Montag, 31. Juli 2017, 12:03 Uhr
~10 Minuten Lesezeit

Nichts bleibt verborgen

Der digitale Alltag der Menschen wird zum Produkt umprogrammiert.

von Christopher Kühn
Bildlizenz CC0

Schon seit der kommerziellen Einführung des Telefons wurden Bürger aller Herren Länder abgehört und ihre Gespräche aufgezeichnet. Die Basis dieser "Mithörerschaft" ist heute nicht anders als damals.

Lediglich das Gerüst, welches auf der immer fester zementierten Basis steht, wurde optimiert und hat mittlerweile so eine Unübersichtlichkeit in der gesamten IT-Branche hinterlassen, dass es heutzutage leider nicht mehr damit getan ist, irgendwelche Kabel umzustöpseln. Aber womit ist es dann getan?

Ich möchte mit diesem Artikel mehrere mögliche Antworten auf diese Frage aufzeigen, um ein wenig Licht ins Dunkel zu bringen und dafür zu sensibilisieren, wie viele Daten man ohne sein Einverständnis preisgibt, und was die vom Volksmund so genannte "Datensammelwut" anrichten kann, wenn man sich nicht dagegen wehrt.

Die Abhöraktionen, welche damals noch stark in den Kinderschuhen steckten, hatten die selbe Basis wie heute: Informationen sammeln und sie entweder für sich selbst, oder gegen andere nutzen. Dafür war jedes Mittel recht, um sich selbst einen Vorteil anderen gegenüber zu verschaffen. Wirtschaftsspionage ist schon seit Anbeginn der Industrialisierung kein überraschendes Phänomen mehr, viel mehr eine Last, mit der Unternehmen zu kämpfen haben, um sich vor selbiger zu schützen.

Mit dem Anbruch des Zeitalters der Digitalisierung wurde vielen Experten aus der Branche schnell klar, dass man hier so richtig aus dem Vollen schöpfen kann, und sie taten dies - nicht nur in der Wirtschaft oder zwischen Staaten, sondern nun auch bei den normalen Bürgern, die wohlgemerkt mit ihren Steuergeldern unfreiwillig Projekte unterstützen, die sich nicht nur gegen sie selbst richten, sondern deren Methoden auch dafür sorgen, dass sie sich beinahe persönlich gegen alle richten, die ein vermeintliches

Problem darstellen.

So ist es in den USA schon Alltag, dass sich Nachbarn gegenseitig mit Kameras, welche auf das Haus des jeweils anderen gerichtet sind, **ausspionieren** (https://youtu.be/NwNWDBVoZA4?t=5m25s). Aber als wäre das noch nicht genug, gibt es polizeiliche sowie private Einrichtungen, die mit der Erlaubnis des Kamerabesitzers eine direkte Verbindung zu diesen Kameras herstellen, um eine Straftat verfolgen zu können.

Diese Technologie basiert auf der, für mich wirklich interessanten und äußerst intelligenten, weil sehr clever bis ins Detail ausgeklügelten, Werbeindustrie. Sie hat es sich zur Aufgabe gemacht, Werbung tausendfach präziser als bisher zu verteilen. Ihre Methoden sind mittlerweile so raffiniert, dass selbst die Big-Data Konzerne heutzutage nicht mehr alle Zusammenhänge im Detail erklären können.

Diese Instrumentalisierung der Daten ist für uns normale Bürger aber leider alles andere als vorteilhaft, da sie tatsächlich nichts dazu beiträgt, uns das preisgünstigste Angebot aufzuzeigen, sondern das, was unserem Konsumentenverhalten entspricht. Wer eine Waschmaschine über sein iPad kauft, bekommt höhere Preise angezeigt als derjenige, der sie über seinen Windows-PC **bestellt** (http://www.chip.de/news/Fieser-Preistrick-bei-Amazon-Apple-Nutzer-zahlen-mehr-aus-Gruenden_84837549.html).

Auch ich bin Opfer einer solchen Marketingstrategie geworden: Für ein Hotelzimmer suchten meine Partnerin und ich, von jeweils unseren eigenen Smartphones, parallel nach dem besten Angebot. Wir nutzten zeitweise die gleichen Portale und bekamen auch dort die gleichen Zimmer vom selben Anbieter angeboten. Nur mussten wir feststellen, dass die Angebote auf dem iPhone meiner Partnerin wesentlich teurer waren als die auf meinem **Android-Smartphone** (https://www.heise.de/mac-and-i/meldung/Hotelportal-Mac-

Nutzer-schlafen-gern-teurer-1626368.html).

