|  |
| --- |
| IU |
| Normen der Informationssicherheit |
| Kurscode |

# Übergeordnete Lernziele

In der heutigen Zeit ist die Abhängigkeit vom Internet und der Vernetzung unserer Welt allgegenwärtig. Die Verbreitung von Social-Media-Plattformen, Tools und interaktiven Technologien nimmt zu. Dies führt zu einer Zunahme von digitalen Fußabdrücken und anderen Nachverfolgungsmethoden der Nutzer:innen. Diese reichen von einfachen Hacking- oder technischen Ansätzen bis hin zu subtilen, sozialen und nicht-technischen Strategien wie Social Engineering, die den menschlichen Geist nutzen und manipulieren. Nahezu alle Aspekte des Lebens und der Interaktion verlagern sich in das Online-Universum, was sowohl für Einzelpersonen als auch für Organisationen erhebliche Sicherheitsbedenken mit sich bringt. Die Sicherung von Informationsbeständen, die organisiertes, verwaltetes und wertvolles Wissen oder Daten darstellen, wird häufig vernachlässigt, obwohl dies sehr kostspielig sein kann.

Dieser Kurs bietet eine Navigationshilfe durch die komplexe Landschaft der Informationssicherheit, einschließlich der damit verbundenen rechtlichen und regulatorischen Anforderungen sowie aller relevanten Normen und Standards, die zum Schutz der Organisationsressourcen umgesetzt werden müssen. Die meisten Organisationen konzentrieren sich auf den Aufbau von IT-Systemen und vernachlässigen dabei den übergeordneten Managementkontext. Dieser umfasst Normen und Standards, die Organisationen dabei unterstützen, ihre Prozesse und Abläufe nach Best Practices und globalen Methoden für das Informationssicherheitsmanagement auszurichten. Die Internationale Organisation für Normung (ISO) ist für die Überprüfung, Verbesserung und Aktualisierung dieser Normen zuständig.

Der Kurs vermittelt zunächst grundlegende Sicherheitskonzepte und Terminologie. Anschließend konzentriert er sich auf das umfassende Informationssicherheits-Framework, das in einer Organisation umgesetzt werden muss – insbesondere ein Informationssicherheits-Managementsystem (ISMS). Sie lernen, wie ein ISMS initiiert wird und wie die Prozesse während und nach der Implementierung umgesetzt, verwaltet und überwacht werden.

# Lektion 1 – Einführung in die Informationssicherheit

**Lernziele**

Nach der Bearbeitung dieser Lektion …

… kennen Sie grundlegende Sicherheitsbegriffe, Konzepte und Ziele der Informationssicherheit.

… kennen Sie Informationssicherheitsstandards und rechtliche Rahmenbedingungen und können diese beschreiben.

… sind Sie in der Lage, Informationssicherheitsstandards, wie die ISO 27000-Reihe und die BSI-Standards zu erläutern.

… können Sie Informationssicherheits-Managementsysteme (ISMS) entwickeln, ihre Feinheiten, einschließlich Maßnahmen und Verfahren, analysieren sowie Maßnahmen zur kontinuierlichen Verbesserung solcher Systeme umsetzen.

# 1. Einführung in die Informationssicherheit

## Einführung

Im Vergleich zu früheren Methoden zur Bewältigung von Herausforderungen im Bereich der Informationssicherheit gehen Organisationen heute bewusster mit dem Thema um. Dies ist aufgrund der ständig wachsenden Bedrohungen in diesem Bereich notwendig geworden. Das Risikoniveau, das sich aus der Schwachstellen- und Bedrohungsanalyse ergibt, steigt kontinuierlich und erreicht in einigen Fällen alarmierende Ausmaße. Die Maßnahmen zur Umsetzung der Informationssicherheit müssen mit der Intensivierung der Aktivitäten böswilliger Akteure Schritt halten. Maßnahmen müssen kontinuierlich überprüft, verwaltet und verbessert werden, um den immer komplexeren und raffinierteren Angriffen und Bedrohungsszenarien zu begegnen. Das Ausmaß und die Bedeutung der Herausforderungen im Bereich der Informationssicherheit nehmen ständig zu. Dementsprechend müssen auch die Maßnahmen zu ihrer Bewältigung angepasst und intensiviert werden. Aber wie sieht die Realität aus?

