WIE SCHÜTZE ICH MEINE PRIVATSPHÄRE?

Ein Plädoyer für digitale Hygiene

Die Macht von Algorithmen, oder warum es ein Irrtum ist zu glauben, die eigenen Daten seien uninteressant und enthielten kein Indiz für gefährliches Verhalten.

VON PHILIPPE WAMPFLER

«Daten, von denen wir nicht wussten, dass es sie gibt, finden Wege, die nicht vorgesehen waren, und sagen aus, worauf wir nie gekommen wären.»

Michael Seemann, Twitter, 13. November 2013

Im frühen 20. Jahrhundert war Typhus ein Problem armer Leute. Deshalb erstaunte es viele, als 1906 in Long Island sechs Menschen im Haus von Charles Warren daran erkrankten, war Warren doch ein reicher Bankier. Ein mit der Aufklärung des Falls betrauter Hygienespezialist verdächtigte schnell die Köchin, Mary Mallon, die kurz vor dem Ausbruch der Krankheit den Haushalt plötzlich verlassen hatte. Nachforschungen ergaben, dass in den Häusern, in denen Mallon gearbeitet hatte, während eines Jahrzehnts Typhusansteckungen aufgetreten waren. Mallon war Trägerin von Bakterien, die die Krankheit auslösten, bei ihr selbst aber kaum Symptome hervorriefen (zudem wusch sie die Hände nicht). Auch nach einer dreijährigen Zwangsquarantäne war die Köchin davon überzeugt, absolut gesund zu sein, und kochte – trotz eines entsprechenden Verbots – unter falschem Namen unter anderem im Sloane-Krankenhaus in New York, wo sich 25 Personen mit Typhus ansteckten, zwei starben daran.

Das Verhalten der Typhus-Mary, wie Mallon genannt wurde, erscheint uns heute erstaunlich, gar kriminell. Und doch verhalten wir uns ganz ähnlich: im Internet. Wie all den von Mallon bekochten Familien ihre hohen Hygienestandards keinen Schutz boten, ist Datensicherheit so lange nutzlos, wie sich nicht alle, die mit den Daten in Kontakt kommen, die virtuellen Hände waschen.

Was die Sicherheit bedroht

Während es für Hygiene in biologischer Hinsicht bewährte und einfache Verfahren gibt, ist es in Bezug auf Datenströme zunächst nicht klar, was dem Händewaschen entsprechen würde und wovor es uns schützen sollte.

Datenschutz und Datensicherheit sind wie Privatsphäre Schlagworte, denen wir täglich begegnen, die wir aber stets so verwenden, dass verschiedene Ebenen und Problemlagen vermischt werden. Juristische, soziologische, politische und philosophische Fragestellungen schwingen mit. Um zu wissen, was wir alle tun können, um die Sicherheit unserer Daten zu gewährleisten – und derjenigen anderer, mit denen wir zu tun haben –, müssen wir uns zunächst darüber Gedanken machen, was diese Sicherheit denn bedrohen könnte.

Erstens kommen Mitmenschen, die wir kennen, infrage. Privatsphäre und Datensicherheit bedeuten oft, dass Nachbarinnen nicht in unser Schlafzimmer blicken, Familienangehörige unsere Geheimnisse nicht aufdecken und Mitarbeiter unser Privatleben nicht beurteilen können. Zweitens sind es Kriminelle, vor denen wir uns fürchten: Diebinnen, die unsere PIN-Codes kennen und auf unser Konto zugreifen können, Einbrecher, die Kopien unserer Schlüssel anfertigen, und HackerInnen, die Zugriff auf unser E-Banking oder unsere Onlineidentität erhalten. Drittens bedrohen Staaten unsere Freiheit, indem sie unter dem Vorwand der Sicherheit immer mehr Menschen ohne gesetzliche Grundlage insgeheim überwachen, obwohl sich diese nichts haben zuschulden kommen lassen. Und viertens agieren Unternehmen ganz ähnlich wie Staaten, aber aus anderen Motiven: Sie rechnen damit, gesammelte Informationen verkaufen zu können. Staaten und Unternehmen beabsichtigen fünftens, aus Datenbanken Prognosen für zukünftige Entwicklungen und Verhaltensweisen abzuleiten. Big Data, wie man dieses Vorgehen nennt, wird Individuen mit vielen Vorteilen angepriesen – etwa in Form von Treueprogrammen –, führt aber letztlich dazu, dass Menschen aufgrund ihrer Datenspuren eingestuft und entsprechend als Risiko oder als Profitquelle behandelt werden.

