Standards zur Datensicherung

Die Sicherheit von Information ist heute zentral. Ein Weg dazu ist ein Security Management auf Basis der ISO 2700x Standards.

Von Andreas Wisler

Informationen und Daten gehören heute für alle Unternehmen zu ihren wichtigsten Gütern, und diese zu schützen ist ein Muss. Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach einer Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur IT-Sicherheit entstanden. Die internationale Norm ISO/IEC 27001:2005 ist eine davon und der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht. Diese Norm spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen berücksichtigt.

Das Wichtigste ist die Risikobeurteilung

Nachfolgend wollen wir uns mit dem ISO-Standard 27001 etwas genauer beschäftigen, der einen aktiven Schutz der Informationen gewährleistet. Nach ISO 27001 soll ein Informationssicherheits-Managementsystem (ISMS) aufgebaut werden, welches die Grundlage zur Identifikation und Beherrschung der Informationssicherheitsrisiken sowie zur Sicherstellung der Zuverlässigkeit von Systemen bietet. Bevor jegliche Massnahmen umgesetzt werden können, muss allerdings zuerst das Risiko bekannt sein. Als Risiko wird nach ISO 73 eine Kombination aus der Wahrscheinlichkeit eines unerwünschten, unerwarteten oder schädlichen Ereignisses und dessen Konsequenzen definiert. Es stellen sich damit zwei Fragen: Welche Ereignisse gilt es zu untersuchen? Welche Konsequenzen können daraus entstehen?

Mögliche Ereignisse, die auf eine Organisation einwirken können, sind zum Beispiel gezielte Angriffe von Personen auf technische oder organisatorische Schwachstellen, Elementarereignisse wie Erdbeben, Feuer, Wassereinbruch oder Blitzschlag, fahrlässige Handlungen oder Fehlbedienung von Systemen, Verstösse gegen Gesetze oder Verträge sowie potentielle Schädigung von Personen.

Die Konsequenzen solcher Ereignisse können je nachdem unmittelbaren monetären Schaden verursachen, aber auch Imageverlust, Verlust der Kreditwürdigkeit oder Entzug von Genehmigungen mit sich bringen. Der ISO-Standard verlangt deshalb für jeden erkannten Informationswert die Risiken bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität und gegebenenfalls weiterer Ziele zu identifizieren und abzuschätzen. Dabei gehen die Bedrohungen, Schwachstellen sowie die Einschätzung von Ausmass und Häufigkeit der Schäden ein.

Wie ein ISMS funktioniert

Wie bereits aus anderen Bereichen bekannt, verwenden auch die ISO-2700X-Normen das PDCA-Modell (Plan-Do-Check-Act) von William Edwards Deming (siehe dazu Grafik). Demnach muss ein Informationssicherheits-Managementsystem immer folgendermassen aufgebaut sein und angewendet werden:

Als erstes gilt es, die ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren festzulegen, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen. Danach müssen das Umsetzen und Durchführen der ISMS-Leitlinie, Massnahmen, Prozesse und Verfahren definiert werden. Schliesslich folgen das Einschätzen und gegebenenfalls Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen sowie das Berichten der Ergebnisse an das Management zwecks Überprüfung. Abschliessend folgen das Handeln, das Ergreifen von Korrekturmassnahmen und Vorbeugungsmassnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und das Überprüfen des Managements und anderen wesentlichen Informationen zur ständigen Verbesserung des ISMS.

Aufbau von ISO 27001

Schauen wir uns die ISO-Norm 27001, die in mehrere Kapitel unterteilt ist, noch ein bisschen genauer an. Der erste grosse Teil der Norm beschreibt die allgemeinen Anforderungen an ein ISMS. Ein wichtiger Aspekt gilt, das haben wir uns ja bereits näher ange-

IN KÜRZE

- Die internationale Norm ISO/IEC 27001:2005 ist ein Standard zum IT-Sicherheitsmanagement und ermöglicht eine Zertifizierung.
- Die Basis dafür bilden die eigenen Risiken, die zum Start unbedingt gefunden und bewertet werden müssen.
- Die ISO-2700X-Normen sind nach dem Plan-Do-Check-Act-Modell aufgebaut und zu handhaben.