Auf meine telefonische Nachfrage, warum die Preise sich hier so stark unterschieden, konnte man mir seitens des Hotels selbstverständlich keine Auskunft geben.

Seit 2013 ist Edward Snowden für mich persönlich „die Kirsche auf der Sahne“. Seine Dokumenten-Leaks zeigen uns allen, dass es ernsthaft schädlich sein kann, wenn man sich auf proprietäre Systeme verlässt. Proprietäre Systeme, wie sie Apple mit iCloud und iOS, Google mit seiner Cloud und seiner Software nutzen, und wie Microsoft es mit Windows seit Jahren dreist **durchzieht** (https://privacytoolsio.github.io/privacytools.io/#win10), haben nämlich einen entscheidenden Nachteil: Sie geben keinerlei Informationen darüber preis, welche Daten zu welchem Zweck in welchem Umfang genutzt und weiter gegeben werden, und wie diese Weitergabe aussieht und genutzt wird. Die alternative Antwort hierauf: Unabhängigkeit durch Open Source Software.

Diese Datensammelwut ist mittlerweile so attraktiv geworden, dass die Firmen, die spezielle Datensammelsoftware entwickeln und verkaufen, an jeder noch so kleinen Ecke vorzufinden sind und natürlich nicht wollen, dass die Leute aufgeklärt werden oder sich dagegen wehren. Zumal diese Unternehmen nicht nur für Big-Data Konzerne arbeiten, sondern diese Software auch den “**14 Augen** (https://privacytoolsio.github.io/privacytools.io/#ukusa)” weltweit anbieten und dabei die Staaten unterstützen, ihre illegalen Aktivitäten weiter auszubreiten.

> ***Deswegen gilt eine Regel für jeden Internetnutzer: Sich selbst und andere vor Benachteiligung schützen!***

Um zu wissen, wie man sich am besten vor dieser Datensammelwut schützt, muss man sich grundsätzlich, mantra artig eine Frage stellen: „Wovor genau will ich mich schützen?“

Und genau darauf gibt es schier unendlich viele Antworten. Denn eines muss jedem Internetnutzer von Anfang an klar sein: Ein gezielter Angriff eines Hackers oder gar einer staatlichen Institution, ist letztlich nicht abwendbar. Kein System ist zu 100 Prozent sicher und unhackbar. Man kann es den Angreifern lediglich schwer machen.

Beschränken wir uns also auf das, was man gegen die allgemeine Datensammelwut tun kann. Denn diese basiert zum größten Teil auf Algorithmen, welche nicht von Menschen kontrolliert, sondern von anderen Computern ausgeführt werden. Und genau das kann man zu seinem Vorteil nutzen.

Sich selbst der Benachteiligung bei Einkäufen von diversen Gütern zu entziehen bedeutet - für den Laien erklärt -, diese Algorithmen “anzulügen”. Sogenannte Plug-Ins für diverse Browser sorgen dafür, dass Tracker, Werbung und das persönliche Profiling angelogen, ausgeblendet oder fehlgeleitet werden.

Nachfolgend eine Übersicht meiner persönlichen Plug-In-Liste für Firefox, mit kurzen Erklärungen:

CanvasBlocker
(https://addons.mozilla.org/de/firefox/addon/canvasblocker/)

Bei CanvasBlocker handelt es sich um ein Plug-In, um den persönlichen Fingerabdruck, welcher durch das **Canvas-Tracking-Verfahren** (https://de.wikipedia.org/wiki/Canvas_Fingerprinting) ermöglicht wird, zu verhindern, indem durch diverse JavaScript Anfragen eine Fehlinformation automatisiert zurück gesendet wird.

Cookie Controller
(https://addons.mozilla.org/de/firefox/addon/cookie-controller/)

Auch wenn Cookies heutzutage nicht mehr als wichtiges Tool zur Datensammlung genutzt werden, gibt es sie nach wie vor, um Seitenbesuche, die man vor und nach dem Besuch einer anderen Internetseite besucht hat, aufzuzeichnen. Einstelltipp: “Cookies denied”, solange es möglich ist.

