IN DIESEM KAPITEL

Bausteine der Informationssicherheit

Grundlegende Konzepte

Abgrenzung zur IT-Sicherheit und zum Datenschutz

Kapitel 1
Verständnis von Informationssicherheit – Basiswissen

Motivation

Wir alle leben in einer Welt, die von raschen technologischen Fortschritten und globalen Vernetzungen geprägt ist. Deshalb stellt Informationssicherheit eine entscheidende Komponente unseres täglichen Lebens und unserer Arbeitswelt dar. Die Gründe, sich mit Informationssicherheit zu beschäftigen, sind zahlreich und in der aktuellen Sicherheitslage wichtiger denn je. Sicher können Sie zu diesen allgemeinen Gründen ein paar individuelle ergänzen.

1. Schutz vor Bedrohungen in einer vernetzten Welt: In einer Ära, in der praktisch alles online ist, sind wir einem breiten Spektrum von Cyberbedrohungen ausgesetzt. Hacker, Malware und Phishing-Angriffe sind an der Tagesordnung. Ohne angemessene Informationssicherheitsmaßnahmen könnten unsere persönlichen Daten, Finanzen und sogar unser Ruf gefährdet sein.

2. Datenschutz und Compliance: Gesetze und Vorschriften zur Privatsphäre, wie die Datenschutzgrundverordnung (DSGVO) in Europa, verlangen von Organisationen, die persönliche Daten verarbeiten, strenge Sicherheitsvorkehrungen. Nichteinhaltung kann zu erheblichen Geldstrafen führen. Mit Sicherheitsstandards wie ISO 27001 können Unternehmen dazu beitragen, dass sie die gesetzlichen Anforderungen einhalten.

3. Vertrauen unserer Kunden und Partner: In einer Zeit, in der Vertrauen ein kostbares Gut ist, ist Informationssicherheit der Schlüssel. Kunden und Geschäftspartner verlassen sich darauf, dass ihre Daten in sicheren Händen sind. Eine robuste Informationssicherheitsstrategie stärkt das Vertrauen und fördert die langfristigen Beziehungen.

4. Kontinuierliche Verbesserung und Anpassung: Die Welt der Informationssicherheit ist ständigen Veränderungen unterworfen. Hacker entwickeln kontinuierlich neue Taktiken, um Sicherheitsmaßnahmen zu umgehen. Eine proaktive Einstellung zur Informationssicherheit ermöglicht es Unternehmen, sich anzupassen und innovative Lösungen zu entwickeln, um mit den neuesten Bedrohungen Schritt zu halten.

5. Geschäftskontinuität: Sicherheitsvorfälle und Datenverluste können verheerend sein. Eine gut durchdachte Informationssicherheitsstrategie, einschließlich Notfall- und Wiederherstellungsplänen, trägt dazu bei, die Geschäftskontinuität sicherzustellen und Ausfallzeiten zu minimieren.

6. Schutz geistigen Eigentums: Unternehmen investieren erhebliche Ressourcen in Forschung und Entwicklung. Informationssicherheit schützt nicht nur sensible Daten, sondern auch geistiges Eigentum vor Diebstahl oder Spionage.

7. Schutz der nationalen Sicherheit: Die Auswirkungen von Sicherheitsverletzungen können weitreichender sein als nur wirtschaftliche Verluste. Nationale Sicherheit und kritische Infrastrukturen sind von Informationssicherheit abhängig, um potenzielle Bedrohungen abzuwehren. In Bereichen sogenannter »kritischer Infrastrukturen« ist Informationssicherheits-Management daher sogar gesetzlich vorgeschrieben.

In einer Zeit, in der unsere Abhängigkeit von digitalen Technologien immer größer wird, ist die Motivation, sich mit Informationssicherheit zu beschäftigen, klar und zwingend. Es geht nicht nur darum, sich vor Bedrohungen zu schützen, sondern auch darum, Vertrauen aufzubauen, die Einhaltung von Gesetzen sicherzustellen und eine widerstandsfähige Zukunft zu gestalten. Informationssicherheit ist kein Luxus, sondern eine Notwendigkeit, die unser tägliches Leben und unsere digitale Zukunft gestaltet.

Dabei sollte klar sein, dass es hundertprozentige Sicherheit nicht gibt und diese auch nicht Ziel sein sollte. Die Welt der IT ist dafür viel zu schnelllebig, und es gibt viel zu viele Facetten, die gar nicht bis ins Detail adressiert werden können. So sind beispielsweise Sicherheitslücken in eingesetzter Software oder sogar in Sicherheitsprodukten nicht unüblich, und es können jeden Tag neue entdeckt werden.

Außerdem wäre hundertprozentige Sicherheit quasi »unbezahlbar« und sicherlich unwirtschaftlich. Aber es geht genau darum, systematisch beispielsweise auf solche Sicherheitslücken zu reagieren und über mehrere Stufen von Sicherheitsmaßnahmen es umso schwerer zu machen, dass ein potenzieller Angreifer ans Ziel kommt.

Dabei geht es ganz besonders auch um den Faktor Mensch, der mitunter eines der größten Einfallstore darstellt, sodass sich der ganzheitliche Ansatz auch mit viel Managementthemen befasst. Es geht also um organisatorische Vorgaben wie Leitlinien und Richtlinien, Prozessabläufe und Verfahrensanweisungen, Schulung und Sensibilisierung neben natürlich auch physischen und technischen Maßnahmen zur Sicherstellung der Informationssicherheit.

Weigert721856_c01.indd 32 Trim Size: 176 × 240 mm 05 Feb. 2025 04:48:36 nachm.

Das Ausnutzen von Menschen oder dem »Faktor Mensch« wird als »Social Engineering« bezeichnet. Social Engineering ist eine Form der Manipulation, bei der Angreifer psychologische Tricks anwenden, um Menschen dazu zu bringen, sicherheitsrelevante Informationen preiszugeben oder entsprechende Handlungen vorzunehmen. Durch das Schaffen von mehr Verständnis und durch die Anwendung geeigneter Schutzmaßnahmen können Sie Einzelpersonen und Organisationen besser gegen diese Art von Angriffen schützen.

Entsprechend ist die Norm ISO 27001 zunächst ein Managementwerkzeug und beinhaltet vor allem dazu passende Bausteine, mit denen Sie diese Managementthemen adressieren können. Daneben gibt es einen Katalog an Sicherheitsmaßnahmen (Anhang A), die quasi wie eine Art Grundsicherung zu verstehen sind. Es ist essenziell, dass das Management, also die Geschäftsführung, hinter der Einführung einer ISO 27001 beziehungsweise einem ISO 27001-Projekt steht. Das kann die Geschäftsführung natürlich auch tun, indem sie nur dem designierten Informationssicherheitsteam freie Hand lässt und sonst operativ nicht stark in Erscheinung tritt. Allerdings wird erwartet, dass das Management den Rahmen vorgibt, Informationssicherheit vorlebt und die Mitarbeiter motiviert, sich dem Thema anzunehmen, und nachvollziehbar erklärt, warum das Thema für das Unternehmen und für die Kunden so wichtig ist. Dabei ist es hilfreich, wenn Mitarbeitervertretungen oder Mitarbeiter, die positiv auf das Team einwirken, mit an Bord sind und die Umsetzung mit ausgestalten.

Informationen

Offenbar geht es bei Informationssicherheit um die Sicherheit von Informationen. Doch was sind eigentlich Informationen? Dieser Begriff umfasst alle Arten von Informationen oder Daten, die in einem bestimmten Kontext Bedeutung haben und für uns deshalb irgendeinen Wert darstellen. Zum Beispiel weil wir sie zur Entscheidungsfindung verwenden müssen.

Sie können Informationen in vielen verschiedenen Formen speichern, als Texte, Zahlen, Bilder, Töne, Videos oder andere Darstellungen, aber auch ganz immateriell in Form von Wissen oder Erkenntnissen in unseren Köpfen.

Gerne unterscheidet man Daten und Informationen in ihrer Definition. Dabei nimmt man an, dass es sich bei Daten um die reinen Zahlen oder Buchstaben ohne Kontext handelt, die dann erst durch Kontext und Bedeutung zu Informationen werden. Wenn Sie diese Informationen mit Erfahrung und Verständnis kombinieren, spricht man von Wissen.

- ✔ **Daten:** Rohdaten sind rohe Fakten und Zahlen ohne Kontext. Zum Beispiel kann eine Liste von Zahlen wie 23, 42, 17 einfach als Daten betrachtet werden.
- ✔ **Informationen:** Wenn diese Daten in einen Kontext gesetzt werden und Bedeutung erhalten, werden sie zu Informationen. Zum Beispiel kann die Information »Die Durchschnittstemperatur im Juli betrug 23 Grad Celsius« aus den rohen Daten abgeleitet werden.

- **Wissen:** Wissen ist die Verinnerlichung und Anwendung von Informationen durch Erfahrung, Lernen und Verständnis. Wissen ermöglicht es, Informationen effektiv zu nutzen und darauf basierende Handlungen zu treffen.

In Organisationen und Unternehmen liegen Informationen in drei verschiedenen Ausführungen vor:

- Digital: Digitale Informationen sind alle Informationen, die durch elektronische Geräte (IT) gespeichert, verarbeitet und übertragen werden. In der Regel werden die meisten Informationen in Unternehmen IT-unterstützt verarbeitet. Beispiele sind Dateien auf Festplatten oder die Dokumentation in einer Webanwendung.
- Analog: Analoge Informationen repräsentieren Daten in physischer Form. Die meisten analogen Informationen liegen in Form von Papier vor. Beispiele sind gefüllte Aktenordner oder handschriftliche Notizen.
- Immateriell: Immaterielle Informationen sind nicht physisch greifbar und existieren als Fachwissen, Konzepte oder Ideen in unseren Köpfen. Sie können sowohl digital als auch analog dargestellt werden, haben aber keinen eigenen materiellen Zustand. Beispiele können neben reinem Wissen auch Patente, Urheberrechte und Geschäftsstrategien sein.

Diese Unterscheidung gilt auch für die Übermittlung von Informationen. Sie können Informationen digital, per E-Mail oder über das Internet austauschen, analog per Post verschicken oder mündlich im Gespräch mitteilen. Denken Sie bei Informationen nicht nur an Text, sondern auch an Grafiken, Bilder und Audio-/Video-Aufzeichnungen. Die »Wordcloud« in Abbildung 1.1 stellt einige Arten von Informationen grafisch aufbereitet dar.

Abbildung 1.1: Zahlreiche Informationen lassen sich in allen Organisationen finden.

Informationswerte (Assets)

Informationen sind für uns wertvoll und müssen deshalb angemessen geschützt werden. Man spricht deshalb auch von Informationswerten, im englischen »information assets«.

ISO 27000 (zu dieser Norm erfahren Sie später noch mehr) fasst es in Kapitel 4.1 hervorragend zusammen:

Organisationen jeder Art und Größe:

- ✔ sammeln, verarbeiten, speichern und übermitteln Informationen;
- ✔ betrachten Informationen und zugehörige Prozesse, Systeme, Netzwerke und Personen als wichtige Werte, die für das Erreichen der Organisationsziele notwendig sind;
- ✔ sind mit einer Reihe von Risiken konfrontiert, welche die Funktionsfähigkeit von Werten beeinträchtigen können; und
- ✔ begegnen ihrem bekannten Gefährdungspotenzial mit der Einführung von Informationssicherheitsmaßnahmen.

Alle Informationen sind einer Reihe von Gefahren ausgesetzt, sei es durch externe, physische Einflüsse wie Feuer oder Überschwemmungen, Diebstahl durch Hacker oder weil sie ganz einfach verloren gehen könnten. Unser Ziel ist es, unsere Informationen dementsprechend zu schützen.

