Studie im Rahmen des KIRAS/K-PASS Forschungsprogrammes

CLEMENTINE: Cybersecurity-Literacy in der Wissensvermittlung der Sekundarstufe in Österreich

Autor:innen:

Beatrix Wais-Zechmann

Cornelia Gerdenitsch

Stephanie Schwarz

Christine Wahlmüller-Schiller

Martin Latzenhofer

Petra Kölndorfer

Valentine Auer

Benjamin Brandic

Michael Steiner

Helmut Sidlo

FFG-Projektnummer: 914120

Das Projekt *„CLEMENTINE“* wurde im Rahmen des Sicherheitsforschungs-Förderprogramms KIRAS/K-PASS durch das Bundesministerium für Finanzen gefördert bzw. finanziert und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt.

Bundesministerium Finanzen

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

K-PASS

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACL – Access Control List
ACSF – Australian Cyber Security Framework
AHS – Allgemeinbildende Höhere Schule
AI – Artificial Intelligence
AIT – Austrian Institute of Technology GmbH
ANIF – Angewandtes Informationsmanagement
ARP – Address Resolution Protocol
ASLR – Address Space Layout Randomization
BIOS – Basic Input/Output System
BKA – Bundeskriminalamt
BMBWF – Bundesministerium für Bildung, Wissenschaft und Forschung
BMI – Bundesministerium für Inneres
BMLV – Bundesministerium für Landesverteidigung
BMF – Bundesministerium für Finanzen
BMS – Berufsbildende mittlere Schule / Fachschule für wirtschaftliche Berufe
BSI – Bundesamt für Sicherheit in der Informationstechnik
CEN – Europäisches Komitee für Normung
CERT – Computer Emergency Response Team
CFI – Control Flow Integrity
CISO – Chief Information Security Officer
CSA – Cybersecurity Austria
CSP – Cyber Sicherheit Plattform
CSS – Cascading Style Sheets
CTF – Capture the Flag
DACH – Deutschland, Österreich, Schweiz
DB – Database / Datenbank
DHCP – Dynamic Host Configuration Protocol
DigComp – Digital Competence Framework for Citizens
DigCompEdu – Digital Competence Framework for Educators
DNS – Domain Name System
DOS/DDOS – Denial of Service / Distributed Denial of Service
DSGVO – Datenschutz-Grundverordnung
e-CF – European e-Competence Framework
EC3 – Europol Cybercrime Centre
ECSF – European Cybersecurity Skills Framework
ECSO – European Cyber Security Organisation
ELK – Elasticsearch, Logstash, Kibana
ENISA – European Union Agency for Cybersecurity
EntreComp – Entrepreneurship Competence Framework
EQF – Europäischen Qualifikationsrahmen
FH – Fachhochschule
FIDO – Fast IDentity Online
FLOSS – Free/Libre and Open Source Software
FW – Fachschulen für wirtschaftliche Berufe
GPO – Group Policy Object
HAK – Handelsakademie
HAS – Handelsschule
HLW – Höhere Lehranstalt für wirtschaftliche Berufe
HTTP(S) – Hypertext Transfer Protocol (Secure)
ICDL – International Certification of Digital Literacy
ICMP – Internet Control Message Protocol
IDS – Intrusion Detection System
iMOOX – Österreichische Bildungsplattform für Massive Open Online Courses (MOOCs)
IKT – Informations- und Kommunikationstechnologie
IOCTA – Internet Organised Crime Threat Assessment
IoT – Internet of Things

IP – Internet Protocol
IPS – Intrusion Prevention System
ISO – International Organization for Standardization
KSA – Knowledge, Skills and Abilities
KSÖ – Kompetenzzentrum Sicheres Österreich
LDAP – Lightweight Directory Access Protocol
LPD – Landespolizeidirektion
MDM – Mobile Device Management
MFA – Multi-Faktor-Authentifizierung
MOOC – Massive Open Online Course
NCSC – National Cyber Security Centre
NICE – National Initiative for Cybersecurity Education
NIST – National Institute of Standards and Technology
O*NET – Online Cybersecurity Skills Database
OCG – Österreichische Computer Gesellschaft
OER – Open Educational Resources
OMAI – Officemanagement und angewandte Informatik
ÖNORM – Österreichische Norm
OWASP – Open Worldwide Application Security Project
PH – Pädagogische Hochschule
PKI – Public Key Infrastructure
SFIA – Skills Framework for the Information Age
SIEM – Security Information and Event Management
SPoT – Single Point of Truth
StGB – Strafgesetzbuch
SQL – Structured Query Language
TCP/IP – Transmission Control Protocol / Internet Protocol
URL – Uniform Resource Locator
US-CISA – Cybersecurity and Infrastructure Security Agency
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
WAF – Web Application Firewall
WLAN – Wireless Local Area Network
WI – Wirtschaftsingenieurwesen
WINF – Wirtschaftsinformatik

Abstract

CLEMENTINE steht für Cybersecurity-Literacy in der wissEnsverMittlung dEr sekuNdarsTufe IN östErreich. Hauptziel des Projekts CLEMENTINE war es, einen Ansatz zur Vermittlung von Cybersecurity-Kompetenzen für Jugendliche im Alter von 14 bis 19 Jahren für die Sekundarstufe II, unter Einbeziehung der Anforderungen aus dem Arbeitsmarkt, zu entwickeln.

Im ersten Schritt des Projekts ging es darum, zu erheben, wer aktuell mit der Vermittlung von Cybersecurity-Kompetenzen in der Sekundarstufe II in Österreich befasst ist und welche Akteur:innen es neben den Schulen gibt. Dazu wurde nach eingehender Recherche eine kategorisierte Auflistung von Akteur:innen im Cybersecurity Bereich erstellt. Um hier ein tieferes Verständnis zu erlangen, wurden zudem qualitative Interviews mit Expert:innen (Lehrende, Schulverwaltung, Interessensvertretungen, etc.) geführt. In Fokusgruppen mit Schüler:innen wurde das Verständnis und Bewusstsein für Cybersecurity erhoben.

Im zweiten Schritt ging es um die Identifikation arbeitsbezogener Cybersecurity Themen und Anknüpfungspunkte in Lehrplänen und Schulmaterialien der Sekundarstufe II in Österreich, mit dem Ziel, Rahmenbedingungen für effektive und Vermittlungsstrategien zu erarbeiten und Potenziale für die Integration von Cybersecurity Themen im Unterricht der Sekundarstufe II zu analysieren. Als Hauptergebnis liegt jetzt ein Vorschlag für inhaltliche Anpassungen der aktuellen Lehrpläne der AHS, HAK und HTL für die höhere- und mittlere Fachschul-Ausbildung und gleichzeitig wurde im Projekt das CLEMENTINE-6-Stufen-Kompetenzmodell für Cybersecurity entwickelt.

Dritter Schritt war die Erarbeitung von exemplarischen didaktischen Konzepten zur Vermittlung von Cybersecurity Themen sowie deren Anknüpfungspunkte im Unterricht im Bereich der Sekundarstufe II in Österreich. Das Ergebnis sind fundierte didaktische Ansätze, eine klare Einteilung und Darstellung digitaler Bildungsmedien sowie eine digitale Übersicht über aktuelle Vermittlungsformate in Form eines Padlets. Digitale Medien stellen einen wirksamen Beitrag zur Cyber-Sicherheitsbildung dar, wenn sie altersgerecht, interaktiv und praxisnah eingesetzt werden. Gamification (ein spielerischer Lern-Ansatz) ist für die Praxis sehr empfehlenswert. Während einfache Informationsmedien eine solide Wissensbasis schaffen, fördern gamifizierte Anwendungen Motivation und Verhaltensänderung der Lernenden. Das ist insbesondere für die Zielgruppe der 14 bis 19-jährigen Teenager sehr zielführend.

Resultierend aus allen Vorarbeiten hat das Projektkonsortium mit den Partnern AIT Austrian Institute of Technology, Center for Technology Experience (Projektleitung) und Center for Digital Safety & Security, ÖIAT (Österreichisches Institut für Angewandte Telekommunikation) und dem Bildungsministerium, gemeinsam mit dem FLL (Future Learning Lab), im Projekt CLEMENTINE aus allen diesen Ergebnissen detaillierte Handlungsempfehlungen für die drei Gruppen Bildungspolitik, Schulleitung und Lehrkräfte erarbeitet.

Die Handlungsempfehlungen betreffen sowohl Basisvoraussetzungen im schulischen Kontext, Lehrkräftequalifizierungsansätze, die Einbindung von externen Expert:innen (auch weibliche Role Models) sowie didaktische Aspekte. Im Zuge der aktuellen bzw. anstehenden Lehrplanreformen wird aus den Erkenntnissen des Projekts CLEMENTINE empfohlen, die Adaptierungsvorschläge auf Basis der Lehrplananalysen aufzugreifen, um Cybersecurity-Kompetenzen entsprechend im Lehrplan zu verankern. Gleichzeitig sollte der Austausch zwischen Schulen und Stakeholder:innen aus der Praxis künftig vertieft und zu diesem Zweck ein Expert:innen-Pool aufgebaut werden.

1 Einleitung

1.1 Ausgangssituation

Im Zuge der Digitalisierung verlagern sich zahlreiche Arbeitsbereiche – etwa Management-, Organisations- und Betriebsprozesse – zunehmend in den digitalen Raum (Cascio & Montealegre, 2016). Diese Entwicklung geht mit einer wachsenden Anzahl potenzieller Angriffsflächen für IT-Systeme einher. So stieg die Zahl der Cyberangriffe auf Unternehmen in Österreich im Jahr 2023 im Vergleich zum Vorjahr um 201 % (KPMG Austria, 2023). Entsprechend gewinnt Cybersecurity ebenso wie die damit verbundenen Kompetenzen von Arbeitskräften zunehmend an Bedeutung.

Untersuchungen zeigen, dass ein Großteil der Cyberangriffe auf menschliches Verhalten zurückzuführen ist, was weltweit zu erheblichen finanziellen Schäden führt (Aldawood & Skinner, 2018). Besonders zielen Angriffe auf menschliche Verhaltensmuster ab – etwa durch Social-Engineering-Techniken wie z.B. Phishing (Mits, 2023). Hinzu kommt, dass neue Technologien wie Künstliche Intelligenz (KI) zusätzliche Unsicherheiten erzeugen (Coeckelbergh, 2020) und neue Angriffsmuster ermöglichen. Organisatorische Cybersecurity umfasst daher nicht nur technische Schutzmaßnahmen, sondern erfordert auch die Förderung sicherheitsbewussten Verhaltens und gezielte Schulungen der Mitarbeitenden (Gerdenitsch et al., 2023; Zwilling et al., 2022). Diese Entwicklungen unterstreichen die Dringlichkeit, das Bewusstsein für Cybersecurity zu stärken und einen verantwortungsvollen Umgang mit digitalen Technologien am Arbeitsplatz zu fördern.

Gleichzeitig verbringen Kinder und Jugendliche immer mehr Zeit online (Statistik Austria, 2022), während die gesellschaftlichen Anforderungen an Cybersecurity-Kompetenzen stetig zunehmen. Für eine effektive Sensibilisierung Jugendlicher ist die Integration entsprechender Themen in den Schulunterricht unerlässlich (Mouheb et al., 2019). Dabei können auch Gamification-Ansätze (Deterding et al., 2011a) unterstützend wirken, indem sie die spielerische Motivation gezielt aufgreifen (Hendrix et al., 2016). Um junge Menschen adäquat auf die Anforderungen der digitalen Arbeitswelt vorzubereiten, kommt der schulischen Bildung eine Schlüsselrolle zu. Entscheidend ist hierbei, Cybersecurity-Inhalte ansprechend, motivierend und didaktisch wirksam zu vermitteln.

Bislang werden diese Kompetenzen im schulischen Kontext unzureichend vermittelt und Jugendliche demnach nicht ausreichend auf die spezifischen Herausforderungen im späteren Berufsleben vorbereitet. Genau hier setzt das Forschungsprojekt *CLEMENTINE* an und liefert erste Analysen und Konzepte.

1.2 Zielsetzungen im Projekt

Um den beschriebenen Herausforderungen zu begegnen, wurde im Rahmen des Projekts *CLEMENTINE* ein Ansatz zur Vermittlung von Cybersecurity-Kompetenzen für Jugendliche im Alter von 14 bis 19 Jahren für die Sekundarstufe II, unter Einbeziehung der Anforderungen aus dem Arbeitsmarkt, entwickelt.

Die Entwicklung des Ansatzes basierte auf mehreren methodischen Zugängen: Es wurden relevante Akteur:innen identifiziert, Expert:innen sowie Jugendliche befragt und bestehende pädagogische Ansätze systematisch gesammelt. Darüber hinaus wurden Lehrpläne und Schulmaterialien analysiert und darauf aufbauend didaktische Möglichkeiten zur Integration von Cybersecurity in die schulische Bildung erarbeitet. Potenzielle Umsetzungsszenarien hinsichtlich ihrer Chancen und Barrieren wurden im Rahmen von Workshops mit Stakeholder:innen reflektiert.

Das Projekt verfolgte dabei drei zentrale Subziele:

1) Erlangung eines **strukturierten Überblicks über wesentliche Akteur:innen** für die Vermittlung von Cybersecurity-Kompetenzen in der Sekundarstufe II in Österreich
2) Identifikation **arbeitsbezogener Cybersecurity Themen** und **Anknüpfungspunkte in Lehrplänen und Schulmaterialien** der Sekundarstufe II in Österreich
3) Erarbeitung von **exemplarischen didaktischen Konzepten** zur Vermittlung von Cybersecurity Themen sowie deren Anknüpfungspunkte im Unterricht im Bereich der Sekundarstufe II in Österreich

1.3 Struktur des Berichtes

In diesem Bericht wird zunächst in Abschnitt 2 eine fundierte Begriffsdefinition von Cybersecurity vorgenommen, um eine klare Grundlage für die weiteren Ausführungen zu schaffen.

Abschnitt 3 widmet sich den beteiligten Akteur:innen und ihren unterschiedlichen Perspektiven. Hierbei wird zunächst ein strukturierter Überblick über die zentralen Akteur:innen gegeben, die in diesem Themenfeld in Österreich eine Rolle spielen. Anschließend werden die Ergebnisse aus den geführten Interviews und Fokusgruppen präsentiert, die mit Jugendlichen, Expert:innen sowie Vertreter:innen des Arbeitsmarkts (CISOs) aus den Branchen Energie, Handel und Banken geführt wurden. Diese ermöglichen einen vielfältigen Einblick in Erwartungen, Herausforderungen und Vermittlungskonzepte an Cybersecurity-Kompetenzen.

Darauf aufbauend fasst Abschnitt 4 die wesentlichen arbeitsbezogenen Cybersecurity-Themen zusammen, die für die Vorbereitung junger Menschen auf die Arbeitswelt aus heutiger Sicht relevant sind und sich im Lehrplan der Sekundarstufe II widerspiegeln sollten.

Im Anschluss folgt Abschnitt 5, der sich mit der Analyse bestehender Lehrpläne sowie ausgewählter Schulmaterialien auseinandersetzt. Dabei wird nicht nur der aktuelle Stand der Vermittlung von Cybersecurity-Inhalten dargestellt, sondern auch Empfehlungen zur Adaptierung aufgezeigt.

Schließlich wird in Abschnitt 6 eine Übersicht über didaktische Konzepte gegeben sowie exemplarische, didaktische Ansätze vorgestellt, die innovative Wege aufzeigen, Cybersecurity-Themen im Unterricht zu verankern.

Zudem gibt Abschnitt 7 einen Überblick über Medienformate in der Cybersecurity-Bildung, analysiert ausgewählte Medienformate, zeigt Strategien für deren curriculare Integration und gibt eine im Projekt entwickelte Mediensammlung in Form eines Padlets.

In Abschnitt 8 gibt der Bericht ein Fazit, das die wesentlichen Erkenntnisse zusammenführt, dabei die Ergebnisse der abgehaltenen Interviews und Workshops mit den beteiligten Stakeholder:innen integriert und Handlungsempfehlungen für die weitere Entwicklung und Implementierung von Cybersecurity-Vermittlungsansätzen für 14 bis 19-jährige Schüler:innen in Österreich ausspricht.

Der Bericht schließt in Abschnitt 9 mit einer Zusammenfassung und einem Ausblick.

2 Der Begriff Cybersecurity

2.1 Begriffsdefinition Cybersecurity

Für den Begriff Cybersecurity existiert keine umfassende allgemeingültige Definition, vielmehr hat sich dieser Terminus aus dem Kontext der Disziplin Informations- und Kommunikationstechnologie (IKT) evolutionär entwickelt. Ursprünglich am Beginn der 1990er-Jahre etablierte sich der weitgehend technikbezogene Begriff **Informationstechnologiesicherheit (IT Security)**. Aus dieser Zeit stammt die Interpretation, dass IT Security sich aus drei bis fünf Subzielen (genannt Security-Mechanismen) zusammensetzt (Pfleeger, 1997). Aus den ersten drei wurde der bekannte „CIA-Ansatz" abgeleitet (von den Anfangsbuchstaben der englischsprachigen Begriffe):

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)
- Optional: Authentizität (Authenticity)
- Optional: Nicht-Abstreitbarkeit (Non-Repudiation)
- *Später*, ebenso optional: Privacy (Datenschutz)

Diese rein technische Interpretation griff offensichtlich zu kurz, und man erweiterte die Perspektive auf die Information an sich, die geschützt werden soll – also auch analoge Informationsträger wie Papier– sowie auf den Umgang der Information durch Menschen. Dieser zusätzliche Fokus auf Prozesse, Richtlinien und Informationsweitergabe manifestierte sich im Begriff der **Informationssicherheit (Information Security)**. Nichtsdestotrotz wurde immer noch ein Ansatz der Perimetersicherheit verfolgt, d.h. Information wird durch Menschen, Prozesse, Geräte innerhalb einer definierten Umgebung (zumeist die Organisation, für die man arbeitete) verarbeitet. Mit dem um die 2000er-Jahre aufkommenden Outsourcing der Informationstechnologie musste der Informationsaustausch auch formalisiert geregelt werden, also von einem definierten Bereich (Kundenorganisation) zu einem anderen (IT-Dienstleister). In diese Zeit fällt auch der zumindest in Mitteleuropa sukzessiv verstärkte Datenschutzgedanke.

Durch die aufkommende Vernetzung, speziell durch mobile Geräte, verschwammen die Grenzen der speziell geschützten Bereiche zusehends. Zudem wurde jede Komponente, die das Internet-Protokoll (Internet Protocol, IP) „sprach" ein potenzielles Informationssicherheitsrisiko und die Perimetersicherheit funktionierte so nicht mehr effektiv. Einerseits drängten zuvor abgeschirmte Komponenten, wie z.B. produktionsnahe Leitsysteme (Operational Technology), Steuergeräte aus dem privaten Bereich (Smart Home), kleinteilige massenhaft verfügbare Umgebungssensorik (Internet of Things, IoT) gewissermaßen in die IT, andererseits wurden dadurch unzählige neue Funktionen „remote" – also von der Ferne – nutzbar. Ermöglicht wurde dies auch durch die Zunahme der technischen Leistungsfähigkeit der mobilen Netze (Mobilfunk, Wireless Local Area Networks, WLAN) und der Kapazitätszunahme in den Backbones[1]. Gleichzeitig forcierte die Implementierung vieler neuer Prozesse, Produkte, Funktionalitäten sowie die enge verzahnte Vernetzung über die ursprünglichen Organisationsgrenzen hinaus eine Verlagerung von diversen Anwendungen und Services in eine digitale Welt. Diese disruptive Komplexitätszunahme – ausgelöst durch den verstärkten Kommunikationsaspekt und die Digitalisierung – transferierte den Informationssicherheitsbegriff zur **Cybersicherheit (Cybersecurity)**.

Der Begriff Cybersecurity hat sich aus der Historie heraus also fließend entwickelt und mündet ebenso nicht in eine eindeutige Definition. Hier einige Definitionsbeispiele:

- Die US Cybersecurity & Infrastructure Agency (US-CISA) versteht Cybersecurity als „*die Kunst Netzwerke, Systeme, Geräte, Daten und sensible Informationen vor unautorisiertem Zugang oder kriminellen Verwendungen zu schützen und die Vertraulichkeit und Verfügbarkeit von Informationen zu bewahren"* (Pfleeger, 1997). Dies ist eine sehr wertorientierte Definition, die sich also mehr auf die Werte (Assets) in einem Informationsnetzwerk bezieht.
- Der IT-Konzern IBM konstatiert, dass „*Cyber-Security-Maßnahmen darauf ausgelegt sind Bedrohungen gegen vernetzte Systeme und Anwendungen zu bekämpfen, unabhängig davon, ob diese von innerhalb oder außerhalb einer Organisation ausgehen"* (IBM, n.V.). In dieser Annäherung wird der Bedrohungsansatz betont, der von außen die Assets stets in ihrer Integrität bedroht.
- Der EU-Cybersicherheitsakt besagt, dass „*Cybersicherheit nicht nur eine Frage der Technologie ist, sondern eine, bei der das menschliche Verhalten ebenso wichtig ist"* und beschreibt diesen Begriff als „*alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die NutzerInnen solcher*

[1] https://de.wikipedia.org/wiki/Backbone_%28Telekommunikation%29

Systeme und andere von Cyberbedrohungen betroffenen Personen zu schützen" (Bundeskanzleramt, n.V.; European Commission, 2019). Diese Definition rückt neben der andauernden Bedrohung für die Assets den menschlichen Akteur und sein Verhalten in den Vordergrund.

- Die EU-Agentur für Cybersecurity (*ENISA*) meint: „*Cybersecurity umfasst alle Aktivitäten, die erforderlich sind, um den Cyberspace, seine Nutzer und die betroffenen Personen vor Cyber-Bedrohungen zu schützen, sowie alle Aspekte der Prävention, Vorhersage, Toleranz, Erkennung, Schadensbegrenzung, Beseitigung, Analyse und Untersuchung von Cyber-Vorfällen"* (Tirtea, 2017). Die ENISA anerkennt, dass es sich bei Cybersecurity um ein umfassendes Ökosystem handelt, in dem sich die Akteure bei der Nutzung der Technik einfügen.

Für das Projekt *CLEMENTINE* greifen die obigen Definitionen nach Ansicht der Autor:innen durchwegs zu kurz. Insbesondere soll das statische Element (Assets) grundsätzlich geschützt werden (Schutzziele). Die vernetzte (weil Grenzen verschwimmen) und komplexe Charakteristik (weil auf diversen Ebenen vonstattengehend, z.B. Physik, Technik, Organisation, Mensch, Prozess, Produkt, Funktionalitäten, Zusammenspiel mit Partnern, sowie vor allem die Kommunikation in Kombination mit dem Verhalten der Menschen) führt zu einem hochgradig dynamischen Umfeld, das sich evolutionär in einer immensen Geschwindigkeit entwickelt hat und die Gesellschaft vor immer wieder neue Herausforderungen stellt. Diese spezifische Kombination aus Verhalten und Kommunikation spannt unmittelbar eine große Bandbreite an Angriffsvektoren und Schwachpunkten auf und die Menschen, die sich in der digitalen Welt bewegen möchten, sind dazu angehalten, sich darin möglichst friktionsfrei zu bewegen, während sich die Rahmenbedingungen ständig weiterentwickeln.

Im Rahmen einer MindMap (siehe Abbildung 1) haben wir uns dem Begriff Cybersecurity angenähert. Im Sinne der oben diskutierten Definitionsproblematik wurden die unterschiedlichen Einflussfaktoren kategorisiert und herausgearbeitet. Zunächst ist das *Asset* ausschlaggebend, der eigentlich zu schützende Wert. Dabei ist es unerheblich, ob dieser Wert eine Hardware, Software, Prozesse, Personen, Informationen darstellt. Die *Sicherheit*, der Schutz manifestiert sich in den sogenannten Schutzzielen, in der Informationstechnologie-, Informations- und letztlich Cyber-Sicherheit traditionellerweise Vertraulichkeit, Integrität, Verfügbarkeit und als Erweiterung Authentifizierung, Nicht-Abstreitbarkeit und eventuell Datenschutz. Durch die disruptiven Entwicklungen im Bereich der *Kommunikation* und demgemäß den Kollaborationsmöglichkeiten erfolgte auch ein Umdenken im Sicherheitsparadigma, z.B. weg von der Perimeter-Sicherheit („Systemaußengrenzen schützen") hin zum Zero-Trust-Ansatz („Niemandem wird vertraut"). Die mit der Kommunikation einhergehende Auflösung der Systemgrenzen betont auch *Verhalten*saspekte der Nutzenden. Treibende Faktoren hier sind die Sicherstellung der Identität, des Bewusstseins, der Fähigkeiten und der Usability. Beide Einflussfaktoren stellen in Kombination die heute dominierende Angriffsfläche dar. Security-*Maßnahmen* sind demgemäß auch sehr vielschichtig, sie können technischer, organisatorischer und auch persönlicher Natur sein. Aufgrund des sich hochdynamischen und komplexen Themenfelds Digitalisierung und Cybersicherheit erfordert eine *kontinuierliche Verbesserung* rasche Änderungs- und Anpassungsfähigkeit.

Auf Basis dieser Überlegungen wurde für das Projekt die folgende Begriffsdefinition formuliert:

Definition Cybersecurity:

Unter den Begriff Cybersecurity versteht man Technologien, Handlungen und organisatorische Maßnahmen, die die Sicherheit und den Schutz von Informationswerten in Form von digitalen Daten zum Ziel haben.

Cybersecurity umfasst somit verschiedene Aspekte: vom verantwortungsvollen Verhalten der Nutzer:innen über technologische Möglichkeiten, allgemeine Grundkonzepte und Kenntnisse der Abläufe und Verwendungsmöglichkeiten bis hin zur konkreten Umsetzung risikominimierender Maßnahmen.

Besonders hervorzuheben ist der Aspekt der intensiv vernetzten Kommunikation in Kombination mit dem menschlichen Verhalten bei der Nutzung von Informations- und Kommunikationstechnologie (IKT). Dies erfordert ein hohes Maß an Bewusstsein über Verantwortung, mögliche Auswirkungen und Verhaltensrichtlinien in der digitalen Welt.

Sämtliche Maßnahmen zur Sicherstellung der Cybersecurity – sei es auf persönlicher, technischer oder organisatorischer Ebene – formen ein umfassendes digitales Ökosystem, das sich kontinuierlich weiterentwickeln und anpassen muss

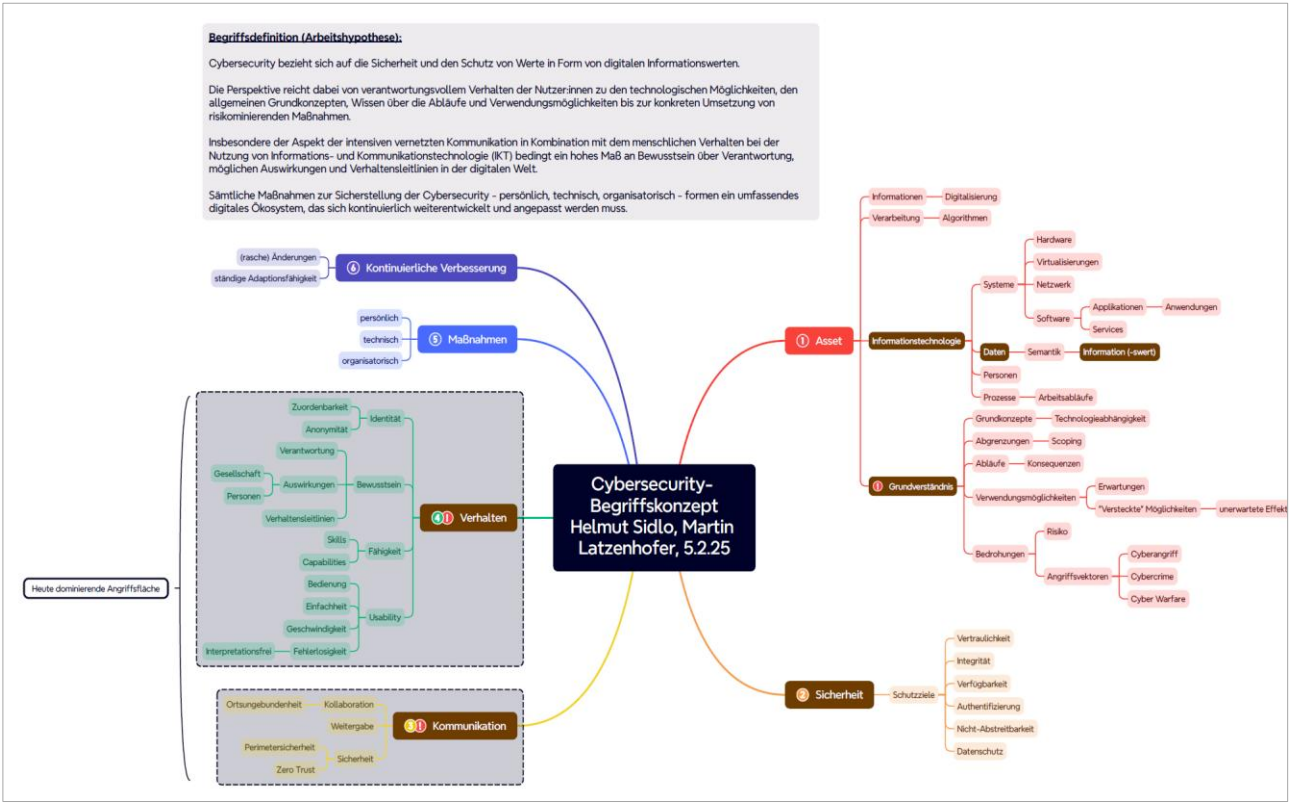

Abbildung 1: MindMap zur Begriffsdefinition von Cybersecurity

2.2 Existierende Cybersecurity Frameworks und Ansätze

Grundsätzlich versucht man dem komplexen, weil sehr breit und vielschichtig angelegten Begriff Cybersecurity einen inhaltlich strukturierten Rahmen zu geben, um daraus die diversen Anforderungen abzuleiten, die es hier insbesondere im Hinblick auf Fertigkeiten und Fähigkeiten (Skills und Capabilities) der Personen gibt. Mithilfe von Frameworks und Rahmenmodellen kann die persönliche und intellektuelle Weiterentwicklung unterstützt werden, sowohl in der Ausbildung als auch im Rahmen beruflicher Fortbildungen, gezielt Wissen zu generieren und sich anzueignen. Die nachfolgende Tabelle 1 gibt einen Abriss der Frameworks und Ansätze wieder, die im Zusammenhang mit Cybersecurity-Bildung (Literacy) relevant sind.

Tabelle 1: Zusammenfassung existierender Cybersecurity Frameworks und Ansätze

Framework	Herkunft	Zentrale Merkmale	Nutzungsintention
ECSF	EU	EU-zentriert, an den EQR angelehnt	Mobilität innerhalb der EU und Personalplanung
NICE	USA	Personalplanung, Kenntnisse-Fähigkeiten-Kompetenzen (KSA)	Nationale Rollen- und Ausbildungsabstimmung
ACSF	Australien	Personalplanung, Kenntnisse-Fähigkeiten-Kompetenzen (KSA)	Nationale Rollen- und Ausbildungsabstimmung
e-CF	EU	Breiter IKT-Bezug, EQR-Abstimmung	Qualifikationsrahmen
SFIA	UK	Allgemeine IT, Kompetenzniveaus	Abstimmung mit organisatorischen Tätigkeitsprofilen
DigComp	EU	Bürger:innen	Gesellschaft
O*NET	USA	Breite Berufsübersicht, nicht spezifisch für IKT oder Cybersecurity	Enthält Aufgaben und Wissen – auch zu Cybersecurity-Berufen

Das **European Cybersecurity Skills Framework (ECSF)** wurde von der Europäischen Agentur für Cybersecurity (ENISA) veröffentlicht und bietet eine europäische Perspektive auf Cybersecurityrollen und -fähigkeiten, um ein gemeinsames Verständnis der Anforderungen an die Belegschaft zu fördern. ECSF

umfasst zwölf professionelle Rollenprofile, wie beispielsweise „Risk Analyst“ und „Incident Responder“. Es legt besonderen Wert auf Wissen, Fähigkeiten und Kompetenzen (Knowledge, Skills, and Abilities, KSAs) für jede Rolle. Das Framework ist an den Europäischen Qualifikationsrahmen (EQF) angepasst, um die Anerkennung von Fähigkeiten und Qualifikationen in den EU-Mitgliedstaaten zu unterstützen.

Das **NICE Cybersecurity Workforce Framework (NICE Framework)** wurde vom National Institute of Standards and Technology (NIST) in den USA veröffentlicht. Es kategorisiert Cybersecurityrollen in sieben Domänen (Workforce-Kategorien) und beschreibt 52 spezifische Arbeitsrollen. Der Aufbau des Frameworks umfasst Kategorien (als übergeordnete Gruppierungen von Cybersecurity-Arbeit), Fachgebiete (oder Specialty Areas, decken spezifische Bereiche der Cybersicherheitsarbeit ab), Arbeitsrollen (detaillierte Beschreibungen spezifischer Positionen), Wissen, Fähigkeiten und Kompetenzen (KSAs) sowie Aufgaben, die sowohl technische als auch nicht-technische Anforderungen beschreiben.

Das **Australian Cybersecurity Framework (ACSF)** wurde von der Australian Cybersecurity Growth Network (AustCyber) veröffentlicht und bezieht sich vorrangig auf Arbeitskräfteentwicklung und Spezialisierung in Australien. Der Aufbau ähnelt dem NICE-Framework, ist jedoch speziell auf den australischen Kontext zugeschnitten. Es beinhaltet Kernkompetenzen sowie branchenspezifische Rollen.

Das **e-CF (European e-Competence Framework)** wurde vom Europäischen Komitee für Normung (CEN) veröffentlicht. Es handelt sich um ein umfassendes ICT-Framework, das auch Cybersecurityrollen und -fähigkeiten umfasst. Der Aufbau beinhaltet 41 Kompetenzen, die in fünf Dimensionen unterteilt sind, einschließlich spezifischer Rollen im Bereich Cybersecurity. Weiters zeichnet es sich durch seine Ausrichtung an den Bedürfnissen der Industrie und der Bildung auf europäischer und internationaler Ebene aus.

Das **SFIA (Skills Framework for the Information Age)** wurde von der SFIA Foundation im Vereinigten Königreich veröffentlicht. Es ist ein allgemeines Framework für ICT- und digitale Fähigkeiten, in dem Cybersecurity als Teilbereich enthalten ist. Es definiert professionelle Fähigkeiten auf sieben Verantwortungsebenen, wobei Cybersecurityrollen in die breitere Definition von IT-Fähigkeiten eingebettet sind.

Das von der EU vorgeschlagene **DigComp** (**Digital Competence Framework for Citizens)** dient als Referenzrahmen für die Entwicklung und das Verständnis digitaler Kompetenzen in der EU. Der ursprüngliche Rahmen beschreibt digitale Kompetenzen anhand drei Leistungsniveaus (Grundlagen, Mittelstufe, Fortgeschrittene) und fünf Kompetenzbereichen, wovon einer Sicherheit thematisiert. Mittlerweile wurde der Rahmen weiterentwickelt (Carretero et al., 2017) und an verschiedene Bereiche und Zielgruppen angepasst, wie zum Beispiel EntreComp für Unternehmer:innen (Bacigalupo et al., 2016), das DigCompConsumers für Verbraucher:innen (Brečko & Ferrari, 2016), Digcompedu für Pädagog:innen (Redecker, 2017) und einem Framework für Arbeitskräfte (Oberländer et al., 2020).

Die **O*NET Online Cybersecurity Skills Database** wurde vom US-amerikanischen Arbeitsministerium veröffentlicht. Sie dient als allgemeines berufliches Framework mit detaillierten Profilen für Cybersecurity Jobs. Die Struktur umfasst: Die Zuordnung von Rollen wie „Information Security Analyst“ zu den erforderlichen Fähigkeiten, Aufgaben und Technologien. Dieses Framework bietet eine systematische Übersicht über die beruflichen Anforderungen im Bereich der Cybersecurity.

3 Akteur:innen an der Schnittstelle Cybersecurity und Schule

3.1 Überblick über Akteur:innen an der Schnittstelle Cybersecurity und Schule in Österreich

Gleich zu Projektbeginn startete die Recherche zu den wesentlichen Akteur:innen an der Schnittstelle Cybersecurity und Schule in der oberen Sekundarstufe in Österreich, einerseits, um einen Überblick über beteiligte Personen, Aktivitäten und Initiativen im Themenbereich zu schaffen und andererseits, um den Akteur:innenrahmen für das Projekt festzulegen. In den folgenden Tabellen sind die wesentlichen Akteur:innen aus dem Bildungsbereich, der Forschung sowie Interessensvertretungen, Vereine & Initiativen im Kontext Cybersecurity-bezogenen Wissensaustauschs und -vermittlung im Sinne eines Gesamtüberblicks zusammengetragen, wie per 30. November 2025 ermittelt, ohne Anspruch auf Vollständigkeit (Abbildung 2).

3.1.1 Wissensvermittlung – Schulen

Organisation	Beschreibung
Mittelschule und AHS-Unterstufen	Digitale Grundbildung als Pflichtgegenstand in der Sekundarstufe I https://www.bmb.gv.at/Themen/schule/zrp/dibi/dgb.html
Schulversuch CyberHAK **Standort: Vienna Business School / VBS Floridsdorf in Wien**	Berufliche Handelsschule mit Spezialisierung auf IT & Cybersicherheit: Neben wirtschaftlicher Ausbildung erhalten Schüler:innen eine fundierte Grundausbildung in Cybersecurity/IT-Sicherheit, Sicherheitsmanagement, Recht & Wirtschaftsinformatik; Ausstattung der Klassen mit Laptops und Kooperation mit Behörden/Wirtschaft. https://www.vbs.ac.at/vienna-business-school/ausbildungszweige/cyberhak-handelsakademie-hak/
Schulversuch CyberHAK **Standort: BAK Horn / HAK Horn**	Kombination aus klassischer HAK-Wirtschaftsausbildung, Grundausbildung in Cyber-Security / IT-Sicherheit sowie öffentlich-verwaltenden Fächern. Fokus auf Sicherheits-, Gefahren- und Krisenmanagement für Unternehmen, Institutionen, Organisationen und NGOs, und auf den Schutz kritischer Infrastruktur (Energieversorgung, Hardware, Software, …) https://hakhorn.ac.at/horner-hak-schwerpunkt-auf-cyber-sicherheit/
Schulversuch CyberHAK **Standort: HAK Tamsweg**	Zusammenarbeit zwischen Pädagog:innen der HAK Tamsweg und externen Lehrbeauftragten: Expert:innen des Bundesministeriums für Inneres (Bundeskriminalamt); Expert:innen der Abteilung des Katastrophenschutz Salzburg sowie Persönlichkeiten privater Sicherheitsunternehmen. https://www.haktamsweg.at/management-cyber-security.html
HAK Digital Business	Fachbereich Wirtschaftsinformatik: in integrierter Form umfassende Allgemeinbildung, höhere kaufmännische Bildung und eine IT-Spezialausbildung. https://www.hak.cc/die-hak-has/schulformen/spezielle-ausbildungen/hak-db
HTL mit Security-Schwerpunkt **Standort: HTL Hollabrunn**	HTL mit Security-Schwerpunkt und klarem Fokus auf technischen Aspekten: Netzwerke, sichere Systeme, Programmierung als Basis für IT-Security-Techniker:in, Admin oder Entwickler:inkarriere in Sicherheitskontexten. Insbesondere Cybersecurity-Zertifikat für die IT-Klassen. https://www.htl-hl.ac.at/web/news/article/introduction-to-cybersecurity-zertifikat-fuer-die-it-klassen/
HTL St. Pölten (Informatik-Abteilung,	Ausbildungsschwerpunkt „Cyber-Security“: Unterricht in sicheren Netzwerken, Sicherheitskonzepte von Betriebssystemen,

Schwerpunkt Cyber-Security)	Netzwerksicherheit, sichere Programmierung, Big Data / KI & Sicherheitsaspekte. Kooperation mit einer Fachhochschule (FH St. Pölten) zur praxisnahen Security-Ausbildung https://www.htlstp.ac.at/2022/06/22/informatikerinnen-besuchten-cy-sec-workshop-an-der-fh-st-poelten/

3.1.2 Wissensvermittlung – (Fach)Hochschulen & Universitäten

Organisation	Beschreibung
FH Campus Wien	(berufsbegleitendes) Masterstudium „Security and Safety“ mit Schwerpunkt IT-Security bzw. Sicherheit. → siehe „Security and Safety“ bei FH Campus Wien (Cyber Security Austria)
FH Joanneum	Masterstudium „IT- und Mobile Security“ (Cybersecurity & Ethical Hacking) — Ausbildung in IT-/Mobile-Sicherheit, Software Security, Hacking, Betriebssystem- und Netzwerksicherheit. https://www.fh-joanneum.at/it-und-mobile-security/master/en/
FH Kärnten	Studienzweig Netzwerk- und Kommunikationstechnik (Bachelor), Communication Engineering (Master) https://www.fh-kaernten.at/en/study-program-1
FH OÖ (Campus Hagenberg)	Studiengänge „Sichere Informationssysteme“ (Bachelor) sowie Sicherheits-/IT-Security-Master bzw. Security Management – IT-Security, Secure Info Systems etc. https://www.fh-ooe.at/sib (Bachelor) und https://www.fh-ooe.at/sim bzw. https://www.fh-ooe.at/ism (Master)
FH Technikum Wien	Masterstudienlehrgang IT-Security (Karrierepfade Security Operator, Security Manager, Security Technical Expert) https://www.technikum-wien.at/studiengaenge/master-it-security/
FH Wiener Neustadt	Lehrgang "Cybercrime-Experte/Expertin" spezialisiert auf Cybercrime, sowie umfassendes Verständnis für Technik und Recht. https://www.fhwn.ac.at/studiengang/cyber-crime-investigation#top
Hochschule für Angewandte Wissenschaften St. Pölten	Masterstudiengang “Cyber Security and Resilience” https://www.ustp.at/de/studium/informatik-security/cyber-security-and-resilience
Pädagogische Hochschulen	Teilweise Fachbereiche für Information und Kommunikation, die digitale Bildungsinhalte im Lehramtsstudium verankern (z.B. PH Steiermark). https://www.phst.at/fortbildung-beratung/fortbildung/digitale-bildung/
Cybersecurity Campus Graz / TU Graz (IAIK)	Studienangebot & Forschung im Bereich Information Security / Cybersecurity über das Institut für angewandte Informationssicherheit (IAIK) bzw. Cybersecurity Campus; Spezialisierung auf Informationssicherheit. https://cybersecurity-campus.tugraz.at/ und https://www.iaik.tugraz.at
TU Graz, Institute of Information Security	Masterstudium mit Schwerpunkt „Information Security“ / entsprechende Studienprogramme im Bereich Informationssicherheit. https://www.isec.tugraz.at/

TU Wien	Informatikstudium (Bachelor & Master) mit Möglichkeit zur Vertiefung / Schwerpunktsetzung im Bereich Security/Cybersecurity — Kurse und Module in Security & Privacy, IT-Security, Security Engineering. https://www.tuwien.at/en/studies/studies (mit Cybersecurity-Modulen)
Universität Wien	Informatik (BSc & MSc) mit Vertiefung in Security & Privacy / Information Security — Kurse u.a. zu Network Security, Security & Privacy Engineering, Software-Security etc. https://sec.cs.univie.ac.at/
Universität Klagenfurt (AAU)	Masterstudium „Artificial Intelligence and Cybersecurity“ https://www.aau.at/studien/master-artificial-intelligence-and-cybersecurity/

3.1.3 Wissensvermittlung – kommerziell

Organisation	Beschreibung
Epicenter.academy	Workshops zur digitalen Selbstverteidigung für Schulen https://epicenter.academy/workshops/workshops-schulen
Berufsförderungsinstitut Österreich (BFI)	Basiskurs IT-Security https://www.bfi.wien/kurs/6226/K13668/itsecurity-elearning/25BTDE0449
ICDL IT-Security	ICDL Wahlmodul IT-Security angeboten durch die Österreichische Computer Gesellschaft (OCG) https://www.icdl.at/it-security
incite Ausbildungs- und Schulungsveranstaltungs GmbH	Reihe von Aus- sowie Weiterbildungen im Rahmen der gemeinsamen Initiative des Fachverbands UBIT und des BMI "GEMEINSAM.SICHER – fIT im Netz": Lehrgang "Data & IT Security", Zertifizierung zum "Certified Data & IT Security Expert" https://www.incite.at/de/suchergebnis.html?searchterm=security
ovos media gmbh	Das kostenlose Cyber Security Quiz bietet einen breiten Überblick über die Cybersecurity Herausforderungen, von Schadsoftware über Online-Betrug bis hin zu Datenschutz und Hass im Netz. https://ovosplay.com/cybersecurity-quiz/
TÜV Austria Akademie GmbH	Verschiedene Kurse und Zertifizierung zu Informations- & Cybersicherheit. https://www.tuv-akademie.at/kursprogramm/informations-cybersicherheit
Wiener Volkshochschulen	Kursangebote IKT-Sicherheit https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Aus-und-Weiterbildung/VHS.html
WIFI - Wirtschaftsförderungsinstitut der Wirtschaftskammer Österreich	Kursangebot IKT-Security (Basis, Aufbau, Zertifizierung) https://www.wifiwien.at/kurs/28102x-it-security-fuer-anwenderinnen-basis?vanr=28102025

