ISO 27001

AUSWEIS FÜR IHRE INFORMATIONSSICHERHEIT

von Andreas Wisler

Die Anforderungen an die Informationssicherheit steigen stetig. Täglich ist von neuen Schwachstellen zu lesen, Angriffe auf Firmen und Privatpersonen nehmen zu, und die gesetzlichen und regulativen Anforderungen sind immer aufwändiger zu erfüllen. ISO 27001 ist ein Informationssicherheits-Framework, welches den Umgang mit diesen Themen für das eigene Unternehmen vereinfacht.

Informationssicherheit ist ein aktuelles Thema. Viele Firmen möchten die eigenen und fremden Daten sicher aufbewahren und schützen. Um für Kundinnen und Kunden, Lieferanten und Partner auch einen Nachweis zu haben, wird eine Zertifizierung nach ISO 27001 immer wichtiger. ISO 27001 ist ein Framework, um ein Informationssicherheits-Managementsystem, kurz ISMS, aufzubauen, zu unterhalten und stetig weiterzuentwickeln.

Das Framework besteht aus verschiedenen (Sub-)Standards. Laufend kommen weitere dazu, vor allem im Bereich der sektionsspezifischen Standards in bestimmten Bereichen wie Telekommunikation, Gesundheitswesen und Energieversorgung. Für die eigene Unternehmung sind ISO 27001 und ISO 27002 die wichtigsten Dokumente.

DER RAHMEN DER NORMEN

ISO 27001 beschreibt dabei den Aufbau des Frameworks. Die Kapitel umfassen den Kontext der Organisation (Aufbau, Prozesse, involvierte Stellen, Geltungsbereich und das Managementsystem), Anforderungen an die Führung (Verantwortung und Zuständigkeiten, Leitlinie), der Planung (Risiko-Analyse, Umsetzungspläne), die Unterstützung (Ressourcen, Kompetenzen, Schulungen, Kommunikation), den Einsatz (Planung und Kontrolle), die Auswertung (Überwachung, Messung, Analyse und Auswertung) sowie die stetigen Verbesserungen.

Im zweiten Teil, dem ISO 27002, geht es um konkrete Massnahmen. Total handelt es sich um 114 sogenannte Controls, aufgeteilt in 14 Kapitel. Dabei werden Themen wie die Organisation, Sicherheit des Personals, Management von Werten, Zugriffskontrolle, physische Sicherheit, Betriebssicherheit, Unterhalt und Wartung, Beziehungen mit Lieferanten, Management von Sicherheitsvorfällen sowie Business-Continuity-Management angesprochen.

MANAGEMENT-ANFORDERUNGEN

Mit dem alleinigen Auftrag, ein ISMS aufzubauen, ist die Geschäftsleitung aber heute nicht aus dem Schneider. Mit der Überarbeitung im Jahr 2013 kamen weitere Anforderungen dazu, die die GL 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

In der Norm 100-1 des BSI (Bundesamt für Sicherheit in der Informationstechnik Deutschland) steht dazu Folgendes: «Wenn

Zielvorgaben aufgrund fehlender Ressourcen nicht erreichbar sind, sind hierfür nicht die mit der Umsetzung betrauten Personen verantwortlich, sondern die Vorgesetzten, die unrealistische Ziele gesetzt bzw. die erforderlichen Ressourcen nicht bereitgestellt haben.» Dies zeigt, dass es nicht reicht, sich zur Informationssicherheit zu bekennen, sondern diese muss aktiv gesteuert und zum Erfolg gebracht werden.

Oft stehen solche Systeme in der Kritik, dass viel Papier erstellt werden muss, dies aber für das Unternehmen nur wenig bringt. Dies ist sicherlich teilweise richtig. Auch für ISO 27001 müssen einige Dokumente erstellt werden. Aus Erfahrung von verschiedenen Firmen, sind dies aber Dokumente, die ein Unternehmen auch ohne Zertifizierung erstellen sollte. Gerade die Leitlinie zum Umgang mit der Informationssicherheit ist essenziell. Auch die Risikoanalyse ist wichtig und wird auch für das interne Kontrollsystem IKS nach OR 728a gefordert.

