ISO 27001: Risikomanagement

Kapitel 6 der ISO-Norm 27001 setzt sich mit der Planung auseinander. Der Schwerpunkt ist dabei der Umgang mit Risiken und Chancen. Die Norm verlangt, dass die im Kapitel 4.1 (Kontext) und 4.2 (Verstehen der Erfordernisse und Erwartungen interessierter Parteien) erkannten Anforderungen berücksichtigt werden. Daher ist es essenziell wichtig, die beiden Kapitel sauber durchzuarbeiten und möglichst genau das Unternehmen zu verstehen, inklusive aller Schnittstellen.

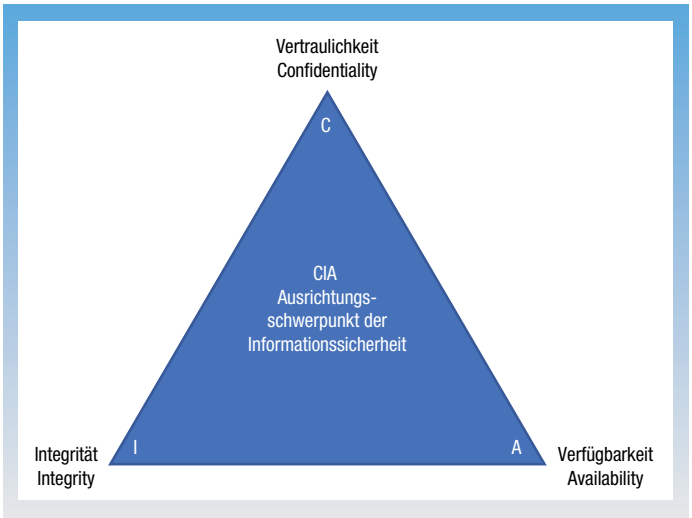

Bild 1: Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen.

Weiter gilt es die Chancen und Risiken zu bestimmen, damit die Ergebnisse des ISMS auch die gesetzten Ergebnisse erreichen, negative Auswirkungen reduziert oder noch besser verhindert und das ISMS fortlaufend verbessert wird. Das Risiko-Management ist also keine einmalige Aufgabe. Die Anforderungen an ein Unternehmen können sich jederzeit verändern. Neue Gesetze, neue Dienstleistungen, ein neuer Mitbewerber, ein (Sicherheits-)Vorfall usw. können jederzeit eintreten und neue Risiken schaffen oder eliminieren. Jede Massnahme, die getroffen wird, sollte auf seine Wirksamkeit bewertet werden. Im Kapitel 9 werde ich dazu weitere Hinweise geben.

Es gilt also nun, einen Risikobeurteilungsprozess zu etablieren. In der Norm wird zwar immer von einer Informationssicherheitsrisikobeurteilung gesprochen, ich versuche aber immer dieses Thema in das gesamte Firmen-Risikomanagement zu integrieren. Die Informationssicherheit sollte keine Insellösung sein. Die Norm verlangt, dass Kriterien zur Akzeptanz von Risiken definiert werden: wann sind Risiken akzeptiert, das heisst es wird nichts (mehr) unternommen und wann müssen zwingend Massnahmen ergriffen werden.

Risikoanalyse: Kriterien definieren

Für die Durchführung einer Risikoanalyse sollten die Kriterien definiert werden, also: Wer, wie, wann, Art der Dokumentation, usw. Es ist wichtig, dass bei einer erneuten Durchführung konsistente und vergleichbare Ergebnisse erzielt werden.

Wie ist nun das Vorgehen, um eine gute Aussage erhalten zu können? In einem ersten Schritt werden die vorhandenen Prozesse identifiziert. Was wird in diesen gemacht? Welche Daten werden verarbeitet? Welche Kritikalität haben diese Prozesse? Welche Personen sind involviert? Welche (technischen) Systeme werden genutzt? Somit haben wir bereits Prozesse und Werte. Im englischen wird das Wort Asset verwendet, was etwas genauer sagt, um was es geht. Es sind dabei nicht nur Server, Laptops usw. gemeint, sondern auch Papier-Unterlagen, Wissen, Patente usw. Im Kapitel A.8 gehe ich genauer auf das Werte-Management ein. Die identifizierten Werte werden einem Besitzer (Owner, Verantwortlicher) zugewiesen und die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen bestimmt (Bild 1).

Verfügbarkeit (Availability)

Die Verfügbarkeit eines Systems wird umschrieben mit der Eigenschaft, sämtliche Daten und Funktionen zu einem bestimmten Zeitpunkt zur Verfügung stellen zu können.

Integrität (Integrity, Unversehrtheit)

Lässt ein System unbefugte oder unbeabsichtigte Veränderungen an Daten oder an der Software zu, so ist deren Integrität verletzt. Es kann somit nicht mehr garantiert werden, dass alle sicherheitsrelevanten Objekte vollständig, unverfälscht und korrekt sind.

