Risiko-Management mit ISO 27005

Im jährlich durchgeführten Allianz Risk Barometer gab es in diesem Jahr eine Verschiebung. Neu sind Cyber-Risiken auf dem ersten Platz gelandet. Die Bedrohung durch Ransomware-Angriffe, Datenschutzverletzungen oder IT-Ausfälle beunruhigt die Unternehmen sogar noch mehr als Geschäfts- und Lieferkettenunterbrechungen, Naturkatastrophen oder die Covid-19-Pandemie, die alle Unternehmen beschäftigt hat. Um diesen Risiken begegnen zu können, ist das Management dieser unumgänglich. ISO 27005 ist hier ein gutes Werkzeug, das schrittweise durch den Prozess führt.

Ein risikobasierter Ansatz, um die vielen aktuellen Themen zu behandeln, ist für jedes Unternehmen essenziell. Die Zeit reicht schlicht nicht mehr aus, alle Themen bis ins Detail zu behandeln. Es muss klar sein, wo der Schuh am meisten drückt und dort angesetzt werden. So verlangt nicht nur die ISO 27001 dieses Vorgehen sehr ausführlich, zeigt aber gleichzeitig keine Möglichkeit, wie die Risiko-Bewertung durchzuführen ist. Die ISO 27005 beschreibt einen möglichen Ansatz, wie Risiken im Bereich der Informationssicherheit behandelt werden können. Die Norm ist aktuell nur in Englisch verfügbar und wurde bereits im Juli 2018 veröffentlicht, also auch schon über vier Jahre alt. Im Moment findet eine Überarbeitung statt. Mit einer Neuveröffentlichung ist jedoch nicht mehr in diesem Jahr zu rechnen.

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

In Kapitel 6 wird der Informationssicherheitsrisikoprozess vorgestellt. Er orientiert sich an ISO 31000 (Risk Management – Guidelines), siehe dazu Bild 1. In der Norm wird folgender Ablauf im Detail beschrieben:

- die Auswahl der Kriterien für die Risiko-Bewertung (7.2.2), die Risiko-Auswirkungen (7.2.3) und die Risiko-Akzeptanz (7.2.4);
- die Definition des Umfangs und der Grenzen des Informationssicherheits-Risiko-Managements (7.3 und A.2);
- die Risiko-Identifikation (8.2: Werte, Bedrohungen (Beispiele in Anhang B), vorhandene Kontrollen, Schwachstellen (Beispiele in Anhang D), Konsequenzen);
- die Risiko-Analyse (8.3);
- die Risiko-Bewertung (8.4);
- die Risiko-Behandlung (9.1), die Umsetzung von Risiko-Minderungsplänen (9.2 und Anhang F), die Akzeptanz (9.3 und 10), die Vermeidung (9.4) sowie die Abwälzung von Risiken (9.5, die Norm spricht dabei von Sharing);
- die Kommunikation der Risiken (11);
- die Überwachung, Überprüfung und Verbesserung des Risiko-Managements (12);
- die Ermittlung von Vermögenswerten (Anhang B.1.3) und die Bewertung von Vermögenswerten (Anhang B.2.3);
- Risiko-Einschätzung (Beispiele in Anhang E.2.1).

Wie ersichtlich ist, werden im ersten Schritt die Kriterien definiert. Welche Einstufung wird verwendet? Wird dabei eine 3x3, 4x4, 5x5 oder eine noch grössere verwendet? Wer regelmässig meine Artikel liest, weiss, dass ich kein Fan von 3x3 bin, da hier schlicht nicht genügend unterschieden werden kann und erfahrungsgemäss die meisten Risiken in der Mitte liegen. Dies spricht auch gegen die anderen Matrizen mit einer ungeraden Zahl. Je grösser, umso weniger ist das Problem der Mitte aber vorhanden. Ich bin ein Fan der 4x4-Matrix, denn hier gibt es keine Mitte, aber genügend Unterscheidungsmöglichkeiten.

Nach der Erfassung der Risiken muss sich das Unternehmen entscheiden, in welches Feld diese gehören.

Die beiden erwähnten Achsen sind die Eintritts-Wahrscheinlichkeit und die Auswirkung. Bei einem 4x4-Modell könnten diese beispielsweise so aussehen (Bild 2).

Damit eine Unterscheidung erfolgen kann, gilt es die Begriffe beziehungsweise die Kriterien zu definieren. Dies kann verschiedene Themengebiete umfassen, es gilt jeweils der höchste Wert.

