

Dieses Dokument enthält
in der Anlage Arbeitshilfen.
Wie Sie diese öffnen,
erfahren Sie [hier](#).

Informationssicherheit richtig implementieren und integrieren

TÜV Media

Die ISO/IEC 27001 im IMS

- Leseprobe

Autor:

Dr.-Ing. Wolfgang Kallmeyer
Partner der TÜV Rheinland Consulting GmbH

Leseprobe

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7406-0854-5 (Print)
ISBN 978-3-7406-0856-9 (E-Book)

© by TÜV Media GmbH, TÜV Rheinland Group, 1. Auflage, Köln 2023
www.tuev-media.de

® TÜV, TUEV und TUV sind eingetragene Marken.
Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Die Inhalte dieses Werks wurden von Verlag und Redaktion nach bestem Wissen und Gewissen erarbeitet und zusammengestellt. Eine rechtliche Gewähr für die Richtigkeit der einzelnen Angaben kann jedoch nicht übernommen werden. Gleiches gilt auch für Websites, auf die über Hyperlinks verwiesen wird. Es wird betont, dass wir keinerlei Einfluss auf die Inhalte und Formulierungen der verlinkten Seiten haben und auch keine Verantwortung für sie übernehmen. Grundsätzlich gelten die Wortlaute der Gesetzestexte und Richtlinien sowie die einschlägige Rechtsprechung.

Zur Nutzung der Broschüre

Praktisch jedes Unternehmen auf dieser Welt kommt mit dem Thema Informationssicherheit in Berührung. Daten in jedweder Form werden erstellt, genutzt, versendet und gespeichert, sie sind allgegenwärtig. Neben Geld sind Daten das Schmiermittel für unsere Zivilisation und den wirtschaftlichen Erfolg. Das Internet ist die Datenautobahn für Informationen aller Art. Um den Verkehr auf dieser Autobahn störungsfrei fließen zu lassen, sind Regeln notwendig, aber auch wirksame Kontrollen und ggf. auch Sanktionen gegen die, die sich nicht an die Regeln halten oder nicht halten wollen.

In dieser Broschüre erfahren Sie, warum Informationssicherheit in unserer digitalen Welt immer mehr an Bedeutung gewinnt. Dies gilt nicht nur für Unternehmen, sondern für alle Organisationen, Behörden und auch für jeden einzelnen Menschen. Wir erläutern Ihnen, welche Felder der Informationssicherheit heute von Bedeutung sind.

Sie erhalten Kenntnis darüber, was die International Standard Organisation (ISO) mit der Norm ISO/IEC 27001:2022 „Informationssicherheitsmanagementsystem (ISMS)“ erreichen möchte, welchen Zweck und welche Schutzziele damit verfolgt werden. Wir erläutern Ihnen die Struktur der ISO/IEC 27001 und die grundlegenden Forderungen, die an ein ISMS zu stellen sind. Dabei werden auch die Veränderungen in der Norm durch die Revision im Jahr 2022 gezeigt.

Die ISO/IEC 27001 reiht sich ein in eine größere Gruppe von Managementsystemnormen der ISO. Welche Interaktionen mit den drei wichtigsten anderen weltweiten ISO-Normen (9001, 14001 und 45001) bestehen, haben wir in einem eigenen Abschnitt beschrieben. Wo gibt es aufgrund der Harmonized Structure (HS) Überschneidungen, die genutzt werden können, wo liegen die Unterschiede. Außerdem erläutern wir Ihnen die Regelwerke des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Beiträge des BSI gehen das Thema mehr von der praktischen Seite der IT-Sicherheit an. In Ergänzung zur ISO/IEC 27001 entsteht durch die Kombination beider Sichtweisen, Managementsystem und operative IT-Sicherheit, ein ganzheitliches Bild gelebter Informationssicherheit.

Kein Managementsystem der ISO kommt ohne die Berücksichtigung regulatorischer Forderungen in Form von Rechtsvorschriften aus. Wir geben Ihnen einen Überblick über die wesentlichen Rechtsvorschriften, die in der Informationssicherheit Anwendung finden und die beim Aufbau eines ISMS berücksichtigt werden müssen.

