Informationssicherheit nach KISS

© depositphotos, Rawpixel

Raubt Ihnen Informationssicherheit den Schlaf? Mit der Implementierung eines Informations-Sicherheits-Management-Systems (ISMS) nach ISO 27001 ist ein wesentlicher Schritt in Richtung eines kontrollierten Umgangs mit Informationen im ganzen Unternehmen getan, nicht nur bei der IT.

Almut Eger und Walter Rüegg

Die Erfindung des mechanischen Webstuhls im 18. Jahrhundert gehört zur ersten industriellen Revolution. Die Welt wurde auf den Kopf gestellt durch die Elektrizität und Mechanisierung (z.B. Fliessbandarbeit), welche die zweite industrielle Revolution einläutete. Mit dem Einsatz von Robotern im Produktionsumfeld zu Beginn der 70er-Jahre begann die dritte Revolution. Was bringt nun die Industrie 4.0 und vor allem in welchen Bereichen? Welche Auswirkungen haben aktuelle Anwendungen wie Social Media oder Apps? Welche Informationswerte sind wichtige Unternehmenswerte?

Streben nach Vernetzung

Diese Entwicklung hat offensichtlich noch lange nicht den Höhepunkt erreicht, denn die Technologie verändert sich rasant und spezifische Trends in einzelnen Industrien, regulatorische Massnahmen und noch nicht veröffentlichte Bedrohungen aus dem Darknet tauchen immer wieder als aktuelle Themen auf. Was kommt als Nächstes? Auf was muss sich ein KMU oder ein grösseres Unternehmen und dessen Mitarbeiter noch einstellen? Wo werden inskünftig Regulatorien noch stärker greifen, wo reagieren die Unternehmen, wo können sie überhaupt noch agieren? Wie bringt man Bekanntes und Unbekanntes in Einklang mit dem Thema Informationssicherheit?

Integriertes Managementsystem

Die Autoren sind überzeugt, dass ein Gesamtsystem, das sich stetig mit den Veränderungen und Ereignissen auseinandersetzt und mit geeigneten Massnahmen sich an die neuen Herausforderungen anpasst, das Überleben der Unternehmung sichert. Das Zusammenwirken der ISO-Managementsysteme ist mehr als die Summe der einzelnen Normen. Die Einführung der Informationssicherheit gilt es in Abstimmung des vorhandenen Managementsystems zu planen, umzusetzen, zu implementieren und zu überprüfen.

Es ist sowohl für grössere wie kleinere Unternehmen höchste Zeit, die eigene Informationssicherheit zu überprüfen, aber ohne das Rad «neu zu erfinden». Es ge-

nügt, diese Sicherheitsanforderungen in Anwendung von bereits erprobten Mechanismen und in bestehenden Strukturen zu implementieren. So kann das Unternehmen validiert und die Resilienz gesteigert werden, und der Weg zu einer allfälligen Zertifizierung wäre auch nicht mehr weit.

Fünf Faktoren einer optimal gelebten Informationssicherheit

Erstens – Sicherheit unter der Kosten- und Effizienz-Lupe: Dass ein Schutz von Leistungen und Informationswerten nicht ohne Aufwand zu haben ist, leuchtet ein. Aber Zusatzkosten sollten dennoch nicht entstehen – ausser sie sind auch ein Effizienzgewinn für die geschäftsrelevanten Leistungen: zum Beispiel der Abbau und die Vermeidung von Redundanzen, die Erhöhung der Transparenz zu sicherheitsrelevanten Faktoren in der Organisation oder die Optimierung der Aufgaben, Kompetenzen und Verantwortungen (AKV) zur optimal gelebten Sicherheitskultur intern und in Zusammenarbeit mit Partnern (für mehr Informationen dazu siehe Artikel Sicherheitsforum 1/16, Seiten 28–32).

