Was bringt ein ISMS?

Täglich ist von neuen IT-Schwachstellen zu lesen. Angriffe auf Firmen und Privatpersonen haben ein neues Hoch erreicht und die gesetzlichen und regulativen Anforderungen sind immer aufwändiger zu erfüllen. Der Aufbau und die Pflege eines Informations-Sicherheits-Management-Systems helfen, die zahlreichen Anforderungen und Wünsche zusammenzubringen und nachhaltig zu steuern.

Andreas Wisler

© depositphotos, Igor Vetushko

Mit einem ISMS existiert ein anerkannter Nachweis, dass im Unternehmen die Informationssicherheit behandelt und verbessert wird.

Informationssicherheit wird zu einem immer wichtigeren Thema für jedes Unternehmen. Während in den vergangenen Jahren das Thema Informationssicherheit eher stiefmütterlich behandelt wurde, ist selbst bei kleinsten Unternehmen die Erkenntnis angekommen, dass Massnahmen zum Schutz der Firmenwerte ein absolutes Muss sind. Jede Firma möchte die eigenen und von Dritten übergebenen Daten sicher aufbewahren und vor Manipulationen oder Zerstörung schützen. Um für Kundinnen und Kunden, Lieferanten und Partner auch einen Nachweis zu haben, sollte ein Informations-Sicherheits-Management-System (ISMS) aufgebaut werden. ISO 27001 definiert Anforderungen, mit welchem das ISMS aufgebaut, unterhalten und stetig weiterentwickelt werden kann. Hat das System einen guten Stand erreicht, kann es durch eine akkreditierte Stelle zertifiziert und ein entsprechender Nachweis ausgestellt werden.

Basis bilden die ISO 27001 und ISO 27002

Die ISO-27000er-Reihe besteht aus verschiedenen (Sub-)Standards. Laufend kommen weitere dazu, vor allem im Bereich der sektionsspezifischen Standards in bestimmten Bereichen wie Telekommunikation, Finanzen, Gesundheitswesen und Energieversorgung. Die Basis bilden aber immer die beiden Normen ISO 27001 und ISO 27002.

ISO 27001 beschreibt den Aufbau des Frameworks. Die Kapitel umfassen den Kontext der Organisation (Aufbau, Prozess, involvierte Stellen, Geltungsbereich und das Managementsystem), Anforderungen an die Führung (Verantwortung und Zuständigkeiten, Sicherheitsrichtlinie), der Planung (Risikoanalyse, Umsetzungspläne), die Unterstützung (Ressourcen, Kompetenzen, Schulungen, Kommunikation), den Einsatz (Planung, Durchführung und Behandlung von Risiken und Chancen), die Auswertung (Überwachung, Messung, Analyse und Auswertung der Ergebnisse) sowie den Umgang mit Abweichungen und der stetigen Verbesserung des ISMS.

Im Anhang werden konkrete Massnahmen gefordert. Total handelt es sich um 114 sogenannte Controls, aufgeteilt in 14 Kapitel. Dabei werden Themen wie die Organisation der Sicherheit, Mitarbeiterprozesse von der Einstellung bis zum Austritt inklusive Awareness, Management von Firmenwerten, Zugriffskontrolle, physische Sicherheit, Betriebssicherheit, Unterhalt und Wartung, Beziehungen mit Lieferanten, Management von Sicherheitsvorfällen sowie Business Continuity Management behandelt. Da jeweils nur ein bis zwei Sätze die Anforderungen beschreiben, hilft die 27002 weiter. Diese folgt der gleichen Struktur und beschreibt mit detaillierten Erklärungen, wie eine Massnahme umgesetzt werden kann (auch Anleitung zur Umsetzung genannt). Teilweise gehen die Erklärungen über mehrere A4-Seiten.

Welche Anforderungen?

Nur mit dem Auftrag, ein ISMS aufzubauen, ist es aber nicht getan. Mit der letzten Überarbeitung im Jahr 2013 kamen klare Anforderungen dazu, die die Leitung des Unternehmens in die Pflicht nimmt. Die Norm definiert die folgenden Anforderungen, die es zu erfüllen gibt:

- Übernahme der Gesamtverantwortung für die Informationssicherheit
- Informationssicherheit in alle Prozesse und Projekte integrieren
- Informationssicherheit steuern und aufrechterhalten
- erreichbare Ziele setzen
- Sicherheitskosten gegen Nutzen abwägen
- Vorbildfunktion

Oft stehen Managementsysteme in der Kritik, dass viel Papier erstellt werden muss, dies aber für das Unternehmen nur einen geringen Mehrwert bringt. Diese Vermutung ist teilweise richtig. Auch für ISO 27001 müssen einige (Pflicht-)Dokumente erstellt werden. Aus meiner Erfah-

rung bei verschiedenen Projekten sind dies aber Dokumente, die ein Unternehmen auch ohne Zertifizierung erstellen sollte. Gerade die Leitlinie zum Umgang mit der Informationssicherheit ist essenziell. Aber auch die Durchführung der Risikoanalyse ist wichtig und wird ebenfalls für das interne Kontrollsystem (IKS) nach OR 728a gefordert.