Decentraleyes
(https://addons.mozilla.org/de/firefox/addon/decentraleyes/)

Eine Software, die vor allem in Kombination mit **uBlock Origin** (https://addons.mozilla.org/de/firefox/addon/ublock-origin/) (dazu gleich mehr) dafür sorgt, dass gewisse APIs* einfach nicht verwendet werden oder dass durch eine “Lüge” eine Abfrage des eigenen PCs verhindert wird. (*APIs sind, einfach erklärt, vorprogrammierte Datenpakete, die z. B. dafür sorgen, dass eine Schriftart einer Internetseite, welche man nicht auf seinem PC hat, trotzdem angezeigt werden kann. Google ist hier Vorreiter. Der Nachteil: Ein API hat beim Aufruf immer das Recht, den PC dahingehend zu untersuchen, ob diese Schriftart vorhanden ist.)

HTTPS Everywhere
(https://addons.mozilla.org/de/firefox/addon/https-everywhere/)

Jeder Aufruf einer Internetseite kann geschützt oder ungeschützt sein. Viele Internetseiten leiten ihre Besucher gerne auf eine ungeschützte Seite, was zur Folge hat, dass alle Informationen, die dort eingegeben werden (z. B. Für einen Online-Shop), völlig unverschlüsselt und somit ungesichert auf deren Server liegen. Um das zu verhindern, kann vor Aufruf jeder Internetseite eine verschlüsselte Verbindung erzwungen werden. Dies verhindert zwar nicht die Speicherung der Daten auf deren Server, aber es sorgt dafür, dass die Daten von niemandem ausgelesen und jemanden zugeordnet werden können, sollte dieser Server einmal gehackt **werden** (https://www.heise.de/newsticker/meldung/Angriff-auf-

Playstation-Network-Persoenliche-Daten-von-Millionen-Kunden-gestohlen-1233136.html).

No Resource URI Leak
(https://addons.mozilla.org/de/firefox/addon/no-resource-uri-leak/)

Selbst wenn keine Internetseite aufgerufen wird, erfasst jeder Browser, selbst, Informationen (Einstellungen, installierte Add-Ons, Passwordmanager usw.). Da kein System zu 100 Prozent sicher ist, ist es immer wieder vorgekommen, dass "interne URL's" zum Profiling genutzt wurden. Um zu verhindern, dass z. B. Mozilla vom Anwender erfährt, welche Add-Ons er nutzt, oder dass ein Hacker dies einsehen kann, wird hier jeglicher "Offline-Verkehr" deaktiviert.

NoScript
(https://addons.mozilla.org/de/firefox/addon/noscript/)

Dieses Add-On empfehle ich ausschließlich für erfahrene Anwender. NoScript deaktiviert standardmäßig die sicherheitskritischsten Scripte von Internetseiten, welche dazu dienen können, ein detailliertes Profil des Besuchers zu erstellen. Leider zerstört dies den Großteil der Internetseiten, da die meisten ohne Script nicht korrekt, oder gar nicht angezeigt werden können. Gute Kenntnisse über die Einstellmöglichkeiten sind deshalb Pflicht.

Privacy Settings
(https://addons.mozilla.org/de/firefox/addon/privacy-settings/)

Dieses Programm verhindert, Daten an Mozilla zu senden, die unter anderem den Akkustand des Laptops erfassen. Diese sind nicht nur unnötig, sondern ihre Menge ist auch so klein, dass man nur wenig Fantasie braucht, um sich vorzustellen, das selbst (vermeintlich) belangloseste Informationen weitergegeben werden. Natürlich könnte man sagen, dass diese Informationen nicht wichtig sind.

Aber es ist nicht die einzelne Information an sich, die wichtig ist, sondern das gesamte Bild, welches dadurch zusammengetragen wird und entsteht. Dieses Add-On sorgt dafür, die Privatsphäre von Firefox um ein Vielfaches zu verbessern, und verhindert die Weitergabe von so ziemlich allem, was ein Browser theoretisch aufzeichnen könnte. Einstelltipp: “Full Privacy” aktivieren.

