Bild: Pixabay

ISO 27001: Neue Massnahmen

Ende Oktober 2022 wurde nach fast neun Jahren die ISO 27001 in einer aktualisierten Form herausgegeben. Während sich beim Informationssicherheits-Managementsystem (ISMS) nur wenig verändert hat, wurde der Anhang komplett überarbeitet. Anstelle 14 Kapiteln sind es nur noch deren vier. Bis anhin waren es 114 Massnahmen, elf kamen dazu und eine einzige wurde gestrichen, sind es neu 93. Falls Sie jetzt das Gefühl haben, der Autor könne nicht rechnen. Doch kann er. Einige Massnahmen wurden sinnvoll zusammengefasst.

Die Massnahmen werden in folgende Kategorien eingeteilt:
- Menschen (Kapitel 8, 34 Anforderungen), wenn sie einzelne Menschen betreffen;
- Physisch (Kapitel 7, 14 Anforderungen), wenn sie physische Objekte betreffen;
- Technologisch (Kapitel 6, 8 Anforderungen), wenn sie die Technik betreffen;
- ansonsten werden sie als organisatorisch (Kapitel 5, 37 Anforderungen) eingestuft.

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

Weiter werden 38 neue Begrifflichkeiten definiert. Teilweise wurden diese aus den folgenden ISO-Normen entnommen: 9000, 15489, 22301, 27301, 27035, 27050, 29100, 29134, 30000, 31000. Damit ist eine einheitliche, normenübergreifende Zusammenarbeit möglich. Gleichzeitig wurden im englischen 33 und im deutschen Entwurf 45 Abkürzungen definiert. Dies macht das Lesen der Norm an vielen Stellen einfacher.

Jede Massnahme wurde mit fünf Attributen mit entsprechenden Werten versehen:
- Die Massnahmenart (Englisch Control type) beschreibt, zu welchem Zeitpunkt eines Informationssicherheitsvorfalls sich die Massnahme auf das Risiko auswirkt: Präventiv (Verhindern des Vorfalls), Detektiv (wenn der Vorfall eintritt) und Korrektiv (nach dem der Vorfall eingetreten ist)
- Die Informationssicherheitseigenschaften (Englisch Information security properties) zeigen, auf welches Grundschutzziel (Vertraulichkeit, Integrität, Verfügbarkeit) sich die Massnahme auswirkt.
- Das Attribut Cybersicherheitskonzepte (Englisch Cybersecurity concepts) ist unterteilt in Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Damit ist eine Verknüpfung mit anderen Normen und Frameworks wie das NIST Cybersecurity Framework möglich.
- Das Attribut Betriebsfähigkeit (Englisch Operational capabilities) teilt sich auf in Governance, Werte-Management, Informationsschutz, Menschliche Sicherheit, physische Sicherheit, System- und Netzwerksicherheit, Anwendungssicherheit, sichere Konfiguration, Identitäts- und Zugangsverwaltung, Bedrohungs- und Schwachstellenmanagement, Kontinuität, Sicherheit der Lieferantenbeziehungen, Recht und Compliance, Informationssicherheits-Ereignis-Management und Vertrauenswürdigkeit.
- Das Attribut Sicherheitsdomäne unterteilt sich in Governance und Ökosystem (Risikomanagement, Cybersicherheitsmanagement), Schutz (IT-Sicherheitsarchitektur und -verwaltung, Identitäts- und Zugangsverwaltung, IT-Sicherheitswartung und physische und umgebungsbezogene Sicherheit), Verteidigung (Erkennung, Management von Computersicherheitsvorfällen) und Resilienz (Betriebskontinuität und Krisenmanagement)

5.7 Bedrohungsintelligenz (Englisch: Threat intelligence)

Anforderung: Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen. Die Organisation muss Prozesse etablieren, um sich über bestehende und neu auftretende Bedrohungen schnell informieren zu können. Dabei müssen sowohl die strategischen (Infors über sich verändernde Bedrohungslandschaft), taktischen (Methoden, Werkzeuge und Technologien von Hackern) sowie operativen Bedrohungsdaten (Details zu Angriffen) ausgewertet werden.

