P/S/R Public Social Responsibility Institut

P/S/R Institut Fachbeitrag

22/2014

Datenschutz in der Cloud?

Herausgeber: P/S/R Institut

Autor: Mag. Birgit Mitterlehner, Bakk.phil. M.A.

Datum: 13. Januar 2014

AUSSERUNIVERSITÄRES INSTITUT PUBLIC SOCIAL RESPONSIBILITY gemeinnützige Gesellschaft mbH
1010 Wien | Annagasse 6 | T +43 (1) 512 09 18 | office@psr-institut.at | psr-institut.org | psr-union.org
FN 369743s | FG: Handelsgericht Wien | UID-Nr. ATU66778178 | DVR: 4010211

Viele nutzen „Cloud Computing", ohne es zu ahnen. Die Beispiele reichen von der Nutzung des eigenen E-Mail-Accounts, Facebook, einem Online-Speicher (wie Dropbox, E-Government-Applikationen) bis zu den Speicherorten der von Videokameras festgehaltenen Inhalten in U-Bahnen und bei öffentlichen Gebäuden (u.v.m). In der Wissenschaft ist von Wissens- und Cybergesellschaft die Rede. Mit dem Phänomen einer Cyber-Kultur gehen die Themen Cyber Demokratie, Cyber Security und Cyber Crime einher.

Was ist eine Cloud?

Cloud-Computing bezeichnet die Speicherung von Daten (z. B. Textdateien, Bilder und Videos) und Software auf entfernten Großrechnern, auf die ein Benutzer (über das Internet) mit dem Gerät seiner Wahl zugreift. Der Grund für die Beliebtheit von Clouds ist, dass sie sehr effizient und mit beinahe jeder Computersoftware kompatibel sind. Dazu werden keine teuren Server oder Speichersysteme benötigt. Ein Effizienzgewinn lässt sich zudem für die Wartung von Server- oder Speichersystemen verzeichnen. Doch Cloud Computing birgt zahlreiche (insbesondere rechtliche) Risiken. Dies beginnt schon bei der Entscheidung zum Cloud Computing, so gibt es zahlreiche Formen der Cloud. Darum sollte man sich eingehend mit diesem Thema beschäftigen, bevor sensible Daten auslagert werden. So gilt es u. a. folgende Fragen zu beantworten:
Können Daten zwischen Clouds übertragen oder abgezogen werden? Ist der Anbieter vertrauenswürdig? Gibt es Daten(schutz)lücken in den AGB?[1]

Wer schützt meine Daten?

Der Datenschutz ist ein besonders heikles Thema in der Cloud. Gerade Unternehmen sind für "ihre" unternehmensbezogenen Daten verantwortlich und müssen diese Verantwortung letztendlich auch übernehmen, wenn Sie sich für eine Cloud entscheiden und Daten auslagern. In Deutschland regelt beispielsweise das deutsche Telekommunikationsgesetz[2] und das deutsche Bundesdatenschutzgesetz[3], dass Unternehmen für Datensicherheit und Telekommunikationssicherheit Sorge zu tragen haben. Diesbezüglich gilt es, das Bewusstsein zu stärken. Um ein Beispiel zu nennen, ist es der US-Regierung nach Maßgabe des US Patriot Act erlaubt, auf Daten Zugang zu erlangen.[4]
Auch security ist ein Thema, denn eine Cloud ist so konzipiert, dass ein „Einbruch" in die Cloud, alle Daten offenlegt. Gerade das Datenschutzrecht hinkt jedoch vielfach der Technologisierung hinterher. Ein weiterer Schritt auf dem Gebiet des Datenschutzes in Europa soll die Datenschutz-

1 Europäische Kommission, Mehr Schwung für das Cloud Computing - 27/09/2012 (2012), http://ec.europa.eu/news/science/120927_de.htm.

2 Telekommunikationsgesetz (TKG) (Bundesrepublik Deutschland), Gesetz vom 22.06.2004 (BGBl. I S. 1190), Art 109.

3 Bundesdatenschutzgesetz (Bundesrepublik Deutschland), Gesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), Art 9.

