ISO/IEC 27018: Noch eine Norm oder eine sinnvolle Ergänzung?

Luca Rechsteiner, Kaufmann mit Berufsmaturität

Im Zeitalter von Smartphone und Tablet ist das medienübergreifende Speichern von Daten zu einem allgemeinen Bedürfnis geworden. Jeder möchte überall auf seine Dateien und Programme zugreifen. Inzwischen gibt es viele Firmen, die dazu Cloud-Lösungen anbieten: Dropbox, Apple, Microsoft – um nur einige zu nennen. Die Cloud-Anbieter werben mit verlockenden Angeboten, wie etwa „25-GB-Speicherplatz gratis!". Die Cloud bringt auf den ersten Blick nur Vorteile. Trotzdem sind viele Benutzer nach wie vor skeptisch und pflegen Zurückhaltung. Es stellen sich Fragen: „Was passiert mit meinen Daten?", „Wer kann meine Daten sehen?", „Wird meine Privatsphäre geschützt?" oder: „Werden meine Daten vertraulich behandelt?". Und wie vertrauensvoll sind Firmen, die geschäftskritische Applikationen in die Cloud verschieben?

Nicht nur Privatpersonen, auch Unternehmen legen ihre Daten und Anwendungen vermehrt in der Cloud ab. Schweizer Firmen, vor allem KMU, üben allerdings noch grosse Zurückhaltung. Die kritischen Fragen überwiegen. Etwa: Was denken die Kunden von uns, wenn wir unsere Daten in Amerika lagern?

Um den Unternehmen bei dieser schwierigen Abwägung eine Hilfestellung zu geben, hat die Internationale Organisation für Standardisierung (ISO) die Norm ISO/IEC 27018 veröffentlicht. Die Norm berücksichtigt alle IT-sicherheitstechnischen Aspekte in der Cloud und basiert auf der bereits bekannten und etablierten Norm der Informationssicherheit ISO/IEC 27001. Die Internationale Organisation für Standardisierung ergänzte die bereits bestehende Kapitelstruktur der ISO/IEC 27002 um relevante Vorgaben und Massnahmen rund um personenbezogene Daten. Die neue Norm erläutert nun die relevanten Aspekte und Themen der Informationssicherheit Punkt für Punkt. Dazu gehören beispielsweise die Informationssicherheitsrichtlinie, die Organisation der Informationssicherheit, Personalsicherheit sowie das Wertemanagement. Für diese Themen bietet die Internationale Organisation für Standardisierung Hilfestellungen und Informationen bezüglich der Must-Haves. Somit werden alle Fragen zum Datenschutz beantwortet.

Seit September 2014 können sich Unternehmen, die Cloud-Produkte anbieten, unter dieser Norm zertifizieren lassen. Die Voraussetzung dafür: Das Unternehmen ist bereits ISO/IEC 27001 zertifiziert. Aus diesem Grund ist eine Zertifizierung der ISO/IEC 27018-Norm grundsätzlich mit weniger Aufwand verbunden als das Zertifizieren der Grundnorm. Die Zertifizierung der Cloud-Norm wird aufrechterhalten, indem sich die Unternehmen durch eine unabhängige Stelle in regelmässigen Abständen prüfen lassen. Verschiedene namhafte IT-Firmen wie Microsoft und Dropbox Inc. haben ihre Cloud-Produkte bereits nach ISO/IEC 27018 zertifizieren lassen.

Was aber nicht ausser Acht gelassen werden darf: Die Datenschutzgesetzgebung ist in jedem Land unterschiedlich. Eine ISO/IEC 27018-Zertifizierung hilft nichts, wenn der Staat ohne Gerichtsbeschluss Zugang zu sämtlichen Daten hat. Als abschreckendes Beispiel hierfür dienen die Vereinigten Staaten von Amerika. In den USA gibt es ein Gesetz, das den Behörden den freien Zugriff auf sämtliche Daten im Land erlaubt. Microsoft oder Dropbox Inc. sind amerikanische Firmen, somit hat der amerikanische Staat theoretisch Einblick in alles, was diese Firmen auf ihren Servern speichern. Deshalb annullierte der europäische Gerichtshof am 6.10.2015 das Safe-Harbour-Abkommen mit den USA. Dieses Abkommen regelt den Datenaustausch zwischen der EU und den USA. Grund für die Aufkündigung dieses Abkommens war die Datenschutzhandhabung in den USA.

Die Folgen dieses Schrittes werden sich erst in den nächsten Jahren zeigen. Ein anderer wichtiger Aspekt, den es zu beachten gilt: Die Zertifizierung einer Norm ist immer nur eine Momentaufnahme. Sie sagt aus, dass sich das Unternehmen umfassend mit der Informationssicherheit auseinandersetzt und sämtliche wichtigen Prozesse nachhaltig implementiert hat. Trotzdem gibt es keine hundertprozentige Sicherheit für den umfassenden Schutz der Daten.

Zurück zur ISO-Norm: Wer sich also fragt, was mit seinen Daten in der Cloud passiert und deshalb skeptisch ist, sollte sich bei potenziellen Cloud-Anbietern nach einer vorhandenen Zertifizierung erkundigen. In der Schweiz ist man damit gut beraten, weil der Datenschutz hier grossgeschrieben wird. Wer in Zukunft in Betracht zieht, eine Anwendung oder Daten in die Cloud zu verlagern und einen ISO/IEC 27018 zertifizierten Anbieter findet, kann sich der Sicherheit seiner Daten gewiss sein.

Fazit

Die einleitende Frage: „ISO/IEC 27018: Noch eine Norm oder eine sinnvolle Ergänzung?“ beantworten wir mit einem klaren Ja. Die Ergänzungen für den Umgang mit der Cloud sind essenziell. Ein mit ISO/IEC 27018 zertifiziertes Unternehmen kann damit ausweisen, dass es alles Notwendige unternommen hat, um seine Daten vollumfänglich zu schützen. Die Norm trägt ausserdem dazu bei, das Verhältnis zwischen Cloud-Anbieter und Cloud-Kunde umfassend zu regeln. Ein Zertifikat für die Norm ISO/IEC 27018 darf allerdings nicht darüber hinwegtäuschen, dass die Behörden in manchen Ländern weitgehende Befugnisse zur umfassenden Dateneinsicht haben. Selbstredend ändert keine ISO/IEC-Norm etwas an dieser Situation.