Unternehmen jeder Größenordnung – ob klein, mittel oder groß – haben in letzter Zeit zunehmend finanzielle Verluste aufgrund von Verstößen gegen die Informationssicherheit erlitten. Die Aktivitäten böswilliger Individuen, darunter Hacking, Ransomware, Man-in-the-Middle-Angriffe und andere, zielen darauf ab, Organisationen zu destabilisieren und handlungsunfähig zu machen. Viele Unternehmen und Organisationen haben noch keine ausreichende Resilienz entwickelt, um mit solchen Störungen ihrer Abläufe umzugehen, wenn ihre Sicherheitsmaßnahmen kompromittiert werden. Große Organisationen sind in vielen Fällen unzureichend ausgestattet, um solche Aktivitäten wirksam zu bekämpfen, und handeln eher reaktiv als proaktiv. Infolgedessen werden solche Sicherheitsverletzungen häufig nicht rechtzeitig gemeldet oder bleiben sogar unentdeckt.

IT-Systeme, in denen Informationen erzeugt, gespeichert, transportiert und verarbeitet werden, werden immer ausgefeilter, die Zahl der Beteiligten und die technischen Aspekte immer komplexer. Die zunehmende Komplexität der Thematik erschwert es den Kund:innen, Vertrauen in die Unternehmen zu entwickeln. Es gibt definierte Sicherheitsniveaus, die Organisationen anstreben sollten, um dieses Vertrauen aufzubauen. Standards wie die ISO 27000-Reihe bieten Leitlinien, wie Unternehmen ihre Sicherheitssysteme gestalten können, um Vertrauen bei allen Stakeholdern zu schaffen. Wissenschaftler:innen wie Beckers et al. (2014) weisen darauf hin, dass „die Umsetzung von Sicherheitsstandards aufgrund der begrenzten Unterstützung bei der Systementwicklung und der Dokumentation in den verfügbaren Standards eine Herausforderung darstellt“ (Übers. des Autors).

Um diese Lücke zu schließen, behandelt diese Lektion die wichtigsten Begriffe, Konzepte und Ziele der Informationssicherheit, Sicherheitsstandards und Frameworks und stellt das Informationssicherheits-Managementsystem (ISMS) vor.

## 1.1 Grundlegende Definitionen, Sicherheitskonzepte und Ziele der Informationssicherheit

Organisationswerte, zu denen auch Informationswerte wie Daten und Informationssysteme gehören, müssen vor sich ständig verändernden Sicherheitsbedrohungen geschützt werden. Es ist unerlässlich, dass Organisationen Sicherheitsaspekte in allen Phasen – Entwicklung, Beschaffung, Installation, Betrieb, Wartung und Außerbetriebnahme – ihrer Organisationswerte berücksichtigen. Dieser Lernzyklus legt die Grundlagen für ein umfassendes Verständnis der Informationssicherheit. Er führt in die grundlegende Terminologie ein und erläutert die zentralen Konzepte und Ziele der Informationssicherheit.

### Geschichte der Informationssicherheit

Nach Whitman und Mattord (2018) beginnt die Geschichte der Informationssicherheit mit dem Konzept der Computersicherheit. Man geht davon aus, dass dieses Konzept während des Zweiten Weltkriegs entstand, als die ersten Großrechner entwickelt wurden. Diese dienten zur Unterstützung von Berechnungen für Kommunikationscodes, die gegen feindliche kryptografische Geräte wie die **Enigma** eingesetzt wurden. Damals wurden, wie aus Berichten hervorgeht, mehrere Sicherheitsstufen eingeführt, um die Geräte und ihre jeweiligen Aufgaben zu schützen. Folglich waren Verfahren und Methoden erforderlich, um die Vertraulichkeit der Daten zu gewährleisten. Der Zugang zu militärischen Einrichtungen wurde teilweise durch Ausweise und physische Schlüssel kontrolliert, und es wurden weitere Maßnahmen ergriffen, um diese sensiblen Geräte und Systeme zu schützen. Der Schutz der nationalen Sicherheit und der Ressourcen war damals bestenfalls rudimentär. Computersicherheit – heute als Informationssicherheit bekannt – war ein unkomplizierter Prozess, der hauptsächlich aus physischer Sicherheit und einfachen Dokumentenklassifizierungssystemen bestand. Die Hauptbedrohungen für die Sicherheit waren der physische Diebstahl von Geräten, Spionage und Sabotage. Im Laufe der Zeit wurden immer komplexere und technologisch anspruchsvollere Maßnahmen zum Schutz von Computersystemen erforderlich, um die nationale Sicherheit zu gewährleisten – einfache und rudimentäre Ansätze reichten nicht mehr aus. Die folgende Tabelle fasst einige der wichtigsten Daten zur Informationssicherheit zusammen.