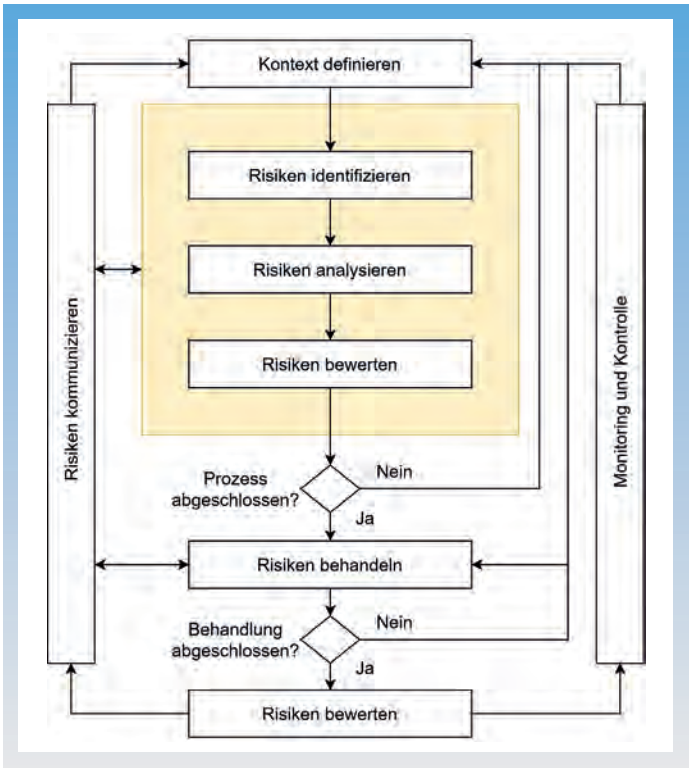

Bild 1: Risiko-Prozess, eigene Darstellung basierend auf ISO 27005:2018.

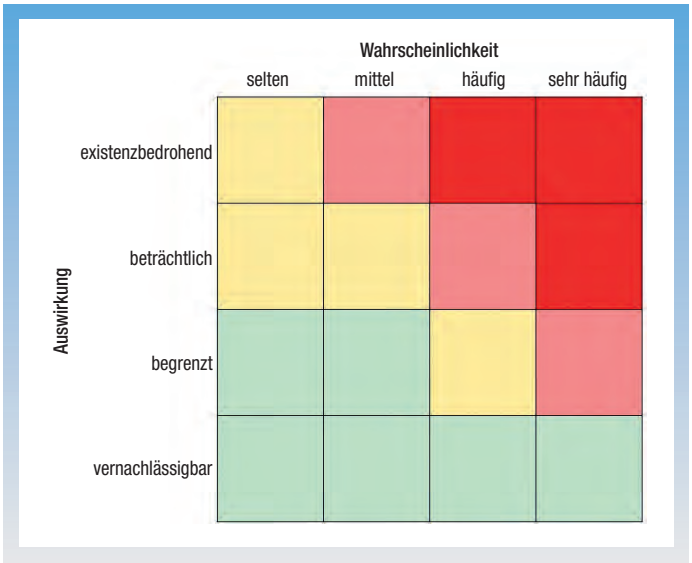

Bild 2: 4x4-Modell.

Auswirkung	Beschreibung
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden. – Der finanzielle Schaden ist irrelevant (CHF 0 bis 5000) – Der Imageverlust ist gering (gelegentliche Beschwerden) – Preisgabe wenig sensibler Daten – Geringe interne Unkosten, ausserhalb nicht bemerkbar
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar. – Der finanzielle Schaden ist tragbar (CHF 5001 bis 50'000) – Der Imageverlust ist bemerkbar (gelegentliche Kritik in den Medien) – Kurzzeitige negative Auswirkungen sind möglich – Keine Datenschutzverletzung – Kosten spürbar, von aussen sichtbar
beträchtlich	Die Schadensauswirkungen können beträchtlich sein. – Finanzieller Schaden ist spürbar (CHF 50'001 bis 100'000) – Der Imageverlust ist gross (schwere Kritik in den Medien) – Ernsthafte negative Auswirkungen möglich – mögliche Datenschutzverletzung – Erhebliche Kosten sind zur Behebung notwendig
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen. – Der finanzielle Schaden bedroht die Existenz (> CHF 100'001+) – Es ist mit bleibendem Schaden zu rechnen – Verlust von Leben/Schwere Rufschädigung – mögliche Datenschutzverletzung – Erhebliche Störung des Betriebs, es besteht Gefahr für das Nicht-Überleben des Unternehmens

