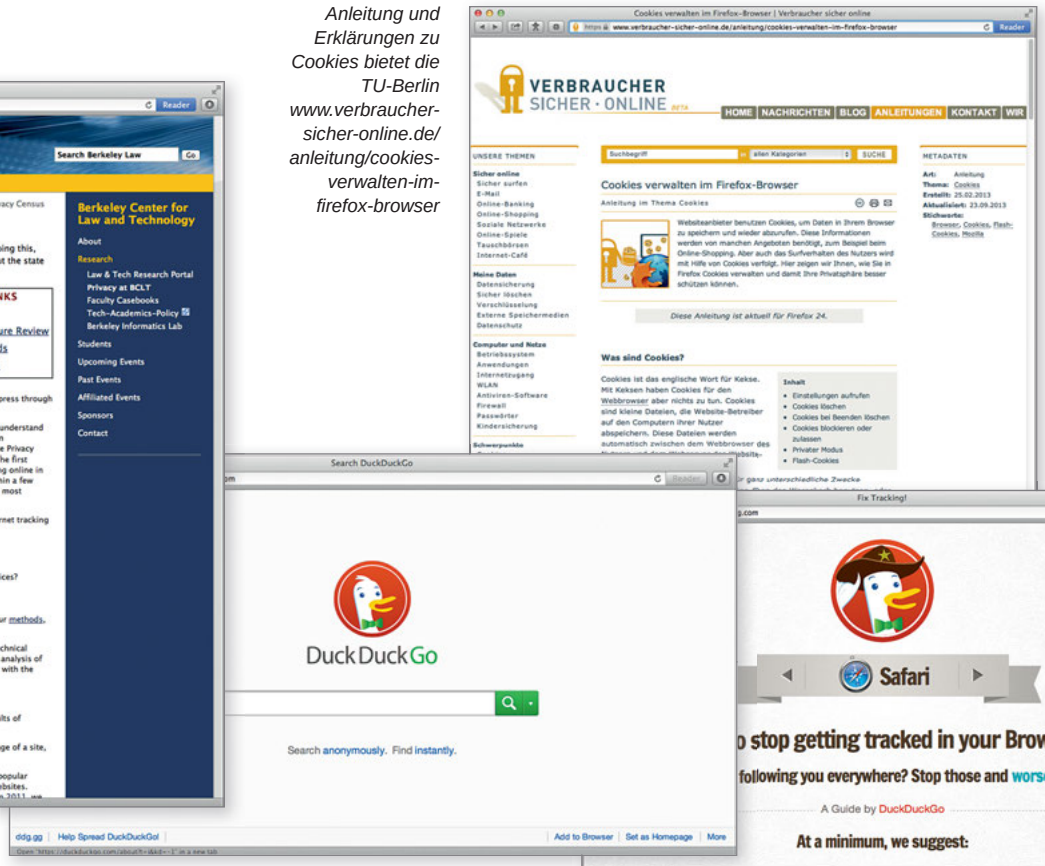
Browserpflege und Datenkekse

Fast alle Webseiten hinterlegen sogenannte Cookies auf dem Rechner des Nutzers. Das sind kleine Dateien, die eine spätere Identifizierung des Nutzers ermöglichen und oft auch die besuchten Bereiche oder Einstellungen sichern. Regelmäßiges, am besten tägliches Löschen dieser Cookies reduziert die Identifizierbarkeit. Die Optionen dazu finden sich in den Einstellungen des jeweiligen Browsers.

