Vertrauen schaffen mit zertifizierter Sicherheit: Informations-Sicherheit für KMU

IT Governance und Compliance verlangen nach internationalen Standards. Unternehmen sind heute international vernetzt und der damit verbundene Datenaustausch sowie die Datenschutzproblematik und andere gesetzlichen Anforderungen zwingen die Unternehmen, ein nach ISO 27001 internes Information Security Management System (ISMS) aufzubauen.

Wolfgang Sidler

Unternehmen stehen vermehrt ansteigenden Bedrohungspotenzialen gegenüber, während gleichzeitig die Haftungsansprüche gegen die Gesellschaften und ihre Geschäftsführungen immer weiter verschärft werden. Die Unternehmensführungen sind somit in zunehmendem Masse verpflichtet, die Erreichung ihrer strategischen Sicherheitsziele zu gewährleisten und damit reale Risiken und die daraus resultierenden wirtschaftlichen Schäden im Unternehmen zu minimieren. Ein wirksames Mittel, um diese Aufgaben zu bewältigen, ist die nachhaltige Einführung eines Information Security Management System (ISMS).
Die Informations- und IT-Sicherheit spielt heute auch für die KMU eine immer wichtigere Rolle – jedoch sind diese Unternehmen oft nicht in der Lage, ein umfassendes IT-Sicherheits-Konzept im Alleingang zu erstellen und zu betreiben.

Wie sieht es bei Ihnen aus?

- Kennen Sie die Risiken und Schwachstellen Ihrer Informatik?
- Wie schützen Sie Ihr Know-how?
- Sind Ihre Daten und Ihre Geschäftsprozesse sicher?
- Welches sind die Anforderungen an die Sicherheitsverantwortlichen von morgen?
- Wie wirkt sich die zunehmende Mobilität auf die Informationssicherheit aus?

Information schützen – Unternehmenswert sichern

Informationen sind für Unternehmen wichtige Geschäftswerte, die für die Leistungserstellung von zentraler Bedeutung sind und demnach wirksam geschützt werden müssen.
Ohne Informationstechnik (IT) kommt heute kein Unternehmen mehr aus, und die laufend neuen Mittel greifen immer stärker in die Geschäftsprozesse ein. Damit wächst die Abhängigkeit von der IT, und es gehört folglich zu den wichtigen Aufgaben des Managements, alles zu unternehmen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, also eine umfassende Informations-Sicherheit zu gewährleisten. Der ständig wachsende Marktdruck verlangt schlanke Strukturen, eine hohe Effizienz und hohe Verfügbarkeit der Daten.
Ausfälle der Infrastrukturen ziehen direkte Einbussen am Ertrag und Unternehmensimage nach sich.
Gefahren wie bösartige Programme oder das Ausspionieren des Nutzungsverhaltens sind die Schattenseiten dieser Informationstechnologie und der weltweiten Vernetzung. Der Selbstschutz wird deshalb immer bedeutender. Das persönliche, verantwortungsvolle und aufmerksame Verhalten bei der Nutzung der IT-Infrastruktur ist deshalb der entscheidende Faktor. Die wahre Herausforderung stellt die Umsetzung und erfolgreiche Durchsetzung der entsprechenden Informations-Sicherheits-Strategie dar.

Sensibilisierung des Managements

Zu den zentralen Aufgaben des Managements einer Unternehmung gehört der Umgang mit Risiken.
So birgt das Erwirtschaften von Gewinn immer auch spezifische Risiken und verschärft wird dies u. a. dadurch, dass Entscheidungen in immer kleineren Zeitintervallen erwartet werden.
Vielfach sind kleinere und mittlere Firmen durch ihre Tagesgeschäfte so stark absorbiert, dass für Aktivitäten ausserhalb der Kernbereiche meist nur wenig oder sogar gar keine Ressourcen übrig bleiben. Viele Unternehmen unterschätzen ihre Abhängigkeit von der IT und sind sich einfach nicht bewusst, wie stark ihr Erfolg von der IT-Sicherheit abhängt.
Neben dem Datenschutzgesetz und zivilrechtlichen Verpflichtungen durch vertragliche Vereinbarungen kann z. B. Organisationsverschulden durch die Verletzung von Organisationspflichten erhebliche Folgen im Schadensfall nach sich ziehen:
- strafrechtliche Ahndung mit Freiheits- oder Geldstrafe
- zivilrechtliche Haftung (Schadensersatz)
- ordnungsrechtliche Verfolgung gegen Führungskräfte des Unternehmens