**Enigma**

Dies war die deutsche Chiffriermaschine, die erst in den 1930er Jahren von polnischen Spezialisten geknackt wurde. Die aus den entschlüsselten Übertragungen gewonnenen Informationen dienten der Vorhersage von Aktionen der deutschen Streitkräfte.

Schlüsseldaten der Informationssicherheit

|  |  |
| --- | --- |
| Datum | Dokument |
| 1968 | Maurice Wilkes spricht über die Sicherheit von *Timesharing-Computern*.  |
| 1970 | Willis H. Ware verfasst den Bericht *Security Controls for Computer Systems*: *Report of Defense Science Board Task Force on Computer Security-RAND Report R-609,* der erst 1979 für die Öffentlichkeit freigegeben wurde. Es wurde als bahnbrechende Arbeit bekannt, welche die Notwendigkeit der Computersicherheit aufzeigte.  |
| 1973 | Schell, Downey und Popek untersuchen den Bedarf an zusätzlicher Sicherheit in militärischen Systemen in *Preliminary Notes on the Design of Secure Military Computer Systems*.  |
| 1975 | Die Federal Information Processing Standards (FIPS) prüft DES (Digital Encryption Standard) im Federal Register.  |
| 1978 | Bisbey und Hollingworth veröffentlichen ihre Studie „Protection Analysis: Final Report“, in dem das von der ARPA ins Leben gerufene Projekt „Protection Analysis“ besprochen wurde, um die Schwachstellen der Betriebssystemsicherheit besser zu verstehen und die Möglichkeit automatischer Techniken zur Erkennung von Schwachstellen in bestehender Systemsoftware zu untersuchen. |
| 1979 | Morris und Thompson verfassen „Password Security: A Case History“, veröffentlicht in *Communications of the Association for Computing Machinery* (ACM). In diesem Artikel wurde die Entwicklung eines Passwortsicherheitssystems für ein Timesharing-System mit Fernzugriff untersucht.  |
| 1979 | Dennis Ritchie veröffentlicht „On the Security Of UNIX“ und „Protection of Data File Contents“, in denen sichere Benutzer-IDs, sichere Gruppen-IDs und die mit diesen Systemen verbundenen Probleme behandelt werden. |
| 1982 | Das U.S. Department of Defense Computer Security Evaluation Center veröffentlicht die erste Version der Trusted Computer Security (TCSEC) Dokumente, die als Rainbow Series bekannt wurden.  |
| 1984 | Grampp und Morris schreiben „The UNIX System: UNIX Operating System Security“. In diesem Bericht untersuchten die Autoren vier wichtige Voraussetzungen für die Computersicherheit: die physische Kontrolle der Räumlichkeiten und Computereinrichtungen, das Engagement des Managements für die Sicherheitsziele, die Ausbildung der Mitarbeiter:innen und die Verwaltungsverfahren zur Erhöhung der Sicherheit.  |
| 1984 | Reeds und Weinberger veröffentlichen „File Security and the UNIX System Crypt Command“. Ihre Prämisse war: „Es gibt keinen Schutz vor Abhörmaßnahmen oder deren Äquivalent auf dem Computer. Daher kann keine Technik gegen den Systemadministrator oder andere privilegierte Benutzer sicher sein… der naive Benutzer hat keine Chance.“  |
| 1992 | Forscher:innen der Internet Engineering Task Force, die am Naval Research Laboratory arbeiten, entwickeln das Sicherheitsprotokoll Simple Internet Protocol Plus (SIPP) und schaffen damit das, was heute als IPSEC Security bekannt ist.  |

Quelle: Andrew Sai (2023), basierend auf Whitman und Mattord (2018).

