GLOBAL 28.08.2017 | André Rebentisch

Seele verloren? Überprüfen Sie Ihre Systemeinstellungen

Der Datenschutz muss dringend verbessert werden.

Im Juni 2017 standen beim Cloud-Anbieter Amazon Web Services die personenbezogenen Daten von 198 Millionen registrierten amerikanischen Wählern offen im Internet. Dieses Riesendatenleck schaffte es sogar in die Hauptnachrichten. Längst vergessen ist, dass bereits im Dezember 2015 der texanische Sicherheitsexperte Chris Vickery anderweitig 191 Millionen Datensätze von amerikanischen Wählern frei zugänglich im Netz fand.

Es ist fraglich, ob eine sichere Verwahrung von Massendaten in der Praxis überhaupt möglich ist. In der Datenverarbeitung sind Pannen kaum zu verhindern und haben komplexe Ursachen. Womöglich hatte der Cloud-Anbieter Amazon nach den akzeptierten Regeln der Kunst gar nichts falsch gemacht. Dennoch bleiben wir mit zwei größtmöglichen Pannen in relativ kurzen Zeitabständen konfrontiert. Wenn Daten über 198 Millionen Personen an einem einzigen Ort liegen, dann beeinträchtigen die Folgen einer einzigen Panne eben auch bis zu 198 Millionen Menschen.

Es ist fraglich, ob eine sichere Verwahrung von Massendaten in der Praxis überhaupt möglich ist.

In Europa hat der Datenschutz, d.h. der Schutz personenbezogener Daten nach dem Grundsatz der informationellen Selbstbestimmung, den Rang eines Bürgerrechts. Weil sich aber das an und für sich gute Prinzip der Datensparsamkeit, d.h. dass man nur so viele Daten speichert wie für die jeweilige Anwendung unbedingt nötig sind, immer schwerer umsetzen lässt und Datenlecks nicht vollständig vermeidbar sind, werden Daten inzwischen „pseudonymisiert“. Pseudonymisierung ist der politisch korrekte Terminus für das Versprechen einer Anonymisierung, das aber nicht unbedingt eingehalten werden kann:

Heute sind verdeckte Identitäten oftmals enttarnbar. Seit es die sogenannte reverse bzw. umgekehrte Bildersuche gibt, hat beispielsweise der schwarze Balken vor den Augen ausgedient. Reale Personen sind erschreckend leicht zu identifizieren, wenn viele pseudonyme Datenquellen zusammengeführt werden. Das funktioniert ähnlich wie die Rasterfahndung bei der Polizei.

Die App-Industrie spitzt das Problem zu: Aus dem „Netz zum Mitmachen aller“ wurde das „Netz zum Abfischen der Daten aller“: Das Finanzierungsmodell der App-Ökonomie basiert auf der Preisgabe von personenbezogenen Daten. Darüber hinaus sammeln unsere Smartphones sehr genaue Standortdaten und wissen oft mehr über unsere Lebensgewohnheiten als wir selbst.

Die EU versucht nun mit der ab Mai 2018 gültigen Datenschutz-Grundverordnung, die gravierenden Lücken des bestehenden Datenschutzrechts in Europa zu schließen. Auf den ruinösen Standortwettbewerb zwischen EU-Staaten im Binnenmarkt, die den bei ihnen ansässigen Datenkonzernen ein geringeres Schutzniveau anbieten, antwortet Europa mit der Zentralisierung des Rechts und härteren Strafen. Derzeit arbeitet der europäische Gesetzgeber zudem an einer Modernisierung des Online-Datenschutzes: Die sogenannte ePrivacy-Verordnung soll 2018 zeitgleich mit der Grundverordnung in Kraft treten. In dieser Spezialgesetzgebung geht es um elektronische Kommunikation, um Chat-Apps wie WhatsApp, die die SMS inzwischen abgelöst haben, unerwünschte elektronische Werbebotschaften und die Verfolgung von Nutzern mithilfe von Browser-Cookies.

Das Finanzierungsmodell der App-Ökonomie basiert auf der Preisgabe von personenbezogenen Daten.

