Bild: Gage Skidmore (CC BY-SA 2.0, http://creativecommons.org/licenses/by-sa/2.0)

Alle Schotten dicht

Wie die IT-Branche auf den Sieg von Donald Trump reagiert

Der Sieg von Donald Trump bei den amerikanischen Präsidentschaftswahlen ändert die Rahmenbedingungen für IT-Sicherheit und Datenschutz. Die Europäer werden ihre Anforderungen an digitale Sicherheit neu definieren müssen.

Von Christiane Schulzki-Haddouti

Mit Hochdruck bringen US-Klimaforscher derzeit ihre Daten in Sicherheit. Einem Bericht der Washington Post zufolge kopieren und sichern die Wissenschaftler alle Daten, die sie in den zurückliegenden Jahrzehnten gesammelt haben. Eine auf viele Server verteilte Online-Datenbank soll als sicherer Hafen dienen.

Die Wissenschaftler befürchten, dass die Leugner des menschengemachten Klimawandels, die Trump in sein Kabinett holen will, ihre Arbeit sabotieren werden. Das US-Energieministerium weigert sich sogar bislang, Trumps Übergangsteam die Namen der Mitarbeiter mitzuteilen, die bislang für das Thema Klimawandel zuständig sind. Die Klimaforscher sehen Verfügbarkeit und Integrität ihrer Daten in Gefahr.

Bei dieser Auseinandersetzung geht es nicht darum, wem die Daten gehören, sondern darum, wer die Kontrolle über ihre Speicherung und Verarbeitung ausübt, wer also die Macht über diese Daten hat. Dieser Streit zwischen Wissenschaftlern und Vertretern der neuen Regierung ist im bevorstehenden Umbruch allerdings nur eine Randerscheinung. Inzwischen geht es ums Ganze.

Datenminimierung und Nichtverkettung

Zum Datenschutz gehören nicht nur Integrität und Verfügbarkeit. In Gefahr sind auch die Datenminimierung, also das Prinzip, nur das unbedingt Nötige zu speichern, sowie die Nichtverkettung, also die grundsätzliche Einschränkung der Rechte zur Verarbeitung, Nutzung und Übermittlung.

Die von Trump angekündigte Einrichtung eines Melderegisters für US-Bürger muslimischen Glaubens ist derzeit der ethische Lackmustest für amerikanische IT-Unternehmen. Für die Betroffenen stellt die Aufnahme in ein solches Register eine massive Bedrohung dar. Der desig-

nierte Präsident hat im Wahlkampf angekündigt, die Bürgerrechte von Muslimen zu beschneiden und sie massenhaft auszuweisen.

Das Online-Magazin „The Intercept" fragte neun große IT-Unternehmen, ob sie ihre Daten für die Errichtung einer solchen Datenbank beisteuern oder ob sie an einer Ausschreibung teilnehmen würden. Twitter lehnte sofort und klar ab; Microsoft bezeichnete die Diskussion als „hypothetisch" und wand sich damit um eine klare Antwort herum. Facebook, Google, Apple, IBM und Uber möchten mit dieser Datensammlung ebenfalls nichts zu tun haben.

Die Ablehnung der Unternehmensführungen fiel nicht besonders deutlich aus. An der Basis der Unternehmen herrscht deswegen Unruhe: 60 Angestellte größerer Tech-Unternehmen unterzeichneten vor einem Treffen zwischen Silicon-Valley-Größen und Donald Trump Mitte Dezember auf http://neveragain.tech eine gemeinsame Absichtserklärung, in der sie eine Beteiligung am Aufbau des Melderegisters ablehnen. Sie kündigen an, eher von ihrem Posten zurückzutreten als an einem Missbrauch der Daten mitzuarbeiten.

Das New York Magazine arbeitete heraus, dass die IT-Industrie die meisten Aufgaben im Zusammenhang mit einem solchen Melderegister bereits erledigt habe. Google und Facebook könnten mit Big-Data-Analysen technisch bereits heute eine Zuordnung ihrer Nutzer vornehmen. Wer während des Ramadan Sonnenaufgangs- und -untergangszeiten googelt, ist wahrscheinlich Muslim, wer das Datum von Hannukah suche, wohl Jude, und wer regelmäßige Kalendereinträge für einen Bibelkreis hat, vermutlich Christ. Je mehr Datenpunkte zur Verfügung stehen, desto sicherer fällt das Ergebnis einer solchen Analyse aus.