Im Schadensfall ist der Nachweis wichtig, dass die Einhaltung der Vorschriften durch Organisationsabläufe geregelt und kontrolliert wird. Dabei existiert für IT-Risiken eine Reihe von Massnahmen zur Minimierung des Haftungsrisikos:
- Durchführung von betrieblichen Risikoanalysen
- Aufbau und Betrieb von Managementsystemen zur Steuerung und Beherrschung der Unternehmensrisiken
- Regelung für den Umgang mit Fremdfirmen (Schnittstellensicherheit)

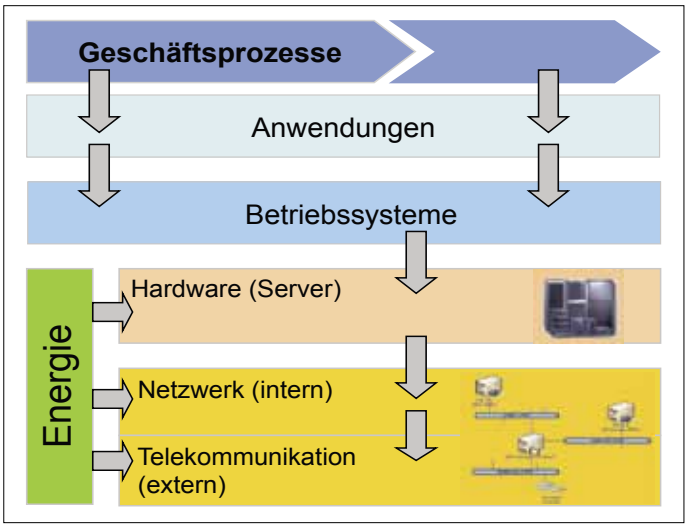

Abbildung 1: Abhängigkeit der Geschäftsprozesse.

Die folgenden externen Faktoren begünstigen bzw. verlangen nach mehr Informations-Sicherheit in einem Unternehmen:
- Gesetzliche Anforderungen (IKS OR 728a seit Juli 2007 in Kraft, DSG etc.)
- Wettbewerb
- ISO 27001 Zertifizierung (Ausschreibungen verlangen eine ISO 27001 Zertifizierung)
- Versicherung (tiefere Prämien)
- Lieferanten/Partner
- Auf Kundenwunsch/Druck

Aufgabenstellung

Ziel muss ein für das jeweilige Unternehmen einheitliches, überschaubares und kosteneffizientes Management für Informationssicherheit sein. Unternehmen, die sich nicht an den Vorgaben eines Standards orientieren, verzichten auf ein international anerkanntes, umfassendes Si-

cherheitssystem, das eine gesamtheitliche Darstellung der Compliance ermöglicht. Das Managementsystem des Standards ISO 27001 folgt dabei dem PDCA-Lebenszyklus (Plan-Do-Check-Act Cycle).

Schritt 1: Informations-Sicherheits-Check (Ist-Aufnahme)

Mit geringem Aufwand wird ein Querschnitt durch die verschiedenen Aspekte der Informations-Sicherheit gemacht. Mit diesem Check erhalten Sie einen groben, aber realistischen Eindruck Ihrer vorhandenen Situation im Bereich der Informations-Sicherheit. Die Analyse erlaubt sehr rasch interessante grafische Auswertungen der erhobenen Daten, die bereits eine zuverlässige Interpretation der Ergebnisse ermöglichen. Die folgenden Bereiche werden untersucht:

- Management Aspekte
- Rechtliche Aspekte
- Organisatorische Aspekte
- Technische Aspekte

Schritt 2: Auswertung Ist-Aufnahme und Delta-Analyse

Der zweite Schritt, nach erfolgter Ist-Aufnahme, ist die Delta-Analyse (Vergleich zwischen Ist- und Soll-Situation). Diese gibt Auskunft darüber, wie gut oder schlecht die aktuell eingesetzten Massnahmen das angestrebte Sicherheitsniveau erreichen. Mit anderen Worten, die Delta-Analyse ermittelt die Differenz zwischen den bereits umgesetzten und den notwendigen Massnahmen (Grundschutz). In einem Workshop werden die Sicherheitsanforderungen (Sicherheitsniveau) erarbeitet. Je nach Art des Unternehmens kann die Sicherheits-Anforderung unterschiedlich ausfallen. Generell gilt, dass 80 % der bekannten Sicherheitsmassnahmen (Grundschutz) ausreichen, um ein Unternehmen angemessen zu schützen. Für spezielle Unternehmenswerte (Systeme oder Programme) wird eine detaillierte Risiko-Analyse (Schritt 3) durchgeführt. Daraus folgend werden entsprechende Sicherheitsmassnahmen definiert und implementiert.

