Informationssicherheit gewährleisten

ISO 27001 Norm als Hilfsmittel

Immer mehr Geschäftsfelder sind IT-getrieben. Dazu gehören auch die Finanz- und Versicherungswirtschaft. Mehr noch: Bei den Systemen für elektronischen Zahlungsverkehr muss man sogar von «kritischen Infrastrukturen» sprechen. Informationssicherheit zu gewährleisten, ist dort ein Gebot der Stunde. Mit ISO 27001 verfügt man über ein nützliches Hilfsmittel zur Implementierung und für den Betrieb eines ISMS.

Simon Kröni und Roland Brunner

Unsere Arbeitswelt ist stärker denn je von funktionierenden digitalen Systemen abhängig. Prozesse werden digitalisiert und als Workflow (teil-)automatisiert abgewickelt. Eine stetig zunehmende Menge an heiklen Daten wird in die Cloud ausgelagert. Immer mehr Unternehmen sind davon abhängig, dass IT-Systeme reibungslos funktionieren. Neben einer klaren und sinnvollen Strukturierung der Abläufe eines Unternehmens ist das Funktionieren und der sichere Umgang von und mit IT-Lösungen und -Infrastrukturen eine der ausschlaggebenden Bedingungen für effizientes Arbeiten.

Neue Opportunitäten bergen stets auch neue Risiken:

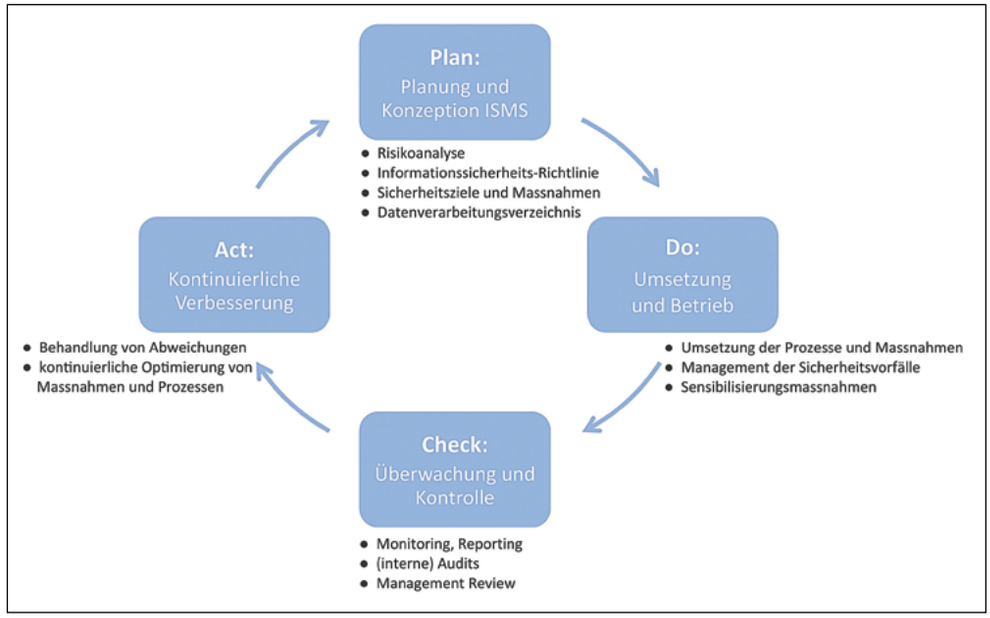
- Cyberkriminalität steigt. Unternehmen sind für Hacker lukrative Angriffsziele. Im Jahr 2017 wurden 40% aller Schweizer KMU Opfer eines Cyberangriffs*.
- Mitarbeitende stellen durch Unwissenheit und fehlende Sensibilisierung ein ernst zu nehmendes Risiko dar:
  > Phishing-Mails werden immer raffinierter dargestellt und sind für Laien kaum als solche identifizierbar.
  > Die Anzahl an notwendigen Passwörtern steigt und nach wie vor wählen viele Mitarbeitende unsichere Passwörter.
- Personenbezogene Daten sind von Gesetzes wegen (Bundesgesetz über den Datenschutz DSG, SR 235.1) geschützt und müssen besonders sicher gespeichert und archiviert werden. Im Schadenfall drohen Bussen und Reputationsschäden.
  > Die europäische Datenschutz-Grundverordnung (DSGVO) erfordert zusätzliche datenschutzfördernde Massnahmen.
  > Branchenverordnungen wie FINMA-Vorschriften, Basel III und EPD (elektronisches Patientendossier), geben allgemeine oder konkrete Vorgaben zum Datenschutz und Datensicherheit.

Um die auftretenden Risiken in der Informationssicherheit und speziell im Datenschutz zu minimieren, bedarf es technischer und organisatorischer Massnahmen. Eine umfassende Hilfestellung bieten die Standards der Normenreihe ISO 2700x, welche sämtliche Bereiche im Unternehmen bezüglich Informationssicherheit abdecken.

ISO 27001/02

Die ISO-Normen 27001/02 wurden erarbeitet, um Anforderungen an die Festlegung, Umsetzung, Pflege und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems zu definieren. Sie unterstützen Unternehmen, sichere Infrastrukturen zu betreiben, die richtigen Massnah-

> ***«Die absolute Sicherheit ist weder in der physischen noch in der digitalen Welt gewährleistet.»***



PDCA Zyklus für ISO 2700x

Simon Kröni ist Projektleiter Managementsysteme und Compliance bei der Neosys AG.

