fluter.

Mich für nichts

Von früh bis spät hinterlassen wir einen Haufen Daten. Unser Autor will herausfinden, wer ihm alles auf der Spur ist (es sind viele)

Bernd Kramer

17.09.2018 Datenschutz 8 Min.

Teil 1: Mir bringt die Post Briefe - und anderen meine Adresse

Elf Uhr morgens, im Treppenhaus hallt das Klappern der Briefkastendeckel. Lange dachte ich, die Post benutzt meine Anschrift nur für einen einzigen Zweck: um mir Briefe zuzustellen. Eine naive Vorstellung.

Im Frühjahr wurde bekannt, dass eine Post-Tochter im vergangenen Jahr während des Bundestagswahlkampfs Daten an Parteien weiterverkauft hat, in anonymisierter Form zwar, aber durchaus kleinteilig. Für Gebäude mit mindestens sechs Haushalten gab sie eine Wahrscheinlichkeit an, dass die Parteien hier Sympathisanten finden könnten – was zum Beispiel die CDU für ihren Haustürwahlkampf nutzte und gezielt dort klingelte.

Adress- und Datenhandel ist ein großes Geschäft, rund 610 Millionen Euro wurden damit im Jahr 2014 in Deutschland umgesetzt, heißt es in einer Studie für das Bundesministerium der Justiz und für Verbraucherschutz. Und die Post wirbt damit, einen besonders großen Datenschatz zu besitzen: Mit 46 Millionen Adressen decke sie „nahezu den gesamten Markt an Privathaushalten ab“, heißt es auf der Homepage. Aber womit handelt die Post eigentlich genau?

Ich richte mir bei Deutsche Post Direkt ein Benutzerkonto ein – als Unternehmer, der online Kundenadressen kaufen will. Und ich staune, was sich alles auswählen lässt. Ich kann Haustierbesitzer herausfiltern und die Leserinnen von Frauenzeitschriften, Menschen mit und ohne Doktortitel. Ich kann auswählen, ob ich lieber eine Adresse aus einer Straße mit vielen oder wenigen Autobesitzern will. Klicke ich in der Auswahlliste auf das Fragezeichensymbol, erklärt mir die Post, woher sie ihre Informationen bekommt. Das Alter der Bewohner zum Beispiel „wird über die Vornamensanalyse der Person ermittelt“ – eine Julia ist wahrscheinlich jünger als eine Roswitha. Ob an einer Anschrift die Bewohner häufig wechseln, lässt sich wiederum aus den Nachsendeaufträgen schließen. Rund 150 „Zielgruppenmerkmale“ bietet die Post zur Auswahl an, 1.000 Adressen gibt es bereits zum Preis von 84 Euro.

Es klingelt an der Tür. Der Paketbote bittet mich, eine Sendung für den Nachbarn anzunehmen – mal wieder. Ich arbeite oft zu Hause, deswegen werden die Amazon-Bestellungen aus dem ganzen Haus regelmäßig in meinem Wohnungsflur zwischengeparkt. Der Bote fragt mich nach meinem Namen, hält mir das Gerät hin, damit ich auf dem Display gegenzeichne. Aber diesmal zögere ich kurz. Wer erfährt eigentlich alles, dass ich ständig Pakete für andere annehme? Die Nachbarn, klar. Und sonst?

Ich erkundige mich beim Bundesverband Paket und Expresslogistik. Mein Name werde in der Sendungsverfolgung dokumentiert, erklärt mir eine Verbandssprecherin. Die Paketunternehmen würden die Informationen aber nicht auswerten und bald nach der Zustellung wieder löschen: Als Dauer-Pakete-für-andere-Annehmer würde ich also nicht gespeichert. Allerdings haben auch die Versender Zugriff auf die Informationen. Theoretisch also könnte auch Amazon meine regelmäßige Mithilfe bei der Zustellung seiner Lieferungen mit der Zeit auffallen. Vielleicht mag man mir beim nächsten Einkauf für meine Hilfe ja mal einen Rabatt geben?