Vertraulichkeit (Confidentiality)

Darunter wird verstanden, dass nur bestimmte Personen oder Prozesse auf Daten oder Systeme zugreifen können oder dürfen. Soll die Vertraulichkeit gewahrt werden, müssen die Daten so gesichert sein, dass ein Zugriff nur denjenigen Nutzern möglich ist, welche durch Zugriffsrechte die Erlaubnis erhalten.

Nun gilt es mögliche Bedrohungen zu identifizieren. Normalerweise tritt ein Risiko dann ein, wenn eine Bedrohung und eine Schwachstelle aufeinandertreffen. Eine Bedrohung alleine muss noch kein Risiko bedeuten. Erst wenn eine Schwachstelle vorhanden ist, ergibt sich ein Risiko. Wenn zum Beispiel eine Schwachstelle in einer Software vorhanden ist, ist dies zwar ärgerlich, aber noch kein Grund in Panik zu verfallen. Sobald aber ein Programm oder schon nur eine Anleitung (sogenanntes Proof of Concept) zur Ausnutzung der Schwachstelle vorhanden ist, existiert eine reale Bedrohung (Bild 2).

Das Risiko bewerten

Das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI hat ein tolles Werkzeug für alle möglichen Bedrohungen erarbeitet. Die Grundschutzkataloge, zu finden unter www.bsi.de/gshb, listen in sechs Kategorien über 700 Gefährdungen auf. Das BSI arbeitet ohne Schwachstellen und weist die Bedrohungen direkt den Werten zu. BSI nennt diese Werte Bausteine. Wenn Sie unsicher sind, welche Bedrohungen für einen Wert existieren, gehen Sie zum entsprechenden Baustein und im ersten Teil werden alle passenden Bedrohungen

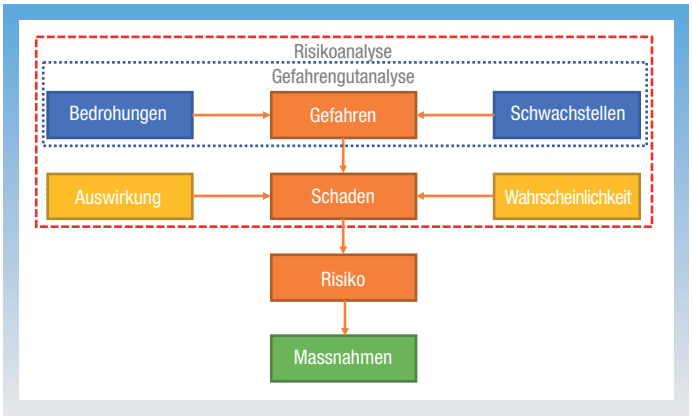

Bild 2: Bedrohungen identifizieren.

Auswirkung	Stufe	Beschreibung
Gering	0	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt weder den Zahlungsfluss, noch die rechtlichen oder vertraglichen Verpflichtungen oder das Ansehen der Organisation.
Mittel	1	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität verursacht zusätzliche Kosten und hat geringe oder mässige Auswirkung auf rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.
Hoch	2	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität hat beträchtliche und/oder unmittelbare Auswirkung auf den Zahlungsfluss, den Betrieb, rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.

Wahrschein-lichkeit	Stufe	Beschreibung
Gering	0	Bestehende Sicherheitsmassnahmen sind solide und lieferten bisher ein angemessenes Schutzniveau. Neue Vorfälle werden zukünftig nicht erwartet.
Mittel	1	Bestehende Sicherheitsmassnahmen sind moderat und lieferten meist ein angemessenes Schutzniveau. Neue Vorfälle sind zukünftig möglich, jedoch nicht sehr wahrscheinlich.
Hoch	2	Bestehende Schutzmassnahmen sind auf einem niedrigen Niveau oder unwirksam. Für zukünftige Vorfälle besteht eine hohe Eintrittswahrscheinlichkeit.

Bild 3: Dreistufiges Risiko-Analysen-Modell.

aufgelistet. So kann der eigene Aufwand massiv reduziert werden.

Hinweis: das BSI überarbeitet gerade die Grundschutzkataloge. Neu spricht das BSI vom Grundschutzkompendium, zu finden unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html. Im aktuellen Stand wurden erst die elementaren Gefährdungen übernommen. Die nächste Erweiterung ist auf 2019 geplant.