3.1.4 Forschung

Organisation	Beschreibung
AIT Austrian Institute of Technology GmbH	Center for Safety & Security, Bereich Cyber Security Consulting & Risk Management https://www.ait.ac.at/themen/cyber-security Center for Technology Experience, Bereich Awareness Trainings & Games https://www.ait.ac.at/themen/capturing-experience/projects/dogana
FORWIT (Rat für Forschung, Wissenschaft, Innovation und Technologieentwicklung)	Unabhängige Beratung der Bundesregierung in den Politikfeldern Forschung, Wissenschaft, Innovation und Technologieentwicklung https://forwit.at/mission/
KIRAS – Sicherheitsforschungs-landkarte	Überblick über Organisationen, Unternehmen und Forschungseinrichtungen im Bereich der Sicherheitsforschung. https://www.kiras.at/landkarte/#themes:pathGroup=.forschung|category-filter:path=default|paging:number=100|paging:currentPage=0
Cybersicherheitsforschung Kybernet-Pass (K-PASS)	K-PASS unterstützt österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Gewinnung des erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Cybersicherheitsforschung Kybernet-Pass (K-PASS)
ÖIAT Research (Österreichisches Institut für Angewandte Telekommunikation)	Forschungsprojekte zu verschiedenen Bereichen der Cyberkriminalität & Cybersicherheit. https://research.oiat.at/de/
SBA Research (Secure Business Austria Research)	Österreichs größtes Forschungszentrum für Informationssicherheit, Security Services & Trainings, Networking und Wissensaustausch (z.B. Cybersecurity-Awareness Stammtisch) https://www.sba-research.org/research/research-groups/
Universität Klagenfurt (AAU)	Forschung über die Cybersecurity Research Group der Universität Klagenfurt. https://www.aau.at/digital-age-research-center/cybersecurity/
Forschungsgruppe Security and Privacy der Universität Wien	Forschungsbereiche: Distributed Ledger Technology in Kooperation mit SBA Research, Development Lifecycle of IT in Production Environments, Assurance and Transparency in Software Protection. https://sec.cs.univie.ac.at/
Vienna Cybersecurity and Privacy Research Center (ViSP)	Netzwerk bzw. Forschungs- und Lehrcluster in Wien, Lehr- und Forschungsangebote im Bereich Security & Privacy. https://informatik.univie.ac.at/en/research/projects/project/361/

3.1.5 Interessensvertretungen, Vereine & Initiativen

Organisation	Beschreibung
A-SIT Zentrum für sichere Informationstechnologie – Austria	Seit 1999 bestehender, gemeinnütziger und unabhängiger Verein, der als kompetente, neutrale Instanz für IT-/Cybersicherheit in Österreich fungiert. Mitglieder müssen öffentliche Institutionen sein: Beratung zu technischem Sicherheitsstandard, Data Protection, Kryptographie und Cyberrisiken und hat eine Rolle bei der nationalen Sicherheitsarchitektur.

	https://www.a-sit.at/
AK NÖ Onlinebetrug-Simulator (in Kooperation mit Universität Wien)	Lern- bzw. Simulationsplattform für Umgang mit Online-Betrug in sicherer, kontrollierter Umgebung. Ziel ist es, das Bewusstsein für Betrugs- und Phishing-Methoden zu schärfen. https://onlinebetrug.aknoe.at/
Austria Cyber Security Challenge (ACSC)	Jährlich abgehaltener Wettbewerb im Bereich Cybersecurity (Capture-the-Flag / CTF), organisiert von Cyber Security Austria mit Unterstützung öffentlicher Stellen. Ziel: Motivierung und Förderung von Schülerinnen, Studierenden, jungen IT-Interessierten für Cybersicherheit; Vernetzung mit Gleichgesinnten, Mentor:innen, potentiellen Arbeitgebern sowie Fachkräfteförderung für Einstiegschancen ins Fachgebiet. https://verbotengut.at/
Cyber Security Austria (CSA)	Gemeinnütziger, unabhängiger und überparteilicher Verein zur Förderung der Sicherheit kritischer bzw. strategischer Infrastruktur sowie der Sensibilisierung für Cybersecurity. CSA organisiert Initiativen, Wettbewerbe und Awareness-Projekte (v.a. Austria Cyber Security Challenge), vernetzt Stakeholder:innen aus Wirtschaft, Verwaltung und Gesellschaft und bietet Plattformen für den Erfahrungsaustausch und Weiterbildung. https://verbotengut.at/
Austrian Trust Circle (ATC)	Initiative von CERT.at und dem österreichischen Bundeskanzleramt; bestehend aus Security Information Exchanges in den einzelnen Bereichen der strategischen Informationsinfrastruktur (CIIP). https://www.austriantrustcircle.at/
“Cyberkids” des Bundeskriminalamts	Präventionsprogramm der Polizei in der Volksschule im Rahmen der Mobilitätsbildung/ Kinderpolizei für Kinder von acht bis zehn Jahren zum sicheren Umgang mit Internet und digitalen Medien. https://www.kinderpolizei.at/cyberkids/start.aspx
Cybersecurity-Awareness-Stammtisch	Gemeinnützige Initiative veranstaltet durch SBA Research und ÖIAT: zum Austausch von Praxiserfahrungen bzgl. Vermittlung von Cybersecurity-Awareness in Unternehmen gemeinsam mit CISO, Mitarbeiter:innen in IT-Abteilungen bzw. Sicherheitsbeauftragten in Unternehmen https://academy.oiat.at/event/cybersecurity-awareness-stammtisch
Cyber-Security-Initiative	Initiative des Bundesministeriums für Inneres (BMI) und Kompetenzzentrums Sicheres Österreich (KSÖ) mit dem Ziel, Awareness bei politischen Entscheidungsträger:innen, Vertreter:innen aus Behörden sowie Top-Entscheider:innen aus der Wirtschaft nachhaltig zu fördern https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Beratung-und-Sensibilisierung/Cyber-Security-Initiative.html
Cyber Sicherheit Plattform (CSP)	Dachorganisation für bestehende Kooperationsformate (u.a. KSÖ, ATC, A-SIT, CERT) gegründet im Rahmen der „Österreichischen Strategie für Cybersicherheit" (ÖSCS) für Informationsaustausch, Kooperationen zwischen Partnern; Beratung und Unterstützung der "Cyber Sicherheit Steuerungsgruppe"; Förderung der Errichtung von Sektor-spezifischen Computer Emergency Response Teams (CERTs). https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Koordination-und-Strategie/Cyber-Sicherheit-Plattform-CSP.html

Digitale Kompetenzoffensive Österreich (DKO)	Programm zur Steigerung digitaler Kompetenzen in Österreich wie u.a. Bewusstseinsbildung und Prävention gegenüber Bedrohungen durch Cyberkriminalität (Cybercrime). https://www.digitalaustria.gv.at/verwaltung/sicherheit/cybersicherheit.html
fit4internet.at (f4i)	Verein zur Förderung digitaler Kompetenzen in Österreich in Anlehnung an das Digitale Kompetenzmodell für Österreich – DigComp AT, „Kompetenzbereich 4 Sicherheit und nachhaltige Ressourcennutzung“ https://www.fit4internet.at/view/verein
Future Learning Lab (FLL)	Verein zur Förderung digitaler Bildungsangebote; betreibt in Zusammenarbeit mit der PH Wien das Future Learning Lab Wien (FLL.wien) als zertifizierter eEducation.Expert.Partner für Bildungsangebote für Schulen, Lehrpersonen, Erwachsene und Unternehmen https://futurelearning.at/
Initiative Cybersecurity des Kompetenzzentrum Sicheres Österreich (KSÖ)	Standardentwicklung für ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der gesamten EU: Zertifizierung über Cyber Trust Austria und das CyberRisk Rating by KSV1870. https://kompetenzzentrum-sicheres-oesterreich.at/initiativen/cybersecurity/
ISACA Austria Chapter	Verein und lokales Chapter der ISACA International (Information Systems Audit and Control Association), fördert professionelle Standards und Methoden in den Bereichen IT-Audit, IT-Governance, Compliance, Risikomanagement und IT-Kontrollen in Österreich. Angebote: Weiterbildung, Networking, Erfahrungs- und Wissensaustausch mit Fachleuten aus Wirtschaft, Verwaltung und Wissenschaft. https://engage.isaca.org/austriachapter/home
Kompetenzzentrum eEducation Austria	Zentrale Säule für digitale Bildung in Österreich — von der Volksschule bis zur Matura. Fokus liegt auf digitaler Grundbildung, Medienkompetenz und informatischer Bildung. https://eeducation.at/community/kompetenzzentrum
Österreichische Computergesellschaft (OCG), Arbeitskreis IT-Sicherheit	Der Arbeitskreis widmet sich den Gebieten Informationssicherheit und IT-Sicherheit. Dazu gehört auch die Förderung eines kritischen Bewusstseins gegenüber Sicherheitsfragen. https://www.ocg.at/ak-it-sicherheit
Saferinternet.at	Initiative für die kompetente und sichere Nutzung von Internet, Handy und Computerspielen, im Speziellen an Kinder, Jugendliche, Eltern und Lehrende gerichtet. https://www.saferinternet.at/
Science Center Netzwerk	Verein und Kompetenzstelle für interaktive Wissenschaftsvermittlung in Österreich https://www.science-center-net.at/
Shecurity - Women in Security	Community für Mädchen, Frauen und FINTA*, die in der Cybersecurity tätig sind oder Interesse an Security haben: Interessengruppen für CISOs, Risikomanagement, Buchclub, Digital Forensik sowie Hackerinnen Trainings. https://www.linkedin.com/company/shecurity-women-in-security/posts/?feedView=all

„UNDER18“ - Gewaltpräventionsprogramm des Bundeskriminalamts	Workshops für 13 bis 7 Jährige u.a. zum Thema Gewaltprävention im Kontext der digitalen Medien. https://under18.at
Watchlist Internet	Unabhängige Informationsplattform des Österreichischen Instituts für angewandte Telekommunikation (ÖIAT) für Privatpersonen und Unternehmen zu aktuellen Betrugsfällen im Internet. https://www.watchlist-internet.at/
Web of Trust - Der Cybersicherheits-Podcast	Vermittlung der notwendigen Kompetenzen, um Cyberkriminalität im Netz schnell zu erkennen und zu meiden, im Rahmen der Digitalen Kompetenzoffensive Österreich (DKO) https://web-of-trust.podigee.io/
Wirtschaftskammer Österreich (WKO), Cyber-Security-Hotline	Telefonische Erstinformation und Notfallhilfe im Fall einer Cyberattacke, Cybercrime Angriffs, Ransomware oder Verschlüsselungstrojanern. https://www.wko.at/it-sicherheit/cyber-security-hotline
WOMENinICT (VÖSI)	Initiative des Verbands Österreichischer Software Innovationen (VÖSI) zur Förderung und Sichtbarmachung von Frauen in der IT-Branche. https://voesi.or.at/voesi-aktiv/special-interest-groups/special-interest-group-womeninict/
Women4Cyber Österreich	Initiative bzw. Netzwerk mit dem Ziel, Frauen im Bereich Cybersicherheit zu vernetzen, zu unterstützen und zu fördern. Angebote: Workshops, Trainings und Mentoring im Bereich Cybersecurity für Frauen. https://shedigital.at/women4cyber-austria/

3.1.6 Öffentliche Verwaltung

Organisation	Beschreibung
Bundesministerium für Bildung (BMB)	Initiativen zum Bereich „Digitale Schule“ v.a. Digitales Lernen, Gegenstand Digitale Grundbildung, Sicheres Internet für Schülerinnen und Schüler, Initiative Saferinternet.at, Initiative Cybermobbing, Online-Fortbildungsangebot für Lehrende - MOOC „Digital Citizenship“ https://www.bmb.gv.at/Themen/schule/zrp/dibi.html
Bundesministerium für Inneres (BMI)	Bundeskriminalamt, Abteilung I/8 – Cybersicherheit und Krisenrechenzentrum, Abteilung IV/5/2 - Netz- und Informationssystemsicherheit, Abteilung IV/DDS/13 – IT-Security https://www.bmi.gv.at/ Das Bundeskriminalamt setzt Aktivitäten und Tätigkeiten im Bereich Internetkriminalität v.a. Cybercrime-Competence-Center C^4, Meldestelle against Cybercrime, Information und Prävention, Cybercrime Reports, Cyberkids/UNDER18. https://www.bundeskriminalamt.at/306/start.aspx
Bundeskanzleramt (BKA)	Plattform Digital Austria, Zuständigkeitsbereiche bis 31.05.2025: Österreichische Strategie für Cybersicherheit; Cyber Sicherheit Plattform (CSP); Austrian Trust Circle (ATC), CERT-Verbund Austria, European Cybersecurity Month (ECSM), Planspiele / Cybersicherheitsübungen – Cyber Europe, Austria Cyber Security Challenge (ACSC), Österreichisches Informationssicherheitshandbuch, Vernetzung und Kooperationen innerhalb der Europäischen Union

	https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/aktivitaeten-und-initiativen.html
CERT.at (Österreichisches Computer Emergency Response Team)	Nationaler Ansprechpartner für IT-Sicherheitsvorfälle: Warnungen, Support für Organisationen und Unternehmen bei Sicherheitslücken, Incident Response. Vernetzung mit weiteren CERTs/CSIRTs im In- und Ausland; sowie Informations- und Beratungsleistungen für Wirtschaft, Verwaltung und Privatpersonen. https://www.cert.at/en/
Cyber Crime Competence Center (C4)	Nationale Sicherheitsinitiative und Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität des Bundeskriminalamts, bestehend aus Expert:innen aus den Bereichen Ermittlung, IT-Forensik und Technik. Zentralstelle für die elektronische Beweismittelsicherung und -auswertung, Ermittlungen im Zusammenhang mit Cybercrime im engeren Sinn sowie die Koordinierung der Bekämpfung von Cybercrime. https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Beratung-und-Sensibilisierung/Cyber-Crime-Competence-Center-C4.html
Abteilung Cybersecurity, Bundesministerium für Landesverteidigung (BMLV)	Das IKT- & Cybersicherheitszentrum des Bundesheeres sorgt dafür, dass die Streitkräfte über eine robuste, widerstandsfähige und interoperable Informations- und Kommunikationstechnologie (IKT) verfügen. https://www.bmlv.gv.at/sk/cyber/iktcyberzentrum.shtml
European Digital Innovation Hubs (EDIHs)	Cybersecurity Beratung, Weiterbildung und Innovationsförderung von KMU und der öffentlichen Verwaltung in der Digitalisierung. https://www.ncc.gv.at/community/netzwerke-und-initiativen.html
IKT Sicherheitsportal	Ressortübergreifende Initiative in Kooperation mit der heimischen Wirtschaft für Maßnahmen zur Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie Bereitstellung zielgruppenspezifischer Handlungsempfehlungen https://www.onlinesicherheit.gv.at/
Nationales Koordinierungszentrum für Cybersicherheit (NCC-AT)	Unterstützung der Innovations- & Industriepolitik im Bereich der Cybersicherheit als Teil des EU-weiten Netzwerks nationaler Koordinierungszentren in Kooperation mit dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC). https://www.ncc.gv.at/

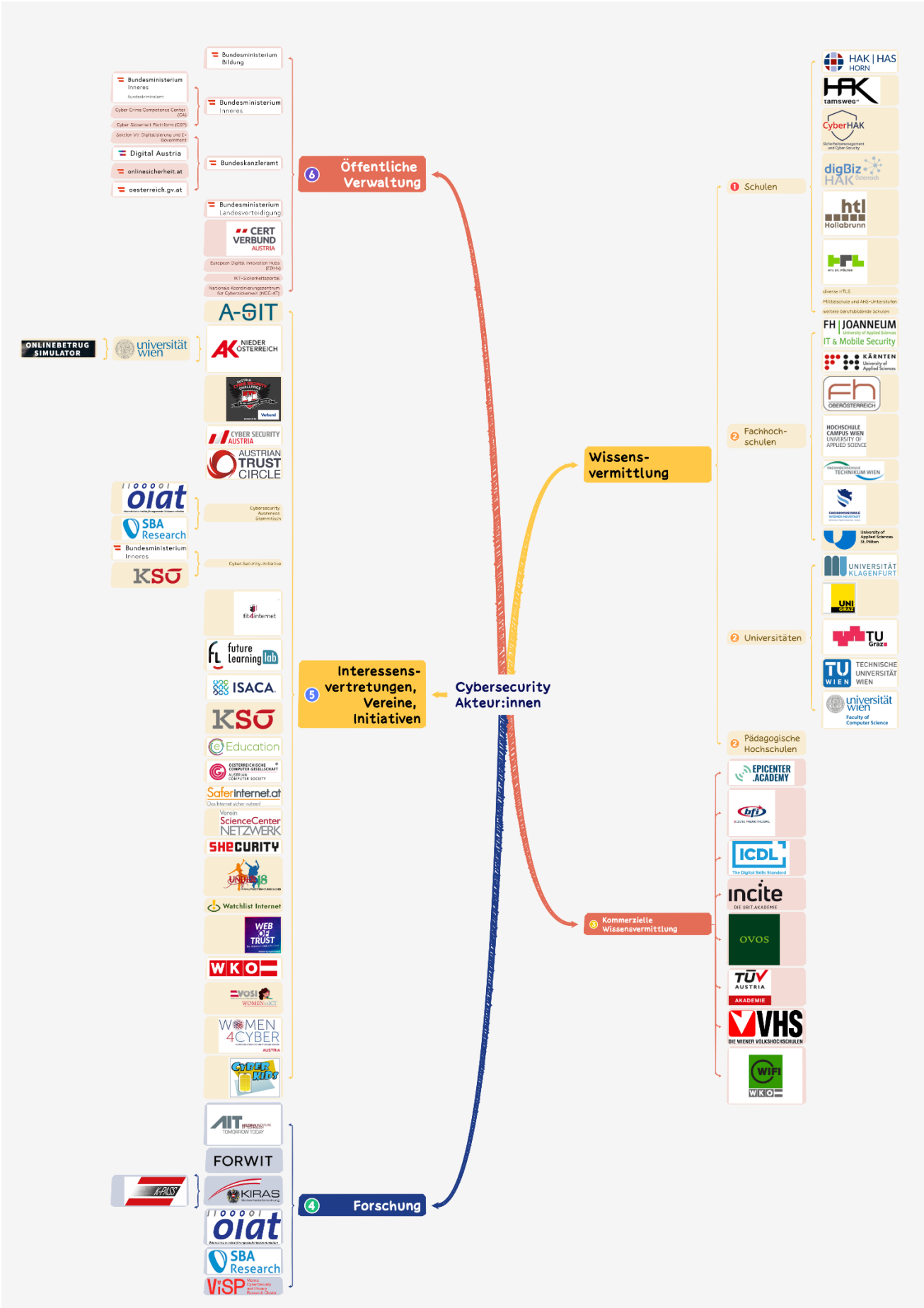

Abbildung 2: Überblick über Akteur:innen an der Schnittstelle Cybersecurity und Schule

3.2 Jugendliche: Cybersecurity-Bewusstsein und -Erfahrungen

Es gibt vermehrt Studien zu Cybersecurity-Bewusstsein bei Kindern und Jugendlichen. Quayyum et al. (2021) beschäftigen sich mit der Frage, inwieweit Cybersecurity-Risiken für Kinder in der Forschung behandelt werden und kommen zum Schluss, dass es hier im Vergleich zu anderen Forschungsfeldern an robusten Bewertungsansätzen und Mechanismen für Effizienznachweise von Cybersecurity-Bewusstseinsmaßnahmen mangelt. (Tirumala et al., 2016) vergleichen drei Altersgruppen hinsichtlich Cybersecurity-Bewusstsein (8-12-Jährigen, 13-17-Jährigen und 18-21-Jährigen). Das Bewusstsein über die Hauptbegriffe im Bereich der Cybersecurity, die Sicherheitssoftware für verschiedene Geräte und die Sicherheitsaspekte für Tablets und mobile Geräte wurden mit 2.214 Teilnehmer:innen evaluiert. In Bezug auf Familiarität mit einschlägigen Begriffen wie Firewall, Privacy, Tracker, Private Mode (Browser), Antivirus, Phishing, Security Warning (Browser & Desktop) zeigte sich, dass die Befragten mit dem **Begriff „antivirus" am vertrautesten** waren, gefolgt von „firewall" und „security warnings". Demgegenüber war das Bewusstsein darüber, was „tracker" bedeutet sehr niedrig in der gesamten Stichprobe. Das Bewusstsein über den Begriff „phishing" steigt mit dem Alter graduell an. Bei 13-17-Jährigen zeigt sich weiters, dass das Bewusstsein über **installierbare Sicherheitssoftware für Tablets und mobile Geräte im Vergleich zu Desktop-Software recht niedrig** ist. In Bezug auf das Bewusstsein von Sicherheitsrisiken, die durch Bluetooth, Werbung und Apps entstehen können zeigt sich, dass das **Bewusstsein über Bluetooth als Sicherheitsrisiko sehr niedrig** ist bei den 13-17-jährigen. Zusammenfassend liegt das Cybersecurity-Bewusstsein bei der Altersgruppe 8-12-jährige bei 19%, bei der Altersgruppe 13-17-jährige bei 32% und bei der Altersgruppe 18-21-jährige bei 41%. Zudem zeigen Olmstead und Smith (2017), dass der Großteil von Internetnutzer:innen bei einem schwierigen Wissensquiz zu Themen und Konzepten der Cybersecurity weniger als die Hälfte der Fragen richtig beantworten kann. Eine Studie des US-amerikanischen Pew Research-Instituts ergab weiters, dass **36% der Amerikaner:innen nie die Datenschutzrichtlinien von Unternehmen lesen**, bevor sie ihre Zustimmung geben. 63 % geben an, wenig oder gar nichts über Datenschutzgesetze und -vorschriften zu wissen. Darüber hinaus wissen 59 % bzw. 78 % der Amerikaner:innen wenig bis gar nichts darüber, wie Unternehmen bzw. die Regierung ihre Daten sammeln und verwenden (European Union Agency for Cybersecurity., 2023).

Zur Adressierung der Frage, wie es um das Cybersecurity-Bewusstsein von Jugendlichen in Österreich aktuell steht, wie und wo das Thema in ihrem Schulalltag Platz findet und wie Cybersecurity zukünftig in der Schule integriert werden könnte, wurde eine **Fokusgruppe mit insgesamt 13 Jugendlichen** durchgeführt. Dabei handelte es sich um eine heterogene Gruppe im Alter von 13 bis 19 Jahren, aus unterschiedlichen Schulformen (u.a. AHS, HTL mit Informatikschwerpunkt, HLW) mit entsprechend diversen Wissensständen zu Cybersecurity-Themen.

Folgende Fragen wurden innerhalb der 2-stündigen Diskussion erörtert:

- Was verbinden die Schüler:innen mit Cybersecurity?
- Welche Bedrohungen sind bekannt und wie werden diese erkannt?
- Woher stammt das vorhandene Wissen zu Cybersecurity? Welche Rolle spielt dabei die Schule?
- Wie sollte Cybersecurity in der Schule integriert werden?

Die Ergebnisse geben nicht nur Einblicke in das Cybersecurity-Bewusstsein der Teilnehmenden, sondern zeigen auch Ansätze auf, wie das Thema in den Schulunterricht integriert werden kann. Im Folgenden werden die Ergebnisse aus den Fokusgruppen dargestellt - mit Blick auf das Cybersecurity-Bewusstsein der Teilnehmenden, den von den Schüler:innen wahrgenommenen Status quo hinsichtlich der Behandlung von Cybersecurity-Themen an ihren Schulen sowie mögliche Wege zur Integration von Cybersecurity in den Unterricht.

3.2.1 Cybersecurity-Bewusstsein und eigene Erfahrungen

Die Einstiegsfrage in das Thema wurde bewusst offen gewählt, um Assoziationen der Jugendlichen zum Begriff Cybersecurity zu erhalten. So kam auf die Frage, was Jugendliche mit Cybersecurity verbinden, als erstes Stichwort Passwortsicherheit. Bewusstsein herrscht beispielsweise darüber, dass nicht die gleichen Passwörter für mehrere Zugänge verwendet werden sollen oder, dass möglichst komplexe Passwörter mit mehr Sicherheit einhergehen. Darauf aufbauend wurde insbesondere das Thema Phishing und Datensicherheit diskutiert. Unterschiedliche Phishing-Nachrichten, die per Mail oder SMS versendet werden, waren den Jugendlichen genauso bekannt wie Anrufe, in denen Kriminelle versuchen an Daten oder Geld zu kommen („*Ich werde die ganze Zeit von irgendwelchen Nummern angerufen*").

Insgesamt wurde die Frage zu Cybersecurity mit unterschiedlichen Onlinebetrugsmaschen beantwortet. Neben Phishing zählen dazu auch Fake-Shops sowie unseriöse Dropshipper[2] (bspw. für Software-Lizenzen, Gaming-Produkte oder über Pinterest beworbene Dropshipper, Kleinanzeigenbetrug), Maschen aus dem Bereich Vorschussbetrug (beispielsweise „Hallo Mama/Hallo Papa"-SMS, Love Scams (Liebesbetrug im Internet)) sowie Bedrohungen aus dem Unternehmensbereich, die insbesondere von HTL-Schüler:innen genannt wurden (beispielsweise DDos-Attacken[3], Brutforce-Angriffe[4], Ransomware[5]). Auch bei den Erkennungsstrategien wurde in erster Linie über unterschiedliche Formen des Phishings gesprochen. Verdächtige Absenderadressen, inkonsistente Formulierungen, Rechtschreib- und Grammatikfehler sind laut Jugendlichen Indizien, um betrügerische Nachrichten zu erkennen. Hinsichtlich betrügerischer Websites wie Fake-Shops wurde vor allem die Überprüfung des Impressums genannt.

Zusammenfassend ist ein Bewusstsein für Cybersecurity vorhanden, wobei der Begriff in erster Linie **mit Online-Betrug in Zusammenhang** gebracht wurde und klassische Maschen wie Phishing am stärksten im Bewusstsein der Jugendlichen sind. Kaum genannt wurden hingegen Betrugsmaschen, die sich auf Social-Media-Plattformen abspielen. Das **Wissen** über die genannten Themen kommt laut Jugendlichen vor allem **aus eigenen Erfahrungen** bzw. bei den Erkennungsstrategien aus dem Lernen aus eigenen Erfahrungen.

3.2.2 Cybersecurity an Schulen: Status Quo

Als wenig hilfreiche Quelle für das Aufbauen von Cybersecurity-Wissen wurde die Schule genannt. Folgende (teils von mehreren Stimmen zusammengefasste) Zitate veranschaulichen die Probleme, die die Jugendlichen im Schulbereich wahrnehmen:

- *„Wir haben noch nie im Unterricht darüber geredet, nicht mal in Informatik oder Digitale Grundbildung."*
- *„Wir lernen sehr viel zu Word und Excel oder wie das Innere eines Laptops aussieht, aber nichts zu Cybersecurity."*
- *„Lehrer:innen interessiert das Thema nicht oder es fehlt an Wissen."*
- *„Es gibt einen Mangel an Lehrer für Digitale Grundbildung, daher werden ‚random' Lehrer gefragt, ob sie das Fach unterrichten wollen."*
- *„Wir hatten einen Informatiklehrer, der viel gemacht hat, aber das Problem war, dass sich bei diesem Thema zu viel ändert."*
- *„Es gibt keine Einschulung, wenn wir Laptops oder Tablets bekommen. Wir müssen zwar einen Vertrag unterschreiben, aber wie wir damit umgehen, lernen wir nicht."*

Die Jugendlichen identifizierten einen **Wissens- und Kompetenzmangel bei Lehrkräften** und berichteten davon, dass Lehrkräfte entweder **kein Interesse** am Thema zeigen oder nicht über die ausreichenden Kenntnisse verfügen, um das Thema in den Unterricht einzubringen. Während in den dafür **passenden Fächern wie Informatik oder Digitale Grundbildung das Thema Cybersecurity kaum angesprochen** würde, würden andere, laut den Jugendlichen unwichtigere, Themen im Vordergrund stehen. Selbst bei engagierten Lehrkräften wurde das Problem der Schnelllebigkeit genannt, die eine **wiederholte Weiterbildung bei Lehrkräften benötigen** würde. Als ein Beispiel des Umgangs mit Cybersecurity-Themen an Schulen wurde die Einführung neuer Geräte und die bzw. die damit einhergehende **fehlende Einschulung** genannt.

3.2.3 Mögliche Integration von Cybersecurity an Schulen

Einig waren sich die Jugendlichen darin, dass Cybersecurity ein wichtiges Thema ist, das mehr Raum finden sollte, und zwar so früh wie möglich. Uneinig waren sich die Jugendlichen allerdings in der Frage, wie eine stärkere Integration von Cybersecurity-Themen im Schulunterricht funktionieren könnte. Herauskristallisiert

[2] Beim Dropshipping wird die bestellte Ware nicht vom Online-Händler, sondern direkt vom Lager des Herstellers oder eines Großhändlers an die Kundinnen und Kunden versendet. Dropshipping an sich ist nicht problematisch, wird aber zunehmend von unseriösen Online-Shops genutzt, die gegen Konsumentenschutzrechte verstoßen.

[3] Bei einem DDoS-Angriff (kurz für Distributed-Denial-of-Service-Angriff) überlasten Angreifer eine Server- oder Netzwerkressource (z. B. Infrastruktur einer Unternehmens-Website) mit einer großen Menge gleichzeitiger Anfragen. Dadurch wird die Ressource so stark beansprucht, dass sie legitime Anfragen nicht mehr bearbeiten kann.

[4] Bei einem Brute-Force-Angriff versuchen Angreifer, Passwörter, Anmeldeinformationen oder Verschlüsselungen durch systematisches Ausprobieren aller möglichen Kombinationen zu erraten.

[5] Ransomware ist eine Art Schadsoftware, bei der ein infiziertes Gerät, Daten oder sogar ganze Unternehmensnetzwerke verschlüsselt werden. Die Angreifer fordern anschließend ein Lösegeld (engl. *ransom*), um im Gegenzug die Entschlüsselung oder den Zugang zu den Daten wieder freizugeben.

haben sich dabei vor allem zwei Möglichkeiten: Integration in den Lehrplan vs. Integration via externer Workshops mit Vor- und Nachteilen, die in Tabelle 2 zusammengefasst sind.

Zudem wurde als Möglichkeit zur Integration in den Lehrplan auch die Etablierung eines eigenen Unterrichtsfaches zu Medienkompetenz inklusive der Behandlung von Cybersecurity-Themen (wiederum über den Lehrplan) benannt sowie die Einbettung des Themas über mehrere Fächer hinweg als Querschnittsmaterie.

Nach konkreten Vermittlungswünschen gefragt, wurde der Wunsch nach einem „**Internetführerschein**“ geäußert, der Kenntnisse zur sicheren Nutzung digitaler Geräte vermittelt und vor der Benutzung der Tablets und Laptops positiv absolviert werden muss. Interaktive Formate wie **Quiz oder andere Gamification-Elemente** wurden als positiv bewertet, allerdings wurde hinsichtlich der jetzigen Verwendung solcher Formate kritisiert, dass oft eine Einführung zu den in den Games behandelten Themen fehlt.

Auch die Idee einer **Kooperation zwischen Schulen und Unternehmen** wurde von den Jugendlichen genannt, insbesondere als Möglichkeit externe Expert:innen hinzuzuziehen. Das Thema „**Lernen aus Fehlern**“ wurde ebenso von den Jugendlichen aufgegriffen - so kam der Vorschlag, bei der Vermittlung von Cybersecurity mit einer **Virtual Machine** (softwarebasierte Nachbildung eines Computersystems) zu arbeiten, in der die Schüler:innen Fehler machen können.

Tabelle 2: Vor- und Nachteile der Integration von Cybersecurity Themen im Lehrplan vs. Workshops durch Externe

Lehrplan	Externe Workshops
Pro: • Einbettung in bestehende Fächer (Informatik & Digitale Grundbildung) • Nachhaltige & langfristige Verankerung des Themas	Pro: • Einladung von externen Expert:innen stellt Kompetenz sicher, auch bei schnelllebigen Themen • Themen, die nicht in den „normalen Unterricht“ eingebettet sind, werden als spannender wahrgenommen
Contra: • Thema zu schnelllebig • Probleme fehlender Expert:innen bleibt bestehen • Fehlende Ressourcen für laufende Weiterbildung	Contra: • Kostspielig (v.a. bei regelmäßigen Workshops)

Die Ergebnisse aus den Fokusgruppen mit Jugendlichen zeigen, dass innerhalb der sehr diversen Fokusgruppe Basiskompetenzen in puncto Cybersecurity vorhanden sind, gleichzeitig wurde sehr wohl Bildungsbedarf hinsichtlich der dynamischen Betrugslandschaft identifiziert. Die Schule spielt bisher eine untergeordnete Rolle in der Vermittlung dieses Wissens, weshalb neue Ansätze für eine nachhaltige Integration in den Unterricht erforderlich sind. Die vorgeschlagenen Maßnahmen und methodischen Ansätze liefern wertvolle Impulse für eine bessere Vermittlung von Cybersecurity-Kompetenzen.

3.3 Perspektiven von Seiten der Expert:innen

Neben der Perspektive von Jugendlichen wurden im Rahmen des Projekts auch weitere zentrale Akteur:innen im Bereich Cybersecurity und Schule eingebunden, um ein umfassenderes Bild der bestehenden Möglichkeiten, Herausforderungen und Barrieren in der Wissensvermittlung zu gewinnen. Ziel war es, jene Personen zu Wort kommen zu lassen, die an der Schnittstelle von Bildung, Schulorganisation und Fachwissen tätig sind und somit entscheidenden Einfluss bei der Umsetzung entsprechender Bildungsmaßnahmen haben.

Zur Beantwortung der Frage, wie Jugendliche bestmöglich auf die zunehmenden Herausforderungen im digitalen Raum vorbereitet werden können, wurden insgesamt **zehn semi-strukturierte Expert:inneninterviews** durchgeführt. Gesprächspartner:innen waren dabei Expert:innen aus dem Bereich Cybersecurity, Lehrpersonen unterschiedlicher Schulformen, Vertreter:innen der Schulverwaltung sowie Expert:innen aus Bildungsinstitutionen. Die Liste der Interviewpartner:innen sind in der folgenden Tabelle 3 aufgelistet.

Tabelle 3: Liste der Expert:innen im Kontext Cybersecurity und Schule

Expert:innen	Hintergrund
Josef Pichlmayr	• Cybersecurity-Experte • Mitbegründer und Obmann Cybersecurity Austria https://verbotengut.at/ • Geschäftsführer IKARUS https://www.ikarussecurity.com/en/about-ikarus/company-history/insights/joe-pichlmayr/ • Vermittlung von Cybersecurity-Wissen in Schulen
Stephanie Jakoubi	• Cybersecurity-Expertin • Vorstand der Cyber Sicherheit Plattform (CSP) • SBA-Research – Forschungscenter für IT-Informationssicherheit (Teil des Management Board, Head of the Strategic Partnership Management, Communication, Events) • Vermittlung von Cybersecurity Awareness in Schulen (z.B. “DieIT-Tag” mit 240 Frauen an Schulen 3./4. Unterstufe)
Thomas Nárosy	• Bildungsexperte • Digital-inklusive Transformations- und Schulentwicklungsprozesse • Digitales Kompetenzmodell für Österreich DigComp 2.2AT • Strategieentwicklung: Digital Upskilling • Lehrkräftefortbildung
Anna Klema	• Ober- und Unterstufenstufenlehrerin für Informatik in einem AHS-Gymnasium im 18. Bezirk (seit 28 Jahren) • E-Education Austria Mitglied • Seit zehn Jahren Leitung Netzwerk E-School Vienna (Projekt der Bildungsdirektion mit dem Bemühen Schulen zu digitalisieren; Unterstützen Schulen beim Fach digitale Grundbildung; Bindeglied Schulen und Bildungsdirektion)
Wolfgang Rosenkranz	• Teamleiter CERT.at (Computing Emergency Response Team); betreiben den Sektor Energy CERT und technischen Betrieb des österreichischen Government CERT • Stellt sicher, dass Organisationen Informationen bekommen bevor Cyber-Angriffe passieren • Energieunternehmen, Behörden, sowie andere Organisationen
Michael Steiner	• Pädagogische Hochschule (ehemaliger AHS-Lehrer für Religion und Informatik) • ComeIT Institut – tätig für informatische Bildung, digitale Bildung, Medienbildung, Schulentwicklung • Mitarbeit am Lehrplan digitale Grundbildung
Frau S. (Anonymisiert)	• Lehrerin am islamischen Realgymnasium (Privatschule) • Starker Digitalisierungsfokus • Klassenvorständin
Herbert Giegerl	• CyberHAK • Direktor HAK Tamsweg (Salzburg) • Seit vier Jahren Angebot „Sicherheitsmanagement und Cybersecurity“ • 2025/26 schließt der erste Jahrgang mit Matura ab
Astrid Holzer	• CyberHAK • Direktorin Vienna Business School (Wien, Floridsdorf) • Seit 2024/25 Jahr Schulversuch „CyberHAK“ mit 30 Schüler:innen • Im Jahr 2026/27 sind zwei erste Klassen geplant
Elisabeth Schmid	• AHS Wolkersdorf • Professorin für Mathematik, Informatik, Geografie und Wirtschaftskunde sowie Digitale Grundbildung • Seit vielen Jahren Administratorin und IT-Kustodin der Schule

3.3.1 Herausforderungen bei der Vermittlung von Cybersecurity-Inhalten

1) Abstraktheit des Themas

„Es besteht die grundsätzliche Problematik: Wenn wir über Cybersecurity sprechen, könnte man genauso sagen, sprechen wir über das Internet/Digitalisierung".

Eine zentrale Herausforderung in der didaktischen Umsetzung besteht in der Abstraktheit des Themas: „Man kann Cybersecurity nicht angreifen." Cybersecurity ist im klassischen Sinn nicht greifbar – Angriffe, Bedrohungen oder Sicherheitslücken sind häufig unsichtbar und schwer nachvollziehbar. Das erschwert Jugendlichen oft den Zugang zum Thema. Besonders betroffen sind Bereiche wie der Umgang mit eigenen Daten, das Bewusstsein für die Konsequenzen digitaler Handlungen oder das Erkennen von Bedrohungen, die im Hintergrund ablaufen. Um diese Unsichtbarkeit und Komplexität didaktisch zu bewältigen, wurden im Projekt drei zentrale Analogien identifiziert, die in der Vermittlungspraxis helfen können, Cybersecurity anschaulicher und erlebbarer zu machen (siehe folgende Abbildung 3).

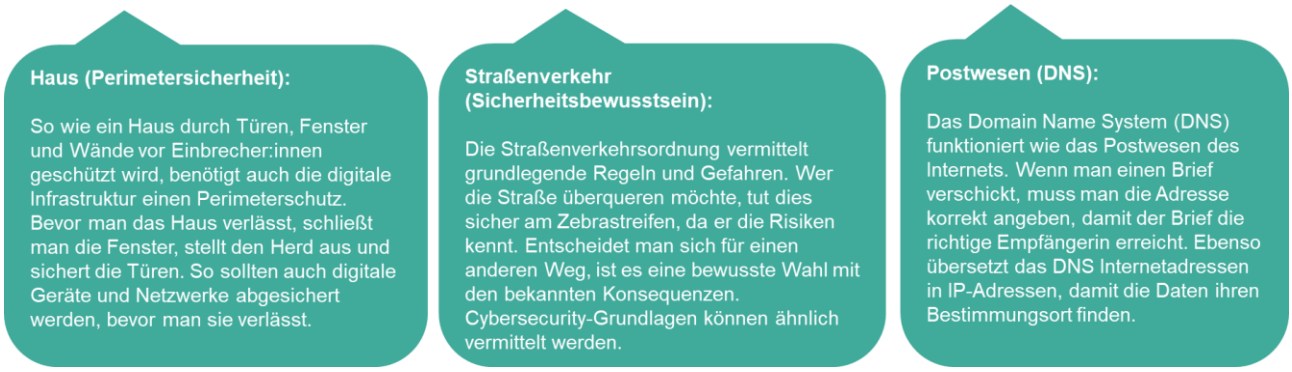

Abbildung 3: Drei beispielhafte Analogien, um Cybersecurity Themen zu vermitteln.

2) Komplexität der Inhalte und unterschiedlicher Reifegrad

Ein zentrales Ergebnis aus der Auseinandersetzung mit den Expert:innen-Inputs sowie einschlägigen Quellen – insbesondere dem ENISA Threat Landscape Report 2030 der Europäischen Agentur für Netz- und Informationssicherheit – ist die **zunehmende Komplexität und Dynamik des Themenfelds Cybersecurity** (European Union Agency for Cybersecurity., 2023). ENISA stellt dabei die Frage in den Raum, mit welchen Bedrohungen unsere Gesellschaft in den kommenden fünf Jahren konfrontiert sein wird. Hierbei werden Supply-Chain-Angriffe oder die zunehmende Bedeutung menschlicher Fehlhandlungen in cyber-physischen Systemen genannt (siehe Abbildung 4).

Abbildung 4: Top 10 der größten Bedrohungen für Cybersecurity im Jahr 2030 laut ENISA (European Union Agency for Cybersecurity., 2023)

In den Interviews wurde betont, dass diese **Entwicklung der Angriffsmuster sowie Veränderungen im Bereich Cybersecurity schneller verläuft,** als viele erwarten („*Veränderungen überholen uns viel schneller als gedacht*").

Frühere Bedrohungsszenarien – wie etwa die Verbreitung eines Computervirus über Disketten oder die Notwendigkeit einfacher Passwortschutzmaßnahmen – waren vergleichsweise überschaubar, leicht verständlich und dementsprechend auch einfacher zu vermitteln. Heute hingegen stehe die Gesellschaft vor hochkomplexen, vernetzten Systemen, deren Schutz tiefgreifendes Spezialwissen erfordert („*Cybersecurity ist hochgradig komplex und ändert sich stark*"). Die Absicherung digitaler Infrastrukturen verlangt Teams von **hochqualifizierten Expert:innen** mit oft jahrelanger Ausbildung. Gleichzeitig steigt die Anfälligkeit dieser Systeme mit ihrer zunehmenden Komplexität (*„Man braucht viele, viele Jahre das zu lernen..."*) – immer weniger Organisationen verfügen über die **Ressourcen oder das Know-how**, um mit diesen Herausforderungen adäquat umzugehen.

In Bezug auf die Vermittlung von Inhalten erfordert der sich ständig wandelnde Charakter digitaler Themen eine kontinuierliche Weiterbildung sowie eine **regelmäßige Aktualisierung des Wissensstands auf Seiten der Lehrkräfte**. Diese Anforderung steht jedoch in einem Spannungsverhältnis zur bestehenden Struktur des Bildungssystems. Daraus ergibt sich eine strukturelle Inkompatibilität zwischen der Dynamik des Themenfelds und den vergleichsweise starren Rahmenbedingungen des Schulsystems. In diesem Zusammenhang wird betont, dass Schule zunehmend als lernende Organisation verstanden werden sollte – also als ein System, das sich kontinuierlich weiterentwickelt, um auf neue Herausforderungen angemessen reagieren zu können.

Die Expert:innen berichten aus ihren Erfahrungen von einer **Lücke im IT-bezogenen Grundlagenverständnis von Jugendlichen**. Viele kennen grundlegende Regeln, Risiken und Grenzen im digitalen Raum nicht. Auch grundlegende IT-Begriffe wie *Hardware*, *Software* oder *IT* können vielfach nicht korrekt zugeordnet werden. Dies macht deutlich, dass die Cybersecurity-Bildung nicht nur spezialisierte Inhalte, sondern insbesondere ein fundiertes Basisverständnis digitaler Technologien vermitteln muss. Mit der Herausforderung der Komplexität der Inhalte verbunden ist die Frage: **Welchen Grad an Komplexität kann man Jugendlichen überhaupt vermitteln**? Jugendliche haben ein sehr unterschiedliches Wissensniveau und einen unterschiedlichen Reifegrad. Das ist sehr unterschiedlich und hängt stark von der individuellen Entwicklung des jungen Menschen ab. Einerseits kann es sein, dass Jugendliche bereits in der Lage sind, die Grundzüge von Continuous Threat and Exposure Management oder grundlegende Aspekte von Cybersecurity zu verstehen (z. B. was ein Virenschutz ist oder wie eine Firewall implementiert wird). Andererseits kann es sein, dass sie sich die Abstraktheit, die mit dem Thema Cybersecurity einhergeht, noch gar nicht vorstellen können. Hier braucht es gezielte didaktische Konzepte, die sich am Reifegrad der jeweiligen Jugendlichen orientieren.

3) Bedarf von aktuellen Lehr-Unterlagen für Cybersecurity

Mehrfach beklagen Pädagog:innen, dass es zu wenig aktuelle, allgemein verständliche und didaktisch aufbereitete Lehrunterlagen zum Thema Cybersecurity gibt. "*Wir verwenden vor allem Materialen von SaferInternet"*. Daher greifen viele Professor:innen zur Hilfe zur Selbsthilfe und suchen sich selbst via Internet die aus Ihrer Sicht passenden Lehrunterlagen. Es besteht der große Wunsch nach didaktisch gut aufbereiteten und aktuellen Lehrunterlagen, die adäquat für die jeweilige Schulstufe passend im Unterricht verwendet werden können.

4) Langfristige Verankerung von Cybersecurity-Denken

Cybersecurity erfordert eine neue Art zu denken – und dieses Denken muss geübt, gefestigt und immer wieder aktualisiert werden. Es reicht nicht aus, Inhalte einmalig zu vermitteln oder lediglich punktuell auf das Thema einzugehen. Vielmehr ist es notwendig, das Thema langfristig und systematisch im Bildungsprozess zu verankern. Wissen zu **Cybersecurity ist kein statisches Wissen, sondern ein kontinuierlicher Lern- und Anpassungsprozess**, der regelmäßige Wiederholung, Anwendung im Alltag und kritische Reflexion verlangt. Teilweise wird auch eine Analogie zur Vermittlung von Regeln zur Straßenverkehrsordnung beschrieben. Diese ist im Bildungsbereich als Querschnittthema verankert und man erklärt Kinder schon erste Konzepte (man muss links und rechts schauen, wenn man über die Straße geht) sehr früh. Man sollte mit der Vermittlung der Inhalte starten, ab dem Zeitpunkt, wo Kinder ein Handy bekommen, das ist meistens schon in der Volksschule[6] der Fall.

