2013/12 Inland

https://jungle.world/artikel/2013/12/der-wolke-bist-du-nie-allein

Cloud-Computing und Datenschutz

In der Wolke bist du nie allein

Von **Elke Wittich**

Immer mehr Bürger nutzen die internetbasierte Datenspeicherung. Der Trend zum Cloud-Computing weckt Begehrlichkeiten bei den Strafverfolgungsbehörden.

26 Fragen mit bis zu zehn Unterpunkten – die Kleine Anfrage der Bundestagsfraktion der Linkspartei zum Thema »Sicherheit, Datenschutz und Überwachung von Cloud-Daten« zu beantworten, dürfte die zuständigen Referenten einige Zeit gekostet haben. Allerdings ist bereits seit Dezember weitgehend bekannt, wie intensiv diverse Ministerien und Behörden daran arbeiten, Cloud-Daten überwachen zu können. Das mit der Schaffung europäischer Telekommunikationsstandards beauftragte gemeinnützige European Telecommunications Standards Institute (ETSI) unterhält derzeit beispielsweise mit dem Komitee »Lawful Interception« eine Arbeitsgruppe, die sich mit Überwachungsstandards beschäftigt. Constanze Kurz, die Sprecherin des Chaos Computer Clubs (CCC), erläuterte Ende vorigen Jahres in einem Artikel, dass in jedem modernen digitalen Kommunikationssystem die Möglichkeit zur Überwachung gleich durch Schnittstellen »zum Erfassen der darüber transportierten Informationen bereits von Anbeginn« miteingebaut ist. »Das Vorhalten dieser standardisierten Schnittstellen, aber auch der Hard- und Software zum Mitschneiden und Abfangen von Datenverkehr und Kommunikation ist in Deutschland den Telekommunikationsunternehmen gesetzlich vorgeschrieben und in der dazugehörigen Überwachungsverordnung sowie in technischen Richtlinien und Pflichtenheften genau festgelegt.«
Damit sich unterschiedliche abhörende Behörden nicht gegenseitig ins Gehege kommen, sind diese Schnittstellen in Europa darauf ausgelegt, »dass fünf ›berechtigte Stellen‹ gleichzeitig Gespräche mitschneiden können«. Die entsprechenden Standards werden bei ETSI erarbeitet, wo unter anderem Militär- und Geheimdienstangehörige sowie Vertreter kommerzieller Security-Firmen an der Erstellung der entsprechenden Richtlinien mitarbeiten. Ministerien und Behörden können dazu Wünsche äußern – und so ist es kaum verwunderlich, dass bei den Normen für die Cloud-Überwachung gleich mehrere deutsche Stellen beteiligt sind: Das Zollkriminalamt sowie das Bundesamt für Verfassungsschutz seien mit der Bundesnetzagentur bei ETSI organisiert, schrieb der Journalist Matthias

Monroy bereits Mitte Dezember. Das Bundeskriminalamt stimmt sich demnach mit den Kollegen vom Zoll ab, während die auf Abhörschnittstellen spezialisierte deutsche Firma Ultimaco direkt in der Arbeitsgruppe aktiv ist.

In Deutschland arbeiten, so eines der Ergebnisse der Kleinen Anfrage der Linkspartei, der Inlandsgeheimdienst und das BKA in einem eigenen Projekt namens »Cloud«, »ungeachtet des Trennungsgebots«, wie der Bundestagsabgeordnete der Linkspartei, Andrej Hunko, moniert. Das Ziel von »Cloud« sei »unter anderem das Überwinden von Passwörtern und Aushebeln von Verschlüsselungstechniken.« Aufträge für die Studie seien auch an private Unternehmen vergeben worden, die Forschungsergebnisse blieben allerdings geheim. Besonders skandalös sei es, dass bei den Überwachungsprojekten »Beteiligte aus den Bereichen Datenschutz, Netzpolitik oder Bürgerrechte« nicht einbezogen wurden. »Dies muss umgehend nachgeholt werden.« Das »ohnehin gestörte Vertrauen in die Freiheit des Internets« werde durch die Behörden untergraben, so Hunko weiter, daher müsse »eine an den Grundrechten orientierte, öffentliche Auseinandersetzung über die Ausforschung von Cloud-Daten« beginnen, bei der das Hauptaugenmerk auf der telekommunikativen Privatsphäre liege. Nutzer müssten sich »darauf verlassen können, dass ihre im Internet abgelegten Daten nicht von Dritten eingesehen werden«. Diese Forderung klingt zwar gut, entspricht aber nicht der Realität. Denn die Faustregel, wonach alle persönlichen Informationen, die man selbst bei einem genutzten Onlineangebot sehen kann, auch für den Betreiber und dessen dazu autorisiertes Personal sichtbar sind, gilt natürlich auch in einer Cloud.

