



10 Schritte zum Betrieb eines eigenen ISMS

Die Informationssicherheit hat unter anderem das Ziel, Vermögenswerte in Form von Informationen zu schützen. Da nicht alle Informationen denselben Schutzbedarf aufweisen, werden mittels systematischer Vorgehensweise die zu schützenden Vermögenswerte identifiziert und qualifiziert. Dieses Vorgehen mündet in ein ISO-basiertes ISMS.

Es gibt kein «One-size-fits-it-all» Informations-Sicherheits-Management-System (ISMS). Die Ausprägung eines ISMS hängt von verschiedenen Faktoren ab. Daher sollte geklärt werden, welche Standards und Regularien für das eigene Unternehmen von Bedeutung sind. Je mehr Standorte und internationale Anforderungen berücksichtigt werden müssen, umso höher ist die Komplexität eines ISMS. Die folgenden zehn Schritte führen zum Betrieb eines eigenen ISMS.

1. Unterstützung durch das Management

Die wichtigste Voraussetzung für ein ISMS ist die volle Unterstützung durch die Geschäftsleitung. Um diese zu erhalten, müssen dem Management die zu erwartenden Resultate sowie die Vorteile eines solchen Systems verständlich dargelegt werden.

2. Team

Damit die Planung und Umsetzung eines ISMS gelingt, braucht es ein kompetentes Team. Eine wichtige Schlüsselrolle fällt dabei dem Chief Information Security Officer (CISO) zu, welcher als Vermittler zum Management auftritt. Er ist für die erforderlichen Genehmigungen zuständig und muss mit den nötigen Kompetenzen ausgestattet sein. Die weiteren Mitglieder setzen sich aus Vertretern aller Abteilungen zusammen, welche vom ISMS-Prozess betroffen sind.

3. Geltungsbereich festlegen

Das Management muss den Geltungsbereich des ISMS definieren. Dieser kann eine Abteilung, eine Niederlassung oder das ganze Unternehmen umfassen. Der Geltungsbereich sollte in der Security Policy dokumentiert sein. Danach werden die zu schützenden Un-

ternehmensprozesse erfasst. Dies ist eine gute Grundlage, um später die Vermögenswerte zu identifizieren und zu bewerten und hilft auch bei der Durchführung einer Business Impact Analyse (BIA).

4. Risiko-Analyse

4.1 Inventar der Vermögenswerte (Assets)

Informationen liegen in unterschiedlicher Form vor. Da es unmöglich ist, Informationen in einem Inventar zu erfassen, müssen die Informationsträger erfasst werden. Die ermittelten und inventarisierten Vermögenswerte (Assets) sollen nach einem passenden System gekennzeichnet werden. Für jedes Asset wird ein Asset Owner (Besitzer) und ein Asset Custodian (Betreuer) definiert.

4.2 Bewertung von Assets (CIA-Methode)

Ein Asset wird nach den Kriterien Confidentiality (Vertraulichkeit), Integrity (Unverfälschtheit) und Availability (Verfügbarkeit) bewertet, der sog. CIA-Methode. Für die Bewertung eines Assets verwenden wir für die C-, I- und A-Werte eine Skala von z. B. 1 (kleine Auswirkung/unwichtig) bis 5 (grosse Auswirkung/sehr wichtig). Das ISMS-Team hat jetzt die Aufgabe, zusammen mit den Asset Ownern festzulegen, welche Werte für C, für I und für A eingesetzt werden sollen. Um den Wert des Assets X festzulegen, bedient man sich folgender Formel:

Asset-Wert = Confidentiality + Integrity + Availability

Wert «Asset X» = 4 + 4 + 4 = **12**
(kritisch/besonders schützenswert)
oder Wert «Asset X» = 2 + 2 + 2 = **8**
(nicht kritisch)

info zum Autor



PINO CUCCARO
Der Autor ist Senior Security Consultant, CISSP

4.3 Risiko - Wert von Assets

Nun muss bestimmt werden, wie hoch das Risiko ist, dass ein Vermögenswert Schaden erleidet. Dazu ist für jeden Vermögenswert zu überlegen, welches die möglichen Bedrohungen sind und wie hoch die Wahrscheinlichkeit ist, dass es tatsächlich zu einem Schaden kommt. Hier kann man entweder quantitative Aussagen treffen und sich z. B. auf statistische Werte und Zahlen von Versicherungen beziehen oder auch qualitative Aussagen tätigen.