Zweitens – Einsatz von Tools zur Wahrung der Informationssicherheit: Ob mit oder ohne Tool, wichtig ist der Überblick über die eigene aktuelle Situation:

- Welche Informationen, Daten, spezifisches Wissen usw. der eigenen Organisation sind hoch relevant und deshalb schützenswert, aus Sicht Persönlichkeitsschutz (siehe Datenschutzgesetze), Unternehmenswerte (siehe Geheimhaltungsverpflichtungen), Ausfallsicherheit (z.B. kritische Infrastruktur)?
- Wie werden sie geschützt, wer ist damit beauftragt, wie wird das kontrolliert?
- Bestehen spezifische Abhängigkeiten, z.B. mit Partnern, Stakeholdern und Regulatoren?
- Diese und weitere Fragen sollen die Entscheidung leiten, mit welchem Aufwand die Wahrung der Informationssicherheit aufrechterhalten werden kann. Das Prinzip KISS «Keep it small and simple» kann damit erreicht werden.

Drittens – Überprüfung der Informationssicherheit intern/extern: Das Überprüfen, ob die Informationssicherheit in der eigenen Organisation an richtiger Stelle und mit dem richtigen Aufwand gewährleistet ist, ist eine ständige Managementaufgabe. Die grösste Herausforderung dabei ist die Vernetzung der Informationen: einerseits im positiven Sinn, zum Beispiel zur Steigerung der Leistungsfähigkeit und Geschwindigkeit (z.B. Internet of Things IoT), andererseits auch im negativen Sinn, weil durch die Vernetzung die Übersicht und Transparenz zu nötigen Schutzmechanismen enorm aufwändig wird. Ohne ein effizient aufgebautes Managementsystem (PDCA-Zyklus mit Sicherstellung kontinuierlicher Verbesserung, siehe auch Beitrag in Sicherheitsforum 4/16, Seiten 34–37) und mindestens punktueller Unterstützung durch Tools (z.B. vom Excel-Sheet bis zu umfangreicheren Softwarelösungen für Sicherheitsmanagement, Prozessmanagement, Continuity Management) ist das heute nicht mehr möglich.

Viertens – Informationssicherheit im Benchmark: Es gibt mehrere Raster, nach denen man sich richten kann. Ein gutes, generisches ist die Norm ISO 27001 mit ihren Folgeprodukten zu Cloud Services (ISO 27017), Personally Identifiable Information (ISO 27018), Erkennen der Resilienzanforderungen (ISO 27031) usw. Nach langjähriger Arbeit mit diesen Vorgaben können die Autoren bestätigen, dass damit die unternehmenseigenen Spezifika bestens strukturiert bearbeitet werden können (d.h. die Norm «passt sich der Unternehmung an», nicht umgekehrt) und gleichzeitig ein aussagekräftiger Benchmark gegeben ist, denn wer eine Zertifizierung nach ISO 270xx nachweisen kann, hat sich den relevanten Themen zur Informationssicherheit gestellt.

Fünftens – Leistungsfähigkeit des ISMS: Die Erfahrung im Umgang mit Informationssicherheit zeigt klar auf, dass optimale Sicherheit nur durch die Brille des integrierten Managements erreicht werden kann. Und dass damit als schöner

© depositphotos, photousvp77

ISO-NORM GIBT DIE STRUKTUR ZUR PLANUNG

Eine bewährte Orientierungshilfe, um die Anforderungen im Bereich Informationssicherheit festzulegen, ist die internationale Norm ISO/IEC 27001: Anforderungen für Aufbau, Implementierung, Wartung sowie laufende Verbesserung eines Informations-Sicherheits-Management-Systems (ISMS). Die Informationssicherheit bezeichnet die folgenden Schutzziele: Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit, Authentizität, Verantwortlichkeit und Verlässlichkeit.

Die Norm ist eine ganzheitliche Betrachtung des integrierten Managements bei der Unternehmung. Ein Zertifikat bietet der Unternehmung die Möglichkeit, die Informationssicherheit gegenüber Behörden, Wirtschaftsprüfern, Partnern und Kunden nachzuweisen.

