Wirtschafts Woche

Spionage

Amerika liest mit

von Thomas Stölzel

Google, Apple & Co. geraten immer wieder in Kritik, weil sie Nutzerdaten horten. Dabei sind die größten Datensammler amerikanische Geheimdienste, die mit immer neuen Technologien Milliarden Mails, Kurznachrichten und Web-Telefonate auswerten.

Spion
Quelle: fotolia.de

Es ist zehn Tage vor Heiligabend, als im Hauptquartier des Kurznachrichtendienstes Twitter in San Francisco ein geheimes Schreiben der US-Regierung eingeht – ein sogenannter Nationaler Sicherheitsbrief. Die Behörden fordern das Internet-Startup darin auf, die Daten einer Handvoll prominenter Nutzer auszuhändigen. Darunter die von Wikileaks-Gründer Julian Assange, der seit der Veröffentlichung geheimer Regierungsunterlagen über Nacht zum Staatsfeind Amerikas avancierte.

Die US-Regierung will nicht nur die Namen derer wissen, die regelmäßig Twitter-Nachrichten von Wikileaks verfolgen – aktuell sind das mehr als eine Million Menschen. Twitter soll auch offenlegen, wem Wikileaks-Mitglieder vertrauliche Direktnachrichten schicken.

Spionage im Namen der Terrorabwehr

Eine richterliche Anordnung brauchen die Beamten dafür nicht, das Schreiben reicht. Und der Empfänger darf noch nicht einmal darüber sprechen: Eine Geheimhaltungsklausel verpflichtet ihn zur Verschwiegenheit. Abertausende Briefe verschicken die Bundespolizei FBI und die Geheimdienste Jahr für Jahr. Abertausende Mal händigten Unternehmen die Daten widerstandslos aus. Twitter nicht. Das Unternehmen zieht gegen die Schweige-Klausel vor Gericht und bekommt recht.

Die Briefe aber, die Unternehmen zur Herausgabe der Daten zwingen, sind nur ein kleiner Baustein in einem groß angelegten Plan, das gesamte Internet zu belauschen. Mit immer neuen Techniken und Analyseverfahren überwachen die USA im Namen der Terrorbekämpfung und Spionageabwehr den Rest der Welt – so lückenlos wie nie zuvor: E-Mails, Web-Telefonate und Online-Datenspeicher, nichts ist sicher vor den Augen Amerikas.

Cloud Computing beschert den US-Behörden europäische Daten

Gerade erst verlängerte US-Präsident Barack Obama zu diesem Zweck das umstrittene Spionagegesetz Patriot Act um weitere vier Jahre. Ein Gesetz, dass den US-Geheimdiensten weitreichende Überwachungskompetenzen zusichert. Das bereitet IT-Verantwortlichen in Europa Kopfschmerzen. Denn zeitgleich verlagern immer mehr Unternehmen Daten und Software ins Internet.

Dieses sogenannte Cloud Computing ist oft billiger, weil Firmen dadurch weniger eigene Server im Keller unterhalten müssen. Laut den Marktforschern von Forrester steigt der weltweite Umsatz mit solchen Diensten von jährlich 41 Milliarden Dollar bis 2020 auf 241 Milliarden Dollar.

Zwar feilen auch Länder wie China und Russland an Netz-Spionagetechniken. Doch die Cloud-Dienste werden zu einem großen Teil von amerikanischen Unternehmen angeboten, darunter Salesforce, Rackspace, Google und Amazon.

Und die müssen auf ihren Servern gespeicherte Informationen auf Anfrage jederzeit an US-Geheimdienste abtreten – oft ohne Begründung seitens der Spione.

Cloud 3
Quelle: Nicholas Blechman

Riesiger Datenstaubsauger

Europäische Konzerne wie Daimler und Royal Dutch Shell fürchten, dass die USA auf diese Weise gesammelte Daten und Geschäftsgeheimnisse gegen sie verwenden könnten, bei internationalen Ausschreibungen zum Beispiel. "Für viele Geschäftskunden ist das ein relevanter Punkt, sie sind beunruhigt", sagt Olaf Vogel, Chefjurist der Telekom-Tochter T-Systems.