Verschlüsseln für die Vertraulichkeit

Ein weiterer Streitpunkt zwischen Trump und dem Silicon Valley ist die Kryptofrage. Die Auseinandersetzung zwischen Apple und der US-Bundespolizei FBI um die Entschlüsselung eines iPhone ist noch lange nicht vom Tisch. In dieser Debatte geht es grundsätzlich um die Schutzziele der Vertraulichkeit und Integrität persönlicher Kommunikation sowie um die Transparenz staatlichen Handelns. Sie wird sicherlich mit einem neuen Fall wieder aufflammen, und dann wird es ums Ganze gehen und nicht nur um ein Smartphone eines bestimmten Herstellers. Trump hat in dieser Frage längst Position bezogen: Seiner Ansicht nach müssen IT-Unternehmen Strafverfolgern grundsätzlich Zugang zu verschlüsselten Informationen verschaffen.

Die Internet Association, eine Interessenvertretung der US-amerikanischen Internet-Industrie, schrieb Donald Trump unmittelbar nach seiner Wahl einen offenen Brief. Darin erinnerte sie ihn vorsorglich daran, dass eine starke Verschlüsselung entscheidend für die nationale und auch die persönliche Sicherheit sei. Sie bewahre kritische Infrastrukturen vor Angriffen und ermögliche es, Bürger vor repressiven Regierungen zu schützen. Wenn Gesetze Hintertüren für Sicherheitsbehörden erzwängen, sei das für die Sicherheit kontraproduktiv.

Schutz vor Massenüberwachung

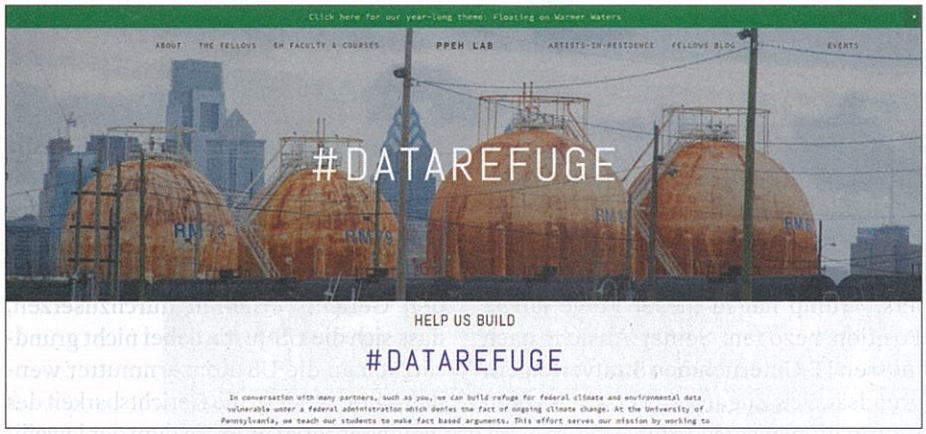
Die Lobby-Organisation mahnte eine weitere Reform der NSA-Befugnisse an und forderte, auch Ausländer vor Massenüberwachung zu schützen. Internationale Rechtshilfeabkommen, die Strafverfolgern den geordneten Zugriff auf Daten in den USA erleichtern, seien gleichwohl notwendig. Sehr wahrscheinlich, und das ist wohl auch die Befürchtung der Internet Association, wird sich die IT-Sicherheitspolitik unter Trump aber genau in die entgegengesetzte Richtung entwickeln: IT-Unternehmen müssten dann beispielsweise Hintertüren für US-Sicherheitsbehörden einbauen. Dabei kann der US-Geheimdienst NSA bereits heute so gut wie jede Kommunikation entschlüsseln. Seit den Snowden-Enthüllungen dürfen sämtliche Plattformen und Dienste als kompromittiert gelten.