DATENSCHUTZ

Sich verändernde Sicherheitsbedürfnisse beziehungsweise Anforderungen bezüglich Personendaten machten die Anpassung der Datenschutzvorgaben nötig: Online Einkaufen war vor Jahren nur ein modischer Trend, heute ist es aber aus dem Alltag vieler Menschen nicht mehr wegzudenken. Das neue Outfit kommt in zwei, die dazu passenden Schuhe in drei Tagen. Perfekt. Ist diesen Personen beim Onlineshopping bewusst, was mit ihren Personendaten geschieht, ob diese verschlüsselt sind oder sogar auf unterschiedlichen Systemen liegen? Sind diese Daten in einem regionalen Rechenzentrum sicher aufbewahrt oder werden diese in der Cloud und noch dazu ausserhalb der Schweiz gehostet? Die Frage nach dem Vertrauen stellt sich: Geht die Gesellschaft mit solchen Risiken heute anders um oder ist das Vertrauen in den Lieferanten, Hoster oder Deliveryservice schlicht grenzenlos? Im Zusatz ISO 27018 wird diesem Aspekt Rechnung getragen, damit die bestehenden Gesetze nicht verletzt werden.

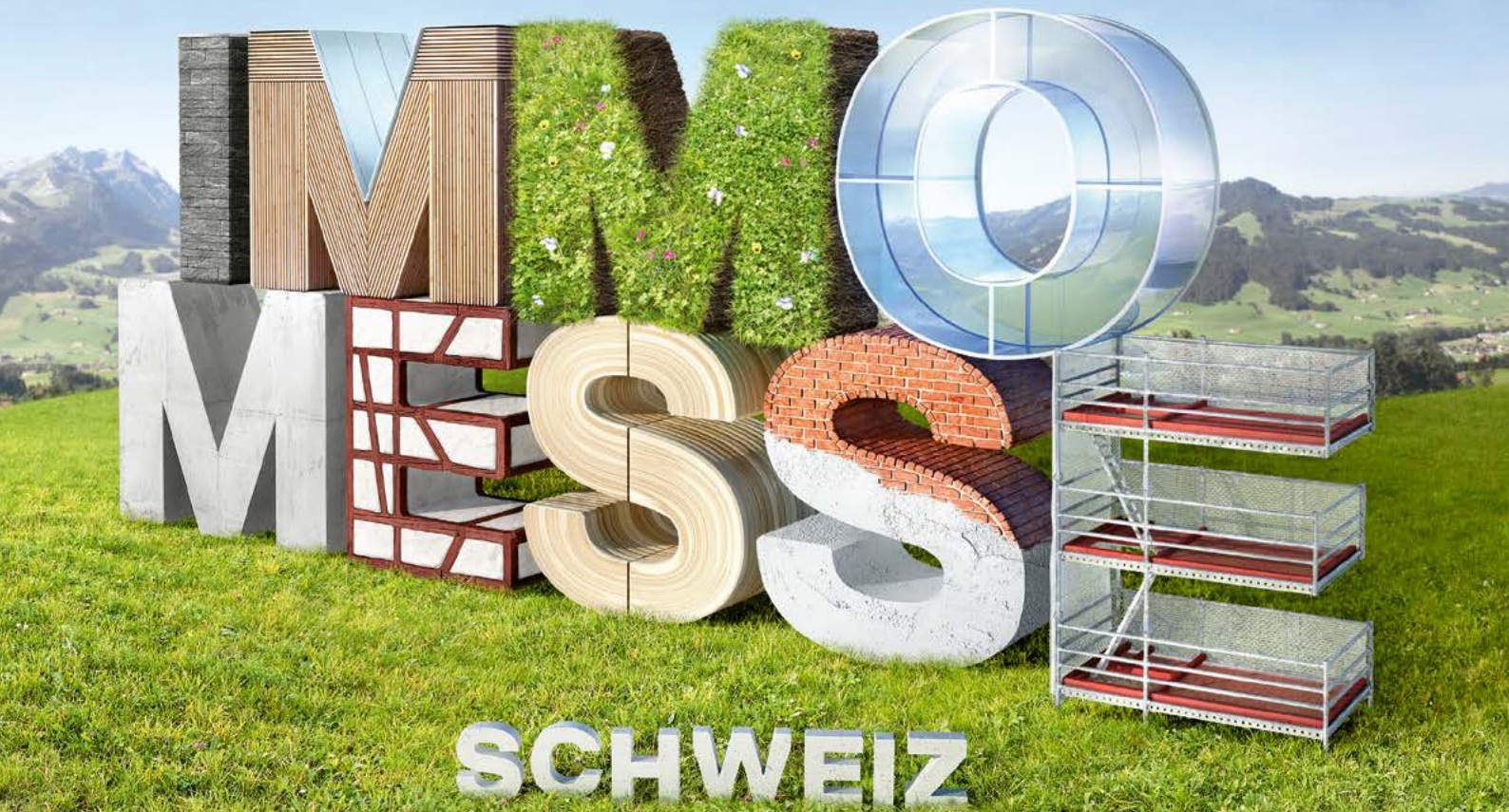
Eine auf europäischer Ebene erfolgte Änderung tritt am 25. Mai 2018 in Kraft. Für alle Schweizer Unternehmen, die grenzübergreifenden Austausch von personenbezogenen Informationen haben, hat das einschneidende Folgen!

