Praxis der Informationssicherheit

NA 043-01-27 AA „IT-Sicherheitsverfahren“

Erfahrungen mit den Normen der Reihe ISO/IEC 27001

Dr.-Ing. *Michael Gehrke*
ist Geschäftsführer der TTS Trusted Technologies and Solutions GmbH, Essen, und Mitglied im Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“.

Dr.-Ing. *Jörg Cordsen*
ist Geschäftsführer der TTS Trusted Technologies and Solutions GmbH, Berlin, und Mitglied im Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“.

Die Internationale Norm ISO/IEC 27001:2005-10 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“ wurde aus dem britischen Standard BS 7799-2:2002 entwickelt. Sie spezifiziert die Anforderungen an Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS).

Seit September 2008 liegt die Norm auch als DIN-Norm vor. Die deutsche Ausgabe wird im DIN betreut vom Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“, der an der internationalen Normungsarbeit im zuständigen gleichnamigen Komitee ISO/IEC JTC 1/SC 27 mitwirkt.

Dieser Beitrag berichtet über Erfahrungen der TTS Trusted Technologies and Solutions GmbH, die bei der Implementierung von Informationssicherheits-Managementsystemen auf Basis der ISO/IEC 27001 sowie anderer Sicherheitsvorgaben gemacht wurden.

Warum braucht man ein Informationssicherheits-Managementsystem?

Den Schutz von Informationen, das heißt die Vertraulichkeit, Integrität, Verfügbarkeit und gegebenenfalls auch die Verbindlichkeit zu gewährleisten, stellt sich für Unternehmen als zunehmend komplexes Unterfangen dar. Die Gründe dafür sind in erster Linie in der Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung sowie in der gestiegenen Komplexität der Informationstechnologien zu sehen. Beispielsweise bindet ein **Kundenunternehmen** etwa 1 800 Zulieferer über mehrere hundert Systeme an sein Unternehmensnetz an.

Eine weitere Rolle spielt natürlich auch die permanente Änderung der Bedrohungslage, die sich unter anderem durch eine gewachsene Bedeutung des Sabotageschutzes, individualisierte Schadsoftware oder auch eine Kommerzialisierung der Wirtschaftsspionage und Hackerszene ausdrückt. Gleichzeitig sind die Ressourcen zum Schutz der Informationen in den Organisationen begrenzt und zum Teil durch Prozess- und Personaloptimierungen sogar reduziert worden.

Auf der anderen Seite wird seit wenigen Jahren auf Verletzungen der Informationssicherheit oder des Datenschutzes sehr sensibel reagiert. Keinem Vorstand oder Unternehmensleiter ist es heute egal, ob sensible Kundeninformationen, Produktpläne oder Ähnliches in fremde Hände geraten könnten. Gesetzgeber und Fachorganisationen reagieren mit Vorgaben zur Compliance und Governance (BilMoG, KonTraG, BASEL II, Cobit, ISO 38500, ...). Unter IT-Compliance wird die Einhaltung und Umsetzung von regulatorischen Anforderungen im weitesten Sinne mit dem Ziel eines verantwortungsvollen Umgangs mit allen Aspekten der Informationstechnik (IT) verstanden. Der Begriff der IT-Governance umfasst alle Maßnahmen zur Organisation, Steuerung und Kontrolle der IT-Systeme eines Unternehmens.

Wie können also Organisationen diesem Dilemma der steigenden Anforderungen und sinkenden Ressourcen entrinnen?

Eine Lösungsmöglichkeit ist die organisationsindividuelle Implementierung geeigneter Sicherheitsmaßnahmen durch ein risiko- und prozessorientiertes Vorgehensmodell.

Prozessorientiertes Vorgehensmodell nach DIN ISO/IEC 27001

In DIN ISO/IEC 27001 ist zunächst ein prozessorientiertes Vorgehensmodell definiert (Bild 1).

