ISO 27001 wird zum Qualitätslabel

Informationssicherheit strategisch managen

Von Andreas Koller und Christian Katz

Studien zeigen: 50 Prozent aller Firmen, die wichtige Daten bei einer Katastrophe verloren haben, konnten sich nie davon erholen. Der wirkungsvolle Schutz von Informationen ist für jedes Unternehmen eine Notwendigkeit. Der Management Standard ISO 27001 hilft sehr praxisorientiert, einen solchen Schutz aufzubauen.

Die strategische Bedeutung von Information im Wertschöpfungsprozess, die globale Vernetzung von Unternehmen, aber auch schnell wachsende Bedrohungen verlangen nach wirkungsvollen Managementsystemen, die einen lebbaren und bezahlbaren Informationsschutz ermöglichen.

Mehr als nur IT und elektronische Daten

Weltweiter Standard

Mitte Oktober 2005 wurde der Standard ISO 27001 für Information-Security-Management-Systeme (ISMS) verabschiedet. ISO 27001 übernimmt im Wesentlichen den erfolgreichen British Standard BS 7799 und ersetzt diesen. Weltweit wurden bereits mehr als 2000 ISMS nach BS 7799 aufgebaut und zertifiziert. Marktkenner erwarten in der Folge ein rasantes Wachstum der Zertifizierungen. Das ISO-27001-Zertifikat wird als Qualitätslabel für risikobewusste Unternehmensführung anerkannt werden.

Gründe für die rasche Verbreitung von ISO 27001 sind:

- Der Standard beschränkt sich nicht auf technologische Massnahmen, sondern legt den Schwerpunkt auf eine ganzheitliche Informationssicherheit.
- Sicherheit wird als Prozess verstanden. Dies ist eine wirkungsvolle Unterstützung des Managements, da Prozesse gezielt geplant, betrieben, überwacht, gemessen und optimiert werden können (Grafik).
- Der Standard ist mit anderen wichtigen internationalen Standards (ISO 9001/ISO 14001) harmonisiert. Benutzerfreundliche, integrierte Managementsysteme lassen sich ohne Überschneidungen realisieren.

Was heisst Informationssicherheit managen?

Im allgemeinen Sprachgebrauch wird IT-Sicherheit oft mit Informationssicherheit gleichgesetzt. Dies ist nicht zutreffend, denn IT-Sicherheit beschränkt sich lediglich auf die IT-Infrastruktur und elektronische Daten.

Informationssicherheit ist umfassend und meint den Schutz aller relevanter Informationen, Informationsquellen, Informationsträger und zugehöriger Infrastruktur. Das Ziel ist die Gewährleistung von

- **Vertraulichkeit:** Beschränkung des Informationszugangs auf berechtigte Nutzer,
- **Integrität:** Sicherung der Richtigkeit und Vollständigkeit der Information,
- **Verfügbarkeit:** Sicherung des bedarfsorientierten Zugangs zu Informationen.

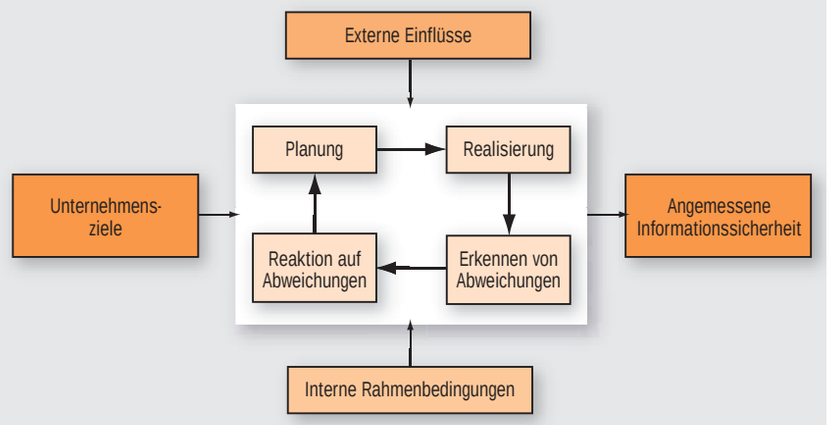
Es geht dabei nicht nur um Hard-, Software und elektronische Daten, sondern auch um Papierdokumente, Gebäude, Kommunikationsmittel und vertrauliche Informationen in den Köpfen von Mitarbeitern und Lieferanten.

Das ISMS basiert auf der Analyse der Geschäftsrisiken und umfasst alle Massnahmen, die zur Gewährleistung der Informationssicherheit notwendig sind. Das heisst: Informationssicherheit ist kein IT-Thema, sondern gehört zur professionellen Corporate Governance und ist eine Aufgabe in der Kompetenz und Verantwortung der Unternehmensleitung.