Cybersecurity sollte heute nicht mehr ausschließlich als technische Notwendigkeit im Unternehmenskontext betrachtet werden, sondern im weiteren Sinne als **Bestandteil der digitalen Lebenswelt** verstanden und

[6] https://www.bmb.gv.at/Themen/schule/zrp/dibi/saferinternet/ndg.html

diskutiert werden. Die Allgegenwärtigkeit digitaler Systeme und die zunehmende „Smartifizierung" des Alltags führen zu einer **exponentiellen Zunahme der Kritikalität**: Mit jeder weiteren Vernetzung vergrößert sich auch die potenzielle Angriffsfläche. Prognosen über die nächsten zehn Jahre sind dabei nur begrenzt verlässlich – nicht zuletzt, weil wir heute noch nicht wissen, welche Technologien und Systeme künftig zum Alltag gehören werden („*Wir wissen nicht einmal, welche Systeme wir in zehn Jahren verwenden werden. Forecasts sind oft eine Utopie*."). Insofern sei jeder Versuch, konkrete Bildungsinhalte zu formulieren, stets eine Momentaufnahme.

5) Diskrepanz zwischen Wissen und Verhalten

Ein weiterer zentraler Aspekt – insbesondere bei Jugendlichen – ist die Diskrepanz zwischen Wissen und tatsächlichem Verhalten. Zahlreiche Studien zeigen, dass allein das Verstehen von Cybersecurity-Grundlagen nicht automatisch zu sicherem Verhalten führt. Dieses Phänomen wird unter anderem in der „Theory of Planned Behavior" (Ajzen, 1991) sowie der „Theory of Reasoned Action" (Ajzen & Fishbein, 1975) beschrieben. Bei Jugendlichen ist die Problematik besonders ausgeprägt, da ihre Nutzung digitaler Technologien häufig sozial motiviert ist. Sich nicht zu beteiligen – etwa auf einer Plattform – kann zu Ausgrenzung führen. Sicherheit steht dabei oft nicht im Vordergrund. In der Praxis bedeutet das: Sicherheitsvorkehrungen werden umgangen, etwa durch das Teilen von Passwörtern oder durch Tricks, um Filtersysteme zu unterlaufen. Solche Umgehungsstrategien sind weit verbreitet und lassen sich kaum verhindern. Nicht nur bei Jugendlichen, sondern bei der gesamten Bevölkerung haben wir auch das Thema der Motivation: „*die meisten Personen, die mit digitalen Geräten zu tun haben, wollen die Geräte bedienen, hätten gern, dass sie einfach funktionieren und sich nicht permanent darüber Gedanken machen, ob sie gerade angegriffen werden können oder nicht*". Deshalb ist es entscheidend, nicht allein auf individuelle Verantwortung zu setzen, sondern auch strukturelle Maßnahmen zu schaffen. Dazu zählen klare Regeln und Schutzmechanismen – etwa Smartphone-Verbote an Schulen, wie sie in Australien, Frankreich oder Teilen Skandinaviens und nun auch in Österreich seit 01. Mai 2025 bestehen. Sie entlasten Kinder und Jugendliche und setzen Verantwortung dort an, wo sie hingehört: im System.

Diese Entwicklungen und Herausforderungen werfen grundlegende Fragen für die Gestaltung von Bildungsangeboten auf, die sich Lehrkräfte während der Vermittlung stellen sollten:

- Was ist ein realistisches Ziel bei der Vermittlung von Cybersecurity-Kompetenzen?
- Welche Inhalte sollen vermittelt werden – und mit welcher fachlichen Tiefe und Komplexität? Welche Komplexität ist möglich zu vermitteln?
- Wie kann gewährleistet werden, dass Lehrkräfte über aktuelles und relevantes Wissen verfügen – und dieses auch langfristig aufrechterhalten können?

3.3.2 Verortung von Cybersecurity im Lehrplan

Ein zentrales Ergebnis aus den Projektarbeiten und Gesprächen mit Expert:innen ist die Frage nach der sinnvollen Verortung des Themas Cybersecurity im schulischen Kontext. Es wurde mehrfach betont, dass **Cybersecurity klar und explizit in einem Fach curricular verankert sein muss**. Wird das Thema ausschließlich als Querschnittsmaterie verstanden und auf verschiedene Fächer verteilt, besteht die Gefahr, dass es in der praktischen Umsetzung untergeht oder nur punktuell behandelt wird (*„Wenn es in vielen Fächern Thema ist, gibt es die Gefahr, dass es untergeht")*. Daher ist die formale Integration in ein verbindliches Fach – wie **Digitale Grundbildung** – von zentraler Bedeutung.

Ergänzend zur festen Verankerung im Fach Digitale Grundbildung sollte Cybersecurity auch in anderen Unterrichtsfächern **thematisiert und geübt werden**. So lassen sich beispielsweise Aspekte wie Fake News sinnvoll im Deutsch- oder Geschichtsunterricht aufgreifen; Datenschutz und Urheberrecht bieten sich etwa für den Ethik-, Informatik- oder Rechtsunterricht an. Diese fächerübergreifende Behandlung unterstützt eine ganzheitliche Auseinandersetzung mit dem Thema und trägt zur Alltagsrelevanz bei. Cybersecurity eignet sich zudem hervorragend als Querschnittsthema, das fächerübergreifend unterrichtet werden kann – etwa im Rahmen von Projekttagen oder epochalem Unterricht. Wichtig sei dabei, die Relevanz des Themas sowohl in seiner **gesellschaftlichen Gegenwartsbedeutung** als auch mit **Blick auf zukünftige Anforderungen** deutlich zu machen, um **Aufmerksamkeit und Motivation bei Schüler:innen und Lehrkräften** gleichermaßen zu erzeugen.

Hervorgehoben wurde auch, dass reines Vermitteln von Inhalten nicht ausreiche. Stattdessen seien **wiederholte Übungsmöglichkeiten und das Etablieren von Routinen** im Umgang mit sicherem digitalem Verhalten entscheidend. Dies widerspricht einem verbreiteten didaktischen Paradigma, Inhalte lediglich

einmalig zu behandeln. Für das Vertiefen sind praktische Übungen zentral, anhand welcher man immer und immer wieder Inhalte einübt und vertieft.

Ein weiterer zentraler Punkt betrifft die Begrifflichkeit im Lehrplan: Es wurde deutlich betont, dass der **Begriff Cybersecurity** explizit im Curriculum genannt werden müsse. Nur so könne sichergestellt werden, dass dem Thema die notwendige Verbindlichkeit und Sichtbarkeit im schulischen Alltag zukommt. *(„Alles, was im Lehrplan steht, hat eine gewisse Verbindlichkeit – Cybersecurity muss als Thema und als Begriff im Lehrplan stehen.“)*

3.3.3 Gestaltung der schulischen Lehre

1) Lernzielformulierung

Ein zentrales **Lernziel** sollte der Förderung von **Cybersecurity-Bewusstsein**, also der Bewusstseinsbildung im Umgang mit digitalen Technologien zukommen. Dabei sollen Jugendliche nicht nur technisches Wissen erwerben, sondern vor allem ein reflektiertes Verständnis für Risiken, Konsequenzen und eigenes Verhalten im digitalen Raum entwickeln, nämlich:

- sich der Gefahren und Risiken im digitalen Raum bewusst sein.
- verstehen, welche Auswirkungen bestimmte Handlungen oder Aktivitäten im Netz haben können.
- in der Lage sein, ihr Verhalten entsprechend bewusst und verantwortungsvoll zu gestalten – oder zumindest reflektiert entscheiden zu können.
- vermittelt bekommen, dass Cyberangriffe nicht immer gezielt erfolgen, sondern prinzipiell jede Person betroffen sein kann.

Insbesondere im Kontext von Organisationen – d.h. im späteren Arbeitsumfeld – sollen Jugendliche:

- in der Lage sein, sicherheitsrelevante Richtlinien und Policies zu verstehen,
- den Sinn und Zweck solcher Regelungen nachvollziehen können,
- und bereit sein, diese zu akzeptieren und umzusetzen.

Diese Lernziele zielen darauf ab, nicht nur technisches Grundverständnis zu schaffen, sondern auch die Einstellung der Lernenden zur Thematik zu verändern – hin zu einem bewussteren, kritischeren und verantwortungsvolleren Umgang mit digitalen Technologien im schulischen wie beruflichen Alltag. In den Interviews wurde zudem mehrfach betont, dass Cybersecurity ein hochkomplexes und sich dynamisch entwickelndes Themenfeld sei. Gleichzeitig wurde aber auch hervorgehoben, dass sich bestimmte Grundlagen kaum verändern und daher einen stabilen Anker für die schulische Vermittlung bieten können. Daher soll die **Vermittlung auf zwei grobe Themenbereiche** fokussieren:

(1) **Vermittlung von Grundlagenwissen**: Trotz sich wandelnder Technologien, Angriffsmuster und Rahmenbedingungen bleibt die Vermittlung grundlegender Kenntnisse zentral. Die Grundlagen der digitalen Welt – etwa zu Aufbau und Funktion von Computern, Softwarestrukturen und Netzwerken – bilden das Fundament, auf dem weiterführende Inhalte aufbauen können. Ein solides Verständnis dieser Strukturen ermöglicht es Jugendlichen, neue Bedrohungen und Entwicklungen besser einzuordnen. *(„Die Technologie, die Angriffsmuster und die Geschwindigkeit verändern sich – aber die Basics bleiben gleich.“)*

(2) **Systemverständnis**: Neben technischen Grundlagen wurde auch die Notwendigkeit betont, ein Systemverständnis zu entwickeln – also die Fähigkeit, das „große Ganze“ zu erkennen und Zusammenhänge zu verstehen. *(„Man muss irgendwie darstellen, dass alles zusammenhängt – und dass es sehr wohl Auswirkungen hat, wie ich mit meinen Geräten umgehe und wie ich mich generell in der digitalen Welt bewege. Das braucht Zeit, um das verständlich zu machen.“*). Ziel ist es, Jugendlichen ein vernetztes Denken zu ermöglichen, sodass sie die Auswirkungen ihres eigenen digitalen Handelns besser abschätzen können. Dazu gehören unter anderem:
   a. das Verständnis der technischen Funktionsweise alltäglich genutzter Anwendungen (z. B. Wie funktioniert Snapchat?),
   b. die Einsicht, dass digitale Geräte miteinander verbunden sind (z. B. Risiken durch IoT-Geräte wie Botnetz-Angriffe),
   c. die Frage, wie und wo Daten gespeichert werden – insbesondere im Kontext großer Technologiekonzerne,
   d. sowie ein Bewusstsein für die Bedeutung politischer und gesellschaftlicher Entscheidungen und Einflüsse auf digitale Infrastrukturen.

Schließlich wurde erwähnt, dass eine **gewisse Haltung – ein Grundmisstrauen** vermittelt werden müsse. Neben Grundlagen, die man wissen sollte, bräuchte es ein Grundverständnis dafür, dass es genauso leicht möglich ist ein böses Programm zu schreiben wie ein gutartiges Programm. Es muss verstanden werden, dass der Digitalisierung, den Programmen und Geräten nicht bedingungslos vertraut werden kann.

Diese Aussagen unterstreichen die didaktische Herausforderung: Neben der Vermittlung technischer Fakten geht es vor allem darum, Verständnis für Zusammenhänge, Verantwortungsbewusstsein und kritisches Denken zu fördern – zentral für jede zukunftsorientierte Cybersecurity-Bildung.

2) Vermittlung von Inhalten

Als **digitale Lehrmittel und Formate** zur Unterstützung des Unterrichts wurden verschiedene digitale und hybride Vermittlungsangebote als besonders hilfreich identifiziert:

- Digitale Erklärvideos, Podcasts und interaktive Schulbuchformate wie *schubu.org*[7]
- Gamification-Ansätze, die spielerische Elemente gezielt zur Förderung von Cybersecurity-Kompetenzen nutzen (siehe Abschnitt 6 Didaktische Ansätze zur Vermittlung von Cybersecurity in der Sekundarstufe II)
- Wettbewerbsformate wie die *Austria Cyber Security Challenge*[8]
- *Saferinternet*-Kampagnen[9]
- Interaktive Lernplattformen und Tools, z. B.: HackTheBox[10], TryHackMe[11], HackingLab[12], Bug-Bounty-Programme wie YesWeHack[13] oder HackerOne[14]
- Lernformate wie die Übungsfirma North GRC[15]
- Ein klar geäußerter Bedarf betrifft den Bereich Simulationen: *„Es braucht mehr gezielte interaktive Simulationsplattformen zum Ausprobieren.“* Solche Plattformen könnten den Lernenden ermöglichen, reale Bedrohungsszenarien in einer sicheren Umgebung kennenzulernen und darauf zu reagieren – ein entscheidender Beitrag zum Aufbau von Handlungskompetenz.
- Weitere kommerzielle Vermittlungsangebote werden im Abschnitt 6 Didaktische Ansätze zur Vermittlung von Cybersecurity in der Sekundarstufe II umfassend dargestellt.

Zudem wurde die **Einbindung von externen Cybersecurity-Expert:innen an Schulen** als besonders wirkungsvolles Mittel identifiziert, um das Thema Cybersecurity für Schüler:innen greifbarer, praxisnäher und authentischer zu gestalten. Insbesondere kann man damit der Herausforderung zur Aktualität der Cybersecurity-Inhalte begegnen. Zudem ermöglicht der direkte Austausch mit Fachleuten, Einblicke in reale Bedrohungsszenarien, aktuelle Entwicklungen und berufliche Perspektiven zu erhalten. Gleichzeitig kann so ein realistisches Bild davon vermittelt werden, welche Anforderungen und Herausforderungen mit digitalen Sicherheitsfragen in der Arbeitswelt verbunden sind. Darüber hinaus wurde betont, dass der Kontakt mit Expert:innen nicht nur zur Wissensvermittlung, sondern auch zur Motivationsförderung beiträgt – insbesondere dann, wenn praktische Erfahrungen geteilt werden. Genannte Beispiele und potenzielle Partner:innen für die Umsetzung solcher Angebote waren

i) Workshops und Schulbesuche durch Saferinternet.at,
ii) Fachvorträge von Security-Expert:innen oder CISOs (Chief Information Security Officers) aus Unternehmen,
iii) Kooperationen mit Initiativen und Institutionen wie DigitalCity.Wien, Wirtschaftsagentur Wien, SBA Research, CERT.at, Cybersecurity Austria.

Einzelne Initiativen dieser Art wurden bereits erprobt, stießen jedoch auf strukturelle Hürden. So berichtete ein:e Interviewpartner:in: *„Ein Kollege hat eine Gruppe aus der Cybersecurity-Szene zusammengestellt, die bereit war, an Schulen zu gehen. Es war jedoch sehr schwierig, Zugang zu erhalten – selbst für einen kurzen*

[7] https://schubu.org/
[8] https://verbotengut.at/
[9] https://www.saferinternet.at/
[10] https://www.hackthebox.com/
[11] https://tryhackme.com/
[12] https://hacking-lab.com/
[13] https://www.yeswehack.com/
[14] https://www.hackerone.com/
[15] https://www.northgrc.de/

Vortrag am Vormittag.“ Dies verdeutlicht den **Bedarf an klaren Rahmenbedingungen**, um solche Kooperationen langfristig und niederschwellig zu ermöglichen.

Die erfolgreiche Integration von Cybersecurity in schulische Bildungsprozesse erfordert ein Zusammenspiel mehrerer Akteur:innen. Im Projekt wurde wiederholt betont, dass insbesondere ein **„Dreiergespann“ aus Lehrkräften, Eltern bzw. Erziehungsberechtigten und Schüler:innen** angesprochen und eingebunden werden muss, um nachhaltige Wirkung zu erzielen (siehe **Error! Reference source not found.**). Alle Beteiligten müssen ein grundlegendes Verständnis davon entwickeln, was Cybersecurity bedeutet und welche Relevanz das Thema für Bildung, Alltag und Berufsleben hat.

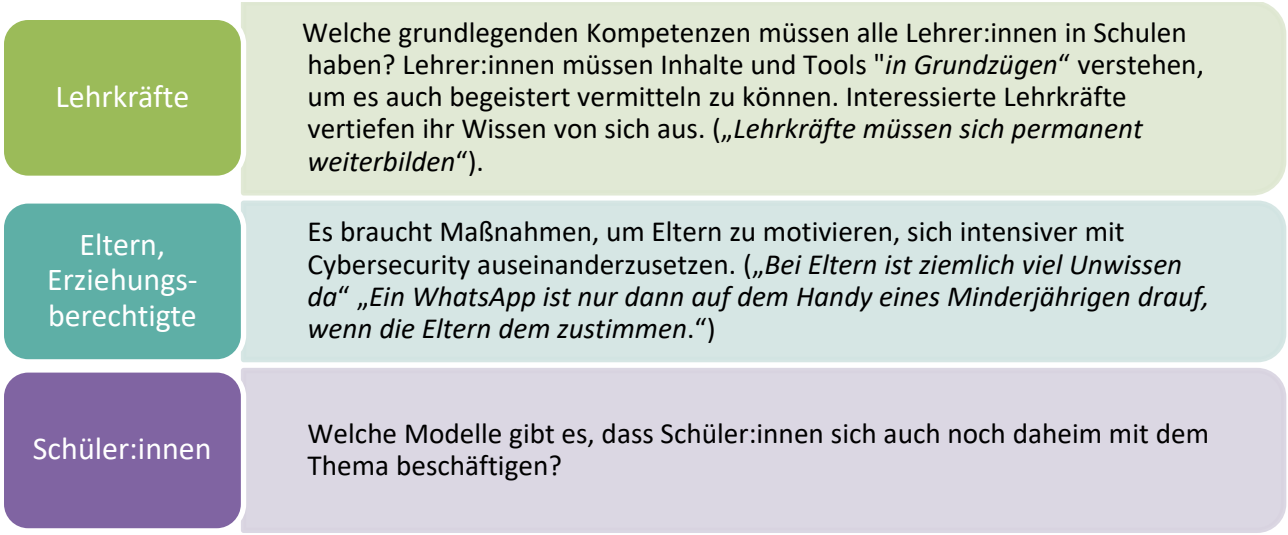

Abbildung 5: Dreiergespann für Cybersecurity-Themen

Exkurs: KI-Bots als Lehrkräfte als Reaktion auf die Dynamiken im Bereich Cybersecurity?

In den Interviews wurde deutlich, dass die Geschwindigkeit und Komplexität der Entwicklungen im Bereich Cybersecurity traditionelle Lehrer:innenfortbildungen zunehmend überfordert. („*Es läuft darauf hinaus, dass wir aus der Cloud lernen. Eigentlich sollte man alle Bemühungen, Lehrkräfte zu qualifizieren, über Bord werfen – wir können gar nicht mehr mit der Komplexität mitkommen.*“)

Statt auf klassische Fortbildungsmaßnahmen zu setzen, wurde die Idee benannt, **KI-gestützte Bots wie Siri oder Gemini als digitale Lehrkräfte einzusetzen**. Kinder und Jugendliche würden dann direkt aus der Cloud lernen – unterstützt von Bots, die Inhalte personalisiert und in Echtzeit vermitteln. Voraussetzung dafür sei, dass der Bot den Kindern und Jugendlichen gegenüber wohlwollend agiere. Ein Bot könnte die bestmögliche Chance darstellen, um mit der aktuellen Informationsflut umzugehen. Besonders hervorgehoben wurde Siri als bereits funktionierender Assistent – allerdings nur dann, wenn man bereit ist, umfassend persönliche Daten zu teilen. Einerseits bieten solche Systeme eine realistische Möglichkeit, mit der technologischen Entwicklung Schritt zu halten. Andererseits ist der „Preis“ dafür ziemlich hoch – und nicht nur finanzieller Natur, sondern vor allem gesellschaftlich und ethisch im Hinblick auf Datenschutz, Abhängigkeiten von Tech-Konzernen, und pädagogische Verantwortung.

3.3.4 Qualifizierung der Lehrkräfte

Bei der Qualifizierung von Lehrkräften zeigt sich ein vielschichtiger Bedarf: Lehrpersonen benötigen nicht nur fundiertes fachliches Wissen, sondern auch didaktische, kommunikative und medienpädagogische Kompetenzen, um das Thema altersgerecht, sicher und anschlussfähig zu unterrichten.

Dabei gibt es besondere Anforderungen an Lehrkräfte. Diese sehen sich zunehmend mit einer ambivalenten Wissenslage konfrontiert: Einerseits verfügen viele Jugendliche über technisches Vorwissen oder ein „vermeintliches Halbwissen“, das auf Internetquellen oder eigener Nutzung basiert.

- „*Jugendliche haben ein gewisses vermeintliches Wissen – eher so ein Halbwissen – dies dann klar und richtig zu stellen erfordert, dass man sich mit der Materie sehr, sehr gut auskennt*.“

- *„SchülerInnen wissen in spezifischen Bereichen mehr als die LehrerInnen*“; „*Ich finde uns LehrerInnen fehlt ganz viel an Wissen – die SchülerInnen sind uns da voraus“*

Daraus ergibt sich ein hoher Anspruch an die fachliche Tiefe der Lehrkräfte. Andererseits sind Jugendliche häufig noch nicht in der Lage, Zusammenhänge korrekt einzuordnen oder Risiken realistisch zu bewerten. Betont wird zudem, dass das Selbstverständnis der Rolle als Lehrkraft überdacht werden muss: **Lehrkräfte werden im Kontext von Cybersecurity eher zu Lernbegleiter:innen und Coaches**, die externe Expertise einbinden und gemeinsam mit den Schüler:innen Lernprozesse gestalten. Für all diese Anforderungen braucht es **ausreichend Schulungsmöglichkeiten** für die Lehrkräfte.

Bisher wurde der Zugang zu qualitativ hochwertigen Fort- und Weiterbildungsangeboten als unzureichend bewertet (*„die PH ist hier der falsche Ansprechpartner*“). Benötigt wird eine **systematische Qualifizierungsstruktur sowie zeitlich und didaktisch flexible Formate**, um Wissen auf- und ausbauen zu können. Bisher eignen sich die Lehrkräfte das Wissen selbstgesteuert und autonom an. Informationsressourcen, die dabei genutzt werden, sind Saferinternet, Bundeskriminalamt (BKA) – Polizei – LPD Wien, Fachtagungen wie EduDay, eBazar, Interpädagogica, Pädagogische Konferenzen, sowie online Angebote. Weitere Kooperationspartner, die dabei genannt werden, sind Fachhochschulen, Unternehmen, Kompetenzzentrum sicheres Österreich (KSÖ), Cybersecurity Expert:innen, Innenministerium, Bundeskriminalamt oder die Landesregierungen.

Dabei ist wiederkehrendes Thema der **Wunsch nach stärkerer Zusammenarbeit mit externen Expert:innen**, etwa in Form von Vorträgen, Workshops oder Co-Teaching-Modellen. Lehrkräfte könnten dabei fachlichen Input übernehmen, um diesen didaktisch-methodisch aufzubereiten. Kooperationen mit externen Partner:innen gelten als Schlüssel, um aktuelles und anwendungsnahes Wissen ins Klassenzimmer zu bringen – vorausgesetzt, es bestehen geeignete Rahmenbedingungen und Zugangsmöglichkeiten. Zusammenfassend lässt sich festhalten, dass es derzeit sowohl online als auch offline an ausreichend qualitativen Fortbildungsangeboten für Lehrkräfte im Bereich Cybersecurity mangelt. Für die sogenannte Transferzeit – also den Zeitraum, der benötigt wird, um Lehrkräfte entsprechend auszubilden und weiterzubilden – ist es wesentlich, externes Wissen und externe Inhalte gezielt in das Bildungssystem einzubringen. Hier spielen Cybersecurity-Expert:innen aus Wirtschaft, Wissenschaft und Zivilgesellschaft eine zentrale Rolle. Damit diese Expert:innen jedoch effektiv in schulische Prozesse eingebunden werden können, braucht es geeignete strukturelle und organisatorische Rahmenbedingungen an Schulen. Dazu zählen u. a. zeitliche Freiräume, offene Formate der Zusammenarbeit sowie die Bereitschaft zur Öffnung der Schule gegenüber externem Input.

Exkurs: Good Practice CyberHAKs

Die drei CyberHAKs (Wien Floridsdorf, Horn, Tamsweg) in Österreich haben gemeinsam ein Lehrkonzept für Cybersecurity entwickelt und sich die nötigen Inhalte in engem Austausch angeeignet. Einmal jährlich veranstalten alle drei Standorte zu Schulbeginn einen Cybersecurity-Kick-off, bei dem sich Lehrkräfte vernetzen, Erfahrungen austauschen und Expert:innen aus dem Bereich einladen.

Die Kompetenzvermittlung basiert auf einer Kombination aus weitergebildeten Lehrkräften (mit Basisausbildung) und der Zusammenarbeit mit externen Fachkräften, etwa aus dem Innenministerium, dem Bundeskriminalamt oder der Landesregierung. So konnten etwa Fortbildungen wie eine mehrtägige Stabsausbildung ermöglicht werden. Als Kooperationspartner für weitere Qualifizierungen bieten sich auch Fachhochschulen (FHs) und (Anwar et al., 2017)(PHs) an.

Besonders hervorgehoben wurde, dass ein Großteil der Weiterbildung bisher in der Freizeit der Lehrkräfte stattfand – ein klarer Hinweis auf den Bedarf nach besseren strukturellen und zeitlichen Rahmenbedingungen für schulinterne Qualifizierung.

3.3.5 Rahmenbedingungen

Die erfolgreiche Vermittlung von Cybersecurity in Schulen setzt klar definierte organisatorische und inhaltliche Rahmenbedingungen voraus. Analog zur digitalen Grundbildung gilt: Digitale Kompetenz entsteht nicht von selbst, sie braucht ausreichend Zeit, qualifiziertes Personal und geeignete Ressourcen. Die bloße Bereitstellung von Geräten wie Laptops oder iPads reicht nicht aus, wenn Lehrkräfte weder die notwendigen Kenntnisse noch die passende Software oder didaktische Unterstützung haben.

- Ein zentrales Element ist daher die *Qualifizierung der Lehrkräfte*, wie bereits im vorigen Abschnitt beschrieben.
- Weiters ist eine *zentrale Kontaktadresse* für Lehrkräfte bei Vorfällen notwendig. Lehrkräfte benötigen Handlungsspielräume, Unterstützung bei Vorfällen sowie verlässliche Ansprechstellen – idealerweise eine zentrale Stelle im Bildungsministerium, die sowohl technische als auch pädagogische Hilfestellung bietet. Beispiele wie genannte Vorfälle von Cybermobbing zeigen, dass Schulen derzeit häufig überfordert sind, insbesondere bei Themen mit strafrechtlicher Relevanz. Es gibt keine klare Stelle, an die sich Lehrkräfte in diesen Fällen wenden können. Daher wird der Wunsch nach einer zentralen Kontaktadresse – sowohl für Lehrkräfte als auch für Schüler:innen – wurde mehrfach betont. (Notwendig ist zudem ein Blackout-Management und ein Jugendschutzkonzept für das Thema Cybersecurity.)
- Klärung *rechtlicher Rahmenbedingungen*. Themen wie Darknet oder Hacking sind pädagogisch wichtig, können jedoch aus rechtlichen Gründen nicht praxisnah vermittelt werden. (Beispiel: Darknet und Hacken interessiert die Jugendlichen besonders und manche Jugendliche kommen damit in Berührung. Im Unterricht kann man dies ansprechen, aber Lehrkräften ist oftmals nicht klar, ob sie es ihnen zeigen dürfen beziehungsweise man sich dabei strafbar macht.)
- *Rahmenbedingungen für die Einbindung von ExpertInnen*: Mehrfach wird der Bedarf der Einbindung externer Expert:innen formuliert sowie der Aufbau klarer Kooperationsstrukturen, etwa mit IT-Dienstleistern, Cybercrime-Hotlines oder Polizei- und Präventionsstellen. Hier braucht es Rahmenbedingungen, die definieren, wer wie in Schulen eingeladen werden kann.
- Auch auf systemischer Ebene, etwa bei *Prüfungsformaten* (z. B. Reifeprüfung), stellt sich die Frage nach geeigneten Expert:innen und Verantwortlichkeiten, da es bislang kein formales Lehramtsstudium für Cybersecurity gibt.

Diese in den Interviews genannten Punkte sind ein Teil der notwendigen Rahmenbedingungen und wurden von verschiedenen Teilnehmer:innen mehrfach genannt. Im Zuge der Verankerung von Cybersecurity im Unterricht sollten diese Themen unbedingt mitbedacht werden.

3.3.6 Gender

Ein Thema, das in den Interviews wiederholt angesprochen wurde, ist die Frage nach Geschlechter(un)gerechtigkeit in der Vermittlung von Cybersecurity. Studien deuten darauf hin, dass sich Frauen in Bezug auf ihre Selbstwirksamkeit im Bereich Cybersecurity tendenziell geringer einschätzen als Männer (Anwar et al., 2017). Daraus ergeben sich die zentralen Fragen:

- *Wie kann sichergestellt werden, dass Schülerinnen die gleichen Chancen wie Schüler bei der Vermittlung von Bildungs- und Berufsangeboten erhalten?*
- *Wie kann verhindert werden, dass Mädchen benachteiligt werden?*

Ziel sollte es sein, stereotype Rollenzuschreibungen zu vermeiden und weibliche Vorbilder im Cybersecurity-Bereich sichtbar zu machen, um der Benachteiligung von Mädchen aktiv entgegenzutreten. Aus den Interviews ging hervor, dass bei gemischten Klassen oft beobachtet wird, dass Mädchen „untergehen". Burschen drängen sich in den Vordergrund und übernehmen lautere Rollen, wodurch Mädchen seltener zu Wort kommen. Gleichzeitig zeigen Erfahrungswerte, dass die Motivation bei Burschen häufig stärker auf Wettbewerb basiert, während Mädchen sich tendenziell stärker für gemeinschaftsorientierte Ziele („*for the greater good*") begeistern lassen. Diese (stereotypischen) Unterschiede wirken sich insbesondere auf die Wirksamkeit gamifizierter Lernformate aus, die oft auf Wettbewerb ausgerichtet sind und dadurch eher männliche Schüler ansprechen. Es stellt sich daher die Frage: *Welche didaktischen Maßnahmen können ergriffen werden, um eine geschlechtergerechte Ansprache in der Cybersecurity-Bildung zu gewährleisten?* Hier sind ein paar Punkte, die aus den Interviews als wichtig hervorgingen beziehungsweise als mögliche Strategie genannt wurden:

- Alle Themen für alle („*Zentral ist, dass alle das Gleiche hören*"): Es ist essenziell, dass alle Schüler:innen die gleichen Inhalte erhalten („*Alle Themen sollen Allen angeboten werden*"). Eine geschlechtergetrennte Themenvergabe – *„Buben hacken und mit Mädchen thematisiert man Cybermobbing"* – ist zu vermeiden.
- Gemischte vs. getrennte Settings: Da in gemischten Klassen Mädchen oft weniger zu Wort kommen, könnten phasenweise getrennte Unterrichtseinheiten sinnvoll sein. Es stellt sich allerdings die Frage, ob durch ein geschlechtergetrenntes Setting nicht geschlechtsstereotype erst recht befeuert werden, wie der nächste Punkt beschreibt.
- Gendersensible Didaktik statt Stereotypisierung: Gleichzeitig darf es nicht zu einer Festschreibung geschlechtsspezifischer Motivationen kommen. Mädchen können ebenso kompetitiv sein wie

Burschen gemeinschaftsorientiert – daher ist es wichtig, vielfältige Zugänge für alle anzubieten. Formate sollten verschiedene Motivationsformen ansprechen, um individuelle Stärken unabhängig vom Geschlecht zu fördern.

4 Cybersecurity-Themenbereiche & Perspektive aus dem Arbeitsmarkt

Im Rahmen des zweiten Subziels des *CLEMENTINE*-Projekts wurde die Identifikation arbeitsbezogener Cybersecurity-Themen vorgenommen. Aufbauend auf den Erkenntnissen aus den Fokusgruppen mit Schüler:innen und den Interviews mit Expert:innen an der Schnittstelle Schule und Cybersecurity wurden mittels weiterer Expert:innen-Interviews sowie einer Umfrage mit Cybersecurity-Verantwortlichen arbeitsmarktrelevante Cybersecurity-Themen identifiziert und branchenspezifische Anforderungen (Banken, Energie, Handel) erhoben, um Einblicke in die unternehmerische Praxis zu gewinnen.

4.1 Perspektive aus dem Arbeitsmarkt

Es wurden **vier qualitative Interviews** mit Cybersecurity-Verantwortlichen aus den Branchen Banken, Energie und Handel durchgeführt sowie mit dem Leiter des nationalen Computer-Notfallteam CERT.at (Computing Emergency Response Team), das eine zentrale Rolle bei der Koordinierung der Incident-Response bei österreichischen und internationalen Cybervorfällen spielt.

Aus den Interviews lassen sich folgende Erkenntnisse ableiten:

(1) Risiken und Anforderungen im Unternehmen

In allen Interviews wurde **Phishing und Social Engineering** als derzeit größte Bedrohung für Unternehmen identifiziert. Insbesondere da bei diesen Angriffen auf menschliche Schwächen abgezielt wird – ein einziger Klick genügt, um ein Unternehmen zu kompromittieren. Mitarbeiter:innen spielen entsprechend eine zentrale Rolle bei der Abwehr solcher Gefahren. Für den schulischen Bereich wurde in diesem Kontext der Wunsch geäußert, dass Lehrkräfte idealerweise mit den aktuellsten Phishing-Methoden vertraut sein sollten – zumindest mit den häufigsten Vorgehensweisen zum Zeitpunkt des Unterrichts.

Neben dieser direkten Bedrohung wird die **mangelnde technische Grundkompetenz** als eine der größten Herausforderungen genannt *(„Was mir fehlt, ist das Basiswissen: Wie funktioniert IT überhaupt? Ohne dieses Wissen kann man Cybersecurity nicht verstehen.“*). Dazu gehören z. B. das fehlende Verständnis dafür, wie E-Mails funktionieren, wie Authentifizierung abläuft oder wie Daten sicher geteilt werden können. Mehrere Interviewpartner:innen betonen, dass Mitarbeitende häufig reine „Klick-Anwender:innen“ seien – **ohne Bewusstsein für die Abläufe im Hintergrund**.

Eine weitere Herausforderung, die für die befragten Unternehmen zunehmend eine Rolle spielt, ist die **fehlende Trennung – teils auch die bewusste Vermischung – der beruflichen und privaten Nutzung** von Geräten oder Accounts. Dies eröffnet neue Angriffsvektoren, bspw. durch Phishing-Angriffe auf private Logins, die sich durch die zunehmende Vermischung auch auf beruflicher Ebene auswirken können.

(2) Langfristig relevante Themen und Zukunftsthemen

Folgende Cybersecurity-Themen wurden von den Interviewpartner:innen als **langfristig relevant** benannt:

- Phishing & Social Engineering
- Grundlagenwissen zur IT-Infrastruktur (z. B. Netzwerke, E-Mails, Firewalls)
- Patch- und Schwachstellenmanagement
- Datenklassifikation und sicherer Umgang mit Daten
- Regulatorische Basiskonzepte (z. B. NIS2, Risikomanagement oder das NIST-Framework)
- Kritisches Denken & Datenschutz im Alltag

Gemäß den Expert:innen werden diese Themen unabhängig von technologischen Trends als zentral für die Abwehr von Cyberangriffen betrachtet, weshalb sie sich besonders gut für die Verankerung in Lehrplänen eignen. Zusätzlich dazu sollte jedoch mittels flexibel einsetzbarer Module auf aktuelle Entwicklungen reagiert werden können. Gegenwärtig werden folgende Themen als **besonders zukunftsrelevant** wahrgenommen bzw. als bereits relevant, jedoch noch viel zu selten abgedeckt:

- Künstliche Intelligenz auf drei Ebenen *(„Deepfakes, generative KI – das ist schon jetzt da. Aber in Schulungen fehlt das komplett.“*):
  - Professionalisierung von Cybercrime durch generative KI und Deepfakes
  - Kritischer Umgang mit der zunehmenden Anzahl unterschiedlicher KI-Tools
  - Kritische Bewertung des Datenschutzes bei der Nutzung von KI-Tools
- Cloud-Nutzung und Sicherheit
- Digitale Souveränität und Plattformabhängigkeit

Aufgrund der Schnelllebigkeit digitaler Technologien wurde der Wunsch an Schüler:innen geäußert eine hohe Lernbereitschaft, eine Art „Updatewillen“ mitzubringen. Das Bedürfnis, sich kontinuierlich über neue Betrugsformen und Bedrohungen zu informieren, sei eine zentrale Kompetenz im Bereich Cybersecurity,

(3) Schulungsinhalte und -formate

Die Interviewpartner:innen wurden auch gefragt, welche Inhalte sie in ihren Schulungen behandeln und welche Formate sie als erfolgsversprechend wahrnehmen. Alle Unternehmen bieten **Pflichtschulungen an, die an alle Mitarbeiter:innen gerichtet sind und sich auf die „Basics“ konzentriere**n (z. B. Phishing-Erkennung, Passwortsicherheit, Datenklassifikation, Social Engineering). Zusätzlich dazu werden unterschiedliche Lernformate wie Spiele (Brettspiele, Escape Rooms), Awareness-Kampagnen mit **Storytelling** oder **interaktive E-Learnings** angeboten.

Als zentral für die erfolgreiche Durchführung solcher Formate wird das **Herstellen von Relevanz** genannt: *„Es geht nicht darum, immer neue Schulungen zu machen, sondern die Leute zu erreichen. Das geht nur, wenn sie es als relevant empfinden“.* Orientieren sich Schulungsinhalte am Unternehmenskontext und der Rolle der Mitarbeitenden, steigt die Relevanz deutlich. Ein „One-Size-Fits-All“-Ansatz wird hingegen als wenig effektiv bewertet. Zentral ist dabei, einfache und verständliche Sprache zu verwenden.

Alle Interviewten unterstützen die Idee, **Sicherheitskompetenzen früh zu fördern**. Bei Jugendlichen gilt dabei, dass sie besonders gut erreichbar sind, wenn sie den **persönlichen Bezug** erkennen – etwa beim Schutz ihres Smartphones, ihrer Accounts oder ihrer persönlichen Daten. Um mögliche Fehlentwicklungen (z. B. Schulhacks) früh zu adressieren, sollten **Jugendliche auch hinsichtlich ethischer Grenzen sensibilisiert werden**. Themen wie Pentesting, White-Hat und Black-Hat-Hacking sowie die Beschäftigung mit dem Darknet eignen sich dafür nicht nur besonders gut, sondern stoßen bei den Jugendlichen auch auf großes Interesse.

4.2 Umfrage mit Cybersecurity-Verantwortlichen in Unternehmen

Zusätzlich zu den qualitativen Interviews wurde eine quantitative Umfrage mit Cybersecurity-Verantwortlichen in Unternehmen durchgeführt, um aktuelle Herausforderungen und Kompetenzbedarfe im Bereich Cybersecurity zu erfassen. Die Befragung konzentrierte sich auf drei Fragestellungen:

(1) Welche Cybersecurity-Bedrohungen in Unternehmen durch höhere Kompetenzen von Beschäftigten reduziert werden könnten („*Welche sind die größten Cybersecurity-Bedrohungen/Risiken in Ihrem Unternehmen, die über mehr Cybersecurity-Kompetenzen bei Arbeitnehmer:innen vermieden oder verringert werden können? Bitte beschreiben Sie 2-3 Bereiche (z.B. Ransomware/Erpressung, Advanced Persistent Threats, Insider Threats, Datendiebstahl, Identitätsdiebstahl, Social Engineering, staatliche oder staatlich unterstützte Angriffe.*“).
(2) Welche grundlegenden Cybersecurity-Kenntnisse für Mitarbeitende außerhalb der IT-Sicherheitsabteilungen erforderlich sind („*Was sollten Beschäftigte in Ihrem Unternehmen, die NICHT im Bereich Informationssicherheit tätig sind, in Bezug auf Cybersecurity können/wissen, um CS-Probleme zu vermeiden? Nennen Sie die wichtigsten 3-5 Bereiche (z.B. Umgang mit Passwort-Manager, sicheres Surfen, sicherer Umgang mit Geräten, Erkennen von Bedrohungen, Nachrichten-Verschlüsselung, Software- und Systemaktualisierung*.“).
(3) Welche Kompetenzen sollen bereits in der Schule vermittelt werden, um junge Menschen besser auf die Anforderungen des digitalen Arbeitsmarkts vorzubereiten. (*„Welche Kompetenzen sollten Ihrer Meinung nach in der Schule als Vorbereitung auf den Arbeitsmarkt stärker vermittelt werden?“).*

Die Ergebnisse liefern wertvolle Einblicke in konkrete Bedrohungsszenarien – etwa Phishing, Social Engineering oder Ransomware – sowie in den Bedarf an praktischen Alltagskompetenzen wie Passwortmanagement, sicherer Geräteumgang und Awareness für digitale Risiken.

Insgesamt nahmen 68 Personen an der Umfrage teil, der Großteil davon war in der Branche Information & Consulting beschäftigt (10), gefolgt von Transport & Verkehr (8) und Banken & Versicherung (4). Die Teilnehmenden stammten sowohl aus kleinen und mittleren Unternehmen als auch aus großen Unternehmen, die Unternehmensgröße variierte von 23 bis zu über 40.000 Personen.

Cybersecurity Bedrohungen & Risiken im Unternehmen

Im Rahmen der Umfrage wurden verschiedene Bedrohungen identifiziert, die derzeit als besonders relevant für die Cybersecurity in Unternehmen eingeschätzt werden (siehe Tabelle 4).

Tabelle 4: Cybersecurity Bedrohungen & Risiken im Unternehmen

Themen	Beschreibung
Phishing (19 Nennungen)	• Allgemeines Phishing und Spear-Phishing. • Phishing als Einstiegspunkt für weitere Straftaten, insbesondere Ransomware. • Gefälschte E-Mails zur Täuschung von Mitarbeitenden. • Phishing-Angriffe mit dem Ziel, Daten abzufangen oder Accounts zu übernehmen. • Generative KI professionalisiert Phishing-Nachrichten
Social Engineering (17 Nennungen)	• Mangelndes Wissen über Manipulationstechniken und deren Erkennung. • Konkrete Angriffsformen wie CEO Fraud und Wirtschaftsspionage. • Der Einsatz von Deep Fakes zur Täuschung oder Irreführung.
Datendiebstahl und Datenabfluss (13 Nennungen)	• Diebstahl sensibler Informationen wie Kunden- oder Unternehmensdaten. • Datenabfluss durch unachtsames Verhalten (Umgang mit Datenträgern, Ausdrucken) oder gezielte Angriffe.
Ransomware (8 Nennungen)	• Verschlüsselung von Daten mit anschließender Erpressung. • Verbreitung über infizierte Anhänge oder kompromittierte Systeme.
APTs – Advanced Persistent Threats (3 Nennungen)	• Langfristig angelegte, zielgerichtete Angriffe durch professionelle Akteure. • Oft schwer erkennbar und technisch hochentwickelt.
Shadow-IT (1 Nennung)	• Nutzung von Software oder Hardware außerhalb der offiziellen IT-Freigabe. • Gefahr unkontrollierter Datenverarbeitung und Sicherheitslücken.
DDoS-Angriffe (1 Nennung)	• Überlastung eines Netzwerks/einer Website durch Anfragenflut

Die Auswertung der Umfrage zeigt deutlich, dass Phishing und Social Engineering aktuell als die gravierendsten Bedrohungen im Unternehmenskontext wahrgenommen werden (siehe Abbildung 6). Beide gelten nicht nur als direkte Risiken, sondern auch als Einstiegspunkte für weiterführende Angriffe wie Ransomware oder Datendiebstahl. Weniger häufig genannt, aber sicherheitsrelevant, sind komplexere Angriffsformen wie Advanced Persistent Threats (APTs) sowie organisatorische Schwachstellen wie Shadow-IT. Die Ergebnisse unterstreichen die Notwendigkeit gezielter Awareness-Maßnahmen und technischer Schutzkonzepte, um diesen vielseitigen Bedrohungen wirkungsvoll zu begegnen.

Abbildung 6: Cybersecurity Bedrohungen & Risiken in Unternehmen

Was sollten Beschäftigte im Bereich Cybersecurity wissen und können?

1. Sensibilisierung und Awareness

- Erhöhte Aufmerksamkeit: Beschäftigte sollten in der Lage sein, potenzielle Bedrohungen und Angriffsvektoren (z. B. verdächtige E-Mails, ungewöhnliche Zugriffe) frühzeitig zu erkennen.
- Kritisches Denken: Eine „*gesunde Skepsis und Hausverstand*“ gegenüber ungewöhnlichen Situationen oder Anforderungen hilft, Angriffe wie Phishing oder Social Engineering zu verhindern.
- Awareness-Veranstaltungen: Regelmäßige Schulungen und praxisnahe Sensibilisierungen fördern das Sicherheitsbewusstsein im Unternehmen.

2. Arbeitsplatzsicherheit und Grundprinzipien

- Clean Desktop Policy: Der Arbeitsplatz sollte stets frei von vertraulichen Informationen sein – keine offenen Dokumente oder Notizzettel mit Passwörtern.
- Sicherer Umgang mit Daten: Vertrauliche Informationen – digital oder physisch – müssen geschützt und ggf. verschlüsselt übermittelt werden.
- Geräte sperren: Rechner und mobile Geräte sind immer zu sperren, wenn sie unbeaufsichtigt bleiben.
- Sichere Entsorgung: Dokumente und Datenträger müssen ordnungsgemäß und sicher vernichtet werden.
- Verhalten bei Ausnahmen: Bei ungewöhnlichen Anforderungen (z. B. E-Mails mit Zahlungsaufforderungen) müssen interne Protokolle eingehalten werden.
- Vier-Augen-Prinzip: Prozesse müssen von mindestens zwei Personen überprüft werden.

3. Passwortmanagement und -sicherheit

- Starke Passwörter & Passwort-Manager: Komplexe Passwörter in Kombination mit einem Passwort-Manager erhöhen die Sicherheit.
- Keine Wiederverwendung von Passwörtern: Für jeden Dienst sollte ein eigenes Passwort verwendet werden.
- Zentrale Authentifizierung kritisch prüfen: Drittanbieter-Logins (z. B. via Google oder Facebook) sollten nur mit Bedacht verwendet werden.

4. System- und Endgerätesicherheit

- Updates nicht aufschieben: Sicherheitsupdates sollten immer zeitnah installiert werden.
- Gerätekonfiguration: WLAN, PCs, Tablets und Smartphones müssen sicher eingerichtet und genutzt werden.

