Vertrauen schaffen mit zertifizierter Sicherheit

IT-Governance und Compliance verlangen nach internationalen Standards. Unternehmen sollten darum den Aufbau eines Information-Security-Management-Systems (ISMS) nach ISO 27001 nicht aufschieben. **VON WOLFGANG SIDLER**

Die internationale Norm ISO/IEC 27001:2005, «Information Technology-Security Techniques – Information Security Mangement System-Requirements», spezifiziert die Anforderungen für die Herstellung, die Einführung, den Betrieb, die Überwachung, die Wartung und die Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS) unter Berücksichtigung der Risiken innerhalb einer gesamten Organisation. Dabei werden alle Arten von Organisationen, wie etwa Handelsunternehmen, staatliche Organisationen oder Non-Profit-Organisationen, berücksichtigt.

ISO/IEC 27001:2005 wurde aus dem britischen Standard BS 7799-2 entwickelt und erstmals am 15. Oktober 2005 als internationale Norm vorgestellt. Die technischen Aspekte werden zwar im Anhang A des ISO-27001-Standards kurz erläutert. Es wird aber hier auf den ISO-Standard-17799:2005 verwiesen, der voraussichtlich im kommen-

Wolfgang Sidler ist Senior Security Consultant bei Infoguard und Mitautor des «Sicherheitshandbuches für die Praxis».

den April in die ISO 27002 überführt wird. Unternehmen, welche bereits den ISO 9001 oder den ISO 20000 (ITIL, BS 15000) kennen, können den Sicherheitsstandard ISO 27001 sehr schnell adaptieren, da die Geschäftsprozesse bereits dokumentiert sind.

Sinnvolle Zertifizierung

Eine Zertifizierung nach ISO 27001 ist sinnvoll, da sie die Möglichkeit der Vergleichbarkeit bietet. Mit einer Zertifizierung können Unternehmen sicherstellen, dass Partner- und Zuliefer-Firmen mindestens das gleiche IT-Sicherheitsniveau haben wie sie selbst. IT-Sicherheit ist immer als Kette zu betrachten – sie zerbricht am schwächsten Glied. Die Einführung eines strukturierten ISMS und die konsequente Umsetzung der Standards hilft Unternehmen in Zukunft dabei, die Kosten der IT-Sicherheit in den Griff zu bekommen. Mittel- und langfristig betrachtet werden auch künftige Risiken klar abschätzbar und der Aufwand für eine optimierte IT-Sicherheit wird auf ein Minimum reduziert.

Ein wesentliches Element eines ISMS nach ISO 27001 ist das so genannte Risiko-Management. Dieses basiert auf der systematischen Erkennung von Risiken an Hand von Risikoanalysen und -bewertungen. Auf der einen Seite ermöglicht nur ein funktionierendes Risikomanagement den Einsatz stets angemessener – also auch wirtschaftlich vertretbarer – Informationssicherheits-Massnahmen. Auf der anderen Seite besteht für jede Organisation die Herausforderung der Integration des Informations-Risikomanagements in bereits bestehende Strukturen und Abläufe des Unternehmens.

Die Erfüllung der Anforderungen an den Managementrahmen für Informationssicherheit einer Organisation sowie an die Implementierung von adäquaten Sicherheitszielen und -massnahmen eröffnet jedem Unternehmen den Weg zu einer zukunftsweisenden Zertifizierung des eigenen ISMS nach dem internationalen Standard ISO 27001.

Zur Erreichung der Normkonformität ISO 27001 sind folgende Anforderungen zu erfüllen:

- Einführung und Aufrechterhaltung eines dokumentierten ISMS
- Definition einer Informationssicherheitspolitik
- Durchführen einer systematischen Risiko-Analyse und -Identifikation sowie Überwachung von Risikobereichen
- Festlegung und Umsetzung geeigneter Sicherheitsziele und Massnahmen

Ein ISO-27001-Zertifikat kann ausschliesslich durch akkreditierte Institutionen vergeben werden, welche international anerkannt sind. In der Schweiz ist dies die SQS (Schweizerische Vereinigung für Qualitäts- und Management-Systeme). Das Zertifikat ist drei Jahre gültig. Während der Gültigkeitsdauer werden zwischenjährliche Überprüfungen, so genannte Audits, durchgeführt.

> Wirkungsvoll implementiert und professionell betrieben ist ein ISMS ein wichtiger Pfeiler des Unternehmenserfolgs.

Aufwand und Nutzen eines ISMS

Der interne und externe Aufwand für den Aufbau und Betrieb eines ISMS ist stark abhängig von den Rahmenbedingungen und dem gewählten Vorgehen. Die Durchlaufzeit bis zur Zertifizierung beträgt erfahrungsgemäss vier bis acht Monate.
Ein ISMS bringt dem Unternehmen folgenden Nutzen:

- Hohe Risikotransparenz
- Bewusster Umgang mit Risiken und Reduktion des Risikopotenzials
- Zunehmende Sensibilisierung der Mitarbeiter für eine ganzheitliche Betrachtung der Sicherheitsstrategie
- Sicherstellung der gesetzlichen und vertraglichen Grundlagen (Outsourcing, etc.)
- Koordinierte Sicherheitsmassnahmen mit weniger Überschneidungen und weniger Lücken
- Wirksamkeit der Sicherheit wird optimiert, da nicht nur die technischen Massnahmen, sondern auch die Prozesse betrachtet werden
- Finanzielle Vorteile, geringere Fehlerkosten, weniger Ertragsausfälle
- Sicherstellung der Leistungserbringung dank Business Continuity Management
- Erhöhung des Vertrauens von Kunden, Geschäftspartnern und Lieferanten
- Kommunizierbare und belegbare Informationssicherheit mit internationaler Anerkennung als zusätzlichem Qualitätsgütesiegel
- Möglichkeit, sich mit Unternehmen im selben Bereich zu messen (Benchmarking)

Ein Muss für Risikobewusste

Aktives Management der Informationssicherheit ist ein Muss für alle Unternehmen, die wertvolle Informationen besitzen oder verarbeiten und eine risikobewusste Unternehmensführung anstreben. Wirkungsvoll implementiert und professionell betrieben ist ein ISMS ein wichtiger Pfeiler des Unternehmenserfolgs.

Mit ISO 27001 steht erstmals ein bewährter, global anerkannter und zertifizierbarer Standard für Informationssicherheit zur Verfügung. Bereits bestehende Managementsysteme – wie beispielsweise ISO 9001 Qualitätsmanagement und ISO 20000 ITIL – werden sinnvoll ergänzt und können integriert werden. Dank der Skalierbarkeit des Standards lässt sich ISO 27001 sowohl in KMU als auch in Konzernen effizient anwenden. Es ist zu erwarten, dass sich dieser Standard schnell verbreiten und zu einem Qualitätslabel für eine risikobewusste Unternehmensführung wird. Mit der Verabschiedung von ISO 27001 stehen wir am Anfang dieser Entwicklung. Für ISO 27003 (ISMS Implementation Guidance), ISO 27004 (ISMS Metrics and Measurement), ISO 27005 (ISMS Risk Standard) ist das Standardisierungsverfahren bereits im Gange. ■