Kristin **WEBER**

MENSCH UND INFORMATIONS-SICHERHEIT

Verhalten verstehen
Awareness fördern
Human Hacking erkennen

HANSER

Weber

Mensch und Informationssicherheit

Kristin Weber

Mensch und Informationssicherheit

Verhalten verstehen, Awareness fördern, Human Hacking erkennen

HANSER

Die Autorin:
Prof. Dr. Kristin Weber, Kleinostheim

Bibliografische Information der Deutschen Nationalbibliothek:

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

Lektorat: Sylvia Hasselbach
Copy editing: Sandra Gottmann, Wasserburg
Umschlagdesign: Marc Müller-Bremer, *www.rebranding.de*, München
Titelmotiv: Tom West, unter Verwendung von Grafiken von © stock.adobe.com/bestpixels
Layout: Manuela Treindl, Fürth
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

Print-ISBN: 978-3-446-47645-5
E-Book-ISBN: 978-3-446-48040-7
E-Pub-ISBN: 978-3-446-48077-3

Inhalt

1 Der Faktor Mensch in der Informationssicherheit

Als Annika ihre E-Mails kontrolliert, freut sie sich sehr über die Einladung zur diesjährigen Faschingsparty im Vereinsheim. Schließlich ist diese Party immer das Highlight der Saison. Oft genug hatte sie in den letzten Jahren die tollsten Partymomente mit ihren Social Media Followern geteilt. Die Karten sind immer ausverkauft, und schnelles Handeln ist erforderlich. Kurz kommt es ihr verdächtig vor, dass die Einladung an ihre berufliche E-Mail-Adresse geschickt wird, und das ca. zwei Wochen früher als sonst, dann klickt sie auf den Link zur Anmeldung.

Wie diese Geschichte weitergeht, ist vermutlich klar. Es handelt sich keinesfalls um die erwartete Einladung zur Faschingsparty, sondern um eine gut gemachte Phishing-Mail, in diesem Fall um sogenanntes Spear Phishing. Die Absendenden haben sich gezielt Annikas Social-Media-Gewohnheiten zunutze gemacht und ihr eine speziell auf sie zugeschnittene, geschickt gemachte Falle gestellt. Hinter dem Link verbarg sich eine gefälschte Anmeldeseite, auf welcher Annika noch mehr von ihren persönlichen Daten preisgibt. Log-in- oder Bankdaten gelangen so in die Hände der Fallenstellenden und können für kriminelle Zwecke missbraucht werden.

Ein typisches Beispiel dafür, wie leicht Menschen manipuliert werden können, wie leichtsinnig sie mit ihren Daten umgehen und wie unsicher sie sich immer wieder verhalten? Ja und nein. Immer wieder werden Menschen als das schwächste Glied in der „Sicherheitskette“ bezeichnet – oder als größte Schwachstelle für die Informationssicherheit. In diesem Buch soll es um eine andere Sichtweise auf den Faktor Mensch gehen.

Menschen sollen nicht als Problem, sondern als Teil der Lösung gesehen werden. Der folgende Abschnitt beschreibt diese Sichtweise „Human as a Solution“ ausführlich und formuliert, für wen dieses Buch geschrieben wurde. Der Abschnitt erklärt ebenfalls den kompletten Aufbau des Buches. Der Mensch spielt in der oder für die Informationssicherheit aber nicht nur die Rolle des „Sicherheitsfaktors“. In Unternehmen kann er Opfer, Champion, Vorbild, Fehlerquelle, Bedrohung usw. sein. Abschnitt 1.2 beschreibt diese Rollen sowie Grundbegriffe und Rahmenbedingungen für dieses Buch.

Menschliche Sicherheitsfaktoren sind nur ein Element des komplexen Systems „Informationssicherheit in Unternehmen“. Abschnitt 1.3 stellt daher ein paar grundlegende Überlegungen zur Auswahl von Informationssicherheitsmaßnahmen an. Die Faktoren Sicherheit, Wirtschaftlichkeit und Usability werden gegenübergestellt. Mit Informationssicherheitsmanagementsystemen (ISMS) wird kurz auf einen systematischen Ansatz zur Gewährleistung der Informationssicherheit in Unternehmen eingegangen, in dessen Rahmen auch die Befähigung des Menschen zum Sicherheitsfaktor stattfindet. Risikoorientierung und kontinuierliche Verbesserung gemäß dem PDCA-Zyklus (Plan, Do, Check, Act) liegen den meisten ISMS zugrunde.

1.1 Der Mensch als Lösung

„... people have long been the victims of bad statistics, urban legends, and hoaxes. Any communications medium can be used to exploit credulity and stupidity, and people have been doing that for eons. [...] Semantic attacks directly target the human/computer interface, the most insecure interface on the Internet."

(Schneier, 2000)

Die Sicherheitswissenschaft (Safety Science) beschäftigt sich seit ca. hundert Jahren mit dem „Faktor Mensch" mit dem Ziel, die betriebliche Effizienz zu verbessern und menschliche Fehler, die zu Unfällen führen, zu reduzieren. In dieser Zeit hat die Disziplin eine Entwicklung vollzogen (Ebert et al., 2023; Kaur et al., 2021, S. 7; Zimmermann & Renaud, 2019, S. 13). Zunächst wurde davon ausgegangen, dass Unfälle dadurch verhindert werden können, dass menschliche Fehler eliminiert werden, z. B. durch Automatisierung, strikte Regeln und das Tragen von Schutzausrüstung. In den letzten Jahren wird verstärkt untersucht, wie der menschliche Faktor zum Erfolg in sicherheitsrelevanten Betriebsumgebungen beitragen kann. Forschende fanden heraus, dass in hochkomplexen Systemen (z. B. in der Luftfahrtkontrolle) deutlich weniger Unfälle passieren, als zu erwarten wäre. Flexibilität, Freiheit und die Fähigkeit der Mitarbeitenden, auf unbekannte Situationen zu reagieren, haben zu diesem Plus an Sicherheit beigetragen. Seitdem versucht die Sicherheitswissenschaft, besser zu verstehen, wie Menschen „funktionieren". Sie wollen weg von Schuldzuweisungen und hin zu mehr Eigenverantwortung und dem Lernen aus Fehlern. Menschen werden nicht mehr als Problem, sondern als Teil der Lösung angesehen.