Und da nicht nur die Informationen selbst, sondern auch die verarbeitenden Medien und Systeme wie Laptops, Server, Schränke und Mitarbeitende geschützt werden müssen, ist oft allgemein von »Assets«, also Werten, die Rede. Alles, was für Sie irgendeinen Wert hat, steht auch in Zusammenhang mit Informationen und ist daher vom Thema Informationssicherheit betroffen. Dazu gehören auch die klassischen Vermögenswerte von Unternehmen, wie Anlagen oder Maschinen. Später werden Sie diese Assets einer Bewertung unterziehen, um den Wert aus Sicht der Informationssicherheit zu ermitteln.

Wenn Sie Ihre Assets in Kategorien einteilen, stellen Sie häufig eine Kaskade fest. Informationen werden von Software verarbeitet, Software läuft auf Hardware, Hardware befindet sich in einem Raum, der Raum befindet sich in einem Gebäude und dieses Gebäude befindet sich auf Ihrem Firmengelände. Wenn Sie nun betrachten, welche dieser Kategorien den höchsten Schutzbedarf hat, stellen Sie vielleicht fest, dass es sich dabei um so etwas wie Ihr Rechenzentrum handelt. Das ergibt Sinn, da dort die größte Menge an Informationen zusammenläuft. Man spricht in diesem Fall auch von der Vererbung des Schutzbedarfs vom eigentlichen Information Asset zu den unterstützenden Assets.

Beispiele für Asset-Kategorien sind:

- ✔ **Informationen:** sensible Daten, vertrauliche Geschäftsinformationen, Kundendaten
- ✔ **Geschäftsprozesse:** Arbeitsabläufe, Produktionsprozesse, Supportprozesse

- ✔ **Dienstleistungen:** Cloud-Dienste, externe IT-Dienstleister
- ✔ **Dokumente:** Verträge, Handbücher, Richtlinien
- ✔ **Software:** Anwendungen, Betriebssysteme, Datenbanken
- ✔ **Hardware:** Server, Computer, Netzwerkequipment
- ✔ **Infrastruktur:** Gebäude, Büroräume, Rechenzentren
- ✔ **Personen:** Mitarbeiter, externe Dienstleister, Partner

Informationssicherheit

Informationssicherheit umfasst viele Themenfelder und ist gar nicht so einfach zu fassen. Umso wichtiger ist es, den Begriff und die zugehörigen Details zu definieren. Viele Begriffe klingen ähnlich oder werden – oft fälschlicherweise – synonym verwendet. Gemeinsamkeiten und Unterschiede hängen auch vom Kontext ab und können sich von Organisation zu Organisation unterscheiden. Die Begriffsdefinitionen der ISO-Norm decken sich weitestgehend mit anderen Definitionen aus der entsprechenden Fachliteratur. Daneben gibt es auch weitere Definitionen aus der Gesetzgebung.

Informationssicherheit ist also ein Überbegriff und lässt sich in weitere Teilbereiche unterteilen. Abbildung 1.2 bietet hierfür einen Überblick. So handelt es sich beispielsweise bei IT-Sicherheit um einen solchen Teilbereich und keinesfalls um dasselbe.

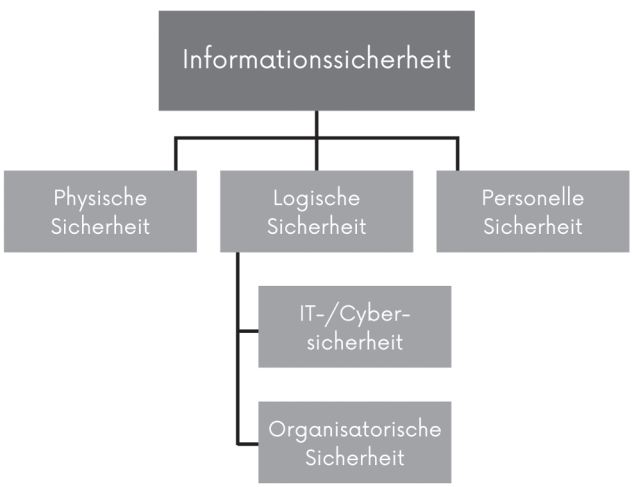

Abbildung 1.2: Informationssicherheit ist ein breites Feld und lässt sich in viele Teilbereiche zerlegen.

IT-Sicherheit

Informationstechnologie, kurz IT, umfasst alle technischen Systeme, die irgendwie Informationen verarbeiten. Im deutschen Sprachgebrauch findet sich noch gelegentlich die

Abkürzung EDV für elektronische Datenverarbeitung. Dieser leicht angestaubte Begriff wird synonym verwendet, in der Fachliteratur aber häufig auch nur für den Softwareteil der IT verwendet, während IT als gesamter, umfassenderer Überbegriff auch Hardware miteinschließt.

Beispiele für typische IT-Systeme sind Endanwendergeräte wie Laptops, Smartphones oder Tablets und Geräte zur Steuerung von IT wie Server, Router oder Switches.

IT-Sicherheit betrifft ausschließlich den Schutz dieser Systeme und Geräte, ist also eine eher technische Disziplin – und damit ein Teilbereich der Informationssicherheit. Da die meisten Informationen, die in Unternehmen und Organisationen verarbeitet werden, IT-unterstützt verarbeitet werden, handelt es sich in der Regel um den größten Teilbereich der Informationssicherheit. Oft auch um den wichtigsten. Dennoch ist es falsch, die beiden Begriffe gleichzusetzen. Genauso falsch und zu klein gedacht wäre es, das Thema Informationssicherheit im Unternehmen in die Verantwortung der IT zu geben.

Viele Unternehmen denken fälschlicherweise, dass es sich bei Informationssicherheit um IT-Sicherheit handelt, und gehen davon aus, dass sich das Thema technisch lösen lässt, zum Beispiel mit dem Kauf einer Software oder mit dem Einsatz neuester Technologie.

Da die gesetzlichen Anforderungen an Informationssicherheit in Unternehmen weiter zunehmen (zuletzt mit der NIS-2 Richtlinie), hört man häufiger Stimmen wie »Wir brauchen hier nichts zu tun, alle unsere Daten sind verschlüsselt« oder »Unsere Daten liegen doch in einem zertifizierten Rechenzentrum«. Die Verschlüsselung von Daten und die Zertifizierung von Rechenzentren sind sicher wichtige Bausteine oder Maßnahmen innerhalb der IT-Sicherheit und damit auch für die Informationssicherheit von bedeutendem Wert. Aber es ist damit nicht getan.

Blickt man in die Norm ISO 27001, so stellt man schnell fest, dass dort auch von physischen Sicherheitsthemen (zum Beispiel die Zutrittskontrolle) oder organisatorischen Themen (zum Beispiel der HR-Einstellungsprozess) die Rede ist. Und alle Maßnahmen müssen kontrolliert und gesteuert, also gemanagt, werden. Durch den Kauf einer neuen Firewall können Sie nicht nachweisen, dass Sie die Informationssicherheit in Ihrem Unternehmen im Griff haben.

Der deutsche Gesetzgeber hat in der Vergangenheit zu diesen falschen Annahmen leider beigetragen, indem die Notwendigkeit von Informationssicherheit in manchen Unternehmen im Rahmen des »IT-Sicherheitsgesetzes« 2021 eingeführt wurde. Aktuell wird allerdings angestrebt, den Begriff IT-Sicherheit in deutschen Gesetzen und Normen durch Informationssicherheit zu ersetzen.

Datensicherheit

Ein Begriff, der ähnlich angestaubt klingt wie die Abkürzung EDV, ist Datensicherheit. Hier gibt es sowohl Verwechslungsgefahr zur Informationssicherheit als auch zum Datenschutz. Datenschutz wird in diesem Kapitel noch gesondert erläutert. Im Rahmen der

Informationssicherheit wollen wir alle Arten von Informationen in jeglicher Form schützen. Daten bezeichnen häufig nur elektronisch verarbeitete Informationen und damit nur einen Teil der zu schützenden Informationen. Auch dieser Begriff geht daher nicht weit genug. Datensicherheit kann synonym zu IT-Sicherheit verwendet werden.

Backups werden auch als Datensicherungen bezeichnet.

Cybersecurity

Begriffe mit dem Bestandteil »Cyber« sind in Mode, in der Presse ist nicht nur von Cybersecurity zu lesen, sondern auch von Cyberangriffen oder Cybercrime. Länder führen ganze Cyberkriege gegeneinander. Unternehmen bieten Produkte zur Cyberabwehr an, um sich gegen Cyberbedrohungen zu schützen. Auch in EU-Gesetzestexten werden die Begriffe »Cybersicherheit« und »Cyberbedrohung« verwendet.

»Cyber« ist ein Begriff, der oft in Verbindung mit Computern, Netzwerken und der digitalen Welt verwendet wird. Ursprünglich abgeleitet von »Cybernetics«, das sich mit der Steuerung und Kommunikation von Maschinen und Lebewesen beschäftigt, hat sich der Begriff in den letzten Jahrzehnten weiterentwickelt und umfasst nun ein breites Spektrum an Konzepten und Technologien, die mit der digitalen und vernetzten Welt verbunden sind.

Cyber bezieht sich allgemein auf die virtuelle, digitale Welt und alles, was mit Computern, Netzwerken und dem Internet zu tun hat. Es wird auch als Abkürzung für Cyberspace verwendet, den Raum, der durch vernetzte Computer und Kommunikationssysteme geschaffen wird. Wenn Sie also Cyber hören, denken Sie an alles, was mit der Onlinewelt und der digitalen Technologie zu tun hat. Ein Cyberangriff ist ein Angriff, der aus dem Internet heraus stattfindet. Für solche Angriffen möchte sich auch die Bundeswehr wappnen, wie man an der Stellenanzeige in Abbildung 1.3 sehen kann.

Abbildung 1.3: Die deutsche Bundeswehr bewirbt offene Stellen für IT-Sicherheitsexpertinnen und -experten mit dem Begriff Cyberangriff. (Quelle: `https://www.karrierekaserne.de/bereiche/it`, Oktober 2024)

Auch international gewinnt der Begriff Cybersecurity immer mehr an Bedeutung. Häufig wird er aber synonym zu IT-Sicherheit verwendet und umfasst auch damit nur den technisch-technologischen Teil der Informationssicherheit.

Eine Mitarbeiterin der Buchhaltung, die wichtige Papiere und Aktenordner mit streng vertraulichen Geschäftszahlen nicht korrekt entsorgt und damit einsehbar für externe Personen macht, begeht einen Verstoß gegen die Informationssicherheit. In diesem Fall würde man aber kaum von »Cyber« sprechen.

Datenschutz

Datenschutz klingt vom Begriff zwar sehr ähnlich zu den bisher genannten, ist aber tatsächlich gänzlich verschieden – und steht manchmal sogar in Widerspruch zur Informationssicherheit. Meistens lassen sich beide Bereiche aber sehr gut miteinander verknüpfen.

Worin liegt aber der große Unterschied? In der Informationssicherheit geht es immer darum, Informationen zu schützen, weil diese per se als Wert für das Unternehmen oder die Organisation betrachtet werden. Datenschutz dagegen bezieht sich auf den Schutz persönlicher Daten und auf die Privatsphäre von Individuen. Er stellt sicher, dass personenbezogene Informationen, wie Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum und andere identifizierende Daten, vor Missbrauch, unbefugtem Zugriff und unrechtmäßiger Verarbeitung geschützt sind.

Der Hintergrund ist hierzulande nicht weniger als ein Grundrecht, nämlich das »Recht auf informationelle Selbstbestimmung«, also das Recht jeder Person, selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen (Allgemeines Persönlichkeitsrecht im Grundgesetz).

Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union ist eines der wichtigsten Regelwerke, das den Datenschutz innerhalb der EU regelt. Sie legt fest, wie persönliche Daten verarbeitet und geschützt werden müssen und welche Rechte betroffene Personen haben. Dazu gehören unter anderem das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung (auch bekannt als »Recht auf Vergessenwerden«) und das Recht auf Datenübertragbarkeit.

Datenschutz ist also spezifisch auf den Schutz personenbezogener Daten und die Rechte der Individuen ausgerichtet. Informationssicherheit ist dagegen ein breiteres Konzept, das den Schutz aller Informationen, unabhängig von ihrer Art, umfasst. Trotz dieser unterschiedlichen Zielsetzungen gibt es viele Überschneidungen (siehe Abbildung 1.4), insbesondere wenn es um die technischen und organisatorischen Maßnahmen (»TOMs«) geht. Diese werden von der DSGVO zum Schutz personenbezogener Daten gefordert und lassen sich häufig genauso zum Schutz aller Informationen anwenden.

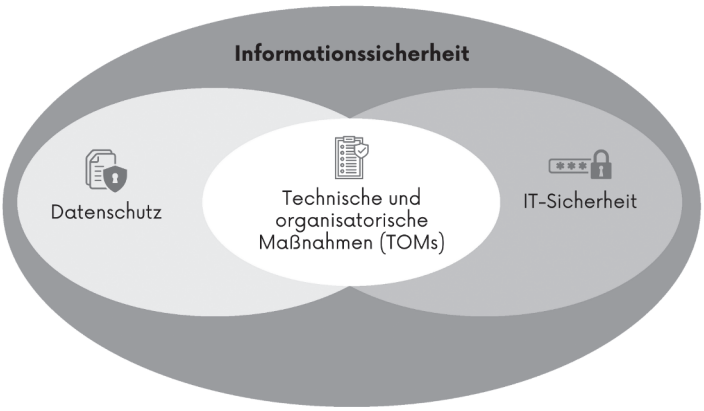

Abbildung 1.4: Zwischen den »TOMs« im Datenschutz und den Maßnahmen der Informationssicherheit gibt es viele Überschneidungen.

Beispiele für solche gemeinsamen TOMs sind:

- ✔ Zugangskontrollen: Sowohl im Datenschutz als auch in der Informationssicherheit ist es entscheidend, dass nur autorisierte Personen Zugriff auf sensible Daten und Informationen haben. Dies kann durch physische Zutrittskontrollen (zum Beispiel Schlüsselkarten) und digitale Zugriffskontrollen (zum Beispiel Passwörter, Zwei-Faktor-Authentifizierung) erreicht werden.
- ✔ Verschlüsselung: Verschlüsselungstechniken werden verwendet, um Daten sowohl bei der Übertragung als auch bei der Speicherung zu schützen. Dies ist eine grundlegende Maßnahme, um die Vertraulichkeit und Integrität von personenbezogenen Daten (im Sinne des Datenschutzes) und anderen sensiblen Informationen (im Sinne der Informationssicherheit) zu gewährleisten.
- ✔ Sicherheitsupdates und Patching: Regelmäßige Aktualisierungen und Patches für Software und Systeme sind notwendig, um bekannte Sicherheitslücken zu schließen und das Risiko von Cyberangriffen zu minimieren. Diese Praxis schützt personenbezogene Daten und alle anderen kritischen Informationen innerhalb eines Unternehmens.
- ✔ Sicherheitsrichtlinien und -schulungen: Die Implementierung klarer Sicherheitsrichtlinien und regelmäßige Schulungen der Mitarbeiter sind entscheidend, um ein Bewusstsein für Sicherheitspraktiken zu schaffen und die Einhaltung von Datenschutz- und Informationssicherheitsvorgaben sicherzustellen. Gut informierte Mitarbeiter können besser dazu beitragen, Sicherheitsverletzungen zu vermeiden.
- ✔ Überwachung und Protokollierung: Die kontinuierliche Überwachung und Protokollierung von Systemaktivitäten helfen dabei, unbefugte Zugriffe und Anomalien frühzeitig zu erkennen. Diese Maßnahmen unterstützen sowohl den Datenschutz, indem sie den unbefugten Zugriff auf personenbezogene Daten verhindern, als auch die Informationssicherheit, indem sie das gesamte Netzwerk und die IT-Infrastruktur schützen.

Durch die Implementierung dieser gemeinsamen technischen und organisatorischen Maßnahmen (TOMs) können Sie sowohl die Anforderungen des Datenschutzes als auch der Informationssicherheit erfüllen. Wenn Sie sicherstellen, dass personenbezogene Daten und andere wichtige Informationen geschützt sind, tragen alle Maßnahmen zu einem umfassenden Sicherheitsansatz bei, der die Erfüllung der Schutzziele aller Daten und Informationen gewährleistet. Abbildung 1.5 stellt dies tabellarisch dar.

	Informationssicherheit	**Datenschutz**
Ziele	Schutz der Organisation (Selbstschutz)	Schutz der Betroffenen (Drittschutz)
Umgang / Gegenstand	Alle Informationen, inkl. personenbezogener Daten Geschäftsprozesse	Personenbezogene Daten Datenverarbeitung
Berücksichtigung von Folgen	Unternehmensrisiken, inkl. Compliance-, Haftungs- und finanzieller Risiken	Datenschutzrisiken und Folgen für Betroffene
Zusammenfassung	Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Daten	Privatsphäre (Privacy) des Einzelnen und dessen personenbezogenen Daten

Abbildung 1.5: Diese Tabelle stellt die Gemeinsamkeiten und Unterschiede von Datenschutz und Informationssicherheit zusammenfassend dar.

Hauptaspekte der Informationssicherheit

Das große Spektrum der Informationssicherheit wird in der Norm ganz bewusst recht knapp definiert: Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information (siehe ISO/IEC 27000, 3.28).

Ergänzend wird angemerkt: Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Zuverlässlichkeit einbezogen werden.

Informationssicherheit entsteht also durch eine Vielzahl von Eigenschaften, die für alle Arten von Informationen gelten sollen. Die zuerst genannten Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit werden häufig auch als Hauptaspekte der Informationssicherheit oder als Schutzziele bezeichnet. Diese drei Hauptaspekte müssen ineinandergreifen, um ein umfassendes Sicherheitskonzept zu schaffen. Jeder Aspekt ist wichtig und voneinander abhängig, da ein Versagen in einem Bereich die anderen gefährden kann. Ein effektives Informationssicherheits-Managementsystem (ISMS) berücksichtigt alle drei Aspekte und implementiert geeignete Maßnahmen, um sicherzustellen, dass die enthaltenen Informationen angemessen geschützt sind.

Die meisten Informationen haben unterschiedlichen Schutzbedarf an die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Produktinformationen und Preise auf Ihrer öffentlichen Webseite müssen korrekt und abrufbar sein, wenn Sie mit einem Onlineshop Geld verdienen möchten. Die Vertraulichkeit der Daten spielt hier aber keine Rolle, da sie ja öffentlich sind.

Genau anders verhält es sich mit geheimen Forschungsergebnissen, die streng vertraulich behandelt werden müssen. Wenn Sie diese analog in Ihrem Bankschließfach aufbewahren, um die Vertraulichkeit sicherzustellen, geht dies zulasten der Verfügbarkeit, da Sie nicht immer und überall auf diese Informationen zugreifen können, sondern für den Zugriff erheblichen Aufwand betreiben müssen.

Die drei Hauptaspekte Vertraulichkeit, Integrität und Verfügbarkeit werden, den englischen Begriffen Confidentiality, Integrity und Availability entsprechend, im allgemeinen Sprachgebrauch gerne mit »CIA« abgekürzt. Wenn Sie im ISMS-Kontext also von CIA hören, ist damit eher selten der amerikanische Geheimdienst gemeint.

Vertraulichkeit (Confidentiality)

Definition nach ISO/IEC 27000, 3.10:

Vertraulichkeit: Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird.

Vertraulichkeit bedeutet, dass nur die richtigen Leute bestimmte Informationen sehen oder benutzen dürfen (siehe Abbildung 1.6). Oder anders gesagt, dass Informationen nur für autorisierte Personen zugänglich sind und vor unbefugtem Zugriff geschützt werden. Und das gilt letztlich auch für Systeme. Der Schutz der Vertraulichkeit stellt sicher, dass sensible Daten wie persönliche Informationen, Geschäftsgeheimnisse oder Finanzdaten nicht in die falschen Hände geraten. In einem Unternehmen bedeutet Vertraulichkeit, dass nur autorisierte Mitarbeiter Zugang zu sensiblen Informationen wie Kundenlisten oder Forschungsergebnissen haben. Zum Beispiel werden Mitarbeiter in der Personalabteilung Zugang zu Gehaltsinformationen haben, aber nicht jeder im Unternehmen sollte diese Informationen sehen können.

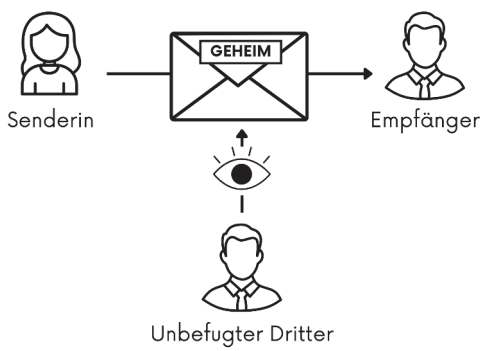

Abbildung 1.6: Schematische Darstellung der Vertraulichkeit

Vielleicht kommt Ihnen beim Thema Vertraulichkeit sofort Verschlüsselung als Schutzmaßnahme in den Sinn. Das ergibt als technische Maßnahme durchaus Sinn. Denken Sie aber auch wieder daran, dass es sich bei Informationen nicht nur um digitale Daten auf Computersystemen handelt, sondern genauso um ausgedruckte Unterlagen auf Papier und um das Wissen in den Köpfen der Mitarbeiter. Aktenschränke und Büroräume abzuschließen und Mitarbeiter zur Geheimhaltung zu verpflichten, sind daher ebenso sinnvolle Maßnahmen.

Maßnahmen zur Gewährleistung der Vertraulichkeit könnten sein:

- ✔ Zugriffskontrollen: Mit der Implementierung von physischen und logischen Zugriffskontrollen können Sie sicherstellen, dass nur autorisierte Benutzer auf sensible Informationen zugreifen können. Dazu gehören der abgeschlossene Aktenschrank, der Tresor und das verschlossene Büro genauso wie Rechte- und Rollenkonzepte bei IT-Systemen. Bedenken Sie: Zu abgeschlossenen Schränken und Türen gehört auch das Konzept, welche Mitarbeitenden welche Schlüssel ausgehändigt bekommen.
- ✔ Verschlüsselung: Die Verschlüsselung von Daten während der Übertragung oder bei der Speicherung hilft dabei, sicherzustellen, dass sie nicht von Unbefugten gelesen werden können. Die Verschlüsselung von Festplatten und mobilen Datenträgern sollte heute bereits zum Standard in Ihrer IT gehören. Bei E-Mails und im Internet gibt es häufig Verschlüsselung, aber nicht immer. Vorsicht ist nach wie vor bei der Benutzung öffentlicher Netzwerke geboten, zum Beispiel bei der Nutzung von freiem WLAN am Flughafen oder im Hotel.
- ✔ Authentifizierung: Der Einsatz von Authentifizierungsmechanismen wie Passwörtern, biometrischen Daten oder Zwei-Faktor-Authentifizierung, um die Identität der Benutzer zu überprüfen, trägt ebenfalls zum Erhalt der Vertraulichkeit bei.

Verschlüsselung gibt es nicht nur in der IT. Von Caesar ist bis heute bekannt, dass er eine einfache Art der Verschlüsselung verwendet hat, um die Vertraulichkeit seiner Nachrichten zu gewährleisten. Dies wird als »Caesar-Verschlüsselung« oder »Caesar-Chiffre« bezeichnet.