- Homeoffice & Reisen: Auch außerhalb des Büros gelten Sicherheitsstandards – etwa beim Arbeiten im öffentlichen WLAN oder beim Transport von Geräten.

5. Phishing und Social Engineering

- Phishing erkennen: Verdächtige E-Mails, manipulierte Links oder falsche Absenderadressen müssen zuverlässig identifiziert und gemeldet werden.
- Spam/Phishing richtig behandeln: Betroffene E-Mails dürfen weder beantwortet noch angeklickt, sondern müssen gemeldet und gelöscht werden.
- Social Engineering im physischen Raum vorbeugen: Angriffsformen wie Tailgating[16], Shoulder Surfing[17] oder Dumpster Diving[18] müssen bekannt und erkannt werden.
- Auswirkungen verstehen: Wer die Gefahren kennt, kann angemessen reagieren und Risiken reduzieren.

6. Sichere Nutzung von E-Mail und Internet

- Kritische Grundhaltung: Nicht jeder Link, Anhang oder Absender ist vertrauenswürdig – Wachsamkeit ist oberstes Gebot.
- E-Mail-Nutzung: Die dienstliche E-Mail-Adresse darf ausschließlich für berufliche Zwecke verwendet werden.
- Internetnutzung: Nur verschlüsselte Kommunikation (z. B. HTTPS) verwenden, keine Schatten-IT (nicht genehmigte Tools und Dienste) nutzen.

7. Kommunikation und Meldewesen

- Ansprechstellen kennen: Beschäftigte müssen wissen, wen sie im Verdachtsfall oder bei Sicherheitsvorfällen kontaktieren.
- Meldepflichten einhalten: Auffällige Aktivitäten oder jeder Vorfall soll weitergeleitet werden.
- Klarheit über offizielle Meldewege: Es muss klar sein, wie und über welche Kanäle sicherheitsrelevante Informationen weitergegeben werden.

Welche Kompetenzen sollten bereits in der Schule vermittelt werden?

Die identifizierten Themen betreffen zentrale Aspekte von Cybersecurity, die im Rahmen der digitalen Grundbildung gezielt vermittelt werden sollten, um Jugendliche auf sicherheitsrelevante Anforderungen in der Arbeitswelt besser vorzubereiten. Grundlegend lassen sich dabei drei übergeordnete Themenbereiche unterscheiden (siehe Erin KrAbbildung 7):

- Hardware
- Software
- Gesellschaft, Verhalten und Umgang mit digitalen Technologien

Erin KrAbbildung 7: Bereiche der Cybersecurity Themen

Wichtig ist hierbei ein multiperspektivischer Blick, in dem man sich mit digitalen Artefakten technologisch (welche Technologien stecken dahinter), interaktiv (wie gehe ich mit den digitalen Artefakten verantwortungsvoll um) und gesellschaftlich/kulturell (welche Regelungen und Rahmenbedingungen beziehungsweise welche ethischen und ökonomischen Implikationen gibt es) beschäftigt.

[16] Beim Tailgating versuchen Angreifer, Zugang zu eingeschränkten physischen Bereichen zu erhalten, indem sie autorisierten Personen folgen (z. B. beim Durchgehen durch Türen).
[17] Beim Shoulder Surfing erspähen Angreifer sensible Daten (z. B. Geheimzahlen wie PIN oder Passwörter, Kreditkartendaten) mittels „Blick über die Schulter“ im öffentlichen Raum.
[18] Beim Dumpster Diving versuchen Angreifer, durch das Durchsuchen von physischem oder digitalem „Müll“ (z. B. ausgedruckte Unterlagen, gelöschte Dateien) an sensible Daten zu gelangen.

Insgesamt kristallisierte sich basierend auf den Ergebnissen der Interviews, den Fokusgruppen mit den Jugendlichen, der Online-Befragung sowie den kontinuierlichen Reflexionen im Projektkonsortium, folgende relevante Themen heraus. Diese Auflistung kann als Grundlage für die curriculare Ausgestaltung im Bereich Cybersecurity dienen und je nach Schwerpunktsetzung oder Interessen erweitert bzw. angepasst werden.

Tabelle 5: Arbeitsbezogene Cybersecurity Themen

Themen	Inhalte
1. Grundlagen der Cybersecurity	• Was ist Cybersecurity? • Welche Arten von Bedrohungen gibt es (Malware, Phishing, etc.) • Welche Arten von Bedrohungen gibt es aktuell? • Wie agieren HackerInnen? • Ethische Aspekte • Digitaler Fußabdruck
2. Sichererer Umgang mit Geräten und Netzwerken	• Wie schütze ich ein Netzwerk? (Netzwerksicherheit) • Schutz vor Malware • Updates und Patching
3. Social Media	• Sicherer Umgang & Schutz der Daten • Fake News, Desinformation, Hate Speech • Sicheres und gutes Verhalten in Online-Umgebungen
4. Erkennen & Vermeiden von Cyber-Bedrohungen	• Phishing, Downloads von gratis Software • Phishing: Kenntnis der aktuell 10 wichtigsten Phishing Vorgehensweisen • Emails (Anhänge, Links)
5. Passwörter	• Passwortschutz • Wie geht man mit Passwörtern um? • Passwortmanager und sichere Verwaltung
6. Datensicherheit und Datenschutz	• Datensicherheit: Schutz der persönlichen Daten • Datenschutz: Bedeutung von Privatsphäre • Datenverschlüsselung
7. Accounts	• Wo erstelle ich mir Accounts - mit welchen Daten? • Schutz der persönlichen Daten in Accounts

5 Analyse existierender Lehrpläne und Schulmaterialien

Bevor eine Analyse der Lehrpläne der Sekundarstufe 2 durchgeführt und gemäß des Projektes *CLEMENTINE* Empfehlungen für allfällige Lehrplanänderungen ausgearbeitet werden, sollte der Begriff Lehrplan einer tieferen Betrachtung zugeführt werden:

Lehrpläne sind für Pädagoginnen und Pädagogen die Grundlage ihrer eigenständigen und verantwortlichen Unterrichts- und Erziehungsarbeit. Aufgabe der Lehrerinnen und Lehrer ist es, durch geeignete Planung und Gestaltung des Unterrichts den einzelnen Schülerinnen und Schülern die Erreichung der im Lehrplan vorgegebenen Ziele zu ermöglichen. Sie sind ein Orientierungsrahmen für Schülerinnen und Schüler sowie Erziehungsberechtigte, über welches Wissen und Können Schülerinnen und Schüler am Ende eines Schuljahres verfügen sollen. Darüber hinaus bilden sie den Bezugspunkt für die Entwicklung von Lehrmitteln sowie für die Aus-, Fort- und Weiterbildung von Lehrpersonen.[19]

Daraus wird ersichtlich, dass es sich um Rahmenvorgaben handelt, die von einer qualifizierten und erfahrenen Lehrperson an die aktuellen Gegebenheiten der jeweiligen Lehreinheit angepasst werden müssen. Dadurch soll sichergestellt werden, dass Lehrende die notwendige Unterrichtsfreiheit erhalten, um einen individuellen und auf die Lernenden zugeschnittenen Unterricht zu gestalten. Dieser Freiheitsgrad ermöglicht es zudem, dass Lehrkräfte – beispielsweise in HTLs – ihre beruflichen Spezialisierungen einbringen und Schulen allgemeine Ausbildungsschwerpunkte setzen können.

Wo Vorteile sind, gibt es auch Nachteile. Nachdem Lehrpläne von Lehrplankommissionen erstellt, diese aber durch einen anderen Personenkreis umgesetzt werden, ergeben sich durch die besprochenen Freiheitsgrade automatisch Diskrepanzen in der Umsetzung und Zielerreichung. Hier einige viel diskutierte[20] und wahrscheinlich ewig ungelöste Widersprüche:

- **Überfrachtung der Lehrpläne**: Bildungsexpert:innen bemängeln, dass die Lehrpläne mit zu vielen Themen und Erwartungen überladen sind. Dies führt dazu, dass Lehrkräfte Schwierigkeiten haben, alle Inhalte angemessen zu behandeln.
- **Unrealistische Zielsetzungen**: Es wird kritisiert, dass die vorgegebenen Ziele in der Praxis kaum erreichbar sind. Die Vielzahl an Themen und Kompetenzen, die vermittelt werden sollen, übersteigt oft die zeitlichen und personellen Ressourcen der Schulen.
- **Mangelnde Flexibilität**: Früher hatten Schulen und Lehrkräfte mehr Freiheit, Inhalte auszuwählen und Schwerpunkte zu setzen. Heute wird erwartet, dass alle Vorgaben vollständig umgesetzt werden, was die pädagogische Kreativität einschränkt.
- **Praktische Umsetzbarkeit**: Lehrer:innenverbände weisen darauf hin, dass die Lehrpläne oft nicht auf die Realität in den Klassenzimmern abgestimmt sind, insbesondere bei großen Klassen und begrenzten Ressourcen.

All dies zusammen führt zu einem **Lehrplan-Dilemma**, das maßgeblich vom zu vermittelnden Fachgebiet – etwa einer sich stark wandelnden technischen Disziplin – sowie von der erforderlichen Qualifikation der Lehrperson abhängt.

Im Konkreten betrachtet sind Lehrpläne generell darauf ausgelegt, Inhalte und Lernziele möglichst klar und nicht einschränkend zu formulieren. Es bleibt in Wirklichkeit aber unklar, in welchem Ausmaß und mit welcher Präzision diese Vorgaben umgesetzt werden. Denn die verwendeten Begriffe sollen einerseits einen „*eigenständigen und verantwortlichen*" Unterricht der Lehrperson zulassen und andererseits baut man auf der **Qualifikation** der Lehrpersonen auf, jene Inhalte automatisch zu ergänzen, die für ein Erlernen der Schüler:innen förderlich bzw. zusätzlich notwendig sind[21].

Diese daraus resultierende **fehlende Einheitlichkeit** führt dazu, dass Unterrichtsinhalte und Lernergebnisse von Schule zu Schule (stark) variieren können, wodurch ein konkreter Vergleich der **Bildungsqualität** erschwert wird. Das Problem erstreckt sich über verschiedene Bildungseinrichtungen und betrifft Schüler:innen sowie Lehrkräfte gleichermaßen. Die Frage nach einer standardisierten Umsetzung ohne den Verlust pädagogischer Freiheit bleibt dabei eine zentrale Debatte.

---

[19] https://www.bmb.gv.at/Themen/schule/schulpraxis/lp.html
[20] Beispiele aus Presse: https://orf.at/stories/3285992/, https://www.sn.at/politik/innenpolitik/lehrer-kritik-an-neuen-lehrplaenen-127275619, https://orf.at/stories/3285995/, https://www.schule.at/bildungsnews/detail/nach-heftiger-kritik-am-neuen-lehrplan
[21] https://www.bmb.gv.at/Themen/schule/schulpraxis/lp.html

Das Lehrplan-Dilemma wird besonders deutlich, wenn es z.B. um die **Vergleichbarkeit** der Digitalen Grundbildung – unter ihren vielfältigen Bezeichnungen – zwischen **unterschiedlichen Schultypen** geht. Zwar mögen die Inhalte auf den ersten Blick identisch erscheinen, doch bedingt die grundlegende Differenzierung zwischen Berufsausbildung und Allgemeinbildung zwangsläufig unterschiedliche Lernziele und Schwerpunktsetzungen. Insbesondere innerhalb der berufsbildenden Schulen führt die Spezialisierung zu einer weiteren Differenzierung, die sich nicht nur in den vermittelten Kompetenzen, sondern auch in der variierenden Anzahl der vorgesehenen Wochenstunden niederschlägt.

Grundsätzlich werden daher in dieser Studie für die angestrebte Cybersecurity-**Kompetenztiefe** folgende Bezeichnungen verwendet:

- Basic
- Intermediate
- Professional

Basis-Curriculum Cybersecurity

Eine mögliche Lösung für diese Herausforderung im Bereich der Cybersecurity könnte, einhergehend mit einem begleitenden klassischen Rahmenlehrplan, ein schultypgerechtes, verbindliches Cybersecurity-Basis-Curriculum sein, das die minimalen Kerninhalte und Qualitätsstandards sichert. Ein solches Konzept könnte nicht nur eine einheitliche Grundbildung in diesem essenziellen Themenfeld gewährleisten, sondern zugleich als Grundlage für ein Zertifizierungsverfahren dienen, das erworbene Qualifikationen objektiv bestätigt und vergleichbar macht. So ließe sich eine Balance zwischen pädagogischer Freiheit und übergreifender Standardisierung erreichen.

Schulungsangebote

Die dargestellten Herausforderungen verdeutlichen, wie entscheidend eine gezielte und adäquate Schulung der Lehrkräfte für die erfolgreiche Umsetzung von Lehrplänen ist. Insbesondere im Bereich der Digitalen Grundbildung ist es essenziell, Lehrpersonen umfassend auf die spezifischen Inhalte, Zielsetzungen und pädagogischen Anforderungen vorzubereiten. Eine standardisierte und praxisnahe Qualifikation trägt dazu bei, die Einheitlichkeit und Vergleichbarkeit der Bildungsqualität zwischen verschiedenen Schultypen zu gewährleisten, ohne dabei die pädagogische Freiheit der Lehrkräfte einzuschränken. Durch eine fundierte Schulung können Lehrkräfte besser befähigt werden, die teils abstrakten Vorgaben der Lehrpläne präzise und verständlich umzusetzen sowie den Unterricht flexibel und individuell auf die Bedürfnisse der Schüler:innen anzupassen. Gleichzeitig wird sichergestellt, dass sowohl allgemeine als auch berufsspezifische Bildungsziele in ihrer jeweiligen Differenzierung effektiv vermittelt werden. Eine qualitativ hochwertige Schulung ist somit ein zentraler Schlüssel, um die Diskrepanz zwischen Lehrplanvorgaben und tatsächlicher Unterrichtspraxis zu überwinden und langfristig eine nachhaltige Verbesserung der Bildungsqualität zu erzielen. Es ist daher notwendig, entsprechende Weiterbildungsprogramme zu etablieren und Ressourcen bereitzustellen, die Lehrkräfte in diesem Prozess optimal unterstützen.

Cybersecurity 6-Stufen-Kompetenzmodell: Das CLEMENTINE-6-Stufen-Modell

Um sämtliche relevanten Cybersecurity-Inhalte in einer Analyse angemessen zu berücksichtigen, wurde ein bestehendes, technisches 5-stufiges Kompetenzmodell des BMBWF als Grundlage herangezogen. Dieses Modell wurde gemäß des Studienauftrags durch zusätzliche Inhalte erweitert und zu einem 6-Stufen-Modell (siehe Appendix: Das CEMENTINE-6-Stufen-Kompetenzmodell) adaptiert. Dieses modifizierte Modell bildet nun die Basis für die weiterführende Analyse der Lehrpläne sowie für die Entwicklung von Empfehlungen zur inhaltlichen Anpassung derselben.

Das kommende Schaubild zeigt die Abgrenzung des Clementine-6-Stufen-Modells zum ursprünglichen 5-Stufen-Modell des BMBWF. Wie bereits bei der “Definition Cybersecurity” ausgeführt, beschreiben die bisherigen Definitionen und so auch das 5-Stufen-Modell des BMBWF “nur” die Übertragungsstrecke zwischen den Computern. Daher wurde entsprechend dem Untersuchungsauftrags der Stude entsprechend das bestehende 5-Stufen-Modell zu einem Clementine-6-Stufen-Modell durch eine Verhaltenskomponente (Stufe 0) erweitert, um nun die vor dem Computer sitzenden Menschen in die Cybersecurity Aktivitäten mit

einzubeziehen.

Abbildung 8: Adaptierung des BMBWF-5-Stufen-Kompetenzmodells zum CLEMENTINE-6-Stufen-Kompetenzmodell

Das aktuelle CLEMENTINE-6-Stufen-Modell konzentriert sich bislang ausschließlich auf technische Aspekte und Handlungsinhalte. Für eine erfolgreiche Implementierung in die Lehre bedarf es jedoch zusätzlich methodischer und pädagogischer Vermittlungstechniken (vgl. Frankfurt-Dreieck), die ergänzend einzubeziehen sind, um eine ganzheitliche Betrachtung sicherzustellen.

Frankfurt-Dreieck – Dagstuhl Erklärung

Das Frankfurter Dreieck[22] ist eine Weiterentwicklung des Dagstuhl-Dreiecks[23], das in der Dagstuhl-Erklärung von 2016 formuliert wurde. Während das Dagstuhl-Dreieck digitale Bildung aus drei Perspektiven betrachtet – der technologischen, der gesellschaftlich-kulturellen und der anwendungsorientierten Perspektive – erweitert das Frankfurt-Dreieck diese Ansätze konzeptionell. Es schließt Lücken des Dagstuhl-Dreiecks, wie die Gestaltung von Informatiksystemen und die Rolle des Individuums als handelndes und medial adressiertes Subjekt (Abbildung 9).

[22] https://dagstuhl.gi.de/fileadmin/GI/Allgemein/PDF/Frankfurt-Dreieck-zur-Bildung-in-der-digitalen-Welt.pdf
[23] https://dagstuhl.gi.de/dagstuhl-erklaerung/

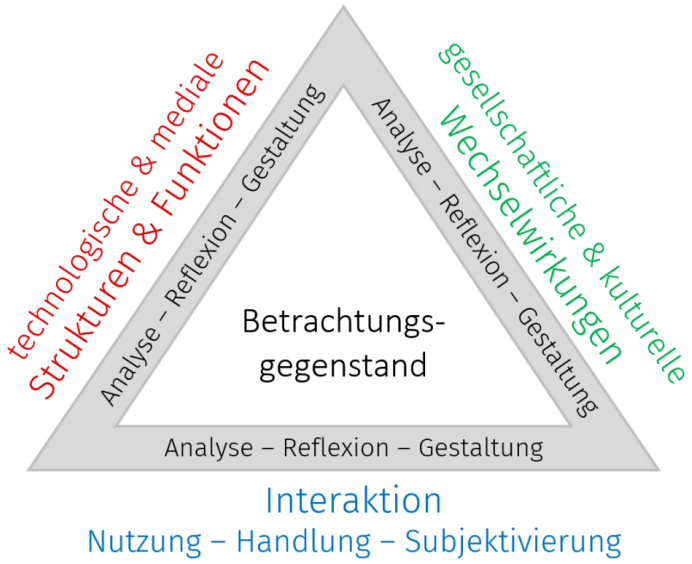

Abbildung 9: Frankfurt-Dreieck (Quelle: https://dagstuhl.gi.de/fileadmin/GI/Allgemein/PDF/Frankfurt-Dreieck-zur-Bildung-in-der-digitalen-Welt.pdf)

Das Modell berücksichtigt drei zentrale Perspektiven:

- **Technologie**: Wie funktionieren digitale Technologien und welche Rolle spielen sie in der Gesellschaft?
- **Kultur**: Wie beeinflussen und formen kulturelle Praktiken den Umgang mit digitalen Technologien?
- **Subjekt**: Welche Positionen und Rollen nehmen Individuen in der digitalisierten Welt ein?

Die Cybersecurity-Bildung steht vor der Herausforderung, abstrakte Konzepte relevant zu vermitteln und Lernende für die ständige Weiterentwicklung der Bedrohungslandschaft zu sensibilisieren. Ziele sind die Entwicklung von Risikobewusstsein, kritischem Denken und praktischen Fähigkeiten zum Schutz im digitalen Raum.

Das Frankfurt-Dreieck kann hier mit seiner multiperspektivischen Erschließung wertvolle Impulse liefern. Die technologisch-mediale Perspektive hilft, die Funktionsweise von Bedrohungen und Schutzmaßnahmen zu verstehen. Die gesellschaftlich-kulturelle Perspektive beleuchtet ethische, rechtliche und soziale Aspekte. Die Interaktionsperspektive fördert sicheres Online-Verhalten im Alltag. Das didaktische Modell bietet einen ganzheitlichen Ansatz, um Cybersecurity-Bildung in der Zusammenschau effektiver und umfassender zu gestalten.

Es wäre daher die Integration des Frankfurt-Dreiecks in dem anstehenden Cybersecurity-Bildungsprozess zu empfehlen. Pädagog:innen und Lehrplanentwickler:innen mögen die Perspektiven des Modells gezielt in ihre Arbeit einbinden, um eine zukunftsorientierte und interdisziplinäre digitale Bildung zu fördern. Dabei gilt es, die technischen Inhalte der Cybersecurity durch gesellschaftlich-kulturelle und methodisch-didaktische Ansätze zu ergänzen, um Lernende nicht nur fachlich, sondern auch persönlich zu stärken und auf die Anforderungen der digitalisierten Welt vorzubereiten. Daher eignet sich das Modell im höchsten Maße, um Cybersecurity und digitale Bildung nachhaltig zu gestalten.

5.1 Übersicht der Lehrpläne – Sekundarstufe 2

Die Lehrpläne der 5. Klasse AHS sowie der HAK von 2014 befinden sich derzeit in Überarbeitung. Auch die HTL-Lehrpläne sollen modernisiert und vereinheitlicht werden. Diese Entwicklungen bieten eine wertvolle Gelegenheit, gezielte Anpassungen im Bereich der Cybersecurity-Bildung einzubringen und entsprechende Inhalte systematisch zu integrieren. Basierend auf den vorliegenden Quellen ist Cybersecurity in den österreichischen Lehrplänen verschiedener Schultypen verankert, wobei der Fokus und die Tiefe je nach Schultyp und Fach variieren. Im Anschluss werden die Lehrpläne hinsichtlich Cybersecurity folgender Schulen analysiert:

- **Allgemeinbildende Höhere Schulen**:
  Lehrplan Digitale Grundbildung - Sekundarstufe 1, Lehrplan Informatik 5. Klasse und Lehrplan Informatik Wahlpflichtfach
- **Handelsakademien und Handelsschulen**:

HAK Lehrplan 2014, HAS Lehrplan 2014 und Spezialisierung CyberHAK

- **Humanberufliche Schulen**:
  HLW Lehrplan 2015, BMS Lehrplan 2015
- **Höhere und mittlere technische und gewerbliche Lehranstalten – relevante Gegenstände aus 62 Lehrplänen**:
  Analyse der Gegenstände „Angewandte Informatik“, „Technologie und angewandte Informatik“, „Medizin- und Gesundheitsinformatik“, „Fachspezifische Softwaretechnik“, „Fachspezifische Informationstechnik“, „Medientechnologie und angewandte Informatik“, des Lehrplan Informatik, des Lehrplans Informationstechnologie, der Gegenstände „Angewandte Informatik und fachspezifische Informationstechnik“, „Informatik und Informationssysteme“, „Informatik, Projekt und Qualitätsmanagement“
- **Mittlere technische gewerbliche und kunstgewerbliche Fachschulen**:
  Analyse des Gegenstands „Angewandte Informatik“, Lehrplan Fachschule Elektrotechnik und technische Informatik, Lehrplan Fachschule Informationstechnologie, Lehrplan Fachschule Informationstechnologie für blinde und sehbehinderte Menschen

Allgemeinbildende Höhere Schulen (AHS)

Die **Digitale Grundbildung** in der AHS-Unterstufe vermittelt essenzielle digitale Kompetenzen. Schwerpunkte sind Medienbildung, informatische Grundlagen, Gestaltungskompetenz sowie gesellschaftliche Aspekte der Digitalisierung. Sie ist in der Oberstufe ein Pflichtfach mit mindestens einer Wochenstunde, mit dem Ziel Schüler:innen auf einen verantwortungsvollen Umgang mit digitalen Technologien vorzubereiten.

- Im Lehrplan für **Digitale Grundbildung** in der Sekundarstufe 1 (Unterstufe) liegt der Schwerpunkt darauf, Schüler:innen Kompetenzen für eine aktive und verantwortungsvolle Teilhabe an der digitalen Welt zu vermitteln. Dies umfasst informatische Kompetenzen, Medienkompetenzen und Gestaltungskompetenzen, mit dem Ziel eines sicheren Umgangs mit Medien und digitalen Technologien im Sinne des Kinderschutzes. Die Analyse des Lehrplans zeigt, dass hier besonders Bezüge zur Stufe 0 (Grundlagen und Verhalten) und Stufe 1 (Allgemeine Einführung und Motivation) des CLEMENTINE-6-Stufen-Modells bestehen. Themen wie die Funktionsweise digitaler Geräte, verantwortungsbewusste Online-Kommunikation, der Schutz persönlicher Daten und das Erkennen von Gefahren im Internet werden behandelt.
- Der Lehrplan **Informatik** für die **5. Klasse** AHS (Oberstufe) ist sehr kurzgehalten und bietet Stichworte, die Grundlagen für Cybersecurity relevante Themen der Stufen 1 bis 3 legen. Konkrete Themen wie Verschlüsselung oder Angriffserkennung werden jedoch nicht explizit genannt.
- Das **Wahlpflichtfach Informatik** an der AHS (Oberstufe) baut auf dem Pflichtfach auf und zielt auf eine erweiterte und vertiefte informatische Bildung ab. Der Lehrplan ist in Inhalts- und Handlungsdimensionen unterteilt und umfasst verschiedene Kompetenzmodule. Zentrale Ziele sind das Entwickeln eines tiefen Verständnisses für die digitale Welt und die Vorbereitung auf ein Informatikstudium, wobei Problemlösung, abstraktes Denken und die Reflexion gesellschaftlicher Auswirkungen wichtig sind.

Die angestrebte Cybersecurity-Kompetenztiefe reicht von Basic bis **Intermediate** in vertiefenden Gegenständen.

Kaufmännische und Humanberufliche Schulen (Handelsakademien HAK, Handelsschulen HAS, Höhere Lehranstalten für wirtschaftliche Berufe HLW, Fachschulen für wirtschaftliche Berufe FW)

In diesen Schulen liegt der Fokus auf der praktischen Anwendung und dem sicheren Umgang mit Informationstechnologien in einem wirtschaftlichen Kontext. Die Cybersecurity-Kompetenzen sind hier überwiegend den **Stufen 1 und 2** des CLEMENTINE-6-Stufen-Modells zuzuordnen. Die angestrebte Cybersecurity-Kompetenztiefe erreicht Intermediate.

- In der **Handelsakademie (HAK)** wird Cybersecurity primär in den Fächern Officemanagement und angewandte Informatik (OMAI) sowie Wirtschaftsinformatik (WINF) behandelt. Themen umfassen sichere Passwörter, Datensicherung und -schutz, Lizenzrecht, sicheres Verhalten in sozialen Netzwerken und das Erkennen von Internetgefahren. Auch rechtliche Aspekte wie Datenschutz, Persönlichkeitsrechte und Urheberrecht im Zusammenhang mit sozialen Netzwerken werden im Fach

„Recht“ behandelt. Der neue HAK Lehrplan (ab 2027) nimmt Cybersecurity als eine der vier Säulen auf und soll die Stufen 1 bis 2, partiell auch Stufe 3 erfüllen. Eine spezialisierte „CyberHAK“ bietet eine Vertiefung, die Stufe 3 durch eine Zertifizierung als Information Security Manager nach ISO 27001 erreicht.

- In der **Handelsschule (HAS)** finden sich gleichlautende Kompetenzen wie in der HAK, jedoch werden die tiefergehenden Kompetenzen aus höheren HAK-Jahrgängen nicht behandelt.
  In den **Humanberuflichen Schulen (HLW/FW)**, z.B. im Fach „Angewandtes Informationsmanagement“ (AINF) in der HLW oder OMAI in der FW, werden bereits frühzeitig viele Cybersecurity-Inhalte vermittelt, die Stufen 1 und 2 betreffen. Dazu gehören die Funktionsweise von Computersystemen, sichere Netzwerknutzung, sichere Passwörter, Datensicherungskonzepte, Virenschutz, Firewalls, sichere Internetnutzung, Urheberrecht, Lizenzmodelle und der verantwortungsbewusste Umgang mit Online-Diensten und sozialen Netzwerken. Später kommen Themen wie Datenschutz, Datensicherheit, Verschlüsselung, Digitale Signatur und die Gefahren ausgegliederter IT-Infrastrukturen (Cloud) hinzu.

Höhere und mittlere technische und gewerbliche Lehranstalten (HTL)

In den HTL gibt es eine große Vielfalt an Lehrplänen. Die Integration von Cybersecurity variiert stark je nach Fachrichtung und Fach. Die angestrebte Cybersecurity-Kompetenztiefe reicht von **Intermediate** bis **Professional**.

- In vielen Fachrichtungen, die „Angewandte Informatik“ nach Anhang 1 haben, werden **Grundlagen der Informationstechnologie und ein Bewusstsein für den Umgang mit Daten** vermittelt, was den Intentionen der **Stufen 1 und 2** entspricht. Die technische Tiefe ist in den ersten Stufen begrenzt, um das allgemeine Verständnis zu fördern. Es gibt Vorschläge, explizite Inhalte der Stufen 1 und 2 in Fächer wie „Angewandte Informatik“ und „Soziale und personale Kompetenz“ zu integrieren.
- In spezialisierten Informatik-Fachrichtungen wie **Informatik** oder **Informationstechnologie**, werden Inhalte der **Stufen 1 bis 3 als fundamentale Konzepte** behandelt. **Stufe 4 (Angriffsmuster und Verteidigungsmaßnahmen)** wird schwerpunktmäßig in fortgeschrittenen Fachgegenständen wie „Netzwerksysteme und Cybersecurity“" und „Programmieren und Software Engineering“ behandelt. Der Lehrplan IT HTL strebt eine Übernahme und explizite Integration der Stufen 1 bis 4 an.
- Andere Fachrichtungen wie **Medizinische Gesundheitsinformatik** (Biomedizin- und Gesundheitstechnik) adressieren ebenfalls **Stufen 1, 2** (und 3), jedoch mit starkem Fokus auf den spezifischen medizinischen Kontext und oft nicht explizit als Cybersecurity ausgewiesen. Es gibt Vorschläge zur Integration von Stufen 1 und 2.
- Fächer wie **Fachspezifische Informationstechnik** (Fachrichtung Elektrotechnik) behandeln Grundlagen in den ersten Jahren, während spezifischere Inhalte in späteren Jahren oder Vertiefungen (z.B. Netzwerktechnik) vorkommen. Vorschläge zielen auf eine explizite Integration der Stufen 1 und 2 ab.
- Fachrichtungen wie **Technologie und angewandte Informatik** (Art and Design), **Medientechnologie und angewandte Informatik** (Grafik- und Kommunikationsdesign, Medien HTL) oder **Angewandte Informatik und fachspezifische Informationstechnik** (Mechatronik) haben Cybersecurity-Inhalte der Stufen 1 und 2 oft nur indirekt, implizit oder in Ansätzen integriert. Es gibt detaillierte Vorschläge zur expliziten schrittweisen Integration dieser Inhalte in die jeweiligen Fächer über mehrere Jahre.

Zusammenfassend lässt sich sagen, dass die österreichischen Lehrpläne eine **breite Basis für Cybersecurity** legen, die sich primär auf grundlegendes Bewusstsein, sicheres Verhalten und den Umgang mit Daten konzentriert (Stufen 1 und 2). Vertiefte technische und rechtliche Aspekte sowie Themen der Angriffserkennung (Stufen 3 und 4) werden vor allem in IT-spezifischen Fachrichtungen der HTL behandelt. Es gibt jedoch in vielen Lehrplänen noch Potential für eine explizitere und systematischere Integration der Cybersecurity-Inhalte.

5.2 AHS – Allgemeinbildende höhere Schulen

5.2.1 Lehrplan Digitale Grundbildung - Sekundarstufe 1

Bildungs- und Lehraufgabe: Der Lehrplan für Digitale Grundbildung zielt darauf ab, Schüler:innen ein breites Spektrum an Kompetenzen zu vermitteln, die sie für eine aktive und verantwortungsvolle Teilhabe an der digitalen Welt benötigen.

Zentrale fachliche Konzepte: Durch die holistische multiperspektivische Bearbeitung von Beispielen sollen Kompetenzen entwickelt werden, um digitale Artefakte zu erkunden, kritisch zu hinterfragen, verantwortungsvoll zu nutzen und zu gestalten. Um dies zu erreichen, sollen im Unterricht nicht nur informatische Kompetenzen und Medienkompetenzen, sondern auch Gestaltungskompetenzen vermittelt werden. Dabei ist eines der Ziele ein sicherer Umgang mit Medien und digitalen Technologien im Sinne des Kinderschutzes. Die Kompetenzen sind in fünf Bereiche unterteilt: Orientierung, Information, Kommunikation, Produktion und Handeln[24].

1.Klasse

Bereich Orientierung:

- Die Schüler:innen beschreiben das Prinzip der **Eingabe, Verarbeitung und Ausgabe** an digitalen Endgeräten und vergleichen ihr persönliches Nutzungsverhalten
- Sie erkunden, was das Digitale im Unterschied zum Analogen ausmacht

Stufe 0: Grundlagen und Verhalten

0.1 Grundlagen eines Computers

Bereich Information:

- Die Schüler:innen nennen verschiedene **Suchmaschinen** und erklären, wie diese funktionieren.
- Sie führen einfache Internetrecherchen durch und schätzen die Qualität der gefundenen Informationen ein.
- Außerdem speichern, kopieren, suchen, ändern und löschen sie Informationen mit einem digitalen Gerät und definieren diese als Daten.

Stufe 0: Grundlagen und Verhalten

0.2 Kommunikationsbedürfnisse, 0.4 Verhalten

Bereich Kommunikation:

- Die Schüler:innen erklären, wie **personenbezogene Informationen** verwendet werden können und treffen Vorkehrungen, um diese zu schützen.
- Sie arbeiten respektvoll und verantwortungsbewusst mit anderen online zusammen.

Stufe 0: Grundlagen und Verhalten
1. Kommunikationsbedürfnisse
2. Verhalten

Stufe 1: Allgemeine Einführung & Motivation;

1.1 Motivation und Sicherheit

1.4 Sicherheitsempfehlungen

Bereich Produktion:

- Die Schüler:innen vollziehen eindeutige **Handlungsanleitungen (Algorithmen)** nach und formulieren diese selbstständig.
- Sie beschreiben verschiedene Darstellungsformen von Inhalten und deren Wirkung.

Stufe 0: Grundlagen und Verhalten

0.4 Verhalten

Bereich Handeln:

- Die Schüler:innen identifizieren gängige physische Komponenten von Computersystemen (Hardware) und beschreiben, wie diese funktionieren.
- Sie beschreiben Mediennutzungsformen und nutzen Hilfesysteme bei der Problemlösung.

Stufe 0: Grundlagen und Verhalten
1.Grundlagen eines Computers
3. Sicherheitsüberlegungen
5. Fähigkeiten und Fertigkeiten (Bewusstsein, Verantwortung, Auswirkungen, Verhaltensrichtlinien)

Anwendungsbereiche:

- Erhebung und Speicherung der Daten von Nutzerinnen und Nutzern sowie deren Verwendung
- Planung, Gestaltung und Auswertung von Umfragen
- Wichtigste Komponenten eines Computers
- Notwendige Funktionen eines Betriebssystems im Normalbetrieb

[24] BGBl. II - Ausgegeben am 6. Juli 2022 - Nr. 267, S.3;
(https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2022_II_267/BGBLA_2022_II_267.html)

2.Klasse

Bereich Orientierung
Die Schüler:innen bewerten, wie die **Zugänglichkeit und Nutzbarkeit von Technologieprodukten** verbessert werden kann und analysieren Interessen und Bedingungen der Medienproduktion. Sie zeigen auf, inwieweit das Digitale im Vergleich zum Analogen das eigene Leben verändert und erkennen, dass Medien nie "neutral" sind.

Stufe 0: Grundlagen und Verhalten

0.4 Verhalten

0.5 Fähigkeiten und Fertigkeiten (Usability, Einfachheit, Interpretierbarkeit)

Bereich Information

- Die Schüler:innen erfassen, filtern, sortieren, interpretieren und stellen **Daten** dar.
- Sie beschreiben, wie Informationen über das Internet bereitgestellt und abgerufen werden, und wenden Lizenzmodelle an.

Stufe 1: Allgemeine Einführung und Motivation

1.2 Grundbegriffe

1.3 Über den Umgang mit Daten im Internet

Bereich Kommunikation

- Die Schüler:innen stellen dar, wie Informationen in kleineren Teilen zerlegt und über das Internet übertragen werden.
- Sie unterscheiden Kommunikationsmedien nach ihrer Verwendung und zeigen Einflüsse auf das Lebensumfeld auf.

Sie erklären den Begriff "Social Media" und verstehen die Interessen der anbietenden Unternehmen

Stufe 0: Grundlagen und Verhalten

0.2 Kommunikationsbedürfnisse

0.4 Verhalten

Stufe 1: Allgemeine Einführung und Motivation

1.1 Motivation zur Sicherheit

1.3 Über den Umgang mit Daten im Internet

Bereich Produktion

- Die Schüler:innen stellen dar, wie Programme Daten speichern und verarbeiten und erstellen einfache Programme in einer geeigneten Entwicklungsumgebung.
- Sie beachten die Rechte am geistigen Eigentum und erstellen visuelle/audiovisuelle Inhalte

Stufe 0: Grundlagen und Verhalten

0.2 Kommunikationsbedürfnisse

0.4 Verhalten

Bereich Handeln

- Die Schüler:innen stellen dar, wie Hardware und Software zusammenarbeiten, verbinden digitale Geräte mit einem Netzwerk und tauschen Daten aus.
- Sie wägen zwischen digitalen Angeboten und eigenen Bedürfnissen ab und gestalten persönliche Handlungsmöglichkeiten unter Berücksichtigung gesundheitlicher und ökologischer Aspekte.

Stufe 0: Grundlagen und Verhalten

1. Grundlagen eines Computers

0.3 Sicherheitsüberlegungen

0.4 Verhalten

Stufe 1: Allgemeine Einführung und Motivation

1.4 Sicherheitsempfehlungen

1.5 Bedrohungsszenarien

Anwendungsbereiche:

- Veränderung des Einkaufsverhaltens
- Onlinespiele (pay-to-win)
- Sensibilisierung für sprachliche, sensorische und motorische Einschränkungen bei der Nutzung digitaler Medien
- Organisation von Daten
- (Visuelle) Darstellung von Daten
- Geschäftsmodelle von Social Media-Diensten, Nutzung von persönlichen und personenbezogenen Informationen
- Fake News, Darstellung und Realität (Manipulation) und dahinterliegende Interessen
- Schutz von personenbezogenen Daten
- Betrug im Internet, Phishing
- Digitaler Arbeitsplatz
- Nachhaltiger Umgang mit digitalen Technologien

- Erkennen von technischen Problemen in der Nutzung von digitalen Geräten
- Konkretisierung von Fehlern im Hinblick auf Meldung an Supportstrukturen

3.Klasse

Bereich Orientierung
- Die Schüler:innen beschreiben Anwendungen von Technik in Umwelt und Gesellschaft und beschreiben, wie **künstliche Intelligenz** viele Systeme steuert.
- Sie analysieren Veränderungen des Mediennutzungsverhaltens und reflektieren Kompromisse im Zusammenhang mit digitalen Technologien.

Stufe 0: Grundlagen und Verhalten
2. Grundlagen eines Computers
0.4 Verhalten

Bereich Information
- Die Schüler:innen erklären Bedingungen sowie Vor- und Nachteile von **personalisierten Suchroutinen**.
- Sie planen und führen die Suche nach Informationen zielgerichtet durch und hinterfragen gefundene Informationen vergleichend.

Stufe 1: Allgemeine Einführung und Motivation
1.2 Grundbegriffe
1.3 Über den Umgang mit Daten im Internet

Bereich Kommunikation:
- Die Schüler:innen erklären, wie **cloudbasierte Systeme** funktionieren und beschreiben einen Kompromiss zwischen der Veröffentlichung von Informationen und der Geheimhaltung.
- Sie gestalten eigene digitale Identitäten reflektiert.

Stufe 0: Grundlagen und Verhalten
0.2 Kommunikationsbedürfnisse
0.4 Verhalten

Stufe 1: Allgemeine Einführung und Motivation
1.2 Grundbegriffe
1.3 über den Umgang mit Daten im Internet

Bereich Produktion
- Die Schüler:innen setzen Elemente des **Computational Thinkings** zur Lösung von Problemen ein und wissen, wie sie Lösungswege in Programmiersprache umsetzen können.
- Sie überprüfen ihre medialen Produktionen auf Barrierefreiheit.

Stufe 0: Grundlagen und Verhalten
2. Grundlagen eines Computers
4. Sicherheitsüberlegungen
5. Fähigkeiten und Fertigkeiten

Bereich Handeln
- Die Schüler:innen erklären am Beispiel, wie Computersysteme in Alltagsgegenständen Funktionen erfüllen und benennen ökologische Problemkonstellationen im Zusammenhang mit Digitalisierung.
- Sie treffen Vorkehrungen, um Geräte vor Schadsoftware zu schützen.

Stufe 0: Grundlagen und Verhalten
3. Grundlagen eines Computers
0.3 Sicherheitsüberlegungen
0.4 Verhalten

Stufe 1: Allgemeine Einführung und Motivation
1.4 Sicherheitsempfehlungen
1.5 Bedrohungsszenarien

Anwendungsbereiche:
- Risiken und Vorteile für die Chancengleichheit bei der Nutzung von Informationstechnologien sowie geeignete Handlungsoptionen
- digitale Barrierefreiheit
- Internet-of-Things
- Manipulative und monoperspektivische Darstellungen von Informationen in populären Medienkulturen
- Verschlüsselungsmethoden für die sichere Übertragung von Informationen
- (sicheres) Passwort, Zweifaktorauthentifizierung
- Physischer und digitaler Schutz von elektronischen Informationen
- Grundlagen der Betroffenenrechte im Datenschutz
- Reale Probleme der Cybersecurity: Cybermobbing, Cybergrooming, Identitätsdiebstahl
- Gezielte bzw. manipulative Darstellungen, z.B. in Diagrammen, durch Bildausschnitte oder Vertonung

- Konfigurationsmöglichkeiten von Betriebssystemen und Kommunikationssystemen, um sie barrierefrei zugänglich machen

4.Klasse

Bereich Orientierung
- Die Schüler:innen reflektieren die **Grenzen und Möglichkeiten von Künstlicher Intelligenz** und begegnen euphorischen und kulturpessimistischen Haltungen argumentativ.
- Sie erkennen die Normativität von digitalen Technologien und Medieninhalten.

Stufe 0: Grundlagen und Verhalten
3. Grundlagen eines Computers
6. Sicherheitsüberlegungen
7. Fähigkeiten und Fertigkeiten

Bereich Information
- Die Schüler:innen führen **Datensicherungen** und -wiederherstellungen aus.
- Sie erklären Gefahren der Erhebung, Auswertung und Verknüpfung von Nutzerdaten und verhalten sich verantwortungsvoll.

Stufe 0: Grundlagen und Verhalten
4. Grundlagen eines Computers

0.3 Sicherheitsüberlegungen

Stufe 1: Allgemeine Einführung und Motivation

1.4 Sicherheitsempfehlungen

Bereich Kommunikation:
- Die Schüler:innen stellen die **Funktion von Protokollen** bei der Datenübertragung dar und entwickeln ein Verständnis für die Konstruktion von Medienwirklichkeit.
- Sie bedenken bei der Auswahl von Social Media, welchen Einfluss die Interessen von Unternehmen haben.

Stufe 1: Allgemeine Einführung und Motivation
1. Motivation zur Sicherheit
2. Grundbegriffe

1.3 Über den Umgang mit Daten im Internet

Bereich Produktion:
- Die Schüler:innen entwerfen und entwickeln Programme iterativ, die **Kontrollstrukturen kombinieren**.
- Sie hinterfragen den Einfluss von Darstellungsformen auf die Wahrnehmung des Inhalts und erstellen einfache Programme oder Webanwendungen.

Stufe 0: Grundlagen und Verhalten

0.4 Verhalten

0.5 Fähigkeiten und Fertigkeiten

Bereich Handeln:
- Die Schüler:innen vergleichen **Abstraktionsebenen** und Interaktionen zwischen Anwendungssoftware, Systemsoftware und Hardwareschichten und setzen Software zur Verschlüsselung von Daten ein.
- Sie reflektieren, inwieweit technische Konfigurationen Optionen einschränken und treffen Vorkehrungen für ihre Eigenständigkeit und informationelle Selbstständigkeit im Kontext von digitaler Vernetzung treffen.

Stufe 0: Grundlagen und Verhalten
4. Grundlagen eines Computers

0.3 Sicherheitsüberlegungen

0.4 Verhalten

Stufe 1: Allgemeine Einführung und Motivation

1.4 Sicherheitsempfehlungen

1.5 Bedrohungsszenarien

Anwendungsbereiche:
- Wichtigste technische Mittel zum Schutz vor Betrug und Missbrauch
- Wichtigste rechtliche und politische Aspekte von Konsumentenrecht
- Phänomen der viralen Verbreitung von Inhalten und entsprechende Handlungsmöglichkeiten
- Datenschutzrechtliche Rechtsgrundlagen (BGBl. II - Ausgegeben am 6. Juli 2022 - Nr. 267 S 3)

Zusammenfassende Analyse

Der Lehrplan für Digitale Grundbildung in Österreich integriert **Cybersecurity als einen wesentlichen Schwerpunkt**, der altersgerecht und praxisnah vermittelt werden soll. Dieser Fokus zieht sich durch alle Kompetenzbereiche und Jahrgangsstufen, wobei die Tiefe und Komplexität der Themen mit dem Fortschreiten der Schuljahre zunimmt.

Die Inhalte des Lehrplans sind in den Kompetenzbereichen **Orientierung, Information, Kommunikation, Produktion und Handeln** verankert. Die zu den Kompetenzbereichen angefügten Anwendungsbereiche bieten konkrete Anknüpfungspunkte für Aspekte der Cybersecurity. Die Lehrplananalyse anhand des CLEMENTINE-6-Stufen-Modells weist besonders Bezüge zu Stufe 0 (Grundlagen und Verhalten) sowie Aspekte zu Stufe 1 (Allgemeine Einführung und Motivation) auf.