Im ersten Schritt sollten die für das Informationssicherheits-Managementsystem (ISMS) wesentlichen Komponenten eingerichtet werden, das heißt, zugeschnitten auf das Unternehmen wird

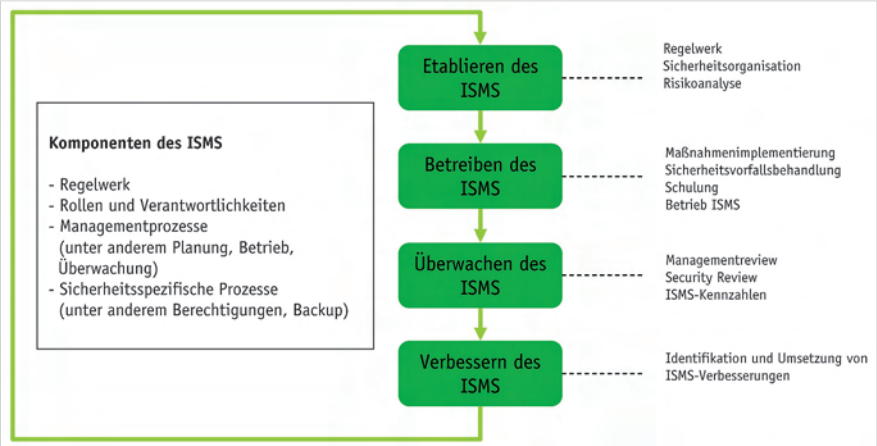

Bild 1: Das Bild Plan-Do-Check-Act-Zyklus der DIN ISO/IEC 27001

eine geeignete Sicherheitsorganisation errichtet sowie ein Regelwerk, das die erforderlichen Vorgaben zur Informationssicherheit in problemadäquaten Sicherheitsrichtlinien ausdrückt. Weiterhin werden mittels einer Schutzbedarfsfeststellung und Risikoanalyse die wichtigsten Bedrohungen für die Informationssicherheit identifiziert und risikomindernde Sicherheitsmaßnahmen definiert.

Der Betrieb des ISMS umfasst die Implementierung der definierten Sicherheitsmaßnahmen, Schulungs- und **Awareness-**Maßnahmen oder die Behandlung von Sicherheitsvorfällen, quasi das Tagesgeschäft des ISMS.

Zur Einleitung der Rückkopplungsschleife erfolgt dann mit der Überwachung des ISMS die Kontrolle, ob die definierten Sicherheitsmaßnahmen ausreichend umgesetzt und wirksam sind. Gleichzeitig wird aber auch überprüft, ob die Aufbau- und Ablauforganisation des ISMS geeignet ist, um die Informationssicherheit in einem wirtschaftlich vertretbaren Rahmen zu gewährleisten. Durch Überwachungsmaßnahmen sollten gegebenenfalls Verbesserungsansätze erkannt und umgesetzt werden.

Ziel dieses prozessorientierten Vorgehensmodells ist es, die Ausprägung und den Umfang des ISMS immer näher an das von der Organisation geforderte Sicherheitsniveau anzupassen. So wird Wichtiges von Unwichtigem getrennt und die knappen Ressourcen dort eingesetzt, wo sie wirklich erforderlich sind.

Was nutzt die Orientierung an Normen?

Neben der Orientierung an der Internationalen Norm ISO/IEC 27001 gibt es weitere Möglichkeiten, ein ISMS einzusetzen. In der TTS wurde hierfür der Begriff „ISMS-Pattern“ geprägt. Mit dem Begriff soll ausgedrückt werden, dass beispielsweise je nach Größe, Internationalität oder auch Geschäftszweck einer Organisation unterschiedliche Verfahrensweisen und Methoden zweckmäßig sind, ein ISMS zu implementieren. Die Spannweite reicht von Selbstauditierungsschemata bis hin zur umfassenden Einsetzung weitreichender Sicherheitskataloge, wie den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik. Und natürlich kann für eine Organisation auch eine Mischform geeignet sein. Grundsätzlich bietet aber die Ausrichtung des ISMS an einer Norm wie der Internationalen Norm ISO/IEC 27001 zusammen mit ISO/IEC 27002 „Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Management der Informationssicherheit“ folgende Vorteile:

- Sie bietet eine Orientierungshilfe, welche Aspekte zur Informationssicherheit relevant sind.
- Sie ist eine Messlatte dafür, welche Sicherheitsmaßnahmen zum „Konsens“ der Sicherheitspraxis gehören.
- Sie ist ein Praxisreservoir für Sicherheitsmaßnahmen.
- Die Darstellbarkeit der erforderlichen Sicherheitsmaßnahmen im Unternehmen sowie zu den Geschäftspartnern wird erleichtert.
- Die Durchsetzbarkeit der erforderlichen Sicherheitsmaßnahmen im Unternehmen als auch zu Geschäftspartnern wird unterstützt.
- Sie erleichtert die Festlegung und Überprüfung von Sicherheitsvorgaben bei der Abgabe von Unternehmensaufgaben an Drittunternehmen (Outsourcing).
- Sie bietet das Potenzial für ein integriertes Managementsystem, in dem Sicherheit zusammen mit anderen Aspekten, wie zum Beispiel Qualität oder Umwelt, betrachtet wird.
- Nicht zuletzt ermöglicht die Norm ISO/IEC 27001 die Zertifizierung des ISMS und unterstützt damit die Vermarktung von Leistungen der entsprechenden Organisation.

Ein weiterer Grund für die Einführung eines ISMS in einem Unternehmen ist die Tatsache, dass die Einhaltung von ISMS-Standards zum Teil auch von Kunden gefordert wird. So hat der Verband der Automobilindustrie (VDA) in seiner Veröffentlichung zum „Integralen Informationsschutz mit IT-Sicherheit, Prototypenschutz und Risk-Management“ die Umsetzung der ISO/IEC 27001 empfohlen.

Robustheit von Informationssicherheits-Managementsystemen

Der Terminus „Robustheit“ ist neben anderen Disziplinen besonders aus dem System- und Softwaredesign bekannt. Robustheit ist die Eigenschaft eines Systems, seine Funktion auch bei Veränderungen der Umgebungsbedingungen aufrechtzuerhalten. Wie robust muss also ein ISMS eigentlich sein, beziehungsweise durch welche Umgebungsbedingungen ist die Funktion des ISMS, die Sicherheit aufrechtzuerhalten, gefährdet?

Die Beratungspraxis hat gezeigt, dass Prüfsteine für die Robustheit eines ISMS besonders die folgenden Situationen sein können:

- M&A-Aktivitäten (Mergers & Acquisitions) eines Unternehmens sorgen häufig dafür, dass ein erreichter Entwicklungsstand eines ISMS eines betroffenen Unternehmensteils stagniert oder sogar zurückgeht.

- Das Outsourcing der Informationsverarbeitung hat zur Folge, dass die üblichen Verfahren in einem ISMS beispielsweise zur Schutzbedarfsanalyse, zur Risikoermittlung und -behandlung oder zum Business Continuity Management angepasst werden müssen. So kann das auslagernde Unternehmen zwar die Schutzbedürfnisse ermitteln, der Dienstleister muss aber die Risikoermittlung und -behandlung übernehmen. Um wirtschaftlich zu arbeiten, besteht zudem die Tendenz, gemeinsam genutzte Ressourcen einzusetzen, sodass kumulierte Risikoanalysen erforderlich werden.
- Der Kostendruck in Form von Personal- und/oder Budgeteinsparungen ist natürlich eine besondere Herausforderung an ein ISMS, weil die Ressourcen noch besser auf die vorhandenen Risiken verteilt werden müssen. Hier sind eindeutig Organisationen im Vorteil, die risikoorientiertes Handeln gewohnt sind.
- Ein Wechsel der Schlüsselpersonen, wie dem Verantwortlichen für Informationssicherheit (Chief Information Security Officer – CISO) oder dem zuständigen Geschäftsführer beziehungsweise Vorstand, kann ebenso positive wie negative Auswirkungen auf die ISMS-Landschaft haben, abhängig davon, wie ausgeprägt das Verständnis von der Wertschöpfung der Informationssicherheit für die eigenen Geschäftsprozesse ist.

In allen Fällen aber wird sich eine vorhandene Zertifizierung des ISMS nach DIN ISO/IEC 27001 positiv auswirken. Denn der Verlust der Zertifizierung, bedingt durch nachlassende Aktivitäten im ISMS, ist ein sichtbarer Beleg für ein sinkendes Sicherheitsniveau und steigende Risiken.