Teil 2: Was? Mein Passwort steht im Internet, und alle können es sehen?

Pling! In meinem E-Mail-Eingang findet sich eine neue Nachricht, Betreff: „Ihr Geld steht bereit“. Ich bin genervt. Woher kommen die ganzen Spam-Nachrichten?

Auf der Internetseite des Hasso-Plattner-Instituts für Digital Engineering der Uni Potsdam kann ich überprüfen, ob meine E-Mail-Adresse in einem der Datensätze auftaucht, mit denen Kriminelle handeln. Vielleicht finde ich hier die Antwort auf die Flut an Müllnachrichten. Ich gebe meine E-Mail- Adresse ein. Und pling, schon finde ich die Auswertung des Hasso-Plattner-Instituts in meinem Postfach: Meine Adresse sei „in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank“ enthalten, lese ich da. Außerdem: mein Passwort! Gleich in fünf Datenbanken! Ich bin erschrocken.

Ich rufe David Jaeger an, der am Hasso-Plattner-Institut promoviert und den E-Mail-Check mitbetreut. So wie mir geht es offenbar sehr vielen. „Bis zu 40 Prozent derjenigen, die ihre Mail-Adresse mit unserem Tool überprüfen, tauchen in irgend- einer dieser Datenbanken auf“, sagt er. Und erklärt mir die Ökonomie des Onlinebetrugs, die über mehrere Etappen läuft. Es beginnt damit, dass Kriminelle über verschiedene Wege Daten sammeln – etwa über Spähsoftware, die man nichtsahnend auf seinen Rechner lädt, oder indem sie Onlinedienste wie das Karriereportal LinkedIn hacken und dort Nutzerkennwörter stehlen. In geschlossenen Foren bieten sie ihre Beute schließlich zum Kauf an. Die Käufer zielen vor allem auf die wenigen Personen, zu denen zum Beispiel auch Kreditkartennummern oder Bankverbindungen hinterlegt sind – auf die leichten und lukrativen Opfer sozusagen. „Am Anfang wird alles genutzt, was sich sehr unmittelbar zu Geld machen lässt“, sagt Jaeger. Ist das abgegrast, wird der Datensatz weiterverkauft, jetzt schon für weniger Geld. Die zweite Riege der kriminellen Käufer versucht zum Beispiel, mit Kombinationen aus Passwörtern und E-Mail-Adressen Amazon-Konten zu kapern und in fremdem Namen Waren zu bestellen – was oft klappt, weil viele Menschen immer dasselbe Passwort benutzen; mit einem bei LinkedIn gestohlenen Kennwort kann ein Betrüger sich oft auch in andere Konten einloggen. Irgendwann ist der Datensatz ausgepresst wie eine Zitrone, und irgendjemand am Ende der Kette stellt ihn frei ins Netz. Dann klappern die Spam-Bots ihn ab und verschicken massenhaft Angebote für Viagra oder dubiose Nahrungsergänzungsmittel, und dort finden ihn auch die Potsdamer Forscher. Bis dahin können aber Jahre vergehen. „Ihre E-Mail-Adresse kann also

noch in diversen anderen Listen stehen, von denen wir bisher gar nichts wissen“, sagt Jaeger.

Einer der Datensätze, in denen laut dem Check des Hasso- Plattner-Instituts meine Mail-Adresse stehen soll, heißt „Exploit.In“, öffentlich geworden ist er 2016. Ich google ein bisschen. Und tatsächlich. In einem Reddit-Forum finde ich eine Dateikennung, mit der ich die Liste bei einem Filesharing- Dienst herunterladen kann. Eine halbe Stunde dauert es, dann habe ich einen Ordner auf meiner Festplatte, 24 Gigabyte groß, fast 687 Millionen E-Mail-Adressen samt Passwort, verteilt auf 111 Textdateien, in denen Nutzerinnen und Nutzer aufgelistet sind. In einer dieser Dateien finde ich in Zeile 6.444.965: mich. Meine E-Mail-Adresse – und ein Passwort, das ich vor Jahren einmal benutzt habe. Mit dem man sich vielleicht immer noch irgendwo einloggen könnte. Mir wird mulmig. Wann war ich zuletzt bei StudiVZ?

