ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Information Security Awareness im Bereich von Hochschulen

in Österreich

Masterarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Laura Nistelberger

is231513

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Dipl.-Ing. Herfried Geyer

Ehrenwörtliche Erklärung

Titel: Information Security Awareness im Bereich von Hochschulen

Art der Arbeit: Masterarbeit

Autor: Laura Nistelberger

Matrikelnummer: is231513

Ich versichere, dass

- ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich das Thema dieser Arbeit bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Ich erkläre hiermit, dass

☒ ich ein Large Language Model (LLM) verwendet habe, um die Arbeit Korrektur zu lesen.

☐ ich ein Large Language Model (LLM) verwendet habe, um Teile des Inhalts der Arbeit zu erstellen. Ich versichere, dass ich jeden generierten Satz/Absatz mit der Originalquelle zitiert habe. Das genutzte LLM ist an entsprechenden Stellen durch eine Fußnote ausgewiesen.

☐ im Zuge dieser Arbeit kein Large Language Model (LLM) zum Einsatz gekommen ist.

Ort, Datum *Unterschrift*

Kurzfassung

Die Zahl gezielter Cyberangriffe auf Hochschulen steigt rasant (180 Vorfälle seit 2022, 40% in Europa). Gleichzeitig fehlen in Österreich etablierte Konzepte, um das Sicherheitsbewusstsein an Hochschulen systematisch zu stärken.

Diese Masterarbeit entwickelt daher einen Rahmen für wirksame Awareness-Programme und untersucht dazu unter anderem die Erstellung einer Grundarchitektur eines hochschulspezifischen Awareness Konzepts, prioritäre Themen eines solchen Programms, gängige Umsetzungshürden und Unterschiede zu Organisationen anderer Branchen.

Die Datengrundlage bilden zwei Online-Erhebungen (12 österreichische Hochschulen; 16 Mitarbeitende der FH St. Pölten) sowie eine Analyse einschlägiger Normen und Leitfäden (ISO 27001, ENISA, NIST).

Alle befragten Hochschulen setzen zwar Sicherheitsmaßnahmen um, doch nur 17% betreiben ein gelebtes ISMS. Awareness basiert meist auf E-Learnings und Workshops. Studierende und nebenberufliche Lehrende bleiben weitgehend unberücksichtigt, und nur 58% der Einrichtungen nutzen spezialisierte Tools für Awareness. Wissenslücken bestanden bei Befragungen der Mitarbeitenden an der FH St. Pölten etwa bei S/MIME und belegen den Bedarf an zielgruppengerechtem Material.

Als Output der Arbeit entsteht ein theoretisches Rahmenwerk in Form einer Excel-Liste, das Zielgruppen („Need-to-Know“), Kernthemen (Phishing, Passwort- und Zugangsschutz, physische Sicherheit, Third-Party-Risiken, Ransomware) und vielfältige Lernmedien integriert. Die Arbeit zeigt, dass die offene Infrastruktur und hohe Fluktuation von Hochschulen ein speziell angepasstes, kontinuierlich evaluiertes Awareness-Programm erfordern.

Abstract

The number of targeted cyberattacks on universities is increasing rapidly (180 incidents since 2022, 40% in Europe). At the same time, there is a lack of established concepts in Austria to systematically strengthen security awareness at universities.

This master's thesis therefore develops a framework for effective awareness programs and examines, among other things, the creation of a basic architecture of a university-specific awareness concept, priority topics of such a program, common implementation hurdles and differences to organizations in other industries.

The data is based on two online surveys (12 Austrian universities; 16 employees of St. Pölten UAS) and an analysis of relevant standards and guidelines (ISO 27001, ENISA, NIST).

Although all respondents implement security measures, only 17% operate a living ISMS. Awareness is mostly based on e-learning and workshops. Students and external teachers are largely ignored and only 58% of institutions use specialized tools for awareness. Surveys of employees at St. Pölten UAS revealed gaps in knowledge, for example with regard to S/MIME, demonstrating the need for target group-specific material.

The output of the work is a theoretical framework provided as an Microsoft Excel-Sheet that integrates target groups ("need-to-know"), core topics (phishing, password and access protection, physical security, third-party risks, ransomware) and diverse learning formats. The work shows that the open infrastructure and high fluctuation of universities require a specially adapted, continuously evaluated awareness program.

Inhaltsverzeichnis

1. Einleitung

Informationssicherheit tangiert in der heutigen Zeit beinahe jeden Lebensbereich. Mit dem Voranschreiten der Digitalisierung sind nicht bloß Unternehmen und staatliche Stellen, sondern auch Einzelpersonen einem wachsenden Risiko ausgesetzt. Datenverlust kann gravierende Folgen haben – von finanziellen Schäden über den Verlust der Privatsphäre bis hin zu lebensbedrohlichen Situationen, beispielsweise im Gesundheitswesen. (vgl. [1])

Zahlreiche Studien, wie etwa die jährlich erscheinende Cybersecurity-Studie des Unternehmens KPMG, demonstrieren, dass die Angriffsfläche im Bereich der Cyberkriminalität beständig wächst. Besonders der sogenannte „menschliche Faktor“ stellt ein zentrales Einfallstor für Angriffe dar. Phishing, Social Engineering, Desinformation sowie unzureichende Sicherheitspraktiken sind mit hoher Eintrittswahrscheinlichkeit und großem Schadenmaß verbunden. (vgl. [2])

Als Reaktion auf die zunehmenden Bedrohungen wurden in Europa neue regulatorische Maßnahmen eingeführt, wie beispielsweise das Netz- und Informationssysteme-Sicherheitsgesetz (NIS), welches vor allem für Betreiber kritischer Infrastrukturen gilt. Ziel dieser Richtlinien ist es, einheitliche Rahmenbedingungen zu schaffen, um die Cybersecurity-Vorbereitungen und -Reaktionen koordinierter und effektiver zu gestalten. (vgl. [3, Seiten 5–6])

Doch wie steht es um Organisationen, die nicht unter diese gesetzlichen Vorgaben fallen? Hochschulen stellen einen solchen Bereich dar: Sie zählen nicht zur „kritischen Infrastruktur“ im Sinne der NIS-Richtlinie und unterliegen primär nur allgemeinen Regelungen wie der Datenschutz-Grundverordnung (DSGVO). Gleichzeitig sind auch sie verstärkt Ziel von Cyberangriffen: Seit 2022 wurden weltweit über 180 Angriffe auf Universitäten dokumentiert, von denen 40,5 % auf Europa entfielen (Stand: März 2025). Die Angriffsformen reichen von Ransomware, Brute-Force-Angriffen und DDoS-Attacken bis hin zur Ausnutzung von Schwachstellen in Software und unautorisiertem Zugriff auf Systeme. (vgl. [4])

Im deutschsprachigen Raum liegt der Forschungsschwerpunkt bislang primär auf Hochschulen in Deutschland. Dort wurde beispielsweise das IT-Grundschutz-Profil für Hochschulen entwickelt, welches die besonderen Herausforderungen durch dezentrale Organisationen und vielfältige IT-Landschaften adressiert. In Österreich fehlt eine umfassende wissenschaftliche Auseinandersetzung mit Informationssicherheitskonzepten im Hochschulkontext. (vgl. [5])

Ein zentraler Aspekt der Informationssicherheit ist der Faktor Mensch. Diese Arbeit widmet sich daher dem Themenbereich der Informationssicherheits-Sensibilisierung, welcher als Bestandteil des Informationssicherheitsmanagements verstanden wird. Während bestehende Studien oft den Menschen lediglich als Sicherheitsrisiko betrachten, rückt diese Arbeit zusätzlich die Rolle von Awareness als Instrument der Konformität in den Fokus.

Die vorliegende Arbeit beleuchtet sowohl allgemeine Herausforderungen von Awareness-Maßnahmen als auch solche, die speziell im Hochschulumfeld auftreten. Ziel ist es, einen konzeptionellen Ansatz für ein Awareness-Programm zu entwickeln, der als Grundlage für Hochschulen dienen und an deren spezifische Gegebenheiten angepasst werden kann.

Dabei werden folgende Forschungsfragen untersucht:

- **Wie könnte ein Konzept zur Informationssicherheits-Sensibilisierung speziell für Hochschulen aussehen?**

  Hierbei ist nicht die umfassende Erstellung eines Sensibilisierungskonzeptes als Ziel im Vordergrund. Der Fokus liegt vielmehr in der genauen Analyse der Zielgruppen, passender beziehungsweise bereits im Hochschulbereich vorhandener Medien und Themengebiete, welche speziell in diesem Bereich an Bedeutung haben. Ebenso behandelt werden ein Umsetzungsplan gemäß des zeitlichen Aspekts sowie die Messung des Erfolgs der Sensibilisierungsmaßnahmen. Jedoch ist bei diesen beiden Themen nur eine oberflächliche Behandlung vorgesehen. Schließlich erfolgt die Erfragung und Analyse der „IST-Situationen“ an Hochschulen bezüglich der Informationssicherheit und diesbezüglicher Awareness-Tätigkeiten.

- **Auf welche Themengebiete der Informationssicherheit müsste dabei besonderes Augenmerk gelegt werden?**

  Für die Behandlung dieser Fragestellung erfolgt eine Untersuchung von Besonderheiten in der Hochschul-IT. Weiters werden besondere Gefahren in diesem Bereich recherchiert und analysiert.
- **Welche Herausforderungen treten bei der Konzeption und Umsetzung auf, und wie kann diesen begegnet werden?**

  Überlegungen bezüglich personellen, zeitlichen und themenspezifischen Herausforderungen werden angestellt. Problemlösungen zu jedem dieser Schwierigkeiten werden identifiziert und bereitgestellt.
- **Unterscheidet sich ein solches Konzept an Hochschulen von jenem in gleich großen Unternehmen anderer Branchen – und wenn ja, inwiefern?**

  Als Grundlage für die Beantwortung dieser Fragestellung dienen Vergleiche von Hochschulen mit Unternehmen anderer Branchen. Dieser Vergleich geschieht hinsichtlich regulatorischer Anforderungen, Unternehmensaufbau, Art der schützenswerten Assets, Kerngeschäft und der Bedrohungen.

1.1. Gliederung der Arbeit

Die Gesamtstruktur dieser Arbeit lässt sich in folgende Abschnitte gliedern:

- **Einleitung**: Die Einleitung (referenziert als Kapitel: 1) gibt einen kurzen Einblick in die Thematik, zeigt die Relevanz von Informationssicherheit an Hochschulen auf und skizziert zentrale Forschungsfragen im Kontext aktueller Bedrohungen und Compliance-Anforderungen.
- **Hintergrund**: Dieser Abschnitt (referenziert als Kapitel: 2) erläutert den Aufbau von Hochschulen, definiert Informationssicherheit und Awareness, zeigt deren Zusammenhang auf und beleuchtet psychologische Aspekte, die für erfolgreiches Awareness-Training relevant sind.
- **Verwandte Arbeiten**: Das Kapitel (referenziert als Kapitel: 3) befasst sich mit der Fragestellung, welche Arbeiten oder Forschungen sich schon mit der Thematik auseinandergesetzt haben, und für diese Arbeit von Nutzen sind. Außerdem wird versucht Unterschiede zu finden, warum sich dieses Werk abhebt.
- **Methodik**: Befasst sich (referenziert als Kapitel: 4) damit, welche Methodik für die Erfüllung der Forschungsfragen ausgewählt wurde.
- **Durchführung**: Die praktische Ausarbeitung (referenziert als Kapitel: 5) gliedert sich in zwei Teile: Zunächst werden spezifische Bedrohungen und Herausforderungen an Hochschulen analysiert und mit anderen Branchen verglichen, anschließend folgt die exemplarische Entwicklung eines Awarenesskonzepts für die FH St. Pölten mit Fokus auf Zielgruppen, Inhalte, Medien und Zeitplan.
- **Ergebnisse**: Dieses Kapitel (referenziert als Kapitel: 6) behandelt die Ergebnisse der praktischen Ausarbeitung und der durchgeführten Umfragen, sowie die Beantwortung der Forschungsfragen.
- **Schlussfolgerung**: In diesem Abschnitt (referenziert als Kapitel: 7) werden die wichtigsten Ergebnisse zusammengefasst und es wird beschrieben, was daraus gelernt werden kann.

2. Grundlagen

Dieses Kapitel zielt darauf ab, durch Erläuterung der nachfolgend verwendeten Begrifflichkeiten ein umfangreiches Verständnis der Thematik zu schaffen. Dies dient der Nachvollziehbarkeit der praktischen Ausarbeitung.

2.1. Grundlagen im Bereich der Hochschulen

Um ein umfassendes Verständnis dieser Arbeit zu erschaffen, erfolgt zunächst eine Erklärung der Begrifflichkeit „Hochschule“. Hierfür beginnt die Erläuterung in Zeiten des Mittelalters, welche als Entstehung von Hochschulen, beziehungsweise höheren wissenschaftlichen Einrichtungen, gilt. Damals entstanden diese durch Zusammenschlüsse genossenschaftlich geprägter Personenverbänden und besaßen bereits eine eigene Verfassung und Gerichtsbarkeit. Als wesentliche Funktion dieser Einrichtungen werden „Die Erzeugung von Wissen und Qualifikation für den gesellschaftlichen Produktionsprozess und Reproduktionsprozess – dazu zählen ökonomische und kulturelle Subsysteme“ aufgelistet. (vgl. [6], [7])

Konkrete Definitionen können dem Universitätsgesetz 2002 (UG), sowie dem Fachhochschulgesetz (FHG) entnommen werden. In jenen werden Universitäten als wissenschaftliche Einrichtungen mit Forschung und Lehre bezeichnet. Wohingegen Fachhochschulen die Beschreibung als praxisorientierte Hochschule mit berufsbezogener Ausbildung zugesagt wird. Weiters sind Hochschulen Einrichtungen des tertiären Bildungsbereiches zuzuordnen. Dies bedeutet, dass es sich um Erwachsenenbildung im dritten Bildungsweg mit akademischem Abschluss handelt. (vgl. [8], [9])

Weiters ist zu erwähnen, dass es in Österreich über 70 Einrichtungen gibt, welche sich in staatliche Universitäten (23 Einrichtungen), Fachhochschulen (21 Einrichtungen), pädagogische Hochschulen (14 Einrichtungen), Privatuniversitäten (17 Einrichtungen) und Privathochschulen (2 Einrichtungen) gliedert. Diese unterscheiden sich unter anderem jeweils durch die Anzahl, sowie Schwerpunkte der Studienrichtungen, regulatorische Anforderungen, Organisationsform und Zugangsbeschränkungen. (vgl. [10], [11], [12])

Wie auch Unternehmen anderer Branchen unterliegen Hochschulen diverser gesetzlicher Anforderungen. Zu diesen zählen unter anderem:

- **Universitätsgesetz 2002 UG- Bundesgesetz über die Organisation der Universitäten und ihre Studien**: Das vorliegende Gesetz bildet die Rechtsgrundlage für öffentliche Universitäten. Es regelt das Organisationsrecht (z. B. Leitung, Finanzierung, Organe etc.), die Studien (z. B. Studienarten, Zulassung, Prüfung, akademische Grade etc.) sowie das Personal. (vgl. [8])
- **Fachhochschulgesetz**: Das Fachhochschulgesetz (FHG) findet im Besonderen Anwendung auf Fachhochschulen und konstituiert seit 1993, mit einer Reorganisation im Jahr 2021, die Rechtsgrundlage für die Einrichtung dieser Institutionen. Des Weiteren definiert es die Modalitäten der Akkreditierung solcher Einrichtungen. Darüber hinaus beinhaltet das Gesetz, in Analogie zum Universitätsgesetz (UG), Bestimmungen hinsichtlich der Organisation, des Personals und der Studiengänge. (vgl. [9])
- **Privathochschulgesetz und Privatuniversitätsgesetz**: Das Privathochschulgesetz (PrivHG) und Privatuniversitätengesetz (PUG) regeln die Einrichtung von Privathochschulen und -universitäten. Diese sind in der österreichischen Rechtsordnung verankert. Das Privathochschulgesetz trat 2021 in Kraft und weist in diesem Zusammenhang eine Reihe von Parallelen zum Fachhochschulgesetz und zum Hochschulgesetz auf. So sind sowohl das PrivHG und PUG als auch die zuvor genannten Gesetze bindend für die Akkreditierung der Studien, die Organisation der Lehranstalten sowie die Personalsituation. (vgl. [13], [14])
- **Hochschulgesetz**: Das vorliegende Gesetz befasst sich mit organisationsrechtlichen Regelungen und dient zudem der Regelung der Studien. In diesem Zusammenhang werden Gebiete wie die Arten der Studien, die Zulassung und die Prüfungen festgelegt. Der vorliegende Rechtstext findet ausschließlich Anwendung bei pädagogischen Hochschulen, deren Aufgabe in der Ausbildung von Lehrkräften besteht. (vgl. [15])
- **Hochschulqualitätssicherungsgesetz**: Das Hochschulqualitätssicherungsgesetz findet Anwendung in öffentlichen Universitäten, privaten Hochschulen, Fachhochschulen, pädagogischen Hochschulen sowie bei der Agentur für Qualitätssicherung und Akkreditierung in Österreich. Es regelt zahlreiche Bestimmungen zum Thema Qualitätssicherungsverfahren und umfasst auch Regelungen beziehungsweise das Meldeverfahren für Studien ausländischer Bildungseinrichtungen. Darüber hinaus enthält das Gesetz Bestimmungen zur Wahrung der Integrität im wissenschaftlichen und künstlerischen Studien-, Lehr- und Forschungsbetrieb. (vgl. [16])

Neben den vorliegenden Gesetzestexten finden zudem die Datenschutzgrundverordnung (DSGVO) sowie das Arbeitsrecht Anwendung. Die zuvor beschriebenen Rechtsgrundlagen bieten auch in der Regel selbst einen Paragrafen bezüglich des Datenschutzes an.

Die Analyse der vorliegenden Gesetzestexte ergab, dass keine präzisen Vorschriften bezüglich der Informationssicherheit beziehungsweise der IT-Sicherheit festzustellen sind. Einzig die Integrität der Lehre und Forschung sowie der Datenschutz im Sinne der DSGVO wurden berücksichtigt. (vgl. [17], [11])

2.1.1. Aufbau von Hochschulen

Die Organisationsformen der Hochschulen in Österreich sind unterschiedlich und hängen hauptsächlich von ihrer Trägerschaft und Rechtsform ab. (vgl. [11])

Öffentliche Universitäten existieren als juristische Personen des öffentlichen Rechts nach dem Universitätsgesetz 2002 und haben keine klassische Unternehmensform. Sie agieren als autonome Körperschaften mit staatlicher Finanzierung. (vgl. [8])

Im Gegenteil dazu unterliegen Privatuniversitäten dem Privathochschulgesetz und sind oft in einer Form einer GmbH organisiert. Sie müssen von der AQ Austria akkreditiert werden und finanzieren sich in der Regel aus den Studiengebühren. Ein Beispiel wäre die Sigmund Freud Privatuniversität GmbH. (vgl. [13])

Fachhochschulen basieren auf dem Fachhochschulgesetz und sind oft in der Form einer GmbH oder einem vergleichbaren Modell organisiert. Die Eigentümer können private Unternehmen oder öffentliche Institutionen wie Bundesländer oder Kammern sein. Einige Beispiele sind die Technikum Wien GmbH und die FH St. Pölten GmbH. (vgl. [9], [18], [19])

Pädagogische Hochschulen sind Bundeseinrichtungen und existieren als solche oder als GmbH. (vgl. [11])

Zusätzlich zu diesen Hochschultypen gibt es Spezialhochschulen wie die Donau-Universität Krems, die als juristische Person des öffentlichen Rechts existiert. Während öffentliche Hochschulen eher Körperschaften des öffentlichen Rechts sind, sind private Hochschulen und Fachhochschulen normalerweise GmbHs. (vgl. [20])

Österreichische Hochschulen, vor allem größere Universitäten und Fachhochschulen, verfügen über eine Vielzahl von Abteilungen, die Administration und Organisierung aufrechterhalten. Die genaue Struktur variiert je nach Größe und Feld der Hochschule, aber die folgenden Abteilungennamen sind am häufigsten:

- **Rektorat & Hochschulleitung** – die höchste Instanz bestehend aus Rektoren, Vizerektoren und möglicherweise einer Geschäftsführung.
- **Buchhaltung & Controlling** – Ist zuständig für die Finanzplanung, das Budget und Buchhaltung.
- **Personalabteilung** – Diese Abteilung ist verantwortlich für Personalmanagement, Gehaltsabrechnungen und Arbeitsrecht.
- **Studienabteilung** – Für die einzelnen Studien ist diese Abteilung verantwortlich und befasst sich mit der Verwaltung von Studienbewerbungen, Einschreibungen, Prüfungswesen und Studierendenservices.
- **Marketing & Öffentlichkeitsarbeit** – Diese Abteilung ist zuständig für die interne und externe Kommunikation, Social Media, Werbung, Eventmanagement und für das generelle Branding der Hochschule.
- **IT-Abteilung** – Kümmert sich um die Betreuung der digitalen Infrastruktur, der Netzwerke, der Softwarelösungen und um den technischen Support für Studierende und Mitarbeitende.
- **Rechtsabteilung** – Diese Abteilung befasst sich mit der Bearbeitung von Verträgen, Datenschutz und Rechtsfragen.
- **Forschungsförderung** – Ist verantwortlich für die Unterstützung bei Forschungsprojekten, Fördermittelanträgen und Kooperationen mit externen Partnern.
- **International Office** – Diese Abteilung kümmert sich um die Organisation von Austauschprogrammen und Kooperationen mit anderen Hochschulen.
- **Facility Management** – Ist verantwortlich für die Verwaltung der Gebäude, deren Infrastruktur und Sicherheit.
- **Bibliothek & Informationsmanagement** – Hier erfolgt die Bereitstellung wissenschaftlicher Ressourcen, welche auch verwaltet werden müssen.
- **Qualitätsmanagement** - Diese Abteilung soll die akademischen Standards gewährleisten und ist außerdem zuständig für die Evaluierung von Lehr- und Forschungsleistungen.
- **Karriere- und Alumni-Service** – Dieser Service soll Studierende unterstützen Netzwerke zu schaffen, und außerdem bei der Jobvermittlung hilfreich sein.

(vgl. [21], [22])

Beispiel Aufbau einer Hochschule

Beispielhaft wird der Aufbau der FH St. Pölten aufgezeichnet:
An der Spitze steht die Hochschulleitung, die für die übergreifende Steuerung und Entwicklung der FH verantwortlich ist. Untergeordnet befinden sich die nachfolgenden Abteilungen.
Die erweiterte Hochschulleitung gewährleistet eine effiziente Zusammenarbeit bei der Entscheidungsfindung in strategischen und übergeordneten Angelegenheiten.
Ein weiteres Organ ist die Geschäftsführung, die für die wirtschaftliche und organisatorische Leitung der FH zuständig ist. Hier fallen wiederum Bereiche wie die „E³UDRES² Lead Coordination“, die sich mit der Koordination von Bildungsprogrammen und internationalen Kooperationen beschäftigt, oder die „FH-Services“ in den Zuständigkeitsbereich.
Das Kollegium besteht aus der Leitung des Kollegiums, deren Stellvertretenden sowie Vertretenden der Studiengangsleitungen, haupt- und nebenberuflich Lehrenden, Forschenden sowie den Studierenden.
Die Departments decken die jeweiligen speziellen Studiengänge ab und sind für die inhaltliche und organisatorische Gestaltung der Studiengänge verantwortlich.
(vgl. [22])

interpretierte Bedeutung von Awareness für den Aufbau der Hochschule

Die Hochschulleitung ist für die Gesamtverantwortung der strategischen Führung des Instituts zuständig und muss sicherstellen, dass Security Awareness ein integraler Bestandteil der Hochschulkultur wird.

Die erweiterte Hochschulleitung dagegen kann die Implementierung von Security Awareness sowohl durch die Koordinierung sicherheitsrelevanter Entscheidungen in den verschiedenen Fachbereichen als auch gezielten Schulungen ihrer Mitglieder unterstützen.

Das Geschäftsmanagement spielt eine zentrale Rolle in der organisatorischen Umsetzung von Sicherheitsmaßnahmen, vor allem im Bereich Informationstechnologie-Sicherheit und Datenschutz.

Das Kollegium, bestehend aus Lehrenden, Forschenden und Studierenden. Dieses ist eine wichtige Zielgruppe für Security Awareness. Es kann durch gezielte Schulung und Richtlinien die Awareness aller Mitglieder sichergestellt werden.

Zusätzlich spielen alle unmittelbaren Abteilungen, darunter der IT-Support, das Facility Management, Recht und der Datenschutzbeauftragte eine wichtige Rolle bei der Umsetzung des Sicherheitsbewusstseins.

