So geht digitale Selbstverteidigung

So geht digitale Selbstverteidigung

Wir sind allzu neugierigen Einblicken im Internet nicht schutzlos ausgeliefert. Eine Anleitung, um wenigstens ein Minimum an digitaler Selbstbestimmung und Datenkontrolle zu erlangen.

von Andreas Geppert

Die «digitale Selbstverteidigung» bezeichnet Massnahmen zum Schutz der persönlichen Privatsphäre und der persönlichen Daten. Warum ist das überhaupt notwendig? Firmen sammeln Ihre Daten, integrieren sie mit solchen aus anderen Quellen, bilden Profile und verwenden sie für personalisierte Werbung, politisches Targeting, Kreditwürdigkeitsbeurteilungen und andere computerisierte Entscheidungen. Aus der Gesamtheit der Daten lassen sich weitere Eigenschaften ableiten oder vorhersagen, die oft sensitive Aspekte einer Person wie etwa die sexuelle Orientierung betreffen. Daten gehen häufig verloren oder werden gestohlen und werden dann von Kriminellen zum Beispiel für Identitätsdiebstahl verwendet. Wie der Datenmissbrauch von Personendaten durch rechtsextreme Polizeibeamte (NSU 2.0) in Deutschland gezeigt hat, sind staatliche Datensammlungen dabei nicht unbedingt sicherer. Und wie Whistleblower Edward Snowden aufgezeigt hat, sammeln selbst Staaten wie die USA Daten auf Vorrat in einem Ausmass, das weit über das verhältnismässige Reagieren auf einen konkreten Verdachtsfall hinausgeht.

Sind Sie mit dem Sammeln Ihrer Daten nicht einverstanden, müssen Sie zur Selbsthilfe schreiten. Mit Hilfe dieses Artikels können Sie den ersten Schritt der digitalen Selbstverteidigung unternehmen. Setzen Sie die Tips um, werden Sie noch nicht zum Grossmeister der Privatsphäre und Datenkontrolle mit schwarzem Gürtel. Aber zum gelben oder orangenen könnte es reichen.

Überwachung der Überwacher

Hinsichtlich des Datensammelns sind Betriebssystemhersteller wie Microsoft (Windows) oder Google (Android) im Vorteil, da das Betriebssystem nicht nur Zugriff auf alle Daten hat, sondern generell eine Black Box ist: Das Datensammeln[1] kann von ausserhalb nicht einfach unterbunden werden, zumindest nicht mit einem gelben Gürtel. Alle anderen Datensammler müssen sich Daten anderweitig besorgen. Zusätzlich zu den Daten, die im Rahmen der Dienstleistung anfallen und benötigt werden (zum Beispiel Likes in sozialen Medien), sind hier besonders Cookies und Tracker zu nennen. Das sind kleine Dateien auf Ihrem Computer beziehungsweise Softwarebausteine in Webseiten und Apps, die Sie identifizieren und Datensammlern helfen, Sie im Internet und auf dem Smartphone zu überwachen.

Wenn Sie wissen, wer Sie wie stark überwacht, können Sie sich besser gegen Überwachung wehren. Vollständige Transparenz ist hier nicht möglich, aber es gibt eine breite Palette von Möglichkeiten: **Privacy Badger**[2], eine Browser-Erweiterung für den Firefox-Browser, zeigt an, welche Tracker sich auf einer Webseite befinden. **Blacklight**[3] analysiert die Seite hinter der Adresse (URL) und zeigt an, wie viele Tracker, Third-Party-Cookies etc. sich auf der Seite befinden. **Exodus**[4] gibt für andere Apps und Webseiten an, wie viele und welche Tracker diese enthalten. Mit diesen Informationen können Sie sich ein recht genaues Bild verschaffen, welche Apps oder Webseiten Sie wie stark überwachen.

Datenauskunftsbegehren sind schliesslich ein probates Mittel, um sich einen Überblick zu verschaffen, wie viele Daten Migros, Coop, Swisscom oder die SBB über einen gesammelt haben. Gemäss Schweizer Datenschutzgesetz müssen Firmen Auskunft geben, welche Personendaten sie besitzen. Die Verweigerung der Auskunft muss begründet werden und kann angefochten werden. Vorlagen für Datenauskunftsbegehren findet man beim Eidgenössischen Datenschutzbeauftragten oder bei der Digitalen Gesellschaft.