In der **ersten Klasse** liegt der Fokus auf grundlegenden Konzepten, wie die Funktionsweise eines Messengerdienstes, der verantwortungsbewussten Kommunikation im Internet und dem Schutz persönlicher Daten. In der **zweiten Klasse** wird die personalisierte Werbung thematisiert und damit verbundene Aspekte wie Datensammlung, Verarbeitung und Geschäftsmodelle von Social Media-Diensten behandelt. In der **dritten Klasse** werden Themen wie Cloud-Dienste, deren Sicherheitsaspekte und der Schutz von elektronischen Informationen behandelt. Die **vierte Klasse** setzt sich mit der Transformation der Mobilität, künstlicher Intelligenz und den damit verbundenen ethischen und sicherheitsrelevanten Fragen auseinander.

Im Lehrplan verortete Themenbereiche

Grundlagen der Cybersecurity:

- Der Lehrplan behandelt grundlegende Konzepte wie die Bedeutung von Cybersecurity, ihre Ziele und die verschiedenen Bedrohungen. Dazu gehören Malware, Phishing, Social Engineering und Hackerangriffe.
- Die Bedeutung von **Datenschutz und Privatsphäre** wird hervorgehoben.

Sicherer Umgang mit digitalen Geräten:

- Schülerinnen und Schüler lernen, **sichere Passwörter** zu erstellen und zu verwalten.
- Die Notwendigkeit, Software und Betriebssysteme durch regelmäßige **Updates und Patches** aktuell zu halten, wird vermittelt.
- Der Schutz vor Malware durch **Antivirenprogramme und regelmäßige Scans** ist ein weiterer wichtiger Punkt.

Schutz der persönlichen Daten:

- Der Lehrplan behandelt die **Grundlagen der Datenschutz-Grundverordnung (DSGVO)**.
- Schülerinnen und Schüler lernen, wie sie die **Privatsphäre-Einstellungen** in sozialen Netzwerken anpassen und verantwortungsvoll mit persönlichen Informationen umgehen können.
- Einfache **Verschlüsselungstechniken** werden eingeführt.

Erkennen und Vermeiden von Cyberbedrohungen:

- Der Lehrplan sensibilisiert für **Phishing und Social Engineering** und vermittelt, wie man diese Bedrohungen erkennt.
- Das Erkennen von **Fake News und Desinformation** ist ebenfalls ein wichtiges Thema.
- Ein sicheres Verhalten in Online-Umgebungen wie Chatrooms, Gaming-Plattformen und Foren wird gelehrt.

Netzwerksicherheit:

- Die Schülerinnen und Schüler lernen über die sichere Nutzung von WLANs, den Unterschied zwischen öffentlichen und privaten WLANs.

Cybermobbing und Ethik:

- Der Lehrplan behandelt das Erkennen und Handeln bei **Cybermobbing** sowie Rechte und Pflichten im digitalen Raum.
- **Verantwortung im digitalen Raum**, ethische Grundsätze und digitale Zivilcourage werden thematisiert.

Technische Aspekte:

- **Sicherheitschecks** von Geräten und Software auf Schwachstellen werden durchgeführt.
- Die Schülerinnen und Schüler erhalten eine Einführung in die **Grundlagen der Kryptografie**, einschließlich Ver- und Entschlüsselung.
- Einfache **Programmierung von Sicherheitsfunktionen**, z.B. Passwortprüfungen mit Scratch, wird geübt.

Verantwortung in der digitalen Gesellschaft:

- Die Schülerinnen und Schüler lernen, wie man seine **digitale Identität schützt** und werden auf die Herausforderungen der digitalen Welt vorbereitet.
- Es werden **Berufsperspektiven** im Bereich IT-Sicherheit aufgezeigt und globale Herausforderungen wie Cyberkriminalität thematisiert.

Das zentrale fachliche Konzept der **holistischen multiperspektivischen Erschließung digitaler Artefakte** im Sinne des Frankfurter Dreiecks (Technisch-mediale Perspektive, Gesellschaftlich-kulturelle Perspektive und Interaktionsbezogene Perspektive) ermöglicht Themenbereiche der Cybersecurity nicht nur technologisch, sondern in vielschichtigen Wechselwirkungen zwischen Individuen, Gesellschaft und digitalen Systemen zu analysieren, zu reflektieren und produktiv-gestaltend zu bearbeiten. (BGBl. II - Ausgegeben am 6. Juli 2022 - Nr. 267) Die enthaltenen Anwendungsbereiche bieten konkrete Anknüpfungspunkte für Cybersecurity Themen.

Dieses Konzept der multiperspektivischen Erschließung digitaler Artefakte erlaubt eine hohe Flexibilität der Unterrichtsplanung von Lehrenden im Hinblick auf konkrete und aktuelle Betrachtungsmöglichkeiten zu Cybersecurity-Themen. Dieser Ansatz kann zudem geeignet sein, das technologisch orientierte CLEMENTINE-6-Stufen-Modell selbst zu hinterfragen und zu adaptieren.

5.2.2 Lehrplan Informatik 5. Klasse AHS

Bildungs- und Lehraufgabe: Der Lehrplan Informatik für die 5. Klasse AHS in Österreich betont die zentrale Rolle der Informatik im digitalen Zeitalter. Er zielt darauf ab, Schülern ein fundiertes Weltverständnis und eine Basis für zukünftige Berufe zu vermitteln.

Zentrale fachliche Konzepte: Die Kompetenzen sind in vier Bereiche unterteilt: Informatik Mensch und Gesellschaft, Informatiksysteme, Angewandte Informatik, Praktische Informatik. Der Unterricht soll kreatives Gestalten, kritisches Denken und verantwortungsvollen Umgang mit Informationstechnologien fördern. Zudem wird die Bedeutung von Teamarbeit und selbstständigem Lernen hervorgehoben.

Der Lehrplan behandelt Themen wie Datensicherheit, Urheberrecht, Informatiksysteme, angewandte Informatik und praktische Informatik. (BGBl. Nr. 88/1985 zuletzt geändert durch BGBl. II Nr. 204/2024 S 246[25])

1. Informatik, Mensch und Gesellschaft

- Der Lehrplan Informatik 5. Klasse beinhaltet die Bedeutung von Informatik in der Gesellschaft, die Auswirkungen auf Einzelpersonen und die Gesellschaft sowie das Abwägen von Vor- und Nachteilen an Beispielen. Dies fördert das Bewusstsein für die Relevanz von IT-Sicherheit.
- Maßnahmen und rechtliche Grundlagen im Zusammenhang mit Datensicherheit, Datenschutz und Urheberrecht werden gelehrt und angewendet. Dies entspricht dem Schutz personenbezogener Daten und dem Erkennen von Bedrohungen.

Stufe 1: Allgemeine Einführung & Motivation
1.1 Motivation zur Sicherheit
1.2 Grundbegrifflichkeiten
1.4 Sicherheitsempfehlungen
1.5 Bedrohungsszenarien
Stufe 2: „Exploratory“ Tiefergehende Awareness
2.6 Rechtsgrundlagen
2.7 Technische Umsetzungsstrategien

2. Informatiksysteme

- Der Lehrplan behandelt Grundlagen von Betriebssystemen und deren Bedienung. Dies kann als Basis für das Verständnis von Sicherheitsmechanismen dienen.
- Grundlagen der Vernetzung von Computern und die Nutzung lokaler und globaler Netzwerke werden vermittelt. Dies ist relevant für das Verständnis von Angriffsvektoren.
- Der Lehrplan konzentriert sich auf Begriffe und Konzepte der Informatik sowie die Anwendung von Methoden und Arbeitsweisen. Dies schafft eine Grundlage für das Verständnis von Sicherheitskonzepten.
- Es werden Algorithmen erklärt, entworfen, dargestellt und in einer Programmiersprache implementiert. Dies kann in Verbindung mit sicherer Softwareentwicklung relevant sein.

Stufe 3: „Foundational“ Netzwerk-, Geräte- und Anwendungssicherheit, Sicherheitsmanagement
3.2 Gerätesicherheit

[25] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2024_II_204/BGBLA_2024_II_204.html

3.3 Netzwerksicherheit
3.4 Sicherheit von Daten und Webanwendungen
Stufe 4: "Professional" Angriffsmuster und Verteidigungsmaßnahmen
4.1 Sichere Softwareentwicklung

3. Angewandte Informatik

- Der Lehrplan beinhaltet den Einsatz von Standardsoftware zur Kommunikation, Dokumentation, Erstellung, Publikation und multimedialen Präsentation. Dies könnte im Kontext von Social Engineering und Phishing relevant sein.
- Es wird gelehrt, Informationsquellen zu erschließen, Inhalte zu systematisieren, strukturieren, bewerten und verarbeiten. Dies ist relevant für die Analyse von Bedrohungsinformationen.

Stufe 1: Allgemeine Einführung & Motivation
1.2 Grundbegrifflichkeiten.
Stufe 2: „Exploratory" Tiefergehende Awareness
2.2 Über den Umgang mit Daten II
Stufe 3: "Foundational" - Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement
3.4 Sicherheit von Daten und Webanwendungen

4. Praktische Informatik

- Der Lehrplan konzentriert sich auf Begriffe und Konzepte der Informatik sowie die Anwendung von Methoden und Arbeitsweisen. Dies schafft eine Grundlage für das Verständnis von Sicherheitskonzepten.
- Es werden Algorithmen erklärt, entworfen, dargestellt und in einer Programmiersprache implementiert. Dies kann in Verbindung mit sicherer Softwareentwicklung relevant sein.
- Der Lehrplan beinhaltet die Nutzung von Datenbanken und das Entwerfen einfacher Datenmodelle. Dies kann im Zusammenhang mit Datenintegrität und -sicherheit betrachtet werden.

Stufe 2: „Exploratory" Tiefergehende Awareness
2.2 Über den Umgang mit Daten II
Stufe 3: „Foundational" Netzwerk-, Geräte- und Anwendungssicherheit, Sicherheitsmanagement
3.1 Grundlagen der IT-Sicherheit
3.2 Gerätesicherheit

Zusammenfassende Analyse

Der Lehrplan Informatik für die 5. Klasse ist vom Inhalt sehr kurzgehalten und bietet nur Stichworte zu den einzelnen Kompetenzbereichen. Das ermöglicht viel Freiraum in der Unterrichtgestaltung schränkt allerdings den systematischen Kompetenzaufbau ein. Die Analyse anhand des CLEMENTINE-6-Stufen-Modells zeigt, dass in den verschiedenen Kompetenzbereichen Grundlagen für Cybersecurity relevante Themen der Stufen eins bis drei gelegt werden. Dazu gehören allgemeines Bewusstsein, grundlegende Kenntnisse über Systeme und Netzwerke sowie der Umgang mit Informationen. Konkrete Cybersecurity Themen wie Verschlüsselung, Angriffserkennung oder fortgeschrittene Sicherheitsmaßnahmen werden jedoch nicht explizit angeführt.

Relevante Cybersecurity-Themen des „Lehrplan Informatik 5. Klasse" sind:

Bedeutung der Informatik in der Gesellschaft: Verständnis der Auswirkungen auf Einzelpersonen und die Gesellschaft sowie das Abwägen von Vor- und Nachteilen an Beispielen. Dies fördert das Bewusstsein für die Relevanz von IT-Sicherheit.

Maßnahmen und rechtliche Grundlagen im Zusammenhang mit Datensicherheit, Datenschutz und Urheberrecht: Kenntnis und Anwendung dieser Grundlagen. Dies entspricht dem Schutz personenbezogener Daten und dem Erkennen von Bedrohungen.

Grundlagen von Betriebssystemen: Grundlagen verstehen und graphische Oberflächen und Dienstprogramme bedienen können. Dies kann als Basis für das Verständnis von Sicherheitsmechanismen dienen.

Grundlagen der Vernetzung von Computern: Beschreiben und erklären können und lokale und globale Computernetzwerke nutzen können. Dies ist relevant für das Verständnis von Angriffsvektoren.

Begriffe und Konzepte der Informatik: Verstehen und Anwenden von Methoden und Arbeitsweisen. Dies schafft eine Grundlage für das Verständnis von Sicherheitskonzepten.

Einsatz von Standardsoftware: Standardsoftware zur Kommunikation und Dokumentation sowie zur Erstellung, Publikation und multimedialen Präsentation eigener Arbeiten einsetzen können. Dies könnte im Kontext von Social Engineering und Phishing relevant sein.

Informationsquellen erschließen: Inhalte systematisieren, strukturieren, bewerten, verarbeiten und unterschiedliche Informationsdarstellungen verwenden können. Dies ist relevant für die Analyse von Bedrohungsinformationen.

Nutzung von Datenbanken: Datenbanken benutzen und einfache Datenmodelle entwerfen können. Dies kann im Zusammenhang mit Datenintegrität und -sicherheit betrachtet werden.

Rechtliche Gegebenheiten: Die rechtlichen Gegebenheiten verstehen.

Anzumerken ist, dass dieser Lehrplan derzeit im Rahmen einer generellen Lehrplanreform der Sekundarstufe 2 überarbeitet werden soll.

5.2.3 Lehrplan Informatik Wahlpflichtfach AHS

Bildungs- und Lehraufgabe: Das Wahlpflichtfach Informatik schließt an das Pflichtfach in der 5. Klasse an und soll die Schülerinnen und Schüler zu einer erweiterten und vertieften informatischen Bildung führen.

Zentrale fachliche Konzepte: Der semestrierte Lehrplan ist in **Inhalts- und Handlungs-dimensionen** unterteilt, die verschiedene Kompetenzmodule umfassen, von Informatiksystemen und angewandter Informatik bis hin zu Algorithmen und Programmierung. Die Anforderungen aus der Handlungsdimension (Wissen und Verstehen, Anwenden und Gestalten, Reflektieren und Bewerten) können in Hinblick auf die mündliche Reifeprüfung den Aspekten Reproduktion, Transfer, Reflexion und Problemlösung zugeordnet werden. Das Ziel ist es, ein tiefes Verständnis für die digitale Welt zu entwickeln und interessierte Schüler:innen auf ein Studium im Bereich Informatik vorzubereiten, wobei besonderer Wert auf Problemlösung, abstraktes Denken und die Reflexion der gesellschaftlichen Auswirkungen der Informatik gelegt wird. (BGBl. II - Ausgegeben am 6. Juli 2022 - Nr. 267 S 3)

6.Klasse

3.Semester

Bereich Informatiksysteme:

- Technische Grundlagen und Funktionsweisen: Komponenten von Informatiksystemen beschreiben.
- Betriebssysteme und Software: Kernaufgaben von Betriebssystemen beschreiben; Software-Kategorien nennen; Betriebssystem installieren und konfigurieren.

Stufe 1: Allgemeine Einführung & Motivation
1.1 Motivation zur Sicherheit
1.2 Grundbegrifflichkeiten
Indikatoren:

- Bewusstseinsbildung für Bedrohungen, Schutz von Daten.
- Grundlagenwissen über Systeme

Stufe 3: „Foundational" Netzwerk-, Geräte- und Anwendungssicherheit, Sicherheitsmanagement
3.1 Grundlagen der IT-Sicherheit
3.2 Gerätesicherheit
Indikatoren:

- Grundlagen der IT-Sicherheit.
- Erste Einblicke in die Funktionsweise von Betriebssystemen.

Bereich Angewandte Informatik:

- Produktion digitaler Medien: Medienformate beschreiben; Richtlinien für digitale Medien erläutern; Digitale Medien bearbeiten und publizieren; Digitale Produkte bewerten.

Stufe 1: Allgemeine Einführung & Motivation
1. Motivation zur Sicherheit
Indikatoren:

- Grundlagenwissen im Umgang mit Daten und digitalen Medien.
- Schutz personenbezogener Daten.

Stufe 2: „Exploratory" - Tiefergehende Awareness
2.6 Rechtsgrundlagen
Indikatoren: Die rechtlichen Gegebenheiten in Österreich und Europa verstehen

Bereich Praktische Informatik:

- Algorithmen, Datenstrukturen und Programmierung: Algorithmus Begriff erklären; Aufgaben algorithmisch beschreiben; Algorithmen entwerfen, darstellen, implementieren und testen.

Indikatoren: Keine direkte Zuordnung, da der Fokus auf Grundlagen der Programmierung liegt.

4. Semester

Bereich Informatiksysteme:

- Netzwerke: Netzwerke und Protokolle beschreiben; Computernetzwerk konzipieren, aufbauen und verwalten; Internetdienste nennen und nutzen.

Stufe 2: „Exploratory“ - Tiefergehende Awareness;

2.3 Sichere Kommunikation

2.7 Technische Umsetzungsstrategien

Stufe 3: “Foundational”- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.3 Netzwerksicherheit

Indikatoren: Tiefergehendes Verständnis von Netzwerken und Internetdiensten.

Bereich Angewandte Informatik:

- Kalkulationsmodelle und Visualisierung: Funktionsbegriff erklären; Kalkulationsmodelle gestalten und implementieren; Korrektheit reflektieren.

Stufe 2: „Exploratory“ – Tiefergehende Awareness;

2.2 Über den Umgang mit Daten II

Bereich Praktische Informatik:

- Algorithmen, Datenstrukturen und Programmierung: Aufgaben modellieren; Komplexere Algorithmen entwerfen, darstellen, implementieren und testen.

Indikatoren: Keine direkte Zuordnung, da der Fokus auf Grundlagen der Programmierung liegt.

7.Klasse

5. Semester

Bereich Informatiksysteme:

- Technische Grundlagen und Funktionsweisen von Informatiksystemen verstehen und erklären (Erweiterung und Vertiefung)

Stufe 3: „Foundational“- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.2 Gerätesicherheit

Indikatoren: Vertiefung der Systemkenntnisse

Bereich Angewandte Informatik:

- Suche, Auswahl und Organisation von Information: Informationen suchen und auswählen; Relevanz und Qualität einschätzen; Werkzeuge der Daten- und Informationsorganisation beurteilen.
- Kalkulationsmodelle und Visualisierung: Grundbegriffe strukturierter Daten benennen; Datenbestände auswerten und visualisieren; Visualisierungen bewerten.

Stufe 2: „Exploratory“ – Tiefergehende Awareness;

2.2 Über den Umgang mit Daten II

Bereich Praktische Informatik:

- Algorithmen, Datenstrukturen und Programmierung: Aspekte der Prozeduralen, Funktionalen und Objektorientierten Programmierung nennen; Aufgaben modellieren; Algorithmen entwerfen, darstellen, implementieren und testen.
- Datenmodelle und Datenbanksysteme: Datenbanken und Fachbegriffe beschreiben; Datenbankmodelle und Tabellen erklären; Daten strukturiert erfassen, abfragen, auswerten und Datenbanken modellieren.

Stufe 3: “Foundational”- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.4 Sicherheit von Daten

Indikatoren:

- Grundlagen im Bereich Datenbanken
- Passende Technologien zur Absicherung von gespeicherten Daten anwenden

6. Semester

Bereich Informationstechnologie, Mensch und Gesellschaft:

- Verantwortung, Datenschutz und Datensicherheit: Für den Schutz von Informatiksystemen sorgen.
- Geschichte der Informatik: Meilensteine der Computertechnik beschreiben; Geschichtliches Wissen in Beziehung zur aktuellen Situation setzen.
- Berufliche Perspektiven: IT-Berufe benennen und kategorisieren; Wissen für die eigene Erwerbsbiographie nutzen; Wirtschaftliche Bedeutung der IT einordnen.

Stufe 3: „Foundational“- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.1 Grundlagen der IT-Sicherheit

3.5 Organisations-, Risiko- und Sicherheitsmanagement

Indikatoren:

- Berufsfelder zu Cybersecurity
- IT Security Strukturen
- Einsatz von Werkzeugen und Scripts zur Informationsbeschaffung von Endsystemen

Bereich Informatiksysteme

- Technische Grundlagen und Funktionsweisen: Digitale Endgeräte bewerten; Fehler diagnostizieren und beheben.
- Netzwerke: Maßnahmen zur Netzwerksicherheit umsetzen; Technische Aspekte von Netzwerken einschätzen; Internetdienste bewerten.

Stufe 3: „Foundational"- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.2 Gerätesicherheit

3.3 Netzwerksicherheit

3.4 Sicherheit von Daten und Webanwendungen

Indikatoren:

- Einsatz von Werkzeugen und Scripts zur Informationsbeschaffung von Endsystemen
- Gesicherte Verbindung zwischen Arbeitsplätzen konfigurieren
- Webanwendungen nach Sicherheitslücken scannen und Analysedaten verstehen.

Bereich Praktische Informatik

- Konzepte der Informationsverarbeitung: Informatische Konzepte benennen; Heuristiken und Konzepte anwenden; Informatische Modelle gestalten.
- Algorithmen, Datenstrukturen und Programmierung: Aspekte der Programmierung nennen; Aufgaben modellieren; Algorithmen entwerfen, darstellen, implementieren und testen.

Indikatoren: Keine direkte Zuordnung, da der Fokus auf Grundlagen der Programmierung liegt.

8.Klasse

7. Semester

Bereich Informationstechnologie, Mensch und Gesellschaft:

- Bedeutung von Informatik in der Gesellschaft: Wissen im digitalen Umfeld anwenden; Einfluss von Informatiksystemen einschätzen.
- Verantwortung, Datenschutz und Datensicherheit: Rechte und Pflichten beschreiben; Aspekte des Datenschutzes erklären; Wissen um Pflichten und Rechte anwenden.

Stufe 2: „Exploratory" – Tiefergehende Awareness

2.6 Rechtsgrundlagen

Stufe 3: „Foundational"- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.5 Organisations-, Risiko- und Sicherheitsmanagement

Indikatoren:

- Die rechtlichen Gegebenheiten in Österreich und Europa verstehen
- IT Security Strukturen in Österreich und Europa sowie deren Aufgaben erklären

Bereich Informatiksysteme:

- Technische Grundlagen und Funktionsweisen: Technische Konzepte verstehen.
- Betriebssysteme und Software: Software bedienen und bewerten.
- Mensch-Maschine-Schnittstelle: Benutzerfreundlichkeit einschätzen

Stufe 3: „Foundational"- Netzwerk, Geräte - und Anwendungssicherheit, Sicherheitsmanagement;

3.1 Grundlagen der IT-Sicherheit

3.2 Gerätesicherheit

Indikatoren:

- Konfiguration und Analyse von Betriebssystem-Ereignissen

Bereich Angewandte Informatik:

- Kommunikation und Kooperation: Einsatz von Kommunikationssystemen bewerten

Indikatoren: Keine direkte Zuordnung

Bereich Praktische Informatik:

- Konzepte der Informationsverarbeitung: Informatische Konzepte benennen; Heuristiken anwenden; Modelle gestalten; Lösungsansätze reflektieren.
- Algorithmen, Datenstrukturen und Programmierung: Softwareentwicklung erklären; Softwareprojekt planen; Entwicklungsschritte reflektieren; Angemessenheit der Werkzeuge einschätzen; Effizienz bewerten; Programmfehler suchen und korrigieren.
- Intelligente Systeme: Bereiche intelligenter Systeme beschreiben; Unterschied zwischen menschlicher und maschineller Intelligenz erklären; Intelligente Systeme anwenden.

Stufe 4:

4.1 Sichere Softwareentwicklung

Indikatoren: Standards bei der Softwareentwicklung kennen und anwenden

8. Semester
Sicherung der Nachhaltigkeit: Wiederholen, Vertiefen und Vernetzen von Inhalten.
Indikatoren: Konsolidierung der Kenntnisse.

Zusammenfassende Analyse

Der semestrierte Lehrplan Wahlpflichtfach Informatik beschreibt die erweiterte informatische Bildung für Schüler der AHS, aufbauend auf dem Pflichtfach der 5. Klasse. Der Lehrplan ist in **Inhalts- und Handlungsdimensionen** unterteilt, die Kompetenzmodule von Informatiksystemen bis hin zu Algorithmen umfassen, mit dem Ziel, ein vertieftes meist technologisch ausgerichtetes Verständnis für die digitale Welt zu entwickeln. Die Analyse anhand des CLEMENTINE-6-Stufen-Modells zeigt, dass in den verschiedenen Kompetenzbereichen Anknüpfungsmöglichkeiten für Cybersecurity relevante Themen der Stufen eins bis drei gelegt werden. Die Anforderungen aus der Handlungsdimension (Wissen und Verstehen, Anwenden und Gestalten, Reflektieren und Bewerten) laden zu einer vertieften Auseinandersetzung im Lernprozess ein. Gesellschaftliche Aspekte von Cybersecurity werden kaum adressiert.

Relevante Cybersecurity Themen des „Lehrplan Wahlpflichtfach Informatik“ sind:

Allgemeine Einführung & Motivation

- Bewusstseinsbildung durch Fallbeispiele (z.B. Video-Fallbeispiele, Keylogger).
- Themen wie Schadsoftware, Ethical Hacking, Identitätsdiebstahl, Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien, Schutz personenbezogener Daten und Social Engineering.
- Grundbegriffe wie Antivirus, Malware, Phishing und Cybermobbing.

Umgang mit Daten im Internet

- Erkennen und Vermeiden von „persönlichen“ Angriffen.
- Analyse von Mail-Headern und URLs zur Feststellung der Herkunft von Spam-/Phishing-Mails.
- Sichere Verwaltung und Weitergabe von Daten (z.B. Cloudspeicher).
- Sicheres Löschen von Daten.
- Sicherheitsempfehlungen wie Verhaltensrichtlinien, Sperrbildschirm mit Kennwörtern, Updates und Patches, BIOS-Kennwörter und Verhalten in öffentlichen/privaten Netzen.
- Bedeutung von Kennwörtern (Komplexität, Länge).

Bedrohungsszenarien

- Sicherheitskompromittierung durch externe Geräte (z.B. Rubberducky/bashbunny, Autorun, USB Killer).
- Phishing & CO (Phishing, Whaling, Gophish).
- Verhaltensweisen im Notfall.

Vertraulichkeit & Integrität

- Grundlagen der Verschlüsselung und Hashfunktionen.

Sichere Kommunikation

- Herstellung einer sicheren Verbindung zum Arbeitsplatznetzwerk.
- Einsatz persönlicher Firewalls.
- Sichere Authentifizierungsmethoden (NIST-Richtlinien, Password Safes, Mehrfaktorauthentifizierung).
- HTTPS & Zertifikate.

Rechtsgrundlagen

- Verständnis der rechtlichen Gegebenheiten in Österreich und Europa (IT-Recht/StGB/DSGVO).

Angriffsvektoren

- Themen wie Ransomware, Botnetze, Mobiltelefon als Angriffsziel, Vertrauen in Apps, DOS/DDOS, Cybercrime, Defacements und Reconnaissance.

Netzwerksicherheit

- Grundlagen der IT-Sicherheit.
- Funktionsweise von Netzwerkkomponenten (Switches, Router, Firewall, APs, IDS-IPS).

- Analyse einfacher Protokolle (DHCP, HTTP, DNS, TCP/IP, ICMP, ARP mit Wireshark).
- Konfiguration einer gesicherten Verbindung zwischen Arbeitsplätzen (VPN, FIDO, MFA, HTTPS).
- Einsatz von Standardwerkzeugen für die Netzwerkanalyse (Nslookup, tracert).
- Umsetzung von Maßnahmen zur Netzwerksicherheit.
- Einschätzung der technischen Aspekte von Netzwerken hinsichtlich Verfügbarkeit und Qualität.

Datensicherheit

- Für den Schutz und die Sicherheit von Informatiksystemen sorgen.
- Aspekte des Datenschutzes und der Datensicherheit erklären.
- Wissen um Pflichten und Rechte in Bezug auf die eigene Person und ihre Arbeitsumgebung, auf persönliche und fremde Daten verantwortungsbewusst anwenden.

Anzumerken ist, dass dieser Lehrplan derzeit im Rahmen einer generellen Lehrplanreform der Sekundarstufe 2 überarbeitet werden soll.

5.3 Kaufmännische Schulen – Handelsakademien und Handelsschulen

Der Fokus in den kaufmännischen Schulen liegt auf der praktischen Anwendung und dem sicheren Umgang mit Informationstechnologien in einem wirtschaftlichen Kontext. Es folgt eine detaillierte Recherche der Kompetenzen und darauffolgender Analyse anhand des CLEMENTINE-6-Stufen-Modells.

5.3.1 Handelsakademie Lehrplan 2014

In der Handelsakademie wird das Thema Cybersecurity vordergründig in den zwei IT-Gegenständen Officemanagement und angewandte Informatik (OMAI) sowie Wirtschaftsinformatik (WINF) behandelt.

[HAK] OMAI: 1. und 2. Semester

Bereich Informationstechnologie, Mensch und Gesellschaft:
- sichere Passwörter wählen,
- Daten kopieren, sichern, schützen und aktualisieren,
- lizenzrechtliche Bestimmungen von Software unterscheiden,
- sich in sozialen Netzwerken sicher bewegen.

Lehrstoff: Grundlegende Sicherheitsmaßnahme (Passwörter), sichere Internetnutzung

Stufe 1 (Allgemeine Einführung und Motivation):

- Sicherung des Grundverständnisses aus Sekundarstufe I
- Motivation zur Sicherheit
- Grundbegrifflichkeiten
- Sicherheitsempfehlungen
- Bedrohungsszenarien

Kontext Cybersecurity:

Die genannten Kompetenzen sind die Basis für die Cybersecurity und tragen zur Prävention digitaler Bedrohungen bei. Die Wahl sicherer Passwörter ist eine grundlegende Maßnahme zum Schutz vor unbefugtem Zugriff. Schwache oder mehrfach genutzte Passwörter erhöhen das Risiko erfolgreicher Phishing-Angriffe. Regelmäßige Backups (sicherer Umgang mit Daten) schützen vor Datenverlust durch technische Defekte oder Cyberangriffe. Verschlüsselung und aktuelle Sicherheitsupdates verhindern das Ausnutzen von Schwachstellen.

Die Kenntnis lizenzrechtlicher Bestimmungen gewährleistet nicht nur die rechtmäßige Nutzung von Software, sondern minimiert auch Sicherheitsrisiken. Illegale Kopien enthalten häufig Schadsoftware und stellen eine potenzielle Gefahr dar. Die bewusste Auswahl seriöser Softwarequellen ist daher ein wichtiger Schutzmechanismus. Soziale Netzwerke bergen Gefahren wie Identitätsdiebstahl, Phishing und Datenmissbrauch. Kritischer Umgang mit persönlichen Informationen, sichere Privatsphäre-Einstellungen und das Erkennen manipulativer Inhalte sind essenziell, um Risiken zu minimieren.

Diese Kompetenzen fördern daher ein sicherheitsbewusstes Verhalten und Reduzieren potenzielle Angriffsflächen im digitalen Raum.

[HAK] OMAI: 3. Semester

Bereich Internet:

- im Internet recherchieren, Browserfavoriten verwalten, Dateien komprimieren und uploaden, Dateien in der Cloud speichern, Gefahren des Internets erkennen

Lehrstoff: sicheres Bewegen im Internet

Stufe 1 (Allgemeine Einführung und Motivation):

- Motivation zur Sicherheit
- Über den Umgang mit Daten im Internet
- Sicherheitsempfehlungen
- Bedrohungsszenarien

Kontext Cybersecurity:

Die Fähigkeit, im Internet zu recherchieren, erfordert nicht nur den effizienten Umgang mit Suchmaschinen, sondern auch die kritische Bewertung von Quellen, um Fehlinformationen und Manipulationen zu erkennen. Besonders im Kontext von Cybersecurity ist es wichtig, u. a. Desinformation, Phishing-Websites oder Social-Engineering-Methoden zu identifizieren.

Das Komprimieren und Hochladen von Dateien erfordert grundlegendes Wissen über Dateiformate und sichere Übertragungsmethoden. Insbesondere beim Speichern in der Cloud ist es entscheidend, Verschlüsselungstechniken zu verstehen und sichere Passwörter oder Zwei-Faktor-Authentifizierung zu nutzen, um unbefugten Zugriff zu verhindern.

Die Fähigkeit, Gefahren des Internets zu erkennen, ist eine zentrale Kompetenz im Bereich der Cybersecurity. Dazu gehört das Bewusstsein für Malware, betrügerische E-Mails, Identitätsdiebstahl und datenschutzrelevante Risiken in sozialen Netzwerken.

[HAK] WINF: 6. Semester

Bereich Datensicherheit:
- automatisierte Sicherungen durchführen, Daten wiederherstellen,
- Sicherungen selektiv wiederherstellen, Systeme wiederherstellen (System Recovery),
- die Sicherheit von Daten gewährleisten,

Antivirenprogramme und Firewalls einsetzen.

Lehrstoff: Datensicherheit

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Vertraulichkeit & Integrität
- Über den Umgang mit Daten II
- Sichere Kommunikation

Kontext Cybersecurity:

Automatisierte Sicherungen und die gezielte Wiederherstellung von Daten sind notwendig, um den Verlust wichtiger Informationen infolge von Systemausfällen, Cyberangriffen oder technischen Defekten zu verhindern. Regelmäßige Backups gewährleisten die Integrität von Daten und ermöglichen eine schnelle Wiederherstellung betriebsfähiger Zustände. System Recovery stellt sicher, dass Systeme nach schwerwiegenden Fehlern oder Malware-Infektionen wieder funktionsfähig sind.

Die Sicherheit von Daten erfordert umfassende Schutzmaßnahmen wie Verschlüsselung, Zugriffskontrollen und sichere Speicherlösungen. Sensible Informationen müssen vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden, insbesondere im Hinblick auf Datenschutzvorgaben und Unternehmenssicherheit. Der Einsatz von Antivirenprogrammen und Firewalls ist dabei eine mögliche Verteidigungslinie. Während Antivirenprogramme Schadsoftware erkennen und beseitigen, kontrollieren Firewalls den Datenverkehr und verhindern unautorisierte Netzwerkzugriffe. Die Kombination dieser Sicherheitsmaßnahmen trägt wesentlich zur Stabilität und Widerstandsfähigkeit digitaler Systeme bei.

[HAK] Recht: 8. Semester

Bereich Bearbeitung und Lösung alltäglicher Rechtsprobleme:
- die Bereiche Datenschutz, Persönlichkeitsrechte, Urheber- und Strafrecht im Zusammenhang mit sozialen Netzwerken in Beziehung setzen und ihr eigenes Nutzerverhalten kritisch analysieren sowie rechtliche Risiken erkennen

Lehrstoff: Umgang mit Social Networks, Datenschutz

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Rechtsgrundlagen

Kontext Cybersecurity:

Bemerkenswert ist, dass durch den Unterrichtsgegenstand „Recht“ das Thema Cybersecurity in der Handelsakademie auch fächerübergreifend behandelt wird. Das Verständnis von Datenschutz, Persönlichkeitsrechten, Urheber- und Strafrecht im Kontext sozialer Netzwerke dient dazu, um rechtliche Fallstricke zu vermeiden. Die Veröffentlichung und Weitergabe von personenbezogenen Daten unterliegt strengen Datenschutzrichtlinien.

Persönlichkeitsrechte schützen vor Diffamierung, Identitätsdiebstahl oder unerlaubter Bildnutzung, während das Urheberrecht die rechtmäßige Verwendung fremder Inhalte regelt. Zudem haben Verstöße, etwa durch Cybermobbing oder Verleumdung, oft strafrechtliche Konsequenzen.

[HAK] WINF: 9. Semester

Bereich Datensicherheit:

- mögliche Bedrohungsszenarien für digital gespeicherte Daten aufzeigen,
- Sicherheits- und Sicherungssysteme in Unternehmen bewerten und konfigurieren,
- grundlegende datenschutzrechtliche Bestimmungen unterscheiden,
- grobe Verstöße gegen datenschutzrechtliche Bestimmungen aufzeigen,
- beurteilen, ob Handlungen im Rahmen von IT-Anwendungen gegen entsprechende gesetzliche Bestimmungen verstoßen,
- die Bedeutung der Datenverschlüsselung beschreiben und Daten sicher übertragen,
- E-Business-Anwendungen nutzen.

Lehrstoff: IT und Recht (E-Commerce, E-Government, Urheberrecht, Datenschutz)

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Vertraulichkeit & Integrität
- Über den Umgang mit Daten II
- Sichere Kommunikation
- Digitale Bürgerkarte
- Rechtsgrundlagen
- Technische Umsetzungsstrategien
- Angriffsvektoren

Kontext Cybersecurity:

Im Kontext von IT und Recht, insbesondere in Bezug auf E-Commerce, E-Government und Datenschutz, ist es entscheidend, mögliche Bedrohungsszenarien für digital gespeicherte Daten zu erkennen. Zu diesen Bedrohungen zählen Angriffe wie Ransomware, Phishing, Datendiebstahl oder unbefugter Zugriff durch Insider. Das Bewusstsein für diese Gefahren ist wichtig, um präventive Sicherheitsmaßnahmen zu ergreifen. Sicherheits- und Sicherungssysteme in Unternehmen sind unerlässlich, um Daten vor externen und internen Bedrohungen zu schützen. Die Fähigkeit, solche Systeme zu bewerten und richtig zu konfigurieren dient der Aufrechterhaltung der Unternehmenssicherheit. Dies umfasst die Auswahl geeigneter Firewalls, Verschlüsselungsmaßnahmen sowie regelmäßige Backups und deren Integration in die Unternehmensstrategie.

Das Verständnis datenschutzrechtlicher Bestimmungen umfasst (wie im Unterrichtsgegenstand „Recht“) den Umgang mit personenbezogenen Daten gemäß den Vorgaben der Datenschutzgrundverordnung (DSGVO) sowie das Wissen über Rechte der betroffenen Personen. Grobe Verstöße gegen datenschutzrechtliche Bestimmungen, wie etwa unrechtmäßige Datenweitergabe, das Fehlen einer ausreichenden Einwilligung oder die Nichteinhaltung der Aufbewahrungsfristen, müssen erkannt und entsprechende Maßnahmen eingeleitet werden. Die Fähigkeit, zu beurteilen, ob Handlungen im Rahmen von IT-Anwendungen gegen gesetzliche Bestimmungen verstoßen, ist relevant, um Haftungsrisiken zu vermeiden.

Datenverschlüsselung für die Sicherheit digitaler Informationen gewährleistet den Schutz von Daten bei der Speicherung und Übertragung. Das sichere Übertragen von Daten, etwa durch den Einsatz von HTTPS oder VPNs, schützt die anwendende Person. Schließlich ist die Nutzung von E-Business-Anwendungen im Rahmen von E-Commerce und E-Government ein wesentlicher Bestandteil moderner Geschäftsprozesse. Dabei müssen nicht nur technische, sondern auch rechtliche Rahmenbedingungen berücksichtigt werden, um sicherzustellen, dass alle Transaktionen und Interaktionen rechtmäßig und sicher ablaufen.

5.3.2 Handelsschule Lehrplan 2014

In der Handelsschule sind gleichlautende Kompetenzen wie aus der Handelsakademie zu finden. Es findet keine Unterscheidung, z.B. durch Operatoren, statt. Jedoch werden die tiefergehenden Kompetenzen, vor allem aus den höheren Jahrgängen der Handelsakademie nicht behandelt.

[HAS] OMAI: 1. und 2. Semester

Bereich Informatiksysteme

- Dateien verwalten

Bereich Publikation und Kommunikation

- das Internet effizient nutzen

Lehrstoff: Datensicherung, Informationsbeschaffung im Internet

Stufe 1 (Allgemeine Einführung und Motivation):

- Sicherung des Grundverständnisses aus Sekundarstufe I
- Motivation zur Sicherheit
- Über den Umgang mit Daten im Internet
- Bedrohungsszenarien

[HAS] VWRE: 5. Semester

Bereich:

- den rechtlichen Rahmen im Umgang mit elektronischen Medien erkennen und ihr Nutzerverhalten daran anpassen

Lehrstoff: Recht im Internet (E-Commerce, Signaturgesetz, Fernabsatzbestimmungen des Konsumentenschutzgesetzes, Urheberrecht, Datenschutzrecht)

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Rechtsgrundlagen

[HAS] OMAI: 6. Semester

Bereich Informationstechnologie, Mensch und Gesellschaft:

- Daten sichern und schützen,
- grundlegende datenschutzrechtliche Bestimmungen unterscheiden und grobe Verstöße dagegen aufzeigen,
- beurteilen, ob Handlungen im Rahmen von IT-Anwendungen gegen entsprechende gesetzliche Bestimmungen verstoßen,

E-Business-Anwendungen nutzen.

Lehrstoff: Daten sichern und schützen, E-Business-Anwendungen, gesetzliche Rahmenbedingungen

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Über den Umgang mit Daten II
- Rechtsgrundlagen
- Digitale Bürgerkarte

5.3.3 Spezialisierung CyberHAK

Mit der fortschreitenden Digitalisierung steigt der Bedarf an Expertise im Bereich der IT- und Cybersecurity. Daher sind gut ausgebildete Fachkräfte sehr gefragt. Die Ausbildung an der Handelsakademie – Sicherheitsmanagement und Cyber-Security verbindet Allgemeinbildung, kaufmännisches Wissen, eine fundierte IT-Ausbildung sowie praxisorientierte Inhalte zu Sicherheitsmanagement und Cyber-Security in integrierter Form. Sie richtet sich an Schüler:innen, die eine solide Grundlage für eine spätere Laufbahn bei der Polizei oder für eine Tätigkeit als Sicherheitsexpertin bzw. Sicherheitsexperte in der Privatwirtschaft erwerben möchten.

Die Eckdaten zur Ausbildung

- Die Schüler:innenakquirierung erfolgt aufgrund der Einzigartigkeit der Ausbildung über die Bezirks- und Landesgrenzen hinweg.
- Kombination von traditionellen Ausbildungsinhalten der HAK mit Expert:innenwissen von Polizei, Sicherheit- sowie Katastrophenschutz
- Die Absolvent:innen können sowohl im polizeilichen als auch im privatwirtschaftlichen Sektor arbeiten. Im Rahmen des Unterrichts wird zusätzlich auf das Auswahlverfahren der Polizei vorbereitet.
- Potenzielle Arbeitgeber:innen: Klein- und Mittelbetriebe, Innenministerium, Verteidigungsministerium, Krisen- und Katastrophenmanagement von Bund, Land und Bezirkshauptmannschaften, Wirtschaftskammer, Private Sicherheitsorganisationen, größere Unternehmen mit eigenen Sicherheitsbeauftragten
- Die Schüler:innen absolvieren zusätzlich die Ausbildung zum zertifizierten „Information Security Manager nach ISO 27001“.

Tabelle 6: Stundeplan CyberHAK

2. Schulautonomer Erweiterungsbereich Sicherheitsmanagement & Cyber Security		I.	II.	III.	IV.	V.		23
2.1.	Sicherheitsmanagement			2	2	2	6	I
2.2.	Cyber Security	1	1	2	2	1	7	I
2.3.	Juristisches Praxisfeld Sicherheit				3	-	3	II
2.4.	Psychische und kognitive Eignungsvorbereitung					1	1	III
2.5.	Physische Leistungsfähigkeit					1	1	iVa
2.6.	Information Security Management				1	-	1	I

Der Lehrplan inklusive den Kompetenzen des schulautonomen Erweiterungsbereichs „Sicherheitsmanagement & Cybersecurity“ ist nicht für die Öffentlichkeit zugänglich. Anhand der Zertifizierung zum Information Security Manager nach ISO 27001 ist davon auszugehen, dass dies der Stufe 3 (Netzwerk-, Geräte - und Anwendungssicherheit, Sicherheitsmanagement) des CLEMENTINE-6-Stufen-Modells entspricht.

Handelsakademie Lehrplan NEU 2027: Der neue Handelsakademie Lehrplan soll 2027 in Kraft treten. Aktuell handelt es sich bei der nachfolgenden Recherche um den finalen Entwurf. Anzumerken ist, dass der Lehrplan daher noch nicht in Begutachtung ist und verändert werden kann.

Die zwei Unterrichtsgegenstände „Officemanagement und angewandte Informatik“ sowie „Wirtschaftsinformatik“ werden im neuen Lehrplan zu einem Unterrichtsgegenstand „IT Business & Creative Solutions“ fusioniert.

Kernkompetenzen:

- Probleme der betrieblichen Praxis mithilfe von IT-Tools und künstliche Intelligenz (KI) selbständig lösen
- IT-Applikationen zielorientiert nutzen und die Funktionsfähigkeit sicherstellen
- mit Daten verantwortungsvoll umgehen
- Kreativität mithilfe digitaler Tools anregen

Bereiche:

- P. Kaufmännische Problemlösung mithilfe IT und KI
- K. Kollaboration, Prozesse und IT-Infrastruktur
- D. Data Awareness, KI und Cybersecurity
- L. Digitale Lernwerkstatt

Der Begriff „Cybersecurity“ bildet eines der vier Säulen des neuen Lehrplans und nimmt daher eine zentrale Rolle in der zukünftigen Ausbildung der Schüler:innen ein.

Relevante Kompetenzen:

- Eigenes digitales Nutzungsverhalten reflektieren (1. und 2. Semester)
- Informationen beschaffen und bewerten (1. und 2. Semester)
- Inhalte urheberrechtlich prüfen (1. und 2. Semester)
- Chancen und Risiken künstlicher Intelligenz beurteilen (3. Semester)
- Internet sicher nutzen (4. Semester)
- Daten sicher austauschen (5. Semester)
- Rechtsthematiken mit IT-Bezug darstellen (8. Semester)

Eine detaillierte Recherche anhand des CLEMENTINE-6-Stufen-Modells ist erst möglich, wenn der genaue Lehrstoff feststeht. Es ist aber davon auszugehen, dass die Stufen 1 bis 2, partiell auch Schritt 3 erfüllt werden.

5.4 Humanberufliche Schulen

Der Fokus in den humanberuflichen Schulen liegt ebenso auf der praktischen Anwendung und dem sicheren Umgang mit Informationstechnologien in einem wirtschaftlichen Kontext. Im nachfolgenden werden die Höheren Lehranstalten für wirtschaftliche Berufe (Berufsbildende höhere Schulen - BHS) sowie die dazugehörige Fachschule (Berufsbildende mittlere Schulen - BMS) untersucht.

5.4.1 Höhere Lehranstalt für wirtschaftliche Berufe Lehrplan 2015

In der HLW wird Cybersecurity vordergründig im IT-Unterrichtsgegenstand „Angewandtes Informationsmanagement“ (AINF) behandelt. Ein neuer Lehrplan erscheint frühestens 2028 und es gibt dementsprechend aktuell keinen Entwurf.