Der Internetskeptiker Evgeny Morozov weist immer wieder darauf hin, dass Menschen nicht gezwungen werden, ihre Daten Diensten wie Amazon oder Google zu übermitteln, sondern es freiwillig tun. Dabei werden sie immer weniger von Menschen und immer mehr von Algorithmen beurteilt, die undurchsichtige Verfahren anwenden und viele relevante Kontexte unserer Daten ausblenden. Menschliche Korrekturen und Einschätzungen fallen häufig weg, weshalb der Trost, dass die eigenen Daten uninteressant scheinen und kein Indiz für ein gefährliches Verhalten enthalten, trügerisch und letztlich falsch ist: Wir wissen nicht, aufgrund welcher Kriterien uns Algorithmen in Zukunft als gefährlich einstufen werden, weshalb wir alle etwas zu verbergen haben, auch wenn das auf den ersten Blick anders aussieht. Die Liste von Menschen, denen die USA wegen Bagatellen Visa verweigert haben, wird immer länger. So wurde Adi Schamir, einer der bedeutendsten Kryptografen, ohne Angabe von Gründen von einer wichtigen Konferenz ausgeladen, und dem Autor Ilija Trojanow, der zusammen mit Juli Zeh ausführlich über die Gefahren der Überwachung geschrieben hatte, wurde das Visum verweigert, als er eine Rede in den USA halten wollte.

Surfe sauber! Nicht nur für deine, sondern auch für diejenige von Schwächeren. FOTO: NICOLE STRASSER

e Sicherheit anderer Menschen, insbesondere
EATIVE

Angesichts dieser Bedrohungskonstellation wird sofort klar: Absolute Sicherheit und absoluten Datenschutz gibt es nicht. Mit und vor spezialisierten InformatikerInnen ist niemand sicher – und die arbeiten auch für Kriminelle, für den Staat und die grossen Unternehmen. Daraus ergibt sich eine gewisse Frustration gegenüber dem Problem des Datenschutzes: Die etablierten Kommunikationsformen erlauben uns zwar den fast perfekten Schutz vor neugierigen Mitmenschen, lassen unsere Daten aber in riesige Speicher fliessen, für die weder Gesetze noch Zeit eine Bedeutung haben: Niemand weiss, in welchen Ländern unsere Daten ausgewertet werden und welche Erkenntnisse sich morgen aus den heute gespeicherten Informationen gewinnen lassen.

Und doch gibt es hinsichtlich all dieser fünf Bedrohungslagen vier empfehlenswerte Grundsätze: Daten sparsam anlegen, die angelegten so gut wie möglich schützen, sich beim Datenschutz solidarisch verhalten und weder die Gefahr noch den Nutzen der eigenen Vorkehrungen überschätzen. Da Daten nicht nur dann entstehen, wenn wir einen Computer oder ein Smartphone benutzen, ist das nicht einfach. Jeder Einkauf führt zu einer Datenspur, jede Bahnhofsbenützung oder Autofahrt zu digitalen Videoaufnahmen, jede Kommunikation mit technischen Hilfsmitteln zu sogenannten Metadaten, die zumindest angeben, wer wann miteinander in Kontakt getreten ist. Ob wir telefonieren, Briefe schreiben oder ein soziales Netzwerk benutzen, wird diesbezüglich zunehmend irrelevant. Die USA erfassen sämtliche Briefe digital, Poststellen werden zunehmend mit Video so überwacht, dass die AbsenderInnen von Paketen identifiziert werden können, und Telefongespräche können schon länger problemlos mitgeschnitten werden.