Teil 3: Mit wem stecken meine Apps unter einer Decke?

Den potenziell größten Spion trage ich ständig in der Hosentasche mit mir herum. Er verfügt über ein Mikrofon, das mich abhören, eine Kamera, die mich beobachten kann, Bewegungssensoren und GPS-Empfänger: mein Handy. Außerdem ist es voller Apps, mit denen ich meinen Alltag manage. Aber wem geben diese vielen kleinen Programme weiter, was sie dabei über mich erfahren?

Ich lade „Lumen Privacy Monitor“ herunter, eine Android-App, die Forscher der Universität Berkeley entwickelt haben. Sie soll aufdecken, mit wem die übrigen Apps auf meinem Handy still und unbemerkt im Hintergrund kommunizieren. Eine Art Superspitzel also, den ich auf die vielen anderen kleinen Spione auf meinem Smartphone ansetze.

Dass die Apps mit ihren jeweiligen Herstellern Kontakt halten, „Spotify“ mit Spotify und „Jodel“ mit Jodel, überrascht mich nicht. Aber „Lumen“ zeigt mir an, dass da noch viele andere sind, an die ständig Daten geschickt werden. Etwa an Google. Oder an Facebook. „Die Apps kommunizieren mit externen Dienstleistern, über die zum Beispiel Werbung eingespielt wird. Oder einfach nur der Teilen-Button von Facebook“, erklärt Christian Kreibich, ein deutscher Computerwissenschaftler in Berkeley, der „Lumen“ mitentwickelt hat. „Weil die

verschiedenen Apps oft dieselben wenigen Dienstleister benutzen, können die ein sehr genaues Bild eines Nutzers bekommen und davon, was der mit seinem Gerät macht." Sie sind wahre Datensammelstellen, in denen viele Informationen über mich zusammenfließen.

Was genau, das kann mir auch Kreibich nicht sagen. Der Superspion „Lumen" tappt im Dunkeln, weil die Kommunikation zwischen den Apps und den Diensten in der Regel verschlüsselt wird – was im Prinzip eine gute Sache ist. Manchmal entdeckt „Lumen" aber doch, dass ziemlich sensible Daten abfließen: „WhatsApp" zum Beispiel hat offenbar mehrere Male mein Gerätemodell an Google gesendet. Besonders mitteilungsfreudig war „Clean Master", eine vorinstallierte App, mit der ich den Speicherplatz auf meinem Telefon aufräumen kann. Sie leitet neben dem Gerätemodell auch meine Zeitzone („Europe/Berlin") an den Hersteller und andere Dienste weiter – und meine Android-ID, also die, über die ich eindeutig zu identifizieren bin. Für das, was die App eigentlich leisten soll, ist das völlig unerheblich. Kreibich bezeichnet sie daher als regelrechten Spitzel.

Ironischerweise ist auch „Lumen" selbst ein äußerst neugieriger Späher – aber immerhin im Dienste der Wissenschaft. Was die App auf meinem Handy feststellt, übermittelt sie in einem Datensatz an die Forscher in Kalifornien. Mit den Informationen von Tausenden Handynutzern konnten Kreibich und seine Kollegen kürzlich in einer Studie feststellen, welche Apps besonders häufig Daten weiterleiten: Es sind kostenlose Handyspiele und Bildungs-Apps.

Teil 4: Warum ich im Supermarkt auch ohne Payback-Karte ausgespäht werde

„Haben Sie eine Payback-Karte?", fragt die Kassiererin. Es ist einer der wenigen Momente, in denen ich mich wie ein Mensch fühle, der den Datenschutz ernst nimmt. Wie ein Kunde, der sich bewusst verhüllt, statt sich gläsern zu machen. „Nein", sage ich mit voller Überzeugung. „Natürlich nicht."

