ISO 27001: Der Weg zur Zertifizierung

Die Informationssicherheit ist ein wichtiges Thema. Auch in der Schweiz ist immer wieder von erfolgreichen Angriffen zu lesen, teilweise mit gravierenden Folgen für das betroffene Unternehmen. Mit dem Aufbau eines Informationssicherheitsmanagementsystems, kurz ISMS, wird dieses Thema nicht nur punktuell, zum Beispiel in der IT, angeschaut, sondern über das gesamte Unternehmen. Die Krönung ist die Zertifizierung nach ISO 27001. Akkreditierte Auditoren prüfen, ob das ISMS auch das tut, was definiert wurde. Doch bis dahin ist es ein weiter Weg.

Im ersten Schritt gilt es die Unterstützung der Geschäftsleitung und/oder Verwaltungsrats einzuholen. Bei einigen Massnahmen steht «die oberste Leitung muss». Es ist unmissverständlich klar, wer dafür zuständig ist.

Sobald das Projekt bewilligt wurde, wird ein Projektplan erstellt. Darin sind die involvierten Personen, ein vernünftiger Zeitrahmen sowie die Rahmenbedingungen enthalten.

Die Norm verlangt die Anforderungen an die Informationssicherheit zu definieren. Diese Anforderungen kommen vom eigenen Unternehmen, aber auch von Interessensvertretern, vertraglichen und rechtlichen Anforderungen. Dazu sollten unter anderem die folgenden Fragen beantwortet werden:

- Welche Geschäftsprozesse gibt es und wie hängen diese mit den Geschäftszielen zusammen?
- Welche Geschäftsprozesse hängen von einer funktionierenden, also einer ordnungsgemäss und anforderungsgerecht arbeitenden IT ab?
- Welche Informationen werden für diese Geschäftsprozesse verarbeitet?
- Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (zum Beispiel personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?
- Gibt es Partner, Kunden oder weitere Stellen, die Zugriff auf Firmenwerte benötigen?
- Welche vertraglichen Anforderungen müssen erfüllt werden?
- Gibt es rechtliche Vorschriften, die es einzuhalten gilt?

Erst jetzt wird der Anwendungsbereich definiert. Bei der ISO 27001 kann auch ein einzelner Bereich eines Unternehmens zertifiziert werden, zum Beispiel der Betrieb eines Rechenzentrums für Kunden-Systeme. Wird dies gemacht, müssen die Schnittstellen sehr genau definiert werden, damit klar ist, was darin enthalten ist und was nicht. Anhand dieser Vorgaben wird die Informationssicherheitspolitik geschrieben. Sie definiert die Ziele, Struktur und Organisation der Informationssicherheit.

Ein essenzielles Thema ist die systematische Erfassung und Bewertung von Risiken. Diese Tätigkeit benötigt einiges an Zeit. Erfassen Sie zuerst die Prozesse, die darin verarbeiteten Informationen und die Kritikalität. Diese Kritikalität vererbt sich anschliessend über die genutzten Applikationen auf die Systeme, Netzwerke, Räume und involvierten Personen. Auf diese Kette wirken sich Bedrohungen und Schwachstellen aus. Bewerten Sie die Auswirkungen und die Wahrscheinlichkeiten für verschiedene Szenarien, damit Sie angepasste Schritte definieren und umsetzen können. Der Anhang A der ISO 27002:2013 enthält 114 (beziehungsweise die ISO 27002:2022 93) Massnahmen.

Parallel dazu werden diverse Konzepte erstellt. Auch die Awareness aller Mitarbeitenden gehört dazu. Alle müssen die Regeln können und einhalten. Zu den Aufgaben gehören auch Kontrollen zu diversen Themen der Informationssicherheit.

Je nach den zur Verfügung stehenden Ressourcen steht nach einem halben bis einem ganzen Jahr das Interne Audit an. Die

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

erste Generalprobe. Ein Auditor wird dazu bestimmt, der sowohl das Managementsystem wie auch die umgesetzten Massnahmen auf Herz und Nieren überprüft. Es spielt dabei keine Rolle, ob der Auditor vom eigenen Unternehmen stammt oder von einer externen Firma. Wichtig ist die Unabhängigkeit, welche von der Norm explizit gefordert wird. Der CISO fällt hier in der Regel weg, da er selbst viele Dokumente erstellt oder umgesetzt hat und viele Kontrollen durchführt. Ein externer Auditor bringt zudem oft frischen Wind ins ISMS, stellt vielleicht auch mal eine andere Frage und gibt Empfehlungen zur Verbesserung des ISMS. Es können auch Abweichungen von der Norm festgestellt werden. Lieber beim internen Audit als beim Zertifizierungs-Audit. So bleibt noch genügend Zeit, die Abweichung zu beheben.