Diese gesetzgeberischen Projekte aber werden kaum ausreichen, um den Bürgerinnen und Bürgern Europas die Kontrolle über ihre Daten zurückzugeben, solange das Finanzierungsmodell der App-Ökonomie auf dem Untergraben unseres Datenschutzes beruht. Denn die technischen Neuerungen der App-Ökonomie haben den Datenschutz bereits substanziell geschwächt, und der Gesetzgeber kommt bei dem Tempo der technischen Entwicklung einfach nicht

schnell genug hinterher. Deshalb muss die Gesetzgebung in erster Linie mehr zügig als perfekt allgemeine und zukunftsfähige Prinzipien festlegen.

Neben gesetzlichen Lösungen für wirksameren Datenschutz aber gibt es weitere Ansatzpunkte, die in Betracht zu ziehen sind. Ich will drei nennen:

Oft wählen Nutzer eine für sie bequeme technische Lösung und produzieren damit Nebenwirkungen für andere. Mit dem kostenfreien elektronischen Geburtstagskalender beispielsweise teilen wir die Geburtsdaten unserer Freunde, in sozialen Medien die Bilder ihrer Geburtstagsparty. Selbst der Europäische Rat setzt auf seiner Website die Analytics Software von Google ein. Damit kann der Rat leichter seine Website auf seine Nutzer abstimmen. Der Preis dafür aber liegt in der Weitergabe der Kommunikationsdaten von Bürgern mit dem Online-Portal einer staatlichen Institution. Diese Daten bekommt ein Unternehmen, das als Nebenprodukt seiner Ausforschung für angepasste Werbung auch nachrichtendienstlich verwertbare Erkenntnisse erlangt und mit Daten aus anderen Quellen zusammenführt. Für den Europäischen Rat und die Privatwirtschaft sind solche Angebote bequem, aber es gibt auch Alternativen. Es wäre, erstens, wichtig und vorausschauend, diese Alternativen zu stärken.

Zweitens bieten Maßnahmen des „technischen“ Datenschutzes ein großes und bislang noch weitgehend brachliegendes Potenzial. Insbesondere benötigen Software-Entwickler Referenzsysteme, Beratung und Anleitung, um ihre Systeme leichter datenschutzfreundlich zu gestalten. Derzeit erscheint Entwicklern die Rechtslage zum Teil unklar und nicht eindeutig. Statt es Entwicklern zu überlassen herauszufinden, wie sie gesetzeskonform oder datenschutzfreundlich handeln können, sollte man es ihnen vormachen. Sehr wertvoll für Entwickler sind solide Referenzimplementierungen von Standardsituationen in den gängigen Entwicklungssprachen, mit denen sie auf der rechtssicheren Seite stehen. Nur wenn Behörden vormachen können, wie gerichtsfeste Software-Implementierungen oder Datenschutzerklärungen aussehen, lässt sich das Kunststück auch dem Markt zumuten.

Drittens könnten öffentliche Stellen mit technischen Eingriffen an Schlüsselstellen noch weitreichender als der Gesetzgeber den Datenschutz fördern. Von den meisten infrastrukturellen Basistechnologien des Netzes existieren nur wenige praxisrelevante Lösungen. Für Webserver zum Beispiel gibt es nur zwei bis drei relevante Varianten am Markt. Die Standardeinstellungen dieser Basislösungen

sind ein mächtiger Hebel, die technischen Standards ein anderer. Was hält die EU-Kommission ab, über einen Normungsauftrag die Industrie anzustoßen, durch europäische technische Standards mehr Privatsphäre zu gewährleisten? Für den Schutz der Privatsphäre sollte die öffentliche Hand zudem die Entwicklung insbesondere von quelloffenen Basistechnologien mit Forschungsaufträgen, Kooperationen und anderem Engagement fördern.

Die nachhaltigste Aufweichung unserer Daten-Grundrechte droht aktuell aus der Handelspolitik.