In der Informationssicherheit scheint ein ähnliches Umdenken gerade stattzufinden. Doch noch immer liest man viel zu häufig Schlagzeilen wie:

- „Faktor Mensch – Mitarbeiter als schwächstes Glied der Sicherheitskette"
- „IT-Sicherheit: Der Mensch ist das Problem"
- „Der Faktor Mensch als schwächstes Glied in der Security-Kette"
- „Cybersicherheit 2021: Top 5 Risiken in Unternehmen – 1. Risiko: Der Mensch"

Häufig werden Mitarbeitende als Schuldige für Informationssicherheitsvorfälle verantwortlich gemacht: „(1) If a hacker exploits software vulnerabilities, that is the fault of the IT staff for not keeping the system patched and secure. (2) If someone falls for a phishing message, they did not pay enough attention. (3) If a breach occurs, it is possible that someone leaked their password or chose a weak one." (Zimmermann & Renaud, 2019, S. 10) Auf diese Weise kann jedes unerwünschte Ereignis auf menschliches Versagen zurückgeführt werden, und der Mensch wird als diejenige Komponente des Systems[1] angesehen, welche der Informationssicherheit im Wege steht.

[1] Unternehmen können als „soziotechnische Systeme" angesehen werden, bestehend aus verschiedenen technischen, organisatorischen und menschlichen Komponenten, die auf vielfältige Weise miteinander interagieren und eine Einheit bilden (Klipper, 2022).

Folglich können Informationssicherheitsverstöße vermieden werden, wenn das Verhalten der Menschen überwacht und vor allem eingeschränkt wird. Menschen sind ein Problem, das unter Kontrolle zu bringen ist (Schneier, 2000). Als Lösungen werden vorgeschlagen:

- Menschen so weit wie möglich aus dem System entfernen, d. h., viel automatisieren und technische Sicherheitslösungen den organisatorischen oder personellen Maßnahmen vorziehen
- Mitarbeitende schulen und Awareness-Maßnahmen durchführen, wo das „Entfernen" nicht möglich ist
- Richtlinien für richtiges und falsches Verhalten aufstellen und diese streng durchsetzen

Als Reaktion auf Vorfälle ist es wichtig, die Schuldigen auszumachen, sie zu bestrafen und noch mehr Training zu verordnen. Bezeichnend für diese Sichtweise ist das folgende Zitat:

> *„Zu den bisherigen Ausführungen über Sicherheit kommt der Mensch als weiterer Faktor hinzu. Bei komplexen Systemen spielt es naturgemäß auch eine Rolle, inwieweit die Benutzer Art und Zweck der Benutzung korrekt erfasst haben. Dies bedeutet in letzter Konsequenz, dass ein System … sicher sein und dennoch gefährdend eingesetzt werden kann, falls es vom Benutzer, auch unwissentlich, missbraucht wird und keine Verriegelungsmechanismen dagegen vorhanden sind."*
>
> (Freiling et al., 2014, S. 23)

In Wirklichkeit gibt es bei Informationssicherheitsvorfällen häufig mehrere Ursachen. Der Mensch trägt sicherlich in vielen Szenarien dazu bei, dass etwas Ungeplantes oder Ungewolltes passiert, aber dies ist nicht die ganze Geschichte. Soziotechnische Systeme sind komplex, hochgradig interaktiv und unvorhersehbar, und mehrere Faktoren führen zu unerwünschten Ereignissen (Ebert et al., 2023; Klipper, 2022; Zimmermann & Renaud, 2019, S. 11).

Der Prozess des Umdenkens in der Informationssicherheit sollte sich fortsetzen, und ähnlich wie in der Sicherheitswissenschaft sollte der Mensch nicht mehr als Problem, sondern als Teil der Lösung gesehen werden. Zimmermann und Renaud (2019) schlagen dieses neuen Paradigma – **Humans as Solution** – mit folgenden Prinzipien vor:

- Menschen sind integraler Bestandteil und unverzichtbar für das Funktionieren von soziotechnischen Systemen und tragen damit zur Sicherheit bei.
- Die nicht immer vorhersehbaren Handlungen der Menschen können zu Fehlern führen. Aber – diese Unvorhersehbarkeit ist eine Stärke, da sie weit häufiger zu normalen Abläufen und deren Erfolg beiträgt als zu Fehlern. Werden Menschen aus dem System „eliminiert", können sie nicht aktiv zum Erhalt und zur Verbesserung der Sicherheit beitragen.
- Menschen versuchen grundsätzlich, einen „guten Job zu machen" und nicht Fehler zu verursachen. Halten sie sich nicht an Sicherheitsregeln, dann haben sie meist einen guten Grund dafür, z. B. dass die Regeln sie in der Ausübung ihrer eigentlichen Tätigkeit behindern. Daher sollten Menschen beim Erstellen der Sicherheitsregeln mit einbezogen werden.
- Sicherheitsvorfälle sollten untersucht werden, um daraus etwas zu lernen, und nicht, um Schuldige zu finden.
- Statt sich über Fehler zu ärgern, sollte man auf Erfolge stolz sein. Beispielsweise fallen fast 80 % der Angestellten NICHT auf Phishing herein.

Automatisierung hat auch in diesem Paradigma seine Berechtigung. Es gibt Aufgaben, welche besser durch Computer erledigt werden können, z. B. Aufgaben, die mit hoher Präzision und Geschwindigkeit zu wiederholen sind. Diese Art von Aufgaben können und sollten automatisiert werden. Technische Sicherheitsmaßnahmen können bis zu einem gewissen Grad menschliches Fehlverhalten verhindern oder kompensieren (Beyer et al., 2015). Es gibt aber auch Aufgaben, in welchen Menschen bessere Ergebnisse erzielen, z. B. beim Improvisieren und bei der Entscheidungsfindung unter unvollständigen Informationen. Bei diesen Aufgaben macht Automatisierung keinen Sinn.