2.2. Informationssicherheit

Ein weiterer essenzieller Bestandteil dieser Arbeit ist die Begrifflichkeit Informationssicherheit. Diese befasst sich mit dem Schutz vor Manipulation, Löschung und Kompromittierung von Informationen und Informationswerten. Weiters beschäftigt sie sich mit dem Schutz der IT-Systeme. Informationen können in digital oder auch physisch klassifiziert werden. Im Vergleich zur Informationssicherheit befasst sich die IT-Sicherheit eher mit Informationen, welche in Verbindung mit digitalen Systemen stehen. Daher ist IT-Sicherheit ein Teilbereich der Informationssicherheit. (vgl. [23])

Die Informationssicherheit wird in drei primäre Schutzziele gegliedert: Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Im Englischen hat sich der Begriff „CIA-Triade“ etabliert. Darüber hinaus werden diese Ziele in sekundären Sicherheitszielen detaillierter dargestellt. Nachstehend sind sowohl die primären-, als auch die sekundären Sicherheitsziele genauer erläutert. (vgl. [23], [24])

Vertraulichkeit

Vertraulichkeit beschreibt, dass Informationen nur von befugten Personen, Einrichtungen oder Prozessen eingesehen werden dürfen. Sollte dies nicht gewährleistet sein, so spricht man von Kompromittierung. Mögliche Auswirkungen sind zum Beispiel Strafzahlungen, Imageverlust und Verlust von Wettbewerbsvorteilen. Beim Verkauf der gestohlenen Daten kann sogar ein Schaden an den beteiligten Individuen entstehen. (vgl. [23], [24])

Integrität

Die Integrität gewährleistet die Korrektheit und Vollständigkeit von Informationen. Voraussetzung ist, dass die Eingabe beziehungsweise der Erstzustand korrekt und vollständig war. Änderungen können sowohl beabsichtigt als auch unbeabsichtigt erfolgen. Es sollte ein entsprechender Schutz vor Manipulation oder Beschädigung in Kraft sein. (vgl. [23], [24])

Verfügbarkeit

Verfügbarkeit sichert, dass Informationen in benötigter Menge und Zeit für autorisierte Stellen vorhanden und nutzbar sind. Der Bedarf an Verfügbarkeit richtet sich nach den individuellen Anforderungen. Ein Beispiel wäre ein Dateiserver, welcher nur über die Geschäftszeiten hinweg verfügbar sein soll. Fehlende Kapazitäten (Fehlplanung) spielen auch eine wichtige Rolle. Es könnte zu Problemen wie Prozessbehinderung, einem verspäteten Abschluss von Projekten, Umsatzeinbußen oder Vertragsstrafen, welche bei kritischer Infrastruktur relevant sind, kommen. (vgl. [23], [24])

Authentizität

Authentizität bedeutet die eindeutige Identifizierung von jemandem oder etwas. Beispiele hierfür sind die Zugangs- und oder Zutrittskontrollen. (vgl. [23])

Ordnungsmäßigkeit

Der Begriff Ordnungsmäßigkeit beschreibt die Konformität zu bestimmten Regeln der IT. Vergleichbar ist es mit der Compliance. Unterschieden werden kann zwischen internen und externen Regelungen. Letztere sind zum Beispiel ISO-Standards oder Gesetze. (vgl. [23])

Verantwortlichkeit

Die Verantwortlichkeit ist ähnlich zur Authentizität. Es kann eine zusätzliche Verbindung zwischen Verantwortlichkeit und der jeweilig ausgeführten Tätigkeit geschaffen werden. Ein Beispiel hierfür wäre Logging. (vgl. [23])

Nachvollziehbarkeit

Die Nachvollziehbarkeit beschreibt, dass Aktivitäten und Entscheidungen verstanden und das Zustandekommen rückführbar ist. Beispiele hierfür sind Protokolle und Überwachungsmaßnahmen. (vgl. [23])

Nicht Abstreitbarkeit

„Nicht Abstreitbarkeit“ bedeutet, dass das Senden oder Empfangen nicht abgestritten werden kann. Personen könnten die Aktivitäten ihrer Handlungen verschleiern beziehungsweise abstreiten. Zum Beispiel kann dieser Problematik mithilfe einer elektronischen Signatur entgegengewirkt werden. (vgl. [23])

Nicht Anfechtbarkeit

Die „nicht Anfechtbarkeit“ hat einen rechtlichen Ursprung. Anfechtungsgründe sind beispielsweise Irrtum bezüglich einer Erklärung oder bestimmten Eigenschaften, falsche Übermittlung, Täuschung oder Drohung. (vgl. [23])

Rechtssicherheit

Bei der Rechtssicherheit geht es ebenfalls um rechtliche Aspekte. Sie dient der besseren Planung von rechtlichen Risiken und regelt, dass Vertragspartner Verträge einhalten müssen. (vgl. [23])

Zuverlässigkeit

Zuverlässigkeit bedeutet die Erfüllung von Regeln und Vorgaben. Es besteht ein Zusammenhang zur Ordnungsmäßigkeit. Ein Beispiel wäre ein Fehler in Software und Hardware, welcher zu einem Ausfall führt. (vgl. [23])

Weiters werden Informationen laut ISO/IEC 27001 neben Geschäftsprozessen und -Aktivitäten zu den Primärwerten eines Unternehmens gezählt. Diese liegen in Abhängigkeit zu ihren unterstützenden Werten wie beispielsweise Hard- und Software, Personal und Standort. Somit müssen Informationswerte für die Gewährleistung der CIA-Triade darauf vertrauen, dass ihre zugrunde liegenden Werte sicher fungieren. (vgl. [25])

2.3. Awareness

Die Security Awareness wird allgemein als Maßnahme zur Erhöhung des Sicherheitsbewusstseins eines Unternehmens definiert. Dies dient der Steigerung des Sicherheitsniveaus bezüglich Bedrohungen im Bereich der Informationssicherheit.

Security Awareness wurde bereits früher von zahlreichen Forschenden thematisiert. McLean (1992), Spurling (1995) sowie Thompson und Solms (1997) sind einige davon, um Beispiele aufzuzählen. Diese gehen besonders auf individuelle Verhaltensänderungen und Schulungskonzepte ein. (vgl. [1])

In dieser Arbeit wird der Begriff Security Awareness jedoch aus Governance-Perspektive betrachtet. Behandelt werden vor allem Standards, Best Practices und Normen wie ISO/IEC 27001 oder NIST, die Sicherheitsbewusstsein als Bestandteil eines strukturierten Informationssicherheitsmanagements verstehen.

2.3.1. Definitionen

In diverser Literatur finden sich zahlreiche weitere Definitionen. Jene der Verbände „International Organisation for Standardization“, „Bundesamt für Sicherheit in der Informationstechnik“, „National Institute of Standards and Technology“ und „European Network and Information Security Agency“ werden nachstehend näher erläutert.

Definition „Bundesamt für Sicherheit in der Informationstechnik“

Seitens des Bundesamts für Sicherheit in der Informationstechnik wird das Thema Awareness beziehungsweise Sensibilisierung durch den „BSI-Grundschutz“ behandelt. In diesem findet sich die Thematik im Baustein „ORP.3 Sensibilisierung und Schulung zur Informationssicherheit“ wieder. Mitarbeitende werden hierbei als wesentlich für die Sicherheit des Unternehmens beschrieben. Sie müssen in der Lage sein Sicherheitsziele zu kennen, und deren Erfolg durch Einhaltung der daraus abgeleiteten Maßnahmen umzusetzen. Als Voraussetzung wird ein vorhandenes Sicherheitsbewusstsein, sowie eine Sicherheitskultur, im Unternehmen gesehen. Eine Schulung dient laut BSI dem Zweck jeden Einzelnen auf Gefährdungen aufmerksam zu machen, und daraus weitergehend den resultierenden Handlungsbedarf zu lehren. Weiters werden im genannten BSI-Grundschutz Baustein-Gefährdungen aufgelistet, welche die Relevanz von Security Awareness unterstreichen. Näheres dazu befindet sich im Kapitel 5 dieser Arbeit. (vgl. [26])

Definition „European Network and Information Security Agency“

Die „European Network and Information Security Agency“ (kurz: ENISA) wählt in der Beschreibung vom Prozess Security Awareness einen anderen Ansatz. Hierbei werden zunächst drei Phasen der Bildung unterschieden: „Awareness“, „Training“ und „Education“.

Der Terminus „Awareness“ beschreibt die Befähigung Mitarbeitende zur „First Line of Defense“ auszubilden. Das bedeutet, dass auftretende Risiken proaktiv erkannt, beurteilt und behandelt werden können. Weiters bildet diese Phase das „Was“ einer Bildungsstrategie. In dieser wird eine Veränderung des Verhaltens, beziehungsweise der Verhaltensmuster, in das Bessere als Ziel angesehen. Im Gegensatz zu den beiden anderen, zu Beginn genannten, Tätigkeiten birgt „Awareness“ oft eine wiederkehrende Tätigkeit unter der Nutzung verschiedener Medien mit einer weniger formellen Gestaltung und Länge. Zusammengefasst dient sie dem Wissenstransfer und der Aufmerksamkeitserregung auf eine bestimmte Problematik.

Als zweite Phase wird „Training“ definiert. Dies kann wiederum als das „Wie“ des Prozesses betitelt werden. Im Gegensatz zu „Awareness“ wird nicht nur Bewusstsein für Problematiken gebildet, sondern auch ein Set an Fähigkeiten trainiert, um den Problemstellungen entgegenzuwirken.

Als letzte Phase eines Awareness Programms sollten beide Ansätze kombiniert werden und sich somit in „Education“ weiterentwickeln.

(vgl. [27])

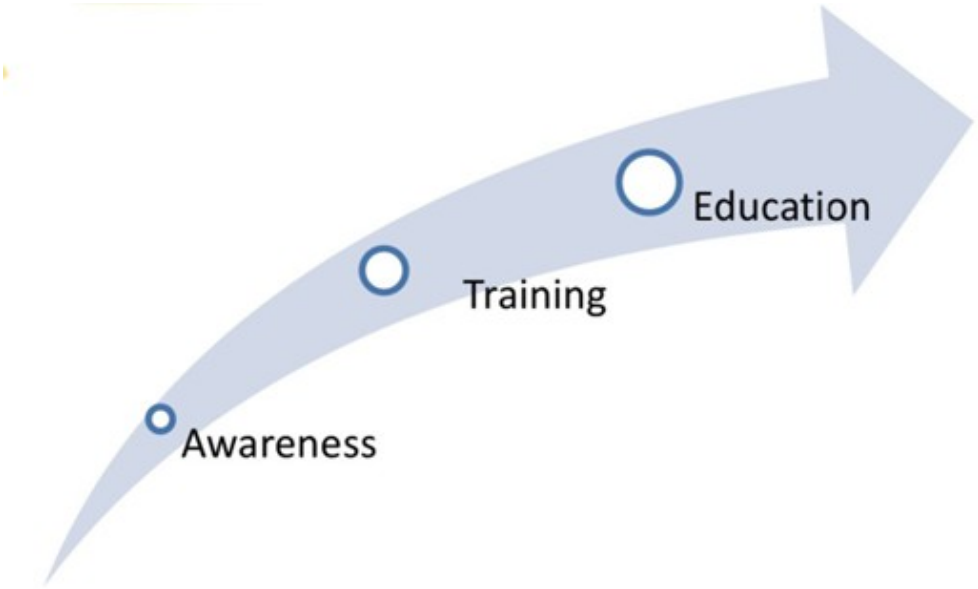

Abbildung 2.1.: Phasen der Awareness [27]

Definition „National Institute of Standards and Technology“

Das "National Institute of Standards and Technology"befasst sich in seinen Publikationen SP 800-50 und SP 800-16 mit der Erstellung von Awareness Programmen. In diesen wird beschrieben, dass es sich bei Awareness nicht um eine Schulung handelt. Sie wird lediglich als Aufmerksamkeitserregung auf Sicherheitsthemen angesehen. Weiters wird zwischen den Rollen des Lernenden und des Lehrenden unterschieden. Erster ist hierbei Empfangender von Informationen, wohingegen Zweiter eine aktive Rolle in der Schulungsumgebung einnimmt. (vgl. [28], [29])

Awareness ist ein kontinuierlicher Lernprozess, bei dem Rücksicht auf die individuellen und unternehmenseigenen Denkweisen genommen wird, um die Wichtigkeit von Sicherheit und der Konsequenzen des Versagens bei Nichteinhaltung aufzuzeigen. (vgl. [28])

Definition „ International Organisation for Standardization“

Die „International Organisation for Standardization“ behandelt das Thema Awareness unter anderem in der Norm „ISO/IEC 27001“ und dem Standard „ISO/IEC 27002“. In Ersterem wird dies als unterstützende Tätigkeit angesehen, welche beschreibt, dass Personen angemessene Schulungen entsprechend ihrem Kompetenzbereich erhalten sollen. Weiters muss gewährleistet werden, dass sich Individuen des Unternehmens der Informationssicherheitspolitik, einer unterstützenden Tätigkeit bezüglich des Informationssicherheitssystems und den Folgen einer Nicht-Erfüllung der bestimmten Anforderungen bewusst sind. (vgl. [25], [30])

Darüber hinaus wird im Standard ISO/IEC 27002:2022 abermals der Bedarf an ausreichender Schulung in den einzelnen Themenkapiteln hervorgehoben. Besonderes Augenmerk zur Thematik des Schulungsbedarfs legt der Punkt „6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung“. Dieser dient dem Zweck der Sicherstellung von Verantwortlichkeiten bezüglich Informationssicherheit der einzelnen Individuen. (vgl. [25], [30])

Eine genaue Analyse, in welchen Controls Security Awareness direkt oder indirekt gefordert wird, befindet sich im Unterabschnitt 2.3.4 dieser Arbeit.

2.3.2. Vergleich

Bei einem Vergleich dieser Definitionen wird deutlich, dass ein starker Fokus auf die Mitarbeitenden gelegt wird. Zudem wird in allen Werken betont, dass Sensibilisierungstätigkeiten eingesetzt werden, um Individuen dazu zu befähigen, Sicherheitsrisiken zu erkennen, und angemessene Maßnahmen zu ergreifen. Eine Gemeinsamkeit besteht ebenfalls in der Dringlichkeit und Notwendigkeit der Durchführung dieser Schulungen. Awareness wird von den Institutionen als fortlaufender Prozess beschrieben.

2.3.3. Die Fünf Dimensionen von Security Awareness

Um Security Awareness vollumfassend zu verstehen, muss auch der über den rein organisatorisch hinausgehende Aspekt differenziert betrachtet werden. Siponen bekräftigt, dass nicht nur Unternehmen und Institutionen zum Schutz von Informationen verpflichtet sind, sondern wirklich alle Personen, die diese als Schutzgut erachten. (vgl. [1])

Informationen zu Security Awareness sollten zielgruppenspezifisch angeboten werden, wobei auch zwischen relevanten und irrelevanten Inhalten unterschieden werden muss. Gleichzeitig sollte die individuelle Meinungsbildung nicht eingeschränkt, sondern mithilfe reflektierter Information unterstützt werden. (vgl. [1])

Im Kontext schlägt Siponen fünf Dimensionen der Security Awareness vor, die auf verschiedene soziale Dimensionen abzielen:

1. **Die organisatorische Dimension**: Diese bezieht sich auf unterschiedliche Zielgruppen innerhalb einer Organisation, wie das obere Management, die IT-/IS-Leitung, das IT-Sicherheitspersonal sowie die Endbenutzer. Diese Gruppen benötigen für sie abgestimmte Informationen und Ausbildungsmöglichkeiten.
2. **Allgemeine Öffentliche Dimension**: Das Ziel ist es, das allgemeine Sicherheitsbewusstsein zu fördern. Die breite Öffentlichkeit wird in IT-erfahrene Personen und Endnutzer eingeteilt. IT-erfahrene Personen sollten ihr Wissen aktiv einbringen und mit Institutionen zusammenarbeiten, um einen Informationsaustausch zu fördern. Endnutzer der IT sollten in der Lage sein, zumindest ein grundlegendes Verständnis von IT-Risiken vorweisen zu können.

3. **Sozio-politische Dimension**: Hier steht die Sensibilisierung für Themen im Zusammenhang mit sozialen und politischen Fragen an erster Stelle. In die Zielgruppe fallen unter anderem Juristen, PR-Verantwortliche, politische Entscheidungsträger und Regierungsinstitutionen. Security Awareness in dieser Dimension ist von Bedeutung für das Wohl der ganzen Gesellschaft.
4. **Computerethnische Dimension**: Die Dimension bezieht sich auf Forschende, die sich mit dem Bereich Computerethik beschäftigen. Da sich diese mit ethischen Fragestellungen rund um IT und Informationssicherheit auseinandersetzen, leisten sie mit ihrer Forschung einen wichtigen Beitrag für die gesamte Gesellschaft bezüglich des Themas Awareness.
5. **Institutionelle Bildungsdimension**: In Bildungseinrichtungen sollte Security Awareness als Allgemeinbildung unterrichtet werden. Der Zweck dieser Dimension ist es, Wissen über dieses Thema mit den Institutionen zu teilen, damit es diese weitervermitteln können. Zwar fördern Programme wie der europäische Computerführerschein technische Kompetenzen, jedoch bleiben soziale, ethische und sicherheitsbezogene Aspekte oft unberücksichtigt.

(vgl. [1])

In dieser Arbeit wird Security Awareness primär auf der organisatorischen Ebene betrachtet. Hochschulen können jedoch, je nach Perspektive, verschiedenen der zuvor erläuterten Dimensionen zugeordnet werden. Einerseits können sie wie ein Unternehmen organisiert werden. In diesem Fall ist die Definition der organisatorischen Dimension unmittelbar anwendbar. Andererseits sind Hochschulen jedoch Bildungseinrichtungen, die die Weiterentwicklung individueller Kompetenzen entscheidend beeinflussen, was auch diese Dimension relevant macht. Viele Hochschulen sind auch eng mit Forschungsbereichen verbunden, in denen Fragestellungen der Computerethik eine zentrale Rolle spielen. Zum Beispiel im Bereich des verantwortungsvollen Umgangs mit Daten oder die ethischen Implikationen neuer Technologien. Die öffentliche und die soziopolitische Dimension fallen dagegen eher aus dem direkten Aufgabenbereich von Hochschulen heraus, da sie schwer steuerbar beziehungsweise kaum adressierbar sind. Allerdings kann argumentiert werden, dass gerade die soziopolitische Dimension Impulse zur Awareness-Vermittlung liefern kann. Insbesondere, da viele Einrichtungen vom Staat finanziert werden, und somit durch staatliche Vorgaben beeinflusst werden. Auch im Bereich der öffentlichen Dimension ist zu vermuten, dass eine umfassende Vermittlung von Awareness in organisatorischen und institutionellen Ebenen Wirkung entfalten wird, die über die Hochschule als Einrichtung hinausgeht. Dies könnte beispielsweise dazu führen, dass Absolvierende ein gesundes Sicherheitsbewusstsein in ihre zukünftigen Arbeitsbereiche oder ihre individuellen Lebensräume integrieren.

2.3.4. Bedeutung von Security Awareness für die IT-Sicherheit

Der effektive Schutz von IT-Systemen hängt nicht allein von technischen Maßnahmen ab, sondern auch davon, dass diese Maßnahmen von den Mitarbeitenden verstanden und korrekt umgesetzt werden. Nur wenn die Anwendenden die Bedeutung von Schutzmaßnahmen erkennen und entsprechend agieren, sind solche Mechanismen wirksam. (vgl. [23, Seite 15])

In vielen Fällen gilt, dass erfolgreiche Angriffe auf Unvorsichtigkeit und Unwissen der Mitarbeitenden beruhen. Der Mensch lässt sich zwar leichter manipulieren als ein technisches System, dennoch hat die Mehrheit der IT-Störungen mit menschlichem Fehlverhalten zu tun. (vgl. [23, Seite 17])

Die im Rahmen der KPMG-Studie benannten Themen Phishing, Social Engineering und E-Mail Compromise sind entscheidende Bedrohungsquellen von Unternehmen. Ein wichtiges Mittel zur Bekämpfung solcher Angriffe ist die Security Awareness, die das Erkennen und Verhindern dieser Bedrohungen ermöglicht. (vgl. [2])

Laut "NIST Special Publication 800-50"kann auch der Schutz von CIAs ohne klares Bewusstsein von Rollen und Verantwortlichkeiten, Prozessen und organisatorischen und technischen Maßnahmen nicht effektiv sein. Der Mensch bleibt das schwächste Glied, weshalb Security Awareness ein fester Bestandteil jeder Sicherheitsstrategie sein muss. (vgl. [28])

Aus Compliance-Sicht ist die Awareness ebenfalls ein Schlüsselaspekt, was beispielsweise aus etlichen Vorgaben der ISO-Publikationen hervorgeht. Besonders deutlich wird dies am CIA-Dreieck:

- Vertraulichkeit steht im Zusammenhang mit dem Vertraulichkeitsniveau. Mitarbeitende müssen den Wert und die Sensitivität von Informationen sowie die sichere Speichermethode und -verwaltung von Informationen verstehen.
- Integrität, ist die Intaktheit von Informationen. Dies erfordert, dass Mitarbeitende in der Lage sind, Daten kompetent einzugeben und Veränderungen in Frage zu stellen. Darüber hinaus ist auch hier die Integrität der Person relevant, wie sie in „ISO/IEC 27002 People Controls“ eingeführt wird. Awareness Maßnahmen können dazu beitragen, Fehlverhalten zu erkennen, und zu vermeiden.
- Verfügbarkeit bezieht sich auf die Bereitschaft von Informationen. Mitarbeitende müssen wissen, welche Systeme zu welcher Zeit und für welche Art von Arbeit verfügbar sind. Der Allgemeinüberblick über Informationen, ihre Kategorisierung und Verständnis von Schutzklassen ist hierbei ebenfalls

wichtig.

Um das Thema erneut aus Sicht der Compliance zu betrachten, werden ISO/IEC 27001 und die dazugehörige Umsetzungshilfe ISO/IEC 27002 herangezogen. Bei der Analyse dieser ist ersichtlich, dass in beiden dieser Vorgaben das Thema Awareness beziehungsweise Sensibilisierung behandelt wird. Dies geschieht zum einen in direkter als auch indirekter Form. (vgl. [25], [30])

In der internationalen Norm ISO/IEC 27001 und der zugehörigen Umsetzungshilfe ISO/IEC 27002 kommt dem Thema Awareness beziehungsweise Sensibilisierung eine wichtige Rolle zu, sowohl direkt als auch indirekt. (vgl. [25], [30])

Explizit wird das Thema Awareness in der ISO/IEC 27001 kaum erwähnt, jedoch ist indirekt in einigen Anforderungen an die Verpflichtungen zum angemessenen Umgang mit Informationssicherheit enthalten. (vgl. [25], [30])

Einige Abschnitte, die indirekt Sensibilisierung enthalten, sind:

- **4.2**: Fordert das Verstehen der Erfordernisse und Erwartungen interessierter Parteien, was ein grundlegendes Bewusstsein für die Anforderungen an das Informationssicherheitsmanagementsystem (ISMS) voraussetzt.
- **5.1 d**: Dieser Abschritt unterstreicht, dass die Wichtigkeit eines funktionierenden ISMS innerhalb der Organisation kommuniziert werden muss.
- **5.2 f**: Befasst sich mit der Bekanntmachung der Sicherheitspolitik.
- **5.3**: Behandelt die Kommunikation der Rollen und Verantwortlichkeiten.
- **6.2 e**: Dieser Abschnitt beinhaltet die Vermittlung von Informationssicherheitszielen.
- **7.2**: Hebt die Rolle von Schulungen zur Erlangung notwendiger Kompetenzen hervor.
- **7.2 c**: Dieses Kapitel beschreibt, dass Maßnahmen eingeleitet werden, wenn Kompetenzdefizite identifiziert werden.
- **10.2**: Eine mangelnde Awareness kann eine Nichtkonformität darstellen und es sollen Korrekturmaßnahmen gesetzt werden.