Wie bereits in diesem Lernzyklus erwähnt wurde, konzentrierte sich die Computersicherheit in der Vergangenheit nur auf den Schutz von Geräten vor Angriffen. Das Internet hat in den letzten Jahren Millionen von Bedrohungen hervorgebracht, die auf die umfangreiche Kommunikation zwischen zahlreichen Computersystemen und Netzwerken zurückzuführen sind, von denen einige ungesichert sind. Seit den 2000er Jahren wächst das Bewusstsein für die Notwendigkeit, die Informationssicherheit zu verbessern. Dieses Bewusstsein geht über die Unternehmensebene hinaus und erkennt an, dass Informationssicherheit für die nationale Sicherheit und Verteidigung von entscheidender Bedeutung ist. Sowohl Regierungen als auch Unternehmen sehen sich zunehmenden Bedrohungen durch **Cyberangriffe** ausgesetzt. Der Schutz computergestützter Steuerungssysteme für öffentliche Versorgungsunternehmen und kritische nationale Infrastrukturen wird immer wichtiger. Darüber hinaus wächst die Besorgnis über Bedrohungen durch Nationalstaaten, die Informationskriege führen. Ein Beispiel hierfür ist der mutmaßliche russische Hackerangriff auf die Ressourcen der Demokratischen Partei der USA während der US-Wahlen 2016 (116. Kongress, 2020).

**Cyberangriff**

Ein böswilliger und vorsätzlicher Versuch einer Person oder Organisation, in das Informationssystem einer anderen Person oder Organisation einzudringen.

### Grundlegende Sicherheitsdefinitionen und Sicherheitskonzepte

Die im Folgenden aufgeführten Definitionen von Informationssicherheit und ausgewählten Konzepten werden in der **ISO**/IEC 27000 bzw. in der ISO/IEC 27000:2014 erläutert oder stammen aus anderen relevanten ISO-Normen. Nach Hintzbergen et al. (2015) ist die ISO/IEC 27000:2014 der erste Teil der gesamten ISO 27000-Normenfamilie und gibt einen Überblick über die Normen und erläutert die in dieser Normenfamilie verwendeten Begriffe. Der Fokus liegt auf Informationstechnologie, Sicherheitstechnik und Informationssicherheits-Managementsystemen. Ziel dieser Definitionen ist es laut ISO, Verwirrung über Begriffe und Definitionen zu vermeiden und ein einheitliches Verständnis zu schaffen. Hintzbergen et al. (2015) zeigen auf, wie die Autor:innen der ISO 27000-Reihe versuchen, Konsistenz zu gewährleisten und ein gemeinsames Verständnis von Begriffen und Bedingungen zu fördern. Sie weisen darauf hin, dass zum Beispiel „Vermögenswert“ in den Normen als „jedes Objekt, das für eine Organisation von Wert ist“ definiert wird. Dies bedeutet, dass jede Norm, unabhängig vom Thema, die gleiche Definition von „Vermögenswert“ verwendet (Hintzbergen et al. 2015). Im Folgenden werden die für diesen Kurs relevanten Definitionen ausgewählt und erläutert:

**ISO**

Eine internationale Organisation zur Entwicklung von Normen, die sich aus Vertreter:innen der nationalen Normungsorganisationen der Mitgliedsländer zusammensetzt.

**Informationsbezogene Definitionen aus der Norm ISO/IEC 27000**

Die nachstehende Tabelle enthält eine Reihe von Begriffen, die unter den weit gefassten Begriff der informationsbezogenen Definitionen fallen. Diese Begriffe und Konzepte beginnen mit Informationen, die als ein Vermögenswert für eine Organisation zu betrachten sind oder Informationen implizieren.