Weiter sollte die Bedrohungsanalyse Ziele (ausgerichtet auf das Unternehmen, die vorhandenen Systeme, usw.) definieren, interne und externe Informationsquellen bestimmen, Verantwortlichkeiten und Art zur Auswertung dieser Quellen sowie die Kommunikation und Weitergabe enthalten.

Die Informationen können dazu genutzt werden Bedrohungen zu verhindern, zu erkennen oder darauf zu reagieren.

5.23 Informationssicherheit für die Nutzung von Cloud-Diensten (Information security for use of cloud services)

Anforderung: 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.

In der bisherigen Ausgabe der ISO 27002:2013 war die Cloud

noch kein Thema. Da neun Jahre später kaum ein Weg an der Cloud vorbeiführt, trägt die Norm mit der neuen Massnahme dem veränderten Umfeld Rechnung. Die Norm sagt dies in klaren Worten: «Es ist von entscheidender Bedeutung, dass die Verantwortlichkeiten sowohl für den Cloud-Dienstleister als auch für die Organisation, die als Cloud-Kunde auftritt, angemessen definiert und umgesetzt werden.».

Dazu gehören die Definition von Anforderungen an die Nutzung, Auswahlkriterien, Rollen und Verantwortlichkeiten, welche Massnahmen selber und welche vom Anbieter umgesetzt werden müssen, die Steuerung von Schnittstellen und Änderungen, vorbereitende Verfahren beim Eintreten von Informationssicherheitsvorfällen, Kriterien zur Überwachung, Überprüfung und Bewertung der Cloud-Dienstleistung sowie Vorgehen bei Änderung oder Ausstieg der Cloud-Nutzung. Dies liest sich einfacher, als es oft ist. Viele Cloud-Dienste sind vordefiniert und können nicht verhandelt werden. Trotzdem sollte versucht werden, die obenstehenden Anforderungen umsetzen zu können. Ein Gespräch kann sich sicherlich lohnen. Auf jeden Fall gilt es die mit der Nutzung verbundenen Risiken zu ermitteln und zu bewerten. Die Norm geht weiter auf die Punkte, die vertraglich gelöst werden sollten, ein:

- Nutzung von anerkannten Normen
- Anforderungen an die Zugangssteuerung (zum Beispiel zusätzlicher Schutz mit 2FA)
- Überwachung und Schutz vor Malware
- Bestimmung/Einschränkung von Ländern oder Regionen
- Unterstützung bei einem Informationssicherheitsvorfall
- Regeln bei der Vergabe an weitere Dienstleister (Supply Chain)
- Mithilfe bei der Sammlung von forensischen Spuren
- Unterstützung und Support, auch beim Verlassen des Cloud-Anbieters
- Möglichkeit zur Erstellung von Sicherheitskopien (Daten und Konfigurationen)
- Rückgabe von Quellcode und Daten, die Eigentum des Unternehmens sind
- Informationspflicht des Anbieters bei Änderungen an der technischen Infrastruktur

5.30 IKT-Bereitschaft für Business Continuity (ICT readiness for business continuity)

Anforderung: Die IKT-Bereitschaft sollte auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.

Wer die bisherige Norm kennt, wird sich vermutlich fragen, was hier neu sein soll. Das Kapitel A.17 behandelte Business Continuity. Bis anhin sollten «nur» die Informationssicherheitsaspekte beim BCM berücksichtigt werden. Ein eigentliches BCM wurde nicht gefordert. Neu wird gefordert, dass die Verfügbarkeit der Informationen und anderer Werte während einer Störung sichergestellt sind. Dazu sollten die Anforderungen auf einer Business Impact Analyse (BIA) basieren, in welcher die Wiederherstellungsdauer (RTO, Recovery Time Objective) und die Wiederherstellungspunkte (RPO, Recovery Point Objective) bestimmt werden. Anhand dieser Grundlage können Strategien und Verfahren erarbeitet werden. Dazu gehören die involvierten Personen, Kontinuitätspläne (inkl. Reaktions- und Wiederherstellungsverfahren), regemässige Übungen und Prüfungen.