[HLW] AINF: 1. und 2. Semester

- kennen die Funktionsweise eines Computersystems,
- kennen die wichtigsten Maßeinheiten der Informatik und können damit arbeiten,
- können Netzwerke sicherheitsbewusst nutzen,
- können sichere Passwörter erstellen und damit verantwortungsvoll umgehen,
- kennen unterschiedliche Datensicherungskonzepte für den privaten Bereich
- sind sich der Notwendigkeit des Einsatzes von Virenschutz und Firewall bewusst,
- können aktuelle Online-Dienste nutzen und Daten online verwalten,
- kennen Grundzüge des Urheberrechts,
- kennen unterschiedliche Lizenzmodelle,
- können sicher im Internet agieren,
- können Informationen auf Plausibilität und Authentizität prüfen,
- können soziale Netzwerke im privaten Bereich verantwortungsbewusst nutzen

Lehrstoff: Betriebssystem, Arbeiten im Netzwerk und ausgegliederte IT-Infrastruktur, Grundzüge des Urheberrechts, Lizenzmodelle, Internet und Internetdienste

Stufe 1 (Allgemeine Einführung und Motivation):

- Sicherung des Grundverständnisses aus Sekundarstufe I
- Motivation zur Sicherheit
- Grundbegrifflichkeiten
- Sicherheitsempfehlungen
- Bedrohungsszenarien

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Über den Umgang mit Daten II

- Rechtsgrundlagen

Kontext Cybersecurity: Im Vergleich zu den kaufmännischen Schulen werden bereits viele Inhalte, die Cybersecurity betreffen, bereits im 1. Jahrgang vermittelt. Die genannten Kompetenzen bilden einen umfassenden Rahmen für den sicheren und verantwortungsvollen Umgang mit digitalen Technologien und Ressourcen. Das Wissen um die Funktionsweise eines Computersystems ist entscheidend, um das Arbeitsgerät grundlegend zu verstehen, von der Hardware über das Betriebssystem bis hin zu den Anwendungen. Das sichere und verantwortungsbewusste Nutzen von Netzwerken dient dem Schutz von persönlichen als auch berufliche Daten vor Bedrohungen wie unbefugtem Zugriff und Cyberangriffen. Dazu gehört auch die Fähigkeit, sichere Passwörter zu erstellen und richtig zu verwalten, um die Datensicherheit zu gewährleisten und Cyberkriminalität zu vermeiden. Ein vertieftes Verständnis verschiedener Datensicherungskonzepte ist notwendig, um private Daten vor Verlust oder Beschädigung zu schützen. Dies umfasst neben einfachen Backup-Strategien auch die Wahl geeigneter Speichermedien und Methoden, die den Zugriff auf gesicherte Daten im Notfall gewährleisten. Die Nutzung von Virenschutzsoftware und Firewalls ist für den Schutz vor Malware und unerwünschten Netzwerkzugriffen von entscheidender Bedeutung. Das Wissen über Urheberrechte und Lizenzmodelle stellt sicher, dass die rechtlichen Rahmenbedingungen beim Umgang mit Software, Medien und anderen digitalen Inhalten respektiert werden. Der verantwortungsvolle Umgang mit Online-Inhalten und die Fähigkeit, diese auf ihre Plausibilität und Authentizität zu prüfen, helfen dabei, Fehlinformationen zu vermeiden und sich sicher im Internet zu bewegen. Die Nutzer:innen müssen sich der möglichen Risiken bewusst sein, die mit der Veröffentlichung von persönlichen Informationen und Interaktionen in sozialen Medien einhergehen. Ein reflektierter Umgang schützt nicht nur die eigene Privatsphäre, sondern trägt auch zur Wahrung der digitalen Etikette und Sicherheit bei.

[HLW] AINF: 6. Semester

- kennen unterschiedliche Soziale Netzwerke und deren Einsatzbereiche,
- wissen um die Notwendigkeit der regelmäßigen Betreuung eines betrieblichen Online-Auftritts Bescheid,
- kennen die wirtschaftliche und gesellschaftliche Bedeutung von Sozialen Netzwerken

Lehrstoff: Online-Publishing: Content Management System, Soziale Netzwerke

Stufe 1 (Allgemeine Einführung und Motivation):

- Motivation zur Sicherheit
- Sicherheitsempfehlungen
- Bedrohungsszenarien

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Über den Umgang mit Daten II

Kontext Cybersecurity: Die Kenntnis verschiedener sozialer Netzwerke und ihrer spezifischen Einsatzbereiche ist nicht nur für Marketing und Kommunikation relevant, sondern auch für die Cybersecurity. Jedes Netzwerk birgt eigene Risiken, wie Phishing, Identitätsdiebstahl oder Malware-Verbreitung, die durch gezielte Sicherheitsvorkehrungen minimiert werden müssen. Die Nutzung von sozialen Netzwerken erfordert ein tiefes Verständnis der damit verbundenen Bedrohungen, wie etwa unsichere Privatsphäre-Einstellungen oder Datenlecks, die die Sicherheit der Anwenderinnen und Anwender gefährden können. Die regelmäßige Betreuung eines betrieblichen Online-Auftritts ist im Hinblick auf Cybersecurity von besonderer Bedeutung, um eine kontinuierliche Überwachung der Netzwerksicherheit, das Implementieren von Sicherheitsprotokollen und den Schutz vor Cyberangriffen zu gewährleisten. Auch der Umgang mit sensiblen Kundendaten auf sozialen Plattformen muss rechtssicher und datenschutzkonform erfolgen, um Sicherheitslücken zu vermeiden. Angesichts dieser Bedrohungen müssen Unternehmen und Einzelpersonen sich der Risiken bewusst sein und proaktive Sicherheitsmaßnahmen ergreifen. Die Integration von Verschlüsselung, Zwei-Faktor-Authentifizierung und einer sicheren Netzwerkinfrastruktur ist entscheidend, um den Schutz der Daten und die Privatsphäre zu gewährleisten.

[HLW] AINF: 7. und 8. Semester

- kennen Möglichkeiten einer ausgegliederten IT-Infrastruktur (z.B. Cloud-Dienste) und deren Nutzen und Risiken
- können die datenschutzrechtlichen Bestimmungen anwenden,
- kennen unterschiedliche Datensicherungskonzepte für den betrieblichen Bereich,
- kennen die Methoden der Verschlüsselung,
- sind sich der Notwendigkeit des Einsatzes von Verschlüsselung bewusst,

- können Online-Services des öffentlichen Bereiches mit Bürgerkartenfunktion nutzen,
- kennen die Bedeutung der digitalen Signatur einschließlich der gesetzlichen Basis,
- kennen die aktuellen IT-Technologien und entsprechende Anwendungsszenarien

Lehrstoff: Ausgegliederte IT-Infrastruktur, Datenschutz und Datensicherheit, E-Government, Digitale Signatur, Verschlüsselung, Neue Medien und Technologien

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Vertraulichkeit & Integrität
- Über den Umgang mit Daten II
- Sichere Kommunikation
- Smart Devices
- Rechtsgrundlagen
- Digitale Bürgerkarte

Ausgegliederte IT-Infrastrukturen wie Cloud-Dienste bieten Flexibilität, bringen jedoch auch Risiken im Hinblick auf Datenschutz und Datenkontrolle mit sich. Ein fundiertes Verständnis dieser Technologien ist notwendig, um ihre Vorteile sicher zu nutzen. Die Anwendung datenschutzrechtlicher Bestimmungen wie der DSGVO schützt sowohl die Privatsphäre als auch vor rechtlichen Konsequenzen. Für Unternehmen sind geeignete Datensicherungskonzepte wie regelmäßige Backups und Notfallwiederherstellungen notwendig, um Daten vor Verlust zu schützen. Verschlüsselung spielt eine wichtige Rolle im Datenschutz, indem sie Informationen vor unbefugtem Zugriff schützt. Die Nutzung sicherer Online-Services mit Bürgerkartenfunktion erleichtert die sichere Interaktion mit öffentlichen Institutionen. Die digitale Signatur gewährleistet die rechtliche Verbindlichkeit digitaler Dokumente und Transaktionen. Das Verständnis aktueller IT-Technologien wie KI, Blockchain oder IoT hilft, deren Chancen und Risiken zu erkennen und verantwortungsbewusst zu nutzen.

5.4.2 Fachschule für wirtschaftliche Berufe Lehrplan 2015

Die Fachschule für wirtschaftliche Berufe (BMS) hat zum Teil ähnliche Kompetenzen wie die höhere Lehranstalt für wirtschaftliche Berufe (BHS). Die Kompetenzen werden einfacher und kürzer formuliert. Im Kern bleibt die Analyse ident zur HLW. Der Unterrichtsgegenstand in der FW nennt sich, wie in der HAK, „Officemanagement und angewandte Informatik“.

[FW] OMAI: 1. und 2. Semester

- Dateien verwalten,
- mit komprimierten Dateien arbeiten,
- freigegebene Netzwerkressourcen nutzen,
- sicher im Internet agieren,
- online recherchieren,
- online kommunizieren,
- mit Daten sicher umgehen,
- Grundzüge des Urheberrechts erläutern

Lehrstoff: Betriebssysteme und Arbeiten im Netzwerk, Internet und Internetdienste, Gesetzliche Bestimmungen

Stufe 1 (Allgemeine Einführung und Motivation):

- Sicherung des Grundverständnisses aus Sekundarstufe I
- Motivation zur Sicherheit
- Grundbegrifflichkeiten
- Sicherheitsempfehlungen
- Bedrohungsszenarien

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Rechtsgrundlagen

[FW] OMAI: 5. Semester

- in sozialen Netzwerken, verantwortungsbewusst arbeiten,
- Daten online verwalten,
- neue IT-Technologien und deren Folgen im gesellschaftlichen Zusammenhang nennen

Lehrstoff: Online-Publishing (Content Management System).

Stufe 1 (Allgemeine Einführung und Motivation):

- Motivation zur Sicherheit
- Sicherheitsempfehlungen
- Bedrohungsszenarien

[FW] OMAI: 6. Semester

- in sozialen Netzwerken verantwortungsbewusst kommunizieren,
- Daten online verwalten
- die datenschutzrechtlichen Bestimmungen anwenden,
- neue IT-Technologien und deren Folgen im gesellschaftlichen Zusammenhang beschreiben

Lehrstoff: Datenschutz und E-Government, Neue Medien und Technologien

Stufe 2 (Tiefergehende Awareness für IT-Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen):

- Rechtsgrundlagen
- Über den Umgang mit Daten II
- Sichere Kommunikation
- Smart Devices
- Digitale Bürgerkarte

Zusammenfassung der Ergebnisse

Die Cybersecurity-Kompetenzen an kaufmännischen (HAK/HAS) und humanberuflichen (HLW/FW) Schulen sind überwiegend den Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells zuzuordnen. Aufgrund der offen formulierten Kompetenzbeschreibungen besteht ein hoher Gestaltungsspielraum im Unterricht. Die Analyse zeigt auf, in welchem Kontext der Rahmenlehrplan Cybersecurity-Unterricht ermöglicht.

Aufgrund der Vielfalt an Kompetenzen kann davon ausgegangen werden, dass Absolvent:innen dieser Schulen mit soliden Kenntnissen im Bereich Cybersecurity abschließen. Für besonders interessierte Schüler:innen bietet die „CyberHAK“ eine spezialisierte Vertiefung, die mit einer Zertifizierung als Information Security Manager nach ISO 27001 abschließt. Diese Qualifikation eröffnet berufliche Perspektiven sowohl im polizeilichen als auch im privatwirtschaftlichen Sektor. Die Kompetenztiefe kann mit **Intermediate** festgelegt werden.

5.5 Höhere und mittlere technische und gewerbliche Lehranstalten

Bei den Höheren technischen und gewerblichen Lehranstalten gibt es 34 unterschiedliche Lehrpläne, welche eine „digitale Grundbildung“ auf unterschiedliche Art und Weise abbilden – siehe auch die folgende Tabelle:

- Bei 13 Lehrplänen wurde bereits eine Standardisierung der digitalen Grundbildung mittels des Faches „Angewandte Informatik“ durchgeführt. Sowohl Umfang als auch Inhalte werden über die „Anlage 1 - Angewandte Informatik“ (Kapitel 5.5.1) geregelt.
- In den Wirtschaftsingenieur Fachrichtungen (10 Lehrpläne) wird die digitale Grundbildung mit facheinschlägigen Lehrinhalten kombiniert im Gegenstand „Informatik und Informationssysteme“ geregelt. Neben den sich daraus ergebenden Unterschieden ist leider auch die digitale Basis sehr unterschiedlich aufbereitet.
- In den Fachrichtungen „Informatik“ und „Informationstechnologie“ teilen sich die Cybersecurity-Inhalte naturgemäß auf mehrere Fachgegenstände auf.
- Im Lehrplan „Elektronik und Technischer Informatik“ wird die digitale Grundbildung im Gegenstand „Fachspezifische Softwaretechnik“ und angrenzenden Gegenständen geregelt, jedoch sehr Hardware-orientiert.
- Sowohl in den Lehrplänen „Medien“ und „Grafik- und Kommunikationsdesign“ gibt es den Gegenstand „Medientechnologie und angewandte Informatik“. Wie auch bei „Biomedizin und Gesundheitstechnik“ und „Technik in Medizin, Life Science und Sport“ einen gleichlautenden Gegenstand „Medizin- und Gesundheitsinformatik“ für digitale Grundbildung. Beide Gegenstände sind eine Mischung aus digitaler Grundbildung und fachspezifischer Anwendungen.

- In allen anderen Fachrichtungen regelt ein Gegenstand mit unterschiedlichen Namen die angewandte Informatik als Kombination aus digitaler Grundbildung und fachspezifischen Anwendungen - ähnlich den Wirtschaftsingenieur (WI) Lehrplänen.

Grundsätzlich sind diese Kategorien nur schwer miteinander vergleichbar, da die ausgewiesenen Lehrinhalte sehr verschieden sind. Im Sinne des besprochen „Lehrplan-Dilemmas" ist jedoch davon auszugehen, dass Cybersecurity-Inhalte implizit behandelt werden. Die anschließenden Analysen werden - bedingt durch die Heterogenität und die teils mehrfach verwendeten Gegenständen in den Lehrplänen – anhand der ausgewiesenen Gegenstände durchgeführt. Die folgende Abbildung zeigt eine Übersicht der Höheren technischen Lehranstalten:

Lehrpläne der Höheren technischen und gewerblichen Lehranstalten (einschließlich der kunstgew. Lehranstalten) - 2015 – BGBl. II Nr. 262/2015 idgF[26]

Tabelle 7: Lehrpläne der Höheren technischen und gewerblichen Lehranstalten (einschließlich der kunstgew. Lehranstalten) - 2015 – BGBl. II Nr. 262/2015 idgF

Anlage	Fachrichtung	Cybersecurity Zielgegenstand	1	2	3	4	5
1	Anlage 1	**Angewandte Informatik**	2	2			
1.1	Art and Design	Technologie und Angewandte Informatik	6	6	7	7	7
1.2	Bautechnik	**Angewandte Informatik**	2	2			
1.3	Biomedizin und Gesundheitstechnik	Medizin- und Gesundheitsinformatik	3	4	2	2	2
1.4	Chemieingenieure	**Angewandte Informatik**	2	2			
1.5	Elektronik und Technische Informatik	Fachspezifische Softwaretechnik	3	4	2	2	2
1.6	Elektrotechnik	Fachspezifische Informationstechnik	2	2	2	2	2
1.7	Flugtechnik	**Angewandte Informatik**	2	2			
1.8	Gebäudetechnik	**Angewandte Informatik**	2	2			
1.9	Grafik- und Kommunikationsdesign	Medientechnologie und Angewandte Informatik	5	5	5	5	6
1.10	Informatik	Diverse Fachgegenstände	na	na	na	na	na
1.11	Informationstechnologie	Diverse Fachgegenstände	na	na	na	na	na
1.12	Innenarchitektur und Holztechnologien	**Angewandte Informatik**					
1.13	Kunststoff- und Umwelttechnik	**Angewandte Informatik**					
1.14	Lebensmitteltechnologie – Getreide- und Biotechnologie	**Angewandte Informatik**					
1.15	Lebensmitteltechnologie - Lebensmittelsicherheit	**Angewandte Informatik**					
1.16	Maschinenbau	**Angewandte Informatik**					
1.17	Mechatronik	Angewandte Informatik und fachspez. Informationstechnik	2	2	2	2	2
1.18	Medien	Medientechnologie und Angewandte Informatik	5	5	5	4	4
1.19	Medieningenieure und Printmanagement	**Angewandte Informatik**	2	2			
1.20	Metallische Werkstofftechnik	**Angewandte Informatik**	2	2			
1.21	Metallurgie und Umwelttechnik	**Angewandte Informatik**	2	2			

26 Lehrplaene_der_Hoeheren_technischen_und_gewerblichen_Lehranstalten_2015_Stand_14_09_2021_a028f44eda.pdf

1.22	WI – Rohstoff- und Energietechnik	Informatik und Informationssysteme	2	2	2	2	4
1.23	WI – Bekleidungstechnik	Informatik und Informationssysteme	2	2	2	2	4
1.24	WI – Betriebsinformation	Informatik und Informationssysteme	2	3	2	2	6
1.25	WI – Holztechnik	Informatik und Informationssysteme	2	2	2	2	3
1.26	WI – Logistik	Informatik und Informationssysteme	2	2	2	2	4
1.27	WI – Maschinenbau	Informatik und Informationssysteme	2	2	2	2	4
1.28	WI – Technisches Management	Informatik und Informationssysteme	2	2	2	2	4
1.29	WI – Textiltechnik	Informatik und Informationssysteme	2	2	2	2	4
1.30	WI – Productmanagement and Future Tecs	Informatik und Informationssysteme	2	2	2	2	4
1.31	WI – Informationstechnologie und Smart Production	Informatik und Informationssysteme	2	2	2	2	4
1.32	Technik in Medizin, Life Science und Sport	Medizin- und Gesundheitsinformatik	3	3	2	2	2
1.33	Material- und Umwelttechnologie	Informatik, Projekt- und Qualitätsmanagement	2	2	2	2	4
1.34	Aviation Technology	**Angewandte Informatik**	2	2			

5.5.1 Anlage 1[27] - Angewandte Informatik

Der Gegenstand „Angewandte Informatik“ wird in der Anlage 1 geregelt und in folgenden Lehrplänen verwendet:

- Aviation Technology
- Bautechnik
- Chemieingenieure
- Flugtechnik
- Gebäudetechnik
- Innenarchitektur und Holztechnologien
- Kunststoff- und Umwelttechnik
- Lebensmitteltechnologie – Getreide- und Biotechnologie Lebensmitteltechnologie - Lebensmittelsicherheit
- Maschinenbau
- Medieningenieure und Printmanagement
- Metallische Werkstofftechnik
- Metallurgie und Umwelttechnik

Wie in der Struktur der Lehrpläne der Höheren und Mittleren technischen und gewerblichen Lehranstalten dargelegt, sind mehrere allgemein gültige Fächer über die „Anlage 1“ für verschiedene Lehrpläne festgelegt. Der darin enthaltene Bereich „Angewandte Informatik“ gewährleistet eine einheitliche Regelung der digitalen Grundbildung.

Die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells sind in der Anlage 1 allgemein dadurch berücksichtigt, dass Grundlagen der Informationstechnologie und ein Bewusstsein für den Umgang mit Daten in verschiedenen Pflichtgegenständen vermittelt werden.

Folgende Lehrplanergänzungen die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells schrittweise in den Lehrplan der ersten beiden Jahrgänge im Pflichtgegenstand "Angewandte Informatik". Die sprachlichen Fächer können zur Sensibilisierung im Bereich der Kommunikationssicherheit beitragen, und die "Soziale und personale Kompetenz" kann allgemeine Verhaltensweisen und Reaktionsmuster unterstützen. Es ist wichtig zu betonen, dass die technische Tiefe der Cybersecurity-Inhalte in diesen ersten Stufen begrenzt bleiben sollte, um das allgemeine Verständnis zu fördern und das Interesse zu wecken.

5.5.1.1 Lehrplanergänzung

1. Jahrgang (1. und 2. Semester)

1. Semester:

Pflichtgegenstand „Angewandte Informatik“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können grundlegende Verhaltensregeln im Umgang mit digitalen Medien und Daten beschreiben und Risiken im digitalen Raum erkennen.*

[27] https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40237785/NOR40237785.pdf

- **Wiederholung und Vertiefung: Das richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten** (aus "Sicherung des Grundverständnisses aus Sekundarstufe I"). Dies könnte zu Beginn des Semesters als Auffrischung wichtiger Grundlagen dienen.
- **Grundlagen: Das Erkennen von Risken und Reaktionsgrundsätze** (aus "Sicherung des Grundverständnisses aus Sekundarstufe I"). Eine erste Einführung in typische Gefahren im digitalen Raum.
- **Motivation: Bewusstseinsbildung durch Video-Fallbeispiele** (Keylogger als Beispiel). Einfache Fallbeispiele (ohne detaillierte technische Analyse) zu Themen wie Passwortsicherheit und verdächtigen E-Mails.
- **Grundlagen:** Grundlegende Einführung und Sensibilisierung für **Schadsoftware**. Was ist Schadsoftware und wie kann man ihr begegnen?

Verbindliche Übung „Soziale und personale Kompetenz“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können die Bedeutung eines verantwortungsbewussten Umgangs mit persönlichen Informationen und digitalen Identitäten reflektieren.*

- Grundlagen des **Schutzes personenbezogener Daten** im Sinne von Vorsichtsmaßnahmen bei der Weitergabe persönlicher Informationen in sozialen Medien und Online-Diensten.

2. Semester:

Pflichtgegenstand "Angewandte Informatik":

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können einfache Bedrohungen und Angriffsversuche erkennen und grundlegende Schutzmaßnahmen anwenden.*

- **Motivation:** Erste Einführung in die Unterscheidung **"Gute Hacker – Böse Cracker?"** und das Konzept des **Ethical Hacking** (motivierend, ohne technische Tiefe).
- **Grundlagen:** Thematisierung von **Identitätsdiebstahl** im Kontext der Datensicherheit und des Schutzes persönlicher Informationen.
- **Bedrohungen:** Erste allgemeine Einführung in **Bedrohungen** und deren **Auswirkungen**.
- **Was tun im Notfall?** Einführung in das richtige Reagieren auf verdächtige Vorfälle (z.B. nicht auf unbekannte Links klicken, Meldung an eine Lehrkraft oder Erziehungsberechtigte).

Pflichtgegenstand „Deutsch“ alternativ oder ergänzend „Englisch“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können Medieninhalte kritisch im Hinblick auf manipulative Absichten (z.B. Phishing) analysieren.*

- **Motivation/Bewusstseinsbildung:** Erste Sensibilisierung für **Angriffsmethoden für Informationsweitergabe** wie einfache Formen von **Phishing** im Kontext der Analyse von Nachrichten (z.B. Erkennen verdächtiger E-Mails). (Siehe Lernergebnisse im Bereich Lesen: "Texte aus eigenen und anderen Kulturen und Lebenswelten; sinnerfassendes [...] Lesen").

2. Jahrgang (3. und 4. Semester)

3. Semester:

Pflichtgegenstand „Angewandte Informatik“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können die grundlegende Funktionsweise der Verschlüsselung zum Schutz von Daten erklären.*

- **Bedrohungen:** Detailliertere Behandlung von **Angriffsvektoren** und **Eskalationsszenarien**.
- **Schutz:** Vertiefung des Themas **Schutz personenbezogener Daten**.
- **Angriffsmethoden:** Einführung in **Social Engineering** als spezifische Form der Bedrohung.
- **Angriffsmethoden:** Konkretere Beispiele für **Angriffsmethoden für Informationsweitergabe** wie **Phishing** und erste Erwähnung von **Whaling** (ohne technische Details).
- **Was tun im Notfall?:** Information über relevante **Ansprechpartner kennen** bei Sicherheitsvorfällen (kann auch schulweit kommuniziert und hier wiederholt werden).

Verbindliche Übung „Soziale und personale Kompetenz“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen verstehen den verantwortungsbewussten Umgang mit digitalen Technologien und reagieren richtig.*

- **Grundlagen:** Vertiefung des verantwortungsbewussten Umgangs mit Technologie, inklusive **richtigem Reagieren** in verschiedenen Situationen.

4. Semester:

Pflichtgegenstand "Angewandte Informatik":

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können grundlegende Prinzipien des Sicherheitsmanagements im Alltag anwenden und die Bedeutung von Cyberkriminalität einschätzen.*

- **Grundlagen:** Einführung des grundlegenden Konzepts von **Verschlüsselung** (ohne technische Tiefe) im Zusammenhang mit Datensicherheit und sicherer Kommunikation.
- **Grundlagen:** Erklärung der Funktionsweise einer **Hashfunktion** (ohne technische Tiefe) als Methode zur Sicherstellung der Datenintegrität.
- **Was tun im Notfall?:** Vermittlung grundlegender Schritte zur **Infektionsbeseitigung initiieren** (als erste Orientierung, ohne detaillierte technische Anleitungen).

Pflichtgegenstand „Deutsch“ alternativ oder ergänzend „Englisch“:

Bildungs- und Lehraufgabe ergänzen: *Die Schüler:innen können Fakten und Meinungen in Texten unterscheiden und kennen die Gefahren der Informationsweitergabe.*

- **Motivation/Bewusstseinsbildung:** Vertiefung der Analyse von **Angriffsmethoden für Informationsweitergabe** wie **Phishing** und **Whaling** im Hinblick auf die Unterscheidung von Fakten und Meinungen in Texten.

5.5.1.2 Zusammenfassende Analyse

Der Lehrplan für die BHS, insbesondere der Gegenstand „Angewandte Informatik“ in Verbindung mit anderen relevanten Fächern, deckt grundlegende Aspekte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells ab. Er vermittelt grundlegende Kompetenzen im Umgang mit digitalen Systemen, adressiert rechtliche Rahmenbedingungen und Datensicherheit explizit und fördert das Bewusstsein für die gesellschaftlichen Auswirkungen von Informationstechnologien.

Übergeordnete Bildungsziele und Fächer wie „Deutsch“, „Englisch“ und die verbindliche Übung „Soziale und Personale Kompetenz“ tragen zusätzlich zur notwendigen kritischen Medienkompetenz und Verhaltenssicherheit bei. Während die Basis gelegt wird, scheinen spezifischere technische Details oder konkrete Bedrohungsszenarien in den vorliegenden Lehrstoffbeschreibungen des Faches „Angewandte Informatik“ weniger im Vordergrund zu stehen.

Allgemeine Berücksichtigung von Stufe 1 und 2 im BHS-Lehrplan (fächerübergreifend):

- **Stufe 1 (Allgemeine Einführung & Motivation):** Diese Stufe zielt auf Bewusstseinsbildung für Bedrohungen, Grundbegriffe und das richtige Verhalten im Umgang mit Daten ab. Der BHS-Lehrplan fördert dies indirekt durch die Entwicklung **sozialer und personaler Kompetenzen** in einer verbindlichen Übung, die Themen wie Umgang mit Informationen und Reflexion des eigenen Verhaltens beinhaltet. Fächer wie „Deutsch“ und „Englisch“ fördern die **kritische Auseinandersetzung mit Medien** und die bewusste Medienauswahl, was relevant ist, um Bedrohungen (z.B. Social Engineering) zu erkennen. Das Fach „Kommunikation und Präsentationstechnik“ behandelt Grundlagen der Kommunikation und Wahrnehmung, die ebenfalls zum Verständnis von manipulationsbasierten Angriffen beitragen können. Rechtliche Grundlagen, die teilweise Stufe 1 zugeordnet werden könnten, werden ebenfalls im Lehrplan behandelt.
- **Stufe 2 („Exploratory“):** Diese Stufe vertieft Awareness für persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen. **Rechtliche Rahmenbedingungen und Normen** sind expliziter Bestandteil des Faches „Wirtschaft und Recht“, wo das Verständnis des **E-Commerce-Gesetzes und Urheberrechts** gefordert wird, und auch im Gegenstand „Angewandte Informatik“ genannt werden. Die Förderung der **persönlichen Sicherheit** wird durch das übergeordnete Bildungsziel, zur

Bewältigung von Alltags- und Berufsleben zu befähigen, sowie durch die Kompetenzen im Umgang mit Daten in verschiedenen Fächern unterstützt.

Berücksichtigung von Stufe 1 und 2 speziell im Gegenstand „Angewandte Informatik“:

Der Lehrplan für den Pflichtgegenstand **"Angewandte Informatik"** enthält spezifische Punkte, die direkt auf Inhalte der Stufen 1 und 2 bezogen sind:

- Im Bildungs- und Lehraufgaben-Bereich „Informatiksysteme, Mensch und Gesellschaft“ wird explizit gefordert, dass Absolvent:innen **„gesetzliche Rahmenbedingungen und Datensicherheit berücksichtigen“** können. Später im Lehrstoff-Bereich werden die **Grundsätze des Datenschutz- und Telekommunikationsgesetzes**, die **Bedeutung des Urheberrechts** und das **Copyright** als Lehrinhalte genannt. Dies sind direkte Anknüpfungspunkte für die rechtlichen Aspekte der Stufen 1 und 2.
- Ebenfalls im Bereich "Informatiksysteme, Mensch und Gesellschaft“ sollen die Schüler:innen die **„gesellschaftlichen Auswirkungen von Informationstechnologien erkennen und zu aktuellen IT-Themen kritisch Stellung nehmen“**. Der Lehrstoff führt hier „gesellschaftliche Auswirkungen der Informationstechnologie“ und „Suchtverhalten“ an. Dies unterstützt die Bewusstseinsbildung und das kritische Denken über die digitale Welt, was ein Ziel der Stufe 1 ist.
- Die Bildungs- und Lehraufgabe fordert auch, dass Daten **„vor Beschädigung und unberechtigtem Zugriff“** geschützt werden müssen. Dies adressiert direkt Aspekte der **Datensicherheit** und der persönlichen Sicherheit im digitalen Raum, die relevant für die Stufen 1 und 2 sind.
- Der Lehrplan legt eine technische Grundlage durch die Behandlung von **Betriebssystemen, Netzwerken**, **Internetnutzung** und dem Umgang mit **Datenbanken** sowie **Algorithmen und Programmierung**. Dieses technische Verständnis ist eine notwendige Voraussetzung, um die Konzepte der Cybersecurity-Stufen 1 und 2 in einem technischen Kontext zu verstehen.

Aspekte, die im Lehrplan „Angewandte Informatik“ weniger explizit erscheinen (basierend auf den vorliegenden Lehrstoffbeschreibungen):

- Während allgemeine Datensicherheit und rechtliche Grundlagen genannt werden, scheinen **konkrete Bedrohungsszenarien** (wie detaillierte Beispiele für Malware oder Social Engineering-Angriffe, die in Stufe 1 genannt werden) oder **technische Grundlagen der Verschlüsselung und Hashfunktionen** (die in Stufe 2 erwähnt werden) in den *expliziten Lehrstoffbeschreibungen* des Faches „Angewandte Informatik“ **nicht direkt aufgeführt** zu sein. Diese Themen könnten jedoch implizit im Unterricht behandelt werden oder sind in anderen Fächern verankert.

5.5.2 Technologien und angewandte Informatik

Der Gegenstand „Technologie und angewandte Informatik“ wird ausschließlich im Lehrplan „Art und Design“ verwendet. Um die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells explizit in den Lehrplan der Höheren Lehranstalt für Art and Design (1.1 Art und Design NOR40237786.pdf) zu integrieren, wird folgende Aufschlüsselung nach Jahrgang und Semester vorgeschlagen. Der sinnvollste Ort für die primäre Integration ist der Pflichtgegenstand „**Technologien und angewandte Informatik**“, da dieser sich bereits mit technologischen Grundlagen und Datenverarbeitung beschäftigt. Andere Gegenstände können optional Inhalte intensivieren.

5.5.2.1 Lehrplanergänzung:

1. Jahrgang - 1. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Technologisches Grundverständnis:** Explizite Behandlung der **Grundlagen von Hardwarekomponenten** (z.B. Computer, Peripheriegeräte, mobile Endgeräte) und **Softwarekategorien** (Betriebssysteme, Anwendungssoftware). Einführung der Begriffe Daten und Informationen und deren Bedeutung.
- **Das richtige Verhalten im Umgang mit Daten:** Einführung grundlegender Prinzipien des sicheren Umgangs mit (vor allem personenbezogenen) Daten. Sensibilisierung für **Passwortsicherheit** (Erstellung sicherer Passwörter, Umgang mit Passwörtern) und den Schutz persönlicher Informationen im digitalen Raum.

1. Jahrgang - 2. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Das richtige Verhalten im Umgang mit Daten (Fortsetzung):** Thematisierung der Gefahren durch unachtsame Datennutzung (z.B. Weitergabe persönlicher Daten). Einführung in **Grundlagen des Datenschutzes** (ohne rechtliche Tiefe, eher Sensibilisierung).
- **Das Erkennen von Risiken und Reaktionsgrundsätze (erste Schritte):** Erste Sensibilisierung für **grundlegende digitale Risiken** wie **Schadsoftware** (Viren, Trojaner – ohne technische Details) und **verdächtige E-Mails**. Einfache **Reaktionsgrundsätze** bei solchen Verdachtsfällen (z.B. nicht auf Links klicken, Meldung an Lehrkraft).

2. Jahrgang - 3. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen – Technologisches Grundverständnis (Vertiefung):** Explizitere Behandlung von **Netzwerk Grundlagen (z.B. einfaches Heimnetzwerk, WLAN)** und deren Funktionsweise. Einführung in die **Grundlagen von Betriebssystemen und Dateimanagement** unter dem Aspekt der Datensicherheit (z.B. Organisation von Dateien, Backup-Grundlagen).
- **Motivation zur Sicherheit:** Einführung von **Fallbeispielen** (vereinfacht) zu Datenverlust, Identitätsdiebstahl und den Auswirkungen von Cyberangriffen zur Bewusstseinsbildung.

2. Jahrgang - 4. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen –** Einführende **Angriffsvektoren** (Grundlagen): Einführung in grundlegende Gefahren im Umgang mit dem Internet wie Phishing (Erkennen von betrügerischen Nachrichten) und gefährliche Webseiten.

Pflichtfach „Design und Kommunikation“ (optional):

- Thematisierung von **sicherem Verhalten in sozialen Medien** (z.B. Privatsphäre-Einstellungen, Umgang mit persönlichen Informationen).

3. Jahrgang - 5. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen – Einführende Angriffsvektoren (Vertiefung):** Detailliertere Behandlung von **Schadsoftware (verschiedene Arten, grundlegende Funktionsweisen)** und **deren Verbreitungswege**. Einführung in **Grundlagen der WLAN-Sicherheit (z.B. sichere Passwörter für WLAN)**.
- **Gute Hacker – Böse Cracker?; Ethical Hacking (Grundlagen):** Einführung des **Konzepts von Ethical Hacking** und dessen Bedeutung für die IT-Sicherheit (ohne praktische Übungen, nur als theoretische Einführung).

3. Jahrgang - 6. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen – Grundlegende technische Umsetzungsstrategien (erste Schritte):** Einführung in die Bedeutung von **regelmäßigen Software-Updates** für die Sicherheit. Erste, einfache Konzepte der **Verschlüsselung (z.B. Wozu dient Verschlüsselung?)**.

Pflichtfach „Design und Kommunikation“ (optional):

- Vertiefung von **Social Engineering (Erkennen manipulativer Taktiken)** im Kontext von Online-Kommunikation.

4. Jahrgang - 7. Semester:

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen – Grundlegende technische Umsetzungsstrategien (Vertiefung):** Detailliertere Behandlung von **Sicherheitsmanagement im Alltag** (z.B. Umgang mit USB-Sticks, öffentliche WLANs). Einführung in **grundlegende Backup-Strategien und deren Bedeutung**.
- **Basiswissen – Identitätsdiebstahl:** Vertiefende Auseinandersetzung mit dem Thema Identitätsdiebstahl (Methoden, Folgen, Schutzmaßnahmen).

4. Jahrgang - 8. Semester (Integration in Technologien und angewandte Informatik):

Pflichtfach „Technologien und angewandte Informatik“:

- **Basiswissen – Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien** (im Überblick): Zusammenfassende Betrachtung der bisher behandelten **Bedrohungen und Angriffsvektoren**. Einführung in **mögliche Auswirkungen von Cyberangriffen** auf Einzelpersonen und Organisationen (ohne detaillierte Eskalationsszenarien).

5. Jahrgang - 9. und 10. Semester

Pflichtfach „Technologien und angewandte Informatik“:

- **Wiederholung und Vertiefung aller Inhalte der Stufen 1 und 2** im Kontext der **beruflichen Anwendung** (z.B. Sicherheit bei der Zusammenarbeit an Projekten, Schutz von Kundendaten, sichere Präsentation von Projekten online).

Pflichtfach „Wirtschaft und Recht“ (optional):

- Kurze Einführung in **grundlegende rechtliche Aspekte der Datensicherheit und des Datenschutzes im beruflichen Umfeld**.

- **Reflexion über die Bedeutung von Cybersecurity** in der Designbranche und die Notwendigkeit, sich kontinuierlich weiterzubilden.

Bei der Umsetzung der Cybersecurity Inhalte sollte der Fokus auf der Sensibilisierung und der Vermittlung grundlegender Verhaltensweisen und Basiswissens liegen, ohne in tiefgreifende technische Details einzutauchen, die über den Rahmen des Pflichtgegenstands "Technologien und angewandte Informatik" hinausgehen.

Es wäre auch wichtig, dass die **Sicherheitsunterweisung und Einschulung** im Labor- und Werkstättenbetrieb auch **Aspekte der IT-Sicherheit** umfassen, wo relevant (z.B. sicherer Umgang mit schuleigenen Netzwerken und Geräten). Durch diese schrittweise und explizite Integration der Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells über alle Jahrgänge hinweg kann ein grundlegendes Bewusstsein und Basiswissen im Bereich Cybersecurity bei den Schüler:innen der Höheren Lehranstalt für Art and Design aufgebaut werden.

5.5.2.2 Zusammenfassende Analyse

Die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells zum Thema Cybersecurity sind im Lehrplan der Höheren Lehranstalt für **Art and Design** nicht als eigenständiger, zusammenhängender Bereich verankert. Jedoch lassen sich in verschiedenen Pflichtgegenständen und Kompetenzmodulen implizite Berührungspunkte und allgemeine Grundlagen erkennen, die in einem weiteren Sinne mit den Themen von Stufe 1 (Grundlagen und Verhalten) und Stufe 2 (Basiswissen) in Verbindung gebracht werden können.

Detailliertere Betrachtung:

Ein grundlegendes technologisches Verständnis wird primär im Pflichtgegenstand „**Technologien und angewandte Informatik**“ in allen Jahrgängen vermittelt.

- **Technologisches Grundverständnis:** Es werden berufsspezifische Hard- und Software behandelt, was eine Basis für das Verständnis digitaler Umgebungen schaffen kann. Allerdings liegt der Fokus hier stärker auf der Anwendung spezifischer Software und Hardware im gestalterischen Kontext (z.B. 3D-Konstruktionssoftware, Software für Bildbearbeitung, Layout und Präsentation, CAD) als auf einem allgemeinen IT-Sicherheitsbewusstsein.

- **Das richtige Verhalten im Umgang mit Daten:** Aspekte des Umgangs mit Daten können implizit in den Lernzielen des Bereichs „Technologien und angewandte Informatik“ enthalten sein, beispielsweise im Hinblick auf Datenerstellung, Datenaustausch und Projektdokumentation. Auch die digitale Bilderfassung und -bearbeitung erfordert einen verantwortungsvollen Umgang mit Dateien. Jedoch wird der Schutz personenbezogener Daten und das richtige Verhalten im Sinne der Datensicherheit (wie in Stufe 1 des CLEMENTINE-6-Stufen-Modells gefordert) **nicht explizit thematisiert.**
- **Das Erkennen von Risken und Reaktionsgrundsätze:** Das **Erkennen von Risiken** wird im Lehrplan **nicht direkt im Kontext von IT-Sicherheit** behandelt. Es gibt jedoch Hinweise auf **Sicherheitsvorschriften im Umgang mit Werkzeugen und Maschinen** in den Werkstätten, was ein allgemeines Bewusstsein für potenzielle Gefahren schulen kann. Eine Übertragung dieser Konzepte auf digitale Risiken erfolgt jedoch **nicht explizit**. **Reaktionsgrundsätze bei IT-Sicherheitsvorfällen** sind im Lehrplan **nicht vorgesehen**.
- **Motivation zur Sicherheit:** Die **Bewusstseinsbildung für IT-Sicherheit** (wie in Stufe 1 des CLEMENTINE-6-Stufen-Modells durch Fallbeispiele etc. angeregt) **findet im Lehrplan keine explizite Erwähnung**. Der Fokus liegt auf der **künstlerischen und designerischen Ausbildung**.
- **Einführende Angriffsvektoren: Spezifische Angriffsvektoren** wie Schadsoftware, Phishing oder Social Engineering (die in Stufe 2 des CLEMENTINE-6-Stufen-Modells angesprochen werden) **werden im Lehrplan nicht explizit behandelt**. Die Sicherheit im Umgang mit **Internetdiensten** wird im Lehrplan zwar im Bereich „**Technologien und angewandte Informatik**“ erwähnt [siehe vorherige Antwort], jedoch **nicht im Detail und mit Fokus auf aktuelle Bedrohungen**.
- **Grundlegende technische Umsetzungsstrategien: Technische Umsetzungsstrategien zur Erhöhung der Sicherheit** im Alltag (z.B. sichere Passwörter, Update-Management, Datensicherung) oder Konzepte wie **Verschlüsselung** sind **nicht als expliziter Lehrstoff** enthalten. Es gibt keine spezifischen Lernziele, die auf die Vermittlung solcher grundlegenden Sicherheitsmaßnahmen abzielen.

Der Lehrplan vermittelt fundierte Kenntnisse und Fertigkeiten in verschiedenen gestalterischen und technischen Bereichen, die den Umgang mit digitalen Werkzeugen und Technologien einschließen. Dies schafft eine allgemeine technologische Basis, die für ein späteres Verständnis von Cybersecurity relevant sein kann. Die spezifischen Inhalte und Lernziele der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells, die sich mit Nutzer:innenverhalten, konkreten Bedrohungen im digitalen Raum und grundlegenden präventiven Sicherheitsmaßnahmen auseinandersetzen, sind jedoch nicht systematisch und detailliert im Lehrplan integriert. Die vorhandenen Berührungspunkte sind eher implizit und im Kontext der Anwendung spezifischer Software oder der allgemeinen Bedienung von Technologien zu sehen.

Empfehlung:

Im Sinne der Sichtbarmachung von Cybersecurity wäre hier eine Teilung des Faches „Technologie und angewandte Informatik“ in „Angewandte Informatik“ (für die digitalen Grundlagen) und „Angewandte Technologie“ (für die fachspezifischen Anwendungen) empfohlen. Eine Angleichung an den in Anlage 1 geregelten Gegenstand „Angewandte Informatik“ wäre wünschenswert und würde zu einer Standardisierung der Inhalte führen.

5.5.3 Medizin- und Gesundheitsinformatik

Der Gegenstand „Medizin- und Gesundheitsinformatik“ wird in folgenden Lehrplänen verwendet:

- Biomedizin und Gesundheitstechnik
- Technik in Medizin, Life Science und Sport

Die beiden Lehrpläne unterscheiden sich im Stundenumfang, in inhaltlichen Schwerpunkten und durch ihr fachliches Umfeld und Vertiefungen.

Beide Lehrpläne beinhalten im Gegenstand „Medizin- und Gesundheitsinformatik“ allgemeine berufsbezogene Lernergebnisse, die Aspekte der Datensicherheit auf Stufe 1 und 2 des CLEMENTINE-6-Stufen-Modells abdecken. Konkret wird in beiden Lehrplänen aufgeführt, dass die Absolvent:innen im Bereich **Datensicherheit** die grundsätzlichen Eigenschaften von Datenschutzbestimmungen kennen, Sicherheitsrisiken erkennen, rechtliche Bestimmungen für den Umgang mit sensiblen Daten umsetzen und Sicherheitsrisiken bewerten können. Diese Kompetenzen entsprechen dem Erkennen von Risiken, dem verantwortungsvollen Umgang mit Daten (insbesondere personenbezogenen Daten) und dem Wissen um rechtliche Rahmenbedingungen (Datenschutz), was Kerninhalte der Stufen 1 und 2 sind.

5.5.3.1 Lehrplanergänzung

Die folgenden Vorschläge beschränken sich auf die Implementierung der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells. Diese werden die beide Lehrpläne eingefügt, wobei der Fokus zunächst auf dem Aufbau eines grundlegenden Verständnisses und sicheren Verhaltens liegt, bevor später spezifischere rechtliche und technische Aspekte behandelt werden. Es ist wichtig, diese Inhalte nicht isoliert zu betrachten, sondern sie in den jeweiligen Fachunterricht zu integrieren und durch Beispiele und Fallstudien aus dem Bereich der Biomedizin- und Gesundheitstechnik zu veranschaulichen.

1. Jahrgang - 1. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- **Grundverständnis der Cybersecurity aus der Sekundarstufe I wiederholen und festigen** werden. Dies beinhaltet: Technologisches Grundverständnis. Das richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten. Das Erkennen von Risiken und Reaktionsgrundsätze.
- Ebenfalls in **Medizin- und Gesundheitsinformatik** sollte die **Motivation zur Sicherheit** thematisiert werden: Bewusstseinsbildung durch Fallbeispiele (z.B. Keylogger-Video). Grundlagen von Schadsoftware. Unterscheidung zwischen „guten“ und „bösen" Hackern (Ethical Hacking). Die Gefahr von Identitätsdiebstahl. Grundlegende Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien mit Fokus auf den Schutz personenbezogener Daten. Einführung in Social Engineering.