Überliefert ist, dass er diese Technik bei militärischen Feldzügen verwendet hat, um geheime Befehle und Informationen sicher an seine Generäle zu übermitteln. Bei den Kämpfen um Gallien wurde diese Methode verwendet, um sicherzustellen, dass seine Gegner nicht seine strategischen Pläne entschlüsseln konnten, wenn sie seine Nachrichten abfangen würden.

Die Caesar-Verschlüsselung ist eine Methode, bei der jeder Buchstabe im Text um eine feste Anzahl von Stellen im Alphabet verschoben wird. Caesar entschied sich beispielsweise, die Buchstaben um drei Stellen zu verschieben. Das bedeutet, dass A zu D wird, B zu E, C zu F und so weiter. So sieht das verschlüsselte Alphabet aus:

Normal: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Verschlüsselt: DEFGHIJKLMNOPQRSTUVWXYZABC

Nehmen wir an, Caesar wollte die Nachricht »ANGRIFF BEI TAGESANBRUCH« senden. Die verschlüsselte Nachricht lautet dann: »DQJULII EHL WDJHVDQEUFK«.

Integrität (Integrity)

Definition nach ISO/IEC 27000, 3.36:

Integrität: Eigenschaft der Richtigkeit und Vollständigkeit.

Integrität bezieht sich auf die Genauigkeit und Vollständigkeit von Informationen und die Sicherheit vor unbefugter oder unbeabsichtigter Änderung (siehe Abbildung 1.7). Der Schutz der Integrität stellt sicher, dass Informationen nicht manipuliert, verfälscht oder unvollständig sind, sodass sie zuverlässig und korrekt bleiben. Nehmen wir an, eine Firma führt ein Bestandsverwaltungssystem für ihre Lagerbestände. Wenn jemand die Daten manipuliert oder falsche Informationen eingibt, könnte das zu erheblichen Problemen führen, wie zum Beispiel falsche Bestellungen oder unzufriedene Kunden. Daten können allerdings nicht nur von Angreifern manipuliert werden, auch technische Fehler oder Systemfehler können die Integrität von Informationen verletzen. Wenn der Temperatursensor in Ihrem Rechenzentrum defekt ist und eine falsche Raumtemperatur übermittelt, ist die Integrität ebenfalls verletzt.

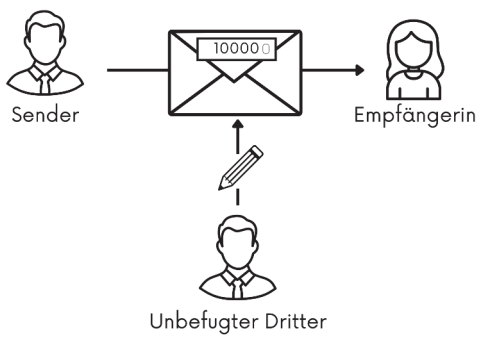

Abbildung 1.7: Schematische Darstellung der Integrität

Maßnahmen zur Gewährleistung der Integrität könnten sein:

- ✔ Hashing: Viele Systeme und Programme verwenden Hashing-Algorithmen, um sicherzustellen, dass Daten nicht verändert wurden. Ein Hashwert kann also verwendet werden, um die Integrität von Daten zu überprüfen.
- ✔ Datenintegritätsprüfungen: Durch regelmäßige Überprüfung und Validierung von Datenbeständen lässt sich sicherstellen, dass sie korrekt und vollständig sind. Im Falle des defekten Temperatursensors könnten Sie mehrere Sensoren verbauen, um die Integrität der übermittelten Daten zu überprüfen.

- ✔ Zugriffskontrollen: Mit der Einschränkung von Schreibzugriffen auf Daten, sodass nur autorisierte Benutzer Änderungen vornehmen können, kann die Integrität von Dokumenten sichergestellt werden. Ebenso hilft eine implementierte Versionierung dabei, Änderungen schneller und einfacher nachvollziehen zu können.

Auch in der analogen Welt lassen sich Beispiele für die Gewährleistung der Integrität finden. Stellen Sie sich vor, Sie arbeiten in einem modernen, digitalisierten Büro und Ihr Chef hat Ihnen den Auftrag gegeben, einen wichtigen Vertrag an einen Geschäftspartner zu senden. Diesmal muss es aber auf Papier sein. Sie schreiben den Vertrag sorgfältig, drucken ihn aus und stecken ihn in einen Briefumschlag. Bevor Sie den Umschlag zukleben, fällt Ihnen ein altes Sprichwort ein: »Ein verschlossener Brief schützt den Inhalt.« Warum ist das so wichtig? Ein verschlossener Briefumschlag schützt natürlich auch die Vertraulichkeit der enthaltenen Informationen. Denn der verschlossene Umschlag verhindert, dass jemand den Inhalt des Briefs liest, bevor er den Empfänger erreicht. Aber durch den verschlossenen Umschlag können Sie auch sicherstellen, dass niemand den Inhalt des Briefs verändert hat. Stellen Sie sich vor, der Briefumschlag wäre offen und jemand könnte den Vertrag herausnehmen, etwas hinzufügen oder ändern und ihn wieder zurücklegen. Der Empfänger hätte keine Ahnung, dass der Vertrag manipuliert wurde. Wenn Ihr Geschäftspartner aber den verschlossenen Umschlag erhält, kann er sicher sein, dass niemand den Vertrag auf dem Weg manipuliert hat.

Verfügbarkeit (Availability)

Definition nach ISO/IEC 27000, 3.7:

Verfügbarkeit: Eigenschaft, zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat.

Verfügbarkeit bedeutet, dass Informationen und Informationssysteme für autorisierte Benutzer dann zugänglich sind, wenn sie benötigt werden (siehe Abbildung 1.8). Der Schutz der Verfügbarkeit stellt sicher, dass Systeme und Daten »jederzeit« verfügbar sind und dass der Geschäftsbetrieb nicht durch Ausfälle oder Angriffe beeinträchtigt wird.

Der Zusatz »wenn sie benötigt werden« ist entscheidend. Gerade in der digitalen Welt wird Verfügbarkeit oft binär definiert, ein System ist verfügbar oder eben nicht. Aus Sicht der Informationssicherheit wird der Begriff nicht so schwarz-weiß interpretiert. Hier ist viel entscheidender die Frage, wie lange eine Information nicht verfügbar sein darf, bevor es zu einer spürbaren Beeinträchtigung des Unternehmens kommt. Selbstverständlich sollten Sie durch geeignete Maßnahmen wie Backups sicherstellen, dass Daten nicht vollständig unwiderruflich verloren gehen können. Von diesem Fall abgesehen gibt es aber durchaus unterschiedliche Zeitspannen, die Systeme nicht verfügbar sein könnten, ohne dass es zu größeren Schäden kommt.

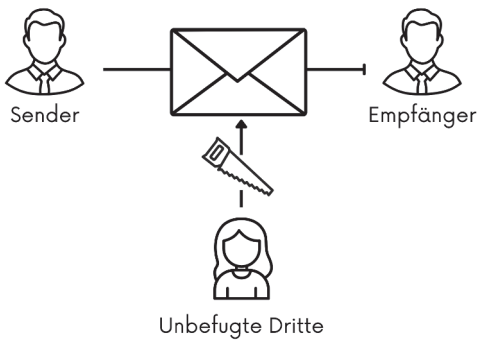

Abbildung 1.8: Schematische Darstellung der Verfügbarkeit

Maßnahmen zur Gewährleistung der Verfügbarkeit könnten sein:

- ✔ Redundanzen: Die Schaffung und Implementierung redundanter Systeme und Datenpfade hilft, sicherzustellen, dass der Ausfall eines einzelnen Systems nicht gleich zu einem Verlust der Verfügbarkeit führt.
- ✔ Backups: Regelmäßige Datensicherungen sind unabdingbar, um im Falle eines Datenverlusts eine schnelle und einfache Wiederherstellung zu ermöglichen.
- ✔ Pläne für Disaster Recovery und Business Continuity: Entwickeln und implementieren Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung Ihres Geschäftsbetriebs, um sicherzustellen, dass Systeme und Daten auch nach einem größeren Ausfall schnell wiederhergestellt werden können.

Es gibt einige Systeme im Geschäftsbetrieb, die nicht ständig gebraucht werden und auch mal ausfallen können, ohne dass es gleich zu einem Schaden kommt. Das System zur Lohnabrechnung könnte jeden Monat drei Wochen ausfallen – solange es im Zeitraum der Lohnzahlung funktioniert, stört Sie das nicht weiter.

Bei dem System, das den Betrieb in Ihren Produktionshallen steuert und aufrechterhält, kann jedoch schon der Ausfall einer Sekunde einen beträchtlichen Schaden anrichten. Einem Automobilhersteller, der in einer Linie etwa 50 Fahrzeuge pro Stunde mit einem durchschnittlichen Wert von 40.000 Euro pro Fahrzeug produziert, entgehen bei einem Fließbandausfall bereits in der ersten Stunde 2 Millionen Euro an Produktionswert.

Authentizität (authenticity)

Definition nach ISO/IEC 27000, 3.6:

Authentizität: Eigenschaft, dass eine Entität das ist, was sie angibt zu sein.

Authentizität ist der erste Nebenaspekt der Informationssicherheit nach ISO-Norm. In machen Gesetzen oder Veröffentlichungen des BSI wird dieser Aspekt auch als viertes

Schutzziel aufgeführt. Daher ist naheliegend, dass dieser Begriff als erster der Nebenaspekte von der ISO genannt wird und auch eine eigene Begriffsdefinition hat. Ein anderes Wort für Authentizität ist »Echtheit«. Dinge oder Informationen sind authentisch, wenn sie echt und vertrauenswürdig sind. Und das sind Information, Identitäten und Daten dann, wenn sie wirklich das sind, für das sie vom Leser oder Benutzer gehalten werden. Wird zum Beispiel ein Dokument oder eine Nachricht verschickt, so ist es ein Thema der Authentizität, dass der Empfänger sich sicher sein kann, dass die Nachricht tatsächlich vom angenommenen Versender stammt.

Maßnahmen zur Gewährleistung der Authentizität könnten sein:

- ✔ Verwendung von digitalen Signaturen: Digitale Signaturen sind kryptografische Mechanismen, die die Authentizität und Integrität von digitalen Dokumenten und Nachrichten gewährleisten. Dabei wird eine digitale Signatur mit einem privaten Schlüssel erstellt, die mit einem öffentlichen Schlüssel des Absenders überprüft werden kann. So stellen Sie sicher, dass die Nachricht oder das Dokument tatsächlich vom Absender stammt und nicht verändert wurde.
- ✔ Authentifizierungsprotokolle: Starke Authentifizierungsprotokolle wie Zwei-Faktor-Authentifizierung (2FA) oder Multi-Faktor-Authentifizierung (MFA) helfen dabei, sicherzustellen, dass nur autorisierte Personen Zugang zu Systemen und Daten haben.
- ✔ Physische Sicherheit und Zugangskontrollen: Stellen Sie mit Schlüsselkarten und Zugangscodes sicher, dass nur autorisierte Personen physischen Zugang zu sensiblen Informationen und Systemen haben. Installieren Sie Überwachungskameras in wichtigen Bereichen, um unbefugten Zugang zu verhindern und zu überwachen.

Lesen Sie noch einmal die Geschichte vom Vertrag im Briefumschlag als Beispiel für sichergestellte Vertraulichkeit und Integrität in der analogen Geschäftswelt. Versetzen Sie sich ein paar Jahrhunderte zurück. Sie befinden im 18. Jahrhundert und sind ein wichtiger Geschäftsmann, der regelmäßig vertrauliche Briefe an seine Handelspartner in ganz Europa sendet. In einer Zeit, in der es weder E-Mails noch verschlüsselte Nachrichten gibt, müssen Sie nicht nur sicherstellen, dass der Inhalt Ihrer Briefe nicht verändert wird, bevor sie den Empfänger erreichen. Sie möchten auch sicherstellen, dass sich der Empfänger sicher sein kann, dass ein Brief auch wirklich von Ihnen kommt. Wie machen Sie das? Hier kommt das Konzept von Siegeln und versiegelten Umschlägen ins Spiel.