IMMO MESSE SCHWEIZ

Immobilien, Bau und Renovation

St.Gallen, 16.–18.03.2018

Eintritt frei · immomesse.ch



Patronat

svit OSTSCHWEIZ

HEV Kanton St.Gallen

Olma Messen St.Gallen

TKF

EINHEITLICHES SYSTEM FÜR IT-SECURITY UND SICHERHEIT VON DATEN UND WISSEN

Das Informations-Sicherheits-Management-System (ISMS) ist als zusammenhängende Summe von Methoden und Regeln zu sehen. Ein solches System erlaubt eine dauerhafte Steuerung und Verbesserung der Informationssicherheit in einer Unternehmung. Dabei ist das primäre Ziel, sämtliche Risiken in Bezug auf die zu verarbeitenden Informationen nicht nur zu kennen, sondern diese auch zielgerichtet zu steuern.
Die Mehrwerte entstehen unter anderem in der Erfüllung regulativer und vertraglicher Anforderungen, des Nachweises dieser Informationssicherheit gegenüber Dritten oder der Verbesserung der Wirtschaftlichkeit durch eine risikoorientierte Massnahmenplanung.
Der Vorteil eines ISMS ist auch, dass es nicht nur die IT-Abteilung betrifft, sondern die ganze Unternehmung. Alle Bereiche müssen sich mit dem Thema auseinandersetzen, nur so ist schliesslich eine durchgängige Implementierung möglich, die von allen Mitarbeitenden gelebt wird.

Zusatzgewinn auch die gewünschte «Schlankheit» erzielt werden kann:

- Rollen, Aufgaben und Kompetenzen sind so implementiert, dass sie aus dem Gesamtkontext ihrer Leistungsverantwortung auch möglichst lückenlose Informationssicherheit hervorbringen (in Bezug auf Umgang mit Daten, Informationen, Assets).
- Controlling und Nachweise zur Einhaltung der Informationssicherheit sind implementiert via Einsatz von Tools, die auch die Prozessleistungen zu optimaler Wertschöpfung unterstützen (z.B. IMS via Prozessmanagement-Tool). So entsteht eine sich gegenseitig befruchtende Steuerung, mit der man die eingangs skizzierte schnelle Entwicklung im Griff behalten kann, auch wenn immer neue Anforderungen an die Sicherheit von Informationen und Wissen gestellt werden.

Praxisbeispiel SKI

Im Kontext der Sicherheit gilt es vor allem die Unternehmen der kritischen Infrastrukturen zu berücksichtigen. In der Schweiz werden, vereinfacht gesagt, drei Sektoren differenziert: Energie, Gesundheit und Verkehr (inkl. Banken). Eine Unterteilung in Teilsektoren wird durch das Bundesamt für Bevölkerungsschutz (BABS) beschrieben (vgl. www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html). Aus denselben Teilsektoren wurden die kritischen Einzelobjekte oder Infrastrukturelemente identifiziert (z.B. Stromversorgung mit Hochspannungsleitung). Auf nationaler Ebene wurden zehn kritische Infrastruktursektoren identifiziert. Basierend auf der SKI-Grundstrategie des BABS wurden von den 10 Sektoren 31 Teilsektoren herausgeschält. 28 Teilsektoren gelten als kritisch. Nachfolgendes Beispiel aus dem Finanzbereich beschreibt eine der kritischen Infrastrukturen.