1. Jahrgang - 2. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- Vertiefung des **richtigen Verhaltens im digitalen Raum**: Erkennen von Gefahren im Internet. Sichere Passwortwahl und -verwaltung. Sicheres Surfen im Internet. Sicherer Umgang mit sozialen Medien. Erkennung von Phishing-E-Mails und gefährlichen E-Mail-Anhängen. Umgang mit infizierten Datenträgern. Keine Installation verdächtiger Software. Sichere Entsorgung alter Geräte. Sicheres Verhalten auf Reisen (z.B. in öffentlichen WLANs).
- Erste Einführung in **Angriffsmethoden zur Informationsweitergabe** in **Medizin- und Gesundheitsinformatik**: Grundlagen von Phishing, Whaling und Gophish (ohne detaillierte technische Analyse).

2. Jahrgang - 3. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- Einführung in grundlegende Konzepte von **Vertraulichkeit und Integrität**: Wie funktioniert Verschlüsselung konzeptionell (ohne technische Tiefe)? Wie funktioniert eine Hashfunktion konzeptionell (ohne technische Tiefe)?
- **Wirtschaft und Recht:** Erste Behandlung **rechtlicher Rahmenbedingungen und Normen** im Kontext von IT-Sicherheit und Datenschutz: Grundlagen der Datenschutz-Grundverordnung (DSGVO) im Hinblick auf personenbezogene Daten im Gesundheitswesen.

2. Jahrgang - 4. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- Thematisierung der **Verfügbarkeit von Daten und Systemen**: Die Bedeutung von Datensicherungen (Backups). Verschiedene Arten von Backup-Medien. Einführung in Cloud-Backups. Die Bedrohung durch Ransomware und grundlegende Schutzmaßnahmen.
- **Wirtschaft und Recht:** Vertiefung der **rechtlichen Rahmenbedingungen und Normen**: Grundlagen des Urheberrechts im digitalen Kontext. Grundlagen der Domainregistrierung. Überblick über relevante Gesetze wie das Telekommunikationsgesetz und das IT-Sicherheitsgesetz (in vereinfachter Form).

3. Jahrgang - 5. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- Wiederholung und Vertiefung der Inhalte aus Stufe 1 und 2 im Hinblick auf spezifische Anwendungen im Gesundheitswesen.

Pflichtfach „Wirtschaft und Recht“:

- Einführung in IT-Grundschutz und Normen wie ISO 27001 (grundlegende Konzepte und Bedeutung).

3. Jahrgang - 6. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- Behandlung der Frage "**Was tun im Notfall?**": Richtig reagieren bei Sicherheitsvorfällen. Kenntnis wichtiger Ansprechpartner (innerhalb der Schule/Organisation). Initiierung von Maßnahmen zur Infektionsbeseitigung (grundlegende Schritte).

4. Jahrgang - 7. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- **Datensicherheit und Datenschutz:** Hier sollten die rechtlichen Rahmenbedingungen (DSGVO etc.) detailliert behandelt und in Bezug zur technischen Umsetzung von Sicherheitsmaßnahmen gesetzt werden. Die Inhalte aus Stufe 2 bilden hier eine wichtige Grundlage.

4. Jahrgang - 8. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- **Datensicherheit und Datenschutz:** Vertiefung der technischen Aspekte von Vertraulichkeit, Integrität und Verfügbarkeit unter Berücksichtigung der rechtlichen Vorgaben.

5. Jahrgang - 9. und 10. Semester:

Pflichtfach „Medizin- und Gesundheitsinformatik“:

- In den höheren Semestern sollten die Grundlagen der Cybersecurity aus Stufe 1 und 2 in den verschiedenen fachspezifischen Gegenständen immer wieder kontextbezogen aufgegriffen und angewendet werden, um das Bewusstsein für Sicherheit in allen Bereichen der Biomedizin- und Gesundheitstechnik zu schärfen.

5.5.3.2 Zusammenfassende Analyse

Lehrplan Biomedizin- und Gesundheitstechnik: Die allgemeinen Cybersecurity-Kompetenzen der Stufen 1 und 2 sind im Standard-Lehrplan (B.6) derzeit in den frühen Jahren (1.-3. Lehrgang) nicht explizit ausgewiesen. Der Lehrstoff der Stufen 1 und 2 müsste in den 1. und 2. Jahrgang des Pflichtgegenstandes „Medizin- und Gesundheitsinformatik“ (B.6) integriert werden, und gleichermaßen im alternativen Schwerpunkt (1.6), da hier die Informatik-Grundlagen gelegt werden, was der Beschreibung der Anwendungsbereiche der Stufen 1 und 2 entspricht. Die im 4. und 5. Jahrgang vorhandenen Security-Themen scheinen über die allgemeine Einführung hinaus zu gehen und wären eher Stufen 3+.

Lehrplan Technik in Medizin, Life Science und Sport: Die allgemeinen Cybersecurity-Kompetenzen der Stufen 1 und 2 sind im Standard-Lehrplan (B.5) derzeit in den frühen Jahren (1. - 4. Lehrgang) nicht explizit ausgewiesen. Der Lehrstoff der Stufen 1 und 2 müsste in den 1. und 2. Jahrgang des Pflichtgegenstandes „Medizin- und Gesundheitsinformatik“ (B.5) integriert werden, da hier die Informatik-Grundlagen gelegt werden, was der Beschreibung der Anwendungsbereiche der Stufen 1 und 2 entspricht. Die im 5. Jahrgang vorhandenen Security-Themen scheinen über die allgemeine Einführung hinaus zu gehen und wären eher Stufen 3+.

In beiden Lehrplänen ist die Integration der allgemeinen, einführenden Cybersecurity-Inhalte der Stufen 1 und 2 am sinnvollsten in den ersten beiden Jahren (1. und 2. Jahrgang) des Pflichtgegenstandes „Medizin- und Gesundheitsinformatik“ (B.6 in Source 1, B.5 in Source 2), da hier die informatischen Grundlagen vermittelt werden, auf denen später aufbauende, fachrichtungsspezifische Sicherheitsthemen (wie sie bereits teilweise in höheren Jahrgängen vorhanden sind) aufbauen können. Der genaue Inhalt der Stufen 1 und 2 müsste allerdings aus der Definition dieser Stufen im CLEMENTINE-6-Stufen-Modell selbst entnommen werden, die in den beiden Lehrplänen fehlt.

5.5.4 Fachspezifische Softwaretechnik

Der Gegenstand „Fachspezifische Softwaretechnik“ wird ausschließlich im Lehrplan „**Elektronik und Technische Informatik**“ verwendet.

Der Lehrplan für Elektronik und Technische Informatik legt den Schwerpunkt auf die Vermittlung technischer Kompetenzen in diesen Fachbereichen. Die grundlegenden Awareness- und Verhaltensaspekte der Cybersecurity, die in den ersten beiden Stufen des CLEMENTINE-6-Stufen-Modells behandelt werden, sind jedoch nicht integriert.

Der Lehrplan enthält derzeit Cybersecurity-Themen hauptsächlich im 10. Semester des 5. Jahrgangs im Fach Fachspezifische Softwaretechnik.

Um die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells explizit in den vorliegenden Lehrplan zu integrieren, basierend auf der Struktur und den Themen der bestehenden Gegenstände, könnte eine Aufschlüsselung wie folgt vorgeschlagen werden.

5.5.4.1 Lehrplanergänzungen

Die Stufen 1 und 2 sollten idealerweise in den früheren Jahren des Lehrplans integriert werden, da sie grundlegende und allgemeine Kenntnisse sowie Verhaltensweisen für alle Schüler:innen der Sekundarstufe II darstellen.

1. Jahrgang - 1. und 2. Semester:

In diesem Jahrgang werden Grundlagen in Fächern wie Hardwareentwicklung, Fachspezifische Softwaretechnik (Fachrichtungsspezifische Software, Programmiersprachen, Hardwarenahe Programmentwicklung) sowie Digitale Systeme und Computersysteme (im Laboratorium und Prototypenbau) gelegt. Hier könnten grundlegende Konzepte und Bewusstseinsbildung aus Stufe 1 integriert werden.

Pflichtfach „Fachspezifische Softwaretechnik“:

- **Stufe 1.1 Motivation zur Sicherheit (Auszüge):** Bewusstseinsbildung für Risiken im Umgang mit Software und Daten, grundlegendes Verständnis von Schadsoftware-Arten (z.B. Virenkonzept auf einfacher Ebene), die Bedeutung von Bedrohungen und deren Auswirkungen auf den Einzelnen.
- **Stufe 1.2 Grundbegriffe (Auszüge):** Einführung einfacher Begriffe wie Malware, Phishing (erkennen auf sehr einfacher Ebene).
- **Stufe 1.3 Über den Umgang mit Daten im Internet (Auszüge):** Grundlegendes Verständnis von Datenspuren, sicheres Verwalten und Weitergeben von Daten (Konzept der Sorgfalt), sicheres Löschen (Konzept).
- **Stufe 1.4 Sicherheitsempfehlungen (Auszüge):** Einfache Verhaltensrichtlinien (z.B. Bildschirmsperre, verantwortungsvoller Umgang mit Geräten), Bedeutung einfacher Kennwörter und deren Schutz.
- **Stufe 1.5 Bedrohungsszenarien (Auszüge):** Was tun im Notfall (grundlegende Reaktionsprinzipien, Ansprechpartner:innen kennen - allgemein).

2. Jahrgang - 3. und 4. Semester:

In diesem Jahrgang vertiefen sich die Grundlagen. Fachspezifische Softwaretechnik behandelt nun auch Web- und Netzwerkprogrammierung auf einfacher Ebene, Kommunikationssysteme und -netze werden im Laboratorium und Prototypenbau eingeführt. Dies bietet Ansatzpunkte für Stufe 1 und beginnende Stufe 2 Inhalte.

Pflichtfach „Fachspezifische Softwaretechnik“:

- **Stufe 1.3 Über den Umgang mit Daten im Internet (Vertiefung):** Analyse einfacher Mail-Header/URLs zum Erkennen von Spam/Phishing. Sicheres Verwalten/Weitergeben (z.B. Cloudspeicher grundlegend sicher nutzen). Das eigene Gerät sichern (einfache Maßnahmen).
- **Stufe 1.4 Sicherheitsempfehlungen (Vertiefung):** Bedeutung von Updates und Patches auf Anwenderebene. Verhalten in öffentlichen Netzen/WLANs (Grundregeln). Bedeutung komplexerer Kennwörter.

Pflichtfach Kommunikationssysteme und -netze (eventuell integriert in Labor/Prototypenbau):

- **Stufe 1.1 Motivation zur Sicherheit (Auszüge):** Ethical Hacking (Konzept: guter vs. böser Hacker).

- **Stufe 1.5 Bedrohungsszenarien (Auszüge):** Angriffsmethoden für Informationsweitergabe (z.B. Phishing vertiefen).

3. Jahrgang - 5. und 6. Semester:

Hier beginnen die Schüler:innen mit komplexeren Systemen und Softwarekonzepten (z.B. Objektorientierung, Betriebssysteme) sowie Netzwerken zu arbeiten. Stufe 2, die tiefergehende Awareness und erste technische Konzepte umfasst, adressiert das.

Pflichtfach „Fachspezifische Softwaretechnik“:

- **Stufe 2.1 Vertraulichkeit und Integrität:** Wie funktioniert Verschlüsselung und Hashfunktion (ohne technische Implementierungstiefe).
- **Stufe 2.2 Über den Umgang mit Daten II:** Backup-Konzepte und Datenwiederherstellung (allgemein), Konzepte der Datenträgerverschlüsselung, sicheres Entsorgen von Datenträgern, Virenscanner (Funktionsprinzip und Einsatz).
- **Stufe 2.4 Digitale Bürgerkarte:** Was ist eine Signatur (Konzept), digitale Signaturen überprüfen (Anwendung), elektronische Signaturen (Handysignatur - Prinzip).
- **Stufe 2.6 Rechtsgrundlagen:** Grundlegende rechtliche Gegebenheiten in Österreich und Europa (Überblick über relevante Aspekte von IT-Recht/DSGVO im Kontext der Softwareentwicklung und Datenverarbeitung).

Pflichtfach „Kommunikationssysteme und -netze“:

- **Stufe 2.3 Sichere Kommunikation:** Sichere Verbindungskonzepte (VPN-Prinzip), Persönliche Firewalls (Konzept und Zweck), Sichere Authentifizierungsmethoden (grundlegende Konzepte wie Mehrfaktorauthentifizierung), Verschlüsselte Kommunikationskanäle (HTTPS und Zertifikate - Funktionsweise auf Anwenderebene).
- **Stufe 2.8 Angriffsvektoren (Auszüge):** Ransomware, Botnetze (grundlegende Konzepte), DOS/DDOS (Prinzip).

4. Jahrgang - 7. und 8. Semester:

In diesem Jahrgang werden fortgeschrittenere Themen behandelt, darunter Betriebssysteme, Netzwerke und Softwareentwicklungsmethoden. Stufe 2 kann hier weiter vertieft werden, insbesondere technische Umsetzungsstrategien und detailliertere Angriffsvektoren.

Pflichtfach „Fachspezifische Softwaretechnik“:

- **Stufe 2.7 Technische Umsetzungsstrategien:** Einführung in Sicherheitsmanagement (ISMS-Konzepte), Grundschutz (BSI-Konzept), einfache Netzwerksicherheitstools (Nutzung), Anonymisierungsdienste (Prinzip und Zweck), Logfiles (grundlegende Bedeutung für Sicherheit), Sandboxing/Virtuelle Maschinen (Sicherheitsaspekte).
- **Stufe 2.8 Angriffsvektoren (Vertiefung):** Mobiltelefon als Angriffsziel, Vertrauen in Apps (grundlegende Prüfung), Cybercrime (Überblick über aktuelle Bedrohungen), Reconnaissance (Konzept der Informationsbeschaffung für Angriffe).

Pflichtfach „Kommunikationssysteme und -netze:“

- **Stufe 2.3 Sichere Kommunikation (Vertiefung):** Detailliertere Betrachtung sicherer Authentifizierungsmethoden (NIST Richtlinien, Password Safes).

Pflichtfach „Digitale Systeme und Computersysteme“:

- **Stufe 2.5 Smart Devices:** Sicherheitsaspekte spezifischer Devices, Einführung in spezifische Suchmaschinen (z.B. Shodan - Zweck verstehen).

5. Jahrgang - 9. und 10. Semester:

Der vorliegende Lehrplan enthält bereits explizite Inhalte zu Datensicherheit und Security im 10. Semester der Fachspezifischen Softwaretechnik. Diese vorhandenen Inhalte decken bereits Aspekte ab, die im CLEMENTINE-6-Stufen-Modell Stufe 3 zu finden sind (z.B. Datensicherheit, Authentifizierungsverfahren und

Security im Kontext von Web- und Netzwerkprogrammierung passen zu Geräte-, Anwendungs- und Netzwerksicherheit).

Diese vorhandenen Inhalte **entsprechen teilweise den Kompetenzstufen 3 und 4** des CLEMENTINE-6-Stufen-Modells, welche für BHS mit IT/Informatik-Schwerpunkt vorgesehen sind. Stufe 1 und 2 sollten, wie oben vorgeschlagen, bereits in früheren Jahren abgedeckt sein, um eine breitere Grundlage zu schaffen. Im 5. Jahrgang könnten sie ggf. kurz wiederholt oder vertieft werden, bevor die spezialisierten Stufe 3/4-ähnlichen Themen behandelt werden.

5.5.4.2 Zusammenfassende Analyse

Obwohl keine verpflichtende digitale Grundbildung vorgesehen ist, umfasst der Lehrplan spezifische Inhalte wie Programmierung (Algorithmen, Objektorientierung), Datenbanken und Datensicherheit – allerdings mit stark fachbezogener Ausrichtung. Allgemeine digitale Kompetenzen, etwa der Umgang mit Bürosoftware, die Nutzung des Internets für Publikation und Kommunikation oder grundlegende Aspekte von Informatiksystemen und deren gesellschaftliche Auswirkungen, sind nicht explizit enthalten. Dennoch werden sie in verschiedenen Unterrichtsfächern implizit behandelt.

Zusammenfassend lässt sich sagen, dass die Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells eine breitere und frühere Einführung von Cybersecurity-Themen in den Lehrplan „Elektronik und Technische Informatik“ nahelegen, als es der vorliegende Lehrplan derzeit explizit vorsieht.

Empfehlung

Angesichts der Anforderungen des modernen Berufsalltags wäre es sinnvoll, einen klar erkennbaren Ausbildungspfad für digitale Grundbildung anzubieten, wie es im Gegenstand „Angewandte Informatik“ in Anhang 1 vorgesehen ist. Digitale Kompetenzen sind nicht nur im technischen Bereich essenziell, sondern auch in Verwaltung, Wissenschaft und vielen anderen Branchen. Der digitale Wandel erfordert zunehmend eine fundierte Auseinandersetzung mit diesen Themen, um den Herausforderungen der Zukunft gewachsen zu sein.

5.5.5 Fachspezifische Informationstechnik

Der Gegenstand „Fachspezifische Informationstechnik“ wird ausschließlich im Lehrplan „Elektrotechnik“ verwendet.

Es ist ersichtlich, dass im Bereich „Angewandte Informatik“ des Faches „Fachspezifische Informationstechnik“ und später insbesondere im Rahmen der schulautonomen Vertiefungen "Smart Systems" und „Netzwerktechnik“ grundlegende und fortgeschrittenere informationstechnische Aspekte behandelt werden, die Berührungspunkte mit der Cybersecurity aufweisen. Dazu gehören Netzwerkeinstellungen, Datensicherung, Datenbankgrundlagen und später spezifische Netzwerk- und Sicherheitsthemen. Allerdings fehlen in den ersten beiden Jahrgängen explizite und umfassende Lehrinhalte, die direkt auf die in Stufe 1 und 2 des CLEMENTINE-6-Stufen-Modells für Cybersecurity-Awareness genannten Punkte abzielen, wie beispielsweise spezifische Bedrohungsszenarien, Social Engineering oder detaillierte Sicherheitsempfehlungen für Endnutzer:innen.

5.5.5.1 Lehrplanergänzungen

Die Integration der ergänzenden Cybersecurity Inhalte sollte kontextbezogen zu den jeweiligen Fächern und Semestern erfolgen und die Komplexität der Themen im Laufe der Zeit allmählich steigern. Es ist wichtig, dass die Lerninhalte praxisnah vermittelt werden und den Schüler:innen die Relevanz von Cybersecurity für ihren zukünftigen Beruf verdeutlicht wird. Die Pflichtfächer „**Fachspezifische Informationstechnik“** und „**Computergestützte Projektentwicklung“** scheinen besonders geeignet für die Integration dieser grundlegenden Konzepte zu sein, da sie bereits informationstechnische Aspekte beinhalten oder eine breite Basis für das Verständnis digitaler Technologien bieten.

1. Jahrgang - 1. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Grundlagen der Cybersecurity:** Einführung in das Thema, Bedeutung im digitalen Alltag.
- **Technologisches Grundverständnis:** einfache Erklärungen von Internet, Daten, Geräten, Netzwerken.
- **Umgang mit Daten:** Sensibilisierung für den richtigen Umgang mit personenbezogenen Daten.

- **Passwortsicherheit:** Bedeutung sicherer Passwörter, grundlegende Regeln.

1. Jahrgang - 2. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Vertiefung Passwortsicherheit:** sichere Passwortwahl und -verwaltung in der Praxis.
- **Sicheres Surfen:** grundlegende Verhaltensregeln.
- **E-Mail-Sicherheit:** Erkennen von Phishing-E-Mails und gefährlichen Anhängen - anhand von Beispielen.
- **Schadsoftware**: Grundlagen und mögliche Auswirkungen,
- **Verhalten bei Infektionen**: grundlegende Reaktionsgrundsätze.
- **Datensicherung** (Wiederholung und Motivation): Wiederholung der Backup-Grundlagen im Kontext von Cyberbedrohungen wie Ransomware.

2. Jahrgang - 3. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Social Engineering** Einführung in Grundlagen und typische Angriffe,
- **Identitätsdiebstahl:** Gefahr und grundlegende Schutzmaßnahmen,
- **Vertraulichkeit**: Einführung in das Konzept der Datenvertraulichkeit,
- **Integrität:** Einführung in das Konzept der Datenintegrität.

2. Jahrgang - 4. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Sicherer Umgang mit Datenträgern**: Vermeidung der Verbreitung von Schadsoftware.
- **Sichere Softwarenutzung**: keine Installation verdächtiger Software.
- **Sichere Entsorgung**: Grundlagen der sicheren Entsorgung alter Geräte und Datenträger.
- **Datensicherung und Wiederherstellung (Vertiefung)** Vertiefung verschiedener Backup-Arten und deren Bedeutung für die Datenverfügbarkeit.

3. Jahrgang - 5. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Öffentliche WLANs** (Gefahren und grundlegende Sicherheitsvorkehrungen),
- **Sicheres Verhalten auf Reisen** (besondere Sicherheitsaspekte),
- **Wiederholung und Vertiefung** der Inhalte aus dem 1. und 2. Jahrgang in Hinblick auf die informationstechnischen Aspekte der Elektrotechnik.

3. Jahrgang - 6. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“:

- **Grundlagen der Verschlüsselung (konzeptionell)** einfache Erklärung ohne technische Details,
- **Grundlagen von Hashfunktionen (konzeptionell)** einfache Erklärung ohne technische Details,
- **Rechtliche Grundlagen** (erste Einführung) grundlegende rechtliche Rahmenbedingungen im Kontext von IT-Sicherheit und Datenschutz, z.B. Erwähnung der DSGVO.

4. Jahrgang - 7. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“ oder **Computergestützte Projektentwicklung** (je nach Schwerpunktsetzung)

- **IT-Grundschutz:** Einführung in grundlegende Konzepte.
- **Normen** (erste Einführung)**:** erste Erwähnung von Normen wie ISO 27001 im Kontext der Informationssicherheit.
- **Datenschutz im Detail:** detailliertere Behandlung der DSGVO etc. in Bezug auf Projektentwicklung und Datenumgang.

4. Jahrgang - 8. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“ oder **Computergestützte Projektentwicklung** (je nach Schwerpunktsetzung)

- **Sicherheitsvorfälle**: Behandlung der Frage "Was tun im Notfall?": **Wichtige Ansprechpartner** (Kenntnis wichtiger interner Ansprechpartner bei Sicherheitsvorfällen), **Grundlegende Maßnahmen zur Infektionsbeseitigung** (einfache Schritte zur Einleitung von Maßnahmen).

5. Jahrgang - 9. und 10. Semester:

Pflichtgegenstand „Fachspezifische Informationstechnik“ und **Pflichtfächer mit informationstechnischem Bezug** wie die Vertiefungsfächer „**Smart Systems“**, „**System Connectivity“ und** „**Netzwerktechnik**“:

Lehrstoff kontextbezogen ergänzen:

- **Kontextbezogene Anwendung** der Grundlagen der Cybersecurity aus Stufe 1 und 2 immer wieder in den verschiedenen fachspezifischen Gegenständen, insbesondere in Fächern mit starkem informationstechnischem Bezug.
- **Bewusstseinsbildung** durch Beispiele und Fallstudien.
- **Vertiefung nach Schwerpunkt**: Je nach gewählter schulautonomer Vertiefung können spezifische Cybersecurity-Themen detaillierter behandelt werden, wie bereits im aktuellen Lehrplan in Ansätzen vorhanden, z.B. sichere Datenverbindungen in Netzwerktechnik.

5.5.5.2 Zusammenfassende Analyse

Die explizite Thematisierung von Cybersecurity scheint im Lehrplan eher in späteren Jahrgängen und im Kontext spezifischer Vertiefungen stattzufinden. Die folgende Aufstellung zeigt die aktuellen Übereinstimmungen:

1. Jahrgang: Lehrstoff zur Cybersecurity-Awareness - explizit im Lehrplan enthalten**:**

- Der Lehrplan erwähnt im Bereich "Angewandte Informatik" die "**sicherheitsrelevante Netzwerkeinstellungen**". Dies kann als ein erster Bezugspunkt zu sicherheitsrelevanten Aspekten im Umgang mit Netzwerken interpretiert werden, auch wenn keine detaillierten Cybersecurity-Inhalte genannt werden.
- Ebenfalls im Bereich „Angewandte Informatik“ wird „**Sicherungsprozesse (Backup, Restore, Recovery)**“ explizit als Lehrstoff genannt. Dies ist ein grundlegender Aspekt der Datensicherheit, der in den Bereich der Cybersecurity fällt.
- Im Fach „Werkstätte und Produktionstechnik“ des 1. Jahrgangs wird die Inbetriebnahme „**grundlegender Komponenten der Netzwerktechnik**“ als Bildungs- und Lehraufgabe genannt. Dies impliziert ein technologisches Grundverständnis von Netzwerken, welches eine Basis für spätere Cybersecurity-Betrachtungen sein kann.
- Auch im Fach „Werkstätte und Produktionstechnik“ wird das Herstellen und Prüfen von „**Netzwerkverkabelungen**“ als Kompetenz angeführt. Dies ist eine praktische Auseinandersetzung mit der physischen Ebene von Netzwerken.

2. Jahrgang: Vertiefende Cybersecurity-Awareness - explizit im Lehrplan enthalten:

- Im Bereich „Prozessdatentechnik“ wird die Fähigkeit genannt, die „**Grundlagen von Datenbanken beschreiben**“ zu können. Dies ist relevant, da Datenbanken ein wichtiges Ziel von Cyberangriffen sein können und ein Verständnis ihrer Grundlagen für die Cybersecurity notwendig ist.
- Im Bereich **Prozessdatentechnik** wird die Fähigkeit genannt, „in Datenbanksoftware Tabellen, Abfragen, Formulare und Berichte erstellen und ändern“ zu können. Dies beinhaltet den Umgang mit sensiblen Daten und erfordert ein Bewusstsein für deren Sicherheit.
- Auch im Prozessdatentechnik finde man die „Aufgabenstellungen analysieren und diese für eine Standarddatenbanksoftware aufbereiten“: Dies kann auch sicherheitsrelevante Aspekte bei der Datenmodellierung und -verwaltung umfassen.

Spätere Jahrgänge - teilweise relevant für Stufe 2-ähnliche Inhalte:

- Im 4. Jahrgang wird im Bereich „Steuerungs- und Leittechnik“ gelehrt, „**Bussysteme der Automatisierungstechnik**“ zu **beschreiben**. Dies ist für die Sicherheit von vernetzten Systemen relevant.
- Im Rahmen der schulautonomen Vertiefung „System Connectivity“ wird im 5. Jahrgang gelehrt, „**Bussysteme zu konzipieren und implementieren**“, inklusive Busprotokollen, was sicherheitsrelevante Aspekte beinhalten kann.
- Im 5. Jahrgang wird das Feld „**Netzwerktechnik**“ explizit im Rahmen der schulautonomen Vertiefung behandelt. Hier werden Inhalte wie das Konfigurieren von Netzwerkkomponenten (Switch, Router), Netzwerkdienste (Konfiguration, Sicherheit), Firewalls und **Security in Netzwerken** gelehrt.
- Ebenso werden die Planung, Dokumentation und Verkabelung von Netzwerken sowie **Fehlersuche und Monitoring** behandelt. Auch **Maßnahmen gegen Schadprogramme und unberechtigten Zugriff** werden thematisiert.
- Ebenfalls im 5. Jahrgang werden „**Verteilte Systeme**“ behandelt, inklusive Client-Server-Prinzipien, **Ausfallsicherheit und Verfügbarkeit**, sowie Datenaustausch zwischen Applikationen und Virtualisierung.
- Die „**Prozessdatentechnik**“ wird ebenfalls in späteren Jahrgängen vertieft, inklusive Datenbankprogrammierung (Relationen) und webbasierter Programmierung (dynamische Webseiten, Skriptsprache).
- Im 5. Jahrgang wird im Bereich Netzwerktechnik die Fähigkeit gelehrt, „**sichere Datenverbindungen zu beschreiben und einzurichten**“.

5.5.6 Medientechnologie und angewandte Informatik

Der Gegenstand „Medientechnologie und angewandte Informatik“ wird in Lehrplänen **Medien bzw. Grafik- und Kommunikationsdesign** verwendet**.**

Der Gegenstand „Medientechnologie und angewandte Informatik“ existiert als Pflichtgegenstand sowohl im Medien Lehrplan, mit einer Wochenstundenanzahl von 23 bzw. 20 im Ausbildungsschwerpunkten wie Multimedia, als auch im Lehrplan der Grafik- und Kommunikationsdesign mit 26 Wochenstunden. Im „**Medien“** Lehrplan zielt der Gegenstand darauf ab, technisches Wissen und Anwendungssicherheit in medialen Technologien zu vermitteln, um mediale Produkte und Projekte umzusetzen. Dies beinhaltet die Analyse und Entwicklung komplexer Anwendungen mit Geräten, Systemen und Verfahren des Fachbereichs. Der Lehrstoff deckt Grundlagen von Geräten, Systemen, Verfahren, physikalischen/chemischen Grundlagen, Technologien, Programmen, Strukturen, Prozessen, Workflows, Materialien, Programmierungselementen (Algorithmen, einfache Programme, Objektorientierung), Datenmodellen und Datenbanken ab. Die speziellen Ausbildungsschwerpunkte wie Film, Animation oder Gamedesign ergänzen und spezifizieren diese Inhalte auf ihre jeweiligen Technologien.

Im **Grafik- und Kommunikationsdesign** liegt der Fokus auf der Umsetzung von Entwürfen, Präsentationen, Produktionsvorbereitungen und Produktionen im Bereich Grafik- und Kommunikationsdesign unter Einsatz von Technologien. Der Gegenstand konzentriert sich auf die grundlegenden Werkzeuge der angewandten Informatik sowie der Bild- und Layoutbearbeitung. Der Lehrstoff umfasst Bereiche wie Betriebssysteme in Produktionsumgebungen, Bild- und Layoutbearbeitung, Drucktechnik (inkl. Materialkunde und Sicherheit im Umgang mit gefährlichen Stoffen), Bilderfassung (Kameratechnik, Optik, Lichttechnik) und Aspekte der Typografie im technischen Kontext.

Vergleicht man die beiden Lehrpläne **Medien bzw. Grafik- und Kommunikationsdesign** hinsichtlich der Einführung von Stufe 1 und 2 Cybersecurity in „Medientechnologie und angewandte Informatik“, lässt sich jedoch kein expliziter Unterschied in der Einführung der Cybersecurity-Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells zwischen den beiden Lehrplänen feststellen. Der Lehrstoff dieses spezifischen Gegenstands konzentriert sich in beiden Schultypen stark auf die **technischen Grundlagen und praktischen Anwendungen**, die für die jeweilige Medienausrichtung relevant sind. Obwohl das CLEMENTINE-6-Stufen-Modell vorsieht, dass die allgemeinen Kompetenzstufen 1 und 2 in **allen BHS-Typen** in Fächern wie „Angewandte Informatik“ vermittelt werden sollen, zeigen die vorliegenden Lehrstoff-Beschreibungen für den Gegenstand „Medientechnologie und angewandte Informatik“ diese spezifischen Inhalte **nicht in detaillierter oder umfassender Form** auf. In Bezug auf den **explizit aufgeführten Lehrstoff** des Gegenstands "Medientechnologie und angewandte Informatik" gibt es jedoch **keine Hinweise auf eine nennenswerte Behandlung** der Stufen 1 und 2 des Cybersecurity-Modells.

5.5.6.1 Lehrplanergänzungen

Durch diese Integrationen von Cybersecurity Inhalten können Studierende ein fundierteres Bewusstsein für Cybersecurity und Datenschutz entwickeln, ohne den Fokus des Lehrplans zu stark zu verschieben. Die

Inhalte aus den Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells würden somit explizit in den Lehrplan einfließen und die Absolvent:innen besser auf die Herausforderungen der digitalen Arbeitswelt vorbereiten.

1. Jahrgang - 1. Semester:

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Wiederholung und Festigung des **Grundverständnisses der Cybersecurity aus der Sekundarstufe I**: Dies beinhaltet technologisches Grundverständnis, das richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten und das Erkennen von Risiken und Reaktionsgrundsätzen.
- Einführung und **Motivation zur Sicherheit**: **Bewusstseinsbildung durch Fallbeispiele** (z.B. Keylogger-Video). Grundlagen von **Schadsoftware**. Erste Unterscheidung zwischen **„guten“ und „bösen“ Hackern (Ethical Hacking)**. Die Gefahr von **Identitätsdiebstahl**. Grundlegende **Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien** mit Fokus auf den Schutz personenbezogener Daten. Einführung in **Social Engineering**.

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Phänomenologie der medialen Vermittlung** könnte die Bedeutung von **Datenspuren im Internet** im Kontext der digitalen Identität und des Datenschutzes thematisiert werden.

1. Jahrgang - 2. Semester:

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Vertiefung des **richtigen Verhaltens im digitalen Raum**: Erkennen von Gefahren im Internet. Sichere Passwortwahl und -verwaltung. Sicheres Surfen im Internet. Sicherer Umgang mit sozialen Medien. Erkennung von Phishing-E-Mails und gefährlichen E-Mail-Anhängen. Umgang mit infizierten Datenträgern. Keine Installation verdächtiger Software. Sichere Entsorgung alter Geräte. Sicheres Verhalten auf Reisen (z.B. in öffentlichen WLANs).
- Erste Einführung in **Angriffsmethoden zur Informationsweitergabe:** Grundlagen von Phishing, Whaling, Gophish – ohne detaillierte technische Analyse.

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Phänomenologie der medialen Vermittlung** könnte die **kommunikative Funktion von Printverfahren und -medien** auch im Hinblick auf Falschinformationen und deren Erkennung (Analogie zu Phishing) diskutiert werden.

2. Jahrgang - 3. Semester:

Pflichtgegenstand „Wirtschaft und Recht“:

- Erste Behandlung **rechtlicher Rahmenbedingungen und Normen im Kontext von IT-Sicherheit und Datenschutz**: Grundlagen der **Datenschutz-Grundverordnung (DSGVO)** im Hinblick auf personenbezogene Daten im digitalen Raum.

Pflichtgegenstand „Typografie“:

- Im Bereich **Typografische Grundlagen und Gestaltung** könnte die Rolle von **vertrauenswürdigen Schriftarten und Quellen** im digitalen Kontext kurz angesprochen werden, um Bewusstsein für potenzielle Risiken (z.B. Einbettung von Schadcode) zu schaffen.

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Einführung in grundlegende Konzepte von **Vertraulichkeit und Integrität**: Wie funktioniert **Verschlüsselung konzeptionell** (ohne technische Tiefe). Wie funktioniert eine **Hashfunktion konzeptionell** (ohne technische Tiefe).

2. Jahrgang - 4. Semester:

Pflichtgegenstand „Wirtschaft und Recht“:

- Vertiefung der **rechtlichen Rahmenbedingungen und Normen**: Grundlagen des **Urheberrechts im digitalen Kontext** (auch im Hinblick auf illegale Downloads etc.), Grundlagen der **Domainregistrierung** (Seriosität von Webseiten), Überblick über relevante Gesetze wie das **Telekommunikationsgesetz** und das **IT-Sicherheitsgesetz** (in vereinfachter Form).

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Thematisierung der **Verfügbarkeit von Daten und Systemen**: Die Bedeutung von **Datensicherungen (Backups)**, verschiedene Arten von **Backup-Medien**, Einführung in **Cloud-Backups**, die Bedrohung durch **Ransomware** und grundlegende **Schutzmaßnahmen**.
- Grundlegende **Sicherheitsempfehlungen** könnten hier im Kontext der Systemnutzung explizit behandelt werden: Bedeutung von **starken Kennwörtern**, **Sperrbildschirm mit Kennwörtern**.

3. Jahrgang - 5. Semester:

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Wiederholung und Vertiefung der Inhalte aus Stufe 1 und 2 im Hinblick auf spezifische Anwendungen im Grafik- und Kommunikationsdesign.
- Grundlegende Konzepte der **sicheren Datenverwaltung und -weitergabe** (z.B. sichere Nutzung von Cloud-Speicher).

Pflichtgegenstand „Wirtschaft und Recht“:

- Einführung in **IT-Grundschutz und Normen wie ISO 27001** (grundlegende Konzepte und Bedeutung).

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Phänomenologie der medialen Vermittlung** könnte die **soziale Funktion und der kommerzielle Gebrauch von elektronischen Medien** auch im Hinblick auf Desinformation und Fake News analysiert werden.

3. Jahrgang - 6. Semester:

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- Behandlung der Frage **„Was tun im Notfall?“**: **Richtig reagieren bei Sicherheitsvorfällen**, **Kenntnis wichtiger Ansprechpartner** (innerhalb der Schule/Organisation), Initiierung von Maßnahmen zur **Infektionsbeseitigung** (grundlegende Schritte).
- Einführung in die Bedeutung von **Updates und Patches** sowie **0-Day-Exploits**.

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Theorie und Praxis von Design und Kommunikation** könnte die **emotionale und kognitive Wirkung visuellen Designs** auch im Kontext von manipulativem Design (z.B. in Phishing-Mails) analysiert werden.

4. Jahrgang - 7. Semester:

Pflichtgegenstand „Wirtschaft und Recht“:

- Detaillierte Behandlung der **rechtlichen Rahmenbedingungen (DSGVO etc.)** in Bezug zur technischen Umsetzung von Sicherheitsmaßnahmen. Die Inhalte aus den vorherigen Semestern zu Datenschutz bilden hier eine wichtige Grundlage.

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Marketing und Werbung** könnten die **Grundlagen, Mechanismen und Phänomene werblicher Kommunikation** auch im Hinblick auf betrügerische Online-Werbung und Phishing-Taktiken analysiert werden.

4. Jahrgang - 8. Semester:

Pflichtgegenstand „Wirtschaft und Recht“:

- Vertiefung der **technischen Aspekte von Vertraulichkeit, Integrität und Verfügbarkeit** unter Berücksichtigung der rechtlichen Vorgaben.

Pflichtgegenstand „Kommunikationsdesign“:

- Im Bereich **Theorie und Praxis von Design und Kommunikation** könnte die Beurteilung von **Kommunikationsdesigns auf ihre Wirkung hin** auch Aspekte der Vertrauenswürdigkeit und Sicherheit umfassen.

5. Jahrgang - 9. und 10. Semester:

Pflichtgegenstand „Medientechnologie und angewandte Informatik“:

- In den höheren Semestern sollten die Grundlagen der Cybersecurity aus Stufe 1 und 2 in den verschiedenen fachspezifischen Gegenständen immer wieder kontextbezogen aufgegriffen und angewendet werden, um das Bewusstsein für Sicherheit in allen Bereichen des Grafik- und Kommunikationsdesigns zu schärfen. Dies könnte beispielsweise bei der Planung und Umsetzung von Online-Projekten, der Erstellung von digitalen Portfolios oder der Zusammenarbeit in Online-Umgebungen geschehen.

Pflichtgegenstand „Wirtschaft und Recht“:

- Vertiefende Auseinandersetzung mit **aktuellen rechtlichen Entwicklungen im Bereich IT-Sicherheit und Datenschutz** sowie deren Auswirkungen auf die Tätigkeit von Grafik- und Kommunikationsdesignern (z.B. im Bereich E-Commerce, Social Media Marketing etc.).

5.5.6.2 Zusammenfassende Analyse

Allgemein sind Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells im Lehrplan der Höheren Lehranstalt für Grafik- und Kommunikationsdesign bereits **indirekt und in Ansätzen** berücksichtigt, auch wenn sie nicht explizit als „Cybersecurity“ oder „IT-Sicherheit“ ausgewiesen sind.

- Die im Lehrplan verankerte **ethische und gesellschaftlich sensible Verantwortung**, die die Gestaltung von Kommunikation mit sich bringt, korrespondiert mit der **Motivation zur Sicherheit** aus Stufe 1. Es wird ein Bewusstsein für die Auswirkungen der eigenen Tätigkeit im digitalen Raum geschaffen, was eine Grundlage für sicherheitsbewusstes Verhalten darstellt.
- Der **Umgang mit digitalen Medien** ist ein Kernbestandteil der Ausbildung im Grafik- und Kommunikationsdesign. Dies beinhaltet den Einsatz verschiedener Software und Technologien zur Erstellung und Bearbeitung von Inhalten. Dabei werden implizit auch Aspekte des **richtigen Verhaltens im Umgang mit Daten** (wenn auch primär im Hinblick auf kreative Prozesse und Urheberrechte) und das **Erkennen von grundlegenden Risiken** im digitalen Raum berührt, wie sie in Stufe 1 thematisiert werden.
- Die in verschiedenen Gegenständen geforderte Fähigkeit zur **Recherche, zum Erstellen von Konzepten und zur Präsentation von Ergebnissen** kann auch die Bewertung von Informationen aus dem Internet und somit erste Schritte zur **Erkennung von unseriösen Quellen** (analog zu Phishing-Erkennung in Stufe 1) umfassen.
- Der Pflichtgegenstand **Wirtschaft und Recht** vermittelt grundlegende rechtliche Kenntnisse. Obwohl der Fokus primär auf wirtschaftlichen und allgemeinen rechtlichen Rahmenbedingungen liegt, können hier auch **erste Berührungspunkte mit datenschutzrechtlichen Aspekten** (DSGVO im Kontext von Unternehmenskommunikation) entstehen, die in Stufe 2 des Modells behandelt werden.
- Fächer wie **Medientechnologie und angewandte Informatik** vermitteln **grundlegende technische Kenntnisse** über Hardware, Software und digitale Prozesse. Dieses Basiswissen ist notwendig, um die in Stufe 1 und 2 angesprochenen **technologischen Grundlagen** (z.B. Funktionsweise des Internets, grundlegende Softwarefunktionen) zu verstehen.
- Die Auseinandersetzung mit der **Wirkung von Design** und der **Theorie und Praxis von Design und Kommunikation** kann auch die bewusste Gestaltung von visuellen Elementen zur **Vermeidung von Täuschung oder Irreführung** beinhalten, was indirekt mit Aspekten der Online-Sicherheit und des Schutzes vor Social Engineering (Stufe 1) in Verbindung steht.

Es ist jedoch festzuhalten, dass eine **explizite und systematische Behandlung** der spezifischen Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells, wie beispielsweise detaillierte technische Analysen von Bedrohungen, spezifische Sicherheitsempfehlungen, die Funktionsweise von Verschlüsselung oder die Analyse von Angriffsmustern, **nicht dezidiert im vorliegenden Lehrplan vorgesehen** ist. Die vorhandenen Berührungspunkte sind eher allgemeiner Natur und im Kontext der spezifischen Lernziele des Grafik- und Kommunikationsdesigns eingebettet.

Empfehlung

Im Sinne der Sichtbarmachung von Cybersecurity wäre hier eine Teilung des Faches „Medientechnologie und angewandte Informatik“ in „Angewandte Informatik“ (für die digitalen Grundlagen) und „Medientechnologie“ (für die fachspezifischen Anwendungen) empfohlen. Eine Angleichung an den in Anlage 1 geregelten Gegenstand „Angewandte Informatik“ wäre wünschenswert und würde zu einer Standardisierung der Inhalte führen.

5.5.7 Lehrplan Informatik

Im Lehrplan Informatik (IF) sind die Inhalte der Stufen 1 bis 3 als fundamentale Konzepte und erste Auseinandersetzung mit der Thematik in **verschiedenen Gegenständen** verankert, während die Inhalte der Stufe 4 mit dem Fokus auf Angriffsmuster und Verteidigungsmaßnahmen schwerpunktmäßig in den fortgeschrittenen Fachgegenständen der Informatik, insbesondere „Netzwerksysteme und Cybersecurity“ und „Programmieren und Software Engineering“ behandelt werden. Folgende Gegenstände unterstützen im IF-Lehrplan Cybersecurity Inhalte:

- Computerarchitekturen und Betriebssysteme
- Programmierung und Softwareengineering
- Datenbanken und Informationssysteme
- Netzwerksysteme und Cybersecurity
- Webprogrammierung und Mobile Computing
- Betriebswirtschaft und Management
- Data Science und Artificial Intelligence
- Systemplanung und Projektentwicklung

5.5.7.1 Lehrplananpassungen

Diese Vorschläge integrieren explizit Inhalte der Stufen 1 bis inklusive 4 des CLEMENTINE-6-Stufen-Modells in den bestehenden Lehrplan und verteilen diese über die fünf Jahre, wobei grundlegende Konzepte in den ersten Jahren eingeführt und in späteren Semestern vertieft werden. Die Zuordnung erfolgt unter Berücksichtigung der thematischen Nähe zu den bestehenden Pflichtfächern. Es ist wichtig zu beachten, dass diese Ergänzungen inhaltlich auf die Sekundarstufe II zugeschnitten sind und die spezifischen Lernziele des Fachbereichs Informatik berücksichtigen sollten. Es sollten daher folgende Inhalte hinzugefügt bzw. im Sinne der Cybersecurity besser im Lehrplan sichtbar gemacht werden:

1. Jahrgang - 1. Semester:

Pflichtfach "Computerarchitektur und Betriebssysteme":

- Explizite Einführung und Wiederholung des **Grundverständnisses der Cybersecurity aus der Sekundarstufe I**, einschließlich: **Technologisches Grundverständnis**. Das **richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten**. Das **Erkennen von Risiken und Reaktionsgrundsätze**.
- Thematisierung der **Motivation zur Sicherheit**: **Bewusstseinsbildung durch Fallbeispiele** (z.B. Keylogger-Video). Grundlagen von **Schadsoftware**. Unterscheidung zwischen **„guten“ und „bösen“ Hackern (Ethical Hacking)**. Die Gefahr von **Identitätsdiebstahl**. Grundlegende **Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien** mit Fokus auf den Schutz personenbezogener Daten. Einführung in **Social Engineering**.

1. Jahrgang - 2. Semester:

Pflichtfach „Programmieren und Software Engineering“:

- Einführung in **sichere Passwortwahl und -verwaltung** im Rahmen der Grundlagen der Programmierung und des Benutzerzugriffs.

Pflichtfach „Datenbanken und Informationssysteme“:

- Thematisierung des **sicheren Surfens im Internet und des sicheren Umgangs mit sozialen Medien** im Kontext der Nutzung von Informationssystemen.
- Einführung in die **Erkennung von Phishing-E-Mails und gefährlichen E-Mail-Anhängen** sowie den **Umgang mit infizierten Datenträgern** und die Notwendigkeit, **keine verdächtige Software zu installieren**.

Pflichtfach „Computerarchitektur und Betriebssysteme“:

- Einführung in **Grundbegriffe** der Cybersecurity: Antivirus, Malware, Phishing. Grundbegriffe und Strategien der Datensicherheit. Digitale Identität.

