Digitalisierung/IT-Sicherheit II

Cybersecurity – Massnahmen und Hilfsmittel

Cyberangriffe gewinnen an Aufmerksamkeit, denn die konkrete Bedrohung mit Auswirkungen auf die IT nimmt zu. Wer trotz der steigenden Gefahren nichts tut, wird im Fall des Eintretens sein Verhalten erklären müssen. Der Beitrag zeigt, was Unternehmen vorbeugend konkret tun können und welche Hilfsmittel es gibt.

› Heinrich A. Bieler

Sicherheit kostet Geld, ist oft unbequem und verlangsamt ein System. Sicherheit trägt im Normalzustand nicht zur Wertschöpfung bei. Solange nichts passiert, ist man versucht, Investitionen in die Sicherheit tief zu halten. Je grösser die Bedrohung im Umfeld, umso grösser wird die Wahrscheinlichkeit eines Ereignisses und desto stärker der Druck, sich um die Sicherheit zu kümmern. Dieser Druck steigt stark, wenn ein Ereignis eintritt, wobei natürlich jeder hofft, dass es ihn nicht als Ersten erwischt.

Kosten quantifizieren

Mit dieser Situation gekonnt umzugehen, nennt man Risikomanagement. Aufgrund der systematischen Analyse im Rahmen des Risikomanagements findet jede Organisation für ihre aktuelle Situation die notwendigen Massnahmen und kann somit auch die Kosten quantifizieren. Es sollte selbstverständlich sein, dass die Massnahmen nur dann einen Wert haben, wenn sie konsequent umgesetzt werden.

Aus der Erfahrung als Zertifizierungsstelle stellen wir oft fest, dass einerseits aufgrund unsystematischer Risikobeurteilung am falschen Ort investiert wird und andererseits Massnahmen nicht konsequent umgesetzt werden.

Das immaterielle Vermögen

Die grössten Werte entstehen heute nicht mehr bei den Unternehmen, die über materielle oder finanzielle Vermögenswerte verfügen, sondern bei denjenigen, die immaterielle Werte am besten verwalten. Dabei kann es sich um so unterschiedliches immaterielles Vermögen wie Software, Patente, geistiges Eigentum, Urheberrechte, Kundendaten, Marken oder Humankapital handeln. Immaterielle Werte machen heute etwa 85 Prozent der Bewertung der im Standard-&-Poor's-Index vertretenen Unternehmen aus. 1975 waren es noch weniger als 20 Prozent.

Information ist ein Aktivposten im Unternehmen. Information kann in vielen Formen vorkommen: auf Papier, elektronisch, auf Film, gesprochen oder per Post übermittelt. Information ermöglicht Chancen zu nutzen, und sie ist Gefahren ausgesetzt. Zur Ermittlung des Wertes des immateriellen Vermögens wurden aufgrund des zunehmenden Bedarfs verschiedene Methoden entwickelt.

Die Bedrohung

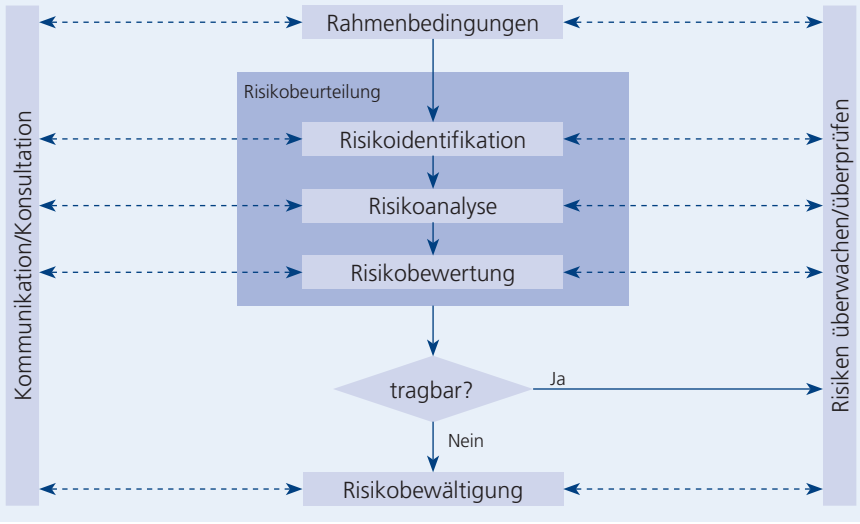
Der Begriff Cybersecurity kommt in der täglichen Berichterstattung immer öfter vor. Es muss auch kaum mehr diskutiert werden, ob man sich als Unternehmen darum kümmern muss. Aufgrund der Entwicklungen im Rahmen der Digitalisierung, die wohl in keiner Strategie mehr fehlt, nehmen die Gefahren zu.

