Eine unternehmerische Dimension

Wer die Herausforderung der Datenflut pragmatisch und effizient meistert, hat definitiv einen Wettbewerbsvorteil gegenüber Mitbewerbern ohne funktionierendes Informations-Sicherheits-Management-System.

Almut Eger und Walter Rüegg

Informationen sind seit Längerem der essentielle Rohstoff für erfolgreiche Unternehmen. Durch die breite Verfügbarkeit von Daten aus den verschiedensten Kanälen (IoT) wird die Herausforderung immer grösser, aus diesen Informationen nutzbringende Erkenntnisse zu gewinnen. Auch der Komplexitätsgrad der Verwaltung der Daten steigt, damit die Nachvollziehbarkeit der Analysen und Entscheidungen gewahrt bleibt. Nicht nur das, sondern auch die revisionssichere und klassifizierungsgerechte Nutzung und Zuordnung der Daten ist zu organisieren. Wer diese Herausforderung pragmatisch und effizient meistert, hat definitiv einen Wettbewerbsvorteil gegenüber Mitbewerbern ohne funktionierendes Informations-Sicherheits-Management-System (ISMS).

Big Data und Unternehmenssicherheit

Sicherheit ist bei den heutigen riesigen Datenmengen ein ganz wesentlicher Aspekt. Das kam auch zur Sprache an der ersten Schweizer Konferenz «Digitale Schweiz» in Biel vom vergangenen November, unter anderem mit folgender These der Workshops: «Ohne nachhaltige Sicherheit und Vertrauen gibt es keine digitale Transformation.»

Das Sammeln und Auswerten von Massendaten hat seinen Höhepunkt noch lange nicht erreicht, die Fragen stellen sich: Wie kann ein Unternehmen die zunehmend wichtige Vernetzung von Informationen zu einem unternehmerischen Mehrwert gestalten? Und wie kann die Datenqualität sichergestellt werden?

Der Mehrwert von Vernetzung entsteht unter anderem dadurch, dass regulative und vertragliche Anforderungen erfüllt werden. Die Informationssicherheit kann so nicht nur intern, sondern auch gegenüber Dritten nachgewiesen werden. Durch einen risikobasierten Ansatz bei der Planung der Massnahmen kann auch die Wirtschaftlichkeit verbessert werden.

ISMS gute Grundlage für DSGV

Die richtige Information zur richtigen Zeit am richtigen Ort mit richtiger Analyse von richtigen Leuten, korreliert mit Big Data, ist ein wesentlicher Erfolgsfaktor und verlangt eine stringente, strukturierte und geordnete Organisation der Informationen mit gesteuertem Zugriff nach Klassifizierung. Im Mai wird das DSGVO/GDPR (Datenschutzgrundverordnung/General Data Protection Regulation) scharf gestellt, die zweijährige Übergangsfrist ist dann abgelaufen. Dann sind PIIs (Personally Identifiable Information) von EU-Bürgern nachweisbar zu managen: Es muss jederzeit aufgezeigt werden können, dass Daten, die auf Personen rückverfolgbar sind, nach den Gesetzen behandelt werden. Die EU ist für die Schweiz der grösste Markt, d.h., praktisch alle Unternehmen in der Schweiz sehen sich mit dieser Thematik konfrontiert. Die Unternehmen, die bereits ein ISMS eingeführt haben, sind nicht etwa aus dem Schneider, sondern haben eine gute Grundlage, um durch Ergänzungen im ISMS die Bedingungen für GDPR ohne grossen Aufwand realisieren zu können.

Mehrwerte mit ISMS

«Ein ISMS gemäss ISO/IEC 27001 schafft hohe Informationssicherheit mit angemessenem Aufwand und ist eine in sich zusammenhängende Sammlung von Methoden, Vorgaben und Regeln innerhalb eines Unternehmens zur dauerhaften Steuerung und Verbesserung der Informationssicherheit.»

