Passwort: Wir sind der Staat

Zugriffe der Polizei auf Daten Dritter, Teil 2

> Im ersten Teil der Serie (RHZ 1/12) hatten wir nach ein paar allgemeinen Betrachtungen diskutiert, wie sich verschiedene Staaten Zugriff auf von privaten Stellen gesammelte Daten von Flugreisenden verschaffen. In dieser Ausgabe soll es wieder Mal um Telekommunikation gehen, und zwar speziell um „Bestandsdaten“ – also die Zuordnung von Telefonnummer, E-Mail- oder IP-Adresse zu einfahrbaren Menschen – und auch ihre Passwörter. Für Auskünfte in diesem Bereich gibt es in der BRD eigens eine Stelle, die Informationen zahlreicher privater Stellen für die Behörden bündelt. Weil das so prima geklappt hat, wurde das Modell auch gleich für die Bestandsdaten der Banken übernommen, was noch Thema TFTP überleitet: Wer weiß, an wen ihr letztes Jahr überwiesen habt?

Während polizeilicher Zugriff auf Verkehrsdaten (wer mit wem wann von wo?) und Inhalte („Abhören“) im Telekommunikationsbereich immerhin noch von Gerichten abgenickt werden muss, sind Bestandsdaten (Name, Adresse, Kennung, ggf.~Passwort usf, also alles, was sich nicht so schnell ändert) im Wesentlichen ungeschützt. Als der Gesetzgeber den einschlägigen §111 Telekommunikationsgesetz verabschiedete, wollte er offenbar das Telefonbuch und den Service der damaligen Bundespost, Namen zu Telefonnummern zu liefern, ins deregulierte Telekomwesen hinüberretten. Der Paragaph verlangt von Telekoms, Namen, Anschriften und Geburtsdaten ihrer Kunden zu erfassen und sie mit Kennungen (also etwa Telefonnummern oder Mailadressen) zu verknüpfen. Zweck: Nutzung durch „Sicherheitsbehörden“ „zur Erfüllung ihrer gesetzlichen Aufgaben“ (§112). Dabei reichen bei der Abfrage nach Wunsch auch „unvollständige Abfragedaten“, auch eine „Ähnlichenfunktion“ ist vorgesehen, womit gemeint ist, dass doch bitte bei Mayer auch noch alle Meyers und Mayrs kommen sollen und Frau Warminski-Leitheußer auch dann noch, wenn nur „irgendsoeine -ski mit Doppelnamen“ reinkommt.

Tatsächlich genehmigt sich der Staat noch einen tieferen Schluck aus der Datenpulle, indem er in §113 TKG gleich noch alle, die „gewerbsmäßig“ irgendeine Telekommunikation vermitteln – das wären dann auch Internetcafes oder die Rechenzentren etwa von Unis – verpflichtet, im „manuellen Verfahren“ auf Wunsch Daten über ihre Nutzer_innen zu liefern (und diese natürlich erstmal zu speichern). Dabei sollen, wo vorhanden, z.B. auch Bankverbindungen (klasse zum Weiterverknüpfen!) oder „Partnernummern“ an die Polizei gehen. Während die großen, öffentlichen Telekoms, die über die Netzagentur abgefischt werden, noch nicht mal selbst wissen, welche ihrer Daten im Sumpf der Staatssicherheit verschwinden, sind die kleinen Klitschen einfach nur zu Stillschweigen über staatliche Verfolgung verpflichtet. So lieben wir den Rechtsstaat.

Telefonbücher bis zum Abwinken

Bei der Verabschiedung des TKG ist die Regierung von atemberaubenden 400000 Stellen ausgegangen, die auf diese Weise verpflichtet werden, und das war 2004. Schon dabei hätte deutlich werden müssen, dass solche Anfragen nicht mehr viel mit „im Telefonbuch nachsehen“ gemein haben; speziell bei Mailadressen oder Nicknames auf Webseiten findet eine Deanonymisierung vorher jedenfalls potenziell anonymer oder pseudonymer Kommunikation statt. Der Zugriff auf Passwörter und Ähnliches ist natürlich noch einmal eine Dimension furchtbarer; immerhin verpflichtet das Gesetz nicht zu deren Speicherung. Das ist nützlich, denn gute Praxis ist, nicht das Passwort zu speichern, sondern nur genug, um die Kenntnis des Passworts prüfen zu können.

Die ganz technikscheuen Abgeordneten mögen all das nicht überrissen haben, die AutorInnen des Gesetzes

wollten aber, ihren öffentlichen Äußerungen nach zu urteilen, genau diese Sorte von universellem Zugriff auf Daten der Bürger_innen haben.