ERFOLGREICHER ABSCHLUSS

Nach der Norm gilt ein Informationssicherheits-System dann als erfolgreich abgeschlossen, wenn folgende Punkte erfüllt sind:

> 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,
> ein Budget für Informationssicherheits-Management zugeteilt wurde und die Aktivitäten zur Informationssicherheit von der Leitung (Topmanagement) unterstützt werden,
> in der Organisation das Verständnis für die Anforderungen an Informationssicherheit verbreitet ist, Risikoanalysen durchgeführt und Notfallvorsorge betrieben wird,
> die Benutzer hinreichend für Informationssicherheit sensibilisiert und geschult sind und die geltenden Sicherheitsvorgaben und Regelungen kennen,
> ein Sicherheitsprozess mit einer regelmässig wiederholten Beurteilung und Verbesserung des ISMS existiert.

ABLAUF ZUR ZERTIFIZIERUNG

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:

1. Unterstützung der Geschäftsleitung einholen
2. Projekt-Plan erstellen
3. Anforderungen und Rahmenbedingungen ermitteln (Interessenvertreter, vertragliche und rechtliche Anforderungen). Dazu sollten unter anderem die folgenden Fragen beantwortet werden:
   a. Welche Geschäftsprozesse gibt es, und wie hängen diese mit den Geschäftszielen zusammen?
   b. Welche Geschäftsprozesse hängen von einer funktionierenden, also einer ordnungsgemäss und anforderungsgerecht arbeitenden IT ab?
   c. Welche Informationen werden für diese Geschäftsprozesse verarbeitet?
   d. Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (zum Beispiel personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?
   e. Gibt es Partner, Kunden oder weitere Stellen, die Zugriff auf Firmenwerte benötigen?
   f. Welche vertraglichen Anforderungen müssen erfüllt werden?
   g. Gibt es rechtliche Vorschriften, die es einzuhalten gilt?
4. Anwendungsbereich definieren (welcher Bereich soll zertifiziert werden?)
5. Informationssicherheitsrichtlinie erstellen
6. Prozess zur Risikoeinschätzung etablieren (Prozesse erfassen, Assets (Werte) definieren), Kritikalität definieren)
7. Risikoeinschätzung durchführen
8. Umsetzung der daraus entstehenden Massnahmen
9. Durchführung von Trainings und Awareness-Schulungen
10. Internes Audit durchführen (Überprüfung der 114 Controls aus ISO 27002)
11. Management-Bewertung durchführen
12. Anmeldung zur Zertifizierung
13. Durchführen des ISO-27001-Audits durch akkreditierte Stelle.

Es lohnt sich dabei, 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 Flut von anderen Tätigkeiten nicht untergeht. Doch nicht alle Schritte können durch eine externe Stelle schnell umgesetzt werden. Gerade die Beschreibung von Prozessen, das Erfassen von Assets (Firmenwerten) und der damit verbundenen Risikoanalyse kann das Unternehmen oft besser und schneller durchführen, sind diese doch schon bekannt. Die erforderlichen Dokumente, der Aufbau des ISMS, eine allenfalls notwendige Anpassung von Prozessen, die Schulung von Mitarbeitern (Schwerpunkt Sensibilisierung) und die Begleitung durch die notwendigen Kontrollen (Internal Audit, Management Review und der zwei- bis dreistufigen Zertifizierung) können abgegeben werden.

Das Resultat dieser Schritte ist ein effektives Informationssicherheitsmodell, durchgängige Prozesse und eine Sensibilisierung aller Mitarbeiter. Gegenüber Kunden, Partnern und weiteren Stellen existiert ein akzeptierter Nachweis über die eigenen Tätigkeiten rund um die Informationssicherheit. ■

ANDREAS WISLER

ist CEO und Senior Security Consultant von goSecurity.

www.gosecurity.ch