Um die Integrität und Authentizität Ihrer Briefe zu gewährleisten, verwenden Sie ein Wachssiegel. Bevor Sie Ihren Brief verschicken, schmelzen Sie etwas Wachs auf die Kante des Umschlags. Bevor das Wachs abkühlt, drücken Sie Ihr persönliches Siegel – also ein kleines Metallwerkzeug mit einem einzigartigen Muster oder Ihrem Familienwappen – in das Wachs. Wenn das Wachs aushärtet, bildet es ein festes Siegel. Ihr Handelspartner erkennt Ihr einzigartiges Siegelmuster und weiß, dass der Brief authentisch, also wirklich von Ihnen, ist.

Zurechenbarkeit (accountability) und Nichtabstreitbarkeit (non-repudiation)

Zurechenbarkeit, oder auch Verantwortlichkeit, bedeutet, dass alle Aktionen, die in einem System durchgeführt werden, eindeutig einer bestimmten Person oder Entität zugeordnet werden können. Dies bedeutet, dass jeder Benutzer für seine Handlungen verantwortlich gemacht werden kann und dass seine Aktivitäten nachvollziehbar sind.

Es ist gut, wenn Sie sicherstellen, dass Benutzer für ihre Handlungen verantwortlich gemacht werden können, da so Sicherheitsvorfälle untersucht werden können und dadurch Betrug und Missbrauch verhindert werden.

Definition nach ISO/IEC 27000, 3.48:

Nichtabstreitbarkeit: Fähigkeit, das Eintreten eines behaupteten Ereignisses oder einer behaupteten Handlung samt ihren ursächlichen Entitäten nachzuweisen.

Nichtabstreitbarkeit stellt sicher, dass eine Person oder Entität nicht bestreiten kann, eine bestimmte Aktion durchgeführt zu haben oder eine bestimmte Nachricht gesendet zu haben. Es geht darum, Beweise zu liefern, dass eine Transaktion oder Aktion tatsächlich stattgefunden hat und von der entsprechenden Person oder Entität durchgeführt wurde. Das ist besonders wichtig bei rechtlich bindenden Transaktionen, wie etwa Vertragsabschlüssen oder Finanztransaktionen.

Die beiden Aspekte sind sehr eng beieinander und ergänzen sich gegenseitig, um eine vertrauenswürdige und überprüfbare Umgebung zu schaffen. Maßnahmen wie Protokollierung, starke Authentifizierung, digitale Signaturen und Audit-Trails sind wesentliche Elemente zur Sicherstellung beider Aspekte.

Der Hauptunterschied zwischen Nichtabstreitbarkeit und Zurechenbarkeit liegt in ihrer Zielsetzung und Anwendung: Nichtabstreitbarkeit konzentriert sich darauf, sicherzustellen, dass eine Person oder Entität nicht bestreiten kann, eine bestimmte Aktion durchgeführt oder eine bestimmte Nachricht gesendet zu haben. Ein Beispiel wäre die Verwendung digitaler Signaturen, um zu beweisen, dass eine bestimmte Person ein Dokument signiert hat. Zurechenbarkeit konzentriert sich darauf, sicherzustellen, dass alle Aktionen in einem System eindeutig einer bestimmten Person oder Entität zugeordnet werden können. Es geht darum, sicherzustellen, dass Benutzer für ihre Handlungen verantwortlich gemacht werden können und dass ihre Aktivitäten nachvollziehbar sind. Ein Beispiel wäre die Protokollierung von Benutzeraktivitäten, um nachzuverfolgen, wer auf welche Daten zugegriffen hat.

Ein praktisches Beispiel zur Verdeutlichung:

Stellen Sie sich vor, Sie arbeiten in einem Unternehmen, das eine wichtige Geschäftstransaktion durchführt. Sie senden einen Vertrag per E-Mail an einen Geschäftspartner und verwenden eine digitale Signatur, um die Nachricht zu signieren.

Nichtabstreitbarkeit: Durch die digitale Signatur können Sie sicherstellen, dass Ihr Geschäftspartner nicht abstreiten kann, den Vertrag von Ihnen erhalten zu haben. Ebenso können Sie nicht abstreiten, den Vertrag gesendet zu haben.

Zurechenbarkeit: Das System protokolliert, dass Sie der Absender der E-Mail sind und dass Sie die digitale Signatur verwendet haben. Es zeichnet auch auf, wann und von welchem Konto die E-Mail gesendet wurde, sodass Ihre Aktion eindeutig Ihnen zugeordnet werden kann.

Zuverlässigkeit (reliability)

Definition nach ISO/IEC 27000, 3.55:

Zuverlässigkeit: Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen.

Zuverlässigkeit ist ein zentraler Begriff sowohl in der Technik als auch im Geschäftsleben, der die Fähigkeit eines Systems, einer Komponente oder einer Organisation beschreibt, ihre Funktionen konsistent und ohne Ausfälle über einen bestimmten Zeitraum hinweg zu erfüllen. Es geht darum, dass etwas oder jemand beständig und vertrauenswürdig ist und die Erwartungen stets erfüllt. In der Informationssicherheit wird dies letztlich durch eine Kombination aus Verfügbarkeit und Integrität erzielt. Denn wenn ein System nicht ausfällt, sind die Anforderungen an die Verfügbarkeit erfüllt, und wenn die enthaltenen Informationen korrekt sind, sind die Anforderungen an die Integrität erfüllt.

In unserer Welt, in der viele Aspekte des Lebens von Technik und vernetzten Systemen abhängen, ist Zuverlässigkeit entsprechend wichtig. Sie ist die Grundlage für sichere und stabile IT-Infrastrukturen. Sicherstellen können Sie das durch Maßnahmen wie regelmäßige Wartung, ausreichende Redundanzen und Qualitätskontrollen.

Die ISO-Norm ist bei der Schreibweise dieses Begriffs nicht besonders konsistent. In der Anmerkung zur Definition der Informationssicherheit (3.28) wird von »Zuverlässlichkeit« gesprochen, einem Wort, das es im deutschen Duden gar nicht gibt. Denn dort finden sich die beiden Begriffe Zuverlässigkeit und Verlässlichkeit.

Bei der eigentlichen Definition des Begriffs (3.55) ist wiederum von »Zuverlässichkeit« die Rede. Und auch bei der Angabe des englischen Originalbegriffs hat sich ein Schreibfehler eingeschlichen, denn dort steht »reliablility» statt der korrekten reliability. Man könnte meinen, das fehlende »l« hätte sich vom deutschen in den englischen Begriff gemogelt.

Falls Sie Probleme mit der Schreibweise des Begriffs Zuverlässigkeit haben sollten, sind Sie damit auf jeden Fall nicht allein.

Weitere Aspekte

Neben den bereits genannten Aspekten und Schutzzielen der Informationssicherheit gibt es noch weitere Begriffe, die ab und zu im selben Atemzug genannt werden. Auf diese Begriffe soll hier nicht im Besonderen eingegangen werden:

- ✔ **Benutzbarkeit:** Systeme sollen so gestaltet sein, dass sie von ihren Anwendern auch benutzt werden können. Wenn die Sicherheitseinstellungen einer Software so

komplex oder so versteckt sind, dass sie vom Anwender nicht korrekt oder sicher konfiguriert werden können, helfen auch die besten Sicherheitsfunktionen nichts.

- ✔ **Resilienz:** Resilienz ist die Fähigkeit eines Systems, einer Organisation oder einer Person, sich von Störungen, Krisen oder unvorhergesehenen Ereignissen schnell zu erholen und den normalen Betrieb wieder aufzunehmen. In der Informationssicherheit bezieht sich Resilienz auf die Fähigkeit von IT-Systemen und Netzwerken, Angriffe, Ausfälle oder andere Betriebsunterbrechungen zu überstehen und weiterhin zuverlässig zu funktionieren. Das umfasst Maßnahmen wie Notfallwiederherstellungspläne, redundante Systeme und regelmäßige Sicherheitsübungen, die sicherstellen, dass der Betrieb auch in schwierigen Situationen aufrechterhalten werden kann.
- ✔ **Verbindlichkeit:** Die Verpflichtung einer Person oder Organisation, bestimmte Zusagen, Vereinbarungen oder Verpflichtungen einzuhalten, wird als Verbindlichkeit bezeichnet. In der Informationssicherheit und im Geschäftsleben bedeutet Verbindlichkeit, dass getroffene Abmachungen, Verträge und Zusagen zuverlässig und konsequent erfüllt werden. Es stellt sicher, dass alle Parteien wissen, dass Vereinbarungen eingehalten werden, was Vertrauen und Zuverlässigkeit in Geschäftsbeziehungen fördert. Verbindlichkeit wird oft durch formelle Vereinbarungen, wie Verträge und schriftliche Zusagen, sowie durch die Einhaltung von Standards und Verfahren gestützt. Verbindlichkeit wird auch gerne im selben Zug mit Nichtabstreitbarkeit genannt.
- ✔ **Compliance:** Compliance bezieht sich auf die Einhaltung von Gesetzen, Vorschriften, Standards und internen Richtlinien, die für eine Organisation relevant sind. Es bedeutet, dass Unternehmen und ihre Mitarbeiter alle gesetzlichen und regulatorischen Anforderungen erfüllen sowie interne Richtlinien und Verfahren befolgen. Compliance ist entscheidend, um rechtliche Risiken zu minimieren, finanzielle Strafen zu vermeiden und das Vertrauen von Kunden und Geschäftspartnern zu erhalten. Organisationen implementieren Compliance-Programme, einschließlich Schulungen, Überwachung und Audits, um sicherzustellen, dass alle Aktivitäten den geltenden Bestimmungen entsprechen.

Organisationen und Managementsysteme

In der Welt der Informationssicherheit spielt die organisatorische Struktur eines Unternehmens eine entscheidende Rolle. Eine klare und effektive Organisationsstruktur ist der Schlüssel für die erfolgreiche Implementierung und Aufrechterhaltung eines robusten Informationssicherheits-Managementsystems (ISMS). Deshalb müssen Sie sich damit beschäftigen, wie verschiedene Organisationen in Unternehmen aufgebaut sind und welche Verantwortlichkeiten dies mit sich bringt.

Die Bedeutung der Organisationsstruktur

Die Organisationsstruktur eines Unternehmens definiert, wie Aufgaben, Verantwortlichkeiten und Befugnisse innerhalb der Organisation verteilt sind. Das ist besonders wichtig, um sicherzustellen, dass Informationssicherheit in den Arbeitsalltag integriert wird. Eine gut funktionierende Organisationsstruktur schafft Klarheit darüber, wer für die verschiedenen

Aspekte der Informationssicherheit verantwortlich ist, von der Risikobewertung bis zur Reaktion auf Sicherheitsvorfälle. Eine gut durchdachte Organisationsstruktur ist ein entscheidender Faktor für den Erfolg einer umfassenden Informationssicherheitsstrategie.