Wenn Sicherheitsbehörden anderer Länder auf Daten in den USA zugreifen wollen, müssen sie sich auf Rechtshilfeersuchen stützen. Die Bearbeitung solcher Anträge nimmt in den USA Monate, manchmal sogar Jahre in Anspruch. Macht Trump seine Ankündigung wahr und setzt seine America-First-Doktrin durch, werden solche Anträge künftig willkürlich nach Opportunität bearbeitet. Umgekehrt wird sich aber die US-Justiz Zugang zu den Servern der US-Unternehmen beschaffen wollen, egal wo auf der Welt diese stehen.

Microsoft versucht in einem laufenden Gerichtsverfahren durchzusetzen, dass sich die US-Justiz dabei nicht grundsätzlich an die US-Konzernmutter wenden kann, sondern die Gerichtsbarkeit des Landes anrufen muss, in dem der jeweilige Server steht. Trump könnte versuchen, die gegenwärtige Rechtslage noch mehr zugunsten des Durchgriffs der amerikanischen Justiz zu verändern.

Für Microsoft stehen in dieser Frage Großaufträge in Europa auf dem Spiel. Niemand wird einem Unternehmen Daten anvertrauen, wenn diese jederzeit an US-Behörden abfließen könnten. Das US-Unternehmen hat sich daher entschlossen, als Treuhänder für die Daten ihrer Cloud-Dienste wie Office 365 die Deutsche Telekom einzusetzen. Damit zwingt Microsoft die US-Justiz, den bereits etablierten, aber mühsamen Weg über offizielle Rechtshilfeersuchen zu gehen. Die Alternative

Der niederländische Datenschützer John Borking stellte gemeinsam mit der kanadischen Datenschützerin Ann Cavoukian 1995 erstmals das Konzept der „Privacy Enhancing Technologies" (PETs) in Kopenhagen vor. Cavoukian prägte ein paar Jahre später den Begriff des „Privacy by Design".



Die Universität von Pennsylvania fürchtet um die Verfügbarkeit und Integrität ihrer in Jahrzehnten gesammelten Klimadaten und baut einen Datenbunker.

wäre gewesen, die Daten derart zu verschlüsseln, dass Microsoft technisch keinen Zugriff darauf hätte.

Mit seinen Maßnahmen erfüllt Microsoft grundlegende Sicherheitsanforderungen deutscher Unternehmen und Behörden. Privatanwender bleiben aber im Zugriff der US-Behörden: Die Dateien der Online-Festplatte OneDrive liegen nicht auf Telekom-Servern. Andere Anbieter wie Amazon, Google oder Dropbox bleiben in diesem Punkt weit zurück und verweisen lediglich darauf, dass sie auch Rechenzentren in Deutschland betreiben. Sicher vor dem Zugriff durch US-Behörden sind die Daten allein dadurch jedoch nicht.

Wie gering Donald Trump den Datenschutz schätzt und wie wenig er einen Cyberwar fürchtet, kann man an seinen Äußerungen ablesen: Er hoffe, dass Russland rund 30.000 E-Mails von Hillary Clinton „finden" werde, hatte er im Wahlkampf getönt.

Europäische Gegenmaßnahmen

Die Europäer werden sich bald entscheiden müssen, wie streng sie ihre Schutzanforderungen gestalten wollen. Im digitalen Raum gehört dazu zentral der Datenschutz mit seinen sieben Gewährleistungszielen. Das sind Verfügbarkeit, Integrität und Vertraulichkeit als klassische Ziele der IT-Sicherheit sowie Datensparsamkeit, Nichtverkettung, Intervenierbarkeit und Transparenz als daraus abgeleitete Datenschutzziele. Trump attackiert sie alle.

Ein wichtiges Gegengewicht ist die Europäische Datenschutzgrundverordnung, die 2018 in Kraft tritt. Sie verlangt von Hard- und Software-Herstellern sowie Datenverarbeitern, diese Ziele mit technisch-organisatorischen Maßnahmen umzusetzen. „Privacy by Default" und „Privacy by Design" sind künftig die Grundlagen für Datenschutz in Europa.