In der Sicherheitswissenschaft wird anerkannt, dass in vielen Fällen „Heldentaten" Unfälle verhindert haben oder schlimmere Folgen abmildern konnten (Pfleeger et al., 2014). Heartfield und Loukas (2018) zeigen durch Experimente, dass Menschen auch in der Informationssicherheit Sicherheitsvorfälle sehr zuverlässig entdecken können. Die Forscher simulierten komplexe Social Engineering-Angriffe, basierend auf Spear Phishing, verschickten USB-Sticks oder falschen Facebook-Accounts. Lediglich 10 % dieser Angriffe wurden von den Anwendenden nicht erkannt. Im Vergleich dazu schlugen die eingebauten technischen Sicherheitssensoren bei 81 % der Angriffe keinen Alarm.

Auch Burkhead (2014, S. 114 f.) stellt fest, dass Menschen nicht nur unverzichtbar beim Erkennen und Melden von Sicherheitsvorfällen sind, sondern auch erfolgreicher und effizienter als Tools. Anwendende merken, dass sich ihr Rechner ungewöhnlich verhält, und melden dies an die Verantwortlichen. Sie können den IT-Helpdesk innerhalb weniger Sekunden darauf hinweisen, dass sie eine Phishing-E-Mail bekommen haben. Sie sprechen Personen auf dem Firmengelände an, wenn diese keinen Ausweis tragen, oder sie geben gefundene USB-Sticks sowie andere dubiose Datenträger ab. Unternehmen sind hochkomplexe Systeme, welche ohne die Unterstützung des Faktors Mensch nicht ausreichend zu schützen sind (Drechsler, 2019, S. 79).

Um besser zu verstehen, wie Menschen dazu beitragen, Sicherheitsvorfälle zu verhindern, sollten auch Erfolge bzw. sogenannte „Near Misses" untersucht werden, also Vorfälle, die gerade noch so verhindert werden konnten (Bair et al., 2018; Beyer et al., 2015). Häufig sind es die gleichen Faktoren, die zu Erfolg oder Misserfolg führen. Daher sollten immer beide mögliche Auswirkungen (Erfolg und Misserfolg) betrachtet werden, bevor über eine Sicherheitsmaßnahme entschieden wird. Was wird dadurch verhindert – im positiven wie negativen Sinne? Statt zu versuchen, Risiken durch zu starre und einschränkende Sicherheitsmaßnahmen zu vermeiden, sollte die Widerstandsfähigkeit gestärkt werden (Zimmermann & Renaud, 2019, S. 19). Menschen sollten die Flexibilität bekommen, ihr Verhalten an das veränderte Verhalten des soziotechnischen Systems anzupassen. Das versetzt sie in die Lage, ihren Beitrag zu leisten, ein gefährdetes System wieder in einen stabilen Zustand zu bringen.

Für das Paradigma *Human as Solution* ist ein Umdenken an vielen Stellen in Unternehmen erforderlich. Die Art und Weise, wie heute noch vielfach mit dem „Faktor Mensch" in der Informationssicherheit umgegangen wird, muss hinterfragt werden. Der Mensch muss als Teil des Systems verstanden werden, seine Bedürfnisse, Fähigkeiten und Eigenschaften in das Design sicherer Lösungen einbezogen werden. Menschen sollten als elementarer Bestandteil des Informationssicherheitskonzepts verstanden werden. Sie sind nicht nur passiv, halten sich an Regeln und reagieren auf Ereignisse. Dürfen sie sich am Thema Informationssicherheit aktiv beteiligen und Verantwortung für ihre Handlungen übernehmen, führt dies zu bewusstem und sichererem Verhalten (Adams & Sasse, 1999, S. 45; Sasse et al., 2023, S. 250).

Als Teil des Paradigmenwechsels muss analysiert werden, warum Menschen sich so oder so verhalten, die Komplexität der Einflussfaktoren muss gewürdigt und die Wechselwirkungen müssen verstanden werden. Die Awareness der Mitarbeitenden für Informationssicherheit ist ein zentraler Baustein für ein sicheres System. Mitarbeitende müssen befähigt werden, ihrer wichtigen Rolle gerecht zu werden. Sie sollen sich nicht stur an Regeln halten, sondern eigenständig entscheiden und so handeln, wie es im Moment erforderlich ist. Eine „Mindfulness" oder gewisse Resilienz erlaubt es ihnen, sich auch in unbekannten, nicht trainierten Situationen richtig zu verhalten.

Dieses Plus an Verantwortung und ein Minus an strengen Vorgaben kann dazu führen, dass es vorsätzlich böswillig handelnden Personen einfacher gemacht wird, Organisationen Schaden zuzufügen (Zimmermann & Renaud, 2019, S. 24). Dieses zusätzliche Risiko steht allerdings im Kontrast zu der Tatsache, dass nicht mehr allen Personen in den Organisationen per se unterstellt wird, dass sie Schaden verursachen wollen. Alle Personen zu gängeln, obwohl sich nur ein sehr kleiner Teil absichtlich schadhaft verhält, ist unverhältnismäßig und zeugt nicht von einer förderlichen Sicherheitskultur.

Zielgruppe und Aufbau

Dieses Buch ist für alle Menschen,

- denen Informationssicherheit am Herzen liegt,
- die Menschen als wichtigen Informationssicherheitsfaktor (und nicht als Risikofaktor) sehen,
- die sich mit Leidenschaft für die Sensibilisierung junger und älterer Menschen für die Informationssicherheit einsetzen,
- die verstehen wollen, warum ihre Awareness-Kampagnen und Awareness-Maßnahmen (nicht) funktionieren,
- die sich in Theorie oder Praxis mit Information Security Awareness beschäftigen (müssen),
- die Inspirationen für Awareness-Maßnahmen, für Sensibilisierungskampagnen oder einfach nur für einen empathischen und effektiven Umgang mit dem Faktor Mensch (in der Informationssicherheit) suchen,
- die Informationssicherheitsmaßnahmen für (und nicht gegen) Menschen entwickeln möchten,
- die Interesse haben, sich mit (Verhaltens-)Psychologie zu beschäftigen, und verstehen wollen, wie Menschen „ticken",
- die Security Champions aus Leidenschaft sind.