Erfahren Sie, wie Sie die Forderungen der ISO/IEC 27001 an das Informationssicherheitsmanagement implementieren und in einem Integrierten Managementsystem (IMS) zusammenfassen können, bestehend aus ISO 9001 (Qualität), ISO 14001 (Umweltschutz) und ISO 45001 (Arbeits- und Gesundheitsschutz). Das heißt da, wo möglich, die Synergien der anderen Managementsysteme zu nutzen, um beim Aufbau des ISMS und dessen Integration in das IMS Redundanzen und somit überflüssige Mehrarbeit zu vermeiden. Die Details dazu haben wir in Form eines Tabellenwerks zusammengestellt, das alle operativen Kapitel von Normkapitel 4 „Kontext der Organisation“ bis Normkapitel 10 „Bewertung“ umfasst. Die Aussagen des Normenanhangs A „Referenz zu Informationssicherheitsmaßnahmen“ wurden dabei berücksichtigt.

Wir unterstützen Sie rund um das Thema Informationssicherheitsmanagement mit Arbeitshilfen und Mustern in Form von Formularen und Tabellen, die Ihnen beim Aufbau und der Integration der ISO/IEC 27001 in ein IMS behilflich sind.

Daten, Daten, Daten

Zielsetzung der Broschüre

Managementsystemnorm

Rechtsvorschriften

Integrieren und Synergien nutzen

Arbeitshilfen



Verweismatrix_27001_neu_alt.xlsx



Verweismatrix_9001_14001_45001_27001.xlsx



Kompatibilitätsmatrix_IMS.xlsx



ISRA_Nohl.xlsx



SoA.xlsx



Nachweise.xlsx

Download

Verweismatrix ISO/IEC 27001:2022 zu ISO/IEC 27001:2013

Die Arbeitshilfe „Verweismatrix_27001_neu_alt“ stellt die Normkapitel der Standards ISO/IEC 27001:2022 und ihrem Vorgänger ISO/IEC 27001:2013 einander gegenüber.

Verweismatrix der Normen im betrachteten IMS

Die Arbeitshilfe „Verweismatrix_9001_14001_45001_27001“ stellt über eine Verweismatrix die Normkapitel der Standards ISO 9001, ISO 14001, ISO 45001 und ISO/IEC 27001 in der Kapitelstruktur bis herab auf die dritte Gliederungsebene mit deren Gemeinsamkeiten sowie Unterschieden einander gegenüber.

Kompatibilität ISO/IEC 27001:2022 zu ISO 9001, ISO 14001, ISO 45001

Die Arbeitshilfe stellt in einer Matrix die ISO/IEC 27001 den Standards ISO 9001, ISO 14001 und ISO 45001 gegenüber und gibt durch farbliche Kennzeichnung Hinweise über die Kompatibilität der grundlegenden Anforderungen im IMS.

Informationssicherheitsrisikobeurteilung ISO/IEC 27001:2022 (nach Nohl)

Die Methode nach Nohl nutzt zur Risikobewertung zwei Kriterien, zum einen die Wahrscheinlichkeit, dass sich das Risiko realisiert, und zum anderen den dadurch entstehenden Schaden (Schadenshöhe). Als Muster ist eine Matrix zur Informationssicherheitsrisikoanalyse nach Nohl beigefügt.

Risikobehandlungsplan (SoA)

Möglichkeiten zur Behandlung von Risiken müssen ausgewählt und implementiert werden. Die getroffenen Maßnahmen sollten in einem Risikobehandlungsplan (SoA – Statement of Applicability bzw. Erklärung zur Anwendbarkeit) übersichtlich dokumentiert werden. Die Arbeitshilfe bietet Ihnen ein Muster für einen erweiterten Risikobehandlungsplan.

Zuordnung ISMS-Prozesse/Nachweise zum Anhang A (ISO/IEC 27001:2022)

Die Arbeitshilfe stellt in einer Matrix, die die Zuordnung der potenziellen operativen ISMS-Prozesse und Nachweise zum Normanhang A der ISO/IEC 27001:2022 her

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

www.qm-aktuell.de

Passwort:

Sie können die Dokumente frei bearbeiten und an Ihre eigenen betrieblichen Anforderungen anpassen.