Dennoch lohnt sich jede Anstrengung in Bezug auf Datenschutz, weil sie den Aufwand erhöht, mit der Informationen gewonnen werden können. Letztlich ist Überwachung heute nur deshalb so leicht möglich, weil sie so billig ist. Kostet sie mehr – an Geld oder Zeit –, findet weniger davon statt.

> Letztlich ist Überwachung heute nur deshalb so leicht möglich, weil sie so billig ist.

Jeder Versuch, die eigenen und fremden Daten zu schützen, startet bei der Einsicht, dass Werkzeuge nicht gleichzeitig gratis, bequem und sicher sein können, sondern nur zwei der drei Eigenschaften aufweisen können. Wer sich also für eine bequeme, sprich alltagstaugliche Variante entscheidet, muss in der Regel dafür zahlen. Ein Beispiel dafür ist Mykolab. Das Schweizer Unternehmen bietet Speicher- und E-Mail-Lösungen an, die denen von Google, Microsoft und Apple entsprechen, mit dem Unterschied, dass alle verwendeten Programme «open source» sind – das heisst keine versteckte Überwachung zulassen –, die Firma in der Schweiz ansässig ist und die Dienstleistungen kostenpflichtig sind.

Alli mini Äntli

Neben der Einsicht, dass heute die Verwendung vieler Gratistools im Gegenzug mit Daten bezahlt wird, ist die Verschlüsselung von verwendeten Werkzeugen ein weiterer entscheidender Faktor. Die einfachsten Schritte sind hier: Software von Mozilla verwenden, also Thunderbird für E-Mail und Firefox als Webbrowser, und Verschlüsselungszusatzprogramme installieren. Eine sehr gute Übersicht bietet prism-break.org, wobei gerade bei verschlüsselten Chats und E-Mails auch die EmpfängerInnen von Nachrichten entsprechende Verschlüsselungssoftware verwenden müssen. Auch die auf Geräten gespeicherten Inhalte können und sollen verschlüsselt werden. Es empfiehlt sich zudem, nur über einen VPN-Zugang auf das Internet zuzugreifen. Der lässt sich auf den meisten Geräten problemlos einrichten und stellt sicher, dass die Interaktion mit Servern besser geschützt erfolgt. Selbstverständlich sollten unterschiedliche Passwörter für jeden Dienst sein, die zudem lang und nicht in Dokumenten gespeichert sind. (Ganz einfache Methode für sichere Passwörter: Aus «Alli mini Entli schwümmed uf em See» wird «Am1A-s2ue3S».) In der Regel sollten Dienste wie →

Was man für mehr Sicherheit tun kann

Wer bisher ohne Gedanken an Datenschutz Standardgeräte und -software benutzt hat, kann mit ein wenig Hilfe von einer Fachperson und den folgenden Tipps seine Sicherheit erhöhen. Ein absoluter Schutz ist dadurch nicht gewährleistet, er hängt – wie im Text dargestellt – stark vom Engagement anderer Unternehmen, dem Schutz durch Gesetze und der Verantwortung von Unternehmen ab. Zudem sollte vor Beginn klar sein, gegen welche Bedrohung Schutz gewünscht wird. Die Tipps ersetzen ein Bewusstsein in Bezug auf die Bedeutung von Daten keinesfalls. Ausführliche Hinweise bietet ein hilfreicher Guide der ARD: phwa.ch/ard.

1. Internetbrowser konfigurieren: Am einfachsten Firefox verwenden und mit nötigen Konfigurationen und Add-ons sicherstellen, dass der Datenverkehr wo möglich verschlüsselt wird, sogenanntes Tracking erschwert wird und keine Scripts ausgeführt werden können. Zu empfehlen ist insbesondere die Installation von HTTPs Everywhere und Disconnect, die man mit Google leicht findet: Suchanfrage «firefox» plus beispielsweise «disconnect».

2. E-Mail sichern: Einen E-Mail-Account eines seriösen Schweizer Anbieters verwenden (z. B. Mykolab) und mit einem E-Mail-Programm darauf zugreifen, das Verschlüsselung ermöglicht. Alle wichtigen Kontakte bitten, diese Verschlüsselung ebenfalls zu nutzen. Als Einstiegslektüre empfiehlt sich phwa.ch/mail.

3. VPN auf allen Geräten einrichten, wenn man fremde WLAN-Verbindungen nutzt: Bei vpnanbieter.net einen Anbieter auswählen und in der Regel ausser Haus auf allen Geräten damit aufs Internet zugreifen.

4. Mobile-Apps zurückhaltend verwenden: Für Laien ist es fast unmöglich zu kontrollieren, welche Daten Apps auf Smartphones wohin versenden. Vorsicht ist angebracht.

Wer Hilfe braucht, ist gut beraten, Fachleute beizuziehen. Eine Sammlung wichtiger Informationen bietet privacyfoundation.ch. Persönliche Hilfe findet man an sogenannten Cryptopartys, für Zürich findet man Veranstaltungen unter cryptoparty.in/zuerich. Gutmütige und interessante HackerInnen besammeln sich in sogenannten Hackerspaces, wo Sicherheit ein wichtiges Thema ist und Kontakte geknüpft werden können. Eine Übersicht findet man unter hackerspaces.ch.

PHILIPPE WAMPFLER

Facebook oder Google nicht benutzt werden, um sich bei weiteren Profilen anzumelden.

Auch die Geräte, also die Hardware, sind nicht vor unbefugten Zugriffen geschützt, weshalb es nicht paranoid ist, nicht verwendete Kameras und Mikrofone mit einem dunklen Kleber abzudecken.

Das Kreuz mit der Bequemlichkeit

Informationsnetzwerke sind so gestaltet, dass Inhalte zugänglich gemacht werden. Das heisst, dass es stets die Möglichkeit gibt, dass sich Unbefugte Zugang verschaffen. Deshalb ist Vertrauen ein zentraler Faktor. Wem kann ich in Bezug auf eine bestimmte Information vertrauen? Nutze ich heute ein Standardsmartphone, um eine Nachricht zu verschicken, so vertraue ich: dem Hersteller des Geräts, dem Anbieter des Internetzugangs, dem Nachrichtenprogramm, dem Nachrichtenserver und dem Empfänger oder der Empfängerin sowie der von ihm oder ihr verwendeten Technologie. Trotz der scheinbaren Einfachheit und Effizienz der Kommunikation – die Nachricht wird getippt und sofort empfangen – ergeben die daran Beteiligten ein unüberblickbares Geflecht, dem gegenüber Vertrauen unmöglich wird, weil kaum ein Unternehmen, das digital operiert, die gespeicherten Daten zuverlässig schützen kann oder darauf verzichtet, sie zu verkaufen.

Mehr Datensicherheit erfordert also den Entzug von bestimmten Informationen aus dem vernetzten System: Will ich meine soziale Situation, meine wirtschaftliche Einbindung oder meine Identität digital abbilden und anderen Einblicke ermöglichen?

Ein Weg zu mehr Schutz wären lokale Netzwerke, deren Daten nicht mit anderen ausgetauscht werden. Der Preis dafür ist eine Einbusse an Bequemlichkeit, denn es bedeutet zum Beispiel, in der Nachbarschaft auf E-Mails und SMS zu verzichten und einander zu besuchen oder Briefe vor die Tür zu legen. Oder ein drahtloses Netzwerk zu installieren, das zwar Geräte verbindet, aber diese nicht ans Internet anschliesst.

Wer im Supermarkt Punkte sammeln will, sollte mehrere Karten verwenden.