Nun gilt es das Risiko zu bewerten, in unserem abgekürzten Verfahren, wie wahrscheinlich eine Bedrohung wirklich eintritt. Dazu hat sich etabliert, die Eintrittswahrscheinlichkeit und die Auswirkungen einzeln zu bestimmen. Je nach Literatur und Quelle werden dazu drei, vier, fünf oder gar mehr Stufen verwendet. Wie viele Sie selber verwenden, spielt keine Rolle. Sie müssen aber genau definieren, was die Stufen für Sie bedeuten. Die Norm fordert ja, dass vergleichbare Resultate bei regelmässigen Risiko-Analysen entstehen. Eine Möglichkeit ist das folgende dreistufige Modell (Bild 3).

In einem nächsten Schritt werden die Werte in einen Zusammenhang gebracht. Ob die Werte nun addiert oder multipliziert werden, ist wieder Definitionssache. Die Norm schreibt dazu nichts vor.

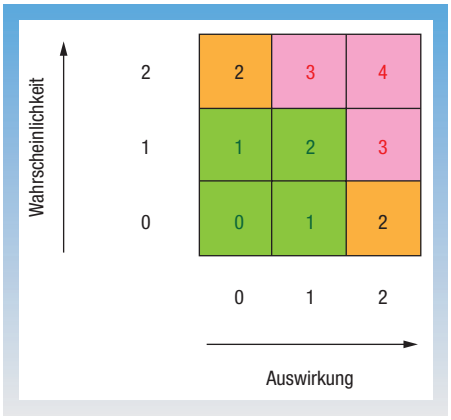

Bild 4: Ergebnis.

In meinem Beispiel addiere ich die beiden Werte. Es entstehen als Ergebnis Werte von 0 bis 4. Nun gilt es Kriterien zur Behandlung dieser Risiken zu bestimmen. Für mein Beispiel ist dies (Bild 4):

- Die Werte 0, 1 und 2 sind akzeptable Risiken Grün), während die Werte 3 und 4 inakzeptable Risiken sind (Rot). Inakzeptable Risiken müssen behandelt werden.
- Sollte jedoch die Auswirkung oder die Wahrscheinlichkeit «Hoch», Wert 2, sein, entscheidet die Geschäftsleitung, ob das Risiko behandelt werden muss oder nicht (Orange).

Schritte zur Reduktion des Risikos

Jedem identifizierten Risiko muss zwingend ein Risiko-Eigentümer zugewiesen werden. Dies kann die gleiche Person/Rolle sein, wie der dazugehörige Wert, muss es aber nicht. Die definierte Person/Rolle muss nun das Risiko bearbeiten oder bewusst akzeptieren. Je nach Ergebnis gilt es die Massnahmen zur Behandlung der Risiken zu priorisieren.

Hinweis: Immer wieder gibt die Risiko-Bewertung Stoff für Diskussionen. In meinen Bewertungen gehe ich immer vom Netto-Risiko aus, das heisst mit bereits getroffenen Massnahmen. Jedes Unternehmen hat bereits Schritte zur Reduktion des Risikos getroffen, zum Beispiel eine Firewall zum Schutz vor Hackern. Es macht für mich wenig Sinn, das Risiko anzuschauen, wie wenn keine Firewall da ist (Brutto-Risiko). Jedoch bietet eine Firewall keinen 100-prozentigem Schutz, es besteht immer ein Restrisiko. Dieses muss sauber erfasst und bewertet werden.

ISO 27001 verlangt, dass der Risiko-Prozess als dokumentierte Information vorliegt. Ich habe gute Erfahrungen gemacht, wenn die erkannten Risiken in einem Ticketing-Tool geführt werden. So sind diese immer sichtbar und jeder Behandlungsschritt kann nachvoll-

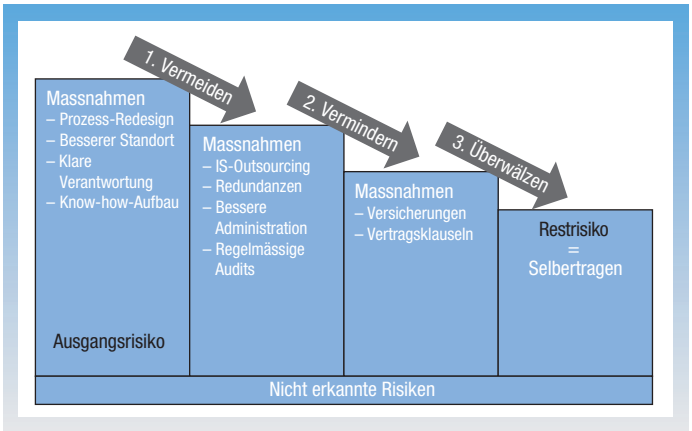

Bild 5: Mögliche Optionen bestimmen.

ziehbar dokumentiert werden. Zudem können auf eine einfache Art und Weise Reminder zur Neubewertung hinterlegt werden.