Die Zunahme der von zu Hause aus Arbeitenden hat, durch die Pandemie angestossen, nicht unbedingt neue Bedrohungen aufgezeigt, sie haben aber an Wahrnehmung gewonnen. Es geht dabei nicht nur um das Arbeiten im Homeoffice, sondern generell um das mobile Arbeiten. Die zunehmende Digitalisierung und die Benutzung von Hilfsmitteln wie zum Beispiel MS Teams erleichtern ortsunabhängiges Arbeiten, machen aber auch abhängig von funktionierenden Systemen und erhöhen die Verletzlichkeit.

Es gibt viele Risiken, von denen einige schwerwiegender sind als andere. Zu diesen Gefahren gehören Malware, die das gesamte System löscht, ein Angreifer, der in das System eindringt und Dateien verändert, ein Angreifer, der Computer benutzt, um andere anzugreifen, oder ein Angreifer, der Kreditkartendaten stiehlt und unberechtigte Einkäufe tätigt. Es gibt keine Garantie dafür, dass selbst mit den besten Vorsichtsmassnahmen nicht doch etwas davon passiert, aber es gibt Schritte, die man unternehmen kann, um das Risiko zu minimieren. Dazu kommt, dass zunehmend Gesetze zu berücksichtigen sind, die zum Motiv haben, für die Gesellschaft eine sichere Basis zu ermöglichen. Dazu zählen die DSGVO im EU-Raum und in der Schweiz das neue Datenschutzgesetz, das auf seine Inkraftsetzung wartet.

Wichtige Themen sind die Informationssicherheit, Netzwerksicherheit, Operative Sicherheit, Sicherheit der Anwendungen, Ausbildung der Endbenutzer und Planung der Geschäftskontinuität. Cybersecurity muss als Grundlage für eine funktionierende, stabile Volkswirtschaft verstanden werden und liegt im Interesse jedes Einzelnen.

Abb. 1: Das Risikomanagement



Die Verantwortung

Auch wenn die hundertprozentige Sicherheit nicht erreicht werden kann, ist es keine Option, nichts zu tun und im Eintretensfall zu argumentieren «dumm gelaufen», «das kann jedem passieren». Es muss bewusst Risikomanagement betrieben werden, das zu dokumentieren ist.

Unter Risikomanagement versteht man alle Tätigkeiten zur Identifikation, Einschätzung, Steuerung und Überwachung von Risiken bezüglich der Zielerreichung im Unternehmen.

Seit der Aktienrechtsrevision 2013 müssen ordentlich revisionspflichtige Unternehmen anstelle des Jahresberichts einen Lagebericht mit einer Risikobeurteilung