Roland Brunner ist Senior Information Security Consultant und Lead Implementer ISO 27001 bei der WiB Solutions AG.

men bei Vorfällen einzuleiten oder Angestellte konsequent zu sensibilisieren. Nebst der Erfüllung von technischen Anforderungen sind auch viele organisatorische Massnahmen zu treffen. Die ISO-Norm für Informationssicherheit deckt einen wichtigen und grossen Teil der Einhaltung der neuen Europäischen Datenschutz-Grundverordnung ab (insbesondere die Rechte der Personen der DSGVO sind z.B. in ISO 2700x nicht geregelt). Diese ist auch für viele Schweizer Unternehmen mit Geschäftsbeziehungen zur EU unabdingbar. Es ist zudem damit zu rechnen, dass mittelfristig ähnliche Anforderungen auch in der Schweiz in Kraft treten werden. Es lohnt sich also in jedem Fall, sich mit den neuen Anforderungen auseinanderzusetzen.

Unternehmen, die bereits Managementsysteme nach ISO 9001 (Qualität), 14001 (Umwelt), ISO 45001 (Arbeitsschutz) oder ISO 50001 (Energie) betreiben, verfügen bereits über einen Grossteil der nötigen Managementsystemstruktur für die Implementierung eines Informationssicherheitsmanagements. Praktischerweise ist die ISO 27001 nämlich nach derselben High-Level-Struktur wie die genannten ISO-Normen aufgebaut.

Analog zu anderen Managementsystemen ist die Voraussetzung resp. der erste Schritt, die eigenen Prozesse und Abläufe zu kennen und zu analysieren. Welche Daten werden wie gespeichert und bearbeitet? Welche (gesetzlichen) Bestimmungen oder Erwartungen müssen zu welchen Daten eingehalten werden? Ist diese Ausgangslage erst einmal geklärt, ist die Integration des Themas Informationssicherheit in bestehende Managementsysteme und Strukturen mit verhältnismässigem Aufwand möglich. Dafür ist nebst Managementsystemwissen auch fachspezifische Expertise für IT-Systeme nötig. Einmal in einem Managementsystem etabliert, ist sichergestellt, dass das Thema, wie andere Themen auch, die nötige Aufmerksamkeit erhält, laufend überwacht und optimiert wird.

Eine Zertifizierung des Systems kann als Nachweis für Kunden und die Öffentlichkeit Sinn ergeben, ist aber nicht zwingend nötig. Auch ohne Zertifizierung ist die Integration in bestehende Managementsystemstrukturen eine einfache Herangehensweise, um die erwartete Sorgfaltspflicht im Bereich Informationssicherheit sowie die gesetzlichen Anforderungen zu erfüllen.

Online-Quick-Check Informationssicherheit.

Fragen an den Experten

Roland Brunner, Senior Information Security Consultant bei der WiB Solutions AG, über realistisches Vorgehen:

Muss sich jedes Unternehmen nach ISO 27001 zertifizieren lassen, um absolute Informationssicherheit gewährleisten zu können?

Roland Brunner: Nein, natürlich nicht. Die Zertifizierung ergibt vor allem für Unternehmen mit eigenen Rechenzentren, IT-Dienstleister und Grosskonzerne Sinn. Orientiert man sich an der ISO 2700x Norm, bedeutet das nicht, dass damit eine Zertifizierung angestrebt werden muss. Das bestehende Framework der Norm stellt eine durchdachte Struktur und sogenannte Control-Patterns zur Verfügung, welche von jedem Unternehmen unter Berücksichtigung der eigenen Bedürfnisse untersucht, genutzt und dokumentiert werden können. Last, but not least, die absolute Sicherheit ist weder in der physischen noch in der digitalen Welt gewährleistet. Es gilt, Risiken zu erkennen, zu klassifizieren, entsprechende Massnahmen zu ergreifen oder die Auswirkungen zu minimieren.

Gibt es Hilfsmittel, welche Unternehmen dabei unterstützen, eine Einschätzung der eigenen Informationssicherheit vorzunehmen?

Der Online-Quick-Check für Informationssicherheit und Datenschutz der WiB Solutions AG bietet Unternehmen die Möglichkeit, anhand von 30 auf Informationssicherheit fokussierten Fragen ihre Lage einzuschätzen; zum einen wird der Reifegrad der relevanten Prozesse und Themen gemessen und zum anderen erhalten Unternehmen eine Einschätzung darüber, welche Themengebiete für die Unternehmung in der Umsetzung wie zu gewichten sind. Nicht alle Themengebiete sind für jedes Unternehmen gleich relevant.

Fazit

Fehlendes Management der Informationssicherheit im ICT-Umfeld ist ein ständiger «Tanz auf dem Vulkan» – es ist sicher, dass ein Ausbruch erfolgen wird, jedoch ist nicht klar, wann, in welcher Stärke und welche Präventionsmassnahmen Risiken vermindern. In diesem Umfeld sind diejenigen Organisationen gut positioniert, welche sich dem Thema stellen und deren Mitarbeitende flexibel genug sind, auf Veränderungen zeitnah zu reagieren. ■

** KMU-Cyber-Angriffe im Jahr 2017 – https://www.kmu.admin.ch/kmu/de/home/aktuell/news/2018/schweizer-kmu-nicht-ausreichend-vor-cyberangriffen-geschuetzt.html*