Informationssicherheits-Managementsysteme wirksam und effizient gestalten

Ausgangssituation

Neben physischen Sachwerten stellen Informationen heutzutage häufig die wahren Werte eines Unternehmens dar. Eine störungsfreie Bereitstellung und Verarbeitung von Informationen dient der Unterstützung der Geschäftsprozesse und sichert dadurch die Erreichung der Unternehmensziele und den Unternehmenserfolg. Die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen muss sichergestellt und angemessen gegen Bedrohungen geschützt werden. Der bewährte Rahmen für ein strukturiertes Management von Informationssicherheitsrisiken ist ein Informationssicherheits-Managementsystem (ISMS). Neben der intrinsischen Motivation zum Informationsschutz gibt es teils branchenspezifische Vorgaben an das Informationssicherheits-Management sowohl von Gesetzgeber und Aufsichtsbehörden (z. B. Bundesanstalt für Finanzdienstleistungsaufsicht) sowie von Kunden- und Marktseite (z. B. über Verträge). Gesetzgeber und Aufsichtsbehörden begegnen der steigenden Bedrohungslage durch Cyberkriminalität vermehrt mit stärkerer Regulierung und härteren Strafen bei Versäumnissen.

Ziele und Handlungsbedarf

Ein ISMS beinhaltet das Aufstellen von Verfahren und Regeln sowie das Etablieren von Maßnahmen und Steuerungsinstrumenten, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern und fortlaufend zu verbessern. Ziel ist es, dass Organisationen in der Lage sind, ihre Informationen vor dem Ausnutzen von (möglichen) Schwachstellen so zu schützen, dass die Schutzziele der Informationssicherheit gewahrt bleiben. Ein ISMS muss in die Managementstrukturen einer Organisation eingebettet werden. Ein hoher Integrationsgrad verschiedener Managementsysteme untereinander und Transparenz über Verantwortlichkeiten, Regelungen und Maßnahmen ermöglichen, dass gleichartige Anforderungen unterschiedlicher Herkunft gebündelt behandelt und Berichtswege verschlankt werden. Dies spart Ressourcen und erhöht die Wirksamkeit der etablierten Regelungen und Maßnahmen.

Wesentliche Handlungsbedarfe zur Etablierung und Fortschreibung eines ISMS sind:

- **Konzeption und Etablierung des ISMS**

  Die Vorgaben und Ziele für die Informationssicherheit sind zu erfassen und das ISMS ist darauf auszurichten. Da es um den Schutz von Informationswerten geht, wird als Basis und Bezugsquelle eine Erfassung dieser Werte (Assets) und ihrer jeweiligen Schutzbedarfe vorgenommen. Anschließend werden zielgerichtet und vorgabenkonform Regelungen und Maßnahmen zur Informationssicherheitsrisiko-Behandlung geplant. Dabei ist ein risikoorientierter Ansatz zu wählen. Das ISMS wird *top-down* in die Organisation eingeführt mit der Informationssicherheits-Politik (IS-Politik) als Leitlinie der obersten Leitung.

Konkrete Aktivitäten hierbei sind (Beispiele):

- Bestimmen des angestrebten Sicherheitsniveaus, Planen und Ausrichten des ISMS
- Erstellen eines Informationsbestände-Registers und Durchführen einer Schutzbedarfsanalyse
- Erstellen von Verfahren und Regelungsdokumenten, z. B. Richtlinien
- Aufbauen und Etablieren der ISMS-Strukturen, Verantwortlichkeiten und Prozesse
- Planen von risikobehandelnden Maßnahmen

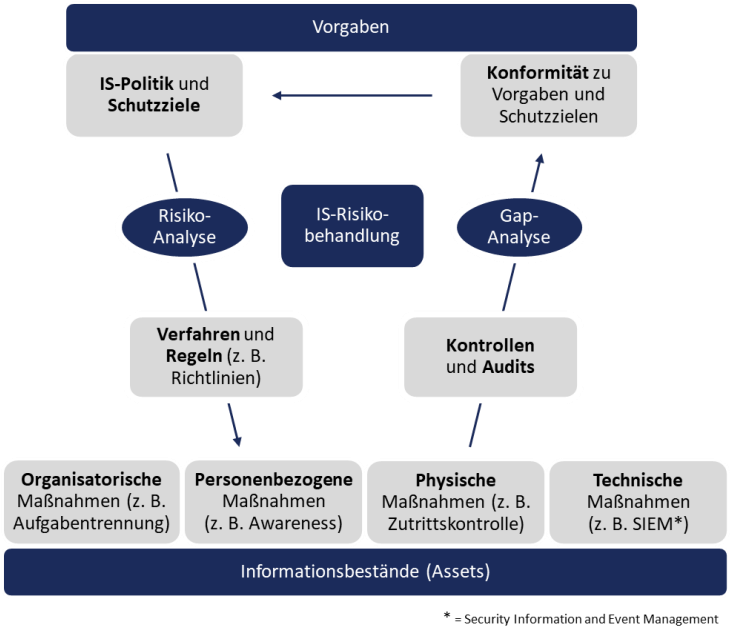

Abb. 1 – Big Picture: Wesentliche Bestandteile eines Informationssicherheits-Managementsystems (ISMS)