Schritt 3: Risiko-Analyse

Die Risiko-Analyse basiert auf der Ist-Aufnahme und der Delta-Analyse. Dabei geht es darum, die Unternehmenswerte zu identifizieren, um die Risiken und Gefahren explizit richtig einschätzen zu können. Ergänzt wird die Informationsgewinnung durch Interviews. Dabei werden folgende Aspekte untersucht:

- Prozessorientierung (Business-Prozess-Analyse)
- Vorgehensmodell
- Struktur der Risiko-Analyse (Business Impact-Analyse)
- Abdeckung der Risiken durch Massnahmen

Diese Risiko-Analyse dient dem Entwurf eines Umsetzungsplans für ein zukünftiges ISMS. Dabei werden folgende Aspekte untersucht und dokumentiert:

- Festlegung des Umfangs (Scope)
- Erhebung der erkannten Risiken gemäss Scope
- Untersuchung der bestehenden Gegenmassnahmen zur Minimierung erkannter Risiken
- Untersuchung der bestehenden organisatorischen Regelungen

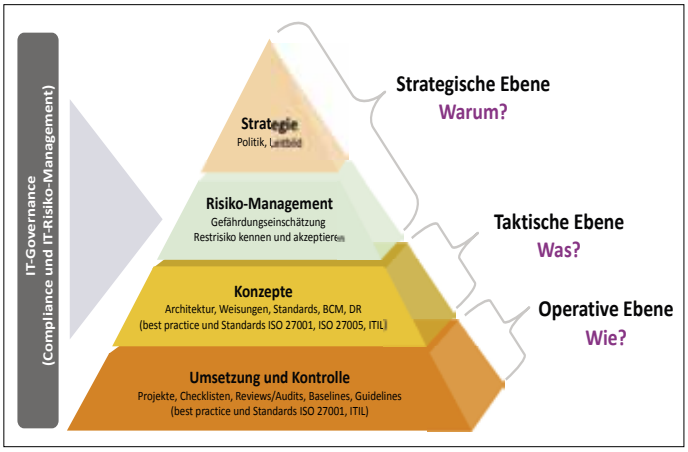

Abbildung 2: Der ISMS-Prozess ist ein Bestandteil der IT-Governance-Pyramide.

Dabei sollte sich der Informations-Sicherheits-Check an den Standard ISO 27001 anlehnen.

Schritt 4: Planung und Umsetzung der Sicherheitsmassnahmen

Ein weiterer Schritt ist die Planung und die Priorisierung der notwendigen Massnahmen zur Erreichung des definierten Sicherheitsniveaus. Danach erfolgt die konkrete Umsetzung dieser Massnahmen. Wir unterscheiden hier zwischen Sofortmassnahmen und längerfristigen Massnahmen.

Schritt 5: Aufbau ISMS

Die IT-Systeme sind entsprechend der IT-Unterstützung für die Geschäftsprozesse einem ständigen Wandel unterworfen, wodurch sich auch die Risiken permanent verändern. Dieser fortlaufenden Veränderung kann nur mit einem Managementprozess begegnet werden. Mittel- und langfristig wird daher die Entwicklung und Einführung eines Managementsystems für Informationssicherheit (ISMS) empfohlen. Die folgenden Schritte sind zwingend für den Aufbau eines ISMS notwendig:

- Festlegung des Umfangs (Scope)
- Festlegung der Sicherheitsstrategie und der Sicherheitsweisung
- Definition der Risikoidentifikation und der Gefahrenanalyse
- Evaluation eines ISMS-Tools für die Dokumentation, Umsetzung und Überprüfung
- Start der Business-Impact-Analyse
- Aufnahme der Werte mit Hilfe einer Infrastruktur-Analyse (Inventar)
- Die Risiken identifizieren und bewerten
- Schreiben von Weisungen, Richtlinien, Prozeduren, Guidelines usw.
- Umsetzung der Weisungen und Prozeduren mit entsprechenden Sicherheitsmassnahmen
- Mitarbeiter entsprechend schulen (Awareness-Kampagne)
- Regelmässige Überprüfung der Effektivität und Wirksamkeit der Sicherheits-Massnahmen (Audit)

Der international anerkannte Standard ISO 27001

Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informations-Sicherheits-Managementsystems (ISMS) unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
Unternehmen, die 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.

Ist eine Zertifizierung nach ISO 27001 sinnvoll?