Der Teilsektor Banken umfasst die Banken selber, Finanzdienstleister, die Börse und Provider der Finanzmarktinfrastrukturen. Bargeldversorgung oder der bargeldlose Zahlungsverkehr sind ein Teil der Basis für das Funktionieren der Wirtschaftskreisläufe. Mit einer Wertschöpfung von mehr als zehn Prozent am Bruttoinlandprodukt kommt diesem Teilsektor eine zentrale wirtschaftliche Bedeutung zu. Für den Schutz kritischer Infrastrukturen der Banken sind somit diejenigen Prozesse von Bedeutung, die sich unter anderem mit der Aufrechterhaltung der Finanzkreisläufe und Zahlungsabwicklung beschäftigen.

GAP-Analyse für ISO 27001 bei Telekommunikationsfirma

Ein Schweizer Unternehmen aus dem Sektor Telekommunikations-Dienstleistungen hatte bereits verschiedene Systeme wie ISO 9001 und ISO 20001 vor Jahren erfolgreich implementiert und zertifiziert. In Anbetracht des sich verändernden Umfeldes und der unter anderem kundenseitig stetig steigenden Anforderungen in Bezug auf Nachweis der Datensicherheit beschloss das Unternehmen, ein Informations-Sicherheits-Management-Systems (ISMS) einzuführen und nach ISO 27001 ff. zu zertifizieren.

Mit den beiden eingeführten Normen verfügte die Unternehmung bereits über ein stabiles Managementsystem, die Anforderungen von ISO 27001 konnten im PDCA-Zyklus ergänzt werden. Die durchgeführte GAP-Analyse zeigte auf, auf welche Vorgaben und Nachweise sie zur erfolgreichen Implementierung der Anforderungen nach ISO 27001 fokussieren musste, womit aber gleichzeitig eine Steigerung der Professionalität der Nachweise erreicht werden konnte. Zum nächsten Zertifizierungstermin, nur ein Jahr später, waren alle Vorgaben erfüllt und es konnte ein gelebtes ISMS aufgezeigt werden. Die Zertifizierung neu im Triple nach ISO 9001, ISO 20001 und ISO 27001 wurde erfolgreich bestanden.

Fazit

Mit der Implementierung eines ISMS nach ISO 27001 ist ein wesentlicher Schritt in die richtige Richtung getan: ein kontrollierter Umgang mit Informationen im ganzen Unternehmen. Die integrierte Sicherheit zu Daten, Dokumenten, Informationen und Wissen generell wird dann erreicht, wenn Informationssicherheit in allen Leistungseinheiten einer Organisation implementiert ist: IT-Prozesse, Kunden- und Partnerkontakte, Kommunikationsmittel und Verhalten bei Kommunikation / Ablage von erhaltenen Informationen, effizientes Controlling und entsprechender Nachweis, dass Informationssicherheit gemäss der Vorgaben von Kunden, Partnern und Regulatoren eingehalten wird. Deshalb wird empfohlen, auch ein ISMS im Sinne eines integrierten Managementsystems zu leben. ■


ALMUT EGER
Senior Consultant und Trainerin für Notfall-/Krisenmanagement, BCM und ISMS bei 4m2s – 4 Management 2 Security GmbH, Zürich und Frankfurt, Auditorin für TÜV Rheinland Cert.

WALTER RÜEGG
Senior Consultant und Trainer für NKM, BCM und ISMS bei 4m2s – 4 Management 2 Security GmbH, Zürich und Frankfurt. Lead Auditor ISO 27001 Informationssicherheit.