Informations- und Kommunikationstechnik

IKT-Sicherheit: Weit mehr als nur eine technische Herausforderung

Informationssicherheit ist nicht nur eine gesetzliche Pflicht, sondern ein wirtschaftliches Gebot. Vorfälle beeinträchtigen nicht nur die Reputation und das Vertrauen von Marken (wie Google, Swisscom u.v.m), sondern auch deren Wert. Für Unternehmen und Behörden sind Informationen von essenzieller Relevanz und die Basis jeglichen Handelns. Zum überwiegenden Teil werden heute Informationen mit Informations- und Kommunikationstechnik (IKT) bearbeitet.

Nicole Heynen

Ohne IT sind heutzutage Geschäftsprozesse kaum vorstellbar. Die Informationssicherheit befasst sich mit dem Schutz der Informationen in diesen Prozessen. Dabei sollte nicht nur der technologische Aspekt betrachtet werden, sondern auch das Analysieren von Organisation, Kultur und Prozessen.

Als Synonyme zur IKT-Sicherheit werden die Begriffe «Informatiksicherheit» und «Datensicherheit» benutzt. Dies ist die Zusammenfassung aller technischen, organisatorischen und personellen Massnahmen, um den Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit für die Schutzobjekte (Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte) der Informations- und Kommunikationstechnik zu gewährleisten.

Zielkonflikte

Sicherheit ist eingebettet in den Kontext von Benutzerfreundlichkeit und Kosten. Die Komponenten dieses Dreiecks beeinflussen sich gegenseitig, und das eine geht im Allgemeinen zulasten des anderen. Soll also die Sicherheit maximal sein, so wird meistens die Benutzerfreundlichkeit leiden und/oder die Kosten werden stark steigen. Welche Komponente bei welchen Schutzobjektzielen mehr gewichtet wird, ist immer wieder ein neuer Entscheidungsfindungsprozess.

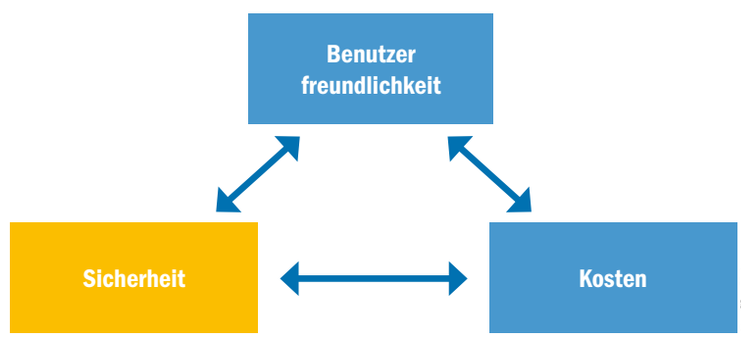
Die Grundlage: Informationssicherheits-Managementsystem (ISMS)

Unter diesem Begriff ist ein umfassendes, ganzheitliches und standardisiertes Managementsystem zu verstehen. Die Norm ISO 27000 beschreibt die Familie der Standards für die Einführung und den Betrieb eines Informationsicherheits-Managementsystems (ISMS).

In den ISO-Standards 27001 und 27002 werden die Grundlagen als Anforderungen und Leitfaden für das Informationssicherheits-Management ausgeführt. Die Norm ISO 27001 «Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen» beschreibt die Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Dabei weist die Norm folgendes Ziel aus:

«Das Informationssicherheits-Managementsystem schützt die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen durch Anwendung eines Risikomanagementprozesses und verleiht dadurch interessierten Parteien das Vertrauen darauf, dass mit Risiken angemessen umgegangen wird.»

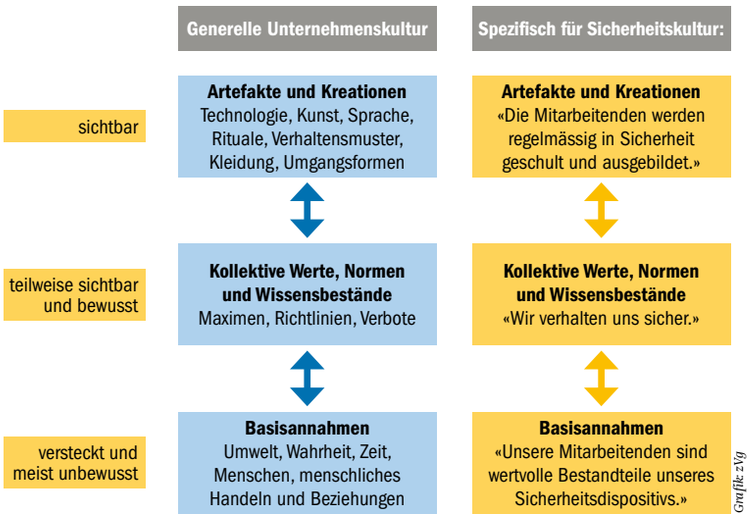
In dieser Norm wird generisch ausgeführt, welche Aufgaben, Zuständigkeiten und Befugnisse die Organisation und die Führung beim Betrieb eines ISMS haben. Es wird darin auf die Planung, die Unterstützung, den Einsatz, die Leistungsauswertung und die Verbesse-



Grafik: zVg

Die Abwägung erfolgt immer von Neuem: Benutzerfreundlichkeit, Kosten und schliesslich auch die Sicherheit definieren das IKT-System.

Nicole Heynen Präsidentin Netzwerk Risikomanagement. (Bild: zVg)



Die drei Ebenen der Unternehmenskultur, erweitert mit sicherheitskulturspezifischen Elementen nach Schein 2010, Schlienger 2007.

rung des ISMS eingegangen. Untenstehend finden sich konkrete Massnahmenziele und Massnahmen, welche die konkreten Bottom-up-Anforderungen an das ISMS darstellen.