Informationsbezogene Definitionen aus der Norm ISO/IEC 27000

|  |  |
| --- | --- |
| Begriff | Definition |
| Informationen | Informationen sind Daten, die in einem bestimmten Kontext für den Empfänger eine Bedeutung haben. |
| Informationssicherheit | Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Darüber hinaus können auch andere Eigenschaften wie Authentizität, Nachvollziehbarkeit, Nichtabstreitbarkeit und Zuverlässigkeit eine Rolle spielen. |
| Informationssicherheitsmanagement | Koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation im Hinblick auf Risiken. Das Risikomanagement umfasst in der Regel Risikobeurteilung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation. |
|  Informationssicherheitsmanagementsystem (ISMS) | Teil des gesamten Managementsystems, das auf einem Geschäftsrisikoansatz basiert, um die Informationssicherheit einzurichten, zu implementieren, zu betreiben, zu überwachen, zu überprüfen, zu erhalten und zu verbessern. Das Managementsystem umfasst Organisationsstrukturen, Politiken, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen. |
| Informationssystem | Anwendung, Dienst, IT-Anlage oder jede andere Komponente zur Informationsverarbeitung. |

Quelle: Andrew Sai (2023), basierend auf Hintzbergen et al. (2015).

**Risikobezogene Definitionen aus ISO/IEC 27000 – Vokabular**

In der folgenden Tabelle finden Sie eine Reihe von Begriffen und Konzepten, die mit dem Wort Risiko beginnen oder risikobezogen sind. Diese beziehen sich auf Risiken und wie diese im Kontext des Kurses zu interpretieren sind.

Risikobezogene Definitionen aus ISO/IEC 27000

|  |  |
| --- | --- |
| **Begriff** | **Definition** |
| Restrisiko | Nach der Risikobehandlung verbleibendes Risiko. Das Restrisiko kann ein nicht identifiziertes Risiko enthalten und wird auch als „einbehaltenes Risiko“ bezeichnet. |
| Risiko | Auswirkungen von Unsicherheit auf die Ziele. |
| Risikoakzeptanz | Die Entscheidung, ein Risiko einzugehen. |
| Risikoanalyse | Ein Prozess, um die Art des Risikos zu verstehen und den Grad des Risikos zu bestimmen. Eine Risikoanalyse bildet die Grundlage für die Risikobewertung und Entscheidungen über die Risikobehandlung. Die Risikoanalyse umfasst eine Risikoeinschätzung. |
| Risikobeurteilung | Die Risikobeurteilung ist der Gesamtprozess der Risikoidentifizierung, Risikoanalyse und Risikobewertung. |
|  Risikobewertung | Ein Prozess, bei dem die Ergebnisse der Risikoanalyse mit Risikokriterien verglichen werden, um festzustellen, ob das Risiko und/oder sein Ausmaß akzeptabel oder tolerierbar ist. |
| Risikoidentifizierung | Der Prozess des Auffindens, Erkennens und Beschreibens von Risiken. Bei der Risikoidentifizierung geht es um die Identifizierung von Risikoquellen, Ereignissen, ihren Ursachen und ihren möglichen Folgen. Bei der Risikoermittlung können auch historische Daten, theoretische Analysen, fundierte Expertenmeinungen und die Bedürfnisse von Stakeholdern berücksichtigt werden. |
|  Risikomanagement | Koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation im Hinblick auf Risiken. |
| Risikomanagementprozess | Eine systematische Anwendung von Managementpolitiken, -verfahren und -praktiken auf die Aktivitäten der Kommunikation, der Beratung, der Festlegung des Kontextes und der Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von Risiken. ISO/IEC 27005:2011, der ISO-Standard für das Risikomanagement im Bereich der Informationssicherheit, verwendet den Begriff „Prozess“, um das Risikomanagement insgesamt zu beschreiben. Die Elemente innerhalb des Risikomanagementprozesses werden als „Aktivitäten“ bezeichnet. |
| Risikobehandlung | Der Prozess der Auswahl und Umsetzung von Maßnahmen zur Risikominderung.  |

Quelle: Andrew Sai (2023), basierend auf Hintzbergen et al. (2015).

Weitere Begriffe und Konzepte, wie z. B. Maßnahme, Leitfaden, Vermögenswert, Angriff, Politik, Präventivmaßnahme, Verfahren, Prozess, Drittpartei, Bedrohung und Schwachstelle, die im Kurs ausführlich behandelt werden, finden Sie auf der ISO-Website. Die IEC bietet die *Electropedia* an, die Normen erarbeitet und veröffentlicht und auf der Website der IEC zu finden ist.