An der Entscheidung für oder gegen bestimmte technische Lösungen wird man ablesen können, wie ernst es den Europäern mit dem Datenschutz wirklich ist. Eine Ende-zu-Ende-Verschlüsselung verhindert wirksam, dass Dienstebetreiber beispielsweise Einblick in die Kommunikation erhalten oder ausländischen Diensten gewähren können.

Ein weiteres Problem sind Systeme, die einen Login verlangen – beispielsweise um sich mit anderen zu vernetzen, um Bestellungen abzuwickeln oder staatliche Dienstleistungen in Anspruch zu nehmen. Hier werden die Nutzer oft gezwungen, unnötig viel von sich preiszugeben. Von Datenminimierung oder Nichtverkettbarkeit sind solche Systeme noch meilenweit entfernt. Datenschutz-Aufsichtsbehörden müssten für bestimmte Fälle den Einsatz von attributbasierten Berechtigungsnachweisen (ABC) verbindlich einfordern. Damit wäre es möglich, die Verkettung von Namen mit Adjektiven wie „Hautfarbe", „Alter" oder „Religion" zu unterbinden. Schon das Design solcher Systeme würde Datamining unmöglich machen, das Grundrechte verletzt.

Das dahinterstehende Konzept des „Identity Protectors" entwickelte der Niederländer John Borking bereits Mitte der 90er Jahre. Dazu motiviert hatte ihn die Geschichte: im Zweiten Weltkrieg besetzten deutsche Truppen die Niederlande – und nutzten die bestehenden Registraturen, um Juden zu finden und zu verhaften. Dabei kam die damals moderne Lochkarten-Technik von IBM zum Einsatz.

Die europäische Datenaufsicht könnte von Unternehmen auch die Implementierung von „Sticky Policies" verlangen. Diese Technik bettet Datenschutzregeln so ein, dass sie unabhängig von Speicher- und Verarbeitungsort der Daten gelten. Damit ließen sich Datenströme und Sicherheitspräferenzen anbieterübergreifend steuern. Der Softwarehersteller SAP hat solche Systeme bereits erfolgreich getestet. Die Größe der Installation ist letztlich eine Frage des Speicherplatzes und der Rechenkapazität. Der Soft- und Hardware-Hersteller Hewlett-Packard hat bereits Konzepte für den Einsatz von „Sticky Policies" in der Cloud und für mobile Geräte entwickelt. Damit ließe sich das Schutzniveau in vielen Bereichen deutlich steigern.

Heikles Erbe

Der noch amtierende Präsident Barack Obama hinterlässt ein heikles Erbe. Er musste oft Dekrete erlassen, um sich gegen den von den Republikanern dominierten Kongress durchzusetzen. Für Trump wäre es ein Leichtes, das Rad durch einen Widerruf dieser Dekrete schnell wieder zurückzudrehen.

Auch unter der Präsidentschaft von Obama blühte die Massenüberwachung. Das geheim tagende FISA-Gericht, das für Auslandsaufklärung und Spionageabwehr zuständig ist, erlaubte regelmäßig Überwachungsmaßnahmen, die weltweit viele Anwender betrafen. Whistleblower wurden in den USA hart angefasst, ihre Position hat sich unter der Präsidentschaft von Obama in keiner Weise verbessert.

Von Trump sind keine Reformen zu erwarten. Wie sein persönliches Treffen mit den Silicon-Valley-Größen verlief, war nicht zu erfahren; um die Welt gingen lediglich Fotos von Larry Page, Tim Cook, Elon Musk und Sheryl Sandberg mit versteinerten oder mühsam beherrschten Mienen.

In wenigen Monaten steht die Überprüfung des „EU-US-Privacy-Shield" an, dem Nachfolger des vor dem Europäischen Gerichtshof gescheiterten Safe-Harbor-Abkommens. Ob es diese Prüfung bestehen wird, ist fraglich. Spätestens seit dem ersten Yahoo-Datenskandal steht in Zweifel, dass der Zugriff der Sicherheitsbehörden auf die Daten europäischer Bürger so zielgerichtet ist, wie es die Übereinkunft verlangt. Hinzu kommt die Ungewissheit, ob die neue US-Regierung die bestehenden Zusicherungen beibehält oder zurücknimmt. *(uma@ct.de)* c't