(vgl. [25], [30])

Direkt angesprochen wird das Thema bis auf einige Ausnahmen nur in Abschnitt 7.3, in dem explizit gefordert wird, dass sich Personen der Informationssicherheitspolitik, ihres persönlichen Beitrags zur Wirksam-

keit des ISMS und der möglichen Folgen der Nichteinhaltung im Klaren sind. (vgl. [30])

In der ISO/IEC 27002 wird das Konzept von Awareness und Sensibilisierung noch deutlicher. Bereits in der Einleitung wird darauf hingewiesen, dass technische Maßnahmen allein nicht ausreichen, um ein angemessenes Maß an Sicherheit zu erreichen. Viel wichtiger sind organisatorische Prozesse, Managementaktivitäten und insbesondere das Bewusstsein der Mitarbeitenden. Dies spiegelt sich unter anderem in Control 6.3 wider, welche explizit vorsieht, dass Mitarbeitende im Rahmen von Awareness und Schulungen mit den relevanten Richtlinien vertraut gemacht werden. (vgl. [30])

Um einen Überblick über Schulungsinhalte bezüglich der Richtlinien zu erhalten, wurde das Dokument auf Forderungen bezüglich der Erstellung solcher Regelungen analysiert. Dabei wurde identifiziert, dass 21,5% der 93 vorgegebenen Controls die Erstellung einer Richtlinie oder themenspezifischen Richtlinie vorsehen. (vgl. [30])

Darüber hinaus verlangen einige Controls explizit, dass sich Mitarbeitende Maßnahmen, die ihre Tätigkeit betreffen, bewusst sind („be aware of“), oder dass gezielte Awareness Maßnahmen umgesetzt werden („provide awareness“). Zur Identifikation dieser Controls wurde erneut das Dokument auf Passagen, in welchen diese Forderungen bestehen, analysiert. 9,6% der Controls befassen sich mit dem Bewusstsein der Mitarbeitenden, sowie 7,5% der Controls im Sinne der Bereitstellung von Sensibilisierungsmaßnahmen. Es kann also angenommen werden, dass Awareness für einen ganzheitlichen Ansatz der Compliance von Bedeutung und nicht nur einer einzigen Control zuzuschreiben ist. Die genaue Auflistung der Controls ist dem Anhang B zu entnehmen(vgl. [30])

2.4. Psychologische Aspekte im Bereich von Sensibilisierung

Wie zuvor beschrieben nimmt der Faktor Mensch eine wesentliche Rolle im Schutz von Informationswerten ein. Dadurch kann es in der Durchführung der Awareness Tätigkeiten zu zahlreichen Komplikationen führen. Diese sind unter anderem verschiedenen psychologischen Aspekten oder kulturellen Unterschieden zuzuschreiben. Aufgrund dessen widmet sich dieser Abschnitt verschiedener Kommunikationsarten, Lerntypen und Lernarten.

2.4.1. Lernen

Jeder Mensch ist ein Individuum, was sich ebenso in den jeweiligen Lernbedürfnissen, und in der Art und Weise wie Informationen aufgenommen werden, widerspiegelt. Auf dies sollte im Bereich der Awareness Rücksicht genommen werden. Laut Studien nimmt diese Individualisierung jedoch mit einer längeren Bildungsdauer ab. Das liegt daran, dass mit fortschreitendem Bildungsweg auch die Lernprozesse stärker standardisiert werden. Dadurch kommt es dazu, dass individuelle Unterschiede in der Lernweise seltener berücksichtigt werden. (vgl. [31])

Der Erfolg des Lernens hängt von unterschiedlichen Faktoren ab. Dazu zählen unter anderem das vorhandene Vorwissen, die angewendeten Lernstrategien, die zur Verfügung stehende Lernzeit sowie die mediale Aufbereitung des Lerninhalts. Motivation und Interesse, metakognitives Wissen und kognitive Fähigkeiten einschließlich Intelligenz spielen ebenso eine zentrale Rolle. Diese Faktoren wirken sich nicht nur auf den Lernprozess selbst aus, sondern auch auf die Nachhaltigkeit des Gelernten und dessen Übertragbarkeit auf neue Situationen. (vgl. [31])

Lernmodelle

Die pädagogische und didaktische Theorie unterscheidet verschiedene Lernparadigmen, die unterschiedliche Lernverständnisse erfassen. Zu den zentralen Beispielen zählen der Behaviorismus, der Kognitivismus sowie der Konstruktivismus. Diese Modelle bieten jeweils unterschiedliche Grundlagen und Ansätze für die Gestaltung von Lernprozessen im Kontext der Awareness. (vgl. [31], [23])

Der Behaviorismus beschreibt, eingegrenzt auf das Lernen, einen reaktiven Vorgang, bei dem das Gehirn als „Black box“ betrachtet wird: Es empfängt einen äußeren Reiz (Stimulus), woraufhin eine messbare Reaktion (Response) erfolgt. Emotionen oder subjektive Erfahrungen gelten in diesem Modell als irrelevant. Lernen erfolgt durch klassische oder operante Konditionierung, Versuch und Irrtum sowie durch Beobachtung. Ein zentrales Element dieses Modells ist, dass gewünschtes Verhalten durch Lob und Belohnung bestärkt, und unerwünschtes Verhalten durch Tadel und Bestrafung gehemmt wird. Lerninhalte werden hierbei auch in kleinen strukturierten Einheiten angeboten, die in einer festgelegten Reihenfolge vermittelt werden. Beispielsweise könnte dieses Modell im Bereich der Awareness angewendet werden, durch den gezielten Versand von Phishing-Mails, woraufhin positives (bei korrekter Erkennung) oder negatives Feedback gegeben wird. (vgl. [31], [23])

Im Gegensatz dazu fokussiert sich der Kognitivismus auf die inneren Prozesse des Lernenden. Lernen wird in diesem Modell als aktiver, zielgerichteter Vorgang verstanden, bei dem die Informationen aufgenommen, verarbeitet und in bestehendes Wissen integriert werden. Prozesse wie Begriffsbildung, Wahrnehmung, Problemlösen, Wiedererkennen und Schlussfolgern sind hierbei von Bedeutung. Die Lehrperson nimmt eher die Rolle eines Tutors oder Lernbegleiters ein, da der Lernende hier mehr auf sich gestellt ist. Lernprozesse zielen hierbei auf das Verständnis und die Einsicht ab, wodurch ein tieferes, transferfähiges Wissen aufgebaut werden soll. Ein Beispiel im Bereich von Awareness wäre, dass Administratoren nach dem Erkennen eines Problems eigenständig Maßnahmen ergreifen, wie beispielsweise das Einrichten mehrerer Terminals zur Erhöhung der Systemsicherheit. (vgl. [31], [23])

Der Konstruktivismus vertritt ein radikal-subjektives Lernverständnis. Lernen geschieht hier nicht durch das bloße Lösen vorgegebener Aufgaben, sondern durch die selbstständige Auseinandersetzung mit offenen, oft mehrdeutigen Problemstellungen. In diesem Modell gibt es objektiv kein „richtiges“ oder „falsches“ Wissen, vielmehr hängt die Erkenntnis von der individuellen Perspektive und Interpretation ab. Lehrpersonen übernehmen hier mehr die Rolle eines Coaches oder Moderators, während Lernende weitgehend autonom agieren. Eine Voraussetzung ist dabei ein gewisses Maß an Vorwissen und Problemlösekompetenz. Im Kontext der Awareness bedeutet das beispielsweise, dass Mitarbeitende eigenständig ein mentales Modell über den potenziellen Bedrohungsgrad durch Angreifer entwickeln und daraus Schutzstrategien ableiten. (vgl. [31], [23])

Der Lernzyklus nach David A. Kolb definiert Lernen als einen Prozess, bei dem vier Phasen zu unterscheiden sind. Lernen beginnt demnach mit einer konkreten Erfahrung, die als Ausgangspunkt für den Erkenntnisgewinn dient. In der Phase Beobachtung und Reflexion wird diese dann verarbeitet. Der Lernende denkt über das Erlebte nach und zieht erste Schlussfolgerungen. Auf dieser Basis werden im nächsten Schritt abstrakte Konzepte, Verallgemeinerungen und Theorien erstellt. Diese dienen dazu, das Geschehene zu erklären, und zukünftiges Handeln in vergleichbaren Situationen vorzubereiten. In der letzten Phase, der aktiven Umsetzung, werden diese Konzepte in der Realität erprobt. Dies generiert wiederum neue Erfahrungen, welche den Lernzyklus erneut in Gang setzen. Lernen ist in diesem Modell somit ein kontinuierlicher Prozess, bei dem Theorie und Praxis in enger Wechselwirkung stehen. (vgl. [32])

Im Kontext des Awareness-Trainings im Bereich Informationssicherheit-Sicherheit lässt sich Kolbs Modell beispielhaft anhand einer Phishing-Situation veranschaulichen. Ein Mitarbeitender erhält eine verdächtige E-Mail mit einem Anhang oder verdächtigen Link. In der Phase der Reflexion wird das Verhalten analysiert: Der Mitarbeitende reagiert entweder korrekt, indem die E-Mail gemeldet, gelöscht, oder auf den Angriff hereingefallen wird. Diese Beobachtung führt wiederum zur Bildung von Annahmen, welches Verhalten in einer solchen Situation angemessen ist. Zum Beispiel, dass Links in unerwarteten E-Mails stets mit Vorsicht zu behandeln sind. Durch gezielte Schulungsmaßnahmen im Rahmen des Awareness Programms werden diese Annahmen entweder bestätigt oder korrigiert. Das führt zu einem Verständnis bei Mitarbeitenden, da sie nun ein Muster von Phishing Angriffen erkennen. (vgl. [32])

Lernstile

Es wird häufig Vesters (1984) Lerntypenmodell herangezogen, welches eine Einteilung in visuelle, auditive, haptische und intellektuelle Lerntypen vornimmt. Dieses basiert auf der Annahme, dass Menschen bevorzugt über Sinneskanäle Informationen aufnehmen und verarbeiten. Obwohl dieses Modell in der Praxis verbreitet ist, wurde es in neuerer Forschung, insbesondere bei der Erwachsenenbildung, kritisch hinterfragt. Wie Schrader in Untersuchungen zeigte, stellt sich das Lernverhalten von Erwachsenen in der beruflichen Weiterbildung viel differenzierter dar, als ursprünglich von Vester angenommen. (vgl. [33])

Daraufhin wurden fünf neue Lerntypen identifiziert. Der Theoretiker zeichnet sich dadurch aus, dass sowohl praktisches als auch theoretisches Lernen für diesen gewinnbringend ist. Anwendungsorientierte hingegen bevorzugen Ausprobieren und Überprüfen von Inhalten und zeigen damit Ähnlichkeiten zum klassischen haptischen Lerntyp. Musterschüler gelten als ehrgeizig und fleißig, sind aber auf strukturierte Anleitung angewiesen. Gleichgültige Lernende zeigen nur geringes Interesse an Weiterbildung und eignen sich nur das Notwendigste an. Der Unsichere verbindet Lernprozesse mit Angst und lässt sich nur durch äußeren Druck und die Einsicht in die Relevanz des Lernens zum Handeln motivieren. (vgl. [33])

Ein weiterer einflussreicher Ansatz stammt von David A. Kolb, der basierend auf seinem Lernzyklusmodell vier grundlegende Lerntypen unterscheidet. Der Divergierer lernt bevorzugt durch konkrete Erfahrungen in Verbindung mit reflektierendem Beobachten. Der Assimilierer bevorzugt theoretische Modelle, reflektiertes Beobachten und abstrakte Begriffsbildung. Konvergierer kombinieren abstrakte Konzeptualisierung mit aktivem Experimentieren. Der Akkomodierer lernt am effektivsten durch konkrete Erfahrungen und aktives Handeln. (vgl. [33])

2.4.2. Kommunikation

Obwohl die Grundlagen der Lernmodelle und die Unterscheidung von Lerntypen wichtig sind, spielt auch die Art der Wissensvermittlung eine wichtige Rolle im Lernprozess. Wie Ellis und Beattie beschreiben, beeinflussen die Stimmlage, Mimik, Gestik, Körperhaltung und manchmal auch Berührung die Wirkung der Kommunikation. Diese nichtsprachlichen Elemente können Inhalte beispielsweise verstärken oder schwächen. (vgl. [34])

Ellis und Beattie unterscheiden in ihrer Analyse der Kommunikation verschiedene Kanäle, über die Informationen übermittelt werden: sprachlich und nonverbal sowie linguistisch und nicht-linguistisch. Die sprachliche Kommunikation umfasst gesprochene oder geschriebene Sprache, während sich die nonverbale Kommunikation auf Körpersprache, Tonfall und andere nichtsprachliche Ausdrucksformen abzielt. Der Kommunikationsprozess selbst wird als Interaktion zwischen Sendenden, Empfangenden und der übermittelten Nachricht definiert. Der Sendende codiert eine Information in Form eines Signals, das an den Empfangenden übermittelt wird. Dieser decodiert das Signal und reagiert mit der Absicht des Sendenden. (vgl. [34])

Unklare Ausdrucksweise, widersprüchliche Signale oder das "Verlieren des roten Fadens"können zu Missverständnissen führen. Zusätzlich können äußere Störfaktoren, wie eine schlechte technische Verbindung oder Hintergrundgeräusche die Kommunikation beeinträchtigen. Kulturelle Unterschiede sollten berücksichtigt werden, da bestimmte Gesten, Redewendungen oder Körpersignale in verschiedenen Kulturkreisen unterschiedliche Bedeutungen haben können. (vgl.[34])

Die Anpassung des Kommunikationsniveaus an das Vorwissen des Empfangenden ist ebenso wichtig für die Kommunikation selbst. Nur wenn die Informationen dem kognitiven und sprachlichen Niveau des Lernenden entsprechen, kann eine zielgerichtete Reaktion erfolgen. (vgl. [34])

Das Kommunikationsquadrat

Für gelungene Kommunikation ist nicht nur der Inhalt der Nachricht entscheidend, sondern auch, wie diese vermittelt und aufgenommen wird. Das Kommunikationsquadrat von Friedemann Schulz von Thun ist ein etabliertes Modell zur Analyse und Optimierung kommunikativer Prozesse. Dieses geht davon aus, dass jede Nachricht vier verschiedene Ebenen beziehungsweise „Seiten“ enthält und potenziell auch auf vier unterschiedlichen Ebenen vom Empfangenden interpretiert werden kann. Das Ziel des Modells ist es, Missverständnisse zu minimieren, indem sowohl Sendenden- als auch Empfangendenperspektive berücksichtigt werden. (vgl. [35])

Die Sachebene bezieht sich auf den reinen Sachinhalt. Hierbei handelt es sich um die objektive Information, die übermittelt werden soll. Die Selbstoffenbarungsebene enthält Informationen über die Person des Sendenden, beispielsweise über Einstellungen, Emotionen oder Haltungen. Auf der Beziehungsebene wird ausgedrückt, wie der Sendende zum Empfangenden steht. Die Appellebene ziehlt auf das Verhalten des Empfangenden ab, also darauf, eine bestimmte Reaktion oder Handlung zu veranlassen. (vgl. [35])

Nachfolgend wird ein Beispiel aus dem Bereich der Security Awareness, nämlich zum Thema Passwortsicherheit beschrieben: Die Aussage „Ihr Passwort ist unsicher und sollte dringend geändert werden“ lässt sich wie folgt analysieren. Auf der Sachebene wird eine objektive Information vermittelt: Das aktuelle Passwort entspricht nicht den Sicherheitsanforderungen. Die Selbstoffenbarungsebene kann in diesem Fall das Verantwortungsbewusstsein des Sendenden zum Ausdruck bringen, in dem Fall eine Fürsorge gegenüber der Sicherheit. Die Beziehungsebene ist sensibler. Die Formulierung könnte als kritisch oder herablassend wahrgenommen werden, je nach Kontext, Tonfall oder Körpersprache des Sendenden. Auf der Appellebene wird klar, dass der Empfangende sein Passwort ändern soll, um den Sicherheitsrichtlinien zu entsprechen. (vgl. [35])

Ebenso wie jede Nachricht vier Seiten hat, besitzt der Empfangende vier „Ohren“, mit denen er die Nachricht interpretieren kann. Über das „Sachohr“ wird der reine Informationsgehalt wahrgenommen. Um auf das Beispiel zurückzukommen, die Information über die Unsicherheit des Passworts. Das „Selbstoffenbarungsohr“ interpretiert, was die Aussage über den Sendenden verrät. Ob dieser zum Beispiel sicherheitsbewusst oder bevormundend wirkt. Über das „Beziehungsohr“ wird beurteilt, wie der Sendende zum Empfangenden steht. Hier kann die Botschaft entweder als unterstützend oder als kritisierend und herabwürdigend aufgefasst werden. Schließlich wird über das „Appellohr“ die intendierte Handlungsaufforderung erkannt, also die Erwartung, das Passwort zu ändern. (vgl. [35])

Missverständnisse entstehen häufig, wenn der Sendende und der Empfangende unterschiedliche Ebenen interpretieren. So kann eine sachlich gemeinte Aussage auf der Beziehungsebene als Angriff empfunden werden, wenn zum Beispiel Tonfall oder Mimik ungeschickt gewählt sind. Ebenso kann ein gut gemeinter Appell durch das Selbstoffenbarungsohr besserwisserisch oder belehrend wirken. Insbesondere in sensiblen Kommunikationsfeldern wie der Awareness, ist eine bewusste Auswahl der Kommunikationsform wichtig. Nur durch eine differenzierte und empathische Ansprache, die sowohl sachlich korrekt als auch beziehungsorientiert gestaltet ist, kann die gewünschte Wirkung erzielt und das Risiko von Missverständnissen reduziert werden. (vgl. [35])

Kommunikationsebenen

Bei der Kommunikation können verschiedene Arten auf verschiedenen Ebenen unterschieden werden. Im Bereich des Awareness Trainings kann das Wissen bezüglich dieser relevant sein, um für mögliche Herausforderungen gewappnet zu sein, und auf die Zuhörenden einzugehen. Beißel beschreibt verschiedene Ebenen der Kommunikation. (vgl. [23])

Einige davon lauten wie folgt: Auf der Ebene der Teilnehmenden kann zwischen Eins-zu-Eins, Eins-zu-Viele und Viele-zu-Viele unterschieden werden. So kann es sich beispielsweise um persönliche Gespräche, Vorträge oder gemeinsame Workshops auf einem ähnlichen Wissenstand handeln. Weiters existiert die Ebene der Kanäle, welche sich mit den Sinnen der Kommunikationsteilnehmenden befasst. Grundsätzlich verfügt der Mensch über fünf Sinne, jedoch sind in diesem Kontext lediglich die visuelle und auditive Wahrnehmung von Bedeutung. Beißel betont, dass es jedoch bei Beeinträchtigungen der Teilnehmenden, wie beispielsweise Sehbeeinträchtigung, zu Ausnahmen kommen kann. Bezüglich der Verdecktheit kann es sich um offensichtliche oder unterschwellige Botschaften handeln. Das heißt der Empfangende nimmt die Informationen direkt und offensichtlich durch Äußerungen war. Anders jedoch ist es bei der unterschwelligen Kommunikation, bei welcher auf emotionale Aspekte gebaut wird, welche das Individuum dazu verleiten sollen, das erwünschte Verhalten aus eigenen Stücken anzunehmen. (vgl. [23])

3. Verwandte Arbeiten

Als Besonderheit dieser Arbeit gilt der Fokus auf den Bereich von Hochschulen in Österreich. Im Gegensatz zu beispielsweise Deutschland ist in Österreich nur wenig Literatur beziehungsweise Forschungen im Bereich der Security Awareness vorhanden. Da Bedrohungen im Bereich der Informationssicherheit stetig steigen und Hochschulen in der Öffentlichkeit stark präsent sind, ist dem Forschungsdrang in diesem Bereich eine wichtige Bedeutung zuzuordnen.

In nachfolgendem Kapitel werden Arbeiten, Publikationen sowie Best Practices, welche mit der Thematik der Trainingsaktivitäten in Bezug auf Informationssicherheit in Verbindung stehen, in Kurzform zusammengefasst.

3.1. Security Awareness: Grundlagen, Maßnahmen und Programme für die Informationssicherheit

In dem Buch „Security Awareness – Grundlagen, Maßnahmen und Programme für die Informationssicherheit“ von Stefan Beißel wird über Trainingsaktivitäten im Bereich Informationssicherheit gesprochen. Der Ausgangspunkt ist, dass das Sicherheitsbewusstsein ein integraler Bestandteil der Unternehmenssicherheit ist. (vgl. [23])

Zunächst wird ein Einblick in die Grundlagen der Informationssicherheit gegeben. Dieser beinhaltet primäre Sicherheitsziele, Bedrohungen, Abwehrmaßnahmen und wirtschaftliche Überlegungen. Hierbei wird betont, dass nicht nur technische Lösungen, sondern insbesondere das Verhalten der Mitarbeiter zur Sicherheit beitragen. Der Autor betont, dass die Unternehmenskultur für ein sicherheitsbewusstes Arbeitsumfeld essenziell ist, für den Erfolg eines Security Awareness Programms. (vgl. [23])

In einem zentralen Kapitel wird dargelegt, welche konkreten Maßnahmen eingesetzt werden sollen, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken. Die Autoren geben Beispiele für Online-, Plakat- und Workshop-Kampagnen. Um eine positive Wirkung zu erzielen, empfehlen sie, alle Aktionspunkte in die bestehenden Betriebsabläufe des Unternehmens zu integrieren. Die Beispiele verdeutlichen, wie die Medien selektiv genutzt werden können, um unterschiedliche Gruppen von Mitarbeitenden zu erreichen. (vgl. [23])

In diesem Zusammenhang wird auch gezeigt, wie man angemessene Awareness Programme entwickelt und plant, sie umsetzt und fortlaufend überwacht und optimiert. Auch Compliance-Vorgaben sind durchaus relevant, da sicherheitstechnische Maßnahmen in Unternehmen wesentlich auch von regulatorischen Vorgaben bestimmt sind. (vgl. [23])

3.2. The new users‘ guide: How to raise information security awareness

Der Leitfaden „The New Users' Guide: How to Raise Information Security Awareness“ von ENISA zeigt die Bedeutung und Notwendigkeit von Security Awareness für Unternehmen und Organisationen auf. Die Veröffentlichung beinhaltet Methoden, Prozessmodelle, Schlüsselindikatoren und Fallstudien, die darauf abzielen, Schulungsprogramme effektiv zu erstellen, und umzusetzen. (vgl. [27])

Es beginnt mit einer Erklärung der Bedeutung von Sicherheitsbewusstsein, da menschliche Fehler die größte Schwachstelle im Bereich der Informationssicherheit sind. Erfolgreiche Awareness Programme sollten mit einer klaren Strategie beginnen, die aus folgenden drei Hauptphasen bestehen: „Plan, Do and Check“. Dazu gehört die Planung, in der Ziele, Zielgruppen, Kommunikationsstrategien, Ressourcen und Budgets definiert werden. Ein weiterer Bestandteil ist die Durchführung, in der die Schulungen in dauerhaften oder regelmäßigen Workshops, E-Trainings oder interaktiven Kampagnen stattfinden. Wie Fallstudien zeigen, tragen weitere Aspekte des Führungsverhaltens zur Wirksamkeit der Security Awareness bei. (vgl. [27])

In der Evaluierungsphase sind dann die KPIs bestimmt, und es werden Umfragen, Fokusgruppen oder Nutzerverhaltensanalysen eingesetzt, um die Programme ständig zu verbessern. Darüber hinaus werden die oben beschriebenen Herausforderungen, die während der Durchführung eines solchen Programms bestehen, und ihre Lösungen erläutert. Dazu gehören elementare Fakten wie die mangelnde Unterstützung des Managements, begrenzte Budgets oder der Widerstand der Mitarbeitenden. (vgl. [27])

3.3. IT-Grundschutz-Profil für Hochschulen

Das IT-Grundschutz-Profil für Hochschulen, ein von ZKI e. V. herausgegebenes Dokument, dient als allgemeine Leitlinie zur Informationssicherheitssicherstellung, die speziell an die Anforderungen von Hochschulen angepasst ist. Es basiert auf dem IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik und wurde in einem breiten Konsens mit einer Vielzahl von fachkundigen Akademikern und IT-Fachleuten entwickelt. Darüber hinaus wird im Abschnitt „Gründe für die Bedeutung“ des IT-Grundschutz-Profils für Hochschulen festgestellt, dass der Sicherheitsaspekt in diesem Bereich erheblich an Bedeutung gewinnt. Dies ist insbesondere auf den offenen Charakter von Universitäten und die weit verbreiteten Netzwerkbedrohungen aus der Cyberwelt zurückzuführen. (vgl. [5])

Ferner bietet es eine standardisierte Vorgehensweise zur Implementierung von Sicherheitsmaßnahmen und dient so Hochschulen als Schablone für ihre eigenen Sicherheitskonzepte. Dazu gehört auch die Analyse einer Referenzarchitektur, die die relevanten Unternehmensprozesse umfasst, darunter Rekrutierung und Zulassung, Immatrikulation und Prüfungen sowie die Informations- und Kommunikationstechnologie-Infrastruktur der Studierenden. Alle erforderlichen Sicherheitsanforderungen werden dabei konsequent anhand des Baukastenprinzips des IT-Grundschutzes modelliert und in Prozesslandkarten abgebildet. Somit erhalten die Hochschulen genaue Anweisungen für die Umsetzung erforderlicher Sicherheitsmaßnahmen. (vgl. [5])

Der Umgang mit den hochsensiblen Daten in der Studierendenverwaltung oder für Prüfungen erfordert vom Informationssicherheitsbeauftragten, zusätzliche Risikoanalysen und sicherheitstechnische Maßnahmen. Darüber hinaus bietet das Profil eine zusätzliche Perspektive auf Best Practices wie Identitätsmanagement, Netzwerksicherheit, Sicherheitsmanagement und Notfallvorsorge. Dadurch erhalten Hochschulen ein ISMS-Toolkit, um das für ihre Anforderungen geeignete Informationssicherheits-Managementsystem zu erstellen. (vgl. [5])

3.4. NIST SP 800-50: Building a Cybersecurity and Privacy Learning Program

Die Veröffentlichung „Building a Cybersecurity and Privacy Learning Program“ (NIST Special Publication 800-50r1) umfasst ein Empfehlungsschreiben zur Schaffung eines Lernprogramms für Cybersicherheit und Datenschutz. (vgl. [28])

CPLP wurde entwickelt, um das Bewusstsein für Cybersicherheitsrisiken zu schärfen, und ein sicheres Umfeld in der Organisation zu schaffen. Dadurch sollen durch Vorbeugung und gezielte Schulungen die Risiken minimiert werden. Die Publikation ist vor allem für staatliche Institutionen gedacht. Dies spiegelt sich in einem weiteren Aspekt der Publikation wider, nämlich die betonte strategische Planung und Anpassung des CPLP an die übergeordneten Ziele der Organisation. (vgl. [28])

Es beinhaltet das Festlegen klarer Lernziele, die Identifikation der Relevanz der Zielgruppe und die Messung der Programmeffektivität. In den meisten Fällen dauert die Implementierung des CPLP mehrere Phasen: Die erste Phase ist die Festlegung von Strategie und Zielen, dann die Festlegung der Relevanz der Zielgruppen und schließlich die Entwicklung der Lerninhalte. Die allgemeinen Schulungen sollten sich somit sowohl auf alle Mitarbeitenden als auch auf spezielle Schulungen für Personen mit größeren Zugriffsrechten oder besonderen Funktionen erstrecken. Mit der Hauptbestimmung, jeden Benutzer zu erreichen, sollten allgemeine Schulungen das Erkennen von schwachen Passwörtern, Phishing-Angriffen und den Umgang mit Daten enthalten. Mitarbeitenden als Privilege Access Holdern sollten ebenfalls spezielle Schulungen erteilt werden. (vgl. [28])

Ein weiteres zentrales Element des CPLP ist fortlaufendes Überprüfen und bewerten der Programmkomponenten. Mithilfe der Datenerfassung auf die Leistungskennzahlen, „Teilnahme am Schulungsprozess“ sowie „Testprüfungsergebnisse“ kann die Wirksamkeit des Programms ermittelt und verbessert werden. Die Metriken sollten regelmäßig mit der Geschäftsleitung diskutiert werden. (vgl. [28])

Außerdem bildet die Integration in die Unternehmenskultur ein zusätzliches Merkmal erfolgreicher CPLPs. Hierzu tragen insbesondere die Führungskräfte bei, indem sie sich zuerst sicher und aktiv am Schulungsprogramm beteiligen. (vgl. [28])

4. Methodik

Für diese Arbeit kam ein kombinierter Ansatz von qualitativer und quantitativer Forschung zum Einsatz. Es wurden Umfragen an Mitarbeitenden der FH St. Pölten sowie an Kontaktpersonen anderer österreichischer Hochschulen durchgeführt, um die Besonderheiten von Hochschulen zu identifizieren und speziell auf die Gedankengänge der Probanden einzugehen.