Im Kapitel 6.1.3 wird dann die Behandlung der Risiken verlangt. In einem ersten Schritt sind die möglichen Optionen zu bestimmen (6.1.3.a). Klassisch sind dies (Bild 5): Risiken können vermieden, vermindert, überwälzt oder akzeptiert werden.

Nun werden alle Massnahmen zur Bewältigung des Risikos ergriffen (6.1.3.b). Hier können wiederum die Grundschutzkataloge eine wertvolle Quelle sein, über 1600 Massnahmen in den sechs Kategorien Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge sind darin enthalten. Da findet sich sicherlich eine passende Massnahme. Ich empfehle wiederum über die Bausteine zu gehen. Dort wird kurz erklärt, was dies für ein Baustein ist, welche Gefährdungen existieren und welche Massnahmen ergriffen werden können. Das dritte Punkt (6.1.3.c) gibt an Zertifizierungsaudits immer wieder Anlass zu Diskussionen. Jede akkreditierte Zertifizierungsstelle sieht dies etwas anderes.

Die Anmerkung 1 verlangt, dass der Anhang, das heisst die 114 Controls angeschaut werden, damit keine Massnahme vergessen wird. Meine Interpretation dieses Punktes ist, dass das Risiko angeschaut und jede Massnahme aus dem Anhang aufgelistet wird, welche das Risiko reduziert oder gar eliminiert. Einige Auditoren, die ich kennengelernt habe, legen dies umgekehrt aus. Aus jedem Control können Risiken entstehen, wenn das Control nicht oder nur teilweise umgesetzt wird. Daher wird jedem Control mindestens ein Risiko zugewiesen. Für mich führen beide Wege zum erwünschten Ziel.

Abweichungen feststellen und entsprechend reagieren

Eine grosse Herausforderung ist die Anforderung aus 6.1.3.d. Hier wird eine Erklärung zur Anwendbarkeit (Statement of applicability, SOA) verlangt. In dieser müssen alle 114 Controls der Norm adressiert werden. Und zwar muss angegeben werden, warum eine Massnahme angewendet beziehungsweise warum eine Massnahme nicht angewendet wurde.

Die nächste Anforderung (6.1.3.e) verlangt einen Plan zur Informationssicherheitsrisikobehandlung. Die erkannten Risiken müssen darin behandelt werden. Sinnvollerweise wird angegeben, was durch wen bis wann umgesetzt wird. Ich empfehle auch anzugeben, wie das Risiko sich verändert, wenn die Massnahme komplett, teilweise oder nicht umgesetzt wird. Der letzte Punkt in diesem Kapitel (6.1.3.f) verlangt von allen Risikoeigentümern eine Genehmigung des aus vorherigem Punkt erstellten Plans. Es genügt also nicht mehr, pauschal durch die Geschäftsleitung das Risiko und den Risikoplan zu akzeptieren, sondern alle involvierten Personen müssen ihre Zusage dazu geben.

Das zweite Kapitel (6.2) verlangt von einem Unternehmen Informationssicherheitsziele zu definieren und diese regelmässig zu aktualisieren, falls erforderlich. Dabei gilt es zuerst abzuklären, was das Unternehmen im Bereich der Informationssicherheit erreichen will. Wichtig ist dabei auch zu definieren, wie diese gemessen werden. Nur was ich messen kann, kann ich auch bewerten und allfällige Abweichungen feststellen und entsprechend reagieren. Mögliche Ziele sind:

- Die klassischen CIA-Anforderungen (Vertraulichkeit, Integrität, Verfügbarkeit)
- Vollständiges Asset-Management inklusive Verantwortlichkeiten
- Schutz durch angepasste Technik, Informationen, Arbeitsprozesse und Wissen
- Schutz der Mitarbeitenden
- Klare Zuordnung und Umsetzung von Verantwortlichkeiten und Kompetenzen
- Aktuelle Dokumentationen
- Aktuelle Risiko-Beurteilung
- Regelmässige Audits durch interne und externe Stellen
- Reduktion von Incidents, zum Beispiel ausgelöst durch Benutzer (Stichwort Awareness)
- Reduktion von Schäden durch potenzielle Vorfälle
- Regelmässige Geschäftsleitungsreports
- Einhaltung von vertraglichen und gesetzlichen Anforderungen
- Angepasste physische Sicherheit
- Erhöhung des Images im Markt

Die Norm verlangt anschliessend einen Plan, wie diese Ziele erreicht werden können, was dazu notwendig ist, wer verantwortlich ist, wann es abgeschlossen ist und wie die Ergebnisse bewertet werden. Mit einer umfassenden Risiko-Analyse ist ein wichtiger, wenn ich der wichtigste Anforderungspunkt der ISO-Norm erfüllt. Alle weiteren Massnahmen uns Schritte basieren auf dieser Bewertung.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

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