5. Business Impact Analyse (BIA)

Zu einer ganzheitlichen Risikobewertung gehört auch die Überprüfung der Schadensauswirkung auf die Businessprozesse. Dies kann anhand einer Business Impact Analyse (BIA) ermittelt werden. Diese berücksichtigt zusätzlich die Zeitkomponente. Je kürzer die tolerierbare Ausfallzeit eines Assets, umso höher sollte deren Priorität gewählt werden. Wenn wir davon ausgehen, dass ein E-Mail-Server maximal einen halben Tag ausfallen darf, geben wir diesem Asset eine BIA-Priorität von 4 (mittlere Priorität). Dies ergibt folgende Berechnung:

Risiko-Wert = Asset-Wert x Eintretenswahrscheinlichkeit eines bestimmten Schadens x BIA-Priorität

Beispiel E-Mail Server:

Risiko-Wert = 12 x 0,4 x 4 = 19,2

6. Risiko-Management

Aus den ermittelten Risiko-Werten kann das ISMS-Team Entscheidungsgrundlagen für das Management erarbeiten. Es geht darum, wie die ermittelten Assets gegen die möglichen Risiken abzusichern sind. Bei Assets, bei denen die Schutzkosten deren Wert übersteigen können, sollte das Risiko bewusst akzeptiert werden. Für die restlichen muss für jedes Risiko-Szenario pro Asset entschieden werden, ob ein Risiko limitiert, nicht eingegangen oder übertragen werden soll.

7. Statement of Applicability (SOA)

Ein SOA ist ein Dokument, welches all die «Controls» (Prüfpunkte) aus ISO 27001 auflistet und für jeden einzelnen definiert, ob und weshalb ein Control in der eigenen Unternehmung Anwendung findet. Diese Aufstellung gibt (externen) Auditoren und Dritten auf Verlangen über den Level der Sicherheitspraxis in der betrachteten Unternehmung Auskunft. Die Implementierung einiger dieser Controls müssen durch entsprechende Policies unterstützt werden.

8. Business Continuity Plan (BCP) & Disaster Recovery (DR)

Der Business Continuity Plan (BCP) definiert die Schutzmassnahmen für die kritischen Geschäftsprozesse, die für den Fortbestand einer Organisation notwendig sind, wenn ein geschäftsbedrohliches Scha-

densereignis eingetroffen ist. Dazu gehört die Berücksichtigung aller damit verbundenen Ressourcen wie Personal, Anwendungen, Daten usw. Da Schäden durch höhere Gewalt, menschliches Fehlverhalten und technisches Versagen alle Unternehmensbereiche kritisch beeinträchtigen können, müssen solche Projekte bereichsübergreifend angesetzt werden. Als Grundlage dient die Business Impact Analyse (BIA). Daraus wird die Ausgestaltung der Notfallstrategie abgeleitet. Um sicherzustellen, dass sich während Notfällen alle Beteiligten wunschgemäß verhalten, ist die Erstellung eines Notfallhandbuchs nützlich. Zu guter Letzt sollte in einem Disaster Recovery Plan (DR) geregelt werden, wie der Übergang vom Notfallbetrieb zum Normalbetrieb ablaufen soll.

9. Auditing

Möchte man ISO 27001-Konformität eines Unternehmens zertifizieren lassen, wird dies durch externe Auditoren durchgeführt. Der erste Schritt des Audits besteht in einem Review der vorhandenen Dokumente. Weitere Bereiche des Audits, die hier nicht näher beschrieben werden sollen, sind: Physical Security, Desktop Security, Vulnerability Assessment und Penetration Testing, Social Engineering und User Awareness.

10. User Awareness

Ein Audit bestätigt einer Unternehmung, ein dokumentiertes Prozess- und Regelwerk für den Umgang mit Informationssicherheit zu besitzen. Es wird durch Dritte bestätigt, dass alle notwendigen Weisungen und Dokumente vorhanden sind. Doch sagt dies leider nichts über die gelebte Informationssicherheit aus. Da die Sicherheit einer Unternehmung vom Beitrag aller Mitarbeitenden abhängt, ist es wichtig, auch diese in den Sicherheitsprozess einzubeziehen. Dazu gehört die Schulung und Sensibilisierung der Mitarbeitenden im Bezug auf sicherheitsrelevante Fragestellungen. Um solche Schulungen stufengerecht und gezielt durchführen zu können, ist es empfehlenswert, wissenschaftlich validierte Fragebögen und Werkzeuge zu nutzen, um den Grad der Informationssicherheitskultur zu messen. Ein weiterer Vorteil solcher Messungen ist, dass das Ergebnis der durchgeführten Massnahmen periodisch überprüft werden kann. Das Ziel eines ISMS ist, dass die wichtigen Vermögenswerte eines Unternehmens sinnvoll geschützt sind und die erfolgten Massnahmen überprüft werden können. Mit der ganzheitlichen Betrachtungsweise von Organisation, Mensch und Technologie kann eine höchstmögliche Sicherheitsstufe erreicht werden. Diese Vorgehensweise unterstützt die Verantwortlichen für Sicherheitsfragen in einem systematischen Vorgehen. Und auch das Management erhält auf die Frage «Wie sicher sind wir?» eine fundierte und gut dokumentierte Antwort.