Unterschiedliche Organisationsmodelle

Unternehmen können verschiedene Organisationsmodelle haben, abhängig von ihrer Größe, Branche und ihren Zielen. Hier sind einige gängige Modelle:

1. Hierarchische Struktur: In dieser traditionellen Organisationsform gibt es klare Hierarchien mit klaren Linien der Autorität. Die Verantwortlichkeiten sind nach oben delegiert, und Entscheidungen werden von Führungskräften getroffen. Die Informationssicherheit wird oft von einer dedizierten IT- oder Sicherheitsabteilung verwaltet.
2. Matrixstruktur: Hier gibt es eine Kombination aus hierarchischen und funktionalen Strukturen. Mitarbeiter können an mehreren Stellen in der Organisation Verantwortlichkeiten für Informationssicherheit haben. Dies kann effektiv sein, wenn verschiedene Abteilungen in die Sicherheitsprozesse eingebunden sind.
3. Flache Struktur: Startups und kleinere Unternehmen tendieren oft zu flachen Strukturen, bei denen die Hierarchien weniger ausgeprägt sind. Dies kann die Kommunikation erleichtern, aber es ist wichtig sicherzustellen, dass die Verantwortlichkeiten klar definiert sind.
4. Virtuelle Teams: In der heutigen globalisierten Welt sind virtuelle Teams, die über geografische Grenzen hinweg arbeiten, immer häufiger anzutreffen. Dies erfordert besondere Aufmerksamkeit für die Sicherheit und die klare Zuweisung von Verantwortlichkeiten, da die Teammitglieder möglicherweise nicht physisch am selben Ort sind.

Verantwortlichkeiten für Informationssicherheit

Unabhängig von der gewählten Organisationsstruktur gibt es bestimmte Schlüsselrollen und Verantwortlichkeiten im Bereich der Informationssicherheit:

1. Informationssicherheitsbeauftragter (CISO): Diese Schlüsselperson ist für die Entwicklung und Umsetzung der Informationssicherheitsstrategie verantwortlich. Der CISO koordiniert die verschiedenen Sicherheitsbemühungen im Unternehmen.
2. IT-Abteilung: Die IT-Abteilung spielt eine entscheidende Rolle bei der Umsetzung technischer Sicherheitsmaßnahmen, von der Netzwerksicherheit bis zur Verwaltung von Benutzerzugriffen.
3. Compliance-Beauftragter: Diese Person überwacht die Einhaltung gesetzlicher und regulatorischer Anforderungen im Bereich der Informationssicherheit, einschließlich Datenschutzvorschriften.
4. Mitarbeiter: Alle Mitarbeiter tragen Verantwortung für die Informationssicherheit, angefangen beim sicheren Umgang mit Passwörtern bis hin zur Meldung von Sicherheitsvorfällen.

Rollen und Verantwortlichkeiten sind ein besonders wichtiger Bestandteil eines ISMS. Die Norm widmet dem Thema ein ganzes Kapitel, das in diesem Buch in Kapitel 11 erläutert wird. Dort finden Sie jede Menge weiterer Informationen zu Rollen.

Im Anhang finden Sie außerdem detaillierte Beschreibungen typischer Stakeholder, auch darunter befinden sich die hier bereits kurz angesprochenen Verantwortlichkeiten.

Die Rolle der Führungsebene

Die Führungsebene eines Unternehmens spielt eine entscheidende Rolle bei der Festlegung der Prioritäten für die Informationssicherheit. Führungskräfte müssen die Bedeutung der Informationssicherheit erkennen und Ressourcen für ihre Umsetzung bereitstellen. Sie dienen als Vorbilder für die gesamte Organisation und setzen den Ton für eine Sicherheitskultur.

Details zur Rolle der Führung, und besonders welche Anforderungen die Norm ISO 27001 an die Führungskräfte einer Organisation hat, finden Sie in Kapitel 11 dieses Buchs.

Die Bedeutung der Kommunikation

Unabhängig von der Organisationsstruktur ist klare Kommunikation entscheidend. Alle Mitarbeiter müssen verstehen, wie Informationssicherheit in ihre täglichen Aufgaben integriert ist. Schulungen, Schulungsprogramme und regelmäßige Kommunikation sind unerlässlich.

Auch zum Thema Kommunikation stellt die Norm Anforderungen. Diese werden in diesem Buch in Kapitel 17 behandelt.

Die Integration der Informationssicherheit in die Organisationsstruktur

Die Integration der Informationssicherheit in die Organisationsstruktur erfordert ein bewusstes Bemühen. Dies kann durch die Einführung von Sicherheitsrichtlinien, Schulungen und die Festlegung klarer Verantwortlichkeiten erfolgen. Eine gut durchdachte Organisationsstruktur und klare Verantwortlichkeiten sind der Schlüssel zur erfolgreichen Integration von Informationssicherheit in die DNA eines Unternehmens.

Management

Management ist mehr als nur ein Schlagwort. Es ist die Kunst, Informationssicherheit in einem Unternehmen zu steuern, zu gestalten und zu optimieren. Es bedeutet nicht nur,

Regeln und Prozesse zu schaffen, sondern auch, sicherzustellen, dass diese effektiv umgesetzt und ständig verbessert werden.

Was ist Management?

Das Wort »Management« hat seine Ursprünge im lateinischen Wort »manu agere«, was so viel bedeutet wie »durch die Hand führen« oder »lenken«. Es bezieht sich auf die Kunst, Ressourcen und Aktivitäten zu organisieren und zu koordinieren, um bestimmte Ziele oder Ergebnisse zu erreichen. Im Kontext der Informationssicherheit bedeutet dies, dass wir Ressourcen einsetzen, um unsere Informationen vor Bedrohungen zu schützen und die Vertraulichkeit, Integrität und Verfügbarkeit zu wahren.

Synonyme für »Managen« können sein: Führen, Verwalten, Steuern, Leiten, Organisieren, Lenken oder Koordinieren. Aber auch Kontrollieren, Messen, Überwachen und Verbessern ergänzen diese Liste gut.

Das Management der Informationssicherheit ist eine komplexe Aufgabe. Von der Entwicklung einer Strategie über die Planung von Ressourcen bis zum Management von Risiken und der damit verbundenen Umsetzung von Sicherheitsmaßnahmen. Zu allem Überfluss bleibt dies nicht ohne Herausforderungen. Diese können von begrenzten Ressourcen bis hin zu einer sich ständig verändernden Bedrohungslandschaft reichen. Effektives Management erfordert die Fähigkeit, flexibel zu sein und auf neue Herausforderungen zu reagieren.

Deming-Kreislauf (PDCA)

Im Bereich des Managements und der Informationssicherheit ist der Deming-Kreislauf (oder »Deming-Cycle«), kurz unter der Abkürzung PDCA bekannt, ein fundamentales Konzept.

Der PDCA-Zyklus, auch bekannt als Deming-Cycle, wurde nach seinem Schöpfer, dem amerikanischen Statistiker und Qualitätsmanagementexperten William Edwards Deming (1900–1993), benannt. Deming gilt als eine der einflussreichsten Figuren im Bereich des Qualitätsmanagements und der kontinuierlichen Verbesserung. Er entwickelte diesen Zyklus in den 1950er-Jahren, um Organisationen eine systematische Methode zur Qualitätsverbesserung zu bieten.

Deming betonte die Bedeutung von kontinuierlicher Verbesserung in Organisationen und glaubte, dass Qualitätsmanagement ein Schlüssel zur Wettbewerbsfähigkeit und zum langfristigen Erfolg von Unternehmen sei. Seine Ideen und Methoden hatten einen erheblichen Einfluss auf die Industrie, insbesondere in Japan, wo der PDCA-Zyklus als »Deming-Rad« bekannt wurde und zur Grundlage des Qualitätsmanagements in Unternehmen wie Toyota wurde.

Der Deming-Cycle (PDCA) symbolisiert eine systematische Herangehensweise an die Verbesserung von Prozessen und Produkten. Er wurde entwickelt, um sicherzustellen, dass Unternehmen ihre Arbeitsweise ständig überprüfen und

optimieren, um höhere Qualitätsstandards zu erreichen. Dieses Konzept wird heute weltweit in verschiedenen Bereichen, einschließlich der Informationssicherheit, angewendet.

Nehmen Sie dieses Rad bitte nicht als Hamsterrad wahr. Der Kreislauf steht für die vier aufeinanderfolgenden Schritte Planung (Plan), Durchführung (Do), Überprüfung (Check) und Verbesserung (Act), wie in Abbildung 1.9 dargestellt.

Abbildung 1.9: Der Deming-Kreislauf, oder kurz PDCA

Planung (Plan)

In diesem ersten Schritt legen Sie Ziele und Prozesse fest. Das umfasst die Identifizierung von Problemen oder Möglichkeiten zur Verbesserung, das Festlegen von Zielen, das Entwickeln von Plänen und die Festlegung von Maßnahmen zur Umsetzung. Man spricht auch von »Vision« und »Mission«.

Die Festlegung von Unternehmenszielen für das kommende Geschäftsjahr fällt genauso in die Phase »Plan« wie die Definition eines neuen Einstellungsprozesses in der Personalabteilung oder die Festlegung einer Richtlinie zum sicheren Umgang mit Mobilgeräten.

Durchführung (Do)

In diesem Schritt setzen Sie die in der Planungsphase entwickelten Prozesse und Maßnahmen um. Wichtig ist dabei, dass die Umsetzung ausreichend dokumentiert wird, um sie später überprüfen zu können.

Überprüfung (Check)

Nach der Durchführung überprüfen Sie Ihre Ergebnisse, um zu sehen, ob die Umsetzung der Prozesse wie geplant geklappt hat. Dies beinhaltet die Sammlung von Daten, die Analyse von Ergebnissen und die Bewertung, ob die Ziele erreicht wurden.

Verbesserung (Act)

Basierend auf den Ergebnissen der Überprüfung ergreifen Sie Maßnahmen, um Prozesse zu optimieren und das Erreichen der Ziele zu fördern. Dies kann Anpassungen an den Plänen oder Prozessen, Schulungen oder andere Maßnahmen zur kontinuierlichen Verbesserung umfassen.

Kontinuierliche Verbesserung ist ein zentraler Aspekt des PDCA-Kreislaufs und des Managements der Informationssicherheit. Es bedeutet, dass Organisationen sich kontinuierlich bemühen, ihre Prozesse, Produkte und Ergebnisse zu verbessern, um effizienter zu werden und höhere Qualitätsstandards zu erreichen.

Warum kontinuierliche Verbesserung wichtig ist:

- ✔ **Anpassung an Veränderungen:** In einer sich ständig verändernden Geschäftswelt ist die Fähigkeit zur kontinuierlichen Anpassung von entscheidender Bedeutung.
- ✔ **Risikominderung:** Durch die kontinuierliche Überprüfung und Verbesserung von Sicherheitsmaßnahmen können Risiken minimiert werden.
- ✔ **Effizienzsteigerung:** Prozesse können optimiert werden, um Ressourcen effizienter einzusetzen.
- ✔ **Kundenorientierung:** Durch kontinuierliche Verbesserung können Kundenbedürfnisse besser erfüllt werden.
- ✔ **Wettbewerbsvorteil:** Organisationen, die kontinuierliche Verbesserung praktizieren, sind oft wettbewerbsfähiger.

Richtlinien, Prozesse und Verfahren

Abbildung 1.10 stellt den Zusammenhang von Richtlinien, Prozessen und Verfahren schematisch dar.

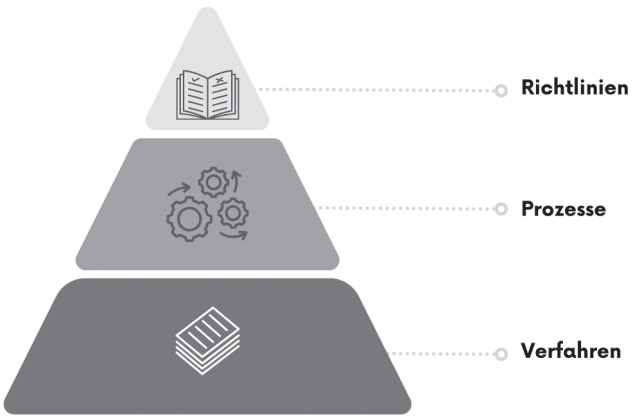

Abbildung 1.10: Richtlinien, Prozesse und Verfahren

Prozesse sind wie der unsichtbare Dirigent in einem gut orchestrierten Konzert. Sie verleihen unserer Arbeit Struktur, Klarheit und Effizienz, und aus diesem Grund schätzen wir Menschen sie sehr. Die Liebe zu Prozessen entspringt aus einer tiefen Sehnsucht nach Ordnung und Effizienz. Prozesse geben klare Anleitungen und bieten einen Pfad, dem man folgen kann. Sie sind wie eine detaillierte Straßenkarte für Aufgaben und Abläufe. In einer Welt, die oft chaotisch und komplex erscheint, sind Prozesse wie eine vertraute Landkarte, die uns den Weg weist.

