ISO 27002:2022 – Informationssicherheit neu organisiert

Wenn Sie diese Zeilen lesen, ist sie da, die neue Ausgabe der ISO 27002. Bei den ISO-Normen hat sich ein Zyklus von ca. fünf bis acht Jahren etabliert. Während die Anforderungen an das ISMS (ISO 27001) unverändert bleiben, hat sich bei den sogenannten Controls einiges getan. Dieser Artikel zeigt, was Sie erwartet und wie Sie die Veränderungen umsetzen können. Sollten Sie noch kein ISMS aufgebaut haben, können Sie direkt mit der neuen Ausgabe starten.

Bereits länger wurde diskutiert, wann der Nachfolger der in die Jahre gekommenen ISO 27002 «Information technology – Security techniques – Code of practice for information» endlich veröffentlicht wird. Normalerweise haben ISO-Normen einen Lebenszyklus von ca. fünf Jahren, hier sind es bereits neun Jahre. Im Januar 2021 wurde dann der öffentliche Draft veröffentlicht. Alle interessierten Personen konnten sich ein Bild machen und eine Rückmeldung geben. Mein Fazit: das Warten hat sich gelohnt. Die neue Ausgabe macht einen aufgeräumten und umfassenden Eindruck. Die Tragweite merkt man bereits im Titel, dieser lautet neu «Information security, cybersecurity and privacy protection — Information security controls». Es ist ersichtlich, dass die Informationssicherheit in einem globalen Kontext angeschaut wird und alle Elemente berücksichtigen möchte (Cybersecurity) und dass auch hier der Datenschutz einen grösseren Stellenwert bekommt (Privacy Protection).

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

Struktur

Am auffälligsten ist die neue Struktur. Während in der alten Norm die Massnahmen in 14 Kapitel unterteilt wurden, sind es nun nur noch deren vier. Es handelt sich um die Themenblöcke 5 Organizational controls (37), 6 People controls (8), 7 Physical controls (14) und 8 Technological controls (34). In Klammern habe ich die Anzahl Massnahmen aufgeführt.

Wer die Norm kennt, hat sicherlich bemerkt, dass es nun «nur» noch 93 Punkte sind, gegenüber den 114 bisherigen. Zusätzlich sind elf neue Massnahmen dazu gekommen. Gestrichen hingegen wurde genau eine einzige Massnahme (Es handelt sich um die 11.2.5 Removal of assets). Keine Angst, ich kann rechnen. Alle anderen Massnahmen wurden sinnvoll zusammengefasst. Ein Beispiel sind die beiden Massnahmen A.5.1.1 und A.5.1.2. Die erste verlangt die Erstellung, Freigabe, Verteilung und Schulung der Informationssicherheitskonzepte. Die zweite die regelmässige, sprich jährliche, Aktualisierung der Konzepte. Diese beiden Punkte sind nun in einem einzigen Satz zusammengefasst.

Mit den zusätzlichen elf Massnahmen erhöht sich der Aufwand zur Umsetzung zwar für ein Unternehmen, aber die neuen Punkte sind wichtig. Beispielsweise wird nun auch ein Augenmerk auf die Cloud gesetzt. Während 2013 dies eher ein Randthema war, ist es heute ohne Cloud-Nutzung in einem Unternehmen undenkbar.

Weiter ist es auch schwieriger Massnahmen als nicht zutreffend auszuklammern, wenn diese im eigenen Unternehmen nicht passen. Dies könnte beispielsweise der Fall sein, wenn ein Unternehmen keine Software entwickelt. Auch die klassischen Punkte «Ladebereiche» oder «Export von Kryptografie» sind in andere Massnahmen integriert worden und können damit nicht mehr ausgeschlossen werden.

Begriffe werden seit einigen Jahren zentral in der ISO 27000 definiert und beschrieben. So muss nicht jede der über 80 bereits erschienen 27000er-Normen dies wiederholen, damit diese einheitlich verwendet werden. Die 2022er-Ausgabe führt trotzdem 37 «neue» Begriffe ein. Teilweise werden diese aus anderen Normen angepasst übernommen (unter anderem aus ISO 9000, 15489, 22301, 27301, 27035, 27050, 29100, 29134, 30000, 31000).

Zum ersten Mal werden auch diverse Abkürzungen aufgezeigt, insgesamt sind es deren 33. Das macht das Lesen, vor allem bei langen Begriffen wie Business Continuity Management einfacher. Nun steht einfach BCM da.

Wie bereits erwähnt, sind nur noch vier Kapitel vorhanden. Folgende Definition wurde dabei getroffen:

- Kategorie «Menschen», wenn sie einzelne (oder mehrere) Menschen betreffen;
- Kategorie «Physisch», wenn sie physische Objekte betreffen;
- Kategorie «Technologie», wenn sie die Technik betreffen;
- ansonsten werden sie als «organisatorisch» eingestuft

Bewertung

Jede Massnahme hat neu eine einführende Tabelle mit folgenden Punkten:

Kontrolltyp

Der Kontrolltyp ist ein Attribut zur Betrachtung von Kontrollen aus der Perspektive, wann und wie sich die Kontrolle auf das Risikoergebnis im Hinblick auf das Auftreten eines Informationssicherheitsvorfalls auswirkt. Die Attributwerte bestehen aus #Präventiv (die Kontrolle wirkt, bevor eine Bedrohung auftritt), #Detektiv (die Kontrolle wirkt, wenn eine Bedrohung auftritt) und #Korrektiv (die Kontrolle wirkt, nachdem eine Bedrohung aufgetreten ist).

Informationssicherheit

Die Informationssicherheitseigenschaften sind die klassischen drei Schutzziele der Informationssicherheit: #Vertraulichkeit, #Integrität und #Verfügbarkeit.

Cybersicherheit

Cybersicherheitskonzepte betrachtet die Massnahmen in zeitlicher Abfolge. Sie leiten sich aus dem in der ISO/IEC TS 27101 beschriebenen Cybersicherheitsrahmenwerk ab. Die möglichen Attributwerte bestehen aus #Identify (Identifizieren), #Protect (Schützen), #Detect (Erkennen), #Respond (Reagieren) und #Recover (Wiederherstellen).

Operative Fähigkeit

Operative Fähigkeiten beschreibt das Themengebiet, zum Beispiel #Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management und #Information_security_assurance. Dies entspricht am ehesten den ehemaligen Kapiteln A.5 bis A.18.

- Sicherheitsdomäne beschreibt die Kontrollen aus der Perspektive der Informationssicherheitsbereiche, Fachwissen, Dienstleistungen oder Produkten.

Im Anhang sind alle Tabellenwerte nochmals zusammengefasst. Damit kann schnell eine passende Massnahme gefunden werden, sollte eine noch fehlen. Es hilft auch den Überblick über die Massnahmen zu behalten.

Aufbau der Massnahmen

Auch der Aufbau der Massnahme hat sich leicht verändert. Die Struktur sieht neu wie folgt aus:

- Control title: Kurzer Name der Massnahme
- Attribute table: damit ist die vorher erwähnte Tabelle gemeint
- Control: Beschreibung der Massnahme (meistens nur ein einziger Satz. Diesen finden Sie auch im Anhang der ISO 27001)
- Purpose: Erläutert den Zweck der Massnahme (verhindert Diskussionen in den Audits)
- Guidance: Implementierungsanleitung für das Massnahme: So kann man es machen, muss es aber nicht. Sie sind weiterhin frei, wie Sie die Massnahme umsetzen. Als Orientierung aber sehr wertvoll.
- Other information: Erläuternder Text oder Verweise auf andere zugehörige Dokumente

Beim Studieren der neuen ISO-Norm ist mir aufgefallen, dass einige Unklarheiten aus der bisherigen Norm präzisiert wurden. Auch wenn Sie das Gefühl haben, die Norm schon in- und auswendig zu kennen, sollten Sie alles nochmals lesen. Einige Überraschungen sind sicherlich auch für Sie enthalten.

Neue Massnahmen

Am Schluss möchte ich Ihnen noch die elf neuen Massnahmen vorstellen. Es handelt sich dabei um die folgenden (Hinweis: eigene Übersetzungen, die von der kommenden deutschen Übersetzung abweichen können):

5.7 Threat intelligence
Informationen über Bedrohungen der Informationssicherheit sollten gesammelt und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.

5.23 Information security for use of cloud services
Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.

5.30 ICT readiness for business continuity
Die ICT-Bereitschaft sollte auf der Grundlage von Geschäftskontinuitätszielen und ICT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und getestet werden.

Hinweis: Das Kapitel A.17 ging schon auf das Thema BCM ein, nun wurde es aber klarer formuliert, was zu tun ist. Ein eigenes BCM ist aber noch immer nicht gefordert. Hier gibt es die ISO 22301, die den Aufbau eines BCM-Managementsystems beschreibt.

7.4 Physical security monitoring
Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.

Hinweis: dies erweitert die physische Zugangsregelung.

8.9 Configuration management
Konfigurationen, einschliesslich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzen sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

Hinweis: dies erweitert die geforderten Betriebsdokumentationen aus A.12.1.1.

8.10 Information deletion
In Informationssystemen und Geräten gespeicherte Informationen sollten gelöscht werden, wenn sie nicht mehr benötigt werden.

Hinweis: hier wird der Datenschutz berücksichtigt.

8.11 Data masking
Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugriffskontrolle und den geschäftlichen Erfordernissen unter Berücksichtigung der rechtlichen Anforderungen eingesetzt werden.

Hinweis: zum Beispiel durch Pseudonymisierung.

8.12 Data leakage prevention
Massnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und Endgeräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

Hinweis: hier rechne ich mit dem grössten Aufwand für ein Unternehmen. So einfach ist diese Massnahme nicht umzusetzen. Ein umfassendes Konzept muss im Vorfeld erstellt werden.

8.16 Monitoring activities
Netze, Systeme und Anwendungen sollten auf anormales Verhalten hin überwacht und geeignete Massnahmen ergriffen werden, um mögliche Vorfälle im Bereich der Informationssicherheit zu bewerten.

Hinweis: damit sind klassische Monitoring-, aber auch Intrusion Detection Systeme gemeint.

8.22 Web filtering
Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.

Hinweis: damit sind unter anderem Web-Filter, wie sie die meisten Firewalls heute bieten, gemeint.

8.28 Secure coding
Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.

Hinweis: dies präzisiert Massnahmen aus dem alten Kapitel A.14.2. Hier waren die Grundsätze «gut» versteckt.

Anhang

Im ersten Teil (Anhang A) werden wie oben erwähnt alle Steuerelemente und Attribute der Massnahmen nochmals aufgezeigt. Es wird ebenfalls aufgezeigt, wie die entsprechenden Massnahmen auszuwählen und zu bewerten sind.

Der Anhang B zeigt die Verknüpfung der neuen Massnahmen zu den Massnahmen aus ISO 27002:2013 sowie umgekehrt von der alten zur neuen ISO 27002:2021. Damit sind Sie nicht auf Grafiken von Beratern angewiesen, die es nur gegen E-Mail-Adresse gibt.

Fazit

Die ISO 27002 hat einen komplett neuen Anstrich bekommen. Die bisherigen Massnahmen wurden in vier Kategorien unterteilt und wo sinnvoll zusammengeführt. Elf Massnahmen sind neu dazugekommen, jedoch nur eine einzige gestrichen. In der Summe sind es nun 93 Massnahmen. Die Erweiterung mit Steuerelementen und Attributen zeigt, was mit einer Massnahme bezweckt wird. Die 2022er-Version hinterlässt einen sauberen und umfassenden Eindruck. Jedoch ist es nicht damit getan, nur die elf neuen Massnahmen umzusetzen, denn in den bekannten Massnahmen «verstecken» sich neue beziehungsweise erweiterte Anforderungen. Für alle aktiven ISMS startet mit der Veröffentlichung eine Übergangs- oder Schonfrist von zwei Jahren. Danach muss Ihr ISMS ebenfalls nach der neuen Norm aufgebaut sein. Da «nur» die Massnahmen ändern, ist dies aber gut machbar.

Hinweis

In der Folge 31 des Podcasts «Angriffslustig» besprechen Andreas Wisler und Sandro Müller die Draft-Version der ISO 27002:2021.
Anzuhören ist der Podcast unter https://podcast5a4372.podigee.io/31-iso-27002-2021.