Die einzelnen Kapitel des Buches können mehr oder weniger unabhängig voneinander gelesen werden. Für ein umfassendes Verständnis der behandelten Inhalte empfiehlt es sich allerdings, das gesamte Buch zu lesen. Gerade das verhaltenspsychologische Verständnis von Awareness ist wichtig, um die Kapitel zum Fördern und zum Messen von Awareness komplett nachvollziehen zu können. Die einzelnen Kapitel beschäftigen sich mit den folgenden Inhalten:

- **Kapitel 1 – Der Faktor Mensch in der Informationssicherheit:** Dieses einführende Kapitel stellte zunächst mit dem Paradigma „Human as Solution" das Grundverständnis über den Faktor Mensch in der Informationssicherheit vor. Zudem definiert es für das Buch grundlegende Begriffe, wie Risiko, Informationssicherheit, ISMS oder Bedrohung,

und beschreibt Rahmenbedingungen. Es stellt die verschiedenen Rollen vor, die Menschen für die oder in der Informationssicherheit in Organisationen haben. Mit Sicherheit, Wirtschaftlichkeit und Usability werden drei Einflussfaktoren auf die Auswahl von Sicherheitsmaßnahmen beschrieben.

- **Kapitel 2 – Der Mensch als Bedrohung:** Das zweite Kapitel widmet sich dem Menschen als Bedrohung für die Informationssicherheit. Zunächst werden typische Szenarien dargestellt, in welchen das richtige Handeln der Menschen eine entscheidende Rolle für die Gewährleistung der Informationssicherheit in Organisationen hat. Im Anschluss wird untersucht, warum sich Menschen nicht immer informationssicher verhalten. Der Rest des Kapitels betrachtet den Menschen als böswillig handelnden Insider in Organisationen. Es beschreibt Hintergründe und Maßnahmen zum Erkennen und Abwehren von Malicious Insidern.
- **Kapitel 3 – Der Mensch als Opfer:** Unstrittig ist, dass Menschen in Organisationen gezielt angegriffen werden, um andere Sicherheitsmaßnahmen zu umgehen. Dafür manipulieren in den meisten Fällen sogenannte Social Engineers Menschen geschickt mit verschiedenen Tricks und Methoden. Wie Social Engineers arbeiten und wie sie bei ihren Angriffen vorgehen, betrachtet das dritte Kapitel. Es schaut sich verschiedene Formen von Social Engineering an und beschreibt psychologische Prinzipien, die zur Manipulation von Menschen eingesetzt werden. Ein umfassendes Verständnis über Social Engineering ist notwendig, um Schutzmaßnahmen dagegen zu etablieren.
- **Kapitel 4 – Information Security Awareness:** Ab dem vierten Kapitel geht es schwerpunktmäßig um die Sensibilisierung der Organisationsmitglieder für Informationssicherheit. Der Begriff Information Security Awareness und verschiedene Konzepte dazu werden vorgestellt, bevor das Verständnis von Awareness basierend auf dem Integrated Behavioral Model näher ausgeführt wird. Aus diesen Erklärungen wird deutlich, dass beim Thema Awareness an einer individualisierten, oder zumindest zielgruppenorientierten, Vorgehensweise kein Weg vorbeiführt. Was Individualisierung im Kontext Awareness bedeutet, ist daher ebenfalls Gegenstand des vierten Kapitels. Im Anschluss wird ein Vorgehensmodell zur zielgerichteten Sensibilisierung von Personen in Organisationen vorgestellt. Das Vorgehensmodell umfasst neun Schritte in zwei Phasen und beginnt mit der Analyse der Ist-Situation.
- **Kapitel 5 – Information Security Awareness fördern:** Basierend auf dem verhaltenspsychologischen Verständnis von Awareness beschreibt das fünfte Kapitel, wie die einzelnen Faktoren von Awareness Wissen/Fähigkeiten, Verhaltensabsicht, Salienz und Gewohnheit gezielt verbessert, verändert oder gefördert werden können. Verschiedene Maßnahmen und deren beabsichtigte Wirkung werden anhand von Beispielen erläutert. Im Kontext Wissen werden beispielsweise Überlegungen zum Lernen und zur Didaktik angestellt. Um Einstellungen und Überzeugungen zu ändern, welche die Verhaltensabsicht formen, sind passende Instrumente Feedback, Vorbilder, Belohnung, unterstützende Tools oder die Beseitigung von Hürden. Zur Förderung der Salienz kommen vielfach Medien und Kommunikation zum Einsatz. Für die Gewohnheitsbildung ist regelmäßige Ausführung des gewünschten Verhaltens im immer gleichen Kontext entscheidend.
- **Kapitel 6 – Messen von Information Security Awareness:** Um Awareness gezielt zu verbessern, muss zunächst der aktuelle Zustand der Awareness bei den Mitgliedern der Organisation bestimmt werden. Das psychologische Verständnis von Awareness liefert verschiedene Ansatzpunkte, um die einzelnen Faktoren zu messen und zu bewerten.

Diese Möglichkeiten beschreibt das sechste Kapitel. In den meisten Fällen basieren Messmethoden auf Varianten von Befragungen und Umfragen. Beispiele demonstrieren einige der vorgestellten Methoden.

- **Kapitel 7 – Ausblick:** Das letzte Kapitel fasst noch einmal die wesentlichen Aspekte der vorangegangenen Kapitel zusammen und gibt einen Ausblick auf weitere spannende Themen im Kontext Mensch und Informationssicherheit, die leider keinen Einzug mehr in dieses Buch gefunden haben.

1.2 Wer bin ich – und wenn ja, wie viele?[2]

Der Fokus dieses Buches liegt auf der Informationssicherheit innerhalb von Unternehmen oder allgemeiner von Organisationen.[3] Es ist somit der Disziplin der Wirtschaftsinformatik zuzuordnen. Die gesellschaftliche Relevanz und private Aspekte von Informationssicherheit werden in Ansätzen, aber nicht vordergründig betrachtet. Somit bezieht sich die Informationssicherheit immer auf die Absicherung von Informationen und Informationssystemen in Unternehmen/Organisationen. In Unternehmen gibt es meist interne oder externe Fachpersonen, deren Aufgabe es ist, die Informationen und Informationssysteme des Unternehmens durch angemessene physische, technische, organisatorische und personenbezogene Maßnahmen zu schützen. Das Vorgehen dabei ist idealerweise systematisch und risikobasiert (vgl. Abschnitt 1.3). Risikobasiert bedeutet, dass die Maßnahmen unter Kosten-Nutzen-Gesichtspunkten ausgewählt werden. Es geht nicht darum (und das ist auch nicht möglich), 100 % Sicherheit zu gewährleisten, sondern unter Abwägung von Aufwand, Kosten und potenziellem Schaden die optimalen Maßnahmen zu treffen.

