

Wir wissen, wo Sie gewesen sind. Wir wissen mehr oder weniger, woran Sie denken», hat der Google-Präsident Eric Schmidt einmal gesagt. Das machte den Konzern zur zweitwertvollsten Firma der Welt nach Apple.

Auch Facebook schwimmt in einem Datenmeer. Dessen Grösse legte der österreichische Jus-Student Max Schrems 2011 offen. Nach zweijähriger Gerichtsschlacht zwang er Facebook zur Herausgabe jener Informationen, die das soziale Netzwerk über ihn gesammelt hatte: Ausgedruckt waren es – mit allen seinen Freunden, allen Einträgen im Newsfeed, allen Fotos und Seiten, auf die er geklickt hatte, und aller Werbung, die er jemals angeschaut hatte – 1200 Seiten. So dicht sind die Profile, dass Facebook Ihre sexuelle Orientierung vorhersagen kann, Ihre politische Zugehörigkeit oder sogar einen Drogenmissbrauch. Das soziale Netzwerk weiss vor Ihrem Coming-out, dass Sie schwul sind und dass Sie verlobt sind, bevor Sie es den Eltern sagen. Es sind nicht nur der Massenexhibitionismus, die Milliarden von Likes und Kommentaren, die Facebook so allwissend machen: Ähnlich wie Google beobachtet die Firma den Surfer auf jeder Website mit einem «Gefällt mir»-Button, egal, ob er den Knopf drückt, egal sogar, ob er bei Facebook eingeloggt ist.

No Free Lunch. Google und Facebook, aber auch viele andere Internetdienste wie Twitter oder Instagram mögen gratis sein in dem Sinne, dass man für ihre Nutzung kein Geld bezahlt. Dafür bezahlt man mit Daten. «Wenn etwas umsonst ist, sind Sie nicht der Kunde. Sie sind das Produkt!», schreibt Bruce Schneier, Autor von «Data and Goliath».

Es sind gewaltige Datenmengen, die da anfallen. Bereits sind über 10 Milliarden Geräte im Internet, mehr, als die Erde Bewohner hat. 2020 sollen es 30 Milliarden sein. Dieses Jahr werden 76 Milliarden Exabyte über das Netz geschickt (ein Exabyte ist eine Milliarde Terabyte, eine heute gängige Festplattengrösse). Gespeichert werden sie in riesigen Rechenzentren, von denen Google und Facebook die grössten haben sollen. «Viele sammeln erst mal alle Daten, aber wissen noch gar nicht, was sie damit machen sollen», sagt ETH-Professor Ernst Hafen.

Besonders beliebt sind Positionsdaten der Handys. Wer ständig weiss, wo Sie ►

«Mit meinem echten Namen geize ich»

Sicherheitsexperte Martin Hellweg erklärt, wie man die Kontrolle über seine Daten behält.

BILANZ: *Martin Hellweg, wie kann man seine persönlichen Daten im Internet schützen?*

Martin Hellweg: Man kann seine Datenspur im Internet nicht gänzlich verhindern – dazu müsste man zurück auf die analogen Bäume klettern. Man kann sie nur minimieren. Das Allerwichtigste ist, dass man für sich selber einteilt: Was ist streng vertraulich, was ist vertraulich, was ist nicht vertraulich? Streng vertraulich bedeutet etwa, dass ein Leck grossen finan-



*«Man kann die Datenspur im Internet nur minimieren»:
Sicherheits-
experte Martin Hellweg.*

ziellen oder emotionalen Schaden für das Leben bedeuten kann – etwa wenn die Mitgliedschaft in einem Seitensprungportal à la Ashley Madison bekannt wird.

Was empfehlen Sie dann konkret?

Dann sollte man den Tor-Browser verwenden. Da bleibt man anonym.

Anonyme Sessions bieten auch gängige Browser.

Die Einstellung bringt aber wenig. Das ist maximal ein Wunsch an die andere Website, keine Daten zu erheben, aber keine Verpflichtung.

Welche Suchmaschine empfehlen Sie?

Mit dem Tor-Browser kann ich jede Suchmaschine benutzen. Angeblich anonyme Suchmaschinen wie DuckDuckGo allein bringen nichts ohne einen sicheren Browser.

Welches Betriebssystem ist am sichersten?

Für Laien kommt nur Windows, Android oder Apple OS in Frage. Android traue ich nicht, denn Google wäre pleite, wenn sie dort keine Daten auswerten würden. Apple und Microsoft müssen das nicht tun, sie verdienen primär mit ihren Produkten Geld. Von diesen beiden bevorzuge ich Apple, weil es ein geschlossenes System ist. Manche mögen das nicht, aber in Sachen Sicherheit ist das robuster.

Sind E-Mails ein Problem?

Ja, wenn man sie über Gratis-Mailanbieter wie Gmail versendet. Dort wird mitgelesen und ausgewertet. Ich empfehle, sich für wenig Geld eine eigene Domain zuzulegen und den Mailverkehr über einen Schweizer Mail-Hoster wie Metanet oder Hostpoint abzuwickeln. Die lesen keine Daten und löschen sie nach einer Weile. Bei US-Anbietern stellt sich grundsätzlich die Frage nach der Hintertür, die einzubauen sie gesetzlich verpflichtet sind. Diese Tür kann nicht nur die NSA nehmen, sondern auch ein Hacker.

Beim Online-Shopping: Kreditkarte oder PayPal?

Wenn es vertraulich ist, dann sollte sich zwischen Ihrem Namen und der Bezahlung kein Zusammenhang herstellen lassen. Dann kann man nur eine Prepaid-Karte wie Paysafecard oder OK-Prepaid verwenden. Die kann man beim Kiosk kaufen. Oder eine Geschenkkarte, etwa von Amazon. Wichtig ist auch, sich ein paar Pseudonyme zuzulegen. Die Firmen haben keinen Anspruch auf meinen Klarnamen. Mit meinem echten Namen geize ich.

Martin Hellweg (48), bekannt als Unternehmenssanierer (u.a. Swissmetal), ist seit 2007 zugleich mit seiner Firma Virtual Bodyguard im Privatsphäre- und Reputationsschutz tätig. Er ist Autor des Buchs «Safe Surfer».