7.4 Physische Sicherheitsüberwachung (Physical security monitoring)

Anforderung: Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.

Auch die Anforderungen an die physische Sicherheit waren in der 2013er-Version ein Thema (Kapitel A.7). Diese werden nun verschärft. Es sollten Überwachungssysteme vorgesehen werden, dazu können Wachpersonal, Einbruchalarm (zum Beispiel Kontakt-, Schall- oder Bewegungsmeldern), Alarme für alle Aussentüren und zugänglichen Fenster sowie Videoüberwachungssysteme gehören. Insbesondere der Zutritt zu kritischen Systemen sollte ständig überwacht werden.

Natürlich gilt es auch diese Systeme zu schützen, damit nicht Unbefugte auf Überwachungsdaten zugreifen können. Die Alarme sollten zentral ausgewertet werden. Für die Speicherung müssen die Gesetze und Vorschriften beachtet werden, zum Beispiel die Löschpflicht bei Videoaufnahmen.

8.9 Konfigurationsmanagement (Configuration management)

Anforderung: Konfigurationen, einschliesslich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

Die technischen Anforderungen wurden im Kapitel A.12 behandelt. Neben der Dokumentation muss gewährleistet sein, dass Sicherheitseinstellungen von Hardware, Software, Diensten und dem Netzwerk nicht durch Unbefugte verändert werden. Dazu sind Prozesse und Werkzeuge zu definieren, mit denen dies umgesetzt werden kann. Auch Rollen, Verantwortlichkeiten und Verfahren gehören dazu. Die Norm empfiehlt Standardvorlagen für die sichere Konfiguration zu erstellen. Basis dafür können öffentliche Leitfäden sein (zum Beispiel von SANS, www.sans.org/information-security-policy/ oder die CIS-Benchmarks, www.cisecurity.org/cis-benchmarks-overview). Firmenintern gehören die definierten Schutzstufen, die Informationssicherheitspolitik sowie Ergebnisse von Prüfungen dazu. Zu einer sicheren Konfiguration sollten die Anzahl von administrativen Accounts eingeschränkt, nicht benötigte Accounts und Funktionen deaktiviert, Standardkennwörter sofort geändert und vorhandene Sicherheitseinstellungen genutzt werden.

Neben den korrekten Einstellungen sollten diese auch sicher verwaltet werden. Dazu wird auf den Change-Management Prozess verwiesen (8.32). Folgende Informationen gilt es zu speichern: Eigentümer, Datum/Zeit der letzten Änderung sowie die Version der genutzten Vorlage.

Der dritte Schritt umfasst die Überwachung und Bewertung der Konfigurationen. Sollten Abweichungen festgestellt werden, muss darauf reagiert und Korrekturmassnahmen eingeleitet werden.

8.10 Löschung von Informationen (Information deletion)

Anforderung: Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.

Während die 2013er-Ausgabe den Schutz von Aufzeichnungen verlangt und auch kurz deren Löschung erwähnt, geht die neue Massnahme gezielt auf das Thema der Löschung ein. Viele Datenschutzgesetze verlangen ebenfalls die Löschung von Informationen, die nicht mehr benötigt werden. Bei der Löschung sollte ein geeignetes Verfahren definiert werden. Dazu gehören auch Daten auf externen Speichersystemen, in Cloud-Diensten oder bei ausgelagerten bei Lieferanten und/oder Partnern. Die Löschung gilt es als Beweismittel aufzuzeichnen. Nicht vergessen werden dürfen veraltete Versionen, Kopien und temporäre Dateien. Ein Augenmerk sollte daher bei der Wiederherstellung oder bei forensischen Tools beachtet werden. So könnten bereits gelöschte Daten wieder verfügbar sein. Bei Geräten, wie zum Beispiel Smartphones, bei welchen eine Löschung nur schwierig möglich ist, sollte eine Zerstörung oder spezielle Löschverfahren angewendet werden.