Erfolgreicher Abschluss

Wann kann der Projektstatus abgeschlossen werden? Nach der Norm gilt ein Informationssicherheitssystem dann als erfolgreich, wenn folgende Punkte erfüllt sind:

1. Es gibt eine definierte Leitlinie, welche sich an den Zielen und Massnahmen der Geschäftsziele orientiert und an das Vorgehen zum Management der Informationssicherheit der Unternehmenskultur angepasst ist,
2. ein Budget für Informationssicherheitsmanagement zugeteilt wurde und die Aktivitäten zur Informationssicherheit von der Geschäftsführung unterstützt werden,
3. in der Organisation das Verständnis für die Anforderungen an Informationssicherheit verbreitet ist, Risikoanalysen durchgeführt und Notfallvorsorge betrieben wird,
4. die Benutzer hinreichend für Informationssicherheit sensibilisiert und geschult sind und die geltenden Sicherheitsvorgaben und Regelungen bekannt sind sowie
5. ein Sicherheitsprozess mit einer regelmässig wiederholten Beurteilung und Verbesserung des ISMS existiert.

Zertifizierung in 13 Schritten

Wie kann ein Unternehmen nun den Weg in Richtung ISO 27001 einschlagen? Welche Dinge gilt es in welcher Reihenfolge umzusetzen? Nachfolgende Schritte zeigen einen pragmatischen Weg zu einer erfolgreichen Zertifizierung auf:

Erstens: Unterstützung der Geschäftsleitung einholen
Zweitens: Projektplan erstellen
Drittens: Anforderungen und Rahmenbedingungen ermitteln (Interessierte Parteien, vertragliche und rechtliche 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 mit welchem Schutzbedarf werden für diese Geschäftsprozesse verarbeitet?
- Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (z. B. 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?

Viertens: Anwendungsbereich (welcher Bereich soll zertifiziert werden?) und die Schnittstellen zu anderen Bereichen, Lieferanten und Kunden definieren
Fünftens: Informationssicherheitsrichtlinie erstellen
Sechstens: Prozess zur Risikoeinschätzung etablieren (Prozesse und Assets erfassen), Kritikalität definieren
Siebtens: Risiken erfassen, bewerten und Massnahmen definieren
Achtens: Umsetzung der daraus notwendigen Massnahmen
Neuntens: Durchführung von Trainings und Awareness-Schulungen
Zehntens: Internes Audit durchführen (Überprüfung des ISMS und der 114 Controls aus ISO 27002)
Elftens: Managementbewertung durchführen (d. h. Präsentation des aktuellen Standes, Ergebnisse aus Audits und Messungen, Übernahme der Risiken, stetige Verbesserung des ISMS)
Zwölftens: Anmeldung zur Zertifizierung bei einer akkreditierten Stelle
Dreizehntens: Durchführen des ISO-27001-Audits durch Zertifizierer in zwei Stufen

Es lohnt sich dabei, als Unterstützung oder Begleitung auf einen erfahrenen Spezialisten zu setzen. Dieser kennt die notwendigen Schritte, kann an den richtigen Stellen nachfragen und setzt auch etwas Druck auf, damit das Projekt in der Hektik des Tagesgeschäftes nicht untergeht. Doch nicht alle Schritte können durch eine externe Stelle schnell umgesetzt werden. Gerade die Beschreibung von Prozessen und das Erfassen von Assets (Firmenwerten) kann das Unternehmen oft besser und schneller durchführen – sind diese doch schon bekannt. Bei der nachfolgenden Risikoanalyse kann der externe Profi neue Blickrichtungen erwähnen und hinterfragt Dinge, die vielleicht schon immer so gemacht wurden. Die erforderlichen Dokumente, der Aufbau des ISMS, eine allenfalls notwendige Anpassung von Prozessen, die Schulung von Mitarbeitenden (Stichwort Sensibilisierung) und die Begleitung durch die notwendigen Kontrollen (Internal Audit, Managementbewertung) können ebenfalls abgegeben werden.

Welchen Nutzen bringt das?

Durch den Aufbau eines effektiven ISMS können verschiedene Nutzen erreicht werden:

- klare Verbindlichkeit des Managements inkl. Vorbildfunktion
- klare Vorgaben an alle involvierten Stellen
- regelmässige Awareness
- nachvollziehbare Prozesse
- Risiken werden systematisch erkannt, bewertet und behandelt
- (noch) ein Wettbewerbsvorteil
- Reduktion von Audits durch Dritte
- klare Verbindlichkeiten gegenüber Partnern, Lieferanten und Kunden

Fazit

Mit einem ISMS können klare Vorgaben definiert, umgesetzt und geprüft werden. Trotz einem erhöhten initialen Aufwand können durch gemanagte Prozesse in der Folge Geld und interne Ressourcen gespart werden. Zudem existiert ein anerkannter Nachweis, dass in diesem Unternehmen die Informationssicherheit nachhaltig behandelt und verbessert wird. ■

ANDREAS WISLER
Inhaber, Dipl. Ing. FH, CISSP, CISA, ISO 27001 und 22301 Lead Auditor, goSecurity AG, Wiesendangen