Bist du sicher?

Catch me if you can: Unserem Autor Christoph fiel besonders der Abschied von Facebook schwer - schließlich hat er da eine Menge Freunde. Aber als die ihn plötzlich alle beglückwünschten, weil er seinen Account löschen wollte, kam er ins Grübeln

Jeder Klick wird registriert, unser Standort ausgecheckt, unsere Daten gelesen. Dabei gibt es Möglichkeiten, im Internet nicht zum gläsernen Konsumenten zu mutieren. Unser Autor hat den Kampf um seine digitale Mündigkeit aufgenommen

Text: Christoph Schultheis

→ Wir wissen es doch längst: Kaum sind wir online, lauern an jeder Ecke zwielichtige Internetbetrüger auf unsere Unaufmerksamkeit. Und selbst wenn wir unsere Passwörter umklammern wie die Touristin in Neapel ihre Handtasche: Wir werden trotzdem permanent verfolgt, durchleuchtet, ausspioniert, benutzt.

Man muss ja nur mal bei getpos.de oder dein-ip-check.de reinschauen. Solche Geolokationsdienste erkennen millisekundenschnell nicht nur unser Betriebssystem, unseren Browser und Internetanbieter, sondern sogar unseren ungefähren Standort. Gerade mal vier Kilometer liegen sie bei mir daneben. Alle diese Infos schleppe ich bei jedem Klick mit mir herum. Und dann noch diese Cookies, die uns das Surfen erleichtern, mit denen wir aber auch noch durchschaubarer werden. Als ich kürzlich mal einen Zweitaccount bei Facebook eröffnen wollte, wurden mir beim ersten Login trotz falschen Nutzernamens und falscher E-Mail-Adresse gleich ein paar meiner echten Freunde als Facebook-Freunde vorgeschlagen.

Trotzdem verbringe ich weiterhin einen Großteil meiner Lebenszeit im Netz. Natürlich klicke ich dann nicht auf dubiose E-Mail-Anhänge („Dies ist Herr Andrew Liu aus Hongkong, ich habe ein Geschäft Vorschlag von 44,5 Millionen Dollar für Sie"). Ich schaue sogar bei jedem Link vor dem Anklicken kurz in die Statuszeile meines Browsers, wohin er führt. Wenn ich irgendwo einen Kommentar hinterlasse, überlege ich mir gut, was ich schreibe. Oder lasse es bleiben. Und mein Virenschutzprogramm sagt mir: „Sie sind geschützt."

Aber das war's auch schon. Die Warnungen vor Sicherheitslücken, Datenklau und Trojanern habe ich nur mit einem Schulterzucken zur Kenntnis genommen: „Schlimm, aber mal schauen, was es so bei Facebook Neues gibt."

Bis jetzt. Denn ab heute starte ich den Selbstversuch, ab heute werde ich die guten Ratschläge der Internetprofis, der Daten- und Verbraucherschützer, der Nerds und selbst die der Paranoiker einfach mal in die Tat umsetzen! So ungefähr.

Eine erste halbherzige Google-Recherche ist allerdings eher ernüchternd. Stets lande ich in irgendwelchen Foren, in denen sich auch andere nach anonymem Surfen oder Verschlüsselung erkundigen – und es nicht lange dauert, bis sie als potenzielle Terroristen oder notorische Heimlichtuer verdächtigt werden. Das bringt mich nicht weiter.

Also vereinbare ich ein Treffen mit Constanze Kurz. Die Informatikerin hat gemeinsam mit Frank Rieger ein Buch* darüber geschrieben, „wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen". Das Buch kenne ich schon. Ich habe es nicht gemocht, weil es einem auf seinen mehr als 250 Seiten endgültig die digitale Unschuld raubt. Das nervt, denn Constanze und ihr Kompagnon haben leider so verdammt recht. Was wiederum kein Wunder ist. Schließlich sind beide Sprecher des Chaos Computer Clubs (CCC) – eines Zusammenschlusses von Computerfreaks und Netzaktivisten, die immer wieder mit spektakulären Hacks und subversiven Aktionen für Aufsehen sorgen, längst aber auch als Sachverständige vor Gericht oder als Interviewpartner in der Tagesschau gefragt sind. Sogar die Bundesregierung lässt sich in Internetfragen vom CCC beraten. Zugleich versteht sich der Club aber auch als Lobbyist und Propagandist einer „digitalen Mündigkeit". Und genau die will ich ja.