Diese Problematik haben mittlerweile sogar EU-Politiker erkannt. Liberale und grüne Europaabgeordnete forderten Anfang Juli von der EU-Kommission Aufklärung über den Schutz von Informationen. Sie wollen unter anderem wissen, ob es mit EU-Recht vereinbar sei, wenn die USA auf Daten europäischer Nutzer und Firmen zugreifen.

Auch Microsoft-Nutzer stehen im Fokus

Übertrieben ist die Vorsicht nicht. Vor wenigen Wochen erst, bei der Produktvorstellung des neuen Office 365, musste der britische Microsoft-Niederlassungsleiter Gordon Frazer zugeben, dass nicht einmal die Kundendaten auf europäischen Microsoft-Servern vor dem Zugriff der US-Behörden sicher sind: Weil Microsoft ein amerikanisches Unternehmen ist, müsse es Geheimdiensten Zugriff gewähren, selbst auf Großrechner, die im Ausland stehen.

Auch Google teilte auf Anfrage der WirtschaftsWoche mit, dass "die US-Regierung auf außerhalb der USA gespeicherte Daten zugreifen kann". Der Konzern habe schon viele solcher Anfragen erhalten. Wie wenig Internet-Nutzer von diesem Verfahren wissen, zeigte vor wenigen Wochen das Beispiel Dropbox.

Der populäre Web-Speicherdienst, auf dem weltweit 25 Millionen Freiberufler, Kleinunternehmer und Privatkunden Dokumente, Fotos und Dateien aller Art ablegen, löste einen Sturm der Entrüstung aus: Das Unternehmen hatte eine Klausel über die mögliche Datenweitergabe an Geheimdienste in seine Geschäftsbedingungen eingefügt. So groß die Empörung auch war – die Verpflichtung gilt für jede amerikanische Web-Firma.

Das Pikante daran: Selbst wenn ein Gericht nachträglich feststellt, dass eine Behörde solche Informationen unrechtmäßig beschafft hat, muss sie diese nicht vernichten. Sie werden gespeichert in einem der größten Datenarchive der Welt. Dieses gigantische Gedächtnis wird von zwei mit schwarzem Glas verspiegelten Büropalästen aus gesteuert. Hier, in Fort Meade im US-Bundesstaat Maryland, residiert die National Security Agency (NSA), der größte und finanziell am besten ausgestattete Nachrichtendienst der USA.

Jahrelang war selbst seine Existenz so geheim, dass in Washington gespottet wurde, das Kürzel stehe für "No Such Agency", kein solcher Dienst. Dabei sind seine Ausmaße gewaltig: Die NSA beschäftigt drei Mal so viele Mitarbeiter wie die CIA, hat ihre eigene Autobahnausfahrt, und allein die Stromrechnung beläuft sich Schätzungen zufolge auf jährlich 70 Millionen Dollar: Dem Dienst wird die Fähigkeit zugeschrieben, alle sechs Stunden eine Datenmenge abzuschöpfen, die der Informationsmenge der amerikanischen Kongressbibliothek entspricht – der größten Büchersammlung der Welt.

Das große Datensammeln begann nach den Anschlägen vom 11. September 2001. Damals konkurrierten ehemaligen NSA-Mitarbeitern zufolge zwei Systeme: Thinthread sollte Datenverkehr wie E-Mails oder Kurznachrichten scannen und analysieren. Mit Schlüsselwörtern ausgestattet, sollte es ausschließlich verdächtige Kommunikation speichern. Laut Thomas Drake, der mehr als ein Jahrzehnt für die NSA an solchen Projekten gearbeitet hat, gab der damalige NSA-Direktor Michael Hayden jedoch dem rivalisierenden Milliardenprojekt Trailblazer den Vorzug, einem gigantischem Datenstaubsauger.

