Sicherheit in Cloud-Diensten

Um die Cloud führt heute praktisch kein Weg mehr vorbei. Viele Dienste laufen direkt in der Cloud oder nutzen Cloud-Speicher im Hintergrund. Oft werden auch schützenswerte oder sensitive Daten dem Cloud-Anbieter übergeben. Daher ist es wichtig, den richtigen Partner zu haben. Die ISO 27018 ermöglicht es dem Anbieter seinen Kunden zu zeigen, dass er sicher mit den anvertrauten Daten umgeht.

Die ISO/IEC 27018 wurde im Januar 2019 in der zweiten Version veröffentlicht. Sie trägt den Titel «Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors». Wie der Titel verrät, geht es um den Schutz von personenbezogenen Daten und nimmt damit Bezug auf die verschiedenen Datenschutzgesetze.

Ein Blick in die Norm zeigt, dass der Aufbau genau demjenigen der ISO 27001 Anhang A5-A18 entspricht. Die Grundlage für eine erfolgreiche Zertifizierung ist daher auch die Die ISO 27001. Ohne diese Zertifizierung kann die ISO 27018 nicht umgesetzt werden.

Die ISO 27001 beschreibt 114 Massnahmen zur Umsetzung und Sicherstellung der Informationssicherheit. Die 27018er ergänzt beziehungsweise präzisiert diese Punkte um weitere Anforderungen, die es umzusetzen gilt. Die Absicht des Dokuments ist es einen gemeinsamen Satz von Sicherheitskategorien und -kontrollen zu schaffen, die von einem Anbieter von Cloud-Diensten implementiert werden können. Folgende Ziele werden verfolgt:

- dem Anbieter von Public-Cloud-Diensten dabei zu helfen, die geltenden Verpflichtungen einzuhalten;
- dem Public-Cloud-Anbieter zu ermöglichen, in relevanten Angelegenheiten transparent zu sein, damit Kunden gut geführte Cloud-Services auswählen können;
- um Kunden und Verarbeiter beim Abschluss einer vertraglichen Vereinbarung zu unterstützen;
- Kunden eine Möglichkeit ihres Audit- und Compliance-Recht sowie ihrer Verantwortung in Fällen zu bieten, in denen individuelle Audits, die in einer Umgebung mit mehreren Parteien und virtualisierten Servern gehostet werden, technisch unpraktisch (oder gar nicht möglich) sein können und die Risiken für die vorhandenen physischen und logischen Netzwerksicherheitskontrollen erhöhen können.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Begriffe

Analog anderen Normen werden im Kapitel 3 die verwendeten Begriffe genau erklärt. Da viele Erläuterungen gemeinsam in der ISO 27000 enthalten sind, werden hier nur neue beschrieben. Es handelt sich in der Folge nur um sieben zusätzliche Begrifflichkeiten. Darunter sind:

PII
Alle Informationen, die (a) verwendet werden können, um eine Verbindung zwischen den Informationen und der natürlichen Person herzustellen, auf die sich diese Informationen beziehen, oder (b) direkt oder indirekt mit einer natürlichen Person verbunden sind oder sein können.

PII-Controller
Datenschutzbeauftragte, die Zwecke und Mittel für die Verarbeitung personenbezogener Daten festlegen, mit Ausnahme von natürlichen Personen, die Daten für persönliche Zwecke verwenden.

PII-Auftraggeber
Natürliche Person, auf die sich die personenbezogenen Daten beziehen.

PII-Prozessor
Datenschutzbeauftragter, der personenbezogene Daten im Auftrag und nach den Anweisungen eines PII-Verantwortlichen verarbeitet.

Erweiterung der Massnahmen

In Kapitel 5 (analog zur ISO 27002) werden die zusätzlichen oder vertieften Kontrollen beschrieben. Es werden aber nicht alle 114 Kontrollen ergänzt, sondern nur 14. Es handelt sich um folgende Punkte, die ein Cloud-Anbieter umzusetzen hat:

- Erweiterung der Informationssicherheitsrichtlinien um die Verpflichtung zur Einhaltung der geltenden Gesetze zum Schutz von personenbezogenen Daten (5.1.1).
- Erweiterung der Rollen um eine Kontaktstelle für den Cloud-Service-Kunden (6.1.1).
- Das Bewusstsein aller Mitarbeitenden über die möglichen Folgen eines Verstosses gegen die Datenschutz- oder Sicherheitsregeln und -verfahren zu stärken (7.2.2).
- Verfahren planen und üben, sollten Benutzerzugriffskontrolle kompromittiert werden, zum Beispiel im Falle eines Hacker-Angriffes oder Passwort-Diebstahls (9.2.1).
- Für alle Anmeldungen an Cloud-Services sichere Anmeldeverfahren für alle Konten bereitstellen (9.4.2).
- Den Kundinnen und Kunden Informationen zur eingesetzten oder möglichen Verschlüsselung der eigenen Daten zur Verfügung stellen (10.1.1).
- Alle Geräte, Festplatten und Datenträger immer so zu entsorgen, als wären Daten darauf enthalten, auch wenn keine sind (11.2.7).
- Müssen Kundendaten zu Testzwecken verwendet werden, muss eine Risikobewertung durchgeführt werden (12.1.4).
- Die Sicherung der Daten sollte nicht nur intern gemacht werden, sondern auch externe Sicherungen sollten eingeführt werden. Dies können physisch und/oder logisch getrennte Orte sein. Die Art und Weise muss den Kunden klar mitgeteilt werden. Weiter muss der Cloud-Anbieter die Wiederherstellung in festgelegter und dokumentierter Häufigkeit durchführen. Beim Einsatz von Subunternehmen gilt es die Kunden zu informieren (12.3.1).
- Ein besonderes Augenmerk wird auch auf die Ereignisprotokollierung gerichtet. Die Ereignisse müssen mit einer festgelegten, dokumentierten Periodizität überprüft werden, um Unregelmässigkeiten zu identifizieren und Abhilfemassnahmen vorzuschlagen. Weiter muss sich der Cloud-Anbieter überlegen, ob, wann und wie Protokollinformationen dem Cloud-Kunden zur Verfügung gestellt oder von ihm genutzt werden können. Dabei darf der Kunde nur auf seine eigenen Ereignisse zugreifen dürfen (12.4.1).
- Die erwähnten Protokollinformationen gilt es zu schützen und innerhalb eines festgelegten und dokumentierten Zeitraums zu löschen (12.4.2).
- Werden physische Medien für den Transport von Daten genutzt, müssen die Ein- und Ausgänge inkl. Art, Sender/Empfänger, Datum und Uhrzeit protokolliert werden (13.2.1).
- Im Falle eines Informationssicherheitsvorfalles gilt es einen genauen Prozess umzusetzen, der auch Datenschutzverletzungen berücksichtigt (16.1.1).
- Da Kunden oft nicht selber ein Audit beim Cloud-Anbieter durchführen können oder dürfen, muss der Cloud-Anbieter dieses durch eine unabhängige

Stelle durchführen und entsprechende Nachweise zur Verfügung stellen (18.2.1).

Anhang

Der Anhang A.1 bis A.12 geht auf die Datenschutzprinzipien analog der ISO 29100 ein. Folgende Punkte werden behandelt:

- Der Cloud-Anbieter muss seinen Kunden die Möglichkeit zum Zugang, Berichtigung und/oder Löschung der sie betreffenden Informationen ermöglichen.
- Personenbezogene Daten des Kunden dürfen ausschliesslich nach dessen Weisung verarbeitet und nicht ohne ausdrückliche Zustimmung verwendet werden.
- Der Cloud-Anbieter muss seine Kunden über den Standort der Datenverarbeitung informieren.
- Cloud-Anbieter haben den Kunden über jede Verarbeitung der Daten durch Dritte zu informieren.
- Der Kunde muss jederzeit Zugriff auf seine Daten haben, um die Daten unmittelbar zu ändern, zu löschen oder zu korrigieren.
- Cloud-Anbieter dürfen Daten des Kunden nur an Strafverfolgungsbehörden herausgeben, sofern dazu eine gesetzliche Verpflichtung besteht. Zudem müssen die Kunden in diesem Fall über die Herausgabe informiert werden, ausser die Informierung ist gesetzlich verboten.
- Sollten Unbefugte Zugriff auf personenbezogene Daten des Kunden bekommen, so ist dieser umgehend darüber in Kenntnis zu setzen.
- Es müssen verbindliche Regeln über Rückgabe, Transfer und Vernichtung der Daten des Kunden festgelegt werden.
- Es müssen vertragliche Regelungen für die Vorgehensweise bei einer Datenpanne erstellt werden.
- Alle Personen und mögliche Sub-Lieferanten müssen eine Vertraulichkeitsvereinbarung unterschreiben und einhalten.
- Daten müssen, falls möglich, immer verschlüsselt übertragen werden, egal ob physisch oder elektronisch.
- Der Cloud-Anbieter sollte seine technischen und organisatorischen Massnahmen seinen Kunden offenlegen.

Fazit

Cloud-Anbieter sollten sich nach der ISO 27018 zertifizieren lassen, um den Kunden den Nachweis der Einhaltung von Sicherheitsmassnahmen, wie auch die Umsetzung der Datenschutz-Anforderungen zu bieten. Um die Zertifizierung aufrecht zu erhalten, müssen sich die Cloud-Anbieter jährlich von einer unabhängigen Stelle erneut prüfen lassen. Viele Cloud-Anbieter sind bereits zertifiziert, dazu gehören Amazon, Google oder Microsoft. Auch in der Schweiz gibt es immer mehr Cloud-Anbieter, die sich für diese zusätzliche Zertifizierung interessieren. Dieser Zertifizierungsprozess bringt besonders auch für den Cloud-Nutzer den Vorteil, die Einhaltung der Transparenz-, Informations- und Benachrichtigungspflicht überprüft zu haben.