Inhalt

Zur Nutzung der Broschüre	3
1 Bedeutung der Informationssicherheit	7
2 Ziel und Zweck der ISO/IEC 27001:2022	13
3 Die ISO/IEC 27001, Harmonized Structure und IMS-Integration	17
3.1 Struktur der ISO/IEC 27001 (inkl. HS).....	17
3.2 Revision ISO/IEC 27001:2022 – Was gibt es Neues?	19
4 Beziehung zu weiteren Normen und Regelwerken	25
4.1 Weitere Normen zum Informationssicherheitsmanagement	25
4.2 Zusammenspiel mit anderen ISO-Managementsystemnormen ..	28
4.3 IT-Grundschutz des BSI.....	29
5 Regulative Forderungen in der Informationssicherheit	33
6 Integration der Forderungen des ISMS in ein IMS	37
6.1 Einführung	37
6.2 Kontext der Organisation.....	39
6.2.1 Verstehen der Organisation und ihres Kontextes	39
6.2.2 Erfordernisse und Erwartungen interessierter Parteien	39
6.2.3 Festlegen des Anwendungsbereichs des ISMS	40
6.2.4 Informationssicherheitsmanagementsystem	40
6.3 Führung	41
6.3.1 Führung und Verpflichtung	41
6.3.2 (Informationssicherheits-)Politik	41
6.3.3 Rollen, Verantwortlichkeiten und Befugnisse	42
6.4 Planung	43
6.4.1 Umgang mit Risiken und Chancen.....	43
6.4.2 Informationssicherheitsziele und Planung zur Erreichung ..	46
6.4.3 Planung von Änderungen	47
6.5 Unterstützung	48
6.5.1 Ressourcen	48
6.5.2 Kompetenz	48
6.5.3 Bewusstsein	49
6.5.4 Kommunikation.....	49
6.5.5 Dokumentierte Information.....	50
6.6 Betrieb	52
6.6.1 Betriebliche Planung und Steuerung.....	52
6.6.2 „Betrieb“ potenzielle operative Prozesse im ISMS.....	53
6.6.3 Informationssicherheitsrisikobeurteilung.....	62
6.6.4 Informationssicherheitsrisikobehandlung	63
6.7 Bewertung der Leistung	63
6.7.1 Überwachung, Messung, Analyse und Bewertung.....	63
6.7.2 Internes Audit.....	64
6.7.3 Managementbewertung.....	65
6.8 Verbesserung	67
6.8.1 Fortlaufende Verbesserung	67
6.8.2 Nichtkonformität und Korrekturmaßnahmen	68
Quellen	71

- Leseprobe -

1 Bedeutung der Informationssicherheit

Dass es auf der Welt in puncto Informationssicherheit jede Menge zu tun gibt, ist angesichts täglicher, alarmierender Meldungen über Cyberangriffe auf Unternehmen und kritische Infrastrukturen, Beeinflussung demokratischer Wahlen, Wirtschaftsspionage in Schlüsseltechnologien, Desinformationskampagnen zur Beeinflussung von Gesellschaften und anderen Unsicherheitsnachrichten wohl unstrittig. Das Umfeld, in dem Datensicherheit immer wichtiger wird, wächst von Jahr zu Jahr. Der Mensch nimmt vielfach gar nicht mehr bewusst wahr, in welchem Umfang Informations- und Datennutzung sein tägliches Umfeld prägen. Damit geraten aber häufig auch die Gefahren aus dem Blick, die mit dem Umgang mit persönlichen Daten und der Nutzung sozialer Netzwerke sowie des Internets einhergehen.

Ich möchte das an einem persönlichen Beispiel erläutern. Als jemand, der beruflich seit über 20 Jahren mehr als 50.000 km jährlich gefahren ist, und das ohne einen Kratzer am heiligen Blechle, hielt ich mich für einen guten Autofahrer, der alle Gefahren meistern kann. Dass dies eine Selbstüberschätzung war, wurde mir bei der Teilnahme an einem Fahrsicherheitstraining deutlich. Mit jedem Hütchen, das ich umwarf, schrumpfte das Selbstbewusstsein des guten Autofahrers. Als ich, trotz modernster Sicherheitstechnik, in speziellen Tests die Gewalt über mein Fahrzeug verlor und den physikalischen Kräften der Natur ungebremst und ungesteuert ausgeliefert war, kam mir die Erkenntnis, dass ich bisher nur unverdientes Glück hatte, dass mir nichts Schlimmeres widerfahren war. Es braucht manchmal solche Schlüsselmomente, um sich der Gefahren des täglichen Lebens – und dazu gehört auch das unreflektierte Nutzen der Technik – wieder bewusst zu werden. Ein Bewusstsein dafür zu entwickeln, was mit dem Begriff Informationssicherheit gemeint ist und wie wir täglich damit umgehen, ist dazu sicher der erste Schritt.