### Ziele der Informationssicherheit

Informationssicherheit ist wichtig, um Informationen und andere Organisationsressourcen zu schützen. Diese Informationen können gedruckt, auf einem Computersystem gespeichert oder nur im Kopf der Benutzer:innen vorhanden sein. Der Anwendungsbereich der IT-Sicherheit umfasst daher alle Quellen einschließlich elektronisch gespeicherter Informationen und deren Verarbeitung.

Auch wenn Sicherheitsvorfälle auftreten können oder bereits aufgetreten sind, sollten Sicherheitsmaßnahmen, wenn sie implementiert und wirksam sind, dazu beitragen, das Ausmaß und die Schwere der Sicherheitsbedrohungen, mit denen eine Organisation konfrontiert sein kann, zu minimieren und die Kontinuität der Geschäftstätigkeit und den Erfolg der Organisation zu gewährleisten. Solche Bedrohungen und Schwachstellen können nicht beseitigt werden, aber ihre Auswirkungen können durch geeignete Sicherheitsmaßnahmen minimiert werden, so dass weniger Sicherheitsvorfälle auftreten.

Um ein effektives Informationssicherheitsmanagement zu gewährleisten, sollten Kontrollmaßnahmen auf der Grundlage einer Risikobeurteilung und eines Managementprozesses entwickelt und implementiert werden. Diese Kontrollmaßnahmen sollten in ein Informationssicherheitsmanagementsystem (ISMS) integriert werden. Ein ISMS besteht aus einer Reihe von Richtlinien, Prozessen, Verfahren, Organisationsstrukturen, Software und Hardware, die dazu dienen, die Informationswerte einer Organisation zu schützen. Es ist wichtig, dass das ISMS regelmäßig überprüft wird, um es an Veränderungen anzupassen und Verbesserungen an den Systemen vorzunehmen. Diese Anpassungen sollten auch die Geschäftsziele und andere strategische Ziele der Organisation berücksichtigen. Diese Maßnahmen sollten nahtlos in die bestehenden Geschäftsprozesse integriert und operationalisiert werden.

Die CIA-Triade



Quelle: Andrew Sai (2023).

Informationen können wertvoll sein. Der Wert von Informationen beruht auf ihren Eigenschaften, und Änderungen dieser Eigenschaften wirken sich entsprechend auf ihren Wert aus. Die Auswirkungen dieser Veränderungen können je nach Umständen und Nutzer:innen der Informationen unterschiedlich sein.

Um die Ziele zu erreichen, sollten Informationen für die vorgesehenen Nutzer:innen verfügbar, intakt und frei zugänglich sein. Verfügbarkeit, Zugänglichkeit und Integrität von Informationen bedeuten, dass die Nutzer:innen in der Lage sein sollten, rechtzeitig und ohne Beeinträchtigung oder Verzögerung auf die Informationen zuzugreifen. Die Gewährleistung dieser drei Ziele stellt eine Herausforderung für das Informationsmanagement dar. Jeder dieser Aspekte der Triade wird in den folgenden Unterabschnitten ausführlicher behandelt:

#### Verfügbarkeit

Die ISO/IEC 27001:2013-Normen definieren Verfügbarkeit als „Eigenschaft, auf Verlangen einer autorisierten Stelle zugänglich und nutzbar zu sein“ (Hintzbergen, J. et al., 2015). Bei der Verfügbarkeit von Informationen geht es darum, sicherzustellen, dass die Informationen rechtzeitig zur Verfügung stehen, wenn sie benötigt werden. Es ist allgemein bekannt, dass die beiden anderen Aspekte der Triade (Integrität und Vertraulichkeit) ohne Verfügbarkeit wertlos sind. Die Nutzer:innen sollten in der Lage sein, auf Informationen zuzugreifen, wenn sie die erforderlichen Berechtigungen und Bedingungen erfüllen.