DAS SIND DIE ISO-STANDARDS 2700X

Die gesamte ISO-2700x-Reihe besteht aus verschiedenen Standards, die sich ergänzen:

Standard	Inhalt
ISO 27000	Begriffsdefinitionen zum Informationssicherheits-Managementsystem (ISMS)
ISO 27001	Definition der Zertifizierungsanforderungen an ein ISMS
ISO 27002	Leitfaden zur Implementierung, Kontrollfragen
ISO 27003	Einführungshilfe für ein ISMS (in Arbeit)
ISO 27004	Definition von Kennzahlensystemen für ein ISMS
ISO 27005	Risikomanagement zum ISMS
ISO 27006	Kriterien für Institutionen, die das Audit und die Zertifizierung durchführen
ISO 27007	Richtlinien für das Audit (in Arbeit)

schaut, dem Festlegen und dem anschliessenden Umsetzen und Durchführen. Dazu gehören die Definition des Anwendungsbereichs und der Grenzen, die Identifizierung der Risiken inklusive einer Analyse und Bewertung sowie die Optionen für die Risikobehandlung mit anschliessender Auswahl der Massnahmen zur Risikobehandlung. Die Norm verlangt hier unter anderem klar, dass ein Programm zur Schulung und Bewusstseinsbildung umgesetzt wird.

Weiter gehört zu einem ISMS nach ISO 27001 auch das Überwachen und Überprüfen in regelmässigen Abständen dazu. Die Norm verlangt, dass mindestens einmal pro Jahr interne beziehungsweise eigene Audits erfolgen müssen. Diese «internen» Audits dürfen an externe, spezialisierte Firmen in Auftrag gegeben werden. Dies kann sich sicherlich lohnen, kommt doch eine unabhängige Drittmeinung dazu. Alle drei Jahre ist die Zertifizierung zu wiederholen. Sollten in den internen und externen Audits Mängel festgestellt werden, sind diese instand zu stellen und zu verbessern.

Ein weiteres Kapitel im ersten Teil beschreibt die Dokumentationsanforderungen. Die Dokumentationen müssen Aufzeichnungen von Managemententscheidungen enthalten, sicherstellen, dass sich Aktivitäten auf Managemententscheidungen und Grundsätze zurückverfolgen lassen, und sicherstellen, dass die aufgezeichneten Ergebnisse reproduzierbar sind. Es ist wichtig, dass es möglich ist, die Beziehung von den ausgewählten Massnahmen zurück zu den Resultaten des Risikoeinschätzungs- und Risikobehandlungsprozesses nachzuweisen und weiterhin zurück zu der ISMS-Leitlinie und den -Zielen.

Die Verantwortung des Managements

Der zweite Teil des ISO-27001-Standards nimmt das Management in die Pflicht. Es muss in acht Punkten nachweisen, dass es seine Verpflichtungen wahrnimmt. Dazu gehört auch das Ermitteln und Bereitstellen der erforderlichen Ressourcen. Weiter muss die Organisation sicherstellen, dass die Schulungen, das Bewusstsein und die Kompetenzen vorhanden sind.

Wie bereits erwähnt, gilt es, das ISMS mindestens einmal pro Jahr zu überprüfen. Dieses Kapitel der Norm zeigt, was die Managementbewertung im Minimum enthalten muss. Die Ergebnisse der Managementbewertung müssen Entscheidungen und Aktivitäten zur Verbesserung und Wirksamkeit sowie die Aktualisierung des Risikoeinschätzungsplans enthalten.

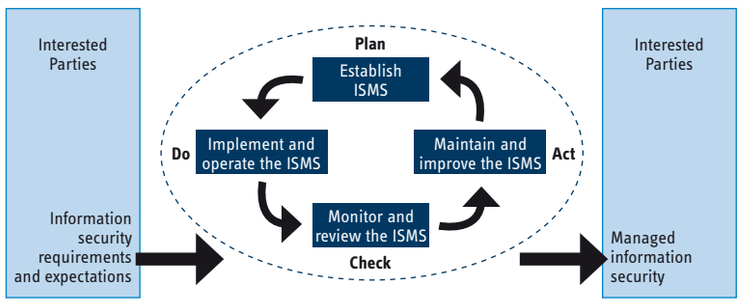
Ein weiteres, eigenes Kapitel widmet sich der Pflege und Verbesserung des ISMS. Wie der PDCA-Zirkel zeigt (siehe Grafik), bewegt sich das ISMS immer weiter. Ein Stillstand ist nicht möglich. Die Organisation muss Massnahmen zur Beseitigung der Ursachen von Nichtkonformitäten mit den ISMS-Anforderungen ergreifen, um deren erneutes Auftreten zu verhindern. Weiter gehören Vorbeugungsmassnahmen dazu, damit potentielle Probleme erst gar nicht auftreten können.

