Netzguide E-Security 2006

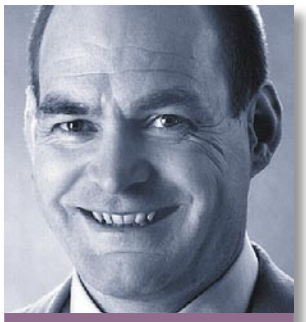
SONDERDRUCK

netzwoche KPMG fg sec

Informationssicherheit strategisch managen

Der wirkungsvolle Schutz von Informationen und deren permanente Verfügbarkeit ist eine existenzielle Notwendigkeit jedes Unternehmens. Der Management-Standard ISO 27001 ist eine praxisorientierte Basis, einen wirkungsvollen Informationsschutz aufzubauen. *Christian Katz, Andreas Koller*

Andreas Koller
Partner bei isms-experten.ch, Geschäftsführer von Avantix AG. Studium der Elektrotechnik/Informatik an der HSR Rapperswil, Quality System Manager, zertifizierter Lead Auditor für ISO 27001. Langjährige Führungs- und Projekterfahrung in der IT Industrie und Anlagenbau.
andreas.koller@isms-experten.ch



Christian Katz
Partner bei isms-experten.ch, Geschäftsführer von wissen.org Katz & Partner. Studium der Mathematik, Informatik und Physik an der Uni Zürich. Seit 10.2005 ist er zertifizierter Lead Auditor für ISO 27001. Er ist erfahrener Berater für Innovation, Effizienz und Wissensmanagement.
christian.katz@isms-experten.ch

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

Mitte Oktober 2005 wurde der Standard ISO 27001 für Information Security Management Systems (ISMS) verabschiedet. ISO 27001 übernimmt im Wesentlichen den British Standard BS 7799, der nun abgelöst wird. Weltweit wurden bereits mehr als 2000 ISMS nach BS 7799 aufgebaut und zertifiziert.

Marktkenner erwarten ein rasantes Wachstum dieser Zertifizierungen. Das ISO-27001-Zertifikat wird als Qualitätslabel für risikobewusste Unternehmensführung anerkannt werden. Gründe dafür 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 (siehe Grafik).
- Der Standard ist mit anderen wichtigen internationalen Standards (ISO 9001/ISO 14001) harmonisiert. Benutzerfreundliche, integrierte Managementsysteme lassen sich ohne Überschneidungen realisieren.

> ***«50 Prozent aller Firmen, die wichtige Daten bei einer Katastrophe verloren haben, konnten sich nie davon erholen. 90 Prozent jener Firmen mussten in der Folge innerhalb von zwei Jahren ihre Geschäftstätigkeit aufgeben.»***
>
> **Quelle: Center for Research on Information Systems, University of Texas**

Informationssicherheits-Management

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

Informationssicherheit ist umfassend und meint den Schutz aller relevanten Informationen, Informationsquellen, Informationsträger und der zugehörigen Infrastruktur. Namentlich die Gewährleistung von

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

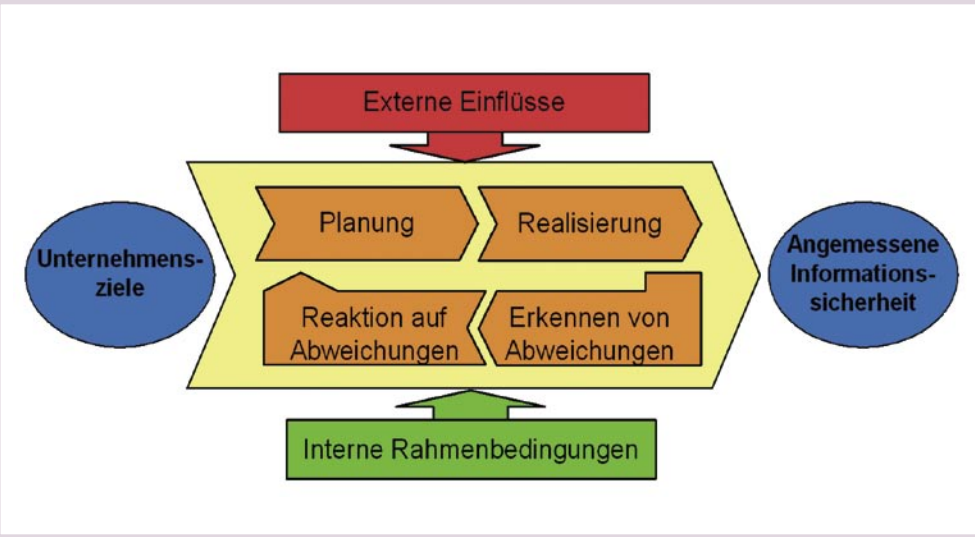
Es geht dabei nicht nur um Hardware, Software und elektronische Daten, sondern auch um Papierdokumente, Gebäude, Kommunikationsmittel und vertrauliche Informationen in den Köpfen von Mitarbeitern und Lieferanten.

Das ISMS basiert auf der Analyse der Geschäftsrisiken und umfasst alle Massnahmen, die zur Gewährleistung der Informationssicherheit notwendig sind.
Damit ist klar, dass Informationssicherheit kein IT-Thema, sondern Aufgabe und Verantwortlichkeit der Unternehmensleitung ist. Informationssicherheit gehört zur professionellen Corporate Governance.

ISO 27001 in der Praxis

Zentrales Merkmal von ISO 27001 ist, dass Informationssicherheit als geplanter, geleb-

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



Sicherheit wird als Prozess verstanden

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 KMUs ein wichtiges Kriterium. Ein «Wasserkopf» wird vermieden.

Zentrales Element bei 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 Assessments 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 eigenen Beispielen 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

Fazit

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 Unternehmenserfolges.

Mit ISO 27001 steht erstmals ein bewährter, global anerkannter und zertifizierbarer Standard für Informationssicherheit zur Verfügung. Bereits bestehende Managementsysteme – etwa der ISO-Standard 9001 Qualitätsmanagement – werden sinnvoll ergänzt und können integriert werden. Dank der Skalierbarkeit des Standards lässt sich ISO 27001 sowohl in KMUs als auch in Konzernen effizient anwenden.

Mit der Verabschiedung von ISO 27001 stehen wir am Anfang einer Entwicklung. Für ISO 27003 (ISMS Implementation Guidance), ISO 27004 (ISMS Metrics and Measurement) und ISO 27005 (ISMS Risk Standard) sind zurzeit weitere Standardisierungsverfahren im Gang.

Die bestimmenden 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.

isms-experten
KOMPETENZZENTRUM FÜR INFORMATIONSSICHERHEIT

Kompetenzzentrum für Informationssicherheit

Im Kompetenzzentrum für Informationssicherheit haben sich Management- und Risikospezialisten, Qualitäts- und Projektmanager, Finanz- und IT Experten zusammengeschlossen. Wir unterstützen Unternehmen beim Aufbau einer umfassenden Informationssicherheit und integrierten Managementsystemen.

Unsere Stärken

- Know- How und Erfahrung aus einer Hand reduziert Überschneidungen und Kosten
- Kurze, zielorientierte Projekte dank erprobter Vorgehensweise
- Beratungsmodell, das Management und Mitarbeiter befähigt (Wissenstransfer)
- Pragmatische Risk Assessment Methodik - "Tell it like a story"
- Bewährtes Dokumentationsgerüst , das alle Anforderungen von ISO9001 / ISO 27001 erfüllt
- Schlanke, integrierte Managementsysteme, die mehrere Standards abdecken

Unser Angebot

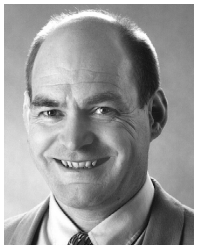
- Beratung bei der Auswahl des für Sie am besten geeigneten Managementsystems
- Massgeschneiderte Unterstützung bei Aufbau und Weiterentwicklung Ihres Managementsystems
- Standortbestimmung und Gap- Analyse
- Audit zum Aufspüren von Verbesserungspotentialen oder als Vorbereitung auf die Zertifizierung
- Schulung und Training

Andreas Koller

Geschäftsführer von Avantix Consult. Studium der Elektrotechnik/Informatik an der HSR Rapperswil (Dipl. Ing. FH), Nachdiplom für Unternehmensführung, Quality System Manager, zertifizierter Lead Auditor für ISO 27001.

Langjährige Führungs- und Projekterfahrung in der IT Industrie und im Anlagenbau.

Tel. +41 (0)71 272 80 00
andreas.koller@isms- experten.ch



Christian Katz

Geschäftsführer von wissen.org Katz & Partner. Studium der Mathematik, Informatik und Physik an der Uni Zürich, zertifizierter Lead Auditor für ISO 27001.

Erfahrener Berater in IT- Projekten, für Wissensmanagement und Managementsysteme.

Tel. +41 (0)71 470 03 30
christian.katz@isms- experten.ch