Weiters erfolgte im Zuge von Umfragen eine Auswertung von Multiple Choice Fragen. Dies diente der Möglichkeit Analysen genauer durchzuführen. Schlussendlich kam die Unterstützung von Grafiken zur Ergebnisdarstellung zum Einsatz.

Als Interviewpartner zur Erhebung des Sicherheitsniveaus an Hochschulen erfolgte die Auswahl relevanter Vertreter dieser Einrichtungen. Vorzugsweise wurde hierfür der jeweilige CISO (Chief Information Security Officer) oder alternativ eine verantwortliche Person der Bereiche Datenschutz oder Informationstechnologie herangezogen.

Die Durchführung der beiden Umfragen erfolgte mittels des Tools Microsoft Forms. Diese beinhalteten einmal 10, und bei der anderen 14 Fragen. Wobei sich diese insgesamt in 13 Single Choice, 9 Multiple Choice und je eine Freitext-Frage gliederten.

Eine weitere Forschungsmethode dieser Arbeit stellte die ausführliche Recherche und der Vergleich zahlreicher Fachliteratur dar. Die Zusammenfassung der wichtigsten Werke können dem Kapitel 3 entnommen werden.

Obwohl durch den kombinierten Ansatz aus qualitativer und quantitativer Forschung eine umfassende Analyse angestrebt wurde, gibt es einige methodische Einschränkungen, die berücksichtigt werden sollten.

Die Durchführung der Umfragen könnte zu einer begrenzten Rücklaufquote geführt haben, was die Repräsentativität der Ergebnisse in Frage stellt. Zudem besteht die Möglichkeit einer selbstselektiven Teilnahme, da womöglich vor allem Personen mit Interesse an der Thematik an der Befragung teilgenommen haben könnten. Dadurch könnten bestimmte, möglicherweise wichtige Perspektiven unterrepräsentiert oder nicht berücksichtigt worden sein.

Schließlich unterliegt auch die Literaturrecherche gewissen Einschränkungen, etwa durch die Verfügbarkeit und zeitgemäße Aktualität der Quellen. Einige relevante Studien oder Daten könnten zum Zeitpunkt der Recherche nicht gänzlich zugänglich gewesen sein, wodurch sich eine potenzielle Begrenzung der theoriegeleiteten Fundierung ergibt.

Trotz dieser Limitationen liefern die verwendeten Methoden wertvolle, wenn auch nicht vollends umfassende Erkenntnisse und ermöglichen eine Beantwortung der Forschungsfragen.

5. Herangehensweise

Dieses Kapitel dient der Beschreibung des Herzstückes der Arbeit: der praktischen Ausarbeitung der Fragestellungen. Es gliedert sich in die Teile „Erhebung des Sicherheitsbedarfs an Hochschulen“ und „Erstellung eines Awareness Konzeptes“. Ersteres befasst sich mit der Erhebung und Identifikation des spezifischen Sicherheitsbedarfs an Hochschulen, sowie den dabei auftretenden Problemen und Herausforderungen.

Der zweite Teil der Ausarbeitung befasst sich mit der Planung und Erstellung eines Security Awareness Konzeptes für Hochschulen. Die tatsächliche Durchführung wird in dieser Arbeit jedoch nicht behandelt. Weiters werden für die auftretenden Problematiken eine mögliche Lösung dargestellt.

5.1. Sicherheitsbedarf an Hochschulen

Um einen allumfassenden Überblick über die IST-Situation bezüglich Informationssicherheit und Awareness im Bereich von Hochschulen in Österreich zu erhalten, erfolgte die Durchführung einer Umfrage. Diese gliedert sich in die Abschnitte Informationssicherheit Allgemein, Awareness Maßnahmen, Security Awareness Tools und weitere Anregungen. Ziel war es zu identifizieren, ob sich Einrichtungen mit dem Thema Informationssicherheit befassen und im Zuge dessen Awareness Tätigkeiten durchführen. Weiters soll analysiert werden, wie Awareness umgesetzt wird und welche Technologien beziehungsweise Medien zum Einsatz kommen. Für die Erstellung der Fragen wurde das Buch [23] zu Hilfe gezogen. Weiters erfolgte eine Abstimmung bezüglich der Umfrage mit der Sicherheitsverantworlichen und weiteren Experten der Fachhochschule St.Pölten. Die Umfrage kann dem Anhang E entnommen werden. Eine genaue Auswertung der Ergebnisse befindet sich im Kapitel 6 dieser Arbeit.

5.1.1. Besonderheiten der Hochschul-IT

Die Strukturen der Informations- und Kommunikationstechnologien von universitären Bildungseinrichtungen unterscheiden sich vielfach von jenen klassischer Unternehmen. Dies liegt speziell an der Vielschichtigkeit der Aufgabenbereiche in Forschung, Lehre und Verwaltung sowie an der stark dezentralen Organisationsweise. Dadurch ergibt sich eine große Mannigfaltigkeit an IT-Landschaften und Verantwortlichkeiten, die sich je nach Fakultät, Fachbereich, Forschungsgruppe oder sogar einzelner Lehrenden stark voneinander abheben. (vgl. [5])

Hochschulen zeichnen sich traditionell durch ein hohes Maß an Offenheit und Zugänglichkeit aus – etwa durch öffentlich erreichbare Netzwerke, Gastzugänge oder öffentlicher IT-Angebote. Ebenso wie in den IT-Komponenten spiegelt sich das Dilemma der öffentlichen Zugänglichkeit auch an den physischen Standorten wider. Kombiniert mit der Ungleichförmigkeit der eingesetzten Systeme und Prozesse, führt das zu einer besonders hohen Angriffsfläche für Cybergefährdungen. Wissenschaftseinrichtungen stehen damit vor der Herausforderung, einerseits die notwendige Freiheit für Forschung und Lehre zu gewährleisten, und andererseits ein ausreichendes Maß an Informationssicherheit zu sichern. (vgl. [36])

Ein zentraler Aspekt ist die große Nutzerschaft, die durch eine hohe Fluktuation gekennzeichnet ist. Studierende, Lehrende, Forschende und externe Projektpartner kommen und gehen in kurzen Zyklen, wodurch es zu einem sehr heterogenen Niveau an Digitalfertigkeit und Sicherheitsbewusstsein kommt. Die Bandbreite reicht von IT-affinen Fachpersonen bis hin zu Nutzenden mit kaum vorhandenem Sicherheitsverständnis. Diese Ungleichheit erschwert die Umsetzung einheitlicher Sicherheitsmaßnahmen erheblich.

Darüber hinaus verarbeiten Hochschulen besonders sensible Daten. Als zentrales Kerngeschäft gelten hierbei die Verarbeitung und Verwaltung von Studierendendaten, die alle Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – betreffen. Die Verletzung dieser Ziele kann nicht nur rechtliche und organisatorische Folgen haben, sondern auch das Vertrauen in die Institution massiv schwächen. (vgl. [5])

Strukturell betrachtet bestehen Hochschulen aus einer Kombination zentraler und dezentraler IT-Systeme. Die zentrale Hochschulverwaltung betreibt typischerweise IT-Dienste und -Infrastrukturen, wie beispielsweise Campus-Management-Systeme, Authentifizierungsdienste oder Verwaltungsnetzwerke. Parallel dazu existieren jedoch eine Vielzahl ergänzender, oft eigenverantwortlich betriebener IT-Angebote in den Fakultäten, Instituten und Forschungsgruppen. Diese Systeme sind häufig unmittelbar mit der zentralen Infrastruktur verbunden, etwa weil Mitarbeitende in beiden Bereichen tätig sind oder Daten ausgetauscht werden müssen. Diese enge technische und organisatorische Verschränkung erhöht das Risiko lateral verlaufender Angriffe: Eine Kompromittierung eines dezentralen Systems – beispielsweise in einer Forschungsgruppe – kann unter Umständen einen Einstiegspunkt in die Hochschul-IT darstellen. (vgl. [37])

Während in Deutschland mit dem IT-Grundschutz-Profil für Hochschulen und dem Zusammenschluss der Rechenzentren im „Verein der Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ (ZKI) bereits Strukturen zur Stärkung der IT-Sicherheit etabliert wurden, fehlt eine vergleichbare koordinierte Initiative bislang in Österreich. Hochschulen in Österreich sind daher oftmals auf eigene Strategien und Maßnahmen angewiesen, um Informationssicherheit angemessen umzusetzen. (vgl. [38])

5.1.2. Bedrohungslage an Hochschulen

Aufgrund von mangelnden Informationen wurde in diesem Kontext auch nach internationalen Quellen gesucht. Die gefundenen Informationen können allerdings auch für lokale universitäre Einrichtungen von Bedeutung sein.

Wie in anderen Organisationen kann auch im Kontext von Bildungseinrichtungen kein absoluter Schutz gewährleistet werden. Darauf weist unter anderem der Wissenschaftsrat hin, der die inhärenten Risiken betont, denen wissenschaftliche Einrichtungen ausgesetzt sind. (vgl. [36])

Eine zentrale Bedrohung ergibt sich aus der einzigartigen Struktur und Offenheit von Hochschulen. Die IT-Landschaft ist häufig dezentral organisiert, was sich in einer Fülle eigenständiger Domains und Subdomains spiegelt. Vor allem öffentlich erreichbare Webanwendungen stellen ein wesentliches Einfallstor für Angriffe dar. Wichtige Informationen können über ungenügend gesicherte Websites womöglich kompromittiert werden. Je mehr offen zugängliche Systeme es gibt – beispielsweise durch getrennt verwaltete Domains einzelner Fakultäten –, desto höher ist die Wahrscheinlichkeit eines Datenschutzverstoßes. Je mehr nicht gewartete oder nur unzureichend aktualisierte Online-Angebote existieren, desto höher ist das Risiko. Forschungen zeigten außerdem, dass Universitäten (in den USA) mindestens einen offenen RDP-Port haben, der eventuell als Eintrittstor verwendet werden kann. (vgl. [39])

Wie aus zuvor getätigten Analysen hervorgeht, ist ein weiteres spezifisches Merkmal von Hochschulen deren physische Zugänglichkeit. Viele Einrichtungen sind für die Öffentlichkeit zugänglich, etwa durch frei begehbare Bibliotheken oder Mensen. Dies erhöht das Risiko des unberechtigten Zugriffs auf Infrastruktur. Zwar sind bestimmte Bereiche durch Zutrittskontrollen geschützt, jedoch kann auch nach den offiziellen Öffnungszeiten nicht von absoluter Sicherheit ausgegangen werden. (vgl. [38])

Auch systematische Schwächen im Passwortmanagement sind nachweisbar. In einer Untersuchung deutscher Bildungseinrichtungen wurden bei 73 Institutionen Nutzergruppen mit identischen Passwörtern festgestellt, die über mehrere Dienste hinweg verwendet wurden. Darüber hinaus nutzten 55 Hochschulen schwache Passwortpraktiken, wobei Kennwörter häufig auf triviale Informationen wie Benutzernamen, den Namen der Hochschule oder den Namen des jeweiligen Dienstes basierten. (vgl. [38])

Zentrale IT-Dienste wie E-Mail, DNS, VPN, Fernzugriff, Single-Sign-On oder auch Druckdienste weisen häufig bekannte Schwachstellen auf, doch die Zusammenhänge sind komplex. Viele Gefährdungen betreffen allerdings nicht exklusiv Hochschulen, sondern ziehen sich durch Behörden und Firmen. Hierzu zählen zum Beispiel veraltete oder stiefmütterlich gewartete Server, mehrfach verwendete oder simple Passwörter und unzureichenden Schutzmaßnahmen. (vgl. [38])

Als besonders anspruchsvoll gilt abermals die Offenheit von Universitäten, da Studierende, Lehrende, Verwaltungsmitarbeitende und externe Partner auf Systeme zugreifen. Dies erfordert scharfe Abgrenzung und gut gesicherte Verwaltungsstrukturen, insbesondere bei kritischen Anlagen wie der zentralen IT-Infrastruktur. (vgl. [38])

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) thematisiert im IT-Grundschutzprofil für Hochschulen spezifische Risiken auf Basis typischer Hochschulabläufe. Aus Gründen der Übersichtlichkeit wird hier jedoch nicht detailliert auf die Risiken der einzelnen behandelten Bausteine eingegangen. (vgl. [5])

Ein weiteres Risiko resultiert aus sogenannten Insiderbedrohungen. Lallie, Thompson, Titis und Stephens schildern, dass Studierende als mögliche Gefährdung besonders zu berücksichtigen sind, da sie oft über umfassendes technisches Wissen verfügen, jedoch nicht immer ausreichend im Bereich Informationssicherheit unterwiesen wurden. Die Motivation reicht von Neugier über Notenmanipulation bis hin zu Frustration oder Unzufriedenheit. Zusätzlich setzen viele Hochschulen auf externe Anbieter - auch für kritische Dienste - was das Risiko durch Dritte ("Third-Party Risk") erhöht. Während DDoS-Angriffe im Vergleich seltener auftreten, stehen Bedrohungen wie Ransomware, Phishing oder Social Engineering deutlich mehr im Fokus. (vgl. [40])

Zusammenfassend ergeben sich für Hochschulen vor allem folgende Gefährdungsschwerpunkte:

- **Physische Sicherheit**: Öffentlich zugängliche Gebäude mit potenziellem Risiko für unbefugten Zutritt.
- **Web-Schwachstellen**: Eine Vielzahl öffentlich erreichbarer Websites und Webanwendungen weisen unzureichende Absicherungen auf.
- **Passwort-Risiken**: Unsichere oder mehrfach verwendete Zugangsdaten erleichtern unberechtigten Eindringlingen den Zugang.
- **Insider Bedrohung**: Mögliche Risiken durch Studierende und Mitarbeiter mit IT-Fachwissen.
- **Abhängigkeiten Dritter**: Die Abhängigkeit von externen Anbietern, auch bei kritischen Diensten, birgt Unsicherheiten.
- **Personelle Anfälligkeiten**: Unzureichende Sensibilisierung im Bereich der Informationssicherheit.
- **Ransomware**: Diese stellen eine erhebliche Bedrohung für die Verfügbarkeit und Integrität der Daten dar.
- **DDos-Attacken**: Weniger häufig, aber potenziell stark störend für den laufenden Betrieb.

5.1.3. Unterscheidung zu anderen Branchen

Um die strukturellen Unterschiede und eventuellen Gemeinsamkeiten ausgewählter Organisationen aus verschiedensten Bereichen zu vergleichen, wurde als Vertreter der „universitären Einrichtungen“ die „FH St. Pölten“ gewählt. Es sei angemerkt, dass als Basis zur Auswahl der Vergleichsorganisationen die öffentliche Web-Verfügbarkeit von Unternehmensinformationen zugrunde lag.

Die Struktur einer Organisation spiegelt nicht nur deren Aufgaben und Ziele wider, sondern beeinflusst auch ihre Verwaltungs- und Kommunikationsprozesse. Der Aufbau variiert stark je nach Branche und Funktion.

Die Fachhochschule St. Pölten ist als Bildungseinrichtung mehrstufig gegliedert: An der Spitze steht die Hochschulleitung, welche durch das Kollegium, die Geschäftsführung und verschiedene zentrale Dienste unterstützt wird. Das Zusammenspiel zwischen Lehre, Forschung und zentraler IT ist besonders wichtig. (vgl. [22])

Das Österreichische Rote Kreuz zeigt einen stark differenzierten Aufbau, der sowohl soziale, medizinische als auch organisatorische Bereiche abdeckt. Hier liegt der Fokus auf operativer Hilfeleistung, humanitärer Unterstützung und internationalen Beziehungen. (vgl. [41])

Werbung Tirol wiederum ist stark projekt- und markenorientiert strukturiert. Die Organisation gliedert sich in funktionale Bereiche rund um Kommunikation, Forschung, Nachhaltigkeit und Marketing. (vgl. [42])

Die SCHIG GmbH ist als bundeseigene Infrastrukturgesellschaft eng mit dem Verkehrsministerium verbunden. Ihr Aufbau fokussiert sich auf technische, juristische und förderungsrelevante Aufgaben sowie Qualitätsmanagement und Aufsicht über Bahnprojekte. (vgl. [43])

Die folgende Tabelle vergleicht die vier Institutionen hinsichtlich Aufbaus, Stakeholder-Fokus und schützenswerter Assets:

Tabelle 5.1.: Vergleich ausgewählter Organisationen

Organisation	**Hauptstakeholder**	**Fokus**	**Schützenswerte Assets**
FH St. Pölten	Studierende, Forschende, Lehrende, Wirtschaft	Bildung & Forschung	Forschungsdaten, Prüfungsunterlagen, Studien- und Personaldaten, IT-Infrastruktur
Österreichisches Rotes Kreuz	Hilfsbedürftige, Ehrenamtliche, Spender, Bevölkerung	Soziale & medizinische Hilfe	Gesundheits- und Einsatzdaten, Spenderverzeichnisse, Kommunikationsnetzwerke, Logistik
Werbung Tirol	Tourismusbranche, Gäste, Medien	Tourismusförderung & Standortmarketing	Marketingstrategien, Markendaten, Projektdaten, Zielgruppenanalysen, Partnernetzwerke
SCHIG GmbH	BMK, Bahnunternehmen, Fahrgäste	Bahn- und Infrastrukturmanagement	Vertrags- und Förderdaten, technische Dokumentation, Qualitätsberichte, Revisionsdaten

Obgleich sich die Ziele der FH St. Pölten, des österreichischen Roten Kreuzes, Werbung Tirols sowie der SCHIG GmbH unterscheiden, weisen alle Einrichtungen bestimmte strukturelle Gemeinsamkeiten auf. Alle Organisationen sind mehrstufig aufgebaut, arbeiten in spezialisierten Abteilungen und bedienen unterschiedliche Stakeholder-Gruppen. Darüber hinaus verarbeiten sie sensible Daten, weshalb Informationssicherheit in jedem Teil einen zentralen Stellenwert hat. Unterschiede ergeben sich vor allem aus dem jeweiligen Zweck – Bildung, humanitäre Hilfe, Standortmarketing oder Infrastrukturmanagement.

Bezüglich der im Kapitel 2 angesprochenen regulatorischen Herausforderungen ist zu erwähnen, dass in anderen Bereichen weitere Gesetzesanforderungen herrschen. Beispiele hierfür wären das Netz- und Informationssicherheitsgesetz(NISG), die Digital Operational Resilience Act(DORA) und Cybersecurity Act. Um keine falschen Annahmen zu treffen, wurde keine Zuweisung dieser Regulatorien an den Beispielunternehmen vorgenommen.