Alternative Apps und Webseiten

Ein gewisser Teil der Daten fällt zwangsläufig im Rahmen des Nutzens einer Dienstleistung an. Stellen Sie eine Suchanfrage, müssen Sie der Suchmaschine mitteilen, wonach Sie suchen. Soll die Suchmaschine Ihre Ergebnisse personalisieren, dann muss sie sich Ihre Identität (also z.B. die IP-Adresse) merken. Wollen Sie ein Buch bei einem Online-Händler bestellen, müssen Sie dem Händler natürlich sagen, welches Buch Sie wollen und wohin es gesendet werden soll. Aus diesen Daten können die Firmen weitere Informationen ableiten und Ihnen zur Verfügung stellen, was durchaus praktisch sein kann (beispielsweise Bücher, die Sie auch noch interessieren könnten). Wollen Sie diese Datensammlung verhindern, können Sie auf alternative Apps ausweichen.

Die grossen Tech-Firmen (auch bekannt als GAFAM – Google, Amazon, Facebook, Apple, Microsoft) verfügen alle in einem oder mehreren Bereichen über monopolartige Marktanteile[5]. Google und Facebook sind eigentlich Online-Werbeunternehmen, die mit personalisierter Werbung sehr viel Geld verdienen. Wenn Sie Ihre

Daten dieser Werbemaschinerie nicht überlassen wollen, können Sie diese Alternativen verwenden:

- **DuckDuckGo** oder **StartPage** als Suchmaschinen. Während DuckDuckGo eine eigenständige Suchmaschine ist, verwendet StartPage zwar den Index von Google, liefert jedoch keine Nutzerdaten an Google. Die Suchergebnisse wie auch die ausgespielte Werbung sind bei beiden nicht personalisiert.
- **Firefox**, **Brave** oder **Tor** als Browser. Firefox und (insbesondere) Brave sind mit besonderem Fokus auf Datenschutz entwickelt worden. Bei Tor wird die Verbindung zu einer Webseite über drei zufällig bestimmte Server des Tor-Netzwerkes aufgebaut; Tor ist somit noch etwas privater als die anderen beiden, allerdings auch langsamer.
- **Thunderbird** (Desktop) oder **K-9** (Android) als E-Mail-Clients. Thunderbird wird wie Firefox von der Mozilla Foundation entwickelt. Für Thunderbird gibt es Erweiterungen, mit denen E-Mails verschlüsselt werden können, so dass die Vertraulichkeit von Nachrichten sichergestellt werden kann, auch gegenüber dem E-Mail-Betreiber. K-9 ist eine E-Mail-App für Android, mit der ebenfalls verschlüsselt werden kann.
- Auf **OpenstreetMap** basierende Apps (z.B. **OsmAnd~**) als Karten-App und zur Navigation.
- In breiten Bevölkerungsschichten ist die frühere SMS abgelöst worden durch Messenger wie **WhatsApp**. **Signal** und **Threema** sind Alternativen dazu, denn die Kommunikation über diese Plattformen ist Ende-zu-Ende-verschlüsselt. WhatsApp verschlüsselt inzwischen zwar auch. Jedoch landen die Metadaten (wer kommuniziert mit wem wie lange und wie oft) und das Adressbuch bei **Facebook**, der Inhaberin von WhatsApp.

Alternative Betriebssysteme und Browser-Erweiterungen

Bei den alternativen Betriebssystemen sind insbesondere Google-freie Android-Versionen zu nennen (z.B. **Fairphone Open** für das Fairphone 2 oder **/e/-OS** für das Fairphone 3). In diesen Betriebssystemen gibt es keine Google-Apps. Als Alternativen für den Play Store können **Aurora** oder **F-Droid** genannt werden. Da der Google Play Store fehlt, lassen sich auch keine weiteren Google-Apps wie Suche, Maps oder Gmail installieren. Die naheliegende Alternative zu Windows im Desktopbereich ist natürlich **Linux**. Eine Gruppe von Studierenden in Zürich hat sich die Verbreitung dieses Open-Source-Betriebssystems zum Ziel gesetzt und **The Alternative**[6] entwickelt.

Tracker (insbesondere Third-Party-Cookies) dienen Ihrer Nachverfolgung im Internet (und allenfalls der Übertragung weiterer Personendaten). Während der Brave-Browser Abwehrmechanismen bereits eingebaut hat, gibt es für Firefox und andere Browser Erweiterungen (Add-Ons), mit deren Hilfe Tracker blockiert werden können. **uBlockOrigin** und der oben bereits erwähnte Privacy Badger sind solche Erweiterungen.

Android- und iOS-Smartphones ermöglichen es, Berechtigungen einzeln zu vergeben. Von dieser Möglichkeit, Berechtigungen

bewusst, selektiv und restriktiv zu vergeben, sollten Sie auf jeden Fall Gebrauch machen. Eine Taschenlampen-App zum Beispiel braucht für ihre korrekte Funktionsweise definitiv keinen Zugriff auf Ihre Kontakte!