Bei der Gelegenheit wollen wir nicht versäumen, darauf hinzuweisen, dass die Telekoms mitnichten *verpflichtet* sind, eine Kopie des Personalausweises anzufertigen, wenn sie Dinge wie SIM-Karten verkaufen. §95 Abs. 4 erlaubt das zwar, verlangt es aber aber nicht, Läden, die es dennoch tun, verraten ein Ausmaß an vorauseilendem Untertanengeist, das sie wirklich nicht als Transporteure für unsere Telefongespräche oder Mails empfiehlt. Bei den anderen schadet mäßiges Flunkern nicht, aber vergesst nicht, dass über Kontonummern „harte“ Zuordnungen mühelos möglich sind.

Abfragen von Telekommunikations-Bestandsdaten haben ein gewaltiges Ausmaß angenommen. Anfang der 90er Jahre waren es schon etliche 100000 pro Jahr, 2008 haben die Behörden 26.6 Millionen Datensätze zu 4.2 Millionen Anfragen bekommen – das heißt, dass im Mittel keine zehn Sekunden zwischen zwei Abfragen vergehen.

Das Verfassungsgericht findet diese Machenschaften in einem Beschluss vom Januar 2012 nicht per se schlimm, da es weitgehend weiter der Illusion vom erweiterten Telefonbuch anhängt und es im Übrigen dem Staat viel Freiheit zur Befriedigung seiner Sicherheitsbedürfnisse zugesteht. Diese Einschätzungen sind um so verblüffender, als dem Gericht nicht entgangen ist, dass die Polizei auf diese Weise Mobiltelefone ebenso wie Mailboxen aufmachen kann und das, was sie darin findet, in aller Regel nicht durch das Telekommunikationsgeheimnis abgedeckt ist. Alles, was das höchste Gericht auszusetzen hatte, war die große Leichtigkeit, mit der das geht. Es würde lieber die eine oder andere Hürde eingerichtet sehen, etwa zur Abfrage von Passwörtern. Angesichts der durchschlagenden Wirkung anderer Richtervorbehalte ist das schon fast rührend naiv, zumal dem Bundestag auch bis zum 30.6.2013 Zeit gegeben wird, die „formell den verfassungsrechtlichen Anforderungen“ nicht entsprechenden Regelungen nachzubessern.

Nochmal im Klartext: Der Zirkus mit PINs durchprobieren in jedem zweiten Tatort ist Quatsch. Die Polizei kann sich auf Zuruf von der Bundesnetzagentur die PIN holen, mit der die SIM-Karte ausgeliefert wurde. Die PIN könnt ihr zwar ändern, aber dann kann die Polizei mit der PUK kontern, und die ist von den Telekoms fest vergeben. Wenn euer Telefon also der Polizei in die Hände fällt, schützt die PIN nicht. Wenn die Polizei ein Telefon mit der PUK aufgemacht hat, ist aber normalerweise die PIN verstellt.

Bankdaten

Die Sache mit der Bundesnetzagentur als Auskunftsstelle für von Privaten gehaltene Daten hat sich so gut bewährt, dass auch gleich die Kontenauskunft so organisiert wurde. Dabei geben die Banken der Bundesanstalt für Finanzdienstleistungen (BaFin) Zugriff auf einen Teil ihrer Kundendateien, und wieder wissen die Banken nicht, was die BaFin so für die Polizei – und inzwischen zahlreiche andere Ämter – recherchiert. Als das Verfassungsgericht 2007 etwas überraschenderweise das ganze Auskunftsverfahren absegnete, war diese Heimlichkeit ein wesentliches Argument; das bestehende Verfahren sei „milderes Mittel“ gegenüber vielen Einzelanfragen an die Banken, die so Kenntnis von Verdachtsmomenten gegen ihre Kund_innen erhalten würden. Schade, dass die Richter_innen nicht auf eine dritte Alternative – überhaupt mal weniger Anfragen – gekommen sind.

Die übertragenen Daten sind zunächst überschaubar: Name, Adresse und Geburtstag des_r Kontoinhaber_in, die Kontonummer und Daten von Eröffnung und Auflösung (die Daten sind nach Auflösung eines Kontos noch drei Jahre in staatlichem Zugriff). Die Polizei bekommt also in diesem Verfahren weder Auskunft über den Kontostand noch über Kontobewegungen. Das ist insofern beruhigend, als sie so nicht z.B. mit dem Argument der Vorbeugung von Straftaten alle Spender_innen für ein neues Autonomes Zentrum erfragen kann (oder auch die Mitglieder der RH, die per Überweisung zahlen). Immerhin sind aber auch die so zu bekommenden Daten süß genug. 2011 kamen von den Repressionsbehörden fast 100000 Anfragen (davon ein gutes Viertel von den Staatsanwaltschaften), eine runde Verdreifachung seit 2004.