Zunächst ist Constanze wichtig, dass ich mir klarmache, worum es bei meinem Selbsttest geht. Um einen Akt des Widerstandes gegen die Datensammelei? Oder darum, mich einfach sicherer zu fühlen? Constanze erzählt von ihrer Schwester in China und dass sie sogar ihrem Vater einen verschlüsselten E-Mail-Account eingerichtet habe, den er inzwischen gern benutze. Das sei einfach, „ja, ein gutes Gefühl", sagt sie.

Am Ende unseres Treffens machen wir gemeinsam eine Liste mit meiner Mediennutzung, die immer länger wird: Wie viele E-Mail-Konten habe ich eigentlich und bei welchen Anbietern? Welchen Browser nutze ich zum Surfen? Und dann der ganze netzbasierte Kram: Skype? Twitter? iTunes? Instagram? Flickr? Facebook etwa? Google Mail?! Vor allem bei den beiden großen

„Du bist mein Vorbild! Goodbye Facebook!"

Datenkraken versteht Constanze keinen Spaß. Außerdem, ich hätte es fast vergessen, sei da ja noch mein Smartphone. Hier geht das Spiel von vorne los: E-Mail, Browser, Apps … „Kein WhatsApp?", fragt Constanze. Ich schüttele schnell den Kopf.

Wieder zu Hause, sehe ich mir meine Mediennutzungsliste noch einmal an. Hinter die Punkte Browser/Surfen, E-Mail und Facebook habe ich ein Ausrufezeichen gemacht. Nun denn.

Keine Frage, wenn ich wirklich die Kontrolle über mein digitales Ich zurückerobern will, gibt es nur eine Konsequenz: bei Facebook abmelden und das Konto löschen. Der Lösch-Button ist sogar leicht zu finden – solange man ihn nicht bei Facebook selber sucht. Gibt man jedoch Facebook bei Google ein, ist „Facebook löschen" einer der Top-Suchvorschläge. Und von da ist es dann auch gar nicht mehr weit bis zum finalen facebook.com/help/delete_account.

Doch vorher schreibe ich noch ein letztes Posting, in dem ich meinen Ausstieg ankündige – mit einem kleinen <3 am Schluss, damit keiner denkt, ich sei zum Facebook-Hasser mutiert. Oder zum Selbstmordkandidaten.

Die Reaktionen allerdings verblüffen mich: Einige meiner Freunde, Kollegen und Facebook-Freunde drücken spontan den

Es geht auch anders

Ein paar Alternativen für Computer und Smartphone

Startpage.com

Die mit dem Europäischen Datenschutz-Gütesiegel ausgezeichnete niederländische Suchmaschine Startpage nutzt unter anderem Google-Suchergebnisse, speichert aber anders als Google keine IP-Adressen des Nutzers und setzt keine Cookies zu dessen Identifizierung.

TextSecure

Mit der kostenlosen App lassen sich verschlüsselte SMS verschicken - vorausgesetzt natürlich, der Empfänger hat die App ebenfalls installiert (und aktiviert). Selbst für Laien ist das Einrichten einer verschlüsselten SMS-Konversation fast schon intuitiv. Nachteile: TextSecure funktioniert nur zwischen Android-Geräten. Und verschlüsselte Nachrichten nehmen erheblich an Größe zu, wodurch das Simsen teurer werden kann.

RedPhone

RedPhone ermöglicht verschlüsselte Telefonate. Die App ist ebenfalls kostenlos, und auch sie lässt sich nur mit Android-Handys nutzen. Die Gespräche werden nicht übers Mobilfunknetz geführt, sondern online per VoIP. Es können also je nach Handyvertrag auch Datenkosten anfallen. Die Sprachqualität ist noch nicht ausgereift (blechern, zeitverzögert, Echo-Effekte).

Orbot

Mit der Mobilversion des Tor-Browsers kann man auch mit Android-Phones anonym surfen. Unterstützt werden bisher allerdings nur der mobile Firefox-Browser und der wenig komfortable, aber noch sicherere Orweb-v2-Browser. Mobil ist das Surfen mit Tor leider noch langsamer als am PC.

Like-Button, andere schreiben unter mein Abschiedsposting anerkennende Kommentare: „… immer einen Schritt voraus“ oder „Hey, das wollte ich Anfang des Jahres auch machen. Hab’s nicht geschafft: Nun bist du mein Vorbild!“ Die Offline-Reaktionen im Freundes- und Kollegenkreis sind ähnlich: Daumen hoch! Nach dem Warum fragt kaum jemand. Das scheint sich von selbst zu verstehen.

