Pressemitteilung

Neuer IT-Ratsbeschluss zur Verwendung von Cloud-Diensten bereits überholt

München, 28. Oktober 2015. Wann dürfen im öffentlichen Dienst Cloud-Angebote genutzt werden? Eine Frage, die in diesem Sommer die Verantwortlichen in der öffentlichen Verwaltung verstärkt beschäftigte. Der Rat der IT-Beauftragten der Bundesregierung verfasste dazu nun einen Beschluss. Dieser Beschluss vom 29. Juli 2015 (1) erklärt vorab, dass eigene IT-Systeme „zu bevorzugen“ sind, Cloud-Dienste von Privatanbietern jedoch eingesetzt werden können, wenn sie den Leistungsanforderungen entsprechen. Der Beschluss fasst die Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung zusammen. Eine zentrale Forderung ist, dass die Cloud-Dienst-Angebote gerade in Bezug auf Sicherheit intensiv zu prüfen sind, bevor Daten und deren Verarbeitung ausgelagert werden.

Wichtiges Kriterium für die Nutzung von Cloud-Diensten ist ein äußerst hohes Maß an Sicherheit, der Rat führt zum Beispiel explizit eine Zertifizierung nach ISO-Standard 27001 an. Einen erweiterten Schutz fordert der Rat insbesondere dann, wenn die ausgelagerten Daten Amtsgeheimnisse beinhalten. Die §§ 203 und 353b StGB, die den Umgang mit personenbezogenen Daten und Geheimnissen behandeln, setzen hierbei den gesetzlichen Rahmen. Professor Alexander Roßnagel, Professor für Öffentliches Recht und Technikrecht an der Universität Kassel, fasst zusammen, was dies genau bedeutet: „Nur wenn technische Maßnahmen die Kenntnisnahme von Geheimnissen ausschließen, dürfen Beamte oder Mitarbeiter des öffentlichen Dienstes eine Public Cloud nutzen.“

Generell muss bei der Verarbeitung der Daten der deutsche Datenschutz im vollen Umfang gewährleistet sein und es muss sichergestellt werden, dass unbefugte Dritte keine Daten einsehen oder bearbeiten können. Für den Fall einer Insolvenz oder eines Verkaufs eines Cloud-Anbieters muss eine zuvor definierte Alternative zur Verfügung stehen. Ferner dürfen keine Cloud-Dienste gewählt werden, die ausländischen Rechtsordnungen unterliegen und anderen Staaten zur Auskunft verpflichtet sind, was etwa bei US-Unternehmen der Fall ist.

Zertifizierungen nach ISO-Standard 27001 sagen jedoch bis heute noch nichts über die tatsächliche Datensicherheit in Cloud-Umgebungen aus (2), denn der Anbieter wird nur nach seinen selbstdefinierten Regeln zertifiziert. Diese Regelungen beziehen sich auf eine strukturierte Arbeitsweise, die eine Voraussetzung für die IT Sicherheit eines Unternehmens ist. Das Schutzniveau für die Daten lässt sich daraus nicht ableiten. Eine Tatsache, die gerade bei Amtsgeheimnissen und personenbezogenen Daten einen Interpretationsspielraum eröffnet und dem Anwender nicht wirklich bei der Bewertung von Angeboten hilft.

Außerdem betrifft die ISO 27001 nur die Infrastruktur einer Organisation, Cloud-Dienste werden dort gar nicht berücksichtigt. Dazu gibt es den im Beschluss nicht adressierten ISO-Standard 27018, der jedoch keine harten Anforderungen formuliert, die einen Vergleich der Datensicherheit von Diensten ermöglichen würden. Dies soll sich durch das unter der Schirmherrschaft des Bundeswirtschaftsministeriums erarbeitete Trusted Cloud Datenschutzprofil (TCDP) (3) bald ändern. Das TCDP beinhaltet einen genauen Anforderungskatalog, der die Cloud-Dienstangebote in Schutzklassen einteilt.

Auf der Basis des Trusted Cloud Datenschutzprofils zertifizierte Cloud-Dienste entsprechen klar definierten Muss-Anforderungen hinsichtlich des Datenschutzes. Drei Schutzklassen geben konkret Auskunft über das Niveau der Datensicherheit und erlauben dem Anwender einen direkten Vergleich. Die höchste Schutzklasse – unter die zum Beispiel Amtsgeheimnisse fallen – muss unter anderem garantieren, dass eine technische Sicherung besteht, die verhindert, dass Dritte die Daten einsehen können. Selbst der Betreiber der Rechenzentren muss von einer möglichen Kenntnisnahme ausgeschlossen sein. In diesem Zusammenhang sieht Roßnagel die in Deutschland entwickelte Sealed Cloud Technologie als „ein gelungenes Beispiel für datenschutzgerechte Technikgestaltung“. Denn die Sealed Cloud ist derzeit noch die einzige Cloud-Umgebung, die mit rein technischen Maßnahmen sicherstellt, dass Daten für Betreiber und unbefugte Dritte nicht einsehbar ist. Die technische Realität und das Trusted Cloud Datenschutzprofil (TCDP) haben die Forderung des Beschlusses nach einer ISO/IEC 27001 also bereits überholt.

Pressemitteilung

Dr. Huber Jäger, GF von Uniscon und IT-Sicherheitsexperte: „Der Beschluss ist ein wichtiger Schritt in die richtige Richtung, da er unter anderem klarstellt, dass die §§ 203 und 353b StGB einzuhalten sind. Die Forderung, eigene IT-Systeme seien zu bevorzugen greift dagegen zu kurz. Man muss sagen, dass IT-Technologien oft einen oder mehrere Schritte weiter sind, als es Beschlüsse widerspiegeln. Es ist höchste Zeit, dass Daten in der Cloud sachgerecht geschützt werden. Die Frage ist, kann Anwendern und IT-Fachkräften von Behörden und öffentlichen Einrichtungen allein zugemutet werden, Cloud-Angebote in Sachen Datensicherheit zu beurteilen, oder sollten sie sich nicht besser mit externen IT-Sicherheitsexperten zusammentun, deren täglicher Job darin besteht, Technologien, Systeme und Angebote auch auf Datensicherheit zu überprüfen?“

(1) http://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragter-fuer-Informationstechnik/IT_Rat_Beschluesse/beschluss_2015_05.pdf?__blob=publicationFile
(2) http://www.computerwoche.de/a/datenschutz-in-der-cloud-wird-moeglich-sogar-mit-zertifikat,3095757
http://www.trusted-cloud.de/media/content/Publikation_TCDP.pdf

Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de

Über Uniscon GmbH

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service IDGARD für Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt

Pressemitteilung

Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 113
presse@uniscon.de
www.uniscon.de

PR-Agentur
Xpand21, Doris Loster
Alter Teichweg 9M
22081 Hamburg
040 / 22 61 49 43
0170 / 215 31 72
uniscon@xpand21.com
www.pr-agentur-xpand21.de