ISACA Switzerland Chapter

Nr. 01 | März 2022 | www.isaca.ch

NEWSLETTER

ISO 27701
Wie kann ein Unternehmen nachweisen, dass es Anstrengungen zur Umsetzung des Datenschutzes umsetzt. Seite @@

ISMS-Audits
Sind ISMS-Audits vergleichbar mit IT-Revisionen? Eklatante Unterschiede des Prüfungsaufwandes sind kaum erklärbar. Seite @@

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite @@

ISO 27701 – Nachweisbarer Datenschutz?

Von Andreas Wisler

Im August 2019 wurde ohne grosses Aufsehen die ISO 27701 veröffentlicht. Im Juli 2021 folgte dann die offizielle deutsche Version der Datenschutz-Norm. Damit kann ein Unternehmen nachweisen, dass es Anstrengungen zur Umsetzung des Datenschutzes umsetzt. Der Standard trägt den offizielle Namen «Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines». Obwohl die Norm schon zwei Jahre verfügbar ist, sind die ersten Zertifizierungen erst seit wenigen Wochen möglich. Zeit als, sich genauer damit zu beschäftigen.

Der Datenschutz ist schon lange ein Thema. Die OECD hat 1980 die erste Version des Privacy Frameworks herausgegeben. In England wurde der Vorgänger zur heutigen ISO 27701 erstellt, der British Standard BS 10012:2017 mit der Erweiterung A1:2018. Mit dieser Erweiterung ist der Standard kompatibel mit der Datenschutz-Grundverordnung der Europäische Union. International fehlte bis dahin ein Pendant. Zwar war mit der ISO/IEC 27552 ein Grundlagen-Dokument vorhanden, doch das genügte nicht. Im August 2019 war es dann so weit, die ISO 27701 wurde offiziell veröffentlicht. Im Juli 2021 kam dann überraschend schnell die deutsche Version davon.

Doch die ISO 27701 kann nicht für sich allein zertifiziert werden. Die Basis ist immer ISO 27001. Bei diesem Standard geht es darum, ein Informationssicherheits-Management-Systeme, kurz ISMS, aufzubauen, zu unterhalten und weiterzuentwickeln. Zu den bereits vorhandenen Punkten kommen weitere Anforderungen.

Die wichtigste Aussage ist etwas versteckt und wird gerne überlesen, hat aber eine enorme Tragweite. Immer wenn im Standard von «information security» geschrieben wird, muss dies durch «information security and privacy» ersetzt werden. Allein diese Ersetzung gibt einiges zu bearbeiten und anzupassen.

Obschon ISO bestimmt hat, dass alle Definitionen in der ISO 27000 gesammelt werden, mussten zwei weitere Begriffe definiert werden. Es handelt sich um den «joint PII controller» (PII steht dabei für dabei für Personally Identifiable Information, personenbezogene Information) und um «privacy information management system», kurz PIMS (Deutsch: Manage-

mentsystem für Datenschutzinformationen). Der erstgenannte Begriff wird dabei wie folgt definiert: «verantwortliche Stelle, die gemeinsam mit einer oder mehreren anderen verantwortlichen Stellen die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten festlegt».

STRUKTUR

Die Struktur orientiert sich an der ISO 27001. In Kapitel 5 werden die notwendigen Erweiterungen zur ISO 27001 definiert. Dabei gibt es nur für die Kapitel 4 (Context of the organization) und Kapitel 6 (Planning) zusätzliche Massnahmen. Doch die haben es in sich. Schon nur die SoA (Statement of Applicability) zu erweitern, gibt einen grossen Aufwand.

In Kapitel 6 folgen die Erweiterungen zu den 114 Controls aus der ISO 27001. Hier ist es gerade umgekehrt. Nur zum Kapitel 17 (Information security aspects of business continuity management) hat es keine Erweiterungen. Glücklicherweise sind es aber «nur» 29 erweiterte Controls.

Leider verwendet der Standard den Begriff «Customer» für drei verschiedene Fälle:

- Vertragsbeziehung zwischen Principal (natürliche/betroffene Person) und Controller (Verantwortlicher)
- Vertragsbeziehung zwischen Controller und Processor (Verarbeitet im Auftrag)
- Vertragsbeziehung zwischen Processor und Sub-Processor

Beim Umsetzen gilt es immer alle drei Fälle zu berücksichtigen, je nachdem in welcher Rolle sich das Unternehmen selbst befindet.

Mit den Erweiterungen ist es aber nicht getan. Das Kapitel 7 definiert zusätzliche 30 Controls, die es umzusetzen gilt, wenn das Unternehmen als Verantwortlicher für die Verarbeitung von personenbezogenen Daten tätig ist. Die Unterkapitel definieren Anforderungen zu «Bedingungen für die Erhebung und Verarbeitung», «Verpflichtungen gegenüber betroffenen Personen», «Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen», «Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten».

Im Kapitel 8 folgen zusätzliche 18 Anforderungen an den Auftragsverarbeiter. Ist ein Unternehmen verantwortliche Stelle und verarbeitet auch selbst Daten, gilt es beide Kapitel umzusetzen. was zusätzliche 48 Controls bedeutet (beinahe eine Verdoppelung).

ANHÄNGE

Im Unterschied zur ISO 27001 sind die Controls nicht in einem eigenen Standard vorhanden (der ISO 27002), sondern sind direkt in einem Dokument abgedruckt. Dies macht den Standard etwas schwer lesbar. Die Anhänge A und B sind normativ, das heisst verbindlich umzusetzen, während die erwähnten Kapitel 7 und 8 informativ sind. Die Kapitel 7und 8 entsprechen damit den Anforderungen aus ISO 27002, während die Anhänge A und B dem Anhang A aus ISO 27001 entsprechen.

Die weiteren Anhänge zeigen die Verknüpfung zu anderen Normen. Der Anhang C verbindet die Controls mit der ISO/IEC 29100 (Privacy framework), der Anhang D mit der Datenschutz-Grundverordnung (DSGVO), Anhang E mit der ISO/IEC27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as Pll processors) und der ISO/IEC 29151 (Code of practice for personally identifiable information protection) und der Anhang F zeigt, wie die Controls aus ISO/IEC 27701 mit den Standards 27001 und 27002 in Verbindung gebracht werden können.

Wer sich bereits mit der ISO/IEC 29100 auseinandergesetzt hat, wird sicherlich bemerken, dass die beiden Kapitel 5.11 Information Security und 5.12 Privacy Compliance nicht übernommen wurden. Da ISO27701 ja auf Basis eines ISMS aufgebaut wird, sind diese Themen bereits genügend abgedeckt.

ZERTIFIZIERUNG

Wie kann sich nun ein Unternehmen zertifizieren lassen? Noch nicht alle Zertifizierungsstellen sind bereit für die neue Norm. Es ist jedoch bereits möglich, diese durchzuführen. Das erste Unternehmen in der Schweiz ist die SERAFE AG (Schweizerische Erhebungsstelle für die Radio- und Fernsehabgabe), welche Mitte November 2021 die aufwendige Auditierung bestand. Damit steht ein Nachweis zur Verfügung, der zeigt, dass der Datenschutz und damit verbunden das Schweizer Datenschutzgesetz eingehalten werden.

Diesem Beispiel werden weitere Firmen folgen, die gegenüber Ihren Kundinnen und Kunden einen Nachweis erbringen möchten, nicht nur die Informationssicherheit, sondern auch den Datenschutz zu berücksichtigen und alles zu unternehmen, die übergegebenen Daten zu schützen.

DER AUTOR

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO 27001 Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.