Wenn man in öffentlichen Bereichen in unfreiwillig mitgehörten Handytelefonaten ganze Familiengeschichten erfährt, mag das ja noch lustig sein, meist ist es jedoch nur lästig. Wenn man aber am Flughafen unter Nennung von Namen unweigerlich mitbekommen muss, was für ein Idiot der Einkäufer eines großen Konzerns ist und wie viel man ihm mehr „aus den Rippen geleiert hat“, als die Ware wirklich wert ist, dann werden nicht nur Grenzen des Anstands überschritten, sondern es wird bereits der Tatbestand der Geschäftsschädigung erfüllt. IT-Experten wissen, dass nach der guten alten Regel des Herrn Pareto 80 % der IT-Vorfälle nicht von Hackern oder anderen Cyberkriminellen verursacht werden, sondern von Mitarbeitern, die sich ihres Tuns nicht bewusst sind oder dessen Bedeutung unterschätzen. Die IT-Fettnäpfchen, in die wir treten können, werden von uns immer häufiger nicht mehr bewusst wahrgenommen, und leider werden die Fettnäpfchen infolge der rasanten Entwicklungsgeschwindigkeit der IT- und Medienwelt von Jahr zu Jahr mehr. Hilfreich ist da als einziges, sich regelmäßig der lauenden Gefahren des persönlichen und beruflichen Umfelds bewusst zu werden. Aus Unternehmenssicht heißt das, bewusstseinsfördernde Maßnahmen zur Verbesserung der Informationssicherheit als einen stetigen Prozess zur Mitarbeitersensibilisierung zu begreifen.

Was gehört alles zu den Informationen und Daten, die geschützt werden müssen, und wer fordert das? Darauf gibt es mehrere Antworten. Zu den Interessenten an Informationsschutzmaßnahmen gehören zum einen die Organisation selbst, aber auch interessierte Parteien der Organisation wie Kunden oder der Gesetzgeber. Laut Definition ist Informationssicherheit der Schutz von Informationen einer Organisation, egal welcher Art oder Herkunft. Darunter fallen alle sensiblen Informationen und Daten, die vor unbefugten oder vorsätzlichen Handlungen, Zugriffen oder Manipulationen anderer geschützt werden müssen, um wirtschaftliche und Reputationsschäden zu vermeiden. Darüber hinaus zählt zur Informationssicherheit auch der Schutz vor höherer

**Bewusstsein
entwickeln**

**Selbst verursachte
Vorfälle**

Was schützen?

Kleines Ereignis, große Auswirkung

Gewalt wie Feuer, Wasser, Erdbeben usw., die einen Verlust von Daten und/oder die Unterbrechung von wichtigen Datenverbindungen bewirken können.

Ein Beispiel ist der temporäre Verlust der Datenautobahnen im Großraum Frankfurt und am Frankfurter Flughafen, weil ein Bagger auf einer Baustelle zufällig ein zentrales Glasfaserkabel unterbrochen hat. Die Folgen waren lokal wie global zu spüren. Im Großraum Frankfurt konnten viele Firmen, so auch die Lufthansa, nicht mehr auf ihr Datennetzwerk zugreifen. Die unmittelbare Folge: Es konnten keine Starts und Landungen von Frankfurt aus mehr stattfinden, und es mussten temporär auch alle Flüge nach Frankfurt abgesagt oder umgeleitet werden. Da Frankfurt eines der großen Luftfahrt-drehkreuze dieser Welt ist, hatte das lokale Ereignis weltweite Auswirkungen auf den Flugverkehr.

Solche Zufallsereignisse machen deutlich, dass eine funktionierende IT unabdingbar für das Funktionieren unserer vernetzten Welt ist und ein Ausfall – aus welchen Gründen auch immer – unser Leben temporär durcheinanderbringt. Staatliche Stellen und große Firmen beschäftigen sich schon lange mit dem Thema kritische Infrastruktur und allem, was dazu gehört. Strom- und Energieversorgung ebenso wie Lebensmittel- und Wasserversorgung und vieles mehr hängen von einer funktionstüchtigen IT-Infrastruktur ab.