Geheimraum im Netzknoten

In ganz Amerika installierten die Abhörspezialisten IT-Anlagen, um Daten aller Art abzufangen. Frühere NSA-Mitarbeiter gehen laut einem Artikel des Magazins "The New Yorker" davon aus, dass der Dienst inzwischen sämtliche E-Mails, die über US-Anbieter verschickt werden, kopiert und abspeichert, um sie später analysieren zu können. Darunter auch Mails, die über in Deutschland beliebte Postfächer von Google Mail, Yahoo Mail und Microsofts Hotmail laufen sowie Internet-Telefonate aus aller Welt. Zwar stoppte die NSA das Projekt Trailblazer 2006, weil der Computerexperte Drake die Details an Journalisten verraten und eine Welle der Kritik ausgelöst hatte. Drake wurde wegen Geheimnisverrats zu einer Bewährungsstrafe verurteilt.

Doch die NSA startete das nächste Datenprojekt: Schon kurz nach dem Ende von Trailblazer beauftragte sie das Technologieunternehmen Science Applications International, das schon Trailblazer entwickelt hatte, mit dem Aufbau eines Nachfolgeprogramms. Diesmal sollte es Executelocus heißen. Was genau sich dahinter verbirgt, ist bis heute nicht durchgesickert. Doch es wäre verwunderlich, wenn Executelocus technologisch schwächer ausgestattet wäre als Trailblazer.

at&t

Etwa zur selben Zeit ließ der pensionierte AT&T-Techniker Mark Klein, ein grauhaariger Mann mit Schnauzbart, rundem Gesicht und Drahtbrille, eine weitere PR-Bombe platzen. Gegenüber der für Datensicherheit und Meinungsfreiheit kämpfenden Electronic Frontier Foundation (EFF) gab Klein sensible Informationen aus seinem Berufsleben preis: Unter Eid beschrieb er die Technik, durch die der US-Telefonriese AT&T Mails und andere Daten seiner Nutzer an die NSA weiterleitet. So betreibe diese in der AT&T-Kommunikationszentrale in San Francisco einen geheimen Raum, von dem aus sie Glasfaserdatenleitungen des Telefonriesen anzapfe, berichtet Klein in der Aussage, die der WirtschaftsWoche vorliegt.

Auch Verizon soll Daten weiterleiten

Über den auf diese Weise angezapften Netzknoten in Kalifornien laufen nicht nur Telefongespräche aus aller Welt, sondern

auch ein großer Teil des internationalen Datenverkehrs sowie Internet-Telefonate zwischen Amerika, Asien und der Pazifikregion. Und das hat offenbar System: Laut der EFF betreibt die US-Regierung ein landesweites Netzwerk aus Überwachungstechnik, die direkt in die Schlüsselanlagen der Telekomunternehmen integriert ist.

Durch das Netzwerk zeichne der Geheimdienst Telefonate, Text-Nachrichten, E-Mails und andere Internet-Kommunikation auf. "Betroffen sind alle AT&T-Kunden, jeder der mit einem AT&T-Kunden kommuniziert sowie alle die, deren Daten im Web irgendwann über ein AT&T-Netz geleitet werden“, warnt die EFF. Laut der Tageszeitung "USA Today" soll auf ähnliche Weise auch AT&T-Konkurrent Verizon sein Netz für die NSA geöffnet haben.

Großkonzerne und Mittelständler geben unbewusst Daten preis

"Solche Internet-Service-Provider sind eine Schwachstelle, weil sie von der Regierung angezapft werden können", warnt ein amerikanischer IT-Manager, der nicht genannt werden will. Dies sei ein noch größeres Risiko als Nationale Sicherheitsbriefe an Rechenzentrumsbetreiber. Nicht nur Großkonzerne, auch Mittelständler geben auf diese Weise sensible Firmengeheimnisse preis, ohne es zu ahnen: Auch sie lagern immer mehr Daten bei Cloud-Diensten im Netz, warnt der Innenexperte der Unions-Bundestagsfraktion, Stephan Mayer.