5.2. Security Awareness Konzept

Im Rahmen dieser Arbeit wird die theoretische Ausarbeitung von Maßnahmen zur Förderung der Informationssicherheitsawareness im Hochschulkontext in Österreich betrachtet. Ausgangspunkt für diese Betrachtung ist die Erkenntnis, dass Security Awareness nicht nur als einmalige Maßnahme, sondern als kontinuierlicher Prozess zu verstehen ist, der wesentlich zur Stärkung der gesamten Informationssicherheit beiträgt. Die Motivation zur Implementierung entsprechender Programme kann dabei vielfältig und nicht immer klar sein: Neben der allgemeinen Erhöhung des Sicherheitsniveaus innerhalb der Organisation zählen unter anderem neue gesetzliche oder regulatorische Vorgaben, der Wunsch nach einer positiven Außendarstellung oder strategische Unternehmensziele zu den initialen Auslösern, auch wenn deren Zusammenhang nicht immer durchschaubar ist. (vgl. [27])

Ein kontinuierlicher Handlungsbedarf ergibt sich insbesondere durch die hohe personelle Fluktuation, wie sie typischerweise in Hochschulen zu beobachten ist. Neue Mitarbeitende und Studierende bringen unterschiedliche Erfahrungsstände und Vorkenntnisse mit, wodurch eine einheitliche Sensibilisierung notwendig wird. Zudem ändern sich gesetzliche Rahmenbedingungen, interne Richtlinien und nicht zuletzt auch die Bedrohungslage im Bereich der Informationssicherheit laufend, was eine Anpassung und Weiterentwicklung bestehender Awareness-Programme erforderlich macht. (vgl. [27])

Die europäische Agentur für Cybersicherheit (ENISA) unterteilt Awareness-Programme in drei Hauptprozesse: „Plan, assess and design“, „Execute and manage“ sowie „Evaluate and adjust“. Der Fokus dieser Arbeit liegt bewusst auf ausgewählten Bausteinen des ersten Prozessbereichs „Plan, assess and design“. Die Gründe für diese Einschränkung liegen in der Zielsetzung der Arbeit, die sich auf konzeptionelle Aspekte der Awareness-Planung konzentriert. Die tatsächliche Durchführung von Maßnahmen sowie deren Evaluierung und kontinuierliche Verbesserung werden explizit nicht behandelt. (vgl. [27])

Es erfolgt eine detaillierte Betrachtung der einzelnen Arbeitsschritte innerhalb des ersten ENISA-Prozesses. Zur besseren Orientierung wird eine grafische Darstellung verwendet, in der jene Tätigkeiten, die im Rahmen dieser Arbeit umfassend behandelt werden, blau markiert sind. Grau hinterlegte Schritte werden teilweise thematisiert, während nicht markierte Aktivitäten aufgrund ihrer unternehmensindividuellen Ausprägung oder fehlender Relevanz für die Zielsetzung der Arbeit ausgeschlossen werden. (vgl. [27])

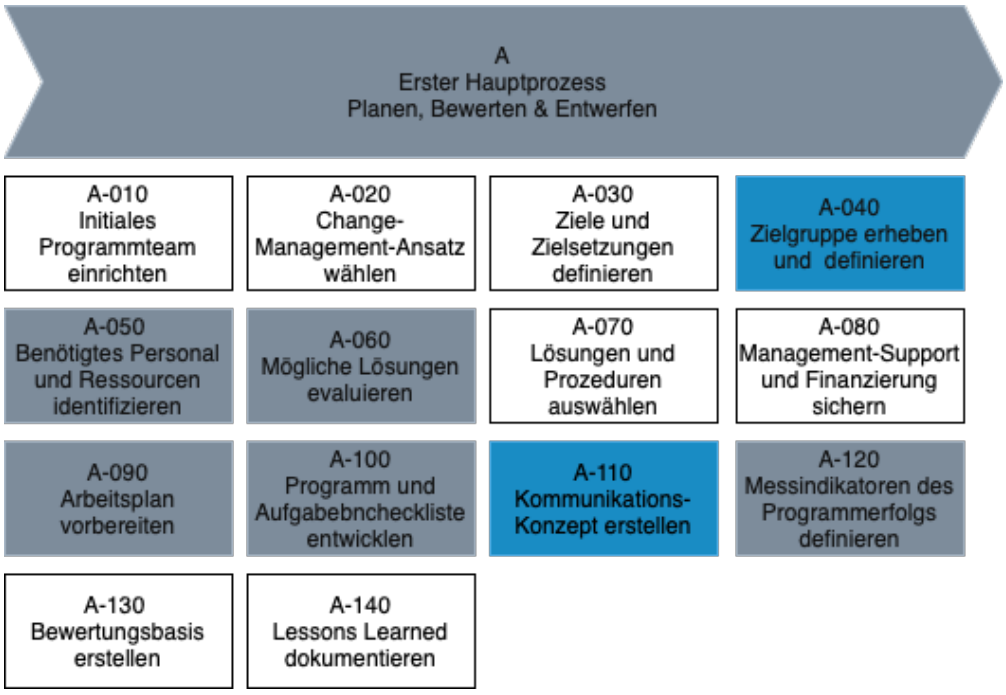

Abbildung 5.1.: ENISA - erster Hauptprozess [27]

- **Ausschluss: A010 – Initiales Programmteam einrichten**: Die Bildung eines Programmteams ist organisationsspezifisch und unterliegt individuellen Gegebenheiten, weshalb eine detaillierte Betrachtung im Rahmen dieser Arbeit nicht zielführend erscheint. Zudem kann externe Unterstützung bei Bedarf unternehmensseitig eingebunden werden.
- **Ausschluss: A020 – Change-Management-Ansatz wählen**: Da Kommunikations- und Veränderungsprozesse stark organisationsabhängig sind, erfolgt in dieser Arbeit keine vertiefte Analyse. Die, im Rahmen dieser Arbeit, durchgeführte Umfrage zeigt zudem, dass ein Großteil der Hochschulen bereits Awareness-Maßnahmen umsetzt.
- **Ausschluss: A030 – Ziele und Zielsetzungen definieren**: Zieldefinitionen variieren stark zwischen Organisationen, ebenso wie die zugrunde liegende Budgetierung und Motivation. Daher erfolgt in dieser Arbeit lediglich eine allgemeine Kontextualisierung möglicher Beweggründe.

- **Bearbeitung: A040 – Zielgruppen erheben und definieren**: Aufgrund der strukturellen Ähnlichkeiten von Hochschulen wird die Zielgruppendefinition umfassend behandelt. Analysiert werden bestehendes Sicherheitsbewusstsein, gewünschtes beziehungsweise. unerwünschtes Verhalten sowie spezifische Bedürfnisse der Zielgruppen.
- **Teilweise Bearbeitung: A050 – Benötigtes Personal und Ressourcen identifizieren**: Personelle Ressourcen werden nicht detailliert betrachtet, da diese stark organisationsspezifisch sind. Es erfolgt jedoch eine theoretische Auseinandersetzung mit den benötigten Ressourcen gemäß ENISA-Empfehlungen.
- **Teilweise Bearbeitung: A060 – Mögliche Lösungen evaluieren**: Die Bewertung potenzieller Lösungsansätze erfolgt exemplarisch durch die Gegenüberstellung von Outsourcing- und Inhouse-Modellen.
- **Ausschluss: A070 – Lösungen und Prozeduren auswählen**: Da sich dieser Teil bereits teilweise mit der Umsetzung der in A50 und A60 beschriebenen Modellen auseinandersetzt, wurde dieser aus dem Scope der Arbeit entfernt.
- **Ausschluss: A080 – Management-Support und Finanzierung sichern**: Die Umfrageergebnisse deuten darauf hin, dass Awareness-Maßnahmen bereits etabliert sind. Eine gesonderte Betrachtung von Managementeinbindung und Budgetierung wird daher nicht vorgenommen.
- **Teilweise Bearbeitung: A090 – Arbeitsplan vorbereiten**: Ein vollständiger Arbeitsplan ist aufgrund des eingeschränkten Betrachtungsumfangs nicht möglich. Eine exemplarische Zeitplanung wird auf Basis der gewonnenen Erkenntnisse vorgeschlagen.
- **Teilweise Bearbeitung: A100 – Programm und Aufgabencheckliste entwickeln**: Es erfolgt eine exemplarische Auflistung potenzieller Aufgaben, jedoch keine vollständige Checkliste aufgrund der Nichtberücksichtigung aller Prozessschritte.
- **Bearbeitung: A110 – Kommunikationskonzept erstellen**: Ein grundlegendes Kommunikationskonzept mit beispielhaften Kanälen, Themen und Medien wird ausgearbeitet. Die Ausgestaltung erfolgt in Bezug auf in Kapitel 2 erläuterte Kommunikationsarten und Lerntypen.
- **Teilweise Bearbeitung: A120 – Messindikatoren des Programmerfolgs definieren**: Theoretische Erfolgsindikatoren werden vorgestellt, jedoch nicht empirisch überprüft.
- **Ausschluss: A130 – Bewertungsbasis erstellen**: Da nicht alle Bereiche vollumfänglich behandelt wurden, wurde dieser Punkt ausgelassen.
- **Ausschluss: A140 – Lessons Learned dokumentieren**: Da keine tatsächliche Umsetzung stattfindet, ist die Reflexion praktischer Erkenntnisse im Sinne von „Lessons Learned“ nicht Bestandteil dieser Arbeit.

Anhand der Auflistung ist auch der Hauptfokus dieser Arbeit, welcher sich auf die Zielgruppen, Themen und Medien des Awareness Programmes fokussiert, ersichtlich.

5.2.1. Zielgruppen

ENISA gibt an, dass es essenziell ist seine Zielgruppe zu kennen, und stellt mögliche Fragestellungen, welche bei der Erhebung nützlich sein können. So sollte zuerst überlegt werden, wen das Programm erreichen sollte und ob alle Lernenden dieselben informationellen Bedürfnisse pflegen. Weiters sollte Rücksicht auf die verschiedenen Wissensstände der Betroffenen gelegt werden. Wie bereits in den theoretischen Hintergründen erläutert, sollte auch auf die Lernbedürfnisse beziehungsweise Kommunikationsmodelle nicht vergessen werden. Es wird empfohlen, die allgemeine Stimmung gegenüber des Themas Informationssicherheit zu beobachten. Beispielsweise ob die Thematik ernst genommen wird oder nicht. [27]

Laut ISO sollten Awareness Maßnahmen an die Rollen und Verantwortlichkeiten des Personals angepasst werden. Dies betrifft sowohl internes als auch externes Personal (externe Berater, Lieferanten, ...). (vgl. [30])

Zielgruppenerhebung und -analyse

Nachstehende Zielgruppen wurden im Kontext von Hochschulen erhoben. Es ist zu beachten, dass diese Aufzählung nicht endgültig ist, und individuell bearbeitet beziehungsweise ergänzt werden sollte.

- Mitarbeitende der Fachhochschule St. Pölten (dazu zählen Hauptberufliche und Nebenberufliche, sowie Forschende)
  - Angestellte
  - Führungspositionen (Geschäftsführung, Abteilungsleiter, Departmentleiter, Fakultätsleiter, Rektorrat)
  - IT-Fachkräfte/Informationssicherheits Fachkräfte
- Third Party
  - Facility Management, Mensa Mitarbeitende
- Studierende

Laut NIST 800-16 erfolgt die Einteilung der Zielgruppen in die Kategorien Geschäftsführung, Programm- und Funktionsmanager, IRM & Security Audit, ADP-Management & Operations und Endbenutzer. Ein Mapping zwischen den erhobenen Zielgruppen und den vorgeschlagenen des NIST Leitfadens könnte wie folgt aussehen (vgl. [29]):

NIST 800-16	**Erhobene Zielgruppen**
Geschäftsführung	Führungspositionen (Geschäftsführung)
Programm und Funktionsmanager	Führungspositionen (Abteilungsleiter / Department Leiter / Fakultätsleiter / Rektorat)
IRM & Security Audit	Informationssicherheits Fachkräfte
ADP Management und Operations	IT-Fachkräfte
Endbenutzer	Angestellte, Studierende

Tabelle 5.3.: Zuordnung der NIST 800-16 Rollen zu den erhobenen Zielgruppen

Bei Betrachtung dieses Vergleichs fällt auf, dass ein eindeutiges Mapping nicht gänzlich möglich ist, und auch nicht alle Zielgruppen vollumfänglich behandelt werden.

Aufgrund dessen erfolgt eine Analyse basierend der Empfehlungen seitens ENISA. Vorschläge, welche in den NIST Publikationen vorhanden sind, werden bei Bedarf angenommen.

Für die genaue Analyse wurde pro Zielgruppe die Vorlage zur Erhebung jener von ENISA verwendet. Dabei wurden die Aspekte Zielgruppe, Definition, Kategorie, benötigtes Wissen, voraussichtliches Wissen und Motivation für Awareness behandelt.

Die tabellarische Auflistung ist dem Anhang A entnehmen. Zusammengefasst wurden folgende Erkenntnisse über die Zielgruppen gewonnen:
(Nicht technische) Angestellte gelten als Mitarbeitende aus allen Abteilungen, welche keinen technischen Fokus in ihren Arbeitstätigkeiten haben. Aufgrund dessen kann ein technisches Vorwissen nicht vorausgesetzt werden, jedoch sind grundlegende Kenntnisse bezüglich Informationssicherheit für den Arbeitsalltag erforderlich. Ziel ist es, diese Zielgruppe bezüglich allgemeiner Themen im Bereich der Informationssicherheit zu sensibilisieren, damit die Mitarbeitenden im Berufs- sowie Privatleben davon profitieren können.

Als Führungspersonal werden Personen in Leitungsfunktionen, wie beispielsweise die Geschäftsführung, Abteilungs- oder Fakultätsleitungen beschrieben. Auch hier ist technisches Wissen nicht vorauszusetzen. Neben Informationssicherheitsgrundsätzen ist auch ein Verständnis bezüglich Auswirkungen von Bedrohungen auf Geschäftstätigkeiten von Nöten. Durch eine angemessene Sensibilisierung sollten Führungskräfte durch ihr Verhalten eine Vorbildfunktion einnehmen.

IT- und Informationssicherheits-Fachkräfte sind technisches Personal innerhalb der Hochschule. Bei dieser Gruppe kann technisches Wissen vorausgesetzt werden. Neben allgemeinen Sicherheitsgrundlagen sollten in diesen Bereichen auch tiefergehende Kenntnisse zu technischen Sicherheitsmaßnahmen geschult werden. Der Bedarf an Sensibilisierung richtet sich hierbei an die Garantie eines sicheren IT-Betriebes.

Externe Dienstleister, wie zum Beispiel Facility Management oder Mensa-Mitarbeitende gelten als Third-Party-Akteure, welche regelmäßigen physischen Zugang zur Hochschule haben. Technisches Wissen kann hier ebenso nicht vorausgesetzt werden. Im Fokus der Sensibilisierung steht die physische Sicherheit. Ziel ist es somit beispielsweise eine Bedrohung durch unbefugte Zutritte zu vermeiden.

Als letzte Zielgruppe wurden Studierende und Alumni erhoben. Diese sind eine Nutzergruppe, welche potenziell über Zugang zu bestimmten IT-Systemen beziehungsweise Applikationen der Hochschule verfügen, und darüber hinaus auch physischen Zutritt zu den Einrichtungen haben. Technisches Wissen ist nicht flächendeckend vorhanden, jedoch bei einigen anzunehmen. Awareness dient der Vorbereitung auf den Berufsalltag und der Vorbildfunktion der Wissenschaft für die Gesellschaft.

Durch die, im Zuge dieser Arbeit, durchgeführte Umfrage konnte identifiziert werden, dass bei vielen der Hochschulen hauptsächlich hauptberufliche Mitarbeitende und Forschende an Awareness Tätigkeiten teilnehmen. Aus diesem Grund wird empfohlen mit jenen Zielgruppen zu beginnen, und bei Bedarf an weitere Gruppierungen auszuweiten.

Zielgruppenverständnis

Um ein besseres Verständnis für die Bedürfnisse und das bestehende Interesse gegenüber des Themas Informationssicherheit zu erlangen, erfolgte die Durchführung einer Umfrage gerichtet an die Mitarbeitenden der Fachhochschule St. Pölten. Diese gliedert sich in die Abschnitte Verständnis IT-Security, Interesse für neue Technologien, Informationssicherheit, Weiterbildung, Schulung für IT-Sicherheit, Informationen zu IT-Sicherheit und weiteren Anregungen. Die Erstellung der Umfrage erfolgte unter Absprache der Sicherheitsverantwortlichen und Experten der Fachhochschule St. Pölten. Bei der Fragenauswahl wurden im Arbeitsalltag gängige Technologien und Werkzeuge berücksichtigt. Die Umfrage kann dem Anhang F entnommen werden. Genaue Ergebnisse sind im Kapitel 6 ersichtlich.

Herausforderungen und Lösungsansätze

Im Zuge der Analyse wurden zentrale Herausforderungen im Kontext der Zielgruppen für Informationssicherheitssensibilisierung identifiziert. Die adressierten Zielgruppen unterscheiden sich in Bezug auf Fachdisziplin, Sprachen, Altersstruktur, Unternehmensposition sowie kulturellen Hintergrund. Diese Diversität erschwert die einheitliche Vermittlung sicherheitsrelevanter Themen. Darüber hinaus besteht vor allem bei fachfremden Personen oftmals ein geringes Grundverständnis für IT-Sicherheitsprinzipien, was durch eine allgemeine Zurückhaltung oder Gleichgültigkeit gegenüber dem Bereich Informationssicherheit verstärkt wird.

Zur Bewältigung dieser Herausforderungen ist ein zielgruppenspezifischer Schulungsansatz erforderlich. Die Aufbereitung der Schulungsinhalte soll didaktisch so erfolgen, dass verschiedene Verständnisniveaus erreicht werden können. Dies umfasst besonders die Verringerung der technischen Fachsprache zugunsten einer mehrdeutigen Terminologie. Die Orientierung an dem sogenannten Need-to-Know-Prinzip gewährleistet darüber hinaus, dass nur für die Zielgruppe relevanten Inhalte, welche im Arbeitsalltag Verwendung finden, vermittelt werden. Außerdem ist eine sprachliche Anpassung des Schulungsmaterials auf Deutsch und Englisch notwendig, damit potentielle Sprachbarrieren vermieden werden.

Ein weiterer zentraler Aspekt ist die Etablierung eines persönlichen Bezugs zur Thematik. Ziel ist es, das Bewusstsein für Informationssicherheit nicht nur auf organisatorischer, sondern auch auf individueller Ebene zu fördern. Durch praxisnahe Beispiele – etwa im Hinblick auf Sicherheitsrisiken im privaten Umfeld – soll verdeutlicht werden, inwiefern jede einzelne Person einen aktiven Beitrag zur Stärkung der Cybersicherheit leisten kann.

Im Zuge der Umfrage an Mitarbeitenden der FH-St.Pölten konnte festgestellt werden, dass teilweise Wissen und Interesse im Bereich der Informationssicherheit vorhanden ist. Die genaue Analyse und Bewertung ist dem Kapitel 6 dieser Arbeit zu entnehmen.

5.2.2. Identifizierung von Personal und Ressourcen

Laut ENISA sollte in erster Linie geschaut werden, welche Ressourcen bereits zur Verfügung stehen. Vorgeschlagen werden Personaleinsätze der Abteilungen IT, HR, Kommunikation, Marketing sowie Training und Entwicklung. (vgl. [27])

Im Kontext einer Hochschule stehen ähnliche Abteilungen zur Verfügung, wie eine bereits durchgeführte Recherche gezeigt hat. Am Beispiel der FH St.Pölten würde auch das Kompetenzzentrum für Lehr-Lernentwicklung und Bildungsangebote (LEARN) für diese Aufgabe zur Verfügung stehen. Dieses fördert eine kontinuierliche Entwicklung der Lehre an dieser Einrichtung. Somit könnte ebenso darüber nachgedacht werden, Awareness-Trainings über diese Plattform anzubieten. (vgl. [44])

5.2.3. Evaluierung möglicher Lösungen

Dieser Arbeitsschritt befasst sich mit der Awareness Strategie des Unternehmens. Unter anderem stellt sich hier die Frage, ob die Durchführung der Tätigkeiten von internem Personal ausgeführt wird, oder ausgelagert werden soll. Outsourcing als Strategie hat sich im Laufe der Zeit immer weiter durchgesetzt. (vgl. [27])
Im Kontext einer Hochschule sollten Überlegungen angestellt werden, ob genügend personelle Ressourcen zur Verfügung stehen würden, welche ebenso über das benötigte Know-How verfügen. Sollte beispielsweise eine Abteilung oder ein Team vorhanden sein, welches sich speziell mit dem Thema Informationssicherheit beschäftigt, ist es denkbar, die Awareness Tätigkeiten vollständig intern handzuhaben. Im Falle eines personellen Ressourcen-Mangels könnte die Wahl eher auf eine externe Auslagerung fallen. Hierbei sollte jedoch beachtet werden, dass bereitgestellte Materialien an die Bedürfnisse der Hochschulen angepasst werden sollten. Von der Verwendung eines generischen „fertigen“ Trainings wird abgeraten. (vgl. [27])

5.2.4. Vorbereitung eines Arbeitsplans

Nachdem entschieden wurde, ob und welche Teile des Programms intern und welche extern ausgeführt werden, erfolgt die Erstellung eines Arbeitsplanes. Im Zuge dieser Arbeit wurde nur beispielhaft ein Plan erarbeitet. Dieser Plan ist in Anlehnung der seitens ENISA bereitgestellten Timeline erstellt worden.

Die Umsetzung erfolgt in vier Phasen. Diese gliedern sich in die Abschnitte Unterschwellig, Aktiv, Interaktiv, Alltäglich.

Ausrollung in 4 Phasen			
Unterschwellig	**Aktiv**	**Interaktiv**	**Alltäglich**
Gedruckte/Visuelle Information: Informationen in Newsletter, Emails, Poster, Flyer	**Dialog:** Verbale Informationen, Meetings und Workshops	**Interaktionen:** Fokusgruppen, Virtuelle Communities zum Austausch, Reviews	**Einsatz im Arbeitsalltag:** Identifizierung des Einzelnen mit dem Thema Awareness und aktives Feedback geben

Abbildung 5.2.: Phasen der Ausrollung

In der ersten Phase werden gedruckte oder visuelle Informationen bereitgestellt. Danach werden im aktiven Schritt verbal Informationen ausgetauscht. Dies könnte beispielsweise in Form von Meetings und Workshops geschehen. In der interaktiven Phase erfolgt ein Austausch in Fokusgruppen oder virtuellen Gemeinschaften. Diese dienen zum Austausch und möglichen Reviews. In der letzten Phase soll Awareness im Arbeitsalltag integriert werden. Dies bedeutet, dass sich jeder einzelne aktiv mit der Thematik identifiziert und anderen aktives Feedback bereitstellen kann. (vgl. [27])

Die Durchführung dieser Schritte ist ein kontinuierlicher Prozess und erstreckt sich über mehrere Durchgänge.

Ein möglicher Arbeitsplan könnte mit einer Vorbereitungsphase von ein bis zwei Monaten beginnen. Hierbei werden erneut genaue Ziele, Themen und Inhalte identifiziert. Weiters erfolgt die Analyse, beziehungsweise die Überarbeitung, der erhobenen Zielgruppen. Ein weiterer Aspekt ist die Bestimmung eines Durchführungsintervalls. Laut ISO sollten regelmäßig Awareness Trainings stattfinden. Darüber hinaus ebenso bei Neueinstellung (Onboarding) und bei Wechsel der Rollen beziehungsweise des Verantwortungsbereichs. Beim Eintritt in das Unternehmen ist zu erwähnen, dass es sich hierbei um die „ersten Berührungspunkte“ beziehungsweise die Grundkenntnisse in diesem Bereich handelt. (vgl. [30])

Die tatsächliche Durchführung erstreckt sich beispielsweise über drei Monate, in welchen sich auf drei bestimmte Themen fokussiert wird. Die Umsetzung erfolgt nach der Reihe, beispielsweise im monatlichen Zyklus.

Am Ende der Durchführung erfolgt die Auswertung. In dieser werden Ergebnisse analysiert, Inhalte evaluiert und überarbeitet, Lessons Learned zur weiteren Überarbeitung erhoben, Feedback eingeholt und schlussendlich ein Bericht erstellt.

Nach der Sammlung der erforderlichen Daten erfolgt die Überarbeitungsphase, in welcher die Reflexion umgesetzt wird. Nachdem alle Anpassungen vorgenommen wurden, erfolgt die erneute Ausführung der Awareness Tätigkeiten.

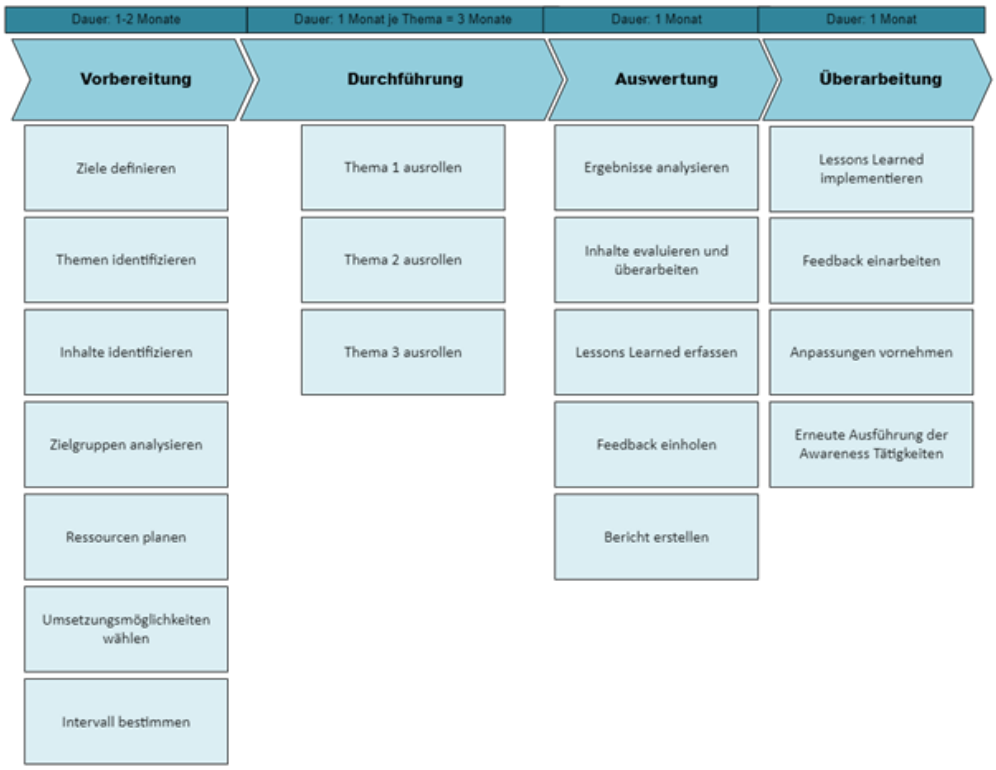

Abbildung 5.3.: Zeitplan

5.2.5. Entwicklung des Programms und Aufgabencheckliste

ENISA beschreibt, dass eine gute Organisation eines Awareness Programms von hoher Relevanz ist. Somit ist es beispielsweise von Vorteil, bei einer längeren Auswahl von Themen eine Priorisierung vorzunehmen. Somit können diese Bereiche über einen längeren Zeitraum, passend der Relevanz, behandelt werden. Dies fördert ebenso den Fokus auf die bestimmten Themengebiete und erlaubt die Rücksichtnahme auf die einzelnen Zielgruppen, ohne diese mit Informationen zu überfluten, oder zu verwirren. (vgl. [27])

Im Zuge dieser Arbeit wurde eine Liste (Anhang G) samt Beschreibung erstellt, welche individuell nach der Relevanz bewertet werden kann. Diese Liste umfasst unter anderem E-Mail und elektronische Kommunikation, physische Sicherheit beziehungsweise Gebäudezutritt und Passwortsicherheit. Die Auswahl der Themen erfolgte durch die von ENISA und NIST vorgeschlagenen Themen, sowie Überschneidungen zu ISO/IEC 27002.