2. Jahrgang - 3. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Explizite Behandlung der **Analyse von Mail-Headern und URLs**, um die Herkunft von Spam-/Phishing-Mails eindeutig feststellen zu können.
- Einführung in **Datenspuren im Internet** und die Bedeutung, Daten sicher zu verwalten und weiterzugeben (z.B. Cloudspeicher verwenden) sowie Daten sicher zu löschen.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Thematisierung des **sicheren Entsorgens alter Geräte** im Kontext der Hardware-Grundlagen.

Pflichtfach „Betriebswirtschaft und Management“:

- Erste Behandlung der **rechtlichen Rahmenbedingungen und Normen im Kontext von IT-Sicherheit und Datenschutz**, insbesondere Grundlagen der **Datenschutz-Grundverordnung (DSGVO)** im Hinblick auf personenbezogene Daten.

Pflichtfach „Computerarchitektur und Betriebssysteme“:

- Einführung in **Sicherheitsempfehlungen**: **Verhaltensrichtlinien** (beispielsweise Abmeldung/Sperren, Clean Desktop…). **Sperrbildschirm mit Kennwörtern**. Bedeutung von **Updates und Patches**; Erwähnung von **0-Day-Exploits**. **BIOS-Kennwörter** – sicherer Bootprozess.
- Einführung in die **Reduktion der Angriffsfläche** durch Abschaltung nicht benötigter Dienste (Gerätehärtung, etc.).
- Einführung in grundlegendes **Monitoring von Diensten/Prozessen**.

Pflichtfach „Programmieren und Software Engineering“:

- Erste Einführung in grundlegende Konzepte von **Vertraulichkeit und Integrität**: Wie funktioniert **Verschlüsselung** konzeptionell (ohne technische Tiefe)? Wie funktioniert eine **Hashfunktion** konzeptionell (ohne technische Tiefe)?

2. Jahrgang - 4. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Vertiefung der **Sicherheitsempfehlungen**: Verhalten in öffentlichen Netzen / öffentlichen WLAN’s / privaten Netzen. Bedeutung von Kennwörtern (Komplexität, Länge), Rainbowtable. Least Privileges. Privatsphäre in Spielen und Chatrooms.
- Einführung in **Bedrohungsszenarien**: Sicherheitskompromittierung durch externe Geräte erklären (Rubberducky / Bashbunny, Autorun, USB-Killer). Grundlagen von Angriffsmethoden zur Informationsweitergabe: z.B. Phishing, Whaling, Gophish (ohne detaillierte technische Analyse).

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Thematisierung der **Sicherung des eigenen Geräts**, einschließlich grundlegender Konfigurationen.

Pflichtfach "Computerarchitektur und Betriebssysteme":

- Einführung in **Datenträgerverschlüsselung** im Rahmen der Speicherverwaltung.
- Thematisierung der **Bedeutung von Datensicherungen (Backups)** sowie verschiedener **Arten von Backup-Medien** und Einführung in **Cloud-Backups**.

3. Jahrgang - 5. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Einführung in einfache **Netzwerksicherheitstools** nennen und bedienen (z.B. ping, ipconfig).
- Einführung in die **Analyse einfacher fundamentaler Protokolle** (z.B. DHCP, HTTP, DNS) mit einfachen Werkzeugen.
- Einführung in das Konzept und die Bedeutung von **Penetration Testing** auf einer theoretischen Ebene.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Behandlung grundlegender Aspekte **sicherer Webentwicklung** im Rahmen der Webprogrammiertechniken.
- Einführung in **Standards bei der Webentwicklung** (z.B. ISO 25000, ÖNORM A7700).

Pflichtfach „Programmieren und Software Engineering“:

- Einführung in **Standards bei der Softwareentwicklung**.

Pflichtfach „Betriebswirtschaft und Management“:

- Einführung in **IT-Grundschutz und Normen wie ISO 27001** (grundlegende Konzepte und Bedeutung).

3. Jahrgang - 6. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Behandlung der Frage „**Was tun im Notfall?**“: Richtig reagieren bei Sicherheitsvorfällen. Kenntnis wichtiger Ansprechpartner. Initiierung von Maßnahmen zur Infektionsbeseitigung (grundlegende Schritte).
- Einführung in das Konzept von **Firewalls**.
- Einführung in grundlegende **Netzwerk-Angriffsvektoren** (z.B. einfache DoS-Angriffe).

Pflichtfach „Programmieren und Software Engineering“:

- Einführung in grundlegende Aspekte des **sicheren Programmierens**.
- Thematisierung des **Einsatzes von Verschlüsselungs- und Hashing-Verfahren in eigenen Programmen** auf einer grundlegenden Ebene.

Pflichtfach „Betriebswirtschaft und Management“:

- Vertiefung der **rechtlichen Rahmenbedingungen** im Hinblick auf IT-Sicherheit und Datenschutz.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Einführung in häufige **Web Application Security Angriffsvektoren** (OWASP Top 10) auf konzeptioneller Ebene.

4. Jahrgang - 7. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Einführung in fortgeschrittenere **Netzwerksicherheitstools** und deren grundlegende Anwendungsmöglichkeiten.

Pflichtfach „Datenbanken und Informationssysteme“:

- Detaillierte Behandlung der **rechtlichen Rahmenbedingungen (DSGVO etc.)** in Bezug zur technischen Umsetzung von Sicherheitsmaßnahmen.

4. Jahrgang - 8. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Einführung in grundlegende **Verschlüsselungs- und Hashing-Verfahren** (ohne tiefe mathematische Details).
- Einführung in die Nutzung einfacher **Exploits** und grundlegender **Metasploit-Module** in einer Laborumgebung.

Pflichtfach „Datenbanken und Informationssysteme“:

- Vertiefung der technischen Aspekte von **Vertraulichkeit, Integrität und Verfügbarkeit** unter Berücksichtigung der rechtlichen Vorgaben.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Einführung in häufige **Angriffsvektoren im Webbereich** (z.B. SQL-Injection, Cross-Site-Scripting) auf konzeptioneller Ebene.
- Einführung in **Gegenmaßnahmen** zum Schutz von Webanwendungen (z.B. grundlegende Firewall-Konzepte).

Pflichtfach „Programmieren und Software Engineering“:

- Behandlung von grundlegenden **Schutzmaßnahmen gegen Injections**.

Pflichtfach „Data Science und Artificial Intelligence“:

- Einführung in Werkzeuge zur **Visualisierung von Daten** im Kontext von Sicherheitsdaten (z.B. einfache Diagramme).

5. Jahrgang - 9. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Einführung in **sichere Authentifizierungsmethoden** (NIST Guidelines, Password Safes, Mehrfaktorauthentifizierung).
- Planung, Durchführung (im Labor) und Dokumentation einfacher **Penetration Tests** unter Verwendung von Tools wie **Kali Linux**.

Pflichtfach „Systemplanung und Projektentwicklung“:

- Einführung in grundlegende Konzepte des Cybersecurity **Risikomanagements** im Kontext von IT-Projekten.
- Integration von **Sicherheitsaspekten** in den Softwareentwicklungsprozess (z.B. Security by Design).

Pflichtfach „Programmieren und Software Engineering“:

- Vertiefung des Einsatzes von **Verschlüsselungs- und Hashingverfahren** in eigenen Programmen.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Praktische Durchführung einfacher **Web Application Security Angriffe** (OWASP Top 10) in einer sicheren Testumgebung und Implementierung grundlegender Gegenmaßnahmen.

5. Jahrgang - 10. Semester:

Pflichtfach „Netzwerksysteme und Cybersecurity“:

- Einführung in **verschlüsselte Kommunikationskanäle** wie z.B. HTTPS und Zertifikate.
- Implementierung geeigneter **Gegenmaßnahmen** gegen Netzwerkangriffe (**IDS/IPS**, Monitoring) auf einer grundlegenden Ebene.

Pflichtfach „Systemplanung und Projektentwicklung“:

- Einführung in die Bedeutung von **Sicherheitsstrategien**.

Pflichtfach „Programmieren und Software Engineering“:

- Einführung in fortgeschrittenere Schutzmaßnahmen wie **Control Flow Integrity (CFI)** und **Address Space Layout Randomization (ASLR)** auf konzeptioneller Ebene.

Pflichtfach „Webprogrammierung und Mobile Computing“:

- Vertiefung der sicheren Webentwicklung und Implementierung fortgeschrittener Gegenmaßnahmen.

Pflichtfach „Data Science und Artificial Intelligence“:

- Einführung in Werkzeuge zur **automatisierten Verhaltensanalyse und Anomalieerkennung** (AI, ELK, SIEM etc.) auf einer konzeptionellen Ebene.

Diese Vorschläge integrieren die Inhalte der Stufe 1 bis inklusive 4 schrittweise und bauen auf den Grundlagen der vorherigen Stufen auf. Die Verteilung berücksichtigt die thematische Nähe zu den bestehenden Fächern und ermöglicht eine kontinuierliche Vertiefung der Konzepte im Laufe der Ausbildung. Es ist entscheidend, dass praktische Übungen in einer sicheren Laborumgebung einen wesentlichen Bestandteil dieser Integration bilden.

5.5.7.2 Zusammenfassende Analyse

Stufe 1 und 2: Allgemeine Einführung und vertiefende Awareness

Die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells, welche eine allgemeine Einführung in die Cybersecurity und eine tiefergehende Awareness für IT-Berufe, persönliche Sicherheit sowie rechtliche Rahmenbedingungen und Normen umfassen, finden sich als Grundlagen und Motivation zur Sicherheit in verschiedenen Unterrichtsgegenständen wieder.

- Im **Pflichtfach „Computerarchitektur und Betriebssysteme“** des 1. Jahrgangs wird ein **Grundverständnis der Funktionsweise von Rechnern** gelegt, was eine Basis für das technologische Grundverständnis aus Stufe 1 darstellt. Auch die Thematisierung der **Sicherheitsunterweisung** im 1. Jahrgang kann als erste Berücksichtigung von richtigem Verhalten im Umgang mit Daten und dem Erkennen von Risiken (Stufe 1) gesehen werden.
- Das **Pflichtfach „Programmieren und Software Engineering“** im 1. und 2. Jahrgang legt Grundlagen im **Umgang mit Daten, Algorithmen und Programmen**, was indirekt Aspekte der Datensicherheit und des sicheren Verhaltens (Stufe 1 und 2) berührt.
- Im **Pflichtfach „Datenbanken und Informationssysteme“** werden im 1. und 2. Jahrgang **Grundlagen im Umgang mit verschiedenen Endbenutzerwerkzeugen und Standardsoftwareprodukten** vermittelt, was ebenfalls Berührungspunkte mit der sicheren Nutzung von Software (Stufe 1 und 2) aufweist.
- Das **Pflichtfach „Netzwerksysteme und Cybersecurity“**, beginnend im 2. Jahrgang, thematisiert explizit **grundlegende Netzwerktechnologien**, was eine Basis für das Verständnis von Bedrohungen und Sicherheitsmaßnahmen (Stufe 1 und 2) schafft. Im 2. Jahrgang werden auch die prinzipiellen Aufgaben und Funktionsweisen von Netzwerkdiensten erläutert. Im 3. Jahrgang werden wesentliche Aspekte und Bedrohungen der Netzwerksicherheit beschrieben und Authentifizierungsdienste angewendet.
- Das **Pflichtfach „Webprogrammierung und Mobile Computing“**, beginnend im 2. Jahrgang, behandelt den **Aufbau von Webseiten und die Kommunikation im Internet**, was Aspekte des sicheren Umgangs mit Daten im Internet (Stufe 1 und 2) impliziert.

- Im **Pflichtfach „Betriebswirtschaft und Management“** des 1. und 2. Jahrgangs werden **rechtliche Grundlagen** behandelt, was eine erste Auseinandersetzung mit den rechtlichen Rahmenbedingungen (Stufe 2) darstellt.

Stufe 3: „Foundational“ - Netzwerk- Geräte - und Anwendungssicherheit, Sicherheitsmanagement

Die Inhalte der Stufe 3 des CLEMENTINE-6-Stufen-Modells, die Netzwerk-, Geräte- und Anwendungssicherheit sowie Sicherheitsmanagement umfassen, sind direkt in den fachspezifischen Pflichtgegenständen der Informatik verankert:

- Das **Pflichtfach „Computerarchitektur und Betriebssysteme“** vertieft im 2. Jahrgang die wesentlichen Komponenten von Betriebssystemen sowie deren Aufgaben, Funktionsweisen und Zusammenwirken. Es werden auch potenzielle Sicherheitsrisiken in Betriebssystemen beurteilt und Maßnahmen zu deren Vermeidung getroffen.
- Das **Pflichtfach „Programmieren und Software Engineering“** legt im 3. Jahrgang Grundlagen für **fortgeschrittene, objektorientierte Programmiertechniken** und behandelt im 4. Jahrgang **Entwicklungstechniken für zuverlässige Systeme**, was Aspekte der Anwendungssicherheit (Stufe 3) berührt.
- Das **Pflichtfach „Datenbanken und Informationssysteme“** thematisiert im 4. Jahrgang, wie **konsistente, datensichere Datenbanksysteme eingerichtet und betrieben** werden können, und behandelt **passende Vorkehrungen zur Einhaltung des Datenschutzes bei der Realisierung von Informationssystemen**.
- Das **Pflichtfach „Netzwerksysteme und Cybersecurity“** im 2. und 3. Jahrgang ist zentral für die Behandlung der Inhalte der Stufe 3. Es werden grundlegende und komplexe Netzwerktechnologien erklärt und Netzwerke hinsichtlich der verwendeten Technologien und Komponenten bewertet. Die Funktionalität von Netzwerkdiensten wird evaluiert und implementiert, und die wesentlichen Aspekte und Bedrohungen der Netzwerksicherheit werden beschrieben.
- Das **Pflichtfach „Webprogrammierung und Mobile Computing"** behandelt im 4. Jahrgang die **Architektur verteilter Systeme** und im 2. und 3. Jahrgang die **Realisierung von Webseiten unter Einsatz von Skriptsprachen**, was Grundlagen für die Anwendungssicherheit im Webbereich (Stufe 3) schafft.
- Im **Pflichtfach „Betriebswirtschaft und Management“** wird im 3. Jahrgang die **Einordnung der Kostenrechnung im betrieblichen Umfeld** behandelt, was indirekt für das Verständnis wirtschaftlicher Aspekte im Sicherheitsmanagement relevant sein kann.
- Das **Pflichtfach „Systemplanung und Projektentwicklung“** beginnt im 3. Jahrgang mit der Erklärung der **theoretischen Grundlagen, Rahmenbedingungen, Prozesse und Kompetenzen im Projektmanagement**, was Grundlagen für das Sicherheitsmanagement (Stufe 3) legen kann.

Stufe 4: „Professional“ - Angriffsmuster und Verteidigungsmaßnahmen

Die Inhalte der Stufe 4 des CLEMENTINE-6-Stufen-Modells, die Angriffsmuster und Verteidigungsmaßnahmen in den einzelnen Fachrichtungen umfasst, werden ebenfalls im Lehrplan berücksichtigt, primär in den fortgeschrittenen Jahrgängen und spezifischen Fachgegenständen:

- Das **Pflichtfach „Programmieren und Software Engineering“** behandelt im 4. und 5. Jahrgang die Erstellung von Software für unterschiedliche Plattformen und Entwicklungstechniken für zuverlässige Systeme, was Aspekte von Verteidigungsmaßnahmen in der Softwareentwicklung beinhaltet.
- Das **Pflichtfach „Datenbanken und Informationssysteme“** thematisiert im 4. Jahrgang die Erkennung von Problemen des Mehrbenutzerbetriebs bei der Entwicklung von Datenbankanwendungen und den Einsatz von Lösungsstrategien, was als eine Form der Verteidigungsmaßnahme gesehen werden kann.
- Das **Pflichtfach „Netzwerksysteme und Cybersecurity“** im 4. und 4. Jahrgang geht explizit auf Maßnahmen zum Schutz von Netzwerken und Systemen ein und behandelt die Definition von Sicherheitsanforderungen und den Einsatz kryptographischer Verfahren. Es werden auch Sicherheitslösungen definiert, angewendet und getestet. Die Analyse und Realisierung komplexer Netzwerke sowie die strukturierte Fehlersuche sind ebenfalls Bestandteile.
- Das **Pflichtfach „Webprogrammierung und Mobile Computing“** behandelt im 4. Jahrgang die Entwicklung sicherer Applikationen für mobile Systeme, was direkt Verteidigungsmaßnahmen im Bereich mobiler Anwendungen adressiert.
- Das **Pflichtfach „Systemplanung und Projektentwicklung“** behandelt im 5. Jahrgang die Entwicklung geeigneter Konzepte für die Datensicherheit und den Datenschutz und die Ableitung

geeigneter Schritte aus den gesetzlichen Vorgaben im Bereich der Informationstechnologie, was wichtige Aspekte von Verteidigungsstrategien darstellt.

Man kann feststellen, dass Inhalte der Stufen 1 bis 3 als fundamentale Konzepte und erste Auseinandersetzung mit der Thematik in verschiedenen Gegenständen verankert sind, während die Inhalte der Stufe 4 mit dem Fokus auf Angriffsmuster und Verteidigungsmaßnahmen schwerpunktmäßig in den fortgeschrittenen Fachgegenständen der Informatik, insbesondere "Netzwerksysteme und Cybersecurity" und "Programmieren und Software Engineering" behandelt werden.

5.5.8 Lehrplan Informationstechnologie

Auch im Lehrplan Informationstechnologie sind Cybersecurity Inhalte der Stufen 1 bis 4 (5) als fundamentale Konzepte mit der Thematik in **verschiedenen Gegenständen** verankert.

Folgende Gegenstände unterstützen Cybersecurity Inhalte:

- IT-Sicherheit
- Systemtechnik
- Netzwerktechnik
- Computerpraktikum
- Informationssysteme
- Informationstechnische Projekte
- Medientechnik
- Softwareentwicklung

5.5.8.1 Lehrplanergänzungen

Der IT- Lehrplan enthält bereits viele Grundlagen der Stufen 1 und 2 in den ersten beiden Jahrgängen im Fach „IT-Sicherheit“. Die fortgeschrittenen Themen der Stufen 3-5 sind dabei primär für die höheren Jahrgänge und die Ausbildungsschwerpunkte vorgesehen und sollten dort vertiefend behandelt werden. Wenn wird Stufe 5 eher konzeptionell als in voller praktischer Breite abzubilden sein. Die Integration der Stufen 1-5 des CLEMENTINE-6-Stufen-Modells in den Lehrplan könnte, unter Berücksichtigung der vorhandenen Gegenstände und ihrer Inhalte, wie folgt aufgeschlüsselt werden:

1. Jahrgang - 1. und 2. Semester:

Pflichtgegenstand „IT-Sicherheit“:

- **Motivation zur Sicherheit:** Bewusstseinsbildung (Video, Fallbeispiele), Schadsoftware, Identitätsdiebstahl, Social Engineering. Ebenso das Wissen um das Verhalten im Notfall: richtig reagieren, Ansprechpartner kennen, Infektionsbeseitigung initiieren.

2. Jahrgang - 3. und 4. Semester:

Dieser Jahrgang sollte nach dem CLEMENTINE-6-Stufen-Modell ebenfalls Stufe 1 und den Beginn von Stufe 2 abdecken. Stufe 2 wird als „Exploratory“ beschrieben und dient der tiefergehenden Awareness.

Pflichtgegenstand „IT-Sicherheit“:

- Vertiefung **Über den Umgang mit Daten**: **Backup anlegen und Daten wiederherstellen, Datenträgerverschlüsselung kennen und benutzen, Sicheres Entsorgen von Dokumenten/Datenträgern**.
- Vertiefung **Sichere Kommunikation**: sichere Verbindung zum Arbeitsplatznetzwerk (z.B. VPN basics), persönliche Firewalls, detailliertere sichere Authentifizierungsmethoden (NIST Guidelines, Password Safes, Mehrfaktorauthentifizierung), Verschlüsselte Kommunikationskanäle (HTTPS, Zertifikat).
- Einführung **Digitale Bürgerkarte** (Signaturkonzepte, Überprüfung, Handysignatur). Konzepte zu **Smart Devices** und spezifischen Suchmaschinen.
- Detailliertere **Rechtsgrundlagen** (IT-Recht, StGB, DSGVO in Österreich und Europa).

- Vertiefung **Technische Umsetzungsstrategien** (Sicherheitsmanagement/-systeme, BSI-Grundschutz Basics, Anonymisierungsdienste, Logfiles – hier Fokus Interpretation, Sandboxing/Virtuelle Maschinen). Detailliertere
- **Angriffsvektoren** (Ransomware, Botnetze, Mobile, App Trust, DOS/DDOS, Cybercrime, Defacements, Reconnaissance, 6 Stufen eines Angriffs).

Pflichtgegenstand „Systemtechnik“:

- Im 3. und 4. Semester werden Betriebssystemkonzepte und -installation sowie **Virtualisierungstechnologien** behandelt, was Stufe 2 **Sandboxing – Virtuelle Maschinen** unterstützt.

Pflichtgegenstand „Netzwerktechnik“:

- Im 3. und 4. Semester werden Schichtenmodelle, Protokolle und Switching/Routing behandelt. Dies bildet die Grundlage für **Sichere Kommunikation** und **Netzwerksicherheitstools** in Stufe 2.

Pflichtgegenstand „Computerpraktikum“:

- Vertiefung der Netzwerk- und Systemtechnikpraxis, die praktische Umsetzung von Stufe 2 Konzepten (z.B. Konfiguration von Systemen/Netzwerkkomponenten, Kabelmessung) unterstützt.

3. Jahrgang - 5. und 6. Semester:

Pflichtgegenstand „Systemtechnik“:

- Vertiefung **Gerätesicherheit**: Sicherstellen sicherer Server-/Clientkonfigurationen, Konzepte wie Group Policies (GPOs),
- Z**entrales Logging** (Anbindung an Monitoring-Systeme).
- Vertiefung **Infrastruktursicherheit**: Zugriffsschutz (z.B. ACLs in Dateisystemen/Diensten), grundlegende Konzepte zur **Netzwerksegmentierung**.

Pflichtgegenstand „Netzwerktechnik“:

- Vertiefung **Infrastruktursicherheit**: Detaillierte Betrachtung von **VLANs** und **Netzwerksegmentierung**. Grundlegende Konzepte von **Zugriffsschutz** in Netzwerken (z.B. Port Security).
- Einführung **zentrales Logging** in Netzwerken. Grundlegende Konzepte von **Sicherheitsarchitekturen** wie Firewalls (Funktionsprinzipien) und VPNs (Notwendigkeit) – der Lehrplan nennt dies in B.6 erst im 4. Jahrgang.

Pflichtgegenstand „Informationssysteme“:

- Vertiefung **Anwendungssicherheit** im Datenbankkontext: Sichere Datenbankanwendungen entwickeln, Fokus auf sichere Schnittstellen und Umgang mit Benutzerrechten/Rollen in der Datenbank.
- Konzepte zu **zentralen Authentifizierungs-/Autorisierungssystemen** (z.B. LDAP-Anbindung für DB-Zugriff).

Pflichtgegenstand „Softwareentwicklung“:

- **Zusätzliche explizite Einfügung aus Stufe 3:** Vertiefung **Anwendungssicherheit**: Sichere Programmierungspraktiken (z.B. Eingabevalidierung, Umgang mit sensiblen Daten). Sichere Konfiguration von Anwendungen.

Pflichtgegenstand „Informationstechnische Projekte“:

- **Organisations-, Risiko- und Sicherheitsmanagement**: Einführung in ISMS (Informationssicherheits-Managementsysteme) nach ISO 27001 (Grundkonzepte).
- Grundkonzepte des **Risikomanagements** in IT-Projekten. Verknüpfung von Qualitätsmanagement mit Sicherheitsstandards (z.B. BSI-Grundschutz Basics).

- Einführung in die Strukturen der IT-Sicherheit in Österreich und Europa (Überblick).

4. Jahrgang - 7. und 8. Semester:

Pflichtgegenstand „Systemtechnik“:

- Vertiefung **Infrastruktur-/Geräte-/Server-/Client-Sicherheit**: Detailkonzepte für Device Hardening, Patching, Group Policies, Software-Management/Distribution, Update Management, Backup Strategien im Unternehmenskontext.
- Vertiefung **Sicherheitsarchitekturen**: Detaillierte Behandlung von Firewalls, IDS/IPS, VPNs, zentralen Authentifizierungs-/Autorisierungssystemen (PKI, Kerberos, ACLs – Implementierung/Anwendung),
- **Access Control** (NAC, 802.1X – Konzepte/Implementierung).
- Vertiefung **Monitoring und BigData**: **Automatisierte Verfahren zur Informationsbeschaffung aus dem Netzwerk/System** (SIEM, Windows Event Forwarding, syslog, Proxylogs – Implementierung/Anwendung).
- **Netzwerk-Angriffsvektoren erkennen** (IDS, Monitoring – Analyse). Einführung **Werkzeuge zur Visualisierung von Daten** (ELK o.ä. – Konzepte/Basics).
- Einführung **Automatisierte Verhaltensanalyse/Anomalieerkennung** (AI, ELK, SIEM – Konzepte/Basics).

Pflichtgegenstand „Netzwerktechnik“:

- Siehe Systemtechnik, aber mit spezifischem **Netzwerk-Fokus** auf Stufe 3 Infrastruktur- und Architektursicherheit sowie Stufe 4 Monitoring/BigData im Netzwerk.
- Detaillierte Behandlung von **Netzwerksicherheit** inkl. Härtung von Netzwerkkomponenten.
- **Verzeichnisdienste** und automatisierte Benutzerverwaltung als Teil von Auth/Auth. Praktische Sicherheitsanalysen.

Pflichtgegenstand „Softwareentwicklung“:

- **Sichere Softwareentwicklung**: Standards kennen/anwenden (NIST, Audits, Safety – Konzepte).
- Integration von **Continuous Integration und Testing** in den Softwareentwicklungsprozess.
- **Verschlüsselungs- und Hashingverfahren in eigenen Programmen einsetzen und anwenden**.
- Einführung in **Formale Verifikation**, **Statische und dynamische Code-Analysen** (Basics, mögliche Buffer Overflows).

Pflichtgegenstand „Informationssysteme“:

- Vertiefung **Anwendungssicherheit** im IS-Kontext: Sichere Datenbankprogrammierung, sicherer Betrieb von CMS.
- Vertiefung **IS-Administration/Sicherheit**: Detaillierte **Accountingsysteme**, Benutzer, Rollen, Rechte, detaillierte **Backup-/Restore-Strategien**.
- Log-Analyse von Datenbanksystemen.

Schwerpunkt „Medientechnik“:

- **Gerätehärtung** für Mediengeräte.
- **Anwendungssicherheit** bei Web-Applikationen, mobilen Apps und CMS.
- **Monitoring** von Medienservern/Webdiensten.

5. Jahrgang - 9. und 10. Semester:

Im Lehrplan primär nur Konzepte einführen und nicht unbedingt vollständige praktische Umsetzungen:

Pflichtgegenstand „Systemtechnik“:

- Vertiefung **Monitoring und BigData** im Systemkontext.
- Analyse komplexer Protokolle – Einführung.

- **Digitale Forensik**: Konzepte des Incident Response Cycle, Schritte der Beweissicherung auf Systemen (laufendes System, Offline-Analyse – z.B. Logfile-Analyse als Artefakt, Festplattenabbilder - Konzept).

Schwerpunkt „Netzwerktechnik“:

- Vertiefung **Monitoring und BigData** im Netzwerk: SIEM, Log-Analyse, Systembelastbarkeit, Schwachstellenanalyse.
- Einführung **Digitale Forensik**: Incident Response Cycle im Netzwerk, Analyse von Netzwerkprotokollen/Logs als Beweismittel,
- Konzepte der Sicherstellung von Netzwerkverkehrsdaten.
- Einführung **Software Security**: Analysekonzepte für Netzwerkdienste oder Firmware (Debugger/Disassembler/Deobfuscation – Konzepte).

Pflichtgegenstand „Softwareentwicklung“:

- Vertiefung **Sichere Softwareentwicklung**: Detaillierte Anwendung von Standards, **Sicherheitstests** als Teil der Teststrategien, tiefere Betrachtung von **statischen/dynamischen Code-Analysen** und häufigen Schwachstellen (z.B. Buffer Overflows).
- Einführung **Software Security**: Konzepte der Malware-Analyse, Umgang mit Debuggern/Disassemblern/Deobfuscation zur Sicherheitsanalyse von Binärdateien oder Skripten – Fokus auf das *Verständnis* dieser Werkzeuge und Techniken.

Pflichtgegenstand „Informationssysteme“:

- Einführung **Digitale Forensik**: Sicherstellung von Daten aus Informationssystemen als Beweismittel. Analyse von Datenbank-Logs als Artefakte.

5.5.8.2 Zusammenfassende Analyse

Basierend auf dem Lehrplan **„Informationstechnologie“** lässt sich analysieren, wie die Inhalte der Stufen 1 bis 5 im vorliegenden Lehrplan berücksichtigt sind. Der IT-Lehrplan enthält einen dezidierten Pflichtgegenstand namens **"IT-Sicherheit"**, der im 1. und 2. Jahrgang mit jeweils einer Wochenstunde unterrichtet wird. Dieser Gegenstand ist in allen alternativen Ausbildungsschwerpunkten (Standard, Netzwerktechnik, Medientechnik) als Pflichtgegenstand im 1. und 2. Jahrgang vorgesehen.

Stufen 1 und 2 (Allgemeine Einführung & Exploratory):

- Der Lehrstoff des Pflichtgegenstands „IT-Sicherheit“ im 1. Jahrgang deckt Bereiche wie „Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien, Schutz personenbezogener Daten, Grundbegriffe und Strategien der Datensicherheit, Social Engineering“ ab. Dies korreliert stark mit den Inhalten der Stufe 1 des CLEMENTINE-6-Stufen-Modells.
- Im 2. Jahrgang werden Themen wie „gesicherte Informationsquellen für aktuelle Sicherheitsbedrohungen“, „Datenspuren“, „Privatsphäre im Internet“, „digitale Identität“, „Grundlagen der Kryptographie“, „Grundlagen der Verschlüsselung und des Hashing“ behandelt. Zudem werden „Benutzerverwaltung“, „grundlegende Berechtigungskonzepte“, „sichere Authentifizierung“, „sichere Verbindungen“, „Werkzeuge der Netzwerksicherheit“, „Zugriffsprotokolle“, „Werkzeuge zur Verschlüsselung“ und „Schadsoftwareschutz“ als Lehrstoff genannt. Diese Inhalte entsprechen weitgehend den Themen der Stufe 2 des CLEMENTINE-6-Stufen-Modells.

Stufe 3 (Foundational): Diese Stufe ist für IT- und Informatikschwerpunkte konzipiert. Der Lehrplan behandelt diverse Stufe-3-relevante Themen, verteilt auf verschiedene technische Pflichtgegenstände:

- **Vertraulichkeit und Integrität mit technischer Tiefe:** Grundlagen der Kryptographie und Hashing sind im Fach "IT-Sicherheit“ im 2. Jahrgang enthalten. Weiterführende mathematische Konzepte von Verschlüsselungs- und Hashfunktionen sowie VPN-Implementierungen finden sich im Lehrstoff des Bereichs "Datenintegrität und Vertraulichkeit" in der Spezialisierung „Netzwerktechnik“ im 5. Jahrgang.
- **Authentifizierung und Autorisierung:** Grundlegende Konzepte sind in „IT-Sicherheit“ (2. Jahrgang) enthalten. Detailliertere Berechtigungskonzepte, Benutzer- und Rollenverwaltung sowie Zugriffsprotokolle finden sich auch im Fach „Informationssysteme“ (4. Jahrgang) und „Systemtechnik“

(Betriebssysteme). Die Implementierung von PKI-Systemen wird in der Spezialisierung „Netzwerktechnik“ im 5. Jahrgang genannt.

- **Sichere Kommunikation (VPN, Firewalls, etc.):** VPN-Realisierungen und Firewall-Architekturen/Implementierungen werden im Fach „Systemtechnik“ (5. Jahrgang) und in der Spezialisierung „Netzwerktechnik“ (5. Jahrgang) behandelt. Sichere Verbindungen sind auch im Fach „IT-Sicherheit“ (2. Jahrgang) erwähnt.
- **Sichere Konfiguration von Betriebssystemen und Diensten:** Konfiguration und Wartung von Serversystemen und Diensten sowie Virtualisierung werden im Fach „Systemtechnik“ (3. und 4. Jahrgang) behandelt. Gerätehärtung wird in der Spezialisierung „Netzwerktechnik“ (4. Jahrgang) erwähnt.
- **Sichere Infrastruktur:** Umsetzung von Sicherheitskonzepten in Unternehmensnetzwerken und Realisierung ausfallsicherer Systemarchitekturen wird im Fach „Systemtechnik“ (4. Jahrgang) sowie in der Spezialisierung „Netzwerktechnik“ (4. und 5. Jahrgang) genannt. Backupstrategien sind im Fach „Informationssysteme“ und „Systemtechnik“ vorgesehen.
- **Sicherheitsmanagement und -prozesse:** Grundlegende rechtliche Rahmenbedingungen sind in IT-Sicherheit (1. Jahrgang) enthalten. Datenschutzgesetze und Normen (Urheberrecht, DSGVO-ähnliche Konzepte) werden auch in „Informationssystemen“ und in der Spezialisierung „Medientechnik“ (5. Jahrgang) behandelt. Qualitätsmanagement (inkl. Normen wie ISO 27001, obwohl nicht explizit benannt) ist Teil der „Informationstechnischen Projekte“. Risikomanagement ist im Fach „Informationstechnische Projekte“ und in der Spezialisierung „Netzwerktechnik“ (4. Jahrgang) enthalten.

Stufe 4 (Professional): Diese Stufe zielt auf Angriffsmuster und Verteidigungsmaßnahmen ab und ist für IT-Schwerpunkte. Einige Inhalte finden sich im IT-Lehrplan, aber nicht alle Bereiche der Stufe 4 scheinen umfassend abgedeckt:

- **Sichere Softwareentwicklung:** Testen und Fehlersuche sind Bestandteile der „Softwareentwicklung“. Explizite Nennungen von Standards (NIST, Audits, Safety), Verschlüsselung/Hashing *im Code*, sowie formale Verifikation, statische/dynamische Code-Analysen, das Finden von Schwachstellen (Buffer Overflows, Memory Corruptions, Fuzzing, Delta Debugging) und spezifische Schutzmaßnahmen (Injections, CFI, ASLR) scheinen im „Softwareentwicklungs“-Lehrstoffs **nicht enthalten** zu sein.
- **Sichere Webentwicklung:** Web-Technologien werden in der Spezialisierung „Medientechnik“ behandelt. Allerdings werden Standards (ISO 25000, ÖNORM A7700), Verschlüsselung/Hashing *in Webanwendungen*, Authentifizierungsmethoden *bei Webanwendungen*, spezifische Angriffsvektoren (WAF Top 10) und Gegenmaßnahmen (WAF) in „Medientechnik“ **nicht explizit genannt**.
- **Monitoring und BigData:** Log-Analyse ist in „IT-Sicherheit“ und „Netzwerktechnik“ enthalten. Netzwerk-Angriffsvektoren erkennen (IDS) und Intrusion Prevention Systems (IPS) werden in der Spezialisierung „Netzwerktechnik“erwähnt. Die explizite Nutzung von spezifischen Werkzeugen (SIEM, ELK etc.) oder automatisierten Verhaltensanalysen/Anomalieerkennung (mittels Artificial Intelligence - AI) ist **nicht detailliert aufgeführt**.

Stufe 5 (Excellence): Diese Stufe ist für spezialisierte Cybersecurity-Ausbildungen vorgesehen. Der HTL-Lehrplan ist ein allgemeiner IT-Lehrplan, keine Cybersecurity-Spezialisierung.

- **Digitale Forensik:** „Forensic“ wird als Lehrstoff im Bereich „Netzwerksicherheit“ in der Spezialisierung „Netzwerktechnik“ im 4. Jahrgang genannt. Es werden jedoch **keine Details** zu Incident-Response-Zyklen, Beweismittelsicherung, Offline-Analyse-Techniken (Speicherdumps, Prozessanalyse, Dateisystemanalyse, File Carving, Timestamps), oder dem Nachvollziehen von Angriffen (Backtracking) gegeben.
- **Reverse Engineering:** Konzepte wie statische/dynamische Analyse, Malware-Analyse, Debugger, Disassemblierung oder Deobfuscation werden **nicht erwähnt**.

Zusammenfassend berücksichtigt der vorliegende HTL-Lehrplan die Inhalte des CLEMENTINE-6-Stufen-Modells in unterschiedlichem Ausmaß:

- **Die Stufen 1 und 2 werden im Pflichtgegenstand „IT-Sicherheit“ im 1. und 2. Jahrgang weitgehend abgedeckt** und erfüllen damit die Anforderung des Modells an alle Schultypen der Sekundarstufe II.

- **Wesentliche Aspekte der Stufe 3 (Foundational) werden im Lehrplan behandelt**, sind aber über verschiedene technische Fächer verteilt (Systemtechnik, Informationssysteme, Netzwerktechnik, Informationstechnische Projekte).
- **Teile der Stufe 4 (Professional) sind vorhanden**, insbesondere in Bezug auf Netzwerksicherheit. Bereiche wie sichere Software- und Webentwicklung sowie detaillierte Monitoring-Techniken, wie in Stufe 4 beschrieben, **scheinen jedoch in den vorliegenden Auszügen nicht oder nicht umfassend aufgeführt zu sein**.
- **Die Inhalte der Stufe 5 (Excellence) werden im allgemeinen IT-Lehrplan, basierend auf den vorliegenden Auszügen, praktisch nicht behandelt**, was mit der Einordnung dieser Stufe für hochspezialisierte Ausbildungen übereinstimmt.

Die didaktischen Grundsätze des Fachs „IT-Sicherheit“, die betonen, dass IT-Sicherheit ein wesentlicher Teil in *allen* fachlichen Gegenständen ist, deuten darauf hin, dass einige Sicherheitsaspekte möglicherweise auch implizit in anderen Fächern behandelt werden, selbst wenn sie im Lehrstoff nicht explizit mit dem Begriff "Sicherheit" verbunden sind (z.B. bei der Konfiguration von Systemen oder der Entwicklung von Anwendungen). Die expliziten Lehrstoffbeschreibungen zeigen jedoch die oben genannten Abdeckungen.

5.5.9 Angewandte Informatik und fachspezifische Informationstechnik

Der Gegenstand „Angewandte Informatik und fachspezifische Informationstechnik“ wird ausschließlich im Lehrplan **Mechatronik** verwendet.

Der Mechatronik Lehrplan ist eine umfassende technische Ausbildung, die Mechanik, Elektrotechnik und Informatik verbindet. Relevante Inhalte zum Thema IT-Sicherheit und Cybersecurity sind primär im Pflichtgegenstand "**Angewandte Informatik und fachspezifische Informationstechnik**" sowie teilweise in anderen Fächern zu finden.

5.5.9.1 Lehrplananpassungen

Der Mechatronik-Lehrplan enthält relevante Grundlagen in Angewandter Informatik und rechtlichen/gesellschaftlichen Aspekten der IT, die den Anforderungen der Stufe 1 (und damit auch Stufe 0) des *CLEMENTINE*-6-Stufen-Modells entsprechen. Dedizierte, technisch tiefergehende Cybersecurity-Inhalte im Sinne der Stufen 2 bis 5 des *CLEMENTINE*-6-Stufen-Modells (z.B. Angriffs- und Verteidigungsmethoden, sichere Softwareentwicklung, Forensik) sind in den vorliegenden Auszügen des Lehrplans **nicht detailliert aufgeführt**. Der Lehrplan konzentriert sich in den IT-Bereichen stark auf die Anwendung in mechatronischen und Automatisierungssystemen.

Es sollten daher folgende Inhalte hinzugefügt bzw. im Sinne der Cybersecurity besser im Lehrplan sichtbar gemacht werden:

1. Jahrgang - 1. und 2. Semester:

Pflichtfach „Angewandte Informatik und fachspezifische Informationstechnik“:

- Integration einer kurzen Einheit zur **Wiederholung und Festigung des technologischen Grundverständnisses aus der Sekundarstufe I**, insbesondere im Hinblick auf die Funktionsweise von Computern und Netzwerken (basierend auf Punkt 1.0 des CLEMENTINE-6-Stufen-Modells – siehe Appendix). Dies könnte als Einführung in die später folgenden Informatik-Themen dienen.
- Thematisierung der **Verfügbarkeit von Daten und Systemen**: Die Bedeutung von **Datensicherungen (Backups)** und verschiedene Arten von Backup-Medien.
- Explizite Behandlung des Themas **„Richtiges Verhalten im Umgang mit (vor allem personenbezogenen) Daten“**. Dies sollte über die reine Datensicherung hinausgehen und auch Aspekte des Datenschutzes im Alltag umfassen.
- Einführung in das **Erkennen von grundlegenden Risiken im digitalen Raum**, beispielsweise durch einfache Beispiele für Schadsoftware und betrügerische E-Mails.
- Beginn der **Motivation zur Sicherheit** durch kurze **Fallbeispiele (z.B. Keylogger-Video)** und die grundlegende Unterscheidung zwischen **„guten“ und „bösen“ Hackern (Ethical Hacking)**.
- Vertiefung des **„richtigen Verhaltens im digitalen Raum“** mit konkreten Anleitungen zu sicherer Passwortwahl und -verwaltung, sicherem Surfen im Internet und dem Erkennen von Phishing-E-Mails und gefährlichen E-Mail-Anhängen.
- Erste Einführung in **Angriffsmethoden zur Informationsweitergabe**, zumindest die **Grundlagen von Phishing** (ohne detaillierte technische Analyse).

- Behandlung von **Datensicherheit und Datenschutz**. Hier sollten die rechtlichen Rahmenbedingungen (DSGVO etc.) detailliert behandelt und in Bezug zur technischen Umsetzung von Sicherheitsmaßnahmen gesetzt werden.
- Behandlung des Themas **„Was tun im Notfall?“**: **Richtig reagieren bei Sicherheitsvorfällen**, Kenntnis wichtiger Ansprechpartner und grundlegende Schritte zur **Infektionsbeseitigung**.
- Einführung in grundlegende Konzepte von **Vertraulichkeit und Integrität**: Wie funktioniert Verschlüsselung konzeptionell (ohne technische Tiefe)? Wie funktioniert eine Hashfunktion konzeptionell (ohne technische Tiefe)?

3. Jahrgang - 5. Semester:

Pflichtfach „**Wirtschaft und Recht“:**

- Die rechtlichen Rahmenbedingungen (DSGVO) im Umgang mit personenbezogenen Daten vertiefen.
- Einführung in **IT-Grundschutz und Normen** wie **ISO 27001 (grundlegende Konzepte und Bedeutung)**.
- Vertiefung der **rechtlichen Rahmenbedingungen und Normen**: Grundlagen des **Urheberrechts im digitalen Kontext**. Überblick über relevante Gesetze wie das **Telekommunikationsgesetz** (in vereinfachter Form). Erste Einführung in **IT-Grundschutzkonzepte**.

In den verschiedenen fachspezifischen Gegenständen wie „Mechatronische Systeme“ und „Automatisierung“, wie auch in höheren Jahrgängen der Angewandte Informatik und fachspezifische Informationstechnik sollten die Grundlagen der Cybersecurity aus Stufe 1 und 2 immer wieder kontextbezogen aufgegriffen und angewendet werden, um das Bewusstsein für Sicherheit in allen Bereichen der Mechatronik zu schärfen. Dies könnte in Form von Projektarbeiten oder Fallstudien erfolgen, die auch Aspekte der sicheren Kommunikation, des sicheren Umgangs mit Daten in industriellen Steuerungssystemen und der Bedeutung von Backups für kritische Systeme beinhalten.

5.5.9.2 Zusammenfassende Analyse

Die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells sind im vorliegenden Lehrplan für Mechatronik bereits in verschiedenen Unterrichtsgegenständen und Kompetenzbereichen auf allgemeine Weise berücksichtigt, auch wenn eine explizite und umfassende Behandlung aus der Perspektive der Cybersecurity nicht immer gegeben ist.

Stufe 1: Allgemeine Einführung & Motivation

- Ein **technologisches Grundverständnis** wird durch das Fach „**Angewandte Informatik und fachspezifische Informationstechnologie**“ vermittelt.
- Das **richtige Verhalten im Umgang mit Daten** wird implizit in **Angewandter Informatik** angesprochen, beispielsweise beim Thema **Datensicherung** und **Schutz vor unberechtigtem Zugriff**.
- Das **Erkennen von Risiken** wird in **Angewandter Informatik** im Kontext der **gesellschaftlichen Auswirkungen von Informationstechnologien** und beim Thema **Virenschutz** und **Firewalls** berührt.
- Die **Motivation zur Sicherheit** in Form von expliziten Fallbeispielen, Identitätsdiebstahl oder Social Engineering ist **nicht explizit** als eigener Lerninhalt ausgewiesen. Jedoch kann die Auseinandersetzung mit den **gesellschaftlichen Auswirkungen von Informationstechnologien** (Angewandte Informatik) eine implizite Motivation schaffen.

Stufe 2: „Exploratory“: Tiefergehende Awareness für Berufe mit IKT-Anwendungsaspekten, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen

- Eine allgemeine **Awareness für Berufe mit IKT-Anwendungsaspekten** kann durch den gesamten Lehrplan und die vermittelten breiten Kompetenzen im Bereich der Mechatronik entstehen, jedoch ist eine spezifische, **explorative Sensibilisierung für Cybersecurity-Berufe nicht vorgesehen**.
- Aspekte der **persönlichen Sicherheit im digitalen Raum** (sichere Passwortwahl, sicheres Surfen etc.) werden **nicht explizit** als eigene Lerninhalte behandelt.
- **Rechtliche Rahmenbedingungen und Normen** werden im Fach „**Wirtschaft und Recht“** behandelt. In „**Angewandter Informatik“** werden Grundlagen des **Datenschutz- und Telekommunikationsgesetzes**, **Urheberrecht** und **Lