Entspannt an die IT-Revision – ISMS sind Commodity!

Ein Managementsystem für Informationssicherheit ist ein wesentlicher Erfolgsfaktor einer Firma und wird von Revisoren und vom Gesetzgeber verlangt. Etablierte Standards, ein definiertes Vorgehen und toolbasierte Unterstützung machen das ISMS zur Commodity. *Gerold Lauper*

Gerold Lauper
ist Leiter des Bereichs Information Security Management bei Keyon
Lauper@keyon.ch

Informationssicherheitsmanagement (ISM) ist eine wesentliche Grundlage für den Geschäftserfolg und die Unternehmensstabilität. Demzufolge wird ein Managementsystem für Informationssicherheit nicht nur von Aufsichtsorganen oder dem Gesetzgeber gefordert, es wird auch von Geschäftspartnern und Kunden erwartet.

Standards weisen den sicheren Weg

International etablierte Standards legen Umfang, Ziele, Vorgehen und Messgrössen fest, zu denen die Konformität (Compliance) eines Systems nachgewiesen werden kann. Die Standards stellen Anforderungskataloge an Managementsysteme für Informationssicherheit dar und geben Orientierungshilfen beim Aufbau eines Managementsystems für Informationssicherheit (ISMS). Verbreitet ist die Anwendung von ISO 27001 und IT-Grundschutz.

> ***«Ein ISMS kann unternehmensspezifisch und schrittweise mit auf dem Markt verfügbaren Komponenten sicher eingeführt werden.»***

ISO 27001 spezifiziert, welche Elemente ein ISMS enthalten muss und welche Anforderungen an das Management der IT-Sicherheit zu stellen sind. Der Standard formuliert Prozesse und Massnahmenziele, überlässt es jedoch dem Anwender, detaillierte Prozesse und Einzelmassnahmen auszuwählen. Der IT-Grundschutz-Standard schliesst hier die Lücke, indem dort konkrete Einzelmassnahmen und Vorgehensweisen für einen normalen Schutzbedarf vorgeschrieben werden.

Verankerung im Betriebsalltag

Alle notwendigen Elemente für die effiziente und rasche Einführung und Durchsetzung von Managementsystemen für Informationssicherheit sind bekannt und verfügbar. Das Zuschneiden an die individuellen Bedürfnisse und Verhältnisse eines Unternehmens wird über die Parametrisierung erreicht. Zu den wichtigsten Bestandteilen gehören:

- Modellieren von Prozessen, Komponenten und Organisationsstrukturen
- Festlegen von Sicherheitszielen und Massnahmen
- Planung der Einführung und Durchsetzung
- Unterstützung für Umsetzung und Betrieb
- Unterstützung für die laufende Kontrolle und Verbesserung
- Mechanismen für Kommunikation, Ausbildung und Sensibilisierung
- Geeignete Dokumentation für Betrieb und Revision

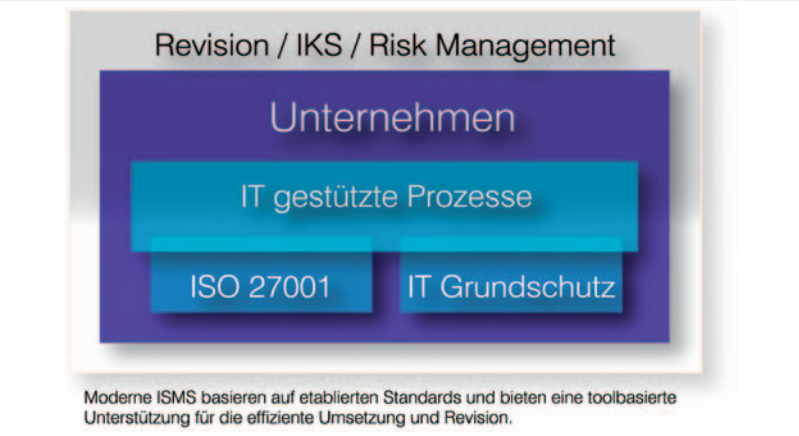
Entscheidend für den Erfolg eines ISMS sind die einfache Integration und die dauerhafte Verankerung im Betriebsalltag.

Die einfache Integration wird über den Einsatz eines Modellierungs- respektive Steuerungstools erreicht. Ein solches Tool bietet eine schnelle und widerspruchsfreie Darstellung der aktuellen Situation des Unternehmens, die anschliessend mit einem fertigen Soll-Modell, basierend auf den Vorgaben der zuvor genannten Standards, verknüpft wird. Daraus resultieren Massnahmen, die umgesetzt werden müssen und Ziele, die entsprechend kontrolliert werden können.