Alle Prozesse bestehen aus diesen Merkmalen, die Teil der Prozessbeschreibung sind:

- ✔ **Prozessname:** Die eindeutige Bezeichnung des Prozesses.
- ✔ **Ziel und Zweck:** Die Zielsetzung oder der Zweck des Prozesses. Beides kann angelehnt sein an eine entsprechend darüber definierte Richtlinie.
- ✔ **Inputs:** Die benötigten Ressourcen oder Informationen, die in den Prozess eingehen. Gegebenenfalls kombiniert mit der Information, wann der Prozess startet (Trigger).
- ✔ **Aktivitäten/Schritte:** Eine detaillierte Ablauffolge der einzelnen Schritte im Prozess. Diese können in darunterliegenden Verfahren präzisiert und detailliert beschrieben werden.
- ✔ **Outputs:** Die erwarteten Ergebnisse des Prozesses.
- ✔ **Rollen und Verantwortlichkeiten:** Festlegung der Rollen und Verantwortlichen.
- ✔ **Kennzahlen/Indikatoren:** Metriken zur Messung des Prozesserfolgs.
- ✔ **Schnittstellen:** Abhängigkeiten zu anderen Prozessen oder Abteilungen.

Prozesse zeichnen sich unter anderem durch folgende Eigenschaften aus:

- ✔ **Definiertheit:** Die genannten Merkmale sind klar definiert und vereinbart.
- ✔ **Wiederholbarkeit:** Prozesse sind wiederholbar und können mehrmals mit demselben oder einem ähnlichen Ergebnis durchlaufen werden.
- ✔ **Zweckgerichtet:** Prozesse verfolgen ein klares Ziel und dienen der Wertschöpfung.

Einer der Hauptgründe, warum Menschen Prozesse lieben, liegt in ihrer Fähigkeit, Effizienz zu steigern. Durch die Festlegung von klaren Schritten und Verantwortlichkeiten können Aufgaben schneller und reibungsloser erledigt werden. Stellen Sie sich vor, wie viel Zeit gespart wird, wenn Sie nicht mehr darüber nachdenken müssen, was als Nächstes zu tun ist. Das ist der Zauber von gut durchdachten Prozessen.

Prozesse sind auch ausgezeichnete Fehlervermeider. Sie enthalten oft bewährte Methoden und Qualitätskontrollen, die das Risiko menschlicher Fehler minimieren. Dies bedeutet weniger »Rückgängigmachen« und mehr Zuversicht in die Arbeit, die erledigt wird. Die Qualität der Ergebnisse wird gesteigert.

Konsistenz ist ein weiterer Grund, warum Menschen Prozesse lieben. Wenn viele Menschen in einer Organisation zusammenarbeiten, ist es entscheidend, dass alle auf die gleiche Weise arbeiten. Prozesse stellen sicher, dass dies geschieht, unabhängig davon, wer die Aufgabe ausführt. Dies fördert die Zusammenarbeit und schafft ein Gefühl von Einheitlichkeit.

Prozesse sind flexibel und anpassbar. Wenn sich Anforderungen ändern oder Schwachstellen identifiziert werden, können Prozesse problemlos geändert und optimiert werden. Sie sind Werkzeuge zur kontinuierlichen Verbesserung.

In einer Organisation sind Vertrauen und Transparenz von entscheidender Bedeutung. Prozesse fördern beides. Jeder in der Organisation weiß, was von ihm erwartet wird, und die Transparenz schafft Verantwortlichkeit. Dies fördert das Vertrauen der Menschen in die Organisation.

Schließlich ermöglichen gut gestaltete Prozesse das Wachstum. Wenn die Arbeit effizient organisiert ist, kann die Organisation wachsen und mehr Aufgaben bewältigen, ohne die Qualität zu beeinträchtigen. Dieser Wachstumsfaktor ist entscheidend für den langfristigen Erfolg.

Kurz gesagt, Prozesse sind wie die Anleitung in einem Modellbau-Set. Sie geben uns die Bausteine und die Schritt-für-Schritt-Anleitung, um etwas Großartiges zu schaffen, sei es in der Arbeit, im Alltag oder in der Freizeit. Die Liebe zu Prozessen entspringt aus ihrer Fähigkeit, Struktur und Effizienz in unsere Welt zu bringen und gleichzeitig Raum für Flexibilität und kontinuierliche Verbesserung zu bieten.

Alle diese Eigenschaften werden in einem Managementsystem benötigt. Wenn wir davon sprechen wollen, Informationssicherheit zu managen, wird uns dies nur mithilfe von Prozessen gelingen. Bestenfalls können Sie alle anfallenden Aufgaben und Arbeiten mit Prozessen definieren – nehmen Sie sich das gerne zum Ziel.

Entscheidend sind die drei Kernprozesse im ISMS, die auch in Abbildung 1.11 dargestellt werden:

- ✔ Asset Management
- ✔ Risikomanagement
- ✔ Maßnahmenmanagement

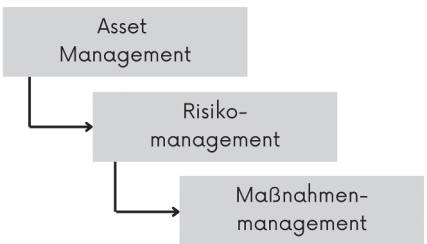

Abbildung 1.11: Die drei Kernprozesse des ISMS drehen sich rund ums Risikomanagement.

Neben den Prozessen gestalten Richtlinien und Verfahren unser Managementsystem. Richtlinien geben – wie der Name schon sagt – eine Richtung vor. Oft werden mit Richtlinien Ziele festgelegt, Vorgaben definiert oder andere Regeln aufgestellt. Sie können damit den Rahmen für unsere Prozesse bilden. Über allen Richtlinien im ISMS schwebt eine übergeordnete ISMS-Leitlinie. Dazu aber später mehr.

Diese Aufteilung bringt Struktur und Klarheit in das Managementsystem. Denn jede dieser Ebenen hat eine spezifische Rolle, die dafür sorgt, dass alle Beteiligten genau wissen, was sie tun müssen und warum das wichtig ist. Ohne diese klare Trennung könnten Informationen verloren gehen, Verantwortlichkeiten unklar sein und Mitarbeiter im Zweifel nicht wissen, was genau von ihnen erwartet wird.

Eine **Richtlinie** gibt die grobe Richtung vor – sie legt die Grundprinzipien und Ziele fest. Denken Sie an die Richtlinie wie an das »Was« und »Warum«. Sie erklärt, welche Standards und Prinzipien für die Sicherheit im Unternehmen gelten und warum diese Standards wichtig sind. Eine Richtlinie richtet sich oft an alle Mitarbeiter und Führungskräfte und dient als oberster Rahmen, an den sich alle halten sollen.

Ein **Prozess** beschreibt den »Weg« – also die einzelnen Schritte, die nötig sind, um die Richtlinie umzusetzen. Prozesse sind oft abteilungsübergreifend und zeigen, wer wann was tun muss, um das gewünschte Ziel zu erreichen. Ein Prozess sorgt dafür, dass alle Beteiligten wissen, wie sie zu einem bestimmten Ziel kommen, und koordiniert die verschiedenen Rollen und Abteilungen. So wird sichergestellt, dass das Ziel der Richtlinie erreicht wird.

Ein **Verfahren** geht ins Detail und erklärt das »Wie« – also die konkrete Umsetzung einzelner Schritte in einem Prozess. Verfahren sind detaillierte Anleitungen, die erklären, wie eine bestimmte Aufgabe ausgeführt werden soll, oft mit klaren Anweisungen, welche Tools oder Methoden zu verwenden sind. Sie

helfen Mitarbeitern, spezifische Aufgaben präzise und konsistent zu erledigen, und minimieren so Fehler oder Missverständnisse.

Die deutsche Sprache ist an dieser Stelle vielfältiger als die englische. Wir können den Begriff »Policy« mit Politik, Leitlinie oder Richtlinie übersetzen. Alle drei Begriffe werden im Deutschen im ISMS-Kontext verwendet, während die Original-Norm nur von »Policies« spricht.

- ✔ Mit »Politik« wird die Kultur eines Unternehmens beschrieben. Spezifisch wird das im Normkapitel 5 beschrieben und gefordert, dazu in einem späteren Kapitel mehr.
- ✔ »Leitlinien« und »Richtlinien« können je nach Gewohnheit der Organisation synonym verwendet werden. Oft – und daher auch in diesem Buch – wird mit Leitlinie ein übergeordnetes Dokument im ISMS beschrieben. Der Begriff der Richtlinien wird dann für alle weiteren Dokumente verwendet, die eine Richtung oder entsprechende Regeln aufstellen. Zum Beispiel eine »Richtlinie zum Umgang mit Mobilgeräten«.

In dieser Art und Weise verwendet auch das BSI in seinem IT-Grundschutz diese Begriffe.

Verfahren dienen unterhalb der Prozesse dazu, die einzelnen Schritte und Aktivitäten eines Prozesses im Detail für die Anwender zu erklären. Im Arbeitsumfeld werden entsprechende Dokumente häufig auch als Verfahrensanweisungen (VA) oder Arbeitsanweisungen (AA) bezeichnet. Sie enthalten gegebenenfalls Schritt-für-Schritt-Anleitungen, der Detailgrad hängt natürlich vom Kontext und von den Anwendern ab.

Anwender kennen oft nur die Verfahrensdokumente, da nur sie für den alltäglichen Einsatz relevant sind. Achten Sie dennoch darauf, dass Ihre Kolleginnen und Kollegen sich auch der darüberliegenden Prozesse und Richtlinien bewusst sind. Besonders die Frage, weshalb es wichtig ist, sich an Prozesse zu halten, lässt sich einfacher beantworten, wenn die Prozesse bekannt sind.

Natürlich können Sie Elemente aus allen drei Typen, also aus Richtlinien, Prozessen und Verfahren, in gemeinsamen Dokumenten beschreiben. Im Umfeld von Managementsystemen werden beispielsweise gerne sogenannte Handbücher verwendet, um viele Dokumentationsanforderungen in einem gemeinsamen Dokument zu behandeln.

Erstellen Sie in Ihrem ISMS zwei Handbücher: Ein Administrationshandbuch für die IT-Administratoren und ein Benutzerhandbuch für die Anwender. Beide Dokumente werden durch eine Handvoll Einzeldokumente für Einzelfälle flankiert, beispielsweise eine Homeoffice-Richtlinie für die Mitarbeiter, die im Homeoffice arbeiten, oder eine Backup-Richtlinie für die IT-Admins, die sich um die Backups kümmern.

Ein gern verwendetes Beispiel zur Veranschaulichung von Prozessen im Alltag ist die tägliche »Morgenroutine«. Vielleicht haben Sie wie die meisten Menschen einen sehr klar festgelegten Ablauf, was an Werktagen nach dem Klingeln des Weckers passiert. Besonders bei Personen mit festen Arbeitszeiten (Schichtdienst) oder bei

Familien mit Kindern lassen sich solche Prozesse finden. Alle Prozesseigenschaften und Besonderheiten lassen sich an diesem Beispiel wunderbar erklären.