Ich weiß ja, was der Handel mit Rabattkarten bezweckt: Er will mich ausforschen. Die amerikanische Supermarktkette Target fand mithilfe solcher Kundenkartendaten zum Beispiel heraus, wie man schon ziemlich früh schwangere Frauen identifiziert: Ab einem gewissen Zeitpunkt neigen sie unter

anderem dazu, parfümfreie Körperpflegeprodukte zu kaufen. Je früher die Händler werdende Mütter erkennen, desto gezielter können sie sie umwerben. Das führte bereits zu kuriosen Situationen: Eines Tages kam ein Vater empört in den Laden, weil die Supermarktkette seiner Tochter Gutscheine für Babykleidung geschickt hatte. Sie gehe doch noch zur Schule, schimpfte der Vater. Target wusste bereits von der Schwangerschaft, bevor die junge Frau es ihrer Familie sagte.

Auch die Deutschen helfen dem Handel sehr bereitwillig beim Datensammeln. Payback, der größte Rabattkartenanbieter, hat nach eigenen Angaben hierzulande 30 Millionen aktive Nutzerinnen und Nutzer. Aber sind die anderen, die sich nicht von ein paar Prämien locken lassen, wirklich so gut getarnt?

Die Händler mit Ladenlokal lassen sich inzwischen einiges einfallen, um ihre Kunden so zu durchleuchten wie die Konkurrenten im Internet. Die Supermarktkette Real erfasste zum Beispiel eine Zeit lang die Gesichter der Kunden an der Kasse, wenn sie auf Werbebildschirme schauten. So lässt sich personalisierte Werbung ausspielen – wie im Internet. Erst nach öffentlichem Protest wurde das Projekt eingestellt, in einigen Filialen der Deutschen Post ist es weiterhin aktiv.

Eine besonders verbreitete Methode macht sich zunutze, dass viele Menschen die WLAN-Funktion ihres Handys nicht ausschalten, wenn sie den Laden betreten. Ein Smartphone sucht in der Regel automatisch nach Netzen in der Nähe und schickt dem WLAN-Sender dabei eine persönliche Identifikationsnummer des Gerätes, die sogenannte MAC-Adresse. Aus der Signalstärke können die WLAN-Sender in den Läden wiederum ermitteln, wo der Kunde sich gerade befindet: Bleibt er besonders lange an der Wursttheke stehen? Traut er sich nur dann an das Regal mit den Kondomen, wenn gerade keine anderen Kunden in der Nähe sind? Oder greift er ganz schambefreit zu? Und wie oft kommt er überhaupt in den Laden? Jeden Tag? Oder nur einmal in der Woche zum Großeinkauf?

Das EHI Retail Institute aus Köln, eine Forschungsein- richtung des Handels, hat kürzlich 44 Handelsketten befragt. Zehn gaben dabei an, die Laufwege der Kunden bereits zu erfassen, 16 planen es für die Zukunft. Das Bayerische Landesamt für Datenschutzaufsicht befürchtet, dass Funksignale des Handys

auch mit anderen Informationen verknüpft werden können, etwa mit Angaben zur EC-Kartenzahlung. Dann wüssten die Händler ziemlich schnell, welches Bewegungsprofil zu welchem Menschen gehört, und statt einer MAC-Adresse, die zweimal in der Woche abends zwischen den Regalen herumirrt, sähen sie dann plötzlich: mich. Auch ganz ohne Payback-Karte.

Bei meinem nächsten Ladenbesuch achte ich darauf, welche WLAN-Netze mein Handy in der Nähe findet. Auch mein Supermarkt taucht in der Liste auf. Am Abend schleppe ich meine Einkäufe nach Hause und schalte zur Erholung Netflix ein. Der Streamingdienst kennt meine Vorlieben schon sehr genau – und schlägt mir „Black Mirror“ vor, eine Serie, die oft von den Überwachungsmöglichkeiten der nahen Zukunft erzählt. Ich nehme mir vor: Von nun an stelle ich das Smartphone öfter aus, sobald ich aus dem Haus gehe.