Abb. 2: Hilfreiche Normen

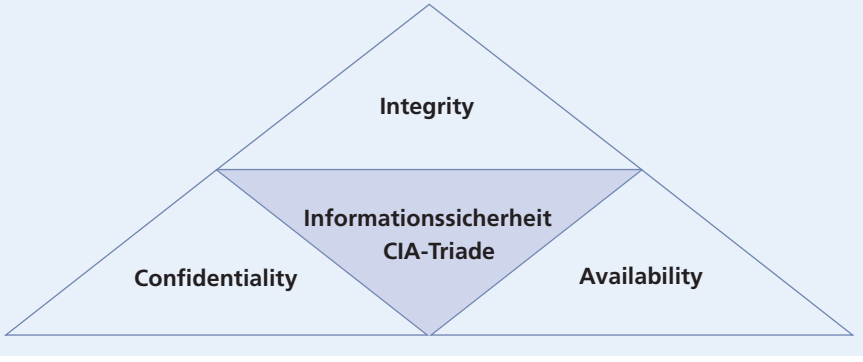
ISO/IEC 27000 Begriffe, Definitionen			
ISO/IEC 27001 Anforderungen (Zertifizierung)	**ISO/IEC 27006** Anforderungen an Zertifizierungsstellen		
ISO/IEC 27002 Leitfaden: Massnahmen generell	**ISO/IEC 27003** Leitfaden ISMS	**ISO/IEC 27004** Überwachen, messen, analysieren, bewerten	**ISO/IEC 27005** Risikomanagement
ISO/IEC 27017 Leitfaden: Massnahmen Cloud Services	**ISO/IEC 27018** Leitfaden: Massnahmen personenbezogene Daten (PII)	**ISO/IEC 27701** Leitfaden: Massnahmen Datenschutz	
ISO/IEC 27009 Sektorspezifische Anwendung	**ISO/IEC 27011** Leitfaden: Telekommunikationsunternehmen	**ISO/IEC 27019** Leitfaden: Energieversorgung	**ISO/IEC 27799** Leitfaden: Gesundheitswesen

erstellen. Der Verwaltungsrat muss ein System zur Risikoerfassung und des Risikomanagements einrichten, damit Risiken im Unternehmen erkannt und richtig behandelt werden.

Der Verwaltungsrat selbst muss sich mit den Risiken auseinandersetzen, die für das Unternehmen von existenzieller Bedeutung sind, sowie die Gesamtrisikolage des Unternehmens steuern beziehungsweise der Risikofähigkeit der Gesellschaft anpassen. Diese Elemente der Risikosteuerung müssen zu einem sinnvollen Ganzen zusammengesetzt werden, das es ermöglicht, Risiken zu erkennen und, wo sie unvermeidbar sind, einzugrenzen.

Die Ausgestaltung dieser Instrumente und die Intensität, mit der sie eingesetzt werden, hängen von der Komplexität, der Grösse und der Ausrichtung des Unternehmens ab. Cybersicherheit ist also ein Thema, mit dem sich die oberste Führung einer Organisation kompetent auseinandersetzen muss.

Abb. 3: Dimensionen potenzieller Auswirkungen von Bedrohungen



Die Massnahmen

Der erste Schritt, um sich zu schützen, besteht darin, die Risiken zu erkennen. Dazu muss man sich mit den Bedrohungen und möglichen Szenarien vertraut machen. Um die Risiken von Cyberangriffen zu minimieren, sollte man grundlegende bewährte Verfahren der Cybersicherheit befolgen.

In Anbetracht der vielen Möglichkeiten, die einem offenstehen, um an Informationen über Bedrohungen zu kommen, deren Relevanz für die eigene Organisation abzuschätzen und sich durch gezielte Massnahmen besser zu schützen, gibt es keinen Grund, nichts zu tun.

Wertvolle und laufend aktualisierte Informationen findet man zum Beispiel auf den Regierungsseiten im Internet (siehe Kasten: Informationsquellen). Es ist dabei sicher sinnvoll, über die Landesgrenzen hinauszuschauen. Eine wertvolle und umfassende Quelle für mögliche Massnahmen ist das Dokument ISO/IEC 27002.

Cybersecurity ist teilweise kompliziert, aber nicht immer komplex. Man sollte den Begriff komplex nicht bei jedem Problem / jeder Herausforderung verwenden, die einem etwas mehr als üblich abverlangt (siehe Box «Stichwort: Komplizierte/Komplexe Probleme»).