Sobald unsere digitalen Profile Lücken aufweisen, taugen sie weniger gut dazu, unser Verhalten zu modellieren. Zusammen mit der Strategie, einige Informationen dem Netz vorzuenthalten, kann es sinnvoll sein, mehrere Profile gleichzeitig und mit anderen Personen zusammen zu verwenden. Wer im Supermarkt Punkte sammeln will, sollte das bei einigen Einkäufen bewusst nicht tun, mehrere Karten gleichzeitig verwenden und diese ab und zu mit Bekannten tauschen. So entstehen zwar Profile, die Realität wird aber verstärkt selektiv und verzerrt abgebildet. Solche Vorgehensweisen ignorieren bewusst die Vorgaben der Unternehmen – oder gehen mit ihnen spielerisch um. Genau das ist die Strategie von Hackerinnen: Sie benutzen Programme spielerisch auf eine Art, die ihre Hersteller nicht beabsichtigt haben. Solche Taktiken gibt es viele: Genauso wie SchülerInnen seit Jahrzehnten Zettel schreiben, die ihre Lehrpersonen nicht lesen können, weil sie einen Code verwendet haben, können wir unsere digitalen Nachrichten so formulieren, dass nur Eingeweihte verstehen, worum es geht. Jugendliche verwenden solche Methoden längst, weil sie davon ausgehen, dass sie keine Privatsphäre im rechtlichen oder lokalen Sinn haben, sondern nur in Bezug auf die Kontrolle über ihre Informationen. Sie gehen also davon aus, dass ihre Nachrichten von allen gelesen werden können. Entsprechend verschlüsseln sie so, dass der öffentliche Status der Nachricht bedeutungslos wird, weil ihr Inhalt nur einem ausgewählten Publikum zugänglich ist. Beliebte Methoden sind Verweise auf Ereignisse, bei denen nur Eingeweihte dabei waren («Bring das mit, worüber wir beim Ausflug nach Luzern so gelacht haben!»), oder das Zitieren bekannter Songtexte, die eine bestimmte Botschaft enthalten.

Und wenn wir alles preisgeben?

Einen radikal anderen Zugang schlägt die Post-Privacy-Bewegung vor. Ihre VertreterInnen, wie der Berliner Christian Heller, glauben nicht daran, dass Privatsphäre in der traditionellen Bedeutung ein Konzept sei, das Menschen schütze – vielmehr mache es sie verletzlich, weil ihre Geheimnisse sie bedrohten. So legt Heller sein ganzes Leben offen: Auf seinem Wiki, plomlompom.de/PlomWiki, dokumentiert er sein ganzes Leben. Seine Termine und Tätigkeiten sind minutiös festgehalten, seine Einnahmen und Ausgaben komplett aufgelistet, selbst die Gegenstände in seiner Wohnung inventarisiert Heller. Er stellt einen kompletten Datensatz seiner selbst ins Netz – so wird irrelevant, was jemand über ihn weiss, weil alle alles wissen können.

Heller ist als weisser, gebildeter und gesunder Mitteleuropäer privilegiert und kann sich diese Haltung deshalb leisten. Sein Vorgehen ist kein Rezept, aber es zeigt, dass uns beide Extrempositionen verbaut sind: Weder können wir verhindern, dass unsere Daten zu Profilen verdichtet werden – das haben Dienste wie Teledata oder Moneyhouse im Bereich der Bonitätseinschätzung unabhängig vom Internet schon lange gemacht –, noch können wir uns vollständige Transparenz erlauben.

Wir sind (oder wären) darauf angewiesen, uns die Hände zu waschen. Nicht nur für unsere Sicherheit, sondern auch für die anderer Menschen, insbesondere auch die Schwacher. Aber digitale Hygiene allein reicht nicht aus – wir brauchen dabei die Unterstützung von Politik und Unternehmen, die sich dem Druck der Geheimdienste und Regierungen entziehen und Lösungen anbieten, die uns als Menschen in den Mittelpunkt stellen.