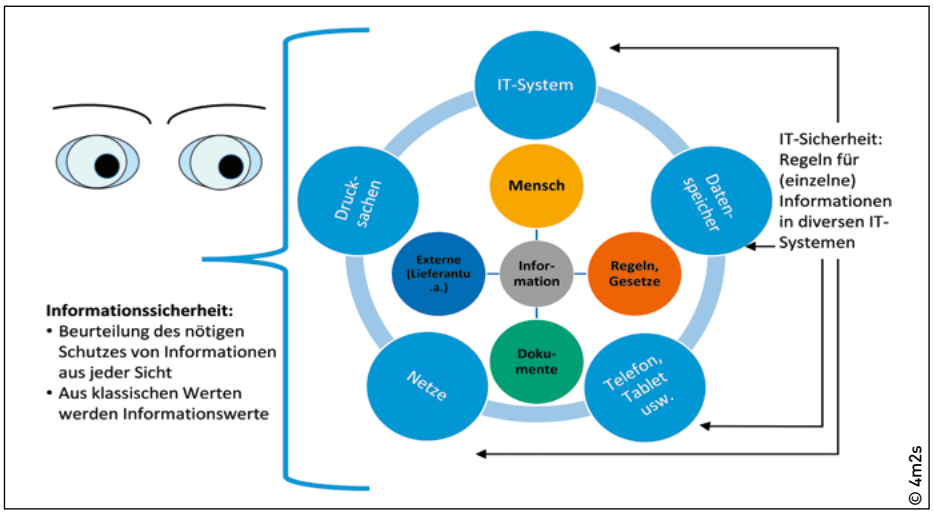
Der Aufbau eines ISMS garantiert zahlreiche Mehrwerte:

- Erfüllung regulativer und vertraglicher Anforderungen (Compliance)
- Nachweisbarkeit der Informationssicherheit gegenüber Dritten
- Identifikation, Bewertung und Behandlung der bestehenden Risiken
- Verbesserung der Wirtschaftlichkeit durch risikoorientierte Massnahmenplanung
- Schwachstellen aufdecken und Zusatzrisiken minimieren
- Steigerung der Widerstandsfähigkeit gegenüber Cyberangriffen

Regeln festgelegt mit ISMS

Ein funktionierendes und wirksames ISMS, das in der Unternehmung in Organisation und Kultur verankert ist, bildet auch die Grundlage für ein effektives Wissensmanagement. Wissen ist bei den Mitarbeitenden beheimatet und steht somit oft mit persönlichen Daten in Verbindung. Was muss dann genau beachtet werden? Wer legt diese Regeln fest, setzt sie um und sorgt für die Anwendung? Woher kommt die Gewissheit, dass die Regeln eingehalten wurden? Die Regeln, wie Informationen klassiert werden und wie mit heiklen Informationen umzugehen ist, sind im Idealfall Teil eines integralen ISMS. Und diese Regeln müssen so ausgestaltet sein, dass sie den neuen Datenschutzrichtlinien nach GDPR genügen. Wissensmanagement ist somit ebenfalls Teil eines integralen ISMS und einer strengen Beurteilung nach Datenschutzrichtlinien.

Heute muss jede Unternehmung jederzeit bereit sein und nachweisen können, wie Wissensmanagement und Zugriff auf Dokumente definiert, geregelt und verfügbar ist. Und wie Wissen, abgeleitet aus der Strategie, weiterentwi-



Integrierter Ansatz des ISMS, nach ISO 27001.

ckelt wird. Zum Beispiel wenn die Finanzmarktaufsicht Finma vor der Tür steht und in einem Audit testen will, ob die Informationen nach den Finma-Regeln behandelt werden. Nur mit einem funktionierenden ISMS können die Nachweise gesichert erbracht werden: wer wann Zugang zu Informationen hat, mit physischem wie auch elektronischem Zugriff.