Die Bewertung erfolgt in einem drei gradigen Schema, wie auch von ENISA empfohlen. Hier werden die Bewertungsgrade als **3 = Crucial**, **2 = important** und **1 = nice to have** beschrieben. (vgl. [27]) Die Betitelungen im Zuge dieser Ausarbeitung lauten „wichtig“, „gut, aber nicht (sofort) notwendig“ und "nicht wichtig".

5.2.6. Erstellung des Kommunikationskonzepts und Auswahl der Medien

ENISA beschreibt Kommunikation als wesentlichen Erfolgsfaktor von Awareness. Diese soll Akzeptanz und Commitment erreichen. Dieser Prozess der Lernenden wird als Kurve beschrieben, in welcher zunächst ein erster Kontakt geschaffen wird. Dieser geht über in Bewusstsein, Verständnis, Engagement, Akzeptanz, Commitment und schließlich Verinnerlichung. Es sollten die Prinzipien der W-Fragen angewandt werden. Das bedeutet:

- Was wird von den Empfangenden erwartet?
- Warum sollten die Empfangenden am Awareness Programm teilnehmen und was wären ihre Vorteile?
- Wann sollten die Empfangenden das Geforderte umsetzen?
- Wie stehen die Handlungen im Zusammenhang mit den Rollen und Verantwortlichkeiten im Unternehmen oder im privaten Leben?
- Wer unterstützt das Programm?
- Wen soll man für weitere Informationen kontaktieren?

(vgl. [27])

Auswahl von Themen

Eine Auswahl möglicher Themen wurde zuvor behandelt. Weiters ist es essenziell diese auch mit den Zielgruppen zu verknüpfen, da nicht alle Zielgruppen über denselben Informationsbedarf verfügen. Eine Einteilung könnte erfolgen in „Grundlagen der Informationssicherheit“, „technische Spezialisierungen“ und „rechtlich Relevant (Beispielsweise Datenschutz)“. Die beiden letzteren Spezifikationen umfassen ebenso die Grundlagen der Informationssicherheit.

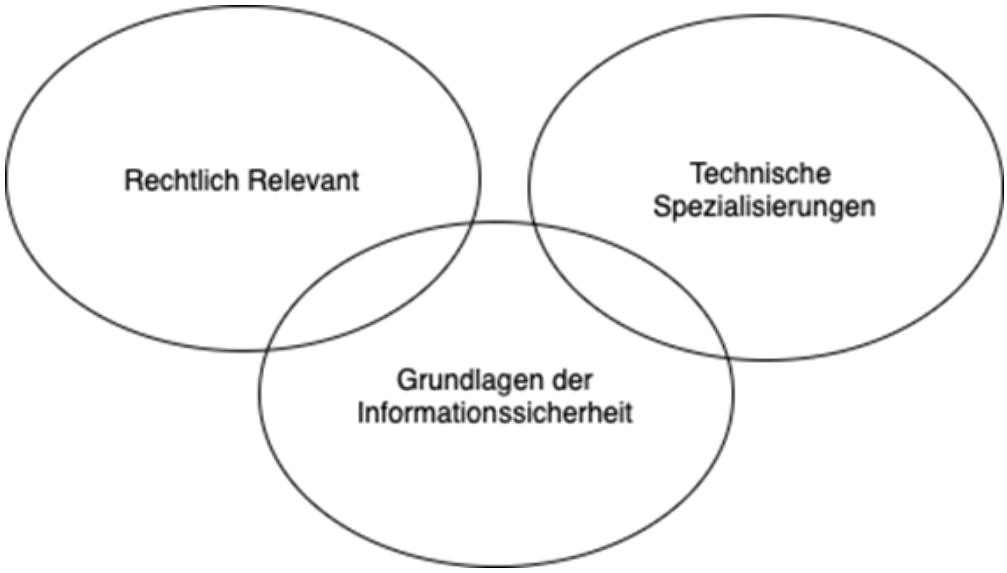

Abbildung 5.4.: Auswahl von Themen

Sollte eine genauere Zuweisung gewünscht sein, kann jede Zielgruppe auch speziell einzelnen Themengebieten zugewiesen werden.

Auswahl von Medien

Nachdem die passenden Themen zu den entsprechenden Zielgruppen erhoben wurden, ist es laut ENISA wichtig den richtigen Kommunikationskanal zu wählen, über welchen die Informationen vermittelt werden. (vgl. [27])

ISO schlägt die Nutzung von Kampagnen, Booklets, Postern, Newsletter, Websiten, Information Sessions, Briefings, E-Learnings und E-Mails vor. (vgl. [30])

Seitens ENISA werden Broschüren oder Magazine, Comics, Distance Learning(Computer Based Training oder Online Training), Education(Education pack, Lehrmaterial), E-Mail, Events(Messen, Meetings, Seminare oder Conferenzen), Leaflets oder Factsheets, E-Newsletter, Zeitungen, Handys, Poster, Radio, Screensaver, SMS, Training, TV, Video (DVD, CD) und Websites vorgeschlagen. Die bereitgestellte Studie im ENISA Guide „How to raise information security awareness“ zeigt, dass oft Richtlinien, Intranetseiten, ein Mitarbeiter Handbuch oder Trainings zur Steigerung eingesetzt werden. (vgl. [27])

Wie die durchgeführte Umfrage an Hochschulen zeigt, ist der Einsatz von E-Learnings, Online-/ und Präsenz Workshops am weitesten verbreitet. Dies überschneidet sich ebenso mit den Angaben der Probanden der Umfrage des IT-Verständnisses der Mitarbeitenden an der Fachhochschule St. Pölten. Hierbei gab die Mehrheit an Präsenz Vorträge/Workshops, Online Vorträge/Workshops, E-Learnings und Blogbeiträge als Medium der Wissensvermittlung zu bevorzugen.

Um die meisten Lerntypen laut Schrader, welche in den theoretischen Hintergründen (2) erläutert wurden anzusprechen, wäre die Wahl von Broschüren, E-Mails, Fragebögen, Handzettel, Orientierungsveranstaltungen oder Sonderveranstaltungen empfehlenswert.

Bei den Lerntypen laut Vester ist ein Mapping auf alle Zielgruppen möglich. Hierbei ergeben sich interaktive Lernprogramme, Schulungsveranstaltungen, Sonderveranstaltungen oder Tabletop als die für alle Typen Passendsten Medien.

Für die Auswertung nach den Lerntypen wurden die Medien, welche im Buch [23] beschrieben werden, herangezogen. Hinterlegt sind die Ergebnisse in den Anhängen C und D.

Vernünftig wäre auch die Wahl bereits vorhandener Medien wie beispielsweise einer Intranet Seite, E-Mail Newsletter oder Schulplattformen (Beispiel Moodle).

Wie auch bei den Zielgruppen ist es möglich auf Problematiken zu treffen. In diesem Themengebiet wurde der eventuelle Widerstand bei der Änderung der Arbeitsweise, ein fehlendes Verständnis für die Thematik und wahllos ausgewählte Schulungsbeispiele ohne passenden Kontext identifiziert. Um diesen Herausforderungen entgegenzuwirken könnte direkte Kommunikation mit den Mitarbeitenden geführt werden, um herauszufinden, warum bestimmte Maßnahmen entgegen ihrer Arbeitsweise fungieren. Weiters ist Empathie und Verständnis ein wichtiger Faktor: Veränderungen können mühsam sein und müssen daher langsam behandelt werden. Ein weiterer hilfreicher Aspekt kann eine Bewusstseinsschaffung im Kontext der Informationssicherheit im privaten Umfeld spielen. Letztlich könnten Schulungsbeispiele an momentane zeitliche Gegebenheiten angepasst werden. So könnte es sich beispielsweise um einen Konnex zur Pandemie handeln oder Unwettern.

Zeitlicher Kontext

Im Sinne des zeitlichen Kontextes - also wann Awareness Tätigkeiten ausgeführt werden könnte die Wahl saisonbedingt gestaltet werden. (vgl. [23]) Im Sinne einer Hochschule wären die Zeiträume Winter- und Sommersemester andenkbar. So könnten beispielsweise auch neu eintreffende Studierende geschult werden. Weiters ist die Wahl von Urlaubszeiten, wie zum Beispiel die Sommermonate, vermutlich unpassender, da die Informationen nicht alle Zielgruppen erreichen.
Eine Einbindung in den Onboarding Prozess ist ebenso eine valide Überlegung. Jedoch sollte darauf geachtet werden neue Mitarbeitende nicht zu überfluten.
Zusätzlich können Impulsvorträge oder Workshops themenbasiert angeboten werden. Eine Informationsvermittlung via Intranet Beiträge wäre seitens Mitarbeitenden der FH St.Pölten ebenso monatlich wünschenswert.

5.2.7. Definition von Messindikatoren

Die Effektivität und das Verbesserungspotential von Awareness Tätigkeiten kann und sollte gemessen werden (vgl. [27]). Wie auch die Umfrage an Hochschulen zeigte, würde die Messung und Auswertung von Erfolgen als sinnvoll erachtet werden. ENISA empfiehlt zur Unterstützung der Erhebung von Messwerten die Verwendung von bewährten Standards wie beispielsweise der Balanced Scorecard oder Six Sigma. (vgl. [27]) Als mögliche Indikatoren könnten zum Beispiel eine Prozentzahl des benötigten Budgets oder Zeit, Mitarbeitendenzufriedenheit im Zuge des Awareness Trainings, Anzahl von bestandenen Tests oder Anzahl von gemeldeter Vorfälle dienen. (vgl. [27]) Weiters sollte berücksichtigt werden, dass diese Messindikatoren ebenfalls an die Zielgruppen angepasst werden müssen, da diese über bestimmte Interessen, Situationen oder Bedürfnisse verfügen. (vgl. [27])

6. Ergebnisse

Dieses Kapitel dient der Auswertung, der beiden durchgeführten Umfragen. Weiters werden anhand dieser Ergebnisse und der weiteren, im Zuge dieser Arbeit getätigten Analysearbeiten, die in der Einleitung gestellten Forschungsfragen beantwortet.

6.1. Umfrage IST-Stand Informationssicherheit an Hochschulen in Österreich

Um den IST-Zustand der Informationssicherheit an Hochschuleinrichtungen in Österreich abzufragen, wurde eine Erhebung durchgeführt. Insgesamt wurden 34 akademische Einrichtungen zur Teilnahme aufgefordert. Die Anzahl der Mitwirkenden erschließt sich auf 12 Probanden, was eine Beantwortungsrate von 35,29% ergibt. Die Vorlage der Umfrage befindet sich in Anhang E.

6.1.1. Allgemein

Im ersten Abschnitt der Umfrage wurde ein grundlegender Überblick über den Stellenwert der Informationssicherheit an den befragten Hochschulen erhoben. Ziel war es, den allgemeinen Umgang mit dem Thema sowie den Reifegrad der bestehenden Sicherheitsmaßnahmen zu erfassen.

Auf die Eingangsfrage - Beschäftigt sich Ihre Einrichtung mit dem Thema Informationssicherheit? - antworteten alle Teilnehmenden mit Ja (n = 12). Dieses einstimmige Ergebnis legt zwar nahe, dass Informationssicherheit in allen befragten Einrichtungen thematisiert wird und somit als relevantes Handlungsfeld anerkannt ist.

Vertiefend wurde in der zweiten Frage erhoben, wie ausgeprägt diese Auseinandersetzung ist, wobei die Ergebnisse ein vielschichtiges Bild zeichneten: Zwei Einrichtungen gaben an, dass lediglich Maßnahmen für Teilbereiche vorhanden seien, etwa in Form von Passwortrichtlinien. Der Großteil der Teilnehmenden (n = 7) berichtete von einem umfassenderen Ansatz, beispielsweise durch den strukturierten Aufbau eines Informationssicherheitsmanagementsystems (ISMS), was allerdings die Frage aufwirft, wie diese Systeme in der Praxis tatsächlich gelebt werden. Zwei weitere Einrichtungen gaben an, dass ein ISMS nicht nur implementiert sei, sondern aktiv gelebt und regelmäßig geprüft werde. Keine der teilnehmenden Einrichtungen verneinte das Vorhandensein von Maßnahmen vollständig.

Diese Ergebnisse lassen den Schluss zu, dass sich die Mehrheit der Hochschulen bereits aktiv mit dem Thema auseinandersetzt und zumindest mittelfristig strukturelle Maßnahmen etabliert hat. Besonders hervorzuheben ist, dass bei keinem der Teilnehmenden ein völliges Fehlen von Sicherheitsmaßnahmen festgestellt wurde. Gleichzeitig verdeutlicht die Spannbreite der Antworten, dass sich die Einrichtungen in unterschiedlichen Stadien der potenziell oberflächlichen Umsetzung befinden können, was sowohl auf unterschiedliche Ausgangslagen als auch auf individuelle Prioritätensetzungen zurückgeführt werden mag, sofern diese überhaupt eindeutig bestimmt werden können.

6.1.2. Awareness-Maßnahmen

Der zweite Abschnitt der Umfrage widmet sich dem Bereich der Awareness-Maßnahmen. Ziel war es, den Status quo der Umsetzung, die eingesetzten Formate, die Zielgruppen sowie die Wahrnehmung der Wirksamkeit zu erfassen.

Auf die Frage, ob Awareness-Maßnahmen im Bereich der Informationssicherheit an der jeweiligen Einrichtung implementiert wurden, antworteten zehn von zwölf Teilnehmenden mit "Ja". Lediglich zwei gaben an, bislang keine derartigen Maßnahmen durchzuführen. Dies deutet darauf hin, dass der überwiegende Teil der befragten Hochschulen sich aktiv darum bemüht, Mitarbeitende und andere Zielgruppen für sicherheitsrelevante Themen zu sensibilisieren.

Im Hinblick auf die konkret eingesetzten Methoden zeigt sich eine vielfältige Nutzung verschiedener Formate. Am häufigsten genannt wurden E-Learnings (n = 7), gefolgt von Präsenz-Workshops (n = 6) und Online-Workshops (n = 5). Darüber hinaus werden auch klassische Informationsmaterialien wie Plakate oder Broschüren (n = 4) sowie Phishing-Simulationen (n = 4) eingesetzt. Unter Sonstiges wurde zusätzlich ein Phishing-Quiz als Maßnahme genannt. Die Bandbreite der eingesetzten Methoden deutet auf ein differenziertes Vorgehen hin, welches sowohl analoge als auch digitale Formate berücksichtigt.

Die adressierten Zielgruppen variieren, wobei hauptberufliche Mitarbeitende mit Abstand am häufigsten an den Maßnahmen teilnehmen (n = 10). Forschende (n = 6) sowie Studierende (n = 2) und nebenberufliche Lehrpersonen (n = 1) sind seltener eingebunden. Eine teilnehmende Einrichtung gab an, dass alle Mitarbeitenden zur Teilnahme verpflichtet sind. Dies unterstreicht den organisationsweiten Anspruch einzelner Hochschulen, Awareness nicht nur als freiwilliges Angebot, sondern als strukturell verankerte Maßnahme einzuführen.

Die subjektive Einschätzung der Wirksamkeit dieser Maßnahmen fällt überwiegend positiv aus: Sieben der zwölf Teilnehmenden bewerten die Maßnahmen als wirksam beziehungsweise ausgereift, während drei dies verneinen. Dies lässt vermuten, dass noch Optimierungsbedarf gesehen wird.

Auf die abschließende Frage, was an den bestehenden Maßnahmen verbessert werden sollte, wurden drei konkrete Verbesserungsvorschläge genannt: eine Erhöhung der Häufigkeit (n = 2), eine inhaltliche Überarbeitung (n = 1) sowie der Wunsch, Erfolge systematisch zu messen beziehungsweise auszuwerten (n = 1). Diese Rückmeldungen legen nahe, dass sowohl strukturelle als auch qualitative Aspekte der Awareness-Maßnahmen in Zukunft stärker berücksichtigt werden sollten.

Insgesamt zeigt sich, dass Awareness-Maßnahmen an den meisten Einrichtungen bereits implementiert sind und eine Vielfalt an Methoden zur Anwendung kommt. Jedoch besteht hinsichtlich Zielgruppenerreichung, Evaluierung der Maßnahmen und kontinuierlicher Weiterentwicklung noch Potenzial zur Optimierung.

6.1.3. Security Awareness Tools

Im dritten Abschnitt der Umfrage wurde untersucht, inwiefern technische Tools zur Unterstützung von Awareness-Maßnahmen in den Einrichtungen zum Einsatz kommen. Diese Tools bieten in der Regel automatisierte Schulungen, Phishing-Simulationen sowie Auswertungsmöglichkeiten zur Sensibilisierung der Mitarbeitenden.

Auf die Frage, ob Tools zur Security Awareness verwendet werden, antworteten sieben der zwölf befragten Einrichtungen mit "Ja", während fünf angaben, keine derartigen Tools im Einsatz zu haben. Dies weist auf eine tendenziell zunehmende Integration technischer Unterstützung im Bereich der Informationssicherheit hin, zeigt jedoch auch, dass ein erheblicher Teil der Hochschulen (rund 42% der Befragten) noch keine entsprechenden Lösungen implementiert hat.

Bei der Nutzung spezifischer Tools wurden zwei Anbieter besonders häufig genannt: Microsoft Defender for Office 365 sowie SoSafe, jeweils mit vier Nennungen. Andere gängige Produkte wie KnowBe4,Proofpoint Security Awareness Training,Cofense oder SANS Security Awareness Training wurden von keiner der Einrichtungen verwendet. Ebenso blieb das Feld Sonstiges unbeantwortet, was nahelegt, dass derzeit kaum individuell entwickelte oder weitere nicht genannte Lösungen zum Einsatz kommen.

Die Konzentration auf nur zwei Tools deutet darauf hin, dass sich einige Anbieter im Hochschulkontext als praktikabel oder besonders integrationsfreundlich erwiesen haben. SoSafe bietet etwa spezifische Inhalte für den deutschen Sprachraum und ist auf europäische Datenschutzanforderungen abgestimmt, was in diesem Kontext ein möglicher Vorteil sein kann. (vgl. [45]) Microsoft Defender for Office 365 hingegen ist oft bereits Bestandteil bestehender Microsoft-Infrastrukturen.

Zusammenfassend lässt sich feststellen, dass etwa die Hälfte der befragten Einrichtungen auf spezialisierte Security-Awareness-Tools zurückgreift. Die geringe Verbreitung anderer Lösungen kann auf begrenzte Ressourcen, mangelnde Bekanntheit oder eine bewusste Entscheidung zugunsten alternativer Maßnahmen hinweisen. Die weitere Entwicklung in diesem Bereich wird maßgeblich davon abhängen, inwiefern die Wirksamkeit dieser Tools intern evaluiert und als Mehrwert wahrgenommen wird.

6.1.4. Weitere Anregungen

Im letzten Teil der Umfrage bestand die Möglichkeit, weiterführende Informationen, Erfahrungen oder Anregungen frei zu formulieren. Eine der Einrichtungen nutzte diese Gelegenheit, um umfassende Einblicke in bestehende Maßnahmen sowie geplante Entwicklungen im Bereich der Informationssicherheit zu geben.

Es wurde mitgeteilt, dass seit dem Jahr 2022 eine Zwei-Faktor-Authentifizierung (2FA) flächendeckend eingeführt wurde. Darüber hinaus wurde im Jahr 2024 ein externer Security Operations Center (SOC) etabliert, welches eine kontinuierliche 24/7-Überwachung sicherstellt. Auch regelmäßige Penetrationstests werden bereits seit mehreren Jahren durchgeführt, was auf ein fortgeschrittenes Sicherheitsniveau und ein hohes Maß an proaktiver Sicherheitskultur schließen lässt.

Zur technischen Überprüfung der Systemlandschaft kommt ein Nessus-Scan zum Einsatz, der die Aktualität und Sicherheit der Systeme regelmäßig prüft. Ergänzend wird ein Darknet-Monitoring durchgeführt, um potenzielle Leaks von E-Mail-Adressen frühzeitig zu erkennen und entsprechende Maßnahmen einleiten zu können.

Des Weiteren ist ein Informationssicherheits-Managementsystem (ISMS) implementiert; die Zertifizierung nach ISO/IEC 27001 ist für das zweite Quartal geplant. Für das Jahr 2025 ist eine Intensivierung der Awareness-Maßnahmen vorgesehen. Im Fokus steht dabei die Ausweitung des Schulungsprogramms, um das Sicherheitsbewusstsein innerhalb der Organisation weiter zu stärken.

Diese Rückmeldung zeigt beispielhaft, wie ein ganzheitlicher und strategisch ausgerichteter Ansatz zur Informationssicherheit in einer Hochschule aussehen kann. Die Kombination technischer, organisatorischer und personeller Maßnahmen, ergänzt durch kontinuierliche Weiterentwicklung, verdeutlicht, welches Niveau durch gezielte Investitionen und Management-Commitment erreicht werden kann.

6.2. Umfrage IT-Verständnis und Erhebung des Schulungsbedarfs (FH-St. Pölten)

Für ein besseres Verständnis bezüglich der Zielgruppen und deren Wünsche im Bereich der Informationssicherheitssensibilisierung erfolgte die Durchführung einer Umfrage. Diese richtete sich an Mitarbeitende der Fachhochschule St. Pölten. Von diesen nahmen 16 Probanden an der Befragung teil. Die Vorlage der Umfrage kann dem F entnommen werden.

6.2.1. Verständnis IT-Security

Im Rahmen der Umfrage wurden die Teilnehmenden zu ihrem allgemeinen Verständnis im Bereich IT-Sicherheit befragt. Die Ergebnisse zeigen sowohl vorhandene Wissensstände als auch potenzielle Lücken, die auf einen konkreten Schulungsbedarf hinweisen.

In der ersten Frage wurde ermittelt, ob den Mitarbeitenden die Verwendung von S/MIME bekannt ist. Nur vier der sechzehn Befragten beantworteten diese Frage mit „Ja“, obwohl die Technologie in der Einrichtung standardmäßig verwendet wird. Dieses Ergebnis lässt auf ein erhebliches Informationsdefizit schließen. Die Diskrepanz zwischen tatsächlicher Nutzung und individuellem Bewusstsein deutet darauf hin, dass technische Sicherheitsmaßnahmen vielfach im Hintergrund ablaufen, ohne dass deren Funktionsweise oder Bedeutung bei den Nutzenden verankert ist.

Die zweite Frage zielte auf das Verständnis von Cookies ab. Die Mehrheit (15 von 16) gab an, dass Cookies dem Tracking dienen – was korrekt ist. Eine Person ordnete Cookies fälschlicherweise der Verschlüsselung zu. Dieses Ergebnis zeigt, dass grundlegende Konzepte der Webtechnologien den meisten bekannt sind, wenngleich vereinzelte Fehlannahmen bestehen.

Zum Thema Phishing gaben sechs Personen an, bereits betroffen gewesen zu sein. Diese Zahl verdeutlicht die reale Relevanz von Social-Engineering-Angriffen in der Praxis und unterstreicht die Notwendigkeit kontinuierlicher Awareness-Maßnahmen. Die Mehrheit (10 Personen) gab an, bislang nicht betroffen gewesen zu sein – was jedoch nicht zwingend bedeutet, dass keine Bedrohung bestand, sondern möglicherweise auf eine unzureichende Erkennung hindeutet.

In der vierten Frage wurde das Sicherheitsverständnis im Hinblick auf Passwortwahl geprüft. Die Mehrheit bewertete das Passwort **1IvessP!9** (12 Stimmen) als sicher, was aus sicherheitstechnischer Sicht zutreffend ist, da es sich um ein Akronym-Prinzip mit Sonderzeichen handelt. Das Passwort **Ich_verwende_ein_super_sicheres_Passwort!1** wurde ebenfalls von acht Personen als sicher bewertet, was in der Theorie korrekt ist, jedoch bei einem möglichen Wörterbuchangriff eine gewisse Schwäche aufweist. Die Passwörter **MeinPasswort1** sowie **Pa$$w0rD** wurden nur von wenigen als sicher eingeschätzt (0 beziehungsweise 2 Stimmen), was darauf hinweist, dass sich bei der Mehrheit ein grundlegend richtiges Verständnis für sichere Passwortgestaltung etabliert hat.