ISO 27002 und ISO 27005

Obwohl die ISO-Norm 27001 klare Anweisungen und Aufgaben enthält, ist es nicht immer einfach, entsprechende Massnahmen abzuleiten. Hier hilft der neue Standard «Information Security Risk Management», kurz ISO/IEC 27005:2008, welcher den Prozess des Security-Risk-Managements beschreibt und entsprechende Handlungsempfehlungen für Unternehmen liefert.

Der Standard ISO 27002 definiert ein Rahmenwerk für das IT-Sicherheitsmanagement und befasst sich mit den erforderlichen Schritten, um ein funktionierendes IT-Sicherheitsmanagement aufzubauen. Gegliedert ist das Werk in elf Managementgebiete mit 39 Massnahmenzielen. Die Massnahmenziele enthalten insgesamt 133 Massnahmen (baseline controls), die zur Zielerreichung umgesetzt werden können. Die elf Managementgebiete umfassen dabei folgende Punkte: Sicherheitsleitlinie, Organisation der Informationssicherheit, Management von organisationseigenen Werten, Personalsicherheit, physische und umgebungsbezogene Sicherheit, Betriebs- und Kommunikationsmanagement, Zugangskontrolle, Beschaffung, Entwicklung und Wartung von Informationssystemen, Umgang mit Informationssicherheitsvorfällen, Sicherstellung des Geschäftsbetriebs und Einhaltung von Vorgaben.

DAS PLAN-DO-CHECK-ACT-MODELL



Quelle: William Edwards Deming

DIE ISO-NORM 27001

Die ISO-Norm 27001 beschreibt das Informationssicherheits-Managementsystem (ISMS) im folgenden Satz: «Die Organisation muss ein dokumentiertes ISMS im Kontext ihrer allgemeinen Geschäftsaktivitäten und der Risiken, der sie sich gegenübersieht, festlegen, umsetzen, durchführen, überwachen, überprüfen, instandhalten und verbessern.»

Probleme vermeiden

Die internationale Norm ISO/IEC 27001:2005 ist so aufgebaut, dass sie Schrittweise umgesetzt werden kann. Zuerst müssen wie erwähnt aber so oder so die eigenen Risiken gefunden und bewertet werden. Hierfür muss man viel Zeit einplanen, denn alle weiteren Schritte hängen von der seriösen Abklärung der Risikostellen ab. Eine externe Hilfe kann hier viel Zeit sparen, kommen doch erfahrene Berater dazu, die bereits in anderen Firmen entsprechende Gefahrenstellen und Risiken erkannt und beurteilt haben.

Bei der eigentlichen Zertifizierung versuchen sich die Auditoren in die Lage des Unternehmens zu versetzen und selber die Risikostellen zu identifizieren. Anschliessend werden diese mit denjenigen des Unternehmens verglichen. Sind alle vorhanden? Sind weitere erkannt worden? Werden entsprechende Massnahmen abgeleitet? Erst danach werden die entsprechenden Massnahmen genauer angeschaut. Dabei geht es weniger um die technischen Details, sondern um die korrekte Erkennung und das Einleiten von Massnahmen. Diese Schritte müssen zwingend dokumentiert werden. Protokolle der Managementsitzungen und internen Audits bilden einen weiteren Kontrollpunkt der Auditoren. Sind auch hier Risiken und passende Massnahmen enthalten? Falls dies regelmässig und vollständig stattfindet, steht einer erfolgreichen Zertifizierung nach ISO 27001 nichts mehr im Wege.

Andreas Wisler ist Dipl. IT Ing. FH, CISSP, ISO 27001 Lead Auditor und Geschäftsführer der GO OUT Production GmbH.