Zwar verstoßen die Telekommunikationsanbieter mit ihrem Gebaren gegen US-Telekommunikationsrecht. Immer wieder versuchen Unternehmen und Privatnutzer gegen AT&T und andere Anbieter zu klagen. Doch die Verfahren verlaufen fast immer im Sande. Die US-Regierung unter George W. Bush hatte den Telefonkonzernen kurz vor Ende ihrer Amtszeit durch eine spezielle Regelung Immunität verschafft. Einer ihrer Unterstützer war auch der heutige US-Präsident Obama.

„Es ist kein technisches Problem. Man kann Daten vor unberechtigtem Zugriff schützen. Es ist ein politisches Problem“, sagt Tim Dunn, Sicherheitsmanager beim US-Cloud-Computing-Anbieter CA Technologies, an den Firmenkunden praktisch all ihre IT auslagern können. Der Brite sitzt im Lenkungsausschuss für Computersicherheit von Neelie Kroes, EU-Kommissarin für die Digitale Agenda. "Wir müssen gegenüber den USA als EU auftreten", fordert er. Derzeit mache jeder Mitgliedstaat seine eigene Datensicherheitspolitik.

Doch selbst Dunn sitzt in der Zwickmühle. Die Zentrale seines Unternehmens liegt im US-Bundesstaat New York. "Wir sind ein amerikanisches Unternehmen. Rechtlich gesehen müssen wir US-Behörden Zugang gewähren, können den Patriot Act nicht brechen", sagt er. In welcher Form die NSA auf CA-Server zugreifen kann, will er nicht sagen, weil er nicht wisse, ob dies offene oder verdeckte Operationen seien. Jedenfalls nimmt der Druck auf die Politik zu. Beim Walldorfer Softwareherstellers SAP, der seinen Kunden seit einem Jahr Betriebswirtschaftssoftware aus der Cloud anbietet, heißt es: „Plötzlich sieht man, dass hier Handlungsbedarf existiert."

Die IT-Branche klagt, dass die Unsicherheit mittlerweile den Aufstieg des Cloud Computing bremse. Viele Unternehmen trauen sich nicht, sensible Daten in externe Rechenzentren zu verlagern. Die meisten, die es doch tun, verlangen, dass ihre Daten auf keinen Fall auf US-Servern gespeichert werden. "Die Kunden reagieren aufgeklärter, stellen Fragen über die Möglichkeiten der US-Regierung und diktieren, was zu tun ist", berichtet Dunn.

Klar jedoch ist: Die Sorgen der Unternehmen sind berechtigt. In der Vergangenheit hatten die USA schon mehrfach von der NSA abgefangene Informationen gegen europäische Wettbewerber eingesetzt: In den Neunzigerjahren hörte der Dienst Telefonate des französischen Rüstungskonzerns Thomson-CSF mit Brasilien ab. Denen zufolge bestach Thomson-CSF Regierungsmitglieder, um einen Satellitenauftrag an Land zu ziehen. Amerika machte dies publik, das Geschäft erhielt US-Konkurrent Raytheon. Ähnlich erging es Airbus ungefähr zur selben Zeit bei einem Auftrag in Saudi-Arabien.

NSA fördert Startups

Als mögliche Schnittstelle zwischen NSA und US-Wirtschaft gilt seit Langem das Advocacy Center im US-Handelsministerium. Das Büro soll Regierungsressourcen koordinieren und für Chancengleichheit gegenüber ausländischen Konkurrenten bei der Vergabe internationaler Großaufträge sorgen. Die Sorge vor solchen Institutionen ist längst keine europäische Debatte mehr: Kanadische Fachmedien etwa warnen Anwälte generell davor, vertrauliche Mandantendaten auf Servern amerikanischer Anbieter zu speichern. Dort sei es unmöglich, Vertraulichkeit zu gewähren.

Auch Privatnutzer sind zunehmend betroffen, nicht nur ihre Mails landen in den gigantischen NSA-Archiven. Aufgrund der wachsenden Verbreitung von Smartphones und Tablet-Rechnern laden immer mehr Menschen persönliche Daten in populäre Web-Speicherdienste wie Evernote oder Dropbox. So sind die Informationen zwar jederzeit von jedem Gerät aus erreichbar, doch genauso einfach für US-Geheimdienste einsehbar. Und das kann Folgen haben.