Vierfache Herausforderung

Ein korrekter Umgang mit Informationen ist die Kernbotschaft von Informationssicherheit. Mit zunehmender Vernetzung von Informationen und Erkenntnissen und mit zunehmender Aufforderung, dies auch zu tun, wird Informationssicherheit vermehrt vielschichtig (denn ein Unternehmen, das die Informationen zu Kunden-/Produktverhalten nicht immer rascher und raffinierter analysiert, hat es immer schwerer auf dem Markt). Dabei stehen folgende vier Herausforderungen im Vordergrund:

- die technische Bewältigung von Big Data und Internet of Things (IoT)
- die methodische Gestaltung von Wissensmanagement, d.h. korrektes «Lagern / Verwalten» und «Anwenden» der Daten, proaktives Vorausdenken zu benötigten Informationen
- die regulatorischen Vorgaben: Der Datenschutz stellt neue Anforderungen ab Mai 2018
- die prozessuale Sichtweise: mit ISMS kann ein Unternehmen nachweisen, dass korrektes Handeln von Seiten der Unternehmung eingefordert wird und dass Fehlverhalten rechtzeitig erkannt wird, bevor Schaden entsteht

Informationssicherheit bekommt somit eine neue unternehmenskritische Dimension.

Praxisbeispiel ICT-Dienstleistungen

Bei Spie ICS, einem Anbieter von ICT-Dienstleistungen für Behörden, Banken etc. in der Schweiz, wurde in den vergangenen eineinhalb Jahren ein wirksames ISMS eingeführt. Das Vorgehen ist beispielhaft und wurde erfolgreich mit der Zertifizierung nach ISO 27001 eingeführt. Durch die Geschäftsleitung initiiert, als internes Projekt installiert und nach den Regeln des Projektmanagements umgesetzt. Im Vordergrund stand nicht die Erfüllung der Norm, sondern der Nutzen des Managementsystems zur geordneten Behandlung der Informationen. Ein wesentlicher Bestandteil ist das Bewusstsein jedes Mitarbeitenden, dass Informationssicherheit auch dort beginnt, wo USB-Sticks nicht frei herumliegen, Besucher in den Officeräumen immer begleitet werden, dass physische Zonen besondere Zutrittsberechtigungen verlangen, erstellte Dokumente klassifiziert werden oder vertrauliche Mails immer verschlüsselt verschickt werden. Aus Erfahrung ist der Mensch der grösste Risikofaktor, deshalb kommt die Einführung des ISMS einem Kulturwandel gleich. Das ISMS verlangt die Messung der Wirksamkeit des ISMS. Das kann zum Beispiel anhand der gemeldeten IS-Vorfälle beurteilt werden: Anzahl und Art der Incidents, umgesetzte Massnahmen etc. Bei Spie ICS ist durch einen Klick auf der Intranet-Homepage eine Meldung ganz einfach ohne Suche und Spezialwissen absetzbar. Je kleiner die Hürde zur Meldung von Abweichungen ist und je umgehender die Behandlung vonstatten geht, umso schneller wirkt das ISMS und verbessert sich stetig. Beim genannten Unternehmen klassisch erfüllt.

Fazit

Mit der Einführung des Informations-Sicherheits-Management-Systems wird der korrekte, geordnete und geführte Umgang mit Informationen im ganzen Unternehmen über alle Stufen und Prozesse sichergestellt. Das beginnt bei der Klassifizierung der Informationen, einem der wesentlichen Schritte am Ursprung der Information – und geht über zu Zugriffsrechten, korrekter Datenhaltung und Umgang/Verwendung von Daten und Informationen.

Es gibt klare Kriterien, wonach ein Dokument als vertraulich oder streng vertraulich klassifiziert wird; und welche Vorgaben daraus zur Handhabung der Dokumente entstehen. So wird auch sichergestellt, dass nur diejenigen Zugriff erhalten, die dafür autorisiert sind. Der Nachweis wird erbracht, dass keine unerlaubten Zugriffe stattgefunden haben. Ausserdem wird überprüft, dass diese Kriterien auf alle Medien wie Papier, USB, SSD, Social Media etc. angewendet werden. Und es gibt Hinweise, was bei Abweichungen zu tun ist.

Mit dem ISMS ist die Grundlage gegeben, diese Mechanismen zu definieren, umzusetzen, in der Organisation zu implementieren und in der Unternehmenskultur zu verinnerlichen. ■


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.