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

TÜVRheinland
Genau. Richtig.

Autor:

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

Bibliografische Informationen der Deutschen Nationalibliothek
Die Deutsche Nationalibliothek 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)

Zur Nutzung der Broschüre

Daten, Daten, Daten

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.

Zielsetzung der Broschüre

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.

Managementsystemnorm

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.

Rechtsvorschriften

Kein Managementsystem der ISO kommt ohne die Berücksichtigung regulativer 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.

Integrieren und Synergien nutzen

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, dass 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.

Arbeitshilfen

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.

Verweismatrix_ 27001_neu_alt.xlsx

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_ 9001_14001_ 45001_27001.xlsx

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.

Kompatibilitäts- matrix_IMS.xlsx

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.

ISRA_Nohl.xlsx

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.

SoA.xlsx

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.

Nachweise.xlsx

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

Download

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

www.qm-aktuell.de/60854-2/

Passwort: **23150**

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

Inhalt

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.

Bewusstsein entwickeln

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.

Selbst verursachte Vorfälle

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 lauernden 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 schützen?

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

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

Kleines Ereignis, große Auswirkung

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 Luftfahrtdrehkreuze 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, Erdrutsche 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