- **Umsetzung von risikobehandelnden Maßnahmen**

  Um Informationen zu schützen und verfügbar zu halten, werden organisatorische, personenbezogene, physische und technische Maßnahmen umgesetzt. Viele einzelne Maßnahmen verleihen einer Organisation eine hohe Resilienz, wenn sie aufeinander abgestimmt und gut miteinander verzahnt sind. Die Umsetzung von unterschiedlichen Einzelmaßnahmen ist notwendig, da die Bedrohungssituationen komplex sind. Es muss zahlreichen Szenarien zur Kompromittierung von Informationen entgegengewirkt werden. Pläne zur Behandlung von Sicherheitsvorfällen und Schadensereignissen und die notwendigen Meldewege sind zu erstellen und zu verproben sowie entsprechende Dokumentation vorzuhalten.

  Konkrete Aktivitäten hierbei sind (Beispiele):

  - Konkretisieren von Maßnahmen und deren Umsetzung initiieren (z. B. Umsetzungsplanung erstellen)
  - Entscheiden über die Umsetzung sowie die notwendigen Ressourcen zu geplanten Änderungen im Unternehmen
  - Etablieren bzw. Anpassen von Prozessen und organisatorischen Strukturen sowie Berichtswegen
  - Bei Bedarf Werkzeugauswahl und Planung des Werkzeugeinsatzes sowie Beschaffung inklusive Dienstleisterprüfung

- **Überprüfung und Steuerung der Wirksamkeit**

  Zur kontinuierlichen Fortschreibung eines ISMS bedarf es der Überprüfung und Steuerung der Wirksamkeit gültiger Regelungen und etablierter Maßnahmen. Es werden hierzu Kontrollen und Kennzahlen in den Prozessen der Organisation etabliert und zur Steuerung herangezogen. Im Rahmen von Audits wird der Umsetzungsgrad der Verfahren und Regeln sowie die Prozesstreue über Interviews und Nachweis-Prüfungen festgestellt. Etwaige Gaps zu den Vorgaben werden einer Risikobewertung unterzogen und Maßnahmen aufgesetzt bzw. Anpassungen am ISMS selbst vorgenommen, um die Sicherheitsziele zu erreichen.

  Konkrete Aktivitäten hierbei sind (Beispiele):
  - Planen und Etablieren wirksamer Kontrollen, die die Zielerreichung des ISMS unterstützen
  - Umsetzen eines übergreifenden Kontrollen- und Kennzahlen-basierten Steuerungssystems
  - Durchführen von internen Audits und Begleiten externer Prüfungen
  - Durchführen von Gap-Analysen und Risikobewertungen
  - Optimieren des Berichtswesens und Durchführen von Managementbewertungen

Unsere Leistungen

Wir beraten Sie bei der effektiven und effizienten Umsetzung der auf Ihr Unternehmen wirkenden Vorgaben. Wir unterstützen Sie bei der Planung, Etablierung und Fortschreibung Ihres ISMS unabhängig davon, ob Sie es neu einführen oder ein bestehendes verändern. Unter Verwendung gängiger Standards und mit unserer Praxiserfahrung erarbeiten wir gemeinsam mit Ihnen ein Zielbild zu Ihren individuellen Handlungsfeldern, entwerfen konkrete Handlungsempfehlungen, erstellen Verfahren und Dokumente sowie Risikobewertungen und Pläne zur Umsetzung von wirksamen Maßnahmen.

Unsere Consultants wirken aktiv mit Ihrem Management und den für das ISMS verantwortlichen Personen von der Lösungsfindung über Anpassungen von Ablauf- und Aufbauorganisation und dem Einsatz von Werkzeuglösungen bis zur Steuerung der eingesetzten Dienstleister. Im Rahmen einer Werkzeugauswahl erarbeiten wir Anforderungskataloge und führen Marktanalysen durch. Wir unterstützen Sie beim Aufbau und bei der Anpassung von Mess- und Steuermechanismen und dem Erstellen von Berichten, erarbeiten Auditpläne und optimieren Ihr Melde- und Berichtswesen intern und zu relevanten Stellen, wie Behörden oder Aufsicht.

Ihr Ansprechpartner:
Markus Heinemann berät seit über 20 Jahren zu Strategien, Prozess- und Organisationsstrukturen für das Management der IT. Seine Erfahrungsschwerpunkte liegen insbesondere in den Branchen Informationstechnologie, Finanzdienstleistung und Automotive.

Telefon: +49 (89) 6137 283 – 12
E-Mail: markus.heinemann@mh-macon.de