Insgesamt zeigen die Ergebnisse, dass ein gewisses Grundverständnis für IT-Sicherheit vorhanden ist, jedoch spezifische technische Aspekte wie S/MIME oder differenzierte Bedrohungslagen (zum Beispiel Erkennung von Phishing-Angriffen) nicht bei allen Teilnehmenden bekannt sind. Daraus ergibt sich ein klarer Bedarf für zielgerichtete und verständlich aufbereitete Schulungsmaßnahmen, insbesondere zur Sensibilisierung für im Hintergrund aktive Sicherheitslösungen sowie zur Vertiefung sicherheitsrelevanter Alltagspraktiken.

6.2.2. Interesse für neue Technologien

Im Rahmen des Abschnitts „Interesse für neue Technologien“ wurde untersucht, inwieweit die Befragten privat oder beruflich moderne Technologien und digitale Werkzeuge nutzen. Die Ergebnisse zeigen ein insgesamt hohes Maß an technischer Affinität und ein breites Spektrum an Nutzungserfahrungen.

Besonders häufig wurden Cloud-Dienste (12 Nennungen), Onlinebanking (12), Browsererweiterungen (13), Passwortmanager (12) sowie die Mehr-Faktor-Authentifizierung (15) angegeben. Letztere stellt mit fast vollständiger Verbreitung unter den Befragten einen zentralen Sicherheitsmechanismus dar, dessen Relevanz offensichtlich erkannt wird. Auch die Nutzung von Passwortmanagern lässt auf ein wachsendes Sicherheitsbewusstsein und eine zunehmende Akzeptanz von unterstützenden Technologien zur Verwaltung sensibler Daten schließen.

KI-gestützte Tools und Sprachmodelle wie ChatGPT wurden von jeweils neun Personen als im Einsatz befindlich angegeben. Dies verdeutlicht eine steigende Offenheit gegenüber innovativen Technologien und deren Integration sowohl im beruflichen als auch im privaten Kontext.

Technologien wie VPNs und Datenschutz-Tools (9), digitale Notiz- und Organisations-Apps (9) sowie E-Learning-Plattformen (7) erfreuen sich ebenfalls signifikanter Beliebtheit, was auf eine aktive Auseinandersetzung mit digitalen Möglichkeiten zur Informationsverarbeitung, Weiterbildung und zum Schutz der Privatsphäre hindeutet.

Weniger verbreitet, aber dennoch genutzt, sind IoT-Geräte (8), Wearables (6) sowie Anwendungen auf Basis von Blockchain-Technologie (5). Letzteres deutet auf eine differenzierte Technologieadaption hin, bei der eher sicherheits- und produktivitätsbezogene Tools im Vordergrund stehen, während experimentellere oder stärker lifestyle-orientierte Anwendungen vergleichsweise seltener genutzt werden.

Insgesamt legen die Ergebnisse nahe, dass die befragten Personen eine hohe digitale Grundkompetenz aufweisen. Dieses Interesse an Technologien bildet eine günstige Voraussetzung für die Integration digitaler Sicherheitsmaßnahmen und für eine effektive Weiterentwicklung von Awareness-Maßnahmen, da vorhandene Tools besser verstanden, akzeptiert und genutzt werden können.

6.2.3. Informationssicherheit

Im Abschnitt Informationssicherheit wurde das persönliche Interesse der Befragten an diesem Themenfeld erfragt. Die Ergebnisse zeigen eine grundsätzlich positive Haltung: 12 von 16 Befragten gaben an, sich interessiert an Informationssicherheit zu fühlen. Weitere drei Personen beschrieben sich als teilweise interessiert, während nur eine Person angab, kein Interesse an dem Thema zu haben.

6.2.4. Weiterbildung

Im Rahmen des Abschnitts Weiterbildung wurde erhoben, welche Formate der Wissensvermittlung die Teilnehmenden bevorzugen. Ziel war es, Rückschlüsse auf die Gestaltung künftiger Schulungs- und Awareness-Maßnahmen im Bereich Informationssicherheit zu ziehen. Die Ergebnisse zeigen eine klare Tendenz hin zu Präsenzveranstaltungen, die von neun Personen als bevorzugtes Lernformat angegeben wurden. Dicht dahinter folgen Online-Vorträge beziehungsweise Workshops mit sechs Nennungen, sowie E-Learnings und Blogbeiträge mit jeweils fünf Nennungen.

Klassische Informationskanäle wie Newsletter und Printmagazine wurden jeweils von drei Teilnehmenden bevorzugt. Unter der Kategorie Sonstiges wurden zudem Fachbücher sowie die Möglichkeit zu interaktiven Präsenzworkshops als besonders hilfreich hervorgehoben – insbesondere zur Klärung individueller Fragen, die über das bereitgestellte Material hinausgehen.

6.2.5. Schulung für IT-Sicherheit

Der Abschnitt Schulung für IT-Security zielte darauf ab, die bisherigen Erfahrungen der Mitarbeitenden mit Schulungsangeboten im Bereich Informationssicherheit zu erfassen sowie deren Bereitschaft zur zukünftigen Teilnahme an entsprechenden Maßnahmen zu ermitteln.

Zunächst gaben 11 der 16 Befragten an, in der Vergangenheit bereits an Schulungen zum Thema IT-Sicherheit teilgenommen zu haben. Dies entspricht knapp 69% der Stichprobe. 5 Personen (etwa 31%) haben bisher keine diesbezüglichen Schulungen besucht.

Hinsichtlich der Wahrnehmung vergangener Schulungen fällt die Bewertung tendenziell positiv aus: 6 Personen (etwa 55% der Schulungsteilnehmenden) berichteten, dass ihnen die Schulung gefallen habe, während weitere 5 Personenangaben, dass sie zumindest teilweise zufrieden waren. Negative Rückmeldungen wurden nicht verzeichnet.

Auf die Frage nach dem Interesse an zukünftiger Teilnahme an Workshops zu Themen der Informationssicherheit, etwa Sicher Surfen, zeigten sich die Teilnehmenden größtenteils offen. Zwar äußerten nur drei Personen ein eindeutiges Interesse, doch neun Teilnehmende machten ihre Bereitschaft von der Relevanz und Gestaltung des jeweiligen Themas abhängig. Lediglich vier Personen signalisierten kein Interesse an zukünftigen Workshops.

6.2.6. Informationen zu IT-Sicherheit

In diesem Abschnitt wurde das allgemeine Interesse der Mitarbeitenden an wiederkehrenden Informationen zum Thema IT-Sicherheit sowie deren präferierte Kanäle und Häufigkeiten der Informationsvermittlung erfasst.

Bezüglich der Frage, ob ein grundsätzliches Interesse am Empfang von Nachrichten zur IT-Sicherheit bestehe, antworteten zehn von 16 Befragten mit Ja. Demnach lag der Anteil bei 62,5%, während sechs Personen (37,5%) kein Interesse äußerten. Bei einer Mehrheit der Teilnehmenden bestand eine grundsätzliche Bereitschaft für fortlaufende Informationen, auch wenn ein bedeutender Teil kein aktives Interesse bekundete.

Bezüglich des favorisierten Informationskanals verteilten sich die Äußerungen annähernd gleichmäßig auf die zwei zur Auswahl stehenden Möglichkeiten: sechs Personen gaben an, Informationen bevorzugt über Teamwork-Beiträge (also Intranet oder interne Plattformen) zu erhalten, während fünf Personen den E-Mail-Newsletter präferierten. Dies lässt vermuten, dass zur Erreichung einer möglichst hohen Reichweite mehrere Kommunikationswege in Betracht gezogen werden sollten, um die unterschiedlichen Gewohnheiten und Präferenzen innerhalb der Zielgruppe zu berücksichtigen.

Hinsichtlich der gewünschten Häufigkeit der Informationsbereitstellung äußerten die meisten Befragten den Wunsch nach einer monatlichen Zustellung (sechs Personen), gefolgt von vierteljährlichen Updates (vier Personen). Keine der Teilnehmenden sprach sich für eine halbjährliche Informationsfrequenz aus, was darauf schließen lässt, dass aus Sicht der Interessierten das Thema regelmäßig und in angemessenen Zeitabständen aufgegriffen werden sollte, um Relevanz und Aktualität sicherzustellen.

6.2.7. Weitere Anregungen

Die abschließende offene Frage diente dazu, den Teilnehmenden die Möglichkeit zu geben, über die konkreten Fragestellungen hinaus weitere Gedanken, Hinweise oder Kritik zu äußern. Von den insgesamt 16 Befragten wurde ein ergänzender Hinweis eingebracht.

Der Hinweis bezog sich auf die Gestaltung der Antwortmöglichkeiten in der Umfrage: Es wurde angemerkt, dass idealerweise jede Frage ein Freifeld, beziehungsweise die Möglichkeit einer Sonstiges-Antwort, enthalten sollte, um individuelle und möglicherweise widersprüchliche Rückmeldungen und gegebenenfalls nicht vorhersehbare Perspektiven abbilden zu können.

In diesem spezifischen Fall wurden jedoch bewusst für manche Fragen geschlossene Antwortformate gewählt, um die Praxisnähe und die realistisch umsetzbaren Optionen im jeweiligen organisationalen Kontext widerzuspiegeln.

6.3. Beantwortung der Forschungsfragen

Die zuvor in der Einleitung dieser Arbeit gestellten Forschungsfragen konnten wie folgt einer Beantwortung unterzogen werden:

- Wie könnte ein Konzept zur Informationssicherheit-Sensibilisierung speziell für Hochschulen aussehen?

Auf Basis der durchgeführten Umfragen und Analysen ergibt sich ein klares Bild hinsichtlich des Status quo sowie der Herausforderungen und Potenziale im Bereich der Informationssicherheit-Sensibilisierung an Hochschulen. Die Auswertung zeigt, dass in den meisten Einrichtungen bereits erste Maßnahmen vorhanden sind, jedoch häufig noch keine umfassende Strategie vorliegt, oder die verantwortlichen Personen mit besagten Maßnahmen noch nicht vollends zufrieden sind.

Ein wirksames Sensibilisierungskonzept sollte mehrere Dimensionen berücksichtigen:

Anpassung an die Zielgruppen

Hochschulen vereinen unterschiedliche Personengruppen wie Führungspositionen, Forschende, Lehrende und Studierende, die sich in ihrem Wissen, ihrem Interesse sowie ihrem Zugang zu sicherheitsrelevanten Informationen unterscheiden. Ein zentrales Element des Konzepts ist daher die Differenzierung nach Zielgruppen. Während beispielsweise hauptberufliche Mitarbeitende häufig bereits geschult wurden, zeigen die Ergebnisse, dass Studierende und Lehrbeauftragte bislang kaum erreicht werden. Aufgrund dessen wird empfohlen, Awareness-Tätigkeiten zunächst auf die primären Zielgruppen zu verteilen, und nach Bewährtheit eines Programms beziehungsweise bei Bedarf Sensibilisierungsmaßnahmen weiter auszubreiten. Darüber hinaus sollte beachtet werden, dass Inhalte und Formate dem jeweiligen „Need-to-Know“-Prinzip folgen sollten.

Vielfältigkeit der Sensibilisierungs Formate

Wie auch die Rückmeldungen aus den Umfragen verdeutlichen, variieren die bevorzugten Lernformate. Während Präsenzworkshops häufig als besonders wirkungsvoll empfunden werden, zeichnen sich E-Learnings durch eine gute Erreichbarkeit aus. Deshalb empfiehlt sich eine Kombination aus interaktiven Präsenzveranstaltungen, digitalen Lernmodulen und regelmäßigen Kurzimpulsen, etwa über Newsletter oder Intranet-Beiträge. Im Zuge der Ausarbeitung wurden unter anderem die Medien interaktive Lernprogramme, Veranstaltungen und E-Mail, vor allem auch in Hinblick auf die Erreichbarkeit aller Lerntypen, als hilfreich identifiziert. Der Einsatz von Security-Awareness-Tools ist derzeit noch begrenzt. Wo bereits Systeme wie zum Beispiel SoSafe oder Microsoft Defender im Einsatz sind, bieten sich Ansätze zur Erfolgskontrolle und Wiederholungsschulung. Hochschulen sollten prüfen, inwieweit bestehende Systeme ausgebaut oder durch spezialisierte Lösungen ergänzt werden können. Empfehlenswert ist es ebenso, vorhandene Technologien, beispielsweise eine zentrale Web-Oberfläche wie Moodle, für Awareness-Tätigkeiten einzubinden.

Frequenz und zeitliche Planung von Schulungsmaßnahmen

Die zeitliche Strukturierung von Awareness-Maßnahmen ist ein zentraler Erfolgsfaktor. Auch die Umfrageergebnisse zeigen, dass sich ein Großteil der Teilnehmenden eine regelmäßige Informationsvermittlung – insbesondere im monatlichen oder quartalsweisen Rhythmus – wünscht. Daraus ergibt sich die Empfehlung, wiederkehrende Formate wie Newsletter, Kurzimpulse oder Micro-Learnings fest in den Kommunikationsplan der Hochschule zu integrieren.

Zudem bietet sich die Integration von Basisschulungen in den Onboarding-Prozess neuer Mitarbeitender und Studierender an. So kann sichergestellt werden, dass bereits beim Eintritt in die Organisation ein Mindestmaß an Sicherheitsbewusstsein geschaffen wird. Ergänzend sollten bestehende Awareness-Angebote in regelmäßigen Abständen aufgefrischt und evaluiert werden, um langfristige Wirksamkeit zu gewährleisten. Ein vorgeschlagener Zeitraum wäre hierbei zu Beginn eines Semesters. Auch freiwillige Auffrischungsworkshops oder themenspezifische Reihen (zum Beispiel „IT-Security im Homeoffice“) könnten als Ergänzung dienen.

- Auf welche Themengebiete der Informationssicherheit müsste dabei besonderes Augenmerk gelegt werden?

Durch die Analyse spezifischer Bedrohungsszenarien, denen Hochschulen ausgesetzt sind, sowie der besonderen Merkmale ihrer IT-Infrastruktur, lassen sich prioritäre Themenfelder ableiten. Im Rahmen von Schulungsmaßnahmen sollte der Fokus insbesondere auf folgenden Bereichen liegen: physische Sicherheit, Web-Schwachstellen, Passwortsicherheit, Insider-Bedrohungen, Abhängigkeiten von Drittanbietern, personelle Risiken, Ransomware sowie DDoS-Angriffe.

Dabei ist zu berücksichtigen, dass nicht alle Themen für jede Zielgruppe gleichermaßen relevant sind. Eine zielgruppenspezifische Aufbereitung der Inhalte orientiert sich am jeweiligen Verantwortungs- und Risikobereich. Diese ist daher essenziell, um eine wirkungsvolle Sensibilisierung zu erreichen.

- Welche Herausforderungen treten bei der Konzeption und Umsetzung auf, und wie kann diesen begegnet werden?

Im Fokus dieser Arbeit standen die Erhebung und Analyse der relevanten Zielgruppen sowie die Planung geeigneter Schulungsthemen und passender Vermittlungsmedien. Dabei wurden eine Reihe von Herausforderungen identifiziert, denen im Rahmen der Konzeptentwicklung gezielt mit entsprechenden Lösungsansätzen begegnet wurde. Die zentralen Aspekte lassen sich in zwei übergeordnete Bereiche gliedern:

Herausforderungen im Bereich der Zielgruppen: Eine zentrale Schwierigkeit liegt in der Heterogenität der Zielgruppen. Hochschulen vereinen Personen unterschiedlichster Fachrichtungen, Altersgruppen, Kulturen und Sprachhintergründe. Hinzu kommt ein oftmals unterschiedliches oder fehlendes Grundverständnis für Informationssicherheit.

Um diese Hürden zu überwinden, empfiehlt es sich, Schulungsinhalte so aufzubereiten, dass sie unabhängig vom technischen Vorwissen verständlich sind. Dies bedeutet insbesondere, komplexe Fachsprache in eine allgemein zugängliche Form zu übersetzen. Die Erstellung von Schulungsmaterialien in mehreren Sprachen – insbesondere Deutsch und Englisch – kann zusätzlich Barrieren abbauen. Weiterhin sollte versucht werden, durch lebensnahe Beispiele den persönlichen Bezug zur Thematik zu stärken, etwa durch die Darstellung von Risiken im privaten Kontext („Wie schütze ich meine Kinder im Internet?“). Ebenso wichtig ist es, die individuelle Rolle jeder Person in der Gewährleistung der Cybersicherheit klar und nachvollziehbar zu kommunizieren.

Herausforderungen bei Maßnahmen, Themenwahl und Medienauswahl: Auf der Umsetzungsebene zeigen sich weitere Herausforderungen, etwa der Widerstand gegenüber Veränderungen in bestehenden Arbeitsabläufen oder das fehlende Verständnis für die Notwendigkeit bestimmter Sicherheitsmaßnahmen. Zusätzlich kann die Wirkung von Schulungen geschwächt werden, wenn Beispiele ohne klaren Bezug zum Arbeitsalltag gewählt werden.

Ein möglicher Lösungsansatz liegt in der aktiven Einbindung der Mitarbeitenden. Durch gezielte Nachfragen kann herausgefunden werden, warum bestimmte Maßnahmen auf Ablehnung stoßen und inwiefern eine Anpassung möglich wäre. Gleichzeitig ist es hilfreich, Verständnis für die psychologischen Prozesse hinter Veränderungswiderständen zu zeigen. Darüber hinaus sollten Schulungsinhalte möglichst aktuell und kontextbezogen gestaltet werden. So können gesellschaftlich relevante Ereignisse (zum Beispiel Pandemie, Naturkatastrophen,...) genutzt werden, um Beispiele mit höherer Relevanz und Wiedererkennungseffekt zu schaffen.

- Unterscheidet sich ein solches Konzept an Hochschulen von jenem in gleich großen Unternehmen anderer Branchen – und wenn ja, inwiefern?

Hochschulen und vergleichbare Organisationen wie das Österreichische Rote Kreuz oder Werbung Tirol weisen strukturelle Gemeinsamkeiten auf, etwa eine mehrstufige Aufbauorganisation, verschiedene Fachabteilungen und den Umgang mit sensiblen Daten. Unterschiede ergeben sich vor allem aus dem jeweiligen Auftrag. Hochschulen adressieren neben Mitarbeitenden auch Studierende als zentrale Zielgruppe, was eine besonders heterogene Ansprache erfordert.

Der Fokus von Awareness-Maßnahmen unterscheidet sich dementsprechend: Während in Unternehmen oft operative Risiken im Vordergrund stehen, spielt an Hochschulen beispielsweise das Thema physische Sicherheit eine größere Rolle. Auch die Vielfalt an Fachrichtungen und das unterschiedliche Vorwissen erfordern eine breitere, zielgruppenorientierte Gestaltung der Inhalte.

7. Conclusio

Die Auswertungen der beiden durchgeführten Umfragen zeigen, dass sich die befragten Einrichtungen aktiv mit dem Thema Informationssicherheit auseinandersetzen. In den meisten Fällen sind bereits umfassende Maßnahmen etabliert oder ein ISMS im Aufbau. Awareness-Maßnahmen wie E-Learnings, Workshops oder Phishing-Simulationen werden vielfach eingesetzt, jedoch besteht teils noch Optimierungsbedarf hinsichtlich Wirksamkeit, Zielgruppenerreichung und Erfolgskontrolle.

Die Nutzung spezieller Security-Awareness Tools ist ausbaufähig. Auf der Mitarbeitendenebene zeigen sich grundlegende Kenntnisse, zugleich aber auch Lücken, etwa beim Verständnis technischer Funktionen wie S/MIME. Das hohe Interesse an digitalen Technologien und Weiterbildung – insbesondere in Präsenz- und Onlineformaten – bietet eine gute Grundlage für zukünftige Awareness-Strategien.

Insgesamt zeigt sich, dass bereits eine stabile Basis existiert, die durch gezielte, zielgruppengerechte Maßnahmen weiter gestärkt werden kann – insbesondere durch praxisnahe Formate, regelmäßige Informationsangebote und eine stärkere Verankerung von Sicherheitsbewusstsein im Arbeitsalltag.

Ein nachhaltiges Sensibilisierungskonzept für Hochschulen sollte modular, praxisnah und ansprechend gestaltet sein – mit Angeboten, die an die unterschiedlichen Zielgruppen angepasst wurden, unter Nutzung bewährter didaktischer Mittel und unter Einsatz unterstützender Tools. Die Erkenntnisse dieser Arbeit bieten eine Grundlage zur Entwicklung und Umsetzung entsprechender Maßnahmen.

Abbildungsverzeichnis

Tabellenverzeichnis

Akronyme

ADP	Automated Data Processing
AQ Austria	Agentur für Qualitätssicherung und Akkreditierung Österreich
Authentizität	Eigenschaft, die Echtheit und Identität sicherzustellen
Awareness	Zustand des Bewusstseins über Informationssicherheitsrisiken und angemessenes Verhalten
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
Compliance	Einhaltung gesetzlicher, regulatorischer und interner Vorgaben
CPLP	Cyber Security Learning Program
DSGVO	Datenschutz-Grundverordnung
ENISA	European Union Agency for Cybersecurity
FH	Fachhochschule
Hochschule	Einrichtung des tertiären Bildungsbereiches, z.B. Universitäten und Fachhochschulen

IEC	International Electrotechnical Commission
Informationssicherheit	Schutz von Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit
Integrität	Korrektheit und Unverfälschtheit von Daten und Informationen
IRM	Information Ressource Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
Kommunikation	Vermittlung von Informationen zwischen Sender und Empfänger
KPMG	Klynveld Peat Marwick Goerdeler (Wirtschaftsprüfungsgesellschaft)
KSÖ	Kuratorium Sicheres Österreich
Lerntypen	Klassifikation von Menschen nach bevorzugtem Lernverhalten oder -kanal
LLM	Large Language Model
NIS	Netz- und Informationssysteme
NIST	National Institute of Standards and Technology
Ordnungsmäßigkeit	Konformität mit internen und externen Vorgaben und Standards
Phishing	Täuschungstechniken zur Erlangung vertraulicher Informationen

Security	Englischer Begriff für Sicherheit, v.a. im Kontext von Informationssicherheit
Sensibilisierung	Maßnahme zur Erhöhung des Bewusstseins für sicherheitsrelevante Themen
UG	Universitätsgesetz
Verfügbarkeit	Sicherstellung, dass Informationen und Systeme bei Bedarf zugänglich sind
Vertraulichkeit	Eigenschaft, dass Informationen nur für autorisierte Personen zugänglich sind
ZKI	Zentren für Kommunikation und Informationsverarbeitung
Zuverlässigkeit	Fähigkeit eines Systems oder Prozesses, dauerhaft korrekt zu funktionieren

Literatur

[1] Siponen, „Five dimensions of information security awareness“, *SIGCAS Comput. Soc.*, Jg. 31, Nr. 2, S. 24–29, Juni 2001, ISSN: 0095-2737. DOI: 10.1145/503345.503348. Adresse: https://doi.org/10.1145/503345.503348.

[2] KPMG Austria und Kompetenzzentrum Sicheres Österreich (KSÖ), „Cybersecurity in Österreich 2024“, KPMG Austria und KSÖ, 2024, Zugriff über interne Studie.

[3] Tania Wallis und Chris Johnson, „Implementing the NIS Directive, driving cybersecurity improvements for Essential Services“, in *Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Juni 2020, S. 1–10. DOI: 10.1109/CyberSA49311.2020.9139641.

[4] Bert Kondruss, *Cyberangriffe auf Unternehmen 2024*, Zugriff am 6. April 2025, 2025. Adresse: https://konbriefing.com/de-topics/cyber-angriffe-2024-ind-logistik.html.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI), *IT-Grundschutz-Profil für Hochschulen*, Zugriff am 6. April 2025, 2022. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Hochschulen.pdf?__blob=publicationFile&v=2.

[6] Gerald Faschingeder, Bernhard Leubolt, Pia Lichtblau, Oliver Prausmüller, Johannes Schimmerl und Angelika Striedinger, „Bildung ermächtigt. Eine Einleitung“, in *Ökonomisierung der Bildung: Tendenzen, Strategien, Alternativen*, Zugriff am 6. April 2025, Wien: Mandelbaum Verlag, 2005, S. 7–14. Adresse: https://www.pfz.at/wp-content/uploads/2020/07/GEP-5-Bildungs%C3%B6konomisierung.pdf.