Die ISO 27005 ist der dazugehörige Standard, der das Risikomanagement für die Informationssicherheit ausführt. Darin wird der klassische Risikomanagementzyklus um spezifische Elemente erweitert, die für Risikomanagementprozesse wichtig sind. Dieser Zyklus wird am Plan-Do-Check-Act-Kreislauf ausgerichtet, damit ein vollständiges Bild des Risikomanagementsystems durch die Verbindung mit dem Führungsprozess entsteht.

ISMS ist also weit mehr als ein technisches Managementsystem. Jedes ISMS muss der Grösse und den Anforderungen eines Unternehmens angepasst werden. Es regelt u.a. Prozesse und Kompetenzen, trägt zur sicheren Datenaufbewahrung bei und gewährleistet, dass die Compliance-Vorgaben eingehalten werden.

Die Einführung sollte von der Geschäftsleitung erfolgen. Diese muss u.a. die erforderlichen personellen, finanziellen und zeitlichen Mittel zur Verfügung stellen. Weiter sollte die Unternehmensstrategie mit der IT-Strategie abgestimmt sein. Die Führungsrolle ist für den Erfolg entscheidend. Eine Informatiksicherheitskultur muss gelebt werden und sollte ein Teil der Unternehmenskultur sein.

Der Erfolgsfaktor: Informatiksicherheitskultur, integriert in der Unternehmenskultur

Eine grosse Gefahrenquelle im IT-Bereich ist oft der Arbeitnehmer. Gemäss internationalen Studien zur IT-Sicherheit am Arbeitsplatz wird festgestellt, dass nur ca. 50% der Mitarbeitenden sich aktiv mit dem Thema «Informationssicherheit» beschäftigen. Viele verlassen sich darauf, dass der Arbeitgeber für Sicherheit sorgt und ergreifen selbst kaum Vorsichtsmassnahmen. Damit die Awareness gesteigert werden kann, muss die Informatiksicherheitskultur ein integrierter Teil der Unternehmenskultur sein.

Nach Schein[1] besteht die Unternehmenskultur aus drei Ebenen. Auf der untersten Ebene befinden sich die Basisannahmen, welche versteckt und meist unbewusst sind. Darin enthalten sind Aspekte wie Wahrheit, Umwelt, Mensch, Handeln oder (soziale) Beziehungen.

Auf der darüberliegenden Ebene, den öffentlich propagierten kollektiven Normen und Regeln, die teilweise sichtbar und bewusst sind, befinden sich die Maximen, Richtlinien, Grundsätze und Verbote. Ideale, Ziele und Werte sind auf dieser Ebene ebenso zu finden wie Ideologien – sie sind überprüfbar an der Realität.

Zuoberst in der Hierarchie finden sich die sichtbaren Artefakte und Schöpfungen. Darunter fallen u.a. Organisationsstrukturen, Prozesse und beobachtbares Verhalten, Technologie, Sprache, Kleidung und Verhaltensmuster.

Schlienger[2] führt zum Thema «Informationssicherheitskultur» aus, dass ein entsprechendes Konzept folgende Eigenschaften umfassen muss :

1.) *Es deckt Scheins drei Ebenen der Unternehmenskultur ab.*
2.) *Es beeinflusst die Mitarbeitenden bezüglich Umgang mit Informationssicherheit.*
3.) *Es ist nicht als Silo im Unternehmen verankert, sondern integral, besonders in den Bereichen Organisation und Technik.*
4.) *Die Kommunikation basiert auf gegenseitigem Vertrauen, gemeinsamen Verständnis der Wichtigkeit von Informationssicherheitsfragen und dem Vertrauen in die umgesetzten Massnahmen.*

Hieraus werden beispielsweise die Ebenen spezifisch für die Sicherheitskultur abgeleitet:

- Artefakte und Kreationen: Die Mitarbeitenden werden regelmässig in Sicherheit geschult und ausgebildet.
- Kollektive Werte, Normen und Wissensbestände: Wir verhalten uns sicher.
- Basisannahmen: Unsere Mitarbeitenden sind wertvolle Bestandteile unseres Sicherheitsdispositivs.

Schlussfolgerung

Das Zusammenspiel von einem Managementsystem im IKT-Bereich mit einer gelebten Sicherheitskultur ist ein Faktor, welcher hilft, das Unternehmen optimal zu schützen. Die «Corona-Zeit» beispielsweise hat Unternehmungen gezwungen, rasche Entscheide zu treffen, um die Kapazität von Homeoffice zu erhöhen oder überhaupt möglich zu machen. Hier konnten kaum sämtliche Sicherheitsvorschriften in einer ersten Phase eingehalten werden. Umso wichtiger ist es gerade in einer solchen Situation, auf risikobewusste Mitarbeiter zählen zu können.

Lücken in der IKT-Sicherheit werden trotz grossen Bemühungen immer vorhanden sein. Es gilt, diese rasch zu finden und zu beheben. Technische Massnahmen sind zentral und die Unternehmensorganisation muss rasch reagieren. Damit können unerwünschte Auswirkungen minimiert und der Wert des Unternehmens geschützt werden. ■

Dieser Fachartikel erscheint in einer MQ-Serie, die von Expertinnen und Experten des Netzwerks Risikomanagement beigesteuert wird:
www.netzwerk.risikomanagement.ch

1 *Schein, Edgar H. (2010): Organizational culture and leadership. 4th ed. San Francisco: The Jossey-Bass business & management series*
2 *Schlienger, Thomas: Informationssicherheitskultur. Messung, Planung und Steuerung. In: DuD · Datenschutz und Datensicherheit (31), S. 487–491*