Wenn Anbieter in ihren Marketingbotschaften ihre Cloud anpreisen, dann wird damit ein Produkt beworben, das einen oder mehrere Teile aus der Welt des Cloud-Computing den potentiellen Kunden zur Verfügung stellen soll. Dabei ist der Begriff Cloud-Computing selbst noch ziemlich neu – erst 2009 wurde die heute allgemein akzeptierte Definition von der US-Behörde National Institute of Standards and Technology (NIST) veröffentlicht. Nach dieser Definition enthält das Cloud-Computing drei Servicemodelle. Unter Servicemodellen versteht man grundsätzliche Arten von Diensten, die einzeln oder in Kombination angeboten werden können. Infrastrukturdienste bieten virtuelle Computer und ganze virtuelle Rechenzentren an, Plattformdienste enthalten die Möglichkeit, eigene Software zu programmieren und laufen zu lassen, während bei den Softwarediensten fertige Programme laufen, die man benutzen kann.
Der Begriff der Cloud kommt aus uralten IT-Infrastrukturdiagrammen. Wenn dort zum Beispiel die Kommunikation zweier Computer über das Internet aufgezeichnet wurde, dann war das Symbol für das Internet eine Wolke. Man weiß nicht, welchen Weg ein Kommunikationspaket durch das Internet nehmen wird, man weiß nur, dass da eine Infrastruktur ist, die sich irgendwie darum kümmern wird, dass das Paket sein Ziel erreicht. Daraus ergibt sich auch die Bezeichnung abstrakte Infrastruktur in der IT: Es ist klar, was am Start und am Ende passiert, und es ist klar, was im Prinzip dazwischen passiert – aber wie genau das alles passiert, das liegt versteckt hinter einer Wolke. Prinzipiell gibt es die Dienste, die man heute als Cloud-Computing bezeichnet, also schon sehr viel länger als den Begriff. Ob man nun eine eigene Webpage auf einem virtuellen Server hat, oder auch nur eigene Fotos ins Netz stellt und Freunden den Zugriff darauf gibt, verwendet wird immer ein Cloud-Dienst.

Dass immer mehr Cloud-Dienste angeboten werden und immer mehr Nutzer finden, hat einen einfachen Grund: Vor ein paar Jahren hatte der durchschnittliche Computernutzer meist nur einen Computer, mit dem alles erledigt wurde, was es so auf einem Rechner zu tun gab. Dazu kam höchstens noch ein Notebook, aber zwei Geräte lassen sich immer noch sehr einfach verwalten. Mittlerweile sind immer mehr Nutzer allerdings mit Computer, Notebook, Tablet, Smartphone und zum SmartTV aufgerüsteten Fernsehern im Internet unterwegs, was zu völlig neuen Problemen führt, denn niemand möchte erst einmal acht Geräte durchsuchen, um eine bestimmte Datei zu finden.

Daten in der Cloud lassen sich dagegen von jedem Gerät abrufen, weil sie sich im Internet befinden. Der Nutzer hat also seine Daten immer da, wo er sie gerade braucht. Diese schicke neue Bequemlichkeit hat jedoch einen Nachteil: Man muss dem Betreiber bedingungslos vertrauen. Denn es ist fast egal, wie gut das eigene Passwort ist – die Mitarbeiter des Unternehmens, dem diese Cloud gehört, werden immer vollen Zugriff haben. Ansonsten wäre es zum Beispiel nicht möglich, Backups zu erstellen – schließlich will niemand eine Cloud-Meldung sehen, dass diese wichtige Datei jetzt leider weg ist, weil beim Anbieter irgendetwas kaputt gegangen ist. Bei vielen Clouds weiß man überdies nicht, in welchem Land die Server stehen, auf denen die eigenen Daten gespeichert werden – und wie es dort um den Datenschutz bestellt ist. Ob ein Betreiber Server in Deutschland hat, sagt zudem noch nichts darüber aus, ob die eigenen Daten auch darauf gespeichert werden und wer in welchen Ländern Zugriff darauf hat und haben muss, um das reibungslose Funktionieren des Dienstes zu ermöglichen. Dass inländische und ausländische Behörden bereits jetzt Cloud-Daten ausspionieren können und sich gegenseitig dabei unterstützen, geht aus der Antwort der Bundesregierung auf die Kleine Anfrage ebenfalls hervor. Der »polizeiliche Austausch ausgeforschter Cloud-Daten mit US-Behörden« laufe wie geschmiert, erklärte Hunko. »Gegenseitige Rechtshilfeersuchen werden über ein Netzwerk auf Ebene der G8-Staaten abgewickelt. Statistiken werden hierüber nicht geführt, das Ausmaß der grenzüberschreitenden Überwachung ist also nicht nachvollziehbar.«
Man sollte sich allerdings nicht nur um seine Cloud-Daten sorgen, falls man aus welchen Gründen auch immer befürchtet, dass sich Geheimdienste für sie interessieren. Welche Sicherungsvorkehrungen die jeweiligen Unternehmen getroffen haben, ist auch Vertrauenssache, da sie für den Nutzer nicht einsehbar sind – denn das ist in der namensgebenden abstrakten IT-Infrastruktur eingeschlossen.

© Jungle World Verlags GmbH