Die nachhaltigste Aufweichung unserer Daten-Grundrechte droht aktuell aus der Handelspolitik. Auf diesem Feld werden derzeit Vorschläge verhandelt, bei denen sich der Gesetzgeber binden soll, auch in Zukunft sinnvoll erscheinende Maßnahmen zu unterlassen, die den freien Fluss der Daten erschweren könnten. Auf dem Spiel steht das Recht des Staates, datenschutzfördernd einzugreifen. Das E-Commerce-Kapitel des geplanten Dienstleistungsabkommens TiSA beispielsweise liest sich wie ein Verbotskatalog von sachgerechten staatlichen Maßnahmen für eine Post-Snowden-Ökonomie, allen voran die kontroversen Verbote einer Offenlegungspflicht für Quellcodes in der staatlichen Beschaffung und einer Datenlokalisierung, d.h. einer „Standortpflicht“ für Daten (man stelle sich z.B. vor, estländische eGovernment-Daten würden in der Cloud gespeichert, der Cloud-Anbieter hat das Rechenzentrum in Russland angesiedelt und es kommt zu politischen Spannungen zwischen den beiden Ländern).

Dahinter steht unter anderem die Zukunftsangst transatlantisch operierender Digitalkonzerne. Wir wissen etwa, dass die höchst sensiblen SWIFT-Daten über den europäischen Zahlungsverkehr, die in ein Rechenzentrum in den USA gespiegelt wurden, dort ungefragt zur Terrorbekämpfung staatlich ausgewertet wurden. Politisch sehr delikat, denn mit SWIFT-Daten ist Industriespionage und politische Erpressung in ungeahnten Ausmaßen möglich.

Nachdem der Europäische Gerichtshof im Fall Schrems die Safe-Harbor-

Erklärung einkassiert hat, welche die Abflüsse von Daten der EU-Bürger in die USA ermöglichte, hat die Europäische Kommission zügig mit der Obama-Administration ein neues „Privacy Shield“-Abkommen geschmiedet. Viele Beobachter rechnen damit, dass auch dieses neue Provisorium gerichtlich gekippt wird – erst recht seitdem Präsident Trump die Zusagen seines Amtsvorgängers nicht umsetzen möchte.

Ohne ein derartiges Abkommen aber wird das Abfließen personenbezogener Daten aus Europa in die USA ungesetzlich, mit sehr teuren Folgen für transatlantisch operierende Konzerne. Deshalb wird nun vorsorglich versucht, alle Einschränkungen des Datenflusses, auch durch den Datenschutz, als angebliche nicht-tarifäre Handelshemmnisse zu bannen. Europa wäre schlecht beraten, aus handelspolitischer Rücksichtnahme unvernünftige Einschränkungen wie das eCommerce-Kapitel von TiSA oder gleichlautende Bestimmungen im Japan-EU-Abkommen anzunehmen, die sich wie ein Betonring um die Gestaltungsmacht unserer Regierungen legen würden.

In Zukunft werden wir uns mehr Gedanken um die gesellschaftlichen Chancen und Risiken der Datenkartelle machen müssen. Es zeigt sich, dass es längst kein ausreichender Ansatz mehr ist, den Datenschutz der „eigenverantwortlichen“ Zustimmung der einzelnen Nutzer zu überlassen. Bereits heute tricksen App-Entwickler die Anwender aufwändig aus, damit sie ihre Zustimmung zu jeglicher Datenverwendung geben. Zahlreiche Witzbolde haben in den Allgemeinen Geschäftsbedingungen verschiedener Apps die Nutzer um die Abtretung der Rechte an ihrer unsterblichen Seele gebeten, und diese bestätigten routinemäßig den Teufelspakt. Eine digitale Bildungsarbeit und Verbraucheraufklärung wird daran strukturell wenig ändern, denn die Nutzer handeln oft sehenden Auges. Ihr Bürgerrecht auf Datenschutz kaufen ihnen die Unternehmen einfach ab, die Seele gibt es gratis dazu.

André Rebentisch
Berlin

André Rebentisch arbeitet als Software-Berater in Berlin zu

Conversational Interface Technologie. Für Kleine und Mittlere Betriebe der digitalen Wirtschaft hat er die europäische Gesetzgebung in Brüssel und Straßburg begleitet, darunter auch die Datenschutz-Grundverordnung, und sich an der offenen Standardisierung von Dokumentaustausch- und Kalenderdaten beteiligt. Jedes Jahr richtet er den OpenTechSummit aus, auf dem sich Entwickler und Kreative über Neuerungen austauschen.