Self-Destructing Cookies
(https://addons.mozilla.org/de/firefox/addon/self-destructing-cookies/)

Auch wenn wir schon “Cookie Controller” nutzen, kommen wir stellenweise nicht darum herum, den ein oder anderen Cookie, zwecks Funktionalität der Internetseite zu erlauben. Damit dieser aber keinen bleibenden Eindruck vom Surfverhalten erhält, muss der Cookie umgehend gelöscht werden. Um dies nicht händisch machen zu müssen, kann man diesem Plug-In eine sekundengenaue Zeitangabe vorgeben, wie lange Cookies behalten werden dürfen, um sie danach automatisch zu löschen. Einstelltipp: 2 Sekunden.

uBlock Origin
(https://addons.mozilla.org/de/firefox/addon/ublock-origin/)

Mein persönliches Lieblings-Plug-In. Es blockiert nicht nur perfekt jegliche Werbung (selbst bei YouTube und Co.), sondern kümmert sich auch darum, “unsichtbare Bilder” zu “belügen”. Diese Bilder findet man in eMails und auf Internetseiten, sind nur 1x1 Pixel groß und beinhalten immer einen Code, der nichts anderes macht, als herauszufinden, wer dieser Empfänger oder Besucher ist, und der dies so tief ins System eingräbt, dass diese Information selbst beim Löschen der gesamten Browseraktivitäten noch vorhanden bleibt. Des Weiteren ist uBlock Origin sehr ressourcenschonend, was dieses Plug-In auch auf älteren PCs einsatzfähig macht. Einstelltipp: **hier** (https://www.kuketz-blog.de/ublock-origin-schutz-gegen-

tracker-und-werbung/).

Dass ich Firefox nutze, liegt daran, dass die Mozilla-Foundation bisher noch die vertrauenswürdigste, Softwarefirma ist, die dafür bekannt ist, einen privatsphärenfreundlichen Browser anzubieten, auch, wenn dies nicht mehr uneingeschränkt gilt. Außerdem sind die Anbieter nach Kenntnisnahme von Sicherheitslücken sehr schnell darin, diese mit einem Update zu schließen.

> ***Unternehmen wie Google Inc. (Google Chrome), Opera Software (Opera Browser) oder Microsoft (Internet Explorer – mittlerweile Edge) verdienen ihren Löwenanteil durch den Verkauf von Nutzerdaten.***

Oder warum ist es mittlerweile gang und gäbe, neue Softwareversionen kostenlos herauszugeben, während sie vor 10 oder mehr Jahren noch zwischen 200 und 1.000 Euro gekostet haben? Genau aus einem Grund: Der Konsument wurde mit seinen Daten zum Produkt umprogrammiert. Wenn die großen Konzerne also mit "sicher und schnell" werben, meinen sie nicht, dass die Daten des Users sicher vor Spionage sind, sondern dass es mit ihrem Browser sicherer ist, auf, zum Beispiel, Amazon einzukaufen, ohne durch jeden noch so kleinen Hackerangriff betrogen werden zu können.

Selbstverständlich gibt es eine wesentlich größere Auswahl an Plug-Ins und Methoden. Allerdings ist die Kombination von einigen Plug-Ins kontraproduktiv, da sie sich möglicherweise gegenseitig blocken können und somit keinerlei Effekt mehr erzielen. Ein zusätzliches Problem, vor dem Datenschützer stehen, ist die Tatsache, dass viele Plug-Ins, welche mit "hoher Sicherheit" und "absoluter Privatsphäre" werben, nur von anderen Herstellern bezahlt werden. Somit kann es im Fall von, zum Beispiel, "Ghostery" passieren, dass die gesammelten Daten über den Internetverlauf eines Users weiter **verkauft werden** (https://www.heise.de/tr/artikel/Die-Geister-

die-ich-rief-1890700.html) trotz des Versprechens, genau dies zu verhindern.

Aber man muss sich immer die Frage stellen: Wenn man nichts zu verbergen hat und die Informationen von sich aus weitergibt, weil man es okay findet, wieso ist es dann für den Staat bzw. die Big-Data Konzerne so unglaublich wichtig, jedes noch so kleine Detail über jeden Einzelnen zu erfahren? Bestimmt nicht, damit der Bespitzelte zum Geburtstag das optimale Geschenk von „Herrn Google“ persönlich überreicht bekommt.

Natürlich beschreibt dieser Artikel, nur die Spitze des Eisbergs „Datensammlung“. Aber einen kompletten Guide zur Frage “Wie bewege ich mich anonym im Internet?” zu erstellen, sprengt den Rahmen dieses Textes.