Normen helfen

Informationssicherheit muss in jeder Organisation ein Thema sein. Stellt sich die Frage, was konkret zu tun ist. Auch in einer komplexen Umgebung hilft systematisches Vorgehen. Der Einsatz von Methoden (Wie ist etwas zu tun?) und Vorgehensmodellen (Was ist zu tun?) erleichtert das Vorgehen und führt zum Erfolg. Sicher hilfreich wäre ein Katalog von Bedrohungen und Massnahmen, den man auf die eigene Organisation anwenden kann. Dieser Katalog steht in Form der Norm ISO/IEC 27002 zur Verfügung.

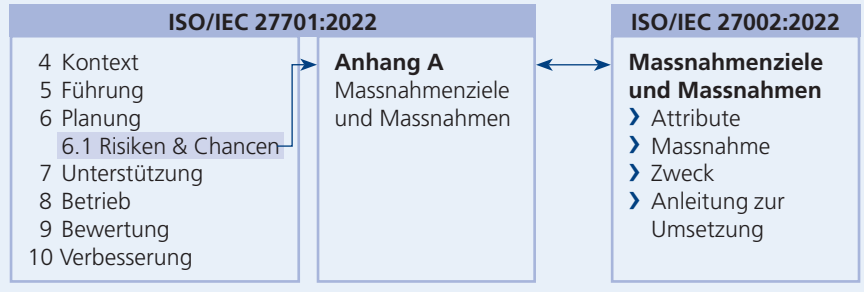
Es stehen mit ISO/IEC 27001 eine etablierte, zertifizierbare Norm und eine grosse Anzahl (ca. 50) Leitfäden zur Verfügung, die bei der Umsetzung im spezifischen Umfeld eine grosse Hilfe sind und Sicherheit geben.

Entwicklung

ISO/IEC 27002 ist ein Leitfaden, der praxisbezogene Hinweise enthält, welche Massnahmen sich im Rahmen der Informationssicherheit bewährt haben und wie diese umgesetzt werden können.

Normen für Managementsysteme gehen mit der Zeit und werden alle fünf Jahre auf ihre Gültigkeit hin überprüft. Nach über neun Jahren ist die überarbeitete ISO/IEC 27002:2022 im Februar endlich erschienen. Bisher hiess die Norm: Information technology – Security techniques – Code of practice for information security controls, neu nennt sie sich: Information security, cybersecurity and privacy protection – Information security controls. Damit ist klar, dass die Informations-

Abb. 4: Normenstrukturen



Neue Massnahmen aus der ISO/IEC 27002

Threat intelligence (Informationen über Bedrohungen): Die Organisation kümmert sich aktiv darum, Angreifer und ihre Methoden vor dem Hintergrund Ihrer IT-Landschaft zu verstehen.

Information security for use of cloud services (Informationssicherheit in Cloud-Diensten): Cloud-Initiativen müssen ganzheitlich von der Einführung über den Betrieb bis hin zur Exit-Strategie betrachtet werden.

ICT Readiness for Business Continuity (Bereitschaft zur Geschäftskontinuität): Die Anforderungen an die IT-Landschaft müssen aus der Business-Prozess-Perspektive abgeleitet werden. Welche Bereitschaft der ICT und welche Kontinuitätsanforderungen sind zu erfüllen?

Physical security monitoring (Überwachung der physischen Sicherheit): Die Vermeidung unautorisierter physischer Zutritte soll mittels Alarmierungs- und Überwachungssystemen verhindert werden.

Configuration management (Konfigurationsmanagement): Die sichere Konfiguration von IT-Systemen und die Härtung gewinnen an Bedeutung. Hardware, Software, Dienste und Netze sind zu behandeln.

Information deletion (Löschen von Informationen): Das sichere Löschen und insbesondere die Wahrung externer Anforderungen, beispielsweise Löschkonzepte, müssen umgesetzt werden (Datenschutzanforderungen).