Sony-Logo
Quelle: dapd

Eine paar unbedachte E-Mails und ein paar als verdächtig eingestufte Dateien könnten die NSA-Großrechner in Kombination als Bedrohung werten. Schlimmstenfalls könnte ein Mechanismus in Gang gesetzt werden, durch den der Namen des Nutzers auf einer Flugverbotsliste landet. Denn natürlich versucht die NSA die gigantischen Datenmengen auszuwerten. Und die Technologien, die dabei helfen, machen enorme Fortschritte. Mittlerweile gibt es Algorithmen, die anhand der Bewegungsprofile von Handynutzern zu prognostizieren versuchen, was sie unter bestimmten Bedingungen abends unternehmen werden. Mit ähnlichen Verfahren entschlüsseln Internet-Werber längst auch die Interessen von Nutzern im Netz.

NSA expandiert stetig

Und die NSA baut ihre Fähigkeiten immer weiter aus. Um riesige Datenmengen speichern und verarbeiten zu können, errichtet der Geheimdienst mehrere neue Rechenzentren. Im texanischen San Antonio hat der Dienst eine frühere Fabrik des Technologieriesen Sony gemietet. Dort entsteht ein 40.000 Quadratmeter großes Rechenzentrum. Im US-Bundesstaat Utah,

einen Steinwurf von der Olympiastadt Salt Lake City entfernt, entsteht ein weiterer Serverpark. Der soll eine Milliarde Dollar kosten und mehr als doppelt so groß werden wie sein Pendant in San Antonio.

Doch das ist nur ein Teil der Expansion. Um an neue Technologien zu gelangen, haben die US-Geheimdienste mit In-Q-Tel eine eigene Investmentgesellschaft gegründet, die seit 1999 Geld in junge Technologiefirmen steckt. 2009 stieg In-Q-Tel etwa in das Startup Visible Technologies ein, das Inhalte von öffentlichen Web-Angeboten wie Twitter, YouTube und unzähligen Weblogs überwachen kann, um sich anbahnende Krisen jeder Art früh erkennen zu können.

NSA spioniert auch im Ausland

In-Q-Tel steckte auch hinter der Entwicklung der Satelliten-Landkarte Key-hole, die später an Google verkauft und in Google Maps umbenannt wurde. Wo die technische Entwicklung nicht schnell genug geht, wird eben nachgeholfen. Damit entwickelte sich die von Akademikern und Elektroingenieuren bevölkerte NSA "in aller Stille in die weltweit führende Organisation für Operationen im virtuellen Raum", schreibt Richard Clarke, ein Ex-Sicherheitsberater der US-Regierung, in seinem gerade auf Deutsch erschienenen Buch "World Wide War". Die NSA habe die IT-Internet-Infrastruktur auch außerhalb der USA gründlich infiltriert, um Organisationen im Ausland auszuspionieren.

Europäische Unternehmen wollen dem nicht länger zusehen. Der britisch-niederländische Mineralölkonzern Royal Dutch Shell hat zwar Microsoft damit beauftragt, Cloud-Computing-Lösungen wie die Multifunktionsplattform SharePoint für den Unternehmensalltag einzurichten. Gespeichert werden die Daten aber nicht im nagelneuen Microsoft-Rechenzentrum in Irland, sondern in Deutschland auf Servern der Telekom-Tochter T-Systems – dort wo sie laut T-Systems sicher vor den neugierigen Augen der US-Geheimdienste sind. Einen ähnlichen Deal plant auch Daimler, heißt es in Stuttgart – selbst wenn der noch nicht in trockenen Tüchern ist.

T-Systems-Chef Reinhard Clemens wirbt inzwischen offen für eine "deutsche Cloud" – nicht ohne Eigennutz. Fühlt sich T-System doch als Betreiber einer solchen berufen. Europas IT-Firmen jedenfalls bescheren die orwellschen Zustände so in den nächsten Jahren sogar Geschäftschancen.