Eine kurze, sehr passende Definition zu **Informationssicherheit** findet sich in den Standards des amerikanischen NIST (National Institute of Standards and Technology):

> *The term „information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.*
>
> (Barker, 2003, S. 15)

Im Unterschied zu IT-Sicherheit umfasst Informationssicherheit auch Informationen, die außerhalb von IT-Systemen existieren, sich also z. B. auf Papier befinden oder in den Köpfen der Mitarbeitenden. Informationssicherheit ist ein umfassenderer und ganzheitlicherer Ansatz als IT-Sicherheit. Informationssicherheit will jegliche Art von Information schützen, egal auf welchem Medium gespeichert, verarbeitet oder übertragen.

---

[2] Richard David Precht, 2007

[3] Im Buch wird häufiger von Unternehmen und Mitarbeitenden oder Belegschaft gesprochen. Dennoch gelten viele Aspekte zur Berücksichtigung des Faktors Mensch für jede Art von Organisation oder Institution, ob Hochschule, Verein oder Gemeinde, und deren Mitglieder analog.

Die drei primären Schutzziele der Informationssicherheit sind Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Um die Vertraulichkeit zu schützen, müssen unautorisierter Zugriff und unbeabsichtigte Bekanntgabe von Informationen unterbunden werden. Integrität bedeutet, Informationen gegen unerlaubte Änderungen zu schützen. Mit der Verfügbarkeit soll sichergestellt werden, dass die gewünschte Information autorisierten Nutzenden zeitnah und zuverlässig zugänglich und nutzbar ist.

Informationssicherheit bezieht sich also nicht immer nur auf den Schutz vor Cyberangriffen, Phishing, Ransomware, Hacking & Co. Weitaus grundlegender ist die kontinuierliche Aufrechterhaltung der Informationsversorgung der Mitarbeitenden im Unternehmen, die auch „nur" durch Hardwarefehler, falsche Konfiguration, unbeabsichtigtes Löschen oder Kabelbrand gefährdet sein kann. Einen Überblick über typische **Gefährdungen** für die Informationssicherheit führt das BSI (Bundesamt für Sicherheit in der Informationstechnik) im IT-Grundschutz auf. In den (nicht mehr gültigen) IT-Grundschutz-Katalogen sind über 650 Gefährdungen gelistet (BSI, 2016).[4] Diese teilen sich auf fünf Kategorien auf: Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen (vgl. Tabelle 1.1). Vorsätzliche Handlungen wie Sabotage, Diebstahl oder Social Engineering machen hier rein mengenmäßig ca. ein Drittel der genannten Gefährdungen aus. Dies sagt allerdings nichts über die Schwere der Gefährdung und auch nichts über das tatsächliche Vorkommen in der Praxis aus. Ähnlich gewichtig sind organisatorische Mängel, zu denen fehlende Regelungen (z. B. Zugangsregeln, Berechtigungen) und fehlende Verantwortlichkeiten gehören, ein unzureichendes Sicherheitsmanagement oder fehlende Sensibilisierung.

Tabelle 1.1 Gefährdungen für die Informationssicherheit (eigene Darstellung)

Nr.	Kategorie	Anzahl Gefährdungen (Anteil)	Beispiele
1	Höhere Gewalt	19 (3 %)	Feuer, Personalausfall, Verschmutzung, technische Katastrophen im Umfeld
2	Organisatorische Mängel	214 (32 %)	Fehlende Regelungen, unzureichende Schulungen, mangelhaft festgelegte Verantwortlichkeiten, Abhängigkeit von Dienstleistern, nicht erkannte Sicherheitsvorfälle
3	Menschliche Fehlhandlungen	124 (19 %)	Fehlbedienung, Sorglosigkeit im Umgang mit Informationen, ungeeignetes Verhalten bei der Internet-Nutzung, Nichtbeachtung von Sicherheitsmaßnahmen
4	Technisches Versagen	101 (15 %)	Defekte Datenträger, Hardwarefehler, Ausfall der Stromversorgung, Störung von Komponenten, Fehlfunktionen
5	Vorsätzliche Handlungen	206 (31 %)	Diebstahl, Manipulation, Social Engineering, Missbrauch von Benutzungsrechten, Ausprobieren von Passwörtern, Sabotage

[4] Das seit 2018 gültige IT-Grundschutz-Kompendium führt nur noch die 47 elementaren Gefährdungen auf, welche allgemeingültiger sind und in der Praxis fast immer vorkommen (s. (BSI, 2023)).

Menschliche Fehlhandlungen sind eine weitere Kategorie, die immerhin auch über hundert verschiedene Gefährdungen ausweist, darunter fahrlässige Zerstörung, fehlerhafte Bedienung oder Konfiguration, Fehleinschätzungen und sorgloser Umgang mit Information. Hier findet sich die Sichtweise „Risikofaktor Mensch“ wieder.

Menschen haben aber nicht nur diese Rolle als Risikofaktor, sondern verschiedene Rollen in der oder für die Informationssicherheit in Organisationen. Die meisten Menschen werden mehrere dieser Rollen gleichzeitig einnehmen. Die einzelnen Rollen sollen im Folgenden kurz erläutert werden.