Data masking (Maskierung von Daten): Mit Maskierungstechniken wie Anonymisierung und Pseudonymisierung den Datenschutz erhöhen. Berücksichtigung rechtlicher Anforderungen.

Data leakage prevention (Verhinderung von Datenverlusten): Massnahmen zur Verhinderung von Datenlecks sind auf Systeme, Netzwerke und Endgeräte anzuwenden, um den unautorisierten Datenabfluss zu vermeiden.

Monitoring activities (Überwachung der Aktivitäten): Netzwerk- und Anwendungsverhalten sollen überwacht werden, um Anomalien zu detektieren.

Web filtering (Webfilter): Der Zugriff auf externe Websites, die Schad-Codes enthalten können, ist mittels Webfilter-Methoden zu verhindern.

Secure coding (Sichere Kodierung): Das sichere Programmieren, die Nutzung von Tools, die Überwachung genutzter Bibliotheken und Repositorien, das Kommentieren und Nachvollziehen von Änderungen und das Vermeiden unsicherer Programmiermethoden sollen die Sicherheit erhöhen (Security by Design).

sicherheit in einem viel breiteren Kontext betrachtet wird. Die Inhalte berücksichtigen zusätzliche Cyberelemente (Cybersecurity). Gleichzeitig bekommt auch der Datenschutz einen grösseren Stellenwert (Privacy Protection).

Die Norm, nach der sich Organisationen zertifizieren lassen können und die heute immer mehr von Unternehmen als Basis für eine vertrauensvolle Zusammenarbeit verlangt wird, heisst ISO/IEC 27001. Weil ein Teil dieser Norm (Anhang A) die Massnahmen aus ISO/IEC 27002 enthält, sind Anpassungen notwendig. Für solche Fälle gibt es die Möglichkeit, anstelle einer neuen Version eine Aktualisierung (Amendment) herauszugeben. Man will an einer Norm nicht mehr als zwei solche Aktualisierungen vornehmen.

Bei der aktuellen Version wurden bereits zwei Ergänzungen vorgenommen, deshalb erscheint eine neue Version, auch wenn sich die Änderungen primär auf den Anhang A beschränken werden. Die Publikation der Norm sollte, so ist es aktuell geplant, im Oktober 2022 erfolgen. Bereits zertifizierte Organisationen haben, nach aktuellem Stand, zwei Jahre Zeit für die Umstellung. Es empfiehlt sich also jetzt schon, mit ISO/IEC 27002 auf die neue ISO/IEC 27001 vorzubereiten.

Die wichtigsten Vorteile der neuen Version für zertifizierte Unternehmen:

- berücksichtigt neue Szenarien und Risiken;
- hilft, andere Sicherheitsperspektiven zu verstehen;
- umfasst Aspekte der Cybersicherheit und des Datenschutzes;
- enthält neue Controls (Massnahmen), um sicherzustellen, dass neue Szenarien und Risiken nicht übersehen werden.

Im Zusammenhang mit der Informationssicherheit bewertet man Bedrohungen und Schwachstellen auf der Grundlage ihrer potenziellen Auswirkungen in den drei Dimensionen: Vertraulichkeit, Integrität und Verfügbarkeit der Vermögenswerte eines Unternehmens. Auf der Grundlage dieser Bewertung implementiert das Unternehmen eine Reihe von Massnahmen, um das Risiko zu verringern.

ISO/IEC 27001 beschreibt Anforderungen, die man erfüllen sollte, wenn man Informationssicherheit gewährleisten will. Diese Norm ist in der Struktur identisch aufgebaut wie andere, bekannte Normen sind: ISO 9001 – Qualitätsmanagement, ISO 14001 – Umweltmanagement, ISO 45001 – Arbeitsschutz etc.

Das ist kein Zufall, sondern Absicht. Mit der sogenannten High Level Structure (HLS) will man es den Anwendern einfacher machen, mehrere Normen anzuwenden. Dabei soll man nicht für jedes Bedürfnis ein isoliertes System aufbauen. Man sollte ein einziges, unternehmenseigenes System pflegen und weiterentwickeln.