Logins, Untertauchen, solidarischer Datenschutz

Viele Webseiten und Apps bieten die Möglichkeit, sich mit dem Facebook- oder Google-Account anzumelden. Wird die Authentisierung an Google oder Facebook delegiert, erfahren diese Firmen dann natürlich auch, wann Sie sich auf welcher Webseite oder App angemeldet haben. Ein Mosaikstein mehr für die Profilbildung! Es empfiehlt sich, für unterschiedliche Apps und Webseiten auch unterschiedliche und schwer zu erratende Passwörter zu verwenden. Da sich niemand mehrere solche Passwörter merken kann, empfiehlt sich der Einsatz eines Passwort-Managers wie **KeePass**. Ein solcher Passwort-Manager ist wie ein Safe, in dem Sie Ihre Passwörter sicher aufbewahren können und der Ihnen zusätzlich auch das Generieren starker Passwörter abnehmen kann. Den Passwort-Manager sichern Sie mit einem Master-Password, das dann allerdings stark (lang und schwer zu erraten) sein sollte.

Viele Datenstaubsauger identifizieren Sie anhand Ihrer IP-Adresse. Sie können diese jedoch verbergen, wenn Sie ein **Virtual Private Network (VPN)** verwenden, denn dann sind Sie mit der IP-Adresse des VPN-Anbieters unterwegs. Bei der Auswahl des VPN-Providers sollten Sie Gratisangebote meiden und darauf achten, dass der Anbieter keine Protokolle (Logs) speichert. Typische Angebote erlauben die Nutzung auf mehreren Geräten, so dass Sie das VPN für den Desktop zu Hause wie auch für das Smartphone nutzen können.

Gesichtsmasken und digitale Selbstverteidigung haben gemeinsam, dass sie Mitmenschen mindestens genauso schützen wie einen selbst. Denken Sie also auch an die Privatsphäre Ihrer Kontakte und Mitmenschen. Gewähren Sie WhatsApp oder einer anderen App Zugriff auf Ihre Kontakte, geben Sie damit persönliche Daten dieser Personen preis. Laden Sie Bilder auf soziale Medien hoch, auf denen andere Personen zu sehen sind, müssten Sie diese um Erlaubnis fragen. In diesem Fall kommt dazu, dass mit Systemen wie **ClearView** und **PrimEyes** Möglichkeiten der Rückwärtssuche existieren; die Identität kann so ausgehend von einem Foto bestimmt werden.

Und die staatliche Überwachung?

Dank Edward Snowden wissen wir, wie eng kommerzielle und staatliche Überwachung zusammenhängen. Seither hat sich diese Zusammenarbeit weiter intensiviert[7]. Alles, was Sie gegen kommerzielle Überwachung tun, hilft so potentiell auch gegen staatliche Überwachung: Suchanfragen, IP-Adressen und andere Daten, die eine Firma gar nicht erst erhält, kann sie auch nicht an staatliche Behörden weitergeben. Gegen einige Formen der staatlichen Überwachung wie etwa Vorratsdatenspeicherung oder Gesichtserkennung ist die digitale Selbstverteidigung machtlos. Diese Überwachungsarten stellen massive Eingriffe in unsere Grundrechte dar und sollten deshalb rechtlich und politisch bekämpft werden.

Jeder und jede kann sich praktisch in der digitalen Selbstverteidigung üben. Im Kern aber ist es eine Reaktion auf Missstände wie ausufernde staatliche Überwachung, unzureichend durchgesetzten Datenschutz und fehlende Regulierung von Internetfirmen. Deswegen möchte ich Sie zum Schluss ermutigen, das eine – die digitale Selbstverteidigung – zu tun und das andere – das netzpolitische Engagement – nicht zu unterlassen. Informieren Sie sich über netzpolitische Themen wie Überwachungsgesetze, elektronische Identität, das neue Datenschutzgesetz und engagieren Sie sich in der Diskussion dieser Themen! ‹

«Eine Taschenlampen-App braucht für ihre korrekte Funktionsweise definitiv keinen Zugriff auf Ihre Kontakte.»

Andreas Geppert

[1] digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/
[2] privacybadger.org/
[3] themarkup.org/blacklight/
[4] exodus-privacy.eu.org/en/
[5] zeit.de/2020/43/us-techkonzerne-google-apple-amazon-facebook-wettbewerbsverzerrung
[6] thealternative.ch/
[7] netzpolitik.org/2020/ermittlungen-in-den-usa-polizei-erhaelt-liste-aller-nutzer-die-nach-einem-schlagwort-gegoogelt-haben/

Andreas Geppert
ist promovierter Informatiker und arbeitet heute als Datenplattformarchitekt. Als Präsident der Fachgruppe Informatik und Gesellschaft der Schweizer Informatik-Gesellschaft (SI) sowie Mitglied der Digitalen Gesellschaft beschäftigt er sich mit gesellschaftlichen Aspekten der Digitalisierung.