Die eigentliche Löschaktion meines Kontos ist dann auch kein Problem. Zumindest technisch. Ein letztes „Bist du sicher?“ – und schon steht dort, wo vorher mein Facebook-Profil war: „Diese Seite existiert leider nicht.“ Wahr ist das allerdings nicht. Facebook lässt mein Konto noch 14 Tage lang unangetastet. Loggt man sich währenddessen wieder ein, verlängert sich die Karenzzeit erneut um zwei Wochen.

Was meine digitale Mündigkeit anbelangt, kommt es mir vor, als hätte meine eigene Entscheidung mich mehr bevormundet als die x-te Änderung der Facebook-AGB. Drinnen die Party, und ich habe mich ausgesperrt und den Schlüssel weggeworfen? Ein „gutes Gefühl“ geht anders.

Zumal etwas Mulmiges geblieben ist. Klar, Facebook muss jetzt ohne meine Daten auskommen – ohne neue Daten. Denn gelöscht wird nur mein Konto. Vieles, was ich die letzten drei Jahre eingegeben habe, bleibt aber offenbar für ewig auf den Facebook-Servern liegen. Ein österreichischer Student hat bereits diverse Anzeigen wegen Facebooks Umgang mit Nutzerdaten bei der irischen Datenschutzbehörde eingereicht – Ausgang ungewiss.

Und Facebook ist ja nicht das einzige Unternehmen, das ungefragt von meinen Internetaktivitäten profitiert. Was aber, wenn ich auch das nicht möchte, wenn ich nicht will, dass mir auf meinem Weg durchs Netz andauernd irgendwer hinterherschnüffelt? Klar, es gibt Einzelfalllösungen wie „Vtunnel“ oder „Hide My Ass!“ und allerlei skurrile Hilfsdienste. Fakenamegenerator.com zum Beispiel, wo ein Klick komplette Scheinidentitäten generiert – inklusive Anschrift, Telefonnummer, Username und Login, E-Mail-Adresse, Gewicht, Größe, Kreditkartendaten, Blutgruppe und Mädchenname der Mutter. Oder auch Frank-geht-ran.de. Und als ich mich gerade daranmachen will, ein FoxyProxy-Plugin zu installieren, lese ich bei Chip.de dies: „Für maximale Sicherheit: Tor macht Sie unsichtbar – Wer so anonym wie möglich im Netz unterwegs sein möchte, kommt an Tor nicht vorbei.“ Klingt perfekt.

Nach der vergleichsweise unkomplizierten Installation des Tor-Browser-Pakets hat sich auf den ersten Blick nicht viel verändert. Am unteren Bildschirmrand ist nun ein neues Icon, eine Zwiebel. Sie ist das offizielle Symbol für Tor, das eigentlich „The onion router“ heißt. Und als ich mich mit einem Zwiebel-Klick ins Tor-Netzwerk einwähle, öffnet sich zuerst ein Firefox-ähnlicher Browser – und begrüßt mich mit den Worten: „You are now free to browse the Internet anonymously.“

Das mit dem „anonymously“ müsste stimmen. Ein kurzer Online-Check zeigt mir eine ganz andere IP-Adresse als meine eigene. Außerdem liegt der Geolokationsdienst nun nicht mehr vier, sondern über 6.000 Kilometer daneben. Denn geortet werde ich auf dem Campus der Rutgers University in Piscataway/New Jersey. Und das nicht einmal lange. Wenig später ist es Skipton, eine Kleinstadt in North Yorkshire, dann das südschwedische Lund, dann Gunzenhausen. Denn genau so funktioniert das Tor-

Netzwerk wohl: Überall auf der Welt stellen Leute ihre Router zur Verfügung, und man selbst spielt „Catch me if you can!“.

Eine Zeitlang habe ich viel Spaß, dem Wechsel meiner unterschiedlichen Identitäten zuzuschauen. Aber dann merke ich, dass ich so „free“ gar nicht bin, wie mir der Tor-Browser versprochen hat. Eher so, als hätte ich mir eine dicke Eisenkugel ans Bein gekettet. Denn das Surfen geht langsam. Sehr. Sehr. Lang. Sam.

Dabei ist die mickrige Übertragungsrate nicht einmal der einzige Preis, den man für die „maximale Sicherheit“ zahlt: Ständig poppen Warnhinweise auf: „Sie haben eine verschlüsselte Seite angefordert, die unverschlüsselte Informationen enthält …“, heißt es dann. Oder: „Externe Applikationen sind im Allgemeinen NICHT Tor-gesichert und können Sie verraten!“

Yessss! Der Geolokator vertut sich um schlappe 6.000 Kilometer

Außerdem kann ich mit Tor keine YouTube-Videos mehr ansehen, und mein RSS-Reader ist auch unbrauchbar. Für die Ansicht von PDF-Dateien schlägt mir Tor lieber einen Online-Viewer namens view.samurajdata.se vor. Und benutze ich die Google-Suche im Browser, heißt es: „Torbutton hat ein Google-Captcha festgestellt. Möchten Sie für Ihre Suchanfrage zu einer anderen Suchmaschine umgeleitet werden?“ Wenn ich die Anfrage bejahe, lande ich immerhin bei Startpage.com, einer cleveren Google-Alternative, die sich selbst als „die diskreteste Suchmaschine der Welt“ bezeichnet – und dabei auch noch brauchbare Suchergebnisse liefert.

Da suche ich dann gleich nach Ideen für mein drittes Großprojekt: Mails verschicken, ohne dass sie (zumindest theoretisch) jeder mitlesen kann. Denn dass mein flinkes, großes, komfortables, webbasiertes Google-Mail-Konto nicht zu meinem neuen Leben in der digitalen Mündigkeit passt, war mir von Anfang an klar.

Nicht ganz so klar war mir, wie viel Zeit und Nerven es mich kosten würde, eine wirklich sichere Alternative einzurichten. Gefunden war die schnell: „GNU Privacy Guard for Windows“, kurz gpg4win, war schließlich vom Bundesamt für Sicherheit in der Informationstechnik in Auftrag gegeben worden und hat sogar ein eigenes kleines Mail-Programm namens Claws mit an Bord.

Über die Tage nach dem Download rede ich ungern: Umgebungsvarianten, Clients, Gateways, Proxys – ich verstand kein Wort. Längst hatte ich neben dem Tor-Browser ein zweites „normales“, schnelles Browserfenster aufgemacht, um herauszufinden, warum zur Hölle meine Installationsversuche immer wieder scheiterten. Doch ich stolperte bloß über Sätze wie diesen: „Die Mail-Inhalte werden mit Triple-DES chiffriert; für zusätzliche Sicherheit sorgt die RSA-verschlüsselte Übergabe der Paket-Header und 3DES-Keys.“ Oder ich landete auf Internetseiten von Neonazis, die ihren Gesinnungsgenossen Tipps für „Weltnetz“ und „E-Post“ geben.

Zum Glück entdeckte ich irgendwann die Seite Verbraucher-sicher-online.de, wo mir endlich in kleinen, öden Schritt-für-Schritt-Videos gezeigt wurde, wie’s geht. Ohne wirklich zu wissen, was ich tat, erstellte ich also ein OpenPGP-Schlüsselpaar, ex- oder importierte und beglaubigte Zertifikate – bis ich tatsächlich verschlüsselte Mails versenden konnte!

Angeblich jedenfalls. Denn selbstverständlich muss, damit in einer Mail von mir nicht nur Buchstabensalat steht, der Adressat ebenfalls das ganze Schlüsselzeugs auf seinem Rechner installieren. Aber kann ich, will ich das alles wirklich jemandem zumuten? Schreibt mir dann überhaupt noch wer? Schließlich schicke ich eine verschlüsselte Mail an Constanze vom CCC, damit ich wenigstens weiß, ob dieser vorerst letzte Schritt auf meinem Weg zur digitalen Mündigkeit tatsächlich von Erfolg gekrönt ist. Noch am selben Abend schreibt Constanze mir zurück: „hQEMAzaHe2yX2-5NHAQf/ZMYQnu/rzr5uZuaHDa0 …“ Nachdem ich ihre Mail entschlüsselt habe, lautet die Antwort: „funktioniert! :}“

Ich bin mir da noch nicht so sicher. ←

**Das Buch „Die Datenfresser“ gibt es bei der Bundeszentale für politische Bildung (bpb); Band 1177; 4.50 Euro*

Darknet

Die Möglichkeiten, die es gibt, weitgehend unerkannt durch die Weiten des Internets zu surfen, haben leider auch eine dunkle Seite: Denn Verschlüsselungstechniken oder Peer-to-peer-Netzwerke,in denen sich einzelne Nutzer manuell miteinander verbinden, oder auch ein Browser wie Tor, bei dem sich die IP-Adresse nicht mehr einem einzelnen User zuordnen lässt, werden auch von Kriminellen genutzt. Eigentlich bezeichnet Darknet lediglich ein Netzwerk von Nutzern, die auf Anonymität bedacht sind – mittlerweile hat sich aber eingebürgert, damit die dunkle Welt von Drogendealern, Pädophilen und anderen zwielichtigen Gestalten zu bezeichnen, die die Anonymität nutzen, um Gesetze zu umgehen.