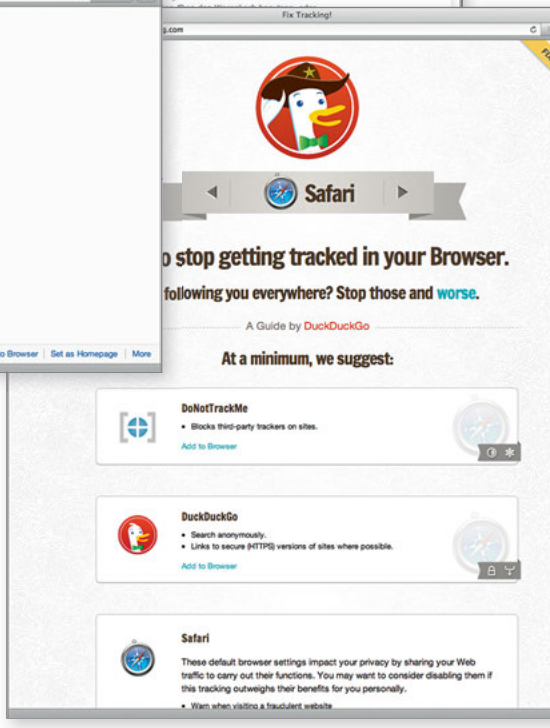
Die neue Technik HTML5 bringt noch eine weitere Kategorie ins Spiel, sogenannter local storage

Die Universität Berkeley erstellt eine detaillierte Untersuchung zum Stand der Online-Privatspäre: www.law.berkeley.edu/privacy census.htm

Anleitung und Erklärungen zu Cookies bietet die TU-Berlin www.verbraucher-sicher-online.de/anleitung/cookies-verwalten-im-firefox-browser



www.duckduckgo.com verspricht Anonymisierung der Suche ohne Weitergabe von Nutzerdaten.



Sammlung von Tools, um Nachverfolgung zu vermeiden: www.fixtracking.com

oder Super Cookies. Eine Suche nach „Super Cookies entfernen" plus dem jeweiligen Browsernamen ergibt zahlreiche Anleitungen dazu.

Missbraucht werden oft Dateien, die der Flash Player ablegt. Mindestens lässt man nachfragen, bevor etwas abgelegt wird. www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager.html

Auch E-Mail birgt viele Risiken: www.sueddeutsche.de/digital/e-mail-ueberwachung-im-alltag-sehr-uebles-verhalten-1.1793066

Passwörter, aber sicher

Die Methoden, Passwörter zu kapern, werden immer ausgefeilter. Neben Wörterbüchern werden zunehmend Muster verwendet, die aus gestohlenen Passwortlisten erzeugt werden.

Als einen Lösungsansatz sei hier das *c't-Magazin* zitiert: „Das System beruht darauf, sich einmalig ein kompliziertes Grundpasswort auszudenken und es mit einem seitenabhängigen Dienstteil zu verknüpfen. Den Dienstteil können Sie zum Beispiel aus dem ersten und den letzten Buchstaben des Domainnamens ohne Endung sowie dessen Länge erzeugen. Aus dem einmalig gelernten Grundpasswort „:xT9:qWBz+0" wird beim Google-Account etwa „ge6:xT9:qW-Bz+0" und bei eBay „ey4:xT9:qW-Bz+0" [*c't* 2011, Heft 2, R. Eikenberg: „Sesam, öffne dich nicht", Seite 152 ff.].

Zu beachten ist, dass man Seiten von kleinen Anbietern, die wahrscheinlich kaum geschützt sind, dann doch mit einem anderen Passwort nutzt, um das Muster nicht leichtfertig preiszugeben.

Der Browser bietet an, verwendete Passwörter zu sichern. Diese werden jedoch kaum geschützt am Rechner abgelegt, weshalb von der Verwendung dieser Funktion abzuraten ist.

Weitere Schritte sind das Abschalten des Netzzugangs, also den DSL-Router per Steckdosenleiste über Nacht und am Wochenende abzuschalten, um die Angriffsfläche und Kontrollierbarkeit zu reduzieren. Regelmäßig aktualisierte Virensoftware zu haben, sollte eine Selbstverständlichkeit sein.

Die fast unübersehbare Anzahl von Gefahren bei der Internetnutzung sollte einen dazu veranlassen, Schritt für Schritt die eigenen Nutzungsgewohnheiten zu überprüfen und mögliche Risiken zu reduzieren.

Diesen und alle früheren Artikel finden Sie als PDF mit Links zum Anklicken auf www.blaek.de in der linken Spalte unter „Ärzteblatt".

Autor

Dr. Marc M. Batschkus, Arzt, Medizinische Informatik, Spezialist für eHealth, eLearning & Mac OS X, Steinstraße 40, 81667 München, E-Mail: mail@batschkus.de