Kritische Naturkatastrophen

Das Ereignis lehrt uns, dass wir immer noch nicht alle kritischen Stellen unserer Infrastruktur kennen und auch keine ausreichenden Möglichkeiten geschaffen haben, damit konstruktiv umzugehen. Damit sind wir bei dem bekannten Spruch der Zahnärzte: „Vorbeugen ist besser als Bohren.“ Leider fehlt es allzu oft an der Bereitschaft zur notwendigen Vorbeugung getreu dem Artikel 3 des Kölner Grundgesetzes: „Et hätt noch emmer joot jejange“ (Es ist bisher noch immer gut gegangen). Wissenschaftler warnen schon lange, dass die Probleme mit der Funktionsfähigkeit kritischer Infrastruktur infolge des Klimawandels und der damit verbundenen Extremwetterereignisse wie Überschwemmungen, Stürme, Erdbeben und vieles mehr nicht kleiner werden. Zudem bleiben uns bekannte Risiken wie Erdbeben oder Vulkanausbrüche auch weiter erhalten. Die Auswirkung unzureichender oder gestörter Informationsübermittlung auf die Rettungsaktivitäten im Erdbebengebiet Türkei/Syrien sind noch nicht alle bekannt, werden im Nachhinein aber sicher noch untersucht werden. Die Zahl der Toten dieser Naturkatastrophe ist erschreckend hoch. Die Frage, wie viele der Opfer noch leben könnten, wenn die notwendigen Informationen zu ihrer Rettung sicher und zeitnah zur Verfügung gestanden hätten, wird wohl nie beantwortet werden.

Gezielt ausgeführte Ereignisse

In noch größerem Umfang gehen Gefahren für die Informationssicherheit von menschengemachten Ereignissen aus. Die Motive sind vielfältig und betreffen ggf. nur einzelne Personen, Firmen und Organisationen bis hin zu staatlichen Institutionen. Auch die Gründe sind vielfältiger Natur: kriminelle Aktivitäten aus Habgier, Diebstahl von geistigem Eigentum und Know-how bis hin zur Beeinflussung der öffentlichen Meinung durch Desinformation und von demokratischen Institutionen (Wahlen). Damit ist die Liste der Grausamkeiten gegen die Informationssicherheit aber noch nicht zu Ende. Die gezielte Störung von kritischer Infrastruktur und der Funktionsfähigkeit von Organisationen mit großer gesellschaftlicher Relevanz wie Unternehmen der Energie- und Wasserversorgung oder Krankenhäusern und Ministerien ist heute Teil der hybriden Kriegsführung, deren Akteure staatliche Stellen oder von staatlichen Stellen geförderte Gruppen sind.

Fehlende Ressourcen kleinerer Akteure

Neben der großen Bühne internationaler Akteure gibt es noch die kleineren Bühnen der großen, mittleren und kleinen Unternehmen und deren Status in der Informationssicherheit. Während sich weltweit agierende Konzerne große IT-Abteilungen leisten können und in ihren Unternehmen einen gewissen Standard an Informationssicherheit und darin eingeschlossen der IT-Sicherheit implementiert haben, ist es bei kleinen und mittelständischen

Unternehmen meist nicht so gut um die Informationssicherheit bestellt. Ein besonderer Schwachpunkt ist dort das Fehlen von Redundanz im personellen wie soft- und hardwaretechnischen Bereich. Verluste bei diesen meist knappen Ressourcen ziehen dann häufig automatisch schwerwiegende Folgen auch in anderen Bereichen des Unternehmens nach sich.

Meist ist es so, dass es nicht nur eine Ursache gibt, wenn Sicherheitsvorkehrung nicht greifen oder versagen, sondern mehrere unglückliche Zufälle gleichzeitig ihre unselige Wirkung entfalten. Die Folgen können Diebstahl von Firmengeheimnissen oder Datenverlust sein, ggf. sind nicht nur die eigenen Daten betroffen, sondern auch die von Kunden, Lieferanten und Geschäftspartnern.

Nachfolgend eine Liste wesentlicher Ursachen bzw. Faktoren:

- Unzureichende Strategie zur Informationssicherheit, weil der Stellenwert des Schutzes von Informationen und Daten nicht realistisch eingeschätzt wird.
- Fehlende Prozesse zur Aufrechterhaltung und Verbesserung eines bestehenden Schutzniveaus. Informationssicherheit ist kein statischer Zustand, sondern entwickelt sich rasant weiter.
- Unzureichende Dokumentation von Informationssicherheitsvorgaben, weil z. B. nicht aktuell, unvollständig, nicht offiziell in Kraft gesetzt, schlecht kommuniziert oder schlicht ignoriert.
- Fehlende Kontrollmechanismen lassen Fehlentwicklungen erst spät oder zu spät erkennen, und fehlende Aufklärung und Sanktionen im Fall von Verstößen verringern die Akzeptanz von Regeln.
- Lückenhafte Konfiguration und Administration von IT-Systemen aufgrund falsch definierter Rollen und unwirksamer Restriktionen bei fehlerhaftem Handeln.
- Unsichere Konfiguration von IT-Systemen, die fehlerhaftes Handeln von Nutzern unerkannt zulassen.
- Nicht gesicherte Vernetzung und Internetanbindung sowie unzureichende Abschottung sensibler IT-Systeme infolge von Konfigurationsfehlern oder wegen unzureichend geschulter Systemadministratoren.
- Nichtbeachtung von Sicherheitserfordernissen oder Vernachlässigung von festgelegten Sicherheitsmaßnahmen (z. B. unverschlüsselter Mailverkehr oder keine wirksame Zutrittskontrolle).
- Einsatz von nicht ausreichend geschulten Anwendern oder Systemadministratoren, die mögliche Infiltration zulassen oder durch fehlerhaftes Handeln ermöglichen.
- Die Wartung von IT-Systemen wird vernachlässigt, weil Wartungsarbeiten nicht oder nicht zeitnah durchgeführt werden, sei es durch Unterlassen oder verspätetes Aufspielen von Sicherheits-Updates.
- Auch der sorglose Umgang mit Passwörtern (z. B. Weitergabe von Passwörtern, nicht ausreichend komplexe Passwörter) öffnet Gefährdungen für die IT-Netzwerke.
- Gebäude und Räume werden nur unzureichend gegen unbefugtes Eindringen oder das Auftreten von Elementarschäden (z. B. Brand, Wasserschäden) geschützt.

Die Liste von Versäumnissen, z. B. falscher Mitteleinsatz, unzureichendes Personal (qualitativ wie quantitativ), nicht Ernstnehmen der Bedrohung, und anderer die Informationssicherheit gefährdender Unterlassungen könnte noch erheblich verlängert werden und wird voraussichtlich auch nie vollständig sein, da sich die IT-Welt mit rasender Geschwindigkeit ändert.

Ursachen

Vom Problem zur Lösung

An dieser Stelle muss man sich die Frage stellen, wie man das Problem löst, denn es ist unstrittig, dass viele Organisationen und Unternehmen beim Thema Informationssicherheit ein mehr oder weniger großes Problem haben. Gemäß einer Definition ist ein Problem der Unterschied zwischen einem Ist-Zustand und einem Soll-Zustand, bei dem uns der Lösungsweg (noch) nicht bekannt ist. Damit ist geklärt, wie man von einem Problem zu einer (lösbaren) Aufgabe kommt. Man benötigt einen Lösungsansatz, der die in der Aufzählung genannten Probleme beseitigt. Ein Instrument, das wir alle kennen und das eine erprobte Lösung für diese Probleme bietet, ist ein Managementsystem.

Digitale und physikalische Sicherheit

Seit 2005 gibt es die ISO/IEC 27001 als zertifizierbaren Standard zum Informationssicherheitsmanagement. Zurzeit ist die zweite Revision der ISO/IEC 27001:2022 „Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsystem – Anforderungen“ [1] gültig.

Mit welchen Themen beschäftigt sich das Informationssicherheitsmanagementsystem nach dieser ISO-Norm? Grob kann man zwei große Themen nennen, in die sich Informationssicherheit gliedert. Die digitale Sicherheit, die unter dem Begriff IT-Sicherheit gefasst wird, und die physikalische Sicherheit, die sich vom gesprochenen Wort über dokumentierte Informationen bis hin zu Betriebsstätten und -einrichtungen erstreckt.

Wichtige Themen der Sicherheit

Eine nicht abschließende Zusammenstellung der wichtigsten Themen, die der Informationssicherheit zugeordnet werden können, zeigt Abbildung 1.