In einem Kapitel wird auf den Umgang mit Risiken und Chancen eingegangen (Kapitel 6.1). Informationssicherheitsrisiken sollten beurteilt und behandelt werden. Als Hilfestellung enthält die Norm den Anhang (A), der eine umfassende, wenn auch nicht abschliessende Liste von Massnahmenzielen und Massnahmen enthält. In den oben aufgeführten Leitfäden findet man weitere Massnahmen zu den speziellen Themen.

Stichwort: Cybersecurity

Cyber – Der Begriff leitet sich ursprünglich aus dem Wort Kybernetik beziehungsweise im Englischen cybernetics ab und beschreibt eine wissenschaftliche Forschungsrichtung, die Systeme verschiedenster Art auf selbsttätige Regelungs- und Steuerungsmechanismen hin untersucht. Der Begriff steht seit Ende des 20. Jahrhunderts für die von Computern erzeugte, virtuelle Scheinwelt.

Unter Cybersicherheit versteht man die Kunst des Schutzes von Netzwerken, Geräten und Daten vor unbefugtem Zugriff oder krimineller Nutzung und die Praxis der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Es scheint, als ob heute alles von Computern und dem Internet abhängt – Kommunikation (zum Beispiel E-Mail, Smartphones, Tablets), Unterhaltung (zum Beispiel interaktive Videospiele, soziale Medien, Apps), Verkehr (zum Beispiel Navigationssysteme), Einkaufen (zum Beispiel Online-Shopping, Kreditkarten), Medizin (zum Beispiel medizinische Geräte, Krankenakten).

Wie viel von Ihrem persönlichen täglichen Leben hängt von der Technologie ab? Wie viele Ihrer persönlichen Daten sind entweder auf Ihrem eigenen Computer, Smartphone oder Tablet und damit meist auch in der Cloud oder auf dem System eines anderen gespeichert?

Stichwort: IT-Sicherheit oder Informationssicherheit

Die IT-Sicherheit ist ein Teil der Informationssicherheit. Während es bei der IT-Sicherheit um den Schutz von Informationen mithilfe von Informationstechnologie (IT) – also die technischen Aspekte – geht, ist die Informationssicherheit deutlich weiter gefasst. Hier sind unter anderem auch räumliche, personelle und organisatorische und andere Aspekte relevant. Dieses erweiterte Verständnis spiegelt sich auch in den verschiedenen Rollen, Aufgaben und Funktionen im Bereich der Informationssicherheit wider.

ISO/IEC 27002 ist ein Leitfaden und gibt auf 168 Seiten Hilfestellung bei der Umsetzung. Die Massnahmen aus dem Anhang A von ISO/IEC 27001 sind aufgeführt, der Zweck der Massnahme wird erläutert und – sehr hilfreich – es sind ausführlich Anleitungen zur Umsetzung aufgeführt.

Praxistipp: Die Korrelationstabellen können helfen, den Zugang zur neuen Struktur zu finden. Weil die Massnahmen inhaltlich teilweise zusammengeführt wurden, kann die Entsprechung im Titel trügerisch sein und die Massnahme enthält inhaltliche Änderungen oder man hat diese bisher anders verstanden, was man nun durch die verbesserte Formulierung erkennt. Man geht also besser alle Massnahmen durch und überlegt sich, ob es noch Handlungsbedarf gibt.

Auf den ersten Blick fällt die geänderte Struktur auf. Man ist bei zwei Ebenen geblieben. Anstelle von bisher 14 Kapiteln hat man sich auf 4 Kapitel mit gut verständlichen Oberbegriffen geeinigt:

- Organisatorische Massnahmen (Organizational controls), 37
- Personelle Massnahmen (People controls), 8
- Physische Massnahmen (Physical controls), 14
- Technische Massnahmen (Technological controls), 34

Die Anzahl der Massnahmen pro Kapitel (Anzahl in Klammern) hat sich dadurch generell erhöht. Insgesamt hat sich die Zahl der Massnahmen von 114 auf 93 reduziert. Das heisst nun aber nicht, dass die Themen reduziert wurden. 61 Massnahmen können als unverändert betrachtet werden. Diverse wurden zusammengefasst. Drei Massnahmen wurden weggelassen und elf neue eingeführt (siehe Box «Neue Massnahmen»).