Ja – eine Zertifizierung bietet die Möglichkeit der Vergleichbarkeit. Mit einer Zertifizierung können Sie sicherstellen, dass Partner- und Zulieferunternehmen 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 Ihnen dabei in Zukunft 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 Informations-Sicherheits-Managements (ISMS) nach ISO 27001 ist das sogenannte Risiko-Management, das auf der systematischen Erkennung von Risiken anhand von Risikoanalysen und Risikobewertungen basiert. Auf der einen Seite ermöglicht nur ein funktionierendes Risiko-Management den Einsatz stets angemessener (d.h. auch wirtschaftlich vertretbarer) Informations-Sicherheits-Massnahmen. Auf der anderen Seite besteht für jede Organisation die Herausforderung der Integration des Informations-Risiko-Managements 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 Informations-Sicherheits-Management-Systems (ISMS) nach dem internationalen Standard ISO 27001.

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

- Einführung und Aufrechterhaltung eines dokumentierten Informations-Sicherheits-Managements-Systems (ISMS)
- Definition einer Informationssicherheitspolitik
- Durchführen einer systematischen Risikoanalyse und Identifikation sowie die Überwachung von Risikobereichen
- Festlegung und Umsetzung geeigneter Sicherheitsziele und Massnahmen

Ein ISO 27001 Zertifikat bzw. eine Anerkennung kann ausschliesslich durch akkreditierte Zertifizierungsinstitutionen (SQS in der Schweiz) vergeben werden, die international anerkannt sind. Das Zertifikat ist drei Jahre gültig. Während der Gültigkeitsdauer werden zwischenjährliche Überprüfungen (Audits) durchgeführt.

Aufwand und Nutzen eines ISMS

Der interne und externe Aufwand für den Aufbau und Betrieb eines ISMS sind 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:

- Schutz der eigenen Person und der Firma vor Haftungsansprüchen
- System zur Einhaltung von Compliance-Anforderungen
- Erhaltung der Geschäftskontinuität (Business Continuity Management)
- Wettbewerbsvorteile durch verfügbare, vertrauliche und integre Unternehmensabläufe
- Schaffung einer Basis zur Überprüfung der Wirtschaftlichkeit von Sicherheitsinvestitionen
- Hohe Risikotransparenz
- Bewusster Umgang mit Risiken, Reduktion des Risikopotenzials
- Zunehmende Sensibilisierung der Mitarbeiter für eine ganzheitliche Betrachtung ihrer Sicherheitsstrategie
- Sicherstellung der gesetzlichen und vertraglichen Grundlagen (Outsourcing usw.)
- Koordinierte Sicherheitsmassnahmen, weniger Überschneidungen, weniger Lücken
- Wirksamkeit der «Sicherheit» optimieren. Technische Massnahmen alleine reichen nicht aus, auch Prozesse werden betrachtet
- Finanzielle Vorteile, kleinere Fehlerkosten, weniger Ertragsausfälle
- Erhöhung des Vertrauens von Kunden, Geschäftspartnern und Lieferanten durch gelebte Sicherheit
- Zertifizierung: kommunizierbare und belegbare Informationssicherheit mit internationaler Anerkennung als zusätzliches Qualitätsgütesiegel, Sicherheit schafft Vertrauen. Wird ein Wettbewerbsfaktor
- Möglichkeit, sich mit Unternehmen im selben Bereich zu messen (Benchmarking)

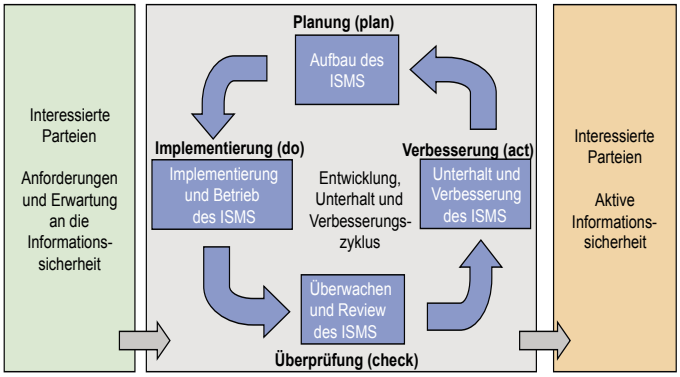

Abbildung 3: Auf ISMS-Prozesse angewendetes PDCA-Modell (Plan-Do-Check-Act).

Fazit

Der ISO 27001 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 KMU ein wichtiges Kriterium. 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 – z. B. ISO 9001 Qualitätsmanagement und ISO 20000 ITIL – werden sinnvoll ergänzt und können integriert werden. Es ist zu erwarten, dass sich dieser Standard schnell verbreitet und zu einem Qualitätslabel für eine risikobewusste Unternehmensführung wird. ■