Vergleichbarkeit von Informationssicherheits-Managementsystemen

Eine Vergleichbarkeit der Systeme ist durch die Zertifizierung alleine nicht gegeben. Durch die Erteilung des Zertifikates wird nur belegt, dass eine Organisation für den „Zertifizierungsbereich“ bestimmte prozessuale und dokumentatorische Anforderungen erfüllt hat. Günstigstenfalls könnte man davon sprechen, dass zwei Organisationen alle Maßnahmen zur Absicherung ihrer individuellen Risiken identifiziert und behandelt haben. Nach wie vor trifft das aber keine Aussage darüber, ob die Risikoexponiertheit zweier Unternehmen vergleichbar ist.

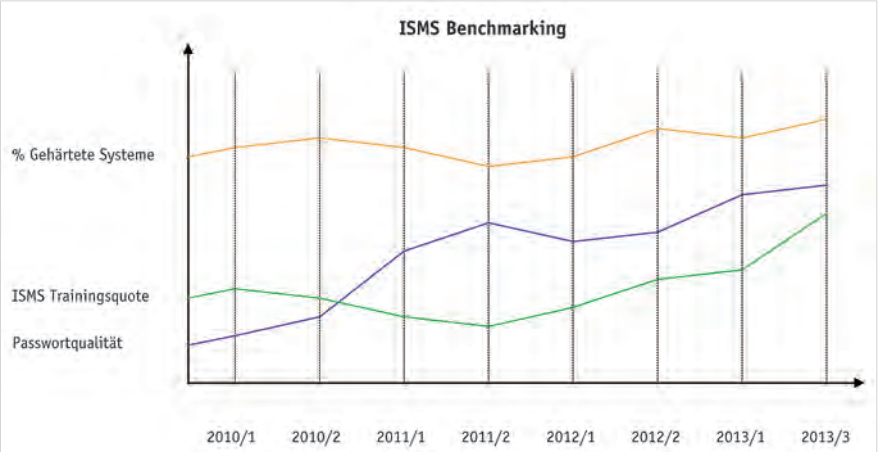

Bild 2: Beispiel für eine vergleichende Darstellung der Entwicklung von Kennzahlen in einem ISMS

Hier ist ein Ansatz über die Messbarkeit von Informationssicherheit hilfreich, wie er in der Internationalen Norm ISO/IEC 27004 „Information technology – Security techniques – Information security management – Measurement“ definiert ist, die mit Ausgabedatum Dezember 2009 veröffentlicht wurde.

Ausblick ISO/IEC 27004

In der Norm ISO/IEC 27004 ist ein Ansatz zur Entwicklung eines Kennzahlenprogramms festgelegt, mit dem die folgenden Ziele erreicht werden sollen:

- Bewertung der Wirksamkeit einzelner Sicherheitsmaßnahmen
- Bewertung der Wirksamkeit des ISMS
- Feststellung des Umsetzungsgrades von Sicherheitsanforderungen
- Unterstützung von Effizienzsteigerungen der Informationssicherheit
- Unterstützung von Managementbewertungen.

Beispiele für solche Kennzahlen sind etwa die Qualität der Passwörter, gemessen am Prozentsatz der Passwörter, die die Passwortrichtlinie einhalten, oder die ISMS Trainingsquote als Prozentsatz der geschulten Mitarbeiter gemessen am Soll.

Für die Managementbewertung (Management Review) sind solche Kennzahlen hervorragend geeignet, in übersichtlicher Form einen Überblick über die Entwicklung des ISMS zu geben (Bild 2). Besonders muss darauf geachtet werden, ein für die jeweilige Organisation passendes Kennzahlensystem zu entwickeln, das ihre individuellen Sicherheitsanforderungen geeignet widerspiegelt und auch mit angemessenem Aufwand realisierbar ist.

Zusammenfassung

Dabei erweist sich die Internationale Norm DIN ISO/IEC 27001 in der praktischen Arbeit als gute Richtschnur zur Realisierung von Informationssicherheit auf Basis eines prozessorientierten Vorgehensmodells.

Informationssicherheit ist heute nicht mehr technologisch begründet, sondern hat sich zur Management-Disziplin entwickelt. Im Mittelpunkt der Informationssicherheit stehen jetzt Prozesse, die es erlauben, kalkulierbar mit den Risiken einer weltweiten Vernetzung, erhöhtem Wettbewerb und aggressiven Bedrohungen umzugehen. ◆