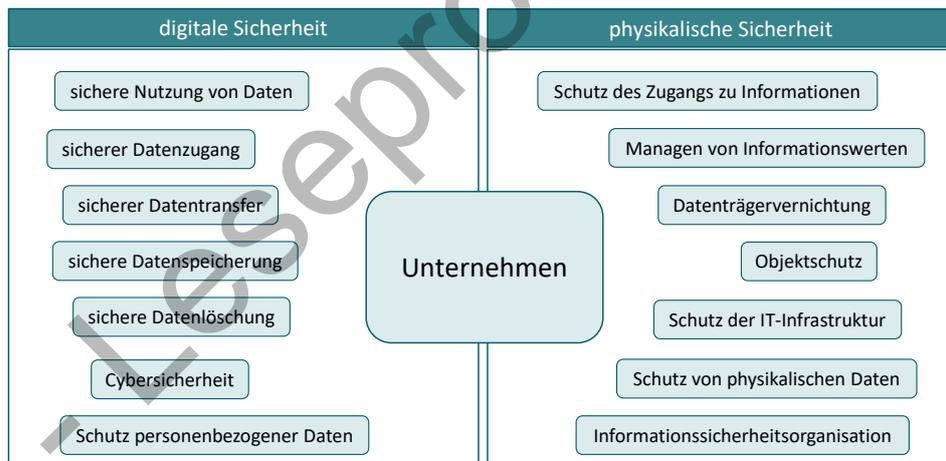


Abb. 1: Themenbeispiele zur Informationssicherheit

Hilfestellung des BSI

Wertvolle Hilfestellung zu den oben genannten Themen bietet auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) [2] an. Rund um die Informationstechnologie werden Organisationen und Unternehmen in vielen Broschüren und Regelwerken sowie Schulungen Lösungen zu Fragen wie sichere Datenspeicherung oder sicherer Datentransport angeboten. Vieles davon wird unentgeltlich oder für geringe Unkostenbeiträge dem interessierten Nutzer zur Verfügung gestellt. Es mangelt also nicht an den richtigen Informationen, woran es häufig mangelt, ist die Bereitschaft, diesem Thema in der Hierarchie der Unternehmensaktivitäten die notwendige Bedeutung beizumessen.

Vernachlässigtes Thema

Informationssicherheit ist wie Rechtskonformität oder Nachhaltigkeit ein Thema, das zwar bekannt ist, dass aber häufig scheinbar nichts mit dem eigentlichen Geschäftszweck der Organisation zu tun hat. Man verdient damit kein Geld, sondern es kostet erst einmal Geld. Das Thema zu vernachlässigen kann im Schadensfall aber noch sehr viel mehr Geld kosten. Denken Sie an eine Versicherung, die nicht mehr auf ihre Kundendaten zugreifen kann, ein

Krankenhaus mit blockierten Patientendaten oder ein Hightech-Unternehmen, dem seine neuesten Forschungsergebnisse abhanden kommen. Die möglichen Folgen sind u. a. gravierende Imageschäden oder große monetäre Verluste, und im schlimmsten Fall sind Menschenleben zu beklagen. Die weltweite Vernetzung von Produktions- und Sicherheitssystemen und künstliche Intelligenz (KI) werden dem Thema Informationssicherheit noch einmal einen riesigen Bedeutungsschub verleihen.

Informationssicherheit war mal leicht, vor Jahrzehnten, als Computerviren in überschaubarer Anzahl und Hacker noch sehr selten anzutreffen waren. Das Internet war zu diesem Zeitpunkt für viele so weit weg und unbekannt wie die Rückseite des Mondes. Zukünftige Generationen werden diese Epoche wohl als das analoge Zeitalter bezeichnen. Es hat nur wenige Jahrzehnte gebraucht, um das digitale Zeitalter zu etablieren. Inzwischen verbringen die Menschen im Internet mehr Zeit als mit Schlafen, und keiner denkt mehr darüber nach. Das Internet verbindet heute alles auf dieser Welt, im Guten wie im Schlechten. Es liegt an uns, was wir daraus machen und welche Folgen es für uns und andere hat, wenn wir zu wenig oder nichts tun.

Nach Aussage des Cybersicherheitsexperten Christian Dörr (Leiter des Fachgebiets Cybersecurity/Enterprise Security am Hasso-Plattner-Institut in Potsdam) entsteht in Deutschland zurzeit jährlich ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten sowie Spionage und Sabotage. Seit dem Ukraine-Krieg nehmen die Cyberangriffe durch staatliche oder staatlich gelenkte Akteure stark zu; im Netz herrscht an vielen Stellen Krieg. Davon betroffen sind alle Bereiche der Wirtschaft und Gesellschaft.