Vordergründig sind Menschen **Anwendende** (auch End User, s. (Kaur et al., 2021, S. 5)), d. h., sie verarbeiten Informationen der Organisation und benutzen dazu deren Informationssysteme. Anwendende sollen sich sicher verhalten. Sie sollen weder unwissentlich noch absichtlich Schaden verursachen (die Informationssicherheit gefährden), und sie sollen sich an die vorgegebenen Regeln und Richtlinien halten. Da Anwendende besondere Fachexpertise in ihrem jeweiligen Fachgebiet, dessen betrieblichen Abläufen und besonderen Anforderungen besitzen, sollten sie auch verstärkt in die Entscheidung über für die Organisation passende Sicherheitsmaßnahmen einbezogen werden (Zimmermann & Renaud, 2019). Behindern die Sicherheitsmaßnahmen die Anwendenden bei der Ausführung ihrer eigentlichen (primären) Arbeit für die Organisation, werden sie meist nicht umgesetzt oder eingehalten (vgl. Abschnitt 2.1.2).

Damit einher geht die Rolle als **Bedrohung** (oder Gefährdung, s. o.). Anwendende, die unbewusst oder bewusst Richtlinien unterlaufen, gefährden die Informationssicherheit der eigenen Organisation. Sie treffen tagtäglich Entscheidungen, welche sicherheitsrelevant sind. Sie posten beispielsweise sensible Informationen auf Social Media, sie lassen ihr Smartphone oder Notebook unbeaufsichtigt herumliegen, sie nutzen unsichere Passwörter oder sperren ihren Bildschirm nicht, wenn sie den Arbeitsplatz verlassen (vgl. Abschnitt 2.1). Geschieht dieses Fehlverhalten ohne böswillige Absicht der Anwendenden, dann handelt es sich um Negligent bzw. Accidental Insider (vgl. Abschnitt 2.2.1).

Menschen können aber auch die Rolle **Angreifende** einnehmen. In dieser Rolle versuchen sie aus verschiedenen Gründen, bewusst die Informationssicherheit der Organisation zu unterwandern und dabei Schaden zu verursachen oder sich selbst einen Vorteil zu verschaffen. Sie stehlen beispielsweise Informationen, um diese zu verkaufen, oder sie verschlüsseln mittels Ransomware einen Teil der IT-Infrastruktur und verlangen Lösegeld von ihren Opfern. Typische Angreifende sind Cyberkriminelle, Hackende, das organisierte Verbrechen, Geheimdienste, staatliche Institutionen oder Wettbewerber (ISACA, 2022, S. 33; KPMG, 2022, S. 20 ff.).

Während die meisten Angreifenden nicht Mitglieder der angegriffenen Organisation sind, gibt es Anwendende, die bewusst und mit böswilliger Absicht der eigenen Organisation schaden. Diese **Malicious Insider** (vgl. Abschnitt 2.2.3) veröffentlichen z. B. vertrauliche Informationen oder sabotieren die eigene IT-Infrastruktur. Gründe für ein derartiges Verhalten finden sich viele. Neben finanziellen Motiven können es ideelle Gründe, aber auch Stress oder persönliche Krisen sein.

Angreifende entscheiden sich häufig bewusst dafür, nicht die technische Infrastruktur anzugreifen. Sie versuchen Sicherheitsmaßnahmen zu umgehen, indem sie gezielt den Menschen angreifen. Der Mensch wird zum **Opfer**. Menschen sind ein lohnendes Angriffsziel, da sie wertvolle Informationen besitzen oder Zugriff darauf haben (vgl. Lauer & Kuntze, 2022, S. 38).

Als Social Engineering werden die meisten Angriffsformen bezeichnet, in welchen Menschen geschickt manipuliert werden (vgl. Kapitel 3). Phishing-Mails dienen häufig dazu, Passwörter abzugreifen, oder Social Engineers geben sich als Technikpersonal aus, um unberechtigten Zugang zu einem Gebäude oder Raum zu erhalten.

Auf der Seite der Verteidigung finden sich Fachpersonen oder **Sicherheitsexpert:innen**. Diese bemühen sich um die Aufrechterhaltung der Informationssicherheit. Ihre Aufgabe ist es, durch technische, physische, organisatorische und personelle Sicherheitsmaßnahmen die Organisation vor potenziellen Gefahren von außen und innen zu schützen und Risiken zu minimieren. Hierunter können verschiedene Rollen subsumiert werden: z. B. Personen, welche

- Regeln aufstellen,
- die Einhaltung von Regeln überwachen,
- Sicherheitslücken aufdecken,
- Sicherheitsvorfälle analysieren,
- andere Personen sensibilisieren,
- die Sicherheit der IT-Infrastruktur überwachen sowie
- technische Sicherheitsmaßnahmen designen, konfigurieren und administrieren.

Besondere Rollen für die Informationssicherheit haben Führungskräfte. Sie sind diejenigen, die das Budget für Sicherheitsmaßnahmen bereitstellen und die Vorhaben ideell unterstützen und fördern. Idealerweise hat ein Unternehmen noch viel mehr **Unterstützende**, so etwa motivierte Mitarbeitende, denen Informationssicherheit ein persönliches Anliegen ist und die nicht nur selbst auf einen sicheren Umgang mit Informationen achten, sondern auch andere motivieren und dabei unterstützen, es ihnen gleichzutun (vgl. Lauer & Kuntze, 2022, S. 46). Häufig werden diese als **Security Champions** bezeichnet (vgl. Abschnitt 5.2.2).

Insbesondere Führungskräfte sollten **Vorbild** für die Mitarbeitenden sein. Wenn sie sich sichtbar informationssicher verhalten und regelmäßig im Team über richtiges Verhalten reden, zeigt es die Stellung der Informationssicherheit für das Unternehmen und untermauert die Bedeutung der aufgestellten Regeln (vgl. Abschnitt 5.2.3). Dies begünstigt das informationssichere Verhalten der anderen Organisationsmitglieder. Sind Vorgesetzte der Meinung, dass die aufgestellten Regeln für sie nicht gelten, vergiftet dies die Sicherheitskultur (Beyer et al., 2015). Zu einer vorgelebten Sicherheitskultur gehört es, Anwendende zu ermutigen, Sicherheitsverstöße zu melden, statt sie für ein mögliches Fehlverhalten zu bestrafen.

