Pressemitteilung

Fakten-Check: Cloud-Zertifizierung nach ISO/IEC 27018 nicht möglich

München, 29. Juni 2015. Seit Standards für den Datenschutz in der Cloud durch die ISO/IEC-Norm 27018 im April 2014 definiert sind, gibt es immer wieder Meldungen von Herstellern, die eine Zertifizierung für die Datenschutzanforderungen durchlaufen haben wollen. Aber ist es überhaupt möglich, eine Zertifizierung nach ISO/IEC 27018 zu erlangen? Wie sieht denn die Prüfung aus und wer ist der Prüfer und Zertifikatsgeber? Sind die in der Cloud gespeicherten Daten tatsächlich sicher vor dem Zugriff Dritter, wie diese Meldungen suggerieren?

Das Bundesministerium für Wirtschaft und Energie (BMWI) hat in Deutschland die Trusted Cloud Initiative ins Leben gerufen, die sich mit der Datensicherheit in Cloud-Diensten beschäftigt und Entwicklungen zur sicheren Datenverarbeitung in der Cloud unterstützt. Für ein mögliches Zertifizierungsverfahren wurde ein Pilotprojekt aus Mitgliedern aus Standardisierung, Forschung, Wirtschaft, Prüfern und Aufsichtsbehörden zusammengestellt, die einen Anforderungskatalog zur Zertifizierung nach den Vorgaben des BDSG und den Umsetzungsempfehlungen des ISO/IEC 27018:2014 entwickelt haben, das Trusted Cloud Datenschutzprofil (TCDP).

Dr. Hubert Jäger arbeitet bei diesem Pilotprojekt mit und ist Geschäftsführer des Münchner Unternehmens Uniscon. Im Gespräch zu Zertifizierungsverfahren von Cloud-Diensten:

Frage: Ist eine Zertifizierung nach ISO/IEC 27018 überhaupt möglich?
Dr. Hubert Jäger: Bei genauer Betrachtung wird klar, dass eine Zertifizierung gemäß der Norm ISO/IEC 27001:2013 vorliegen kann, nicht aber eine nach ISO/IEC 27018:2014, die explizit den Datenschutz im Cloud-Computing behandelt. Formal handelt es sich bei ISO 27018 lediglich um Umsetzungsempfehlungen. Bei solchen ist niemals definiert, welche Anforderungen genau für ein Zertifikat erfüllt sein müssen. Die Auditoren können nämlich nicht anhand einer Liste die einzelnen Anforderungen überprüfen und dann ein Ergebnis ableiten. Die Meldungen zu „27018-Zertifikaten“ beziehen sich auf 27001-Zertifikate, bei denen

zusätzlich einzelne Umsetzungsempfehlungen aus 27018 mitberücksichtigt sind.

Frage: Worin besteht denn genau der Unterschied?
Dr. Hubert Jäger: Die ISO/IEC-Reihe 27000 umfasst Normen für das Informations-Sicherheits-Management, also wie man sich innerhalb einer Organisation um die Sicherheit der Daten kümmert. ISO/IEC 27001:2013 ist der grundlegende Zertifizierungsstandard hierfür, darin geht in erster Linie um Organisatorisches. Der normative Anhang A geht dann auf die IT-Sicherheit ein. Wichtig ist dabei zu wissen, dass für die Zertifizierung ISO/IEC 27001 jede Organisation ihre eigene Risikoanalyse vornimmt und für diese einen passenden Satz an Maßnahmen individuell aussucht. Dadurch ergibt sich, dass ein solches Zertifikat keine Aussage zum Niveau des Datenschutzes und der Datensicherheit erlaubt, sondern es sagt lediglich, dass die zertifizierte Organisation sorgfältig mit dem Thema Informationssicherheit umgeht. Mit welchem Ergebnis bleibt allerdings unklar.

Frage: Sind denn in der Formulierung der ISO/IEC 27018 schon konkrete Vorgaben zur Umsetzung des Datenschutzes bei der Datenverarbeitung in der Cloud definiert?
Dr. Hubert Jäger: Ja, der Standard 27018 geht konkret auf die neuen Herausforderungen des Cloud-Computing ein. Er passt die Umsetzungsempfehlungen des ISO/IEC 27002:2013 an, indem er speziell berücksichtigt, wie Datensicherheit in einer Cloud-Umgebung umzusetzen ist. Zum Beispiel gilt in 27002 noch als positiv, wenn der Administrator möglichst viel sehen, also alle Vorgänge nachvollziehen kann – in 27018 eher negativ. Außerdem werden Anforderungen des Datenschutzes hinzugefügt, wie er in vielen Ländern gesetzlich vorliegt (gemäß ISO/IEC 29100:2011).

Frage: Im Frühjahr 2015 hat die Trusted Cloud Initiative einen Anforderungskatalog für die Datenschutz-ISO 27018 vorgestellt: das Trusted Cloud Datenschutz Profil, kurz TCDP. Ist auf dieser Basis eine Bewertung möglich, die dem Anwender die Sicherheit über seine Daten gibt?
Dr. Huber Jäger: Ja, das TCDP standardisiert die Anforderungen des Datenschutzes bei Cloud-Diensten, einschließlich der Informationssicherheit. Damit der Cloud-Nutzer eine Auswahl zwischen Diensten treffen kann, muss er vergleichen können. Hierfür sind beim TCDP Schutzklassen vorgesehen, die auf den unterschiedlichen Bedarf an Datensicherheit eingehen. Das erleichtert dem Cloud-Nutzer die Erfüllung der Kontrollpflicht erheblich. Außerdem können CIOs Haftungsrisiken vermeiden.

Pressemitteilung

Frage: Worin liegen denn genau die Vorteile des TCDP gegenüber ISO 27001 und 27018?
Dr. Huber Jäger: Das TCDP der Bundesregierung etabliert einen Zertifizierungsstandard für Dienste, also nicht für Management-Systeme. Diese Unterscheidung ist wichtig, denn nur so können einzelne Module eines Cloud-Dienstes separat zertifiziert werden. Damit müssen Prüfer nicht für jeden neuen Dienst alle funktionalen Module erneut untersuchen.

Zudem ist das TCDP ein Compliance-Standard. Damit ist gemeint, dass mit einer Bewertung nach diesem Standard bestätigt wird, dass die gesetzlichen Vorgaben erfüllt sind. Nutzer eines Dienstes, der nach TCDP bewertet wurde, können also darauf vertrauen, dass der Anbieter das Datenschutzgesetz einhält. Voraussetzung ist natürlich, dass sie einen Dienst mit der passenden Schutzklasse auswählen.

Dadurch ist die vom Gesetz vorgesehene Kontrollpflicht eines Nutzers bereits wesentlich vereinfacht. In den Entwürfen zum Europäischen Datenschutzgesetz (Grundverordnung) ist sogar vorgesehen, dass eben diese Kontrollpflicht mit der Auswahl eines Dienstes mit Zertifikat als rechtsverbindlich erfüllt gilt.

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

Pressemitteilung

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