Pressemitteilung

Deutsches Cloud-Zertifikat schafft Vertrauen in die Cloud

München, 16.März 2015.Unternehmen, die sich für Cloud-Dienste entscheiden, können aktuell noch immer schwer einschätzen, wie sicher ihre Daten in den Rechenzentren sind. Personenbezogene Daten müssten jedoch so geschützt werden, dass kein Unbefugter die Daten einsehen kann. Nur, welcher Cloud-Anbieter würde das heute schon garantieren? Die ISO/IEC-Norm 27018 ist ein neuer internationaler Standard für den Datenschutz in der Cloud, der seit April 2014 in Kraft ist. Er legt Mindestanforderungen für Cloud-Anbieter fest. Allerdings fehlte bisher ein konkreter Anforderungskatalog, anhand dessen die angebotenen Dienste auf ihr Sicherheitsniveau geprüft und verschiedenen Sicherheitsstufen zugeordnet werden können.

Sicherheitsexperten aus Industrie, Forschung und Datenschutzaufsichtsbehörden der Trusted-Cloud-Initiative des Bundesministeriums für Wirtschaft und Energie (BMWi), haben sich im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ zusammengefunden und in den vergangenen 18 Monaten den fehlenden Anforderungskatalog für Deutschland erarbeitet, um damit auch die Grundlage einer datenschutzkonformen Zertifizierung zu schaffen. Unter der Leitung von Georg Borges, Professor für Bürgerliches Recht, Rechtstheorie und -informatik an der Universität des Saarlandes, wurde ein detaillierter datenschutzrechtlicher Prüfkatalog erarbeitet. Der im April endgültig vorliegende Anforderungskatalog teilt Cloud-Angebote in drei Schutzklassen ein, wobei die dritte Schutzklasse die höchste ist.

Anhand dieser Schutzklassen können sich Unternehmen bezüglich des Schutzbedarfs für Ihre Daten und Anwendungen orientieren und so schnell die passenden Anbieter identifizieren. Mit diesen Zertifikaten kann sich in Zukunft jedes Unternehmen, das Daten auslagert, sicher sein, dass die eigenen Compliance-Vorgaben auch vom Cloud-Dienstleister eingehalten werden. Zusätzlich soll das Zertifikat Rechtsfolge haben: Indem ein Unternehmen einen Anbieter auswählt, der mit der für die Unternehmensdaten notwendigen Schutzklasse ausgezeichnet ist, erfüllt es seine vom Gesetz vorgeschriebenen Kontrollpflichten. Dadurch können Unternehmen endlich Cloud- Anbieter hinsichtlich des Datenschutzniveaus vergleichen. Außerdem erhalten sie Rechtssicherheit im Hinblick auf ihre Verpflichtungen nach den geltenden Datenschutzgesetzen.

Pressemitteilung

Basierend auf den Umsetzungsempfehlungen der ISO/IEC 27018:2014 und weiteren Evaluationskriterien zur Erfüllung des Bundesdatenschutzgesetzes (BDSG) wird das Sicherheitsniveau der Cloud-Angebote in drei Schutzklassen eingeteilt. Bei der Einstufung werden nicht nur die funktionalen und nicht-funktionalen Merkmale der Infrastruktur, die zum Betrieb des Dienstes gehören, beachtet. Zusätzlich wird auch der Entstehungsprozess aus Sicht der Implementierung und aus Sicht des Einsatzes überprüft, also der gesamte Produktzyklus. Entscheidend ist zum einen für das Verfahren, dass fachlich geeignete und unabhängige Auditoren die Prüfung durchführen. Zum zweiten ist entscheidend, dass die Zertifizierung auf der Grundlage allgemeiner, anerkannter Kriterien erfolgt, die für alle begutachteten Dienste gleichermaßen gelten.

Dr. Hubert Jäger, Mitarbeiter im Pilotprojekt und Geschäftsführer der Uniscon GmbH erklärt: „Bisher fehlte ein Werkzeug, um das Sicherheitsniveau der verschiedenen Cloud-Anbieter einordnen zu können. Im Projekt haben wir technikneutrale Kriterien für eine Einordung in Schutzklassen entwickelt. Denn als Maßstab für den Vergleich verschiedener Dienste genügt es nicht, wenn Cloud-Dienstanbieter selbst eine Risikoanalyse durchführen und dementsprechend mit ihrem Informations-Sicherheitsmanagement reagieren. Es ist vielmehr dringend notwendig, durch die Entwicklung von konkret nachprüfbaren Sicherheitsprofilen eine Orientierung zu geben, die einen Vergleich der Dienste nach Gesichtspunkten des Datenschutzes ermöglicht."

Überblick zu den Schutzklasse I bis III

- Schutzklasse I: Der Dienstanbieter muss durch technische und organisatorische Maßnahmen, die dem Risiko angemessen sind, gewährleisten, dass die Daten nicht unbefugt verwendet, verändert oder gelöscht werden. Die Maßnahmen müssen so gestaltet sein, dass sie dies auch ausschließen, falls technische oder organisatorische Fehler geschehen, einschließlich von Bedienfehlern oder fahrlässiger Handlungen Dritter (Cloud-Nutzer, sonstige Dritte). Vorsätzliche Eingriffe müssen durch einen Mindestschutz erschwert werden.
- Schutzklasse II: Die Maßnahmen müssen auch technische oder organisatorische Fehler durch den Cloud-Anbieter und seine Mitarbeiter ausschließen. Außerdem sind die Daten so zu schützen, dass zu erwartende Eingriffe „hinreichend sicher" verhindert werden. Dazu gehört vor allem der Schutz gegen bekannte Angriffsszenarien.
- Schutzklasse III: Die zuvor genannten Maßnahmen müssen dem Stand der

Pressemitteilung

Technik entsprechen. Außerdem muss der Dienst in der Lage sein, Eingriffe oder auch Missbräuche festzustellen.

- Dienste, welche die Anforderungen der Schutzklasse I nicht erfüllen, sind der Schutzklasse 0 zuzuordnen. Höhere Anforderungen als die der Schutzklasse III beziehen sich auf eine vollständige Nachweisbarkeit der Vertrauenswürdigkeit aller verwendeten Komponenten und führen zur Schutzklasse „III+“.

Mehr dazu erfahren Interessierte auf der CeBIT 2015 am Stand von Uniscon in Halle 007, Stand B62.

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
Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
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