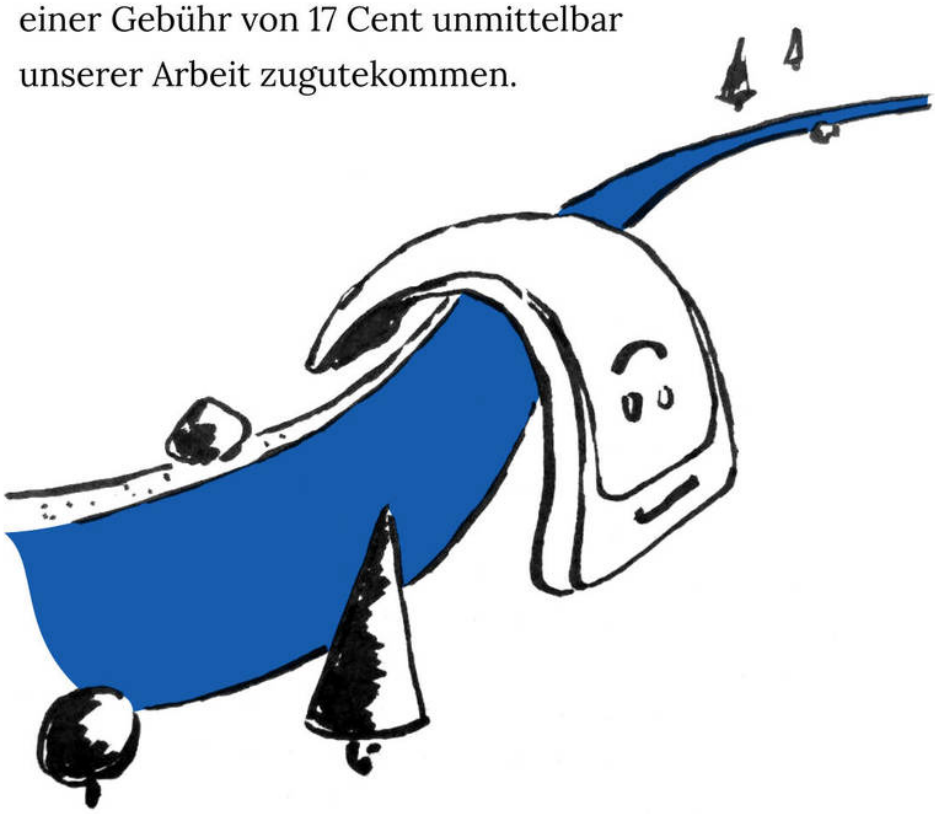
Vor allem zur nur kurz erwähnten OpenSource-Software Alternative ließe sich mindestens ein weiterer Artikel verfassen. Die Resonanz der Leser entscheidet über eine mögliche Serie auf Rubikon, die das Thema Datenschutz detailliert durchleuchten wird.

> ***Das Wichtigste ist: Das beste Plug-In im Browser nützt nichts, wenn der User der davor sitzt von sich aus - bewusst oder unbewusst - alle Daten über sich veröffentlicht. Benutzernamen wie “H_Müller_72” sind wirklich alles andere als sinnvoll, um seine Privatsphäre zu schützen. Vorsicht ist immer besser als Nachsicht. Leichtsinnigkeit gereicht letztlich nur den Leichtsinnigen zum Nachteil.***

Viel Spaß beim Surfen!

Hat Ihnen dieser Artikel gefallen?

Dann unterstützen Sie unsere Arbeit auf die denkbar schnellste und einfachste Art: per SMS. Senden Sie einfach eine SMS mit dem Stichwort **Rubikon5** oder **Rubikon10** an die **81190** und mit Ihrer nächsten Handyrechnung werden Ihnen 5,- bzw. 10,- Euro in Rechnung gestellt, die abzüglich einer Gebühr von 17 Cent unmittelbar unserer Arbeit zugutekommen.



Dieser Artikel erschien bereits auf www.rubikon.news.

Christopher Kühn trifft als Fotograf auf die

unterschiedlichsten Charaktere, dessen Persönlichkeit er durch Gespräche in den Vordergrund stellen kann. Durch seine Arbeit, aber auch aus privatem Interesse ist der Umgang mit digitalem Content somit sein tägliches Brot. Er empfindet Privatsphäre als eines der höchsten Rechte des Menschen, sodass er nicht nur die Fotos seiner Kunden vertrauensvoll behandelt, sondern sich auch bei freien Projekten zum Thema Datenschutz engagiert.

Dieses Werk ist unter einer **Creative Commons-Lizenz** (**Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de)) lizenziert. Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.