Nachdem die Management-Bewertung durchgeführt wurde, kann das ISMS zur Zertifizierung angemeldet werden. In der Schweiz gibt es drei Firmen, die von der schweizerischen Akkreditierungsstelle SAS (www.sas.admin.ch/) akkreditiert sind. Es sind dies KPMG, SQS und Swiss Safety Center. Es können aber auch akkreditierte Stellen aus dem Ausland beigezogen werden. Wichtig ist, dass dieses Unternehmen von einer Stelle akkreditiert ist, die in einem Member-Land der IAF (International Accreditation Forum, https://iaf.nu/) ist.

Der notwendige Prüf-Aufwand für das Audit wird anhand eines Fragebogens bestimmt. In der ISO 27006 ist festgehalten, wie lange ein Audit zu dauern hat und unter welchen Umständen die aufzuwendende Zeit gekürt oder verlängert werden kann. Zwei entscheidende Faktoren bei der Berechnung sind die Anzahl Standorte und die Anzahl Mitarbeitenden im Anwendungsbereich.

Das Audit wird in zwei Stufen durchgeführt. Im ersten Schritt werden die notwendigen Dokumente und der Stand des ISMS geprüft. Ist alles in Ordnung, kann frühestens nach einem Monat oder spätestens nach einem halben Jahr die Vor-Ort-Kontrolle durchgeführt werden. Das ISMS und die Massnahmen werden auf ihre Funktionsweise und Richtigkeit geprüft. Von jedem der 114 beziehungsweise 93 Massnahmen werden Stichproben gezogen. Dabei kann auch mal etwas nicht ganz wie gewünscht funktionieren. Im Audit wird unterschieden zwischen:

- Verbesserung: Möglichkeit, das ISMS zu verbessern. Verbesserungen müssen nicht zwingend umgesetzt werden. Es sollte aber nachvollziehbar sein, warum eine vorgeschlagene Verbesserung nicht umgesetzt wurde.
- Nebenabweichung: die Norm-Anforderung (oder auch eine eigene Definition) wurde nur teilweise erfüllt.
- Hauptabweichung: die Norm-Anforderung wurde nicht erfüllt.

Bei Abweichungen muss die Ursache bestimmt und Korrekturmassnahmen geplant werden. Je nach Kritikalität der Abweichung wird die Wirksamkeit der Korrekturen nach kurzer Zeit oder spätestens beim nächsten Audit kontrolliert. Eine Hauptabweichung kann auch zum Abbruch des Audits führen, dann ist aber vorher bereits einiges schiefgelaufen. Haben Sie aber keine Angst vor Abweichungen! Je komplexer das Unternehmen ist, desto höher ist die Wahrscheinlichkeit, dass im ersten Anlauf noch nicht alle Controls vollständig erfüllt wurden. Sind die Auditoren zufrieden, erhalten Sie kurze Zeit später den Audit-Bericht sowie ein Zertifikat als Nachweis der Funktionsweise Ihres ISMS.

Der gestartete Kreislauf der kontinuierlichen Verbesserung steht nun aber nicht still, sondern dreht sich kontinuierlich weiter. Abweichungen und Verbesserungen erfassen, Massnahmen planen, umsetzen, Wirksamkeit prüfen. Dies ist nun Alltag.

Obwohl auf dem Zertifikat eine Gültigkeit von drei Jahren ausgewiesen ist, findet jährlich ein Audit statt. Im ersten und zweiten Jahr nach der Zertifizierung ist dies das Überwachungsaudit. Es muss spätestens nach einem beziehungsweise zwei Jahre zum auf dem Zertifikat aufgedruckten Datum durchgeführt sein.

Nach drei Jahren steht die Rezertifizierung an. Sie muss so geplant sein, dass eine nahtlose Verlängerung möglich ist. Mindestens einen Monat vor Ablauf, bei einigen Audit-Stellen sogar noch etwas früher, muss es erfolgt sein, damit noch genügend Zeit für den Bericht und die interne Kontrolle übrigbleibt. Die ISO 17021-1 definiert in Ausnahmefällen, das Audit erst bis maximal sechs Monate nach der Gültigkeit durchzuführen. Während dieser Zeit darf jedoch keine Werbung gemacht werden, da das Unternehmen den Status «nicht zertifiziert» hat. Das Datum auf dem neuen Zertifikat ist dann aber um diese Zeit verkürzt abgedruckt.

Der Weg vom Start bis zur Zertifizierung umfasst viele Schritte. Da der Alltag nicht stehen bleibt, ist mit einer Dauer von einem halben bis zu einem ganzen Jahr zu rechnen. In dieser Zeit werden Grundlagen erarbeitet, Risiken erfasst und behandelt, die Mitarbeitenden geschult, diverse Kontrollen durchgeführt und die Informationssicherheit stetig verbessert. Mit der Zertifizierung steht ein Nachweis dieser Anstrengungen und der guten Funktionsweise Ihres ISMS für Kunden, Lieferanten und Partner zur Verfügung.