ISO 27001 in der Praxis

Zentrales Merkmal von ISO 27001 ist, dass Informationssicherheit als geplanter, gelebter, überwachter und sich kontinuierlich verbessernder

Der Sicherheitsprozess



Andreas Koller, und **Christian Katz,** Kompetenzzentrum für Informationssicherheit, Chapfstrasse 18, CH-9032 Engelburg, www.isms-experten.ch, Tel. +41 (0)71 272 80 00, andreas.koller@isms-experten.ch, Tel. +41 (0)71 470 03 30, christian.katz@isms-experten.ch

Die Erfolgsfaktoren

- Commitment der Unternehmensführung: Informationssicherheit ist Chefsache!
- Aktives Mitwirken von Management und Mitarbeitern.
- Sicherheitspolitik, Ziele und Massnahmen sind auf die Kernziele des Unternehmens ausgerichtet.
- Praxisbezogene, systematische Risikoanalyse, die sich am Geschäft orientiert, nicht an komplizierten mathematischen Modellen.
- Pragmatische Vorgehensweise bei der Realisierung des ISMS: Vorhandenes integrieren, optimieren und bei Bedarf ergänzen. Weniger ist mehr!
- Ein bewährtes Grundgerüst für das zu dokumentierende System, das alle von der Norm ISO 27001 geforderten Elemente enthält.

Prozess verstanden wird. Unternehmensziele, externe Einflüsse (Gesetze, Bedrohungen) und interne Rahmenbedingungen (Risikofähigkeit, Geschäftsprozesse usw.) werden berücksichtigt. Die regelmässige Überprüfung der Wirksamkeit ist wichtiger Bestandteil des Systems. Dadurch wird es «lernfähig» und passt sich wechselnden Bedingungen an.

Der Standard lässt bei der Implementierung grosse Flexibilität zu. Es wird festgelegt, was unter bestimmten Rahmenbedingungen getan werden muss, jedoch nicht, wie es getan werden muss. Dies hat den Vorteil, dass schlanke, pragmatische Massnahmen zertifiziert werden können, für KMU ein wichtiges Kriterium, ein «Wasserkopf» wird vermieden.

Zentrales Element der Realisierung ist die Risikoanalyse. Systematisch werden die wichtigen Informationswerte des Unternehmens und die damit verbundenen Risiken identifiziert und der notwendige Schutz festgelegt. Die Risikoanalyse ist die Basis für angemessene Massnahmen.

Die Erfahrung zeigt, dass qualitative Methoden des Risk Assessment ohne mathematischen Ballast sehr schnell zu guten, nachvollziehbaren Ergebnissen führen. Reale «Katastrophenszenarien» werden mit dem Management und verantwortlichen Mitarbeitern systematisch hinterfragt und analysiert. Anstelle von abstrakten Begriffen und Gewichtungsmethoden wird die betriebstypische Terminologie angewandt. Der Bezug zum vertrauten Daily Business ist sehr hoch. Die Vorteile sind:

- Der Gestaltungsprozess wird transparent und verständlich.
- Das Risikobewusstsein wird an den eigenen Geschäftsrisiken geschärft.
- Management und verantwortliche Mitarbeiter können sich wirkungsvoll einbringen und Verantwortung für getroffene Entscheidungen übernehmen.
- Eine hohe Identifikation des Managements mit dem ISMS.

Kosten und Nutzen eines ISMS

Der interne und externe Aufwand für den Aufbau und den Betrieb eines ISMS sind stark abhängig von den Rahmenbedingungen und dem gewählten Vorgehen. Die Durchlaufzeit bis zur Zertifizierung beträgt sechs bis zwölf Monate.

Ein ISMS bringt dem Unternehmen folgenden Nutzen:

- Hohe Risikotransparenz.
- Bewusster Umgang mit Risiken, Reduktion des Risikopotenzials.
- Gesteigertes Risikobewusstsein von Management und Mitarbeitern .
- Koordinierte Sicherheitsmassnahmen: weniger Überschneidungen, weniger Lücken.
- Finanzielle Vorteile, kleinere Fehlerkosten, weniger Ertragsausfälle.
- Sicherstellung der Leistungserbringung dank Business Continuity Management.
- Erhöhung des Vertrauens von Kunden, Geschäftspartnern und Lieferanten dank gelebter Sicherheit.
- Zertifizierung: kommunizierbare und belegbare Informationssicherheit mit internationaler Anerkennung.

Alle müssen Verantwortung übernehmen

Ausblick

Mit ISO 27001 steht erstmals ein bewährter, global anerkannter und zertifizierbarer Standard für Informationssicherheit zur Verfügung. Dank der Skalierbarkeit des Standards lässt sich ISO 27001 sowohl in KMUs als auch in Konzernen effizient anwenden. Wirkungsvoll implementiert und professionell betrieben ist ein ISMS ein wichtiger Pfeiler des Unternehmenserfolges. Und die Entwicklung geht weiter: Für ISO 27003 (ISMS Implementation Guidance), ISO 27004 (ISMS Metrics and Measurement), ISO 27005 (ISMS Risk Standard) ist das Standardisierungsverfahren bereits im Gange. ■