Will die Polizei Einblick in Details von Konten (also etwa Kontostand oder -bewegungen) nehmen, braucht sie ein Strafverfahren; in dessen Rahmen sind auch Angestellte von Banken vor Gericht auskunftspflichtig, und Banken genießen keinen besonderen Schutz vor der Beschlagnahme ihrer Daten. Es scheint eingespielte Praxis zu sein, dass Gerichte einen Durchsuchungs- und Beschlagnahmebeschluss androhen und die Banken das nicht gerade vertrauensfördernde Durchrockern des SEK durch die Schalterräume durch Auslieferung der gewünschten Daten abwenden.

Die Masche wurde bereits 1997 durch den Bundesfinanzhof offiziell geadelt. Wie oft das in der Praxis passiert, wissen wir nicht.

Beginnend mit dem Ottokatalog wurden diversen Geheimdiensten Zugriffsrechte auf Überweisungsdaten eingeräumt. Zwischen 2002 und 2009 kamen aber gerade mal 84 Anfragen. Warum die Chefspione nicht eifriger sind, ist unklar.

Her die internationale Überweisung

Richtig fleißig sind hingegen Geheimdienste der USA. Sie haben nach 9/11 das Terrorist Finance Tracking Program (TFTP) aus der Taufe gehoben. Dabei suchten die dortigen Behörden in den Überweisungdaten vor allem der Firma SWIFT nach Hinweisen auf, nun, irgendwas. SWIFT und ein paar andere Läden dieser Art wickeln internationale Überweisungen ab. Das Absaugen entsprechender Daten aus den Rechnern von SWIFT lief einige Jahre, bevor den EU-Staaten auffiel, dass die USA hier ein bisschen viel abschnorcheln könnten (und dass sie selbst auch sowas haben wollen).

Als SWIFT zusagte, dass europäische Daten in Europa bleiben könnten, ließen sich die USA auf Verhandlungen mit der EU ein; im Ergebnis dürfen die USA Überweisungsdaten nach bestimmten Kriterien bestellen und dann für 5 Jahre speichern sowie nach Belieben („zur Abwehr von Terrorismus und schweren Verbrechen“) verwenden. Dafür darf Europol die Bestellungen ansehen, und europäische Behörden bekommen „Erkenntnisse“ aus TFTP zurück, wenn die US-Behörden das opportun finden.

Das ganze Programm wird von einer Aura der Geheimhaltung umschwebt, die vermuten lässt, SWIFT seziere regelmäßig Aliens. Bekannt ist aber, dass aus den USA jeden Monat eine Sammelanfrage kommt, die für den nächsten Monat alle Überweisungen bestellt, die bestimmten, vermutlich wohl vor allem geographischen, Kriterien entsprechen und dann wohl jeweils rund eine Million Datensätze übertragen werden. Selbst wenn ihr also im EU-Ausland wohnt, dürfte eure Überweisung des RH-Beitrags den US-Behörden im Normalfall verborgen bleiben (es gab aber auch schon Ausnahmefälle).

Noch halten sich die zurückfließenden „Hinweise“ in Grenzen – in den ersten 6 Monaten TFTP (2010/11) kamen 84 in der EU an. Währenddessen kommen EU-Behörden allmählich auf den Geschmack und fragen die USA immer öfter nach „Erkenntnissen“ aus Kontobewegungen. Die letzten veröffentlichten Zahlen lagen aber immer noch unter 10 Anfragen im Monat.

Konsequenterweise plant die EU nun ihr eigenes System unter dem Arbeitstitel TFTS. Die Details sind noch umstritten, klar sind vorläufig nur zwei Punkte. Erstens, dass auch dieses System vor allem Überweisungen betreffen wird, die reputierliche Menschen kaum machen – für die nämlich soll ja das Bankgeheimnis gewahrt bleiben, damit mit dem Bruttosozialprodukt nichts anbrennt. Und zweitens, dass auch TFTS in der Liga von Spezialdemokratie spielen wird, die Konstrukte wie den Artikel 15 aus dem TFTP-Abkommen hervorbringt, wo steht: „Jede Person hat das Recht, frei und ungehindert und ohne unzumutbare Verzögerung auf Antrag in angemessenen Abständen über ihre Datenschutzbehörde in der Europäischen Union zumindest eine Bestätigung darüber zu erhalten, dass alle erforderlichen Überprüfungen durchgeführt wurden.“

Geschäftsgeheimnisträger_innen können so schon mal ihren Weg nach Brüssel planen. Sie haben auch schon, etwa durch die deutsche Delegation beim Rat – also eigentlich Regierungsvertreter –, die nach Mauern bei Informationen über TFTP durch Kommission, Europol und BRD-Innenministerium, in EU-Drucksache 6266/11 folgende Rakete losgelassen hat: „Germany is deeply concerned about this information policy. Repeatedly sidestepping questions or not answering them at all will raise further questions and add to growing scepticism.“

Aus Diplomatesisch übersetzt heißt das: „Ihr habt vollständig ein Rad ab.“ Wenn sogar die das sagen...

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a