Digitales Zeitalter**Enorme Schäden**

- Leseprobe -

- Leseprobe -

2 Ziel und Zweck der ISO/IEC 27001:2022

Zweck der ISO/IEC 27001:2022 sind die Errichtung, Umsetzung und kontinuierliche Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS) in privaten, öffentlichen oder gemeinnützigen Organisationen. Das Ziel der Norm ist dabei, Sicherheit bezüglich aller Arten von Informationen zu gewährleisten. Da stellt sich die Frage: Kann es absolute Sicherheit auf dieser Welt überhaupt geben? Eine Antwort darauf gibt uns der Schriftsteller und Kabarettist Joachim Ringelnatz: „*Sicher ist, dass nichts sicher ist. Selbst das nicht.*“ Er relativiert mit seiner zweiten Aussage seine erste Aussage. Daraus kann man folgern, dass Sicherheit kein Zufallsprodukt, sondern gestaltbar ist und dass man sich gegen negative Einwirkungen in der Informationssicherheit durch proaktives Handeln wirksam schützen kann. Proaktives, also vorausschauendes Handeln kennen wir auch unter dem Begriff Vorbeugung.

Ein weltweit anerkanntes und erprobtes Werkzeug der gezielten Vorbeugung sind Managementsysteme. Sie setzen Regeln, deren Beachtung Strukturen schafft, die negative Zufallsprodukte verhindern sollen. Das wichtigste Werkzeug dafür ist die Planung. Der deutsche Wirtschaftswissenschaftler Günter Wöhe beschreibt Planung als „*die gedankliche Vorwegnahme zukünftigen Handelns durch Abwägen verschiedener Handlungsalternativen und Entscheidungen für den günstigsten (oder sichersten) Weg*“. Planung bedeutet also das Treffen von Entscheidungen, die für die Zukunft etwas verbessern sollen. Dieser Grundsatz lässt sich auf alle Themenstellungen der Welt beziehen, auch auf die Informationssicherheit.

Eines ist heute schon sicher: Die Bedeutung der ISO/IEC 27001 wird weiter zunehmen, da „elektronische Daten“, ihre Speicherung, Verarbeitung und der Transport die Lebensader vieler Organisationen sind. Ohne entsprechende Sicherheit ist man in unserer vernetzten Welt sehr verletzlich gegenüber Hackerangriffen und Datenspionage von außen. Regierungen, Organisationen und Unternehmen können ins Wanken geraten, wenn ihre Daten in falsche Hände geraten oder der Datentransfer gestört wird. Daher hat die Revision im Jahr 2022 dem Thema Cybersicherheit besondere Aufmerksamkeit geschenkt. Dies geht auch schon aus dem neuen Titel „Informationssicherheit, Cybersicherheit und Datenschutz“ hervor (alt: Informationstechnik – Sicherheitsverfahren). Die zweite inhaltliche Erweiterung der Revision betrifft das Thema des Datenschutzes, der aus guten Gründen weltweit immer stärker gesetzlichen Regulierungen unterliegt.

In einem integrierten Managementsystem (IMS) aus mehreren Managementsystemen übernehmen die Forderungen der ISO/IEC 27001 Querschnittsfunktionen in allen Geschäftsprozessen einer Organisation. Es gibt keinen Managementsystemprozess, der ohne Informationen und Daten auskommt, daher ist die Sicherheit dieser Informationen und Daten auch in einem IMS allgegenwärtig.

In der heutigen globalisierten Welt sind nicht mehr nur Betriebsmittel, Infrastruktur, Material und Waren Gegenstände, die den monetären Wert eines Unternehmens ausmachen. Software, IT-Dienstleistungen, Wissen und Informationen bestimmen heute häufig stärker den Wert eines Unternehmens als die Bilanz. Die großen Technologiefirmen haben Börsenwerte, die die körperlichen Werte in der Bilanz um ein Vielfaches übertreffen. Auch der Erfolg eines Unternehmens hängt nicht mehr nur von der Qualität seiner Produkte oder Dienstleistungen, sondern in immer größerem Umfang von den zur Verfügung stehenden Daten und Informationen ab (z. B. Google oder Amazon). Die Mengen an nutzbaren Daten und die Möglichkeiten sowie die Geschwindigkeit ihrer Verarbeitung bestimmen immer häufiger den Markterfolg. Die Aufgabe, diese Werte zu schützen und zu mehren, wird heute meist professionell vom Assetmanagement (Wertemanagement) übernommen.

Vorbeugung

Management-systeme

Informationssicherheit, Cybersicherheit und Datenschutz

IMS