Und für die Eintritts-Wahrscheinlichkeit:

Wahrscheinlichkeit	Beschreibung
selten	Ereignis tritt weniger als alle fünf Jahre einmal ein.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Wird nun ein Risiko erfasst und bewertet, landet es in einem der 16 Felder. Die Farben geben an, wie das Risiko eingestuft wird. Die Farben bedeuten:

Kategorie	Beschreibung
gering (Grün)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten einen ausreichenden Schutz. Das Risiko wird akzeptiert, jedoch beobachtet.
mittel (Orange)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen reichen möglicherweise nicht aus. Es können weitere Massnahmen definiert werden.
hoch (Hell-Rot)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten keinen ausreichenden Schutz vor der jeweiligen hohen Gefährdung. Es sind zwingend weitere Massnahmen zu definieren. Ist dies nicht möglich, müssen genügend Kontrollen definiert werden, um bei einem Eintreten schnell reagieren zu können.
sehr hoch (Rot)	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten keinen ausreichenden Schutz vor der jeweiligen sehr hohen Gefährdung. Es sind zwingend Massnahmen zu definieren und umzusetzen.

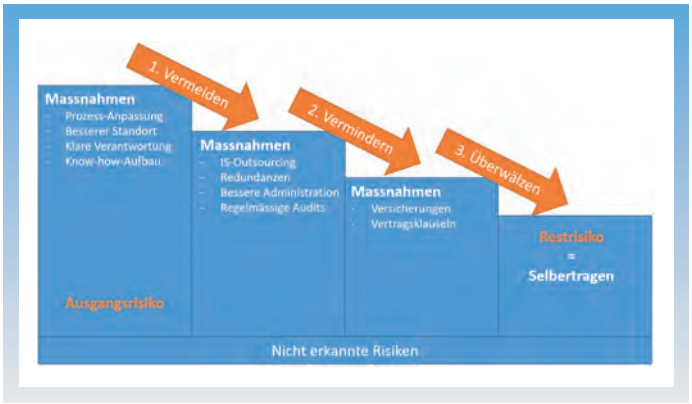

Bild 3: Risiko-Behandlung.

Die anschliessende Risiko-Behandlung kennt klassischerweise folgende Möglichkeiten zur Bewältigung (Bild 3).

- Risikovermeidung durch Prozess-Anpassungen, anderer Standort, klare Verantwortlichkeiten, Aufbau von eigenem Know-how oder der Beendigung einer Geschäftsaktivität, welche dieses Risiko verursacht
- Auswahl von Sicherheitsmassnahmen und -kontrollen (beispielsweise Controls aus Anhang A der ISO/IEC 27001 oder dem umfassenden Grundschutz-Kompendium)
- Risikoübertragung an Dritte, zum Beispiel durch den Abschluss einer Versicherung oder die Unterzeichnung eines Vertrages mit Lieferanten oder Partnern
- Risikoakzeptanz – das (Rest-) Risiko wird bewusst durch die Geschäftsleitung und den Risiko-Eigentümer getragen

Idealerweise wird die Bewertung nicht allein im stillen Kämmerchen gemacht, sondern in einem Workshop mit verschiedenen involvierten Personen. Oft werden die Risiken nicht von allen identisch eingestuft. In der notwendigen Diskussion können alle ihre Meinung mitteilen und es kann ein Konsens gefunden werden. Dabei spielt es keine Rolle, ob das Risiko nun ein Feld mehr links/rechts oder oben/unten ist, sondern dass alle damit einverstanden sind.

Fazit

Das Modell der ISO 27005 ermöglicht es, Risiken umfassend zu erfassen (die Anhänge helfen bei der Auswahl, aber auch das deutsche Bundesamt für Sicherheit in der Informationstechnik hat 47 elementare Gefährdungen definiert) und anschliessend zu bewerten. Je nach Einstufung können (oder müssen) Massnahmen zur Bewältigung oder Kontrolle der Risiken getroffen und umgesetzt werden. Mit diesem Vorgehen kann ein Unternehmen seine Risiken nachhaltig bearbeiten und auf ein erträgliches Mass reduzieren.