4 Vgl. *Ticher Paul*, Data Protection And Web Based Applications (2008), http://www.ictknowledgebase.org.uk/dataprotectionandweb.

Grundverordnung sein, welcher der zuständige Ausschuss im Europäischen Parlament unter heftigen Diskussionen kürzlich zugestimmt hat.

Mittlerweile hat die Europäische Kommission eine eigene Strategie zur „Freisetzung des Cloud-Computing-Potenzials in Europa" verabschiedet[5] und im Rahmen dieser Strategie eine Expertengruppe[6] eingesetzt. Ziel ist es, das Vertrauen in Cloud Computing Dienste zu stärken und auf der Grundlage eines fakultativen Rechtsinstruments sichere und faire Bedingungen für Cloud-Computing-Verträge auszuarbeiten. Darum soll die Expertengruppe in einem ersten Schritt bewährte Verfahren und ausgewogene Vertragsbestimmungen ermitteln. Im Mittelpunkt stehen dabei die Kriterien von Fairness und Zuverlässigkeit. In diesem Sinne beschäftigt sich die Expertengruppe mit der Ausarbeitung sicherer und fairer Muster-Vertragsbedingungen für das Cloud-Computing. So geben Allgemeine Geschäftsbedingungen Nutzern keine Chance, über Vertragsbedingungen zu entscheiden. Entweder sie akzeptieren sie, oder sie können den jeweiligen Dienst nicht nutzen. AGB sind für Nutzer zudem auch oft unverständlich formuliert. Subauftragnehmerstrukturen (z. B. wo sind die Daten wirklich gespeichert) gar nicht nachverfolgbar (ein Beispiel ist Google, einer der großen Provider, der keine geographische Datenspeicherung macht, jedoch zugibt, dass diese (auch) außerhalb Europas stattfindet. So heißt es beispielsweise in den AGB bei Google Docs:
"In particular, Google, its Subsidiaries and Affiliates, and licensors do not represent or warrant to you that:

a) your use of the Services will meet your requirements,
b) your use of the Services will be uninterrupted, timely, secure or free from error,
c) any information obtained by you as a result of your use of the Services will be accurate or reliable, and
d) that defects in the operation or functionality of any Software provided to you as part of the Services will be corrected."[7]

In einer technologisierten und zugleich globalisierten Welt ist es kaum möglich, sämtliche Risiken einer Cloud zu eliminieren. Besonders wichtig ist es, abzuwägen, inwiefern (z. B. in puncto Datenschutz) die Vorteile von Cloud Computing die Risiken überwiegen und Schutzziele definiert werden. Im Bereich der kritischen Infrastruktur sind besonders die Verfügbarkeit, Integrität und Vertraulichkeit wichtige Entscheidungsparameter. Schutzziele könnten sich somit daran orientieren, dass in der kritischen Infrastruktur IT-Störungen nicht dazu führen dürfen, dass die Versorgungskapazität nicht in angemes-

5 Vgl. European Commission, Digitale Agenda: Neue Strategie zur Förderung der Produktivität europäischer Unternehmen und Verwaltungen durch Cloud-Computing (2012), IP/12/1025, http://europa.eu/rapid/press-release_IP-12-1025_de.htm; European Commission, Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?, MEMO/12/713, http://europa.eu/rapid/press-release_MEMO-12-713_en.htm?locale=en.

6 Bestehend aus Vertretern von Cloud-Dienstanbietern, Verbrauchern, KMU, Akademia und Juristen.

7 Section 14.2 AGB Google Docs.

sener Qualität und Quantität möglich ist (Verfügbarkeit), Daten Dritten zugänglich sind und dies die Verfügbarkeit und Integrität der IT-Infrastruktur beeinträchtigt (Integrität). Clouds sind zudem nicht das einzige Risiko. Gerade die Möglichkeiten von privaten Consumer Devices und deren Verwendung am Arbeitsplatz stellen eine vernachlässigte Sicherheitslücke dar. Dies ist umso mehr der Fall, als die Nutzung von privaten Endgeräten von Mitarbeitern am Arbeitsplatz nur schwer zu unterbinden ist. Insbesondere deshalb ist es wichtig, auch hier ein Bewusstsein zu schaffen und Lösungen aufzuzeigen.