Informationen gelten als verfügbar, wenn autorisierte Benutzer:innen ungehindert auf sie zugreifen können. Ein Beispiel hierfür ist die Online-Bibliothek einer Universität. Benutzer:innen bzw. Besucher:innen solcher Online-Ressourcen müssen sich identifizieren, bevor sie auf Bücher oder Materialien zugreifen können. Autorisierte Benutzer:innen werden in das Online-Bibliothekssystem aufgenommen, und nur sie können auf die Inhalte zugreifen.

Die Verfügbarkeit von Informationen kann durch verschiedene Bedrohungen wie Sabotage, Denial-of-Service-Angriffe oder Ransomware beeinträchtigt werden. Eine Maßnahme zur Abwehr solcher Bedrohungen ist die regelmäßige Sicherung der Informationen. Die Verwendung redundanter Netzwerke, Server und Anwendungen ist eine weitere Maßnahme, um die Verfügbarkeit von Informationen zu gewährleisten.

#### Vertraulichkeit

Die ISO/IEC 27001:2013-Normen definieren Vertraulichkeit als die „Eigenschaft, dass Informationen nicht unbefugten Personen, Einrichtungen oder Prozessen zugänglich gemacht oder offengelegt werden“ (Hintzbergen, J. et al., 2015). Informationen erfüllen die Anforderung der Vertraulichkeit, wenn sie vor Offenlegung oder Weitergabe ohne entsprechende Berechtigung an Personen und Systeme geschützt sind. Im Wesentlichen geht es darum, autorisierten Benutzer:innen Rechte und Privilegien für den Zugriff auf Informationen zu gewähren, die üblicherweise in IT-Systemen gespeichert und verarbeitet werden. Der unbefugte Zugriff auf solche Informationen stellt eine Verletzung der Vertraulichkeit dar. Eine Verletzung der Vertraulichkeit kann auf verschiedene Weise erfolgen. Bei manchen Formen handelt es sich um direkte Angriffe, die darauf abzielen, Zugang zu einem System zu erlangen oder eine Anwendung oder Datenbank zu infiltrieren. Ein Beispiel für direkte Angriffe sind Techniken wie **Man-in-the-Middle**-Angriffe **(MITM)**. Um die Vertraulichkeit von Informationen zu schützen, können diese

**MITM-Angriff**

Dabei handelt es sich um einen Angriff, bei dem sich ein:e Angreifer:in zwischen zwei kommunizierenden Parteien positioniert, um die zwischen ihnen übertragenen Daten abzufangen und/oder zu verändern.

* klassifiziert werden, so dass nur autorisierte Benutzer:innen Zugang zu ihnen haben. Informationen, die mit „Klasse A“ gekennzeichnet sind, könnten z. B. bedeuten, dass sie streng vertraulich und nur für wenige Personen, z. B. das Top-Management, bestimmt sind.
* sicher in Dokumentenspeichern oder mit den richtigen Tools und Ressourcen gespeichert werden.
* durch allgemeine und spezifische Sicherheitsrichtlinien geschützt werden, die den Zugriff und die Nutzung definieren.
* durch Aufklärung und Schulung von Endnutzer:innen und anderen Interessengruppen in Bezug auf die Informationssicherheit geschützt werden.

Verbraucher:innen, die das Internet und Online-Ressourcen nutzen, geben häufig persönliche Informationen über sich preis, um einen bestimmten Komfort oder Mehrwert zu erhalten. Wenn Sie sich kostenlos bei vielen Webportalen und Online-Plattformen anmelden, müssen Sie als Gegenleistung personenbezogene Daten (Personally Identifiable Information, PII) angeben, die von Dritten in der Online-Kette kopiert, verkauft, vervielfältigt oder verbreitet werden.

Vertraulichkeit ist, genau wie andere Eigenschaften von Informationen, nicht isoliert zu betrachten. Sie ist wechselseitig abhängig. Ein Merkmal ist der Datenschutz. Es gibt eine Reihe von Maßnahmen, die ergriffen werden könnten, um die Flut von Datenschutzverletzungen einzudämmen oder besser noch zu verringern. Zu diesen Maßnahmen gehören die Klassifizierung und Beschränkung des Datenzugriffs, die Implementierung von Zugriffskontrollrichtlinien, die Verschlüsselung von Daten und die Aktivierung von Multi-Faktor-Authentifizierungssystemen (z. B. 2FA). Ein weiterer guter Ansatz zur Gewährleistung der Vertraulichkeit ist die Bereitstellung von Schulungen und Wissen, das für alle Beteiligten der Informationskette leicht zugänglich ist.