Die Leitung der Organisation hat zudem die Rolle **Verantwortliche**. Trotz Delegation der Informationssicherheitsaufgaben an die Fachpersonen bleibt die Unternehmensleitung verantwortlich für die Aufrechterhaltung der Informationssicherheit. Dennoch sind auch alle Anwendenden im Rahmen der Erfüllung ihrer Aufgaben verantwortlich für die Sicherheit der Informationen und Informationssysteme, soweit dies für sie zumutbar ist (vgl. Lauer & Kuntze, 2022, S. 45). Meist wird diese Verantwortung durch Regeln und Richtlinien definiert, und die Anwendenden werden für das sichere Verhalten entsprechend auch geschult.

Personen, die für das Design, die Entwicklung, die Konfiguration oder den Betrieb von Informationssystemen zuständig sind, können auch eine **Fehlerquelle** sein (vgl. Kaur et al., 2021, S. 4; Lauer & Kuntze, 2022, S. 38). Passieren in der Softwareentwicklung Fehler, werden Vorgaben zum Security by Design nicht eingehalten oder werden falsche Konfigurationen vorgenommen, können Sicherheitslücken entstehen, die durch Angreifende ausgenutzt werden

können. Eine Analyse von erfolgreichen Cyberattacken der vergangenen Jahre führt ca. ein Viertel aller Angriffe auf Konfigurationsfehler zurück (Quader & Janeja, 2021).

Dann gibt es auch noch diejenigen, die von den Sicherheitsmaßnahmen und einer gestiegenen Sicherheit des Unternehmens profitieren. Man könnte sie **Kundschaft** oder Nutznießende nennen. Darunter fallen alle Mitglieder des Unternehmens und einige externe Parteien. Sind die Daten und die IT-Infrastruktur des Unternehmens sicher, so sind auch die (personenbezogenen, sensiblen) Daten der Mitarbeitenden, Kund:innen, Lieferant:innen und anderer Partnerunternehmen in der Hoheit des Unternehmens vor Missbrauch geschützt. Mitarbeitende haben einen „sicheren" Arbeitsplatz, bekommen weiterhin ihren Lohn, und das Unternehmen kann nach wie vor seinen Unternehmenszweck ausüben (z. B. zur Versorgung der Bevölkerung mit medizinischen Dienstleistungen, Bargeld, Ernährung, Trinkwasser oder Energie). Nicht umsonst gibt es mit dem IT-Sicherheitsgesetz 2.0 einige Auflagen zur Vermeidung von Störungen der Informationssysteme für Unternehmen, welche der kritischen Infrastruktur[5] angehören (vgl. Jansen, 2022, S. 71 f.).

Eine weitere Rolle wurde an dieser Stelle noch nicht explizit genannt. Die Anwendenden sollen insbesondere als **Sicherheitsfaktor** verstanden werden, als „letzte Verteidigungslinie", als „wichtigstes Glied in der Sicherheitskette", als „menschliche Firewall", als „Sicherheitssensoren" oder auch als „Stütze des Informationssicherheitskonzepts". Anwendende, die dieser Rolle nachkommen, verhalten sich nicht nur gemäß den aufgestellten Regeln. Sie sind generell aufmerksam und in der Lage, auch in unbekannten, vorher nicht trainierten Situationen, richtig (sicher) zu reagieren. Sie schützen durch ihr umsichtiges Handeln sich und andere vor Gefahren für die Informationssicherheit. Sie melden Gefahren, mögliche Sicherheitsvorfälle oder ungewöhnliches Verhalten ohne Zögern an das Fachpersonal und tragen somit wesentlich dazu bei, dass schnell weitere Maßnahmen zum Schutz der Organisation und ihrer Mitglieder getroffen werden können und Schaden verhindert werden kann.

Die Rollen sind nicht überschneidungsfrei, und es können je nach Detaillierungsgrad weitere gefunden werden. Dieses Buch fokussiert besonders auf die Rollen Anwendende und Sicherheitsfaktor. Angreifende werden nur im Kontext Social Engineering näher betrachtet und in diesem Zusammenhang auch die Rolle Opfer. Der Mensch als Bedrohung – auch in Form von Malicious Insidern – wird ebenfalls Beachtung finden. Aufgrund der hohen Bedeutung, Anwendende in Sicherheitsfaktoren zu verwandeln, werden auch die Rollen Unterstützende, Vorbild und Informationssicherheitsexpert:innen berücksichtigt. Der Fokus ist immer auf den der großen Masse der „normalen" Anwendenden in Organisationen und wie diese für informationssicheres Verhalten sensibilisiert werden können. Spezielle Programme für Führungskräfte oder IT-Personal sollen unberücksichtigt bleiben.

[5] Zur Kritischen Infrastruktur (KRITIS) gehören Unternehmen, die Dienstleistungen anbieten, welche der „Versorgung der Allgemeinheit ... [dienen und] deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde". (BSI-KritisV, § 1)

1.3 Informationssicherheit

Um die Komplexität der Informationssicherheit in Unternehmen zu beherrschen, empfiehlt sich ein organisiertes und strukturiertes Vorgehen. Ein **Managementsystem für Informationssicherheit (ISMS)** bietet eine solch systematische Vorgehensweise und Berücksichtigung aller Aspekte, welche in Organisationen für die Gewährleistung der Informationssicherheit notwendig sind. Dazu gehören die Gestaltung und Umsetzung organisatorischer, personenbezogener, physischer und technischer Sicherheitsmaßnahmen. Vor allem sollen auch Prozesse und Verantwortlichkeiten geschaffen werden, um dies systematisch, auf Dauer angelegt und sich kontinuierlich verbessernd durchzuführen.

Bei der Konzeption ihres ISMS orientieren sich die meisten Unternehmen an etablierten Standards und Rahmenwerken (im Folgenden „Standards“) wie der ISO 27001, dem BSI IT-Grundschutz oder CISIS12. Die ISMS-Standards repräsentieren die kollektive Erfahrung vieler Organisationen („Best Practices“). Sie beschreiben also Prozesse und Maßnahmen, die in der Praxis tatsächlich funktionieren und dem Stand der Technik („State of the Art“) entsprechen. Unternehmen nutzen Standards als Referenz oder Ideengeber für das eigene Vorgehen oder als Nachschlagewerk für geeignete Sicherheitsmaßnahmen. Ist das Ziel eine Zertifizierung nach dem jeweiligen Standard, so müssen die Inhalte, sofern zutreffend, in das eigene ISMS übernommen und können an die eigenen Bedürfnisse angepasst werden.