8.11 Datenmaskierung (Data masking)

Anforderung: Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden. Zum Schutz sensitiver Daten sollten Verfahren wie Maskierung, Pseudonymisierung oder Anonymisierung genutzt werden. Nicht alle Daten müssen so geschützt werden, daher gilt es zu definieren, welche dies sind. Bei der Pseudonymisierung (also dem Ersetzen durch ein Pseudonym) ist es wichtig, dass der Zusammenhang zwischen den verschleierten und ursprünglichen Daten nicht gefunden werden kann. Oft wird dazu ein Hash-Verfahren oder die Verschlüsselung genutzt. Einige Software-Systeme bieten auch bereits fertige Funktionen an, um dies einfach und schnell umzusetzen. Sicherer sind Anonymisierungen, aber gerade für Auswertungen und statische Berechnungen ist diese ungeeignet.

8.12 Verhinderung von Datenlecks (Data leakage prevention)

Anforderung: Massnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

Diese Massnahme ist vermutlich am aufwendigsten umzusetzen. Um Datenlecks zu verhindern, müssen diverse Vorbereitungen getroffen werden:

- Informationen sind zu identifizieren und zu klassifizieren.
– Die (Übertragungs-)Kanäle sind zu überwachen. Dazu gehören E-Mail, mobile Geräte, Speichermedien, aber auch Transferplattformen und Cloud-Speicher.
– Schutz-Massnahmen wie Gateways und Scanner sind zu implementieren.

In einem zweiten Schritt werden Werkzeuge zur Verhinderung von Datenlecks eingesetzt. Anhand der definieren Kriterien werden beispielsweise Verbindungen erkannt und unterbrochen, bevor sensitive Informationen offengelegt werden. Nicht alles kann technisch verhindert werden. Da-

her gilt es die Mitarbeitenden regelmässig auf dieses Thema zu sensibilisieren. Dies beinhaltet auch das Anfertigen von Screenshots oder das Fotografieren des Monitors. Warnungen wie Banner oder Meldungen warnen die Mitarbeitenden, bevor sie eine Tätigkeit ausführen.

8.16 Überwachung von Aktivitäten (Monitoring activities)

Anforderung: Netzwerke, Systeme und Anwendungen sollten auf anormales Verhalten überwacht und geeignete Massnahmen ergriffen werden, um potenzielle Informationssicherheitsvorfälle zu bewerten.

Bevor mit der Überwachung gestartet werden kann, gilt es die Geschäfts- und Informationssicherheitsanforderungen festzuhalten. Dabei müssen Gesetze und Vorschriften bei der Überwachung, Speicherung und Auswertung beachtet werden.

Die Norm erwähnt bei den zu überwachenden Aktivitäten ein- und ausgehenden Netzwerkverkehr, Zugang zu Systemen und Servern, Änderungen von Konfigurationen, Protokolle von Sicherheitstools (dazu gehören unter anderem Antivirenprogramme, IDS, Filter, Firewalls), Eventlogs von Systemen, Nutzung von Ressourcen, usw.

Die gesammelten Informationen gilt es auf Anomalien zu untersuchen. Dazu gehören ungeplante Unterbrüche von Prozessen und Anwendungen, Malware-Aktivitäten, bekannte Angriffsmuster, ungewöhnliches Systemverhalten, unbekannte Anmeldeversuche, Netzwerkscans, ungewöhnliches Benutzerverhalten und vieles mehr. Da dies manuell nicht möglich ist, werden automatisierte Tools oder sogenannte SOC (Security Operation Center) benutzt. Die Reaktion bei Warnmeldungen sollte in beiden Fällen definiert, geschult und regelmässig getestet werden.