Falls Sie alleine mit flexiblen Arbeitszeiten leben, ist die Prozessreife Ihrer Morgenroutine wahrscheinlich nicht besonders hoch. Falls Sie jedoch eine vierköpfige Familie mit Schulkindern und Hund in der Früh managen dürfen, schon. In diesem Fall könnten Sie wahrscheinlich eine ausführliche Prozessbeschreibung verfassen, inklusive Flowcharts und ähnlichen Fragmenten. Oder sogar eine RACI-Matrix erstellen, um die morgens notwendigen Tätigkeiten den verantwortlichen Rollen zuzuweisen. In Form eines »Badplans« lassen sich teilweise sogar solche Elemente finden.

Die Sinnhaftigkeit eines fest definierten Prozesses für diese Morgenroutine liegt dabei auf der Hand. Und das, obwohl sie in den meisten Fällen nicht dokumentiert sein wird. Prozesse müssen nicht zwingend dokumentiert sein, um zu funktionieren. Wichtiger ist es, dass sie bekannt und vereinbart sind, also dass alle Beteiligten damit einverstanden sind.

Stellen Sie sich nun vor, Ihr Morgenroutine-Prozess besteht aus den einzelnen Aktivitäten Aufstehen, Bad, Anziehen, Frühstück, Zähne putzen, Wohnung verlassen. Input sind die aufwachenden Menschen, der Start wird zugleich zeitlich als auch Event-basiert durch den Wecker getriggert. Output sollen ausgehfertige Personen sein. Ein klassischer Messwert ist wie bei vielen Prozessen die Durchlaufzeit – sowohl insgesamt als auch der einzelnen Schritte. Andere KPIs wären die dem Wetter angepasste Kleidung oder ausreichendes Frühstück.

Was sind nun Beispiele für eine Richtlinie und für Verfahren? In einer übergeordneten »Lebens-Richtlinie« könnte zum Beispiel definiert sein, dass Ihnen Pünktlichkeit grundsätzlich wichtig ist. Dieses Ziel wird dann durch den Morgenroutine-Prozess unterstützt. Auf der Verfahrensebene würden Sie beispielsweise beschreiben, wie man korrekt Zähne putzt oder welche Kleidung man bei welchem Wetter anzieht. Für Ihre Kinder sind vor allem die Anleitungen auf dieser Ebene relevant

Die drei Haupt-Dokumententypen Richtlinien, Prozesse und Verfahren werden im Englischen auch gerne als die drei »P« eines Managementsystems beschrieben: Policies, Processes und Procedures. Gelegentlich werden auch Pläne als viertes »P« dazu genommen.

Systeme und Systemtheorie

Die Systemtheorie ist ein Konzept, das tief in unser Verständnis von komplexen Strukturen und Prozessen eingreift. Ein System ist mehr als die Summe seiner Teile. Es ist eine Ansammlung von Elementen oder Komponenten, die miteinander interagieren, um gemeinsam ein bestimmtes Ziel oder Ergebnis zu erzielen. Diese Elemente können physischer, konzeptioneller oder abstrakter Natur sein. Das Wesentliche eines Systems liegt jedoch in

den Verbindungen und Wechselwirkungen zwischen den Elementen. Abbildung 1.12 stellt ein System in seinem Kontext dar.

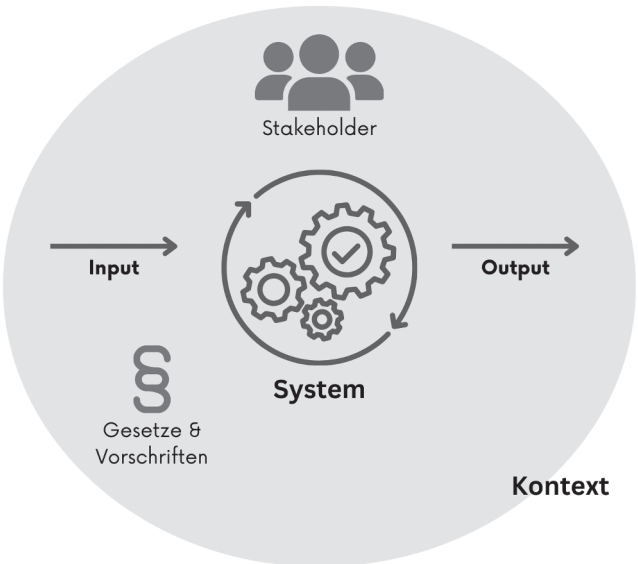

Abbildung 1.12: Ein System befindet sich immer in seinem Kontext. Teile des Kontexts sind zum Beispiel Stakeholder oder gesetzliche Rahmenbedingungen.

Ein gängiges Beispiel für ein System ist ein Auto. Es besteht aus verschiedenen Teilen wie Motor, Rädern, Karosserie und Elektronik, die zusammenarbeiten, um das Auto zu bewegen und den Fahrer von A nach B zu bringen. Diese Teile sind miteinander verknüpft und beeinflussen sich gegenseitig. Änderungen in einem Teil, zum Beispiel eine Änderung der Motorleistung, können Auswirkungen auf das gesamte System haben.

Die Systemtheorie ist ein interdisziplinäres Konzept, das sich mit der Untersuchung und dem Verständnis von Systemen befasst. Sie zielt darauf ab, die zugrunde liegenden Prinzipien und Muster zu identifizieren, die in verschiedenen Arten von Systemen auftreten. Diese Prinzipien können auf vielfältige Weise angewendet werden, von der Biologie über die Physik bis zur Soziologie und dem Management. Dabei werden Systeme als Ganzes betrachtet und die Wechselwirkungen zwischen ihren Komponenten untersucht. Sie legt Wert auf die Idee, dass Veränderungen in einem Teil eines Systems Auswirkungen auf das gesamte System haben können. Dieses Konzept wird als »holistischer« Ansatz bezeichnet.

Ein wichtiger Aspekt der Systemtheorie ist die Betrachtung von Rückkopplungsschleifen. Diese Schleifen können dazu beitragen, Stabilität oder Veränderungen in einem System zu erklären. Wenn Informationen oder Effekte in einem System zirkulieren und sich verstärken oder abschwächen, spricht man von Rückkopplung. Dieses Konzept ist entscheidend, um das Verhalten komplexer Systeme zu verstehen. Das ermöglicht es uns, die Welt um uns herum auf eine neue Art und Weise zu betrachten.

Genau diesen Ansatz machen wir uns in einem Managementsystem wie einem ISMS zunutze. Den Input ins ISMS liefern unterschiedliche Anforderungen an Informationssicherheit: Von unseren Stakeholdern wie Kunden, von gesetzlichen oder behördlichen Auflagen oder von uns selbst. Der Output unseres Managementsystems soll dann ein entsprechendes Niveau an Informationssicherheit sein. Die einzelnen Komponenten und Elemente des ISMS bilden unter anderem die Richtlinien, Prozesse und Verfahren, die Assets, Risiken und Maßnahmen und die unterschiedlichen Ressourcen wie Personen, Tools, Finanzen und das Know-how. Diese Komponenten sollen wie die technischen Bestandteile eines Autos so zusammenarbeiten, dass der entsprechende Output erreicht wird. Aus genau diesem Grund wird gerne davon gesprochen, dass jeder Bestandteil ein »kleines Zahnrad im Getriebe« ist. Abbildung 1.13 stellt einige dieser Bestandteile und wichtige Zusammenhänge dar.

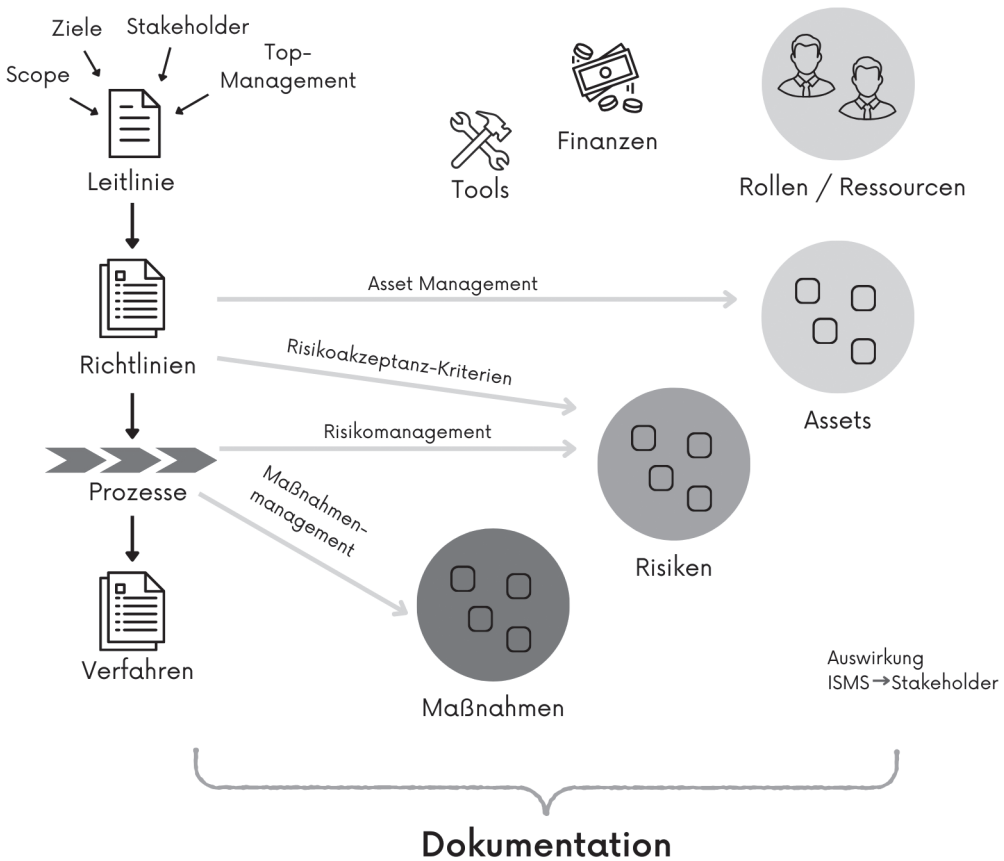

Abbildung 1.13: Kleine ISMS-Übersicht

Der Vergleich zu anderen Systemen im Alltag ist – ähnlich wie bei den Prozessen – auch hier hilfreich. Stellen Sie sich das Straßenverkehrssystem als ein System vor, das kein technisches System ist – und wahrscheinlich deutlich komplexer als Ihr ISMS. Das übergeordnete Ziel (Output) dieses Systems ist Mobilität, also dass sich Personen von A nach B bewegen können. Möglichst schnell und unversehrt könnten entsprechende Unterziele sein.

Die Straßenverkehrsordnung dient als übergeordnete Leitlinie, weitere Gesetze und Verordnungen legen zahlreiche Prozesse und Verfahren fest. Beispiele für Verfahren finden sich viele: »rechts vor links«, »bei Rot stehen, bei Grün gehen« oder das »Reißverschlussverfahren«. Als Rollen lassen sich verschiedene Verkehrsteilnehmer definieren. Fahrzeuge und Infrastruktur wie Straßen und Verkehrszeichen bilden die Assets und Ressourcen. Vieles findet hier risikobasiert statt: Viele Regeln dienen der Unfallverhütung.

Sie werden feststellen, wie wichtig Richtlinien, Prozesse und Verfahren in diesem System sind, sodass der gemeinsame Systemzweck erreicht wird. Und wie wichtig es ist, dass sich alle Beteiligten an diese Vorgaben halten, da das System sonst nicht funktioniert.

Übertragen Sie das analog auf Ihr ISMS!

Weigert721856_c01.indd 64 Trim Size: 176 × 240 mm 05 Feb. 2025 04:48:36 nachm.