Damit man den Überblick behält, ist für jede Massnahme eine Tabelle mit Ausprägungen in fünf Attributen erhalten. Dadurch ist es möglich, je nach Interesse die Massnahmen aus unterschiedlichen Sichten (Views) durch die Zusammenfassung nach beliebigen Hashtags (#) darzustellen. Im Anhang A sind dazu Beispiele aufgeführt. Eine nützliche Spielerei.

- Kategorisierung: präventiv, detektivisch, korrigierend
- Merkmale der Informationssicherheit: Vertraulichkeit, Integrität, Verfügbarkeit (CIA)
- Cybersicherheitskonzepte: Identität, Schutz, Identifizierung, Reaktion, Wiederherstellung
- Operative Fähigkeiten: Governance, Vermögensverwaltung, Informationssicherheit, Sicherheit der Humanressourcen usw.
- Sicherheitsbereiche: Schutz, Governance, Widerstandsfähigkeit
- Control type: Preventive, Detective, and Corrective
- Information security properties: Confidentiality, Integrity, and Availability
- Cybersecurity concepts: Identify, Protect, Detect, Respond, and Recover
- Operational capabilities: Governance, Asset management, Information protection, Human resource security, Physical security, System and network security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier relationships security, Legal and compliance, Information security event management, and Information security assurance
- Security domains: Governance and ecosystem, Protection, Defense, and Resilience

Wer bereits die Version 2013 von ISO/IEC 27002 nutzt, findet im Anhang B eine Korrelationstabelle zwischen den Versionen 2013 und 2022 in beiden Richtungen.

Zertifizierung ist nützlich

Die Frage ist nicht, ob man eine Zertifizierung benötigt, sondern welche Einstel-

Stichwort: Komplizierte/Komplexe Probleme

Kompliziert
Ein kompliziertes Problem (lat. complicare = verwickeln) ist eines, das aufgrund der Menge von Elementen schwer zu überschauen ist, obwohl seine Struktur auf einer endlichen Menge relativ einfacher Regeln aufbaut. Ein solches Problem lässt sich mit entsprechendem Aufwand (Zeit, Ressourcen) lösen. Die Beziehung zwischen Ursache und Wirkung lässt sich ermitteln, denn sie ist deterministisch. Komplizierte Sachverhalte lassen sich formal beschreiben und komplizierte Probleme mit Hilfe von Technik und Fachwissen effizient lösen. Der Grad der Kompliziertheit ist jeweils eine Frage der Wahrnehmung.

Komplex
Ein komplexes Problem (lat. complectere = verflechten) ist eines, dessen zugrundeliegende Struktur viele Verflechtungen und Abhängigkeiten besitzt, seine Ursache-Wirkungszusammenhänge sind unüberschaubar und Regeln können unerwartet ändern. Die Einflussfaktoren können sich durch Wechselwirkungen und Rückkopplungseffekte gegenseitig beeinflussen und oft ist nicht einmal ihre genaue Anzahl bekannt. Entsprechend ist die Lösung nur schwer bis gar nicht voraussagbar.