PDCA-Zyklus

Den meisten Standards inhärent ist das Prinzip der kontinuierlichen Verbesserung. Sie berücksichtigen, dass eine Organisation nie den Zustand erreichen wird, in dem das ISMS „fertig“ ist. Selbst wenn ein akzeptabler (z. B. zertifizierter) Zustand erreicht wurde, gilt es dennoch, das ISMS fortlaufend an neue Rahmenbedingungen anzupassen und das Feedback aus dem laufenden Betrieb einzuarbeiten.

Neue Rahmenbedingungen ergeben sich einerseits durch Änderungen innerhalb des Unternehmens. Die Ziele der Informationssicherheit sollten sich stets an der strategischen Ausrichtung des Unternehmens orientieren. Ändern sich Strategie, Organisation oder Geschäftsprozesse im Unternehmen, ändern sich die Anforderungen an die Informationssicherheit. Schließt das Unternehmen beispielsweise eine große Forschungskooperation ab, muss den Forschungsparteien sicherer Zugriff auf die internen Forschungsergebnisse ermöglicht werden. Eröffnet das Unternehmen mehrere Vertriebsstandorte in anderen Ländern, müssen diese sicher an die zentrale IT-Infrastruktur angebunden werden. Sollen Mitarbeitende im Außendienst über mobile Endgeräte auf die IT-Systeme im Backend zugreifen, muss hierfür eine sichere, mobile Verbindung geschaffen werden. Beschließt das Unternehmen, zukünftig verstärkt auf Cloud-Dienstleistungen und Software-as-a-Service zu setzen, hat dies weitreichende Änderungen am ISMS zur Folge. Nicht nur neue Tools werden angeschafft und technische Sicherheitsmaßnahmen erweitert, dies impliziert auch meist entsprechende Schulungen, Änderungen an den Prozessen in der Informationssicherheit, angepasste oder neue Richtlinien sowie neue Verantwortlichkeiten.

So wie sich das Unternehmen stets weiterentwickelt, so ändert sich auch die Bedrohungslage ständig. In Betriebssystemen, Software und Hardware werden tagtäglich bisher unbekannte Schwachstellen und Sicherheitslücken entdeckt. Mit Meltdown (Lipp et al., 2018) und Spectre

(Kocher et al., 2019) sorgten 2018 beispielsweise zwei Angriffsszenarien auf Prozessoren für großes Aufsehen und einiges an Panik. Die Szenarien nutzen ein normales Verhalten von Prozessoren aus, um unberechtigterweise sensible Daten auszulesen (Kuri, 2018). Ende 2021 wurde mit Log4Shell eine derart kritische Schwachstelle in der weit verbreiteten Java-Bibliothek Log4j bekannt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) sogar die höchste „Warnstufe Rot" ausrief (BSI, 2021).

Um das ISMS regelmäßig an die von innen und außen induzierten Änderungen anzupassen, orientieren sich die meisten Standards am PDCA-Zyklus oder ähnlichen methodischen Ansätzen zur kontinuierlichen Verbesserung. PDCA steht für Plan, Do, Check, Act (vgl. Bild 1.1). Das auch als Deming-Zyklus bekannte Vorgehen stammt aus dem Qualitätsmanagement. PDCA steht für vier Phasen, die zyklisch durchlaufen werden (vgl. Kersten et al., 2020, S. 12; Sowa, 2017, S. 18 f.). In der ersten Phase *Plan* wird das ISMS (oder Teile daraus) konzipiert. Die Ziele der Informationssicherheit und Sicherheitsmaßnahmen werden festgelegt. In der Phase *Do* wird das Konzept umgesetzt, und die Maßnahmen werden implementiert. Danach wird die Umsetzung in der Phase *Check* hinsichtlich Wirksamkeit und Effizienz überprüft. Aufgetretene Sicherheitsvorfälle werden ausgewertet. Die letzte Phase *Act* reagiert auf die Ergebnisse der Check-Phase, bewertet neue Anforderungen und definiert Änderungsbedarf. Fehler werden beseitigt und Sicherheitsmaßnahmen verbessert. Im Anschluss beginnt der Zyklus von vorn.

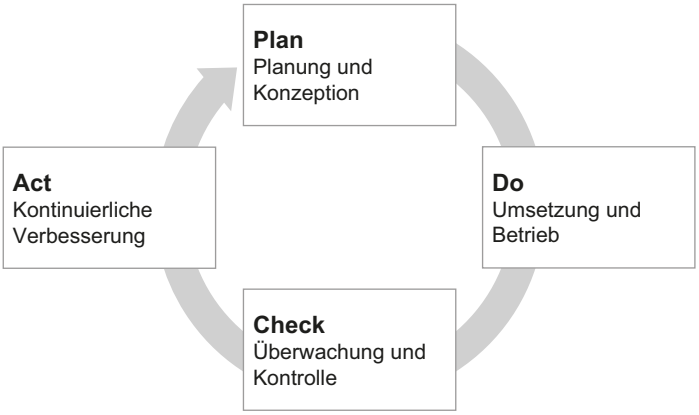

Bild 1.1 Die vier Phasen des PDCA-Zyklus (in Anlehnung an Sowa, 2017, S. 18)

Durch dieses Vorgehen werden nicht nur regelmäßig neue Anforderungen erhoben und im ISMS berücksichtigt, es werden auch die Effizienz und Effektivität der bestehenden Maßnahmen überprüft. Feedback aus der Organisation kann so berücksichtigt und eingearbeitet werden. Das Vorgehen ermöglicht Nachbesserungen, wo nicht die gewünschte Wirkung erzielt wurde oder unerwünschte Nebeneffekte auftraten.

Risikoorientierung

Fragt man Informationssicherheitsexpert:innen, nach welche Kriterien Informationssicherheitsmaßnahmen ausgewählt werden sollten, wird als erste Antwort vermutlich kommen: je sicherer, desto besser. Sicherheit hat die höchste Priorität.