#### Integrität

Integrität ist das dritte Element der Triade. Die ISO/IEC 27001:2013-Normen definieren Integrität als „Eigenschaft des Schutzes der Genauigkeit und Vollständigkeit von Vermögenswerten“ (Hintzbergen, J. et al., 2015). Die Integrität von Informationen bezieht sich auf die Sicherstellung, dass Daten nicht verändert oder verfälscht wurden. Es geht darum, dass die Informationen vollständig, authentisch, genau und zuverlässig sind.

Die Integrität von Informationen kann auf verschiedene Weise verletzt werden. Ein Beispiel ist, wenn ein:e Angreifer:in ein Intrusion-Detection-System umgeht und Dateikonfigurationen ändert, um einen unbefugten Zugriff zu ermöglichen. Ein weiteres Beispiel ist die Manipulation von Systemprotokollen und Dateien durch eine:n solchen Angreifer:in. Auch unbeabsichtigte Integritätsverletzungen können auftreten, z. B. durch einen Insider wie eine:n Mitarbeiter:in. In solchen Fällen wurden fehlende Sicherheitsrichtlinien, Sicherheitsmaßnahmen, Prozesse und Verfahren als Hauptauslöser identifiziert.

Verschiedene Maßnahmen können ergriffen werden, um die Integrität von Informationen zu schützen. Eine häufig angewandte Methode ist das Hashing oder die Verwendung von Hash-Algorithmen, um die Integrität von Daten zu überprüfen. Datenverschlüsselung, digitale Zertifikate und Signaturen sowie die Verwendung vertrauenswürdiger Zertifizierungsstellen (CAs) sind weitere Maßnahmen, die zur Sicherstellung der Integrität eingesetzt werden können. Nichtabstreitbarkeit, d. h. die Unmöglichkeit, etwas zu leugnen oder zu widerlegen, wird ebenfalls verwendet, um die Authentizität und Integrität von Informationen zu gewährleisten.

Mechanismen zur Wahrung der Informationsintegrität werden häufig in präventive und detektive Mechanismen unterteilt. Die häufigste Integritätsverletzung ist die unbeabsichtigte Offenlegung (Alsmadi I., et al. 2018). Benutzer:innen, insbesondere Mitarbeiter:innen von Organisationen, können Informationen verlieren, verlegen oder versehentlich preisgeben, ohne dass dies durch Hacker oder einen elektronischen Angriff verursacht wurde. So posten beispielsweise manche unachtsame Mitarbeiter:innen von Organisationen in sozialen Netzwerken Bilder ihrer Arbeitsplatzbildschirme, auf denen sensible Informationen offen zu sehen sind. Das ist eine unbeabsichtigte Offenlegung. Andere nehmen Kopien ihrer Organisationsdaten mit, die E-Mail-Adressen, Kreditkarteninformationen, Ausweisnummern oder wichtige Unternehmensdateien enthalten können, und verlieren diese durch Diebstahl, Kriminelle oder andere böswillige Benutzer:innen.

### Fragen zur Selbstkontrolle

1. Welches der folgenden Merkmale wird verwendet, um sicherzustellen, dass die Korrektheit der Informationen in der Organisation effektiv abgedeckt ist?
* *Integrität*
* Vertraulichkeit
* Verfügbarkeit
* Authentizität
1. Ein:e Benutzer:in meldet sich bei einem Computersystem an und wird aufgefordert, eine Sicherheitsfrage zu beantworten, z. B. „Wie lautet der Mädchenname Ihrer Mutter?“ Welchen der folgenden Punkte gewährleistet das Computersystem?
* Rechenschaftspflicht
* *Authentifizierung*
* Autorisierung
* Anwendbarkeit
1. Bitte vervollständigen Sie den folgenden Satz.

Die *Enigma* war eine *deutsche* Chiffriermaschine, die erstmals in den 1930er Jahren von *polnischen* Spezialisten geknackt wurde.