[7] Pier-Paolo Pasqualoni, „Österreichische Universitäten im Spiegel der Geschichte: Fallstricke einer Reform der Reform“, in *Ökonomisierung der Bildung: Tendenzen, Strategien, Alternativen*, Gerald Faschingeder, Bernhard Leubolt, Pia Lichtblau, Oliver Prausmüller, Johannes Schimmerl und Ange-

lika Striedinger, Hrsg., Wien: Mandelbaum Verlag, 2005, S. 103–128. Adresse: https://www.pfz.at/wp-content/uploads/2020/07/GEP-5-Bildungs%C3%B6konomisierung.pdf.

[8] Republik Österreich, *Universitätsgesetz 2002*, BGBl. I Nr. 120/2002. Zugriff am 6. April 2025, 2002. Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002128.

[9] Republik Österreich, *Fachhochschul-Studiengesetz*, BGBl. Nr. 340/1993. Zugriff am 6. April 2025, 1993. Adresse: https://www.jusline.at/gesetz/fhstg/gesamt.

[10] Bundesministerium für Bildung und Forschung (BMBF), *Hochschulen: Datenportal des BMBF*, Zugriff am 6. April 2025. Adresse: https://www.datenportal.bmbf.de/portal/de/G110.html.

[11] Wissenschaft und Forschung (BMBWF) Bundesministerium für Bildung, *Universitäten: Hochschulsystem in Österreich*, Zugriff am 24. Februar 2025. Adresse: https://www.bmbwf.gv.at/Themen/HS-Uni/Hochschulsystem/Universit%C3%A4ten.html.

[12] Studieren.at, *Hochschulformen in Österreich: Überblick & Unterschiede*, Zugriff am 6. April 2025. Adresse: https://www.studieren.at/hochschulformen/.

[13] Republik Österreich, *Privathochschulgesetz (PrivHG)*, BGBl. I Nr. 77/2020. Zugriff am 6. April 2025, 2021. Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011248.

[14] „Bundesgesetz über die Elektrotechnik (Elektrotechnikgesetz 1992 - ETG 1992)“. Bundesrecht konsolidiert, Fassung vom 31.12.2020. (2020), Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007385&FassungVom=2020-12-31 (besucht am 27. 04. 2025).

[15] Republik Österreich, *Hochschulgesetz 2005 (HG)*, BGBl. I Nr. 30/2006. Zugriff am 6. April 2025, 2005. Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004626.

[16] Republik Österreich, *Hochschul-Qualitätssicherungsgesetz (HS-QSG)*, BGBl. I Nr. 74/2011. Zugriff am 6. April 2025, 2011. Adresse: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007384.

[17] Bundeskanzleramt Österreich, *Rechtsinformationssystem des Bundes (RIS)*, Zugriff am 6. April 2025. Adresse: https://www.ris.bka.gv.at/.

[18] firmenabc.at. „Technikum Wien GmbH - Firmenbuchauszug Adresse“. (), Adresse: https://www.firmenabc.at/technikum-wien-gmbh_ECgp (besucht am 27. 04. 2025).

[19] Fachhochschule St. Pölten. „Impressum“. (), Adresse: https://www.fhstp.ac.at/de/impressum/impressum (besucht am 27. 04. 2025).

[20] Donau-Universität Krems. „Impressum“. Abgerufen am 27. April 2025. (o.J.), Adresse: https://www.donau-uni.ac.at/de/universitaet/impressum.html.

[21] Johannes Kepler Universität Linz, *Organisation der Johannes Kepler Universität Linz*, Zugriff am 6. April 2025, 2025. Adresse: https://www.jku.at/fileadmin/gruppen/61/Satzung___Co/Organisation/2101_Organisation_V80_2025_01_30_formatiert.pdf.

[22] Fachhochschule St. Pölten, *Organigramm der Fachhochschule St. Pölten*, Zugriff am 6. April 2025, 2025. Adresse: https://www.fhstp.ac.at/de/mediathek/pdfs/infoblaetter/organigramm.pdf.

[23] Stefan Beißel, *Security Awareness*. De Gruyter Oldenbourg, 2019. DOI: 10.1515/9783110668261. Adresse: https://doi.org/10.1515/9783110668261.

[24] International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC), *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*, Zugriff am 6. April 2025, 2018. Adresse: https://www.iso.org/standard/73906.html.

[25] International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC), *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Zugriff am 6. April 2025, 2022. Adresse: https://www.iso.org/standard/27001.

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI), *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit*, Zugriff am 6. April 2025, 2021. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2022.pdf?__blob=publicationFile&v=3.

[27] ENISA, „A New User's Guide: How to Raise Information Security Awareness“, European Union Agency for Cybersecurity, Techn. Ber., 2010. DOI: 10.2824/19110. Adresse: https://doi.org/10.2824/19110.

[28] NIST, „Building a Cybersecurity and Privacy Learning Program (NIST SP 800-50r1)“, National Institute of Standards und Technology, Techn. Ber., 2023. DOI: 10.6028/NIST.SP.800-50r1. Adresse: https://doi.org/10.6028/NIST.SP.800-50r1.

[29] NIST, „Information Technology Security Training Requirements: A Role- and Performance-Based Model (NIST SP 800-16)“, National Institute of Standards und Technology, Techn. Ber., 1998. DOI: 10.6028/NIST.SP.800-16. Adresse: https://doi.org/10.6028/NIST.SP.800-16.

[30] International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC), *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*, Zugriff am 6. April 2025, 2022. Adresse: https://www.iso.org/standard/75652.html.

[31] Lisa Maria Pilotto, *Blended Learning: Konzepte, Didaktik, Beispiele*. Springer Vieweg, Wiesbaden, 2021. DOI: 10.1007/978-3-658-31235-0. Adresse: https://doi.org/10.1007/978-3-658-31235-0.

[32] Josef Schrader, *Lerntypen bei Erwachsenen: Empirische Analysen zum Lernen und Lehren in der beruflichen Weiterbildung* (Analysen und Beiträge zur Aus- und Weiterbildung), 2., ergänzte Auflage. Bad Heilbrunn: Klinkhardt, 2008, S. 296, Zugleich: Marburg, Univ., Diss., 1992 unter dem Titel: Lernstile in der beruflichen Weiterbildung, ISBN: 978-3-7815-1642-7. Adresse: https://www.fachportal-paedagogik.de/literatur/vollanzeige.html?FId=2947614.

[33] Kathrin Quilling, *Lernstile und Lerntypen*, Zugriff am 6. April 2025, 2015. Adresse: https://www.die-bonn.de/wb/2015-lernstile-01.pdf.

[34] Beattie G. und Ellis A.W., *The Psychology of Language and Communication, (1st ed.)* Routledge, Mai 2017, S. 1–291, ISBN: 9781315187198. DOI: 10.4324/9781315187198. Adresse: https://doi.org/10.4324/9781315187198.

[35] Ann-Catrin Fender, „Kommunikation als Medium der Führung – Vier Seiten einer Nachricht und die Kunst des Fragens und des Zuhörens“, *Perspektive Bibliothek*, Jg. 4, Nr. 2, S. 150–171, Dez. 2015. DOI: 10.11588/pb.2015.2.26276. Adresse: https://journals.ub.uni-heidelberg.de/index.php/bibliothek/article/view/26276.

[36] Wissenschaftsrat, *Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum*, 2023. DOI: 10.57674/m6pk-dt95. Adresse: https://doi.org/10.57674/m6pk-dt95.

[37] Bernhard Brandel, Sebastian Porombka und Gudrun Oevel, „IT-Schutz ist kein Projekt, sondern ein Prozess“, *Forschung & Lehre*, 6. Aug. 2020, Zugriff am 6. April 2025. Adresse: https://www.forschung-und-lehre.de/management/it-schutz-ist-kein-projekt-sondern-ein-prozess-3005.

[38] Haya Schulmann und Michael Waidner, „Forschung muss besser geschützt werden“, *Forschung & Lehre*, 6. März 2023, Zugriff am 6. April 2025. Adresse: https://www.forschung-und-lehre.de/management/forschung-muss-besser-geschuetzt-werden-5449.

[39] UpGuard, „The State of University Cybersecurity: Top Three Security Concerns“, UpGuard, Techn. Ber., 2025, Zugriff am 12. April 2025. Adresse: https://content.upguard.com/hubfs/resources/Whitepaper%20-%20State%20of%20University%20Cybersecurity.pdf.

[40] Harjinder Singh Lallie, Andrew Thompson, Elzbieta Titis und Paul Stephens, „Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector“, *Computers*, Jg. 14, Nr. 2, 2025, ISSN: 2073-431X. DOI: 10.3390/computers14020049. Adresse: https://www.mdpi.com/2073-431X/14/2/49.

[41] Österreichisches Rotes Kreuz, *Das Generalsekretariat*, Zugriff am 12. April 2025, 2025. Adresse: https://www.roteskreuz.at/willkommen/das-generalsekretariat.

[42] Tirol Werbung GmbH, *Organisation und Teams*, Zugriff am 12. April 2025, 2025. Adresse: https://www.tirolwerbung.at/unternehmen/organisation.

[43] SCHIG GmbH, *Organigramm*, Stand: Juli 2024. Zugriff am 12. April 2025, 2024. Adresse: https://www.schig.com/unternehmen/organigramm.

[44] „Service- und Kompetenzzentrum für Lehr-Lernentwicklung und Bildungsangebote (LEARN)“, Fachhochschule St. Pölten. (), Adresse: https://www.fhstp.ac.at/de/uber-uns/fh-services/service-und-kompetenzzentrum-fuer-lehr-lernentwicklung-und-bildungsangebote-learn (besucht am 25. 04. 2025).

[45] SoSafe GmbH, *SoSafe Awareness Plattform*, Zugriff am 19. April 2025, 2025. Adresse: https://sosafe-awareness.com/de/.

A. Zielgruppenanalyse

A.1. Zielgruppe: Angestellte

Zielgruppe	Angestellte
Definition	Angestellte der Hochschule aus jeglicher Abteilung, welche nicht IT-spezifisch ist.
Kategorie	Mitarbeitende
Voraussichtliches Wissen	Technisches Wissen kann nicht vorausgesetzt werden.
Benötigtes Wissen	Grundlegendes Wissen bezüglich Informationssicherheit.
Motivation für Awareness	Allgemeine Erhebung des Sicherheitsniveaus sowie Förderung von Sicherheit im privaten Umfeld.

Tabelle A.2.: Zielgruppe: Angestellte

A.2. Zielgruppe: Führungspositionen

Zielgruppe	Führungspositionen
Definition	Führungspositionen in verschiedenen Bereichen. Dazu zählen Geschäftsführungen, Abteilungsleitungen, Rektorate oder Fakultätsleitungen.
Kategorie	Mitarbeitende
Voraussichtliches Wissen	Technisches Wissen kann nicht vorausgesetzt werden.
Benötigtes Wissen	Grundlegendes Wissen bezüglich Informationssicherheit und wie Gefährdungen die Geschäftstätigkeit beeinflussen können.
Motivation für Awareness	Führungsebenen sollten als ein gutes Beispiel den Mitarbeitenden vorangehen.

Tabelle A.4.: Zielgruppe: Führungspositionen

A.3. Zielgruppe: IT-Fachkräfte / Informationssicherheits Fachkräfte

Zielgruppe	IT-Fachkräfte / Informationssicherheits Fachkräfte
Definition	Angestellte der Hochschule aus technischen Abteilungen (beispielsweise der internen IT-Abteilung), Technischen Departments oder Fakultäten. Diese haben direkt mit den Systemen der Hochschule zu tun.
Kategorie	Mitarbeitende
Voraussichtliches Wissen	Technisches Wissen kann vorausgesetzt werden.
Benötigtes Wissen	Grundlegendes Wissen bezüglich Informationssicherheit, sowie technische Aspekte zur Gewährleistung eines sicheren IT-Betriebes.
Motivation für Awareness	Sicherstellung von ordnungsgemäß konfigurierten und gewarteten Systemen.

Tabelle A.6.: Zielgruppe: IT-Fachkräfte / Informationssicherheits Fachkräfte

A.4. Zielgruppe: Facility Management, Mensa Mitarbeitende

Zielgruppe	Facility Management, Mensa Mitarbeitende
Definition	Externe Dienstleister, welche regelmäßig Zutritt zu den Einrichtungen haben (beispielsweise Reinigungskräfte).
Kategorie	Third Party
Voraussichtliches Wissen	Technisches Wissen kann nicht vorausgesetzt werden.
Benötigtes Wissen	Grundlegendes Wissen bezüglich Informationssicherheit, vor allem physische Sicherheit.
Motivation für Awareness	Vermeidung von physischen Bedrohungen wie z. B. unbefugte Zutritte.

Tabelle A.8.: Zielgruppe: Facility Management, Mensa Mitarbeitende

A.5. Zielgruppe: Studierende

Zielgruppe	Studierende
Definition	Studierende und Alumni, welche Zugriff zu bestimmten IT-Systemen der Hochschule haben. Darüber hinaus ist ein physischer Zutritt möglich.
Kategorie	Studierende
Voraussichtliches Wissen	Technisches Wissen kann nicht vorausgesetzt werden. Es kann jedoch die Annahme getroffen werden, dass dies bei einigen vorhanden ist.
Benötigtes Wissen	Grundlegendes Wissen bezüglich Informationssicherheit.
Motivation für Awareness	Vorbereitung auf die Arbeitswelt. Der Bereich der Wissenschaft sollte als gutes Beispiel für die Gesellschaft voran gehen.

Tabelle A.10.: Zielgruppe: Studierende

t

B. Awareness Controls

Controls die Richtlinien verlangen:

5.1 - Informationssicherheitspolitik und -richtlinien (in Policy definiert)

5.2 - Informationssicherheitsrollen und -verantwortlichkeiten (in Policy Definiert)

5.10 - Zulässiger Gebrauch von Informationen und anderen damit verbundener Werte

5.12 - Klassifizierung von Informationen

5.14 - Informationsübermittlung

5.15 - Zugangssteuerung

5.19 - Informationssicherheit in Lieferantenbeziehungen

5.23 - Informationssicherheit für die Nutzung von Cloud-Diensten

5.32 - Geistige Eigentumsrechte

5.34 - Datenschutz und Schutz personenbezogener Daten (pbD)

6.7 - Remote-Arbeit

7.7 - Aufgeräumte Arbeitsumgebung und Bildschirmsperren

7.10 - Speichermedien

8.1 - Endpunktgeräte des Benutzers

8.8 - Handhabung von technischen Schwachstellen

8.10 - Löschung von Informationen

8.13 - Sicherung von Informationen

8.15 - Protokollierung

8.24 - Verwendung von Kryptographie

8.25 - Lebenszyklus einer sicheren Entwicklung

Controls die „be aware of” verlangen:

5.4 - Verantwortlichkeiten der Leitung

5.10 - Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

5.13 - Kennzeichnung von Informationen

5.31 - Juristische, gesetzliche, regulatorische und vertragliche Anforderungen

6.3 - Informationssicherheitsbewusstsein, -ausbildung und -schulung

6.8 - Meldung von Informationssicherheitsereignissen

7.6 - Arbeiten in Sicherheitsbereichen

8.1 - Endpunktgeräte des Benutzers

8.2 - Privilegierte Zugangsrechte

Controls die “Provide awareness” verlangen:

5.7 - Informationen über die Bedrohungslage

5.19 - Informationssicherheit in Lieferantenbeziehungen

5.20 - Behandlung von Informationssicherheit in Lieferantenvereinbarungen

5.27 - Erkenntnisse aus Informationssicherheitsvorfällen

6.3 - Informationssicherheitsbewusstsein, -ausbildung und -schulung

8.7 - Schutz gegen Schadsoftware

8.8 - Handhabung von technischen Schwachstellen

C. Mapping Medium mit Lerntyp laut Vester

Medium	**Lerntyp nach Vester**			
	Visuell	**Auditiv**	**Haptisch**	**Intellektuell**
Audioaufnahme		X		
Aufkleber	X			
Ausstellung	X	X		X
Broschüre	X			
E-Mails	X			X
Fachzeitschriften	X			
Fragebögen	X			X
Handzettel	X			
Interaktive Lernprogramme	X	X	X	X
Intranet	X			
Live-Hacking	X		X	X
Newsletter	X			
Orientierungsveranstaltungen	X	X		
Poster	X			
Remote Training Labs	X			X
Richtlinien und Arbeitsanweisungen	X			
Schulungsveranstaltungen	X	X	X	X
Simulierte Phishing-Angriffe	X		X	X
Sonderveranstaltungen	X	X	X	X
Spielifikation	X		X	X
Tabletop-Übungen	X		X	X

Telefonkonferenzen		X		
Training-in-the-job			X	X
Videos	X	X		
Zertifikate	X			

D. Mapping Medium mit Lerntyp laut Schrader

Medium	**Lerntyp laut Schrader**				
	Theoretiker	**Anwend.-orientierte**	**Muster-schüler**	**Gleich-gültige**	**Unsichere**
Audioaufnahme		X		X	
Aufkleber				X	
Ausstellung	X	X			
Broschüre	X				X
E-Mails	X	X			X
Fachzeitschriften	X				
Fragebögen	X	X	X		
Handzettel	X				X
Interaktive Lernprogramme		X	X		
Intranet	X	X			
Live-Hacking		X			X
Newsletter	X				X
Orientierungsveranstaltungen		X	X		X
Poster				X	
Remote Training Labs		X			
Richtlinien / Arbeitsanweisungen	X				X
Schulungsveranstaltungen		X	X		X
Simulierte Phishing-Angriffe		X			X
Sonderveranstaltungen		X	X		X
Spielifikation		X			
Tabletop-Übungen		X			
Telefonkonferenzen	X				X
Training-in-the-job		X	X		
Videos		X	X		
Zertifikate			X		X
$\sum$	**9**	**16**	**13**	**6**	**9**

Tabelle D.2.: Zuordnung der Medien zu den Lerntypen

E. Umfrage - IST-Stand Security Awareness an Hochschulen

E.1. Informationssicherheit Allgemein

1. **Beschäftigt sich Ihre Einrichtung mit dem Thema Informationssicherheit?**

   ○ Ja ○ Nein

2. **Wie ausgeprägt ist die Auseinandersetzung mit dem Thema Informationssicherheit?**

   ○ Keine Maßnahmen vorhanden

   ○ Maßnahmen für Teilbereiche vorhanden (z.B. Passwortrichtlinien)

   ○ Maßnahmen umfänglich vorhanden (z.B. Aufbau eines ISMS)

   ○ ISMS ist vorhanden und wird gelebt und geprüft

E.2. Awareness Maßnahmen

3. **Sind Awareness Maßnahmen im Bereich der Informationssicherheit implementiert?**

   ○ Ja ○ Nein

4. **Welche Methoden werden eingesetzt?**

   ☐ Phishing Simulationen

   ☐ Präsenz Workshops

   ☐ Online Workshops

   ☐ E-Learnings

   ☐ Plakate/Broschüren

   ☐ Sonstiges _____

5. **Welche Personengruppen nehmen daran teil?**

   ☐ Hauptberufliche Mitarbeitende

   ☐ Nebenberufliche Lektor:innen

- ☐ Studierende
- ☐ Forschende
- ☐ Sonstiges _____

6. **Erachten Sie diese Maßnahme an Ihrer Einrichtung wirksam bzw. ausgereift?**

   ○ Ja ○ Nein

7. **Was sollte aus Ihrer Sicht geändert werden?**

   - ☐ Häufigkeit erhöhen
   - ☐ Inhalte überarbeiten
   - ☐ Erfolge messen/auswerten
   - ☐ Sonstiges _____

E.3. Security Awareness Tools

8. **Haben Sie Tools für Security Awareness im Einsatz?**

   ○ Ja ○ Nein

9. **Welche Tools verwenden Sie?**

   - ☐ KnowBe4
   - ☐ Cofense (früher PhishMe)
   - ☐ Proofpoint Security Awareness Training
   - ☐ Hoxhunt
   - ☐ Mimecast Awareness Training
   - ☐ Microsoft Defender for Office 365
   - ☐ PhishLabs
   - ☐ Barracuda PhishLine
   - ☐ LastPass Security Awareness Training
   - ☐ Elevate Security
   - ☐ CyberRiskAware
   - ☐ SANS Security Awareness Training
   - ☐ Infosec IQ
   - ☐ ESET Cybersecurity Awareness Training
   - ☐ MetaCompliance
   - ☐ SoSafe

☐ Sonstiges _____

E.4. Weitere Anregungen

10. **Gibt es etwas, das Sie gerne noch teilen würden?**

Ihre Antwort eingeben

F. Umfrage - IT-Verständnis und Erhebung des Schulungsbedarfs (FH St. Pölten)

F.1. Verständnis IT-Security

1. Verwenden Sie SMIME?
   - ○ Ja
   - ○ Nein
2. Wissen Sie wozu Cookies dienen?
   - ☐ Tracking
   - ☐ Verschlüsselung
   - ☐ Virenschutz
3. Waren Sie schon einmal von Phishing betroffen?
   - ○ Ja
   - ○ Nein
4. Welches der folgenden Passwörter erachten Sie als sicher?
   - ☐ 1IvessPl9
   - ☐ Ich_verwende_ein_super_sicheres_Passwort!1
   - ☐ MeinPasswort1
   - ☐ Pa$$w0rD

Interesse für neue Technologien

5. Welche der nachstehenden Technologien beziehungsweise Lösungen haben Sie privat oder beruflich im Einsatz?
   - ☐ Cloud
   - ☐ Onlinebanking

- ☐ KI-gestützte Tools & Assistenten (z.B. Grammarly, Copilot)
- ☐ ChatGPT oder andere Sprachmodelle
- ☐ Nutzung von Mehr-Faktor-Authentifizierung
- ☐ IoT-Geräte (z.B. vernetzte Haushaltsgeräte, smarte Überwachungskameras)
- ☐ Browsererweiterungen
- ☐ Wearables & Gesundheits-Tracking (z.B. Smartwatches, Fitness-Tracker)
- ☐ Passwortmanager (z.B. Bitwarden, LastPass)
- ☐ VPN & Datenschutz-Tools (z.B. NordVPN, ProtonMail)
- ☐ Blockchain & Kryptowährungen (Wallets, Smart Contracts)
- ☐ Digitale Notiz- und Organisations-Apps (z.B. Notion, Evernote, OneNote)
- ☐ E-Learning-Plattformen (z.B. Udemy, Coursera, LinkedIn Learning)
- ☐ Sonstiges: _____

F.2. Informationssicherheit

Unter Informationssicherheit versteht man den **Schutz von Informationen** jeglicher Art vor Gefahren oder Bedrohungen. Sie dient der Vermeidung wirtschaftlicher Schäden und der Minimierung von Risiken.
Dabei wird ein ganzheitlicher Ansatz verfolgt, es werden also alle Informationen betrachtet, die für die Organisation von Bedeutung sind, unabhängig davon, wie oder wo diese Informationen verarbeitet oder gespeichert werden.

6. Würden Sie sich interessiert am Thema „Informationssicherheit“ beschreiben?
   - ○ Ja
   - ○ Teilweise
   - ○ Nein

F.3. Weiterbildung

7. Was ist Ihre bevorzugte Art der Wissensvermittlung bzw. des Lernens?
   - ☐ Online Vorträge/Workshops
   - ☐ Präsenz Vorträge/Workshops
   - ☐ E-Learnings
   - ☐ Newsletter
   - ☐ Blogbeiträge

- ☐ Magazine (Printmedien)
- ☐ Sonstiges: _____

F.4. Schulungen für IT-Sicherheit

8. Haben Sie in der Vergangenheit bereits Schulungen zum Thema „IT-Sicherheit“ besucht?
   - ○ Ja
   - ○ Nein
9. Hat es Ihnen gefallen?
   - ○ Ja
   - ○ Teilweise
   - ○ Nein
10. Haben Sie in Zukunft Interesse an Workshops zum Thema Informationssicherheit teilzunehmen?

    (z. B. „Sicher Surfen“)
    - ○ Ja
    - ○ Vielleicht (Themenabhängig)
    - ○ Nein

F.5. Informationen zu IT-Sicherheit

11. Haben Sie Interesse Informationen bezüglich IT-Sicherheit zu erhalten?
    - ○ Ja
    - ○ Nein
12. Über welches Medium würden Sie diese Informationen gerne erhalten?
    - ☐ E-Mail Newsletter
    - ☐ Teamwork Beiträge
13. In welcher zeitlichen Frequenz würden Sie sich über diese Informationen wünschen?
    - ○ Monatlich
    - ○ einmal im Quartal
    - ○ Halbjährlich

F.6. Weitere Anregungen

14. Gibt es etwas, das Sie gerne noch teilen würden?

G. Ergänzende Unterlagen

Der Arbeit wird eine Excel Datei beigelegt, welche weitere Informationen über den praktischen Teil dieser Arbeit besitzt.