8.23 Webfilterung (Web filtering)

Anforderung: Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.

Die grösste Gefahr geht heute vom Internet aus. Webseiten können einfach verändert und mit Malware infiziert werden. Wird eine solche Seite besucht, kann ein Schädling in des Firmennetzwerk gelangen. Diese Technik wird Drive-by genannt. Um dieses Risiko zu verringern, sollten Filter-Systeme eingesetzt werden. Viele Anbieter bieten dazu Blacklisten an. Diese sind mit den firmenspezifischen Anforderungen zu erweitern. Die Mitarbeitenden sind in einer IT-Weisung (die Norm spricht auch von Zulässiger Gebrauch, Acceptable Use Policy) auf diesen Umstand aufmerksam zu machen. Dazu gehören auch Schulungen.

8.28 Sicheres Coding (Secure coding)

Anforderung: Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.

Auch diese Massnahme sollte den erfahrenen Normenlesern bekannt vorkommen. In der 2013er-Ausgabe wird von der Sicherheit in Entwicklungs- und Unterstützungsprozessen gesprochen. Eine eigene Massnahme zur Entwicklungssicherheit fehlt aber.

Bei der Erarbeitung von Grundsätzen der sicheren Software-Entwicklung gehören sowohl die Neu- wie auch die Weiterentwicklung von Software dazu und werden über den gesamten Lebenszyklus angewendet. Diese Richtlinien gelten sowohl für die interne, wie auch für ausgelagerte Entwicklung und enthalten Best-Practice-Ansätze, Anforderungen an die Entwicklungsumgebung, Werkzeuge, Qualifikation von Entwicklern und die Architektur.

Die Norm geht weiter auf sicherheitsrelevante Tätigkeiten während der Entwicklung ein. Dazu gehören sichere Codierungspraktiken, strukturiere Programmierung, die Dokumentation des Codes und das Verbot zur Nutzung unsicherer Techniken ein. Die Nutzung von statischen Anwendungssicherheitstests (Static application security testing, SAST) können Sicherheitsschwachstellen in Software aufdecken (mögliche Angriffsfläche, nicht eingeschränkte Berechtigungen, Erkennung von häufigen Programmierfehlern, usw.).

Nachdem die Software in Betrieb genommen wurde, gilt es die Wartung mittels der Behandlung von Schwachstellen durch Updates, Protokollierung von Fehlern und den Schutz des Quellcodes sicherzustellen.

Insbesondere bei der Verwendung externer Tools und Bibliotheken gilt es erkannte Schwachstellen schnell zu schliessen. Beachtet werden muss auch die Lizenz, beziehungsweise was mit den eingesetzten Komponenten erlaubt beziehungsweise möglich ist.

Fazit

Die neuen Massnahmen erweitern die vorhandenen um wichtige Themen. Gerade die Nutzung von Cloud-Diensten gilt es sicher zu regeln. Auch die Datenschutzanforderungen wurden durch mehrere Massnahmen berücksichtigt. Für die Umsetzung ist genügend Zeit einzuplanen.

In der Schweiz wird es ab ca. April möglich sin, sich nach der neuen Norm zertifizieren zu lassen. Die letzte Möglichkeit für eine Erst- oder Rezertifizierung nach der alten ISO 27001:2013 (Englische Ausgabe)/2017 (Deutsche Ausgabe) ist 18 Monate, beziehungsweise April 2024. Bestehende Zertifizierungen haben noch eine Gültigkeit von drei Jahren, das heisst max. bis Oktober 2025.

Es ist somit noch etwas Zeit vorhanden. Für die Umsetzung ist jedoch genügend Zeit einzuplanen. Es lohnt sich, frühzeitig mit der Planung und anschliessender Umsetzung zu beginnen.