Komplexität ist auch ein Mass für die Überraschung, die einem System oder Problem innewohnt. Die meist multikausale Beziehung zwischen Ursache und Wirkung kann erst im Nachhinein ermittelt werden. Komplexe Sachverhalte lassen sich höchstens in Teilbereichen formal beschreiben. Komplexe Probleme sind daher nicht völlig beherrschbar und können auch nicht allein durch Technik gelöst werden. Sie benötigen Fachwissen und Zeit und können nur von Menschen gelöst werden.

lung man dazu hat. Die Zertifizierung entfaltet in unterschiedlichen Dimensionen ihren Nutzen. Intern hilft sie, das Ziel nicht aus den Augen zu verlieren und täglich und personenunabhängig die von den Kunden und interessierten Parteien erwartete Leistung zu erbringen. Die Organisation erhält zudem eine Rückmeldung über den Grad, in dem Massnahmen umgesetzt werden.

Extern ist das Zertifikat ein Zeichen dafür: Man kann sich darauf verlassen, dass die mit der Norm verbundenen Anforderungen erfüllt werden und dies von einer objektiven und unabhängigen Stelle bestätigt wird.

Natürlich haben Unternehmen eine Übergangsfrist, um ihr ISMS auf den aktuellen Stand zu bringen. Trotzdem sollten sie sich jetzt schon mit der überarbeiteten Norm beschäftigen, denn es hat sich nicht nur der Titel geändert.

Vorgehen

Wer bereits ein Managementsystem implementiert hat und anwendet, ist klar im Vorteil (vgl. ISO 9001). Massnahmen, die mit einem System verknüpft sind, das Prozesse und ihre Wechselwirkung aufzeigt, entfalten ihre Wirkung zuverlässiger als Regeln, die ohne Zusammenhang zu befolgen sind.

- Die einhundertprozentige Sicherheit gibt es nicht. Das ist kein Grund, sich nicht zu schützen.
- Die Massnahmen müssen auf die Organisation abgestimmt sein.
- Eine Organisation muss wissen, wo sie angreifbar ist (Bedrohung, Gefährdung, Risiken).
- Eine Organisation muss sich über mögliche Massnahmen informieren und die für sie zweckmässigen aussuchen.
- Am Schluss zählen umgesetzte Massnahmen und nicht schöne Pläne.
- Zertifizierung schafft Vertrauen und hilft dranzubleiben. «

Informationsquellen

Schweiz: www.ncsc.admin.ch

Deutschland: www.bsi.bund.de

Österreich:
https://www.bundeskanzleramt.gv.at/themen/cybersicherheit.html

Frankreich:
www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france

Italien:
www.esteri.it/en/politica-estera-e-cooperazione-allo-sviluppo/temi_globali/cybersecurity

EU:
www.enisa.europa.eu

USA
www.cisa.gov
www.nist.gov/cyberframework
NIST: www.nist.gov
ISF: www.securityforum.org

Weitere Informationen
www.safetycenter.ch/zertifizierung/systeme-produkte/normen-standards/iso-27001
www.safetycenter.ch/checklisten

Passende Anlässe und Kurse

Safety Compact – Managementbriefing Informationssicherheit ISO 27001

Lehrgang Quality System Manager

Qualitätsmanagement für Führungskräfte

https://akademie.svti-gruppe.ch

Zusätzliche Informationen und Hilfsmittel (Checkliste und Formulare) zum Thema Informationssicherheit
www.safetycenter.ch/cs/Thema-ISMS

Porträt

Heinrich A. Bieler
Head of Certifications, Swiss Safety Center AG

Die Swiss Safety Center AG engagiert sich als Teil der SVTI-Gruppe mit spezifischen Dienstleistungen, Produkten und Qualifizierungen im Sicherheits- und Qualitätsbereich. Swiss Safety Center bietet Lösungen für alle Branchen mit spezifischen Dienstleistungen, Produkten und Qualifizierungen im Sicherheits- und Qualitätsbereich. Dazu zählen Inspektionen, Prüfungen, Zertifizierungen, Begutachtungen, Expertisen sowie Aus- und Weiterbildungen in den Bereichen Risikomanagement, Arbeitssicherheit, Brandschutz, Werkstoffsicherheit und in vielen weiteren Fachgebieten der technischen Sicherheit.

Kontakt

heinrich.bieler@safetycenter.ch
www.safetycenter.ch/zertifizierung