Dauerhaft und gewinnbringend ist ein ISMS, wenn seine Durchsetzung und Kontrolle einfach in den Betriebsalltag integriert werden kann. Toolunterstützt werden hierzu Messgrössen erfasst, die über Managementcockpits kontrolliert und ausgewertet werden können.

Die Module eines ISMS

Umfangreiche Managementsysteme für Informationssicherheit sind auf dem Markt erhältlich und können effizient eingeführt wer-



Der Aufbau eines Managementsystems für Informationssicherheit (ISMS)

den. Insbesondere können mit Hilfe von Unternehmensmodellierungstools Ist-Prozesse und bestehende Komponenten einfach abgebildet und auf der Basis der Vorgaben der Standards beurteilt werden.

Deren modularer Aufbau erlaubt die pragmatische und unternehmensspezifische Einführung eines ISMS in ein Unternehmen. Es beinhaltet im Wesentlichen die folgenden Komponenten:

- **Unternehmensmodellierung und -Steuerung**
  Sie dienen der Erfassung und Modellierung der Unternehmenswerte wie Informationen, Prozesse, Wertschöpfung, Anwendungen, Organisation, IT-Infrastruktur etc. Für die Steuerung werden entsprechende Zielgrössen und Risiken modelliert, bewertet und beurteilt.
- **Standardisierte Prozesse, Massnahmen, Ziele, Messgrössen**
  Sie bilden den Kern eines ISMS und repräsentieren die Vorgaben der Standards. Eine einfache Standortbestimmung hinsichtlich Sicherheit kann durch die Verknüpfung dieser Vorgaben mit dem aktuellen Unternehmensmodell erreicht werden. Weiter lassen sich daraus konkrete Massnahmen ableiten, die für eine bestimmte Zielerreichung umgesetzt werden müssen.
- **Dokumentation, Reports, Weisungen**
  Zielpublikumsorientierte Dokumentation der Einführung, Umsetzung und Durchsetzung des ISMS (Verwaltungsrat, Revision, Geschäftsleitung, Kader, Mitarbeiter etc.). Die Resultate des Sicherheitschecks werden revisionssicher dokumentiert und durch Weisungen und Berichte ergänzt – und dies schnell und widerspruchsfrei auf der Basis der im Unternehmensmodell erfassten Fakten.
- **Webportal**
  Das Webportal bietet eine einheitliche und unternehmensweite Schnittstelle für die Erfassung und Auswertung von Messgrössen sowie für das gezielte Bereitstellen von Weisungen und anderen Informationen an die Mitarbeiter. Durch das in die Unternehmensmodellierung integrierte Webportal wird eine widerspruchsfreie und aktuelle Sicht auf das Unternehmen garantiert.
- **Kommunikationsmanagement und Ausbildung**
  Erfolgsfaktor Mensch. Jeder einzelne Mitarbeiter muss stufengerecht über die Absichten, Vorgaben und Messgrössen des ISMS informiert werden. Informationen müssen gezielt und nachvollziehbar kommuniziert werden. Dies wird erreicht durch den Einsatz von virtuellen Meetingplattformen und Learning-Management-Systemen.
- **Collaboration-Plattform**
  In die Unternehmensmodellierung integrierte, standortübergreifende Plattform zur Umsetzung und Durchsetzung eines ISMS.

ISMS ist ein verstandenes und verfügbares Gut

Die Anwendung solcher Standards auf ein Unternehmen erfordert ein exaktes Massnehmen, Zuschneiden und Verknüpfen aller Komponenten und Prozesse zu einem auf das Unternehmen zugeschnittenen Managementsystem. Das Unternehmen muss hierbei das Ziel verfolgen, die Anforderungen aus verschiedenen Standards zweckmässig zu interpretieren und zu harmonisieren, um so angepasste und wirkungsvolle Managementaktivitäten festzulegen.

Verschiedene Standards, das Wissen und die Tools für eine effiziente und gewinnbringende Einführung und Durchsetzung eines ISMS sind vorhanden. Die pragmatische, phasenweise und modulare Einführung berücksichtigt unternehmensspezifische Gegebenheiten und minimiert das Projektrisiko.

Regulatorien und Bestimmungen, wie beispielsweise die revidierten Artikel im OR, stellen neue Anforderungen an die Unternehmen. Ziel ist es, die Aktivitäten eines Unternehmens messen und beurteilen zu können. Ein ISMS ist das wesentliche Instrument für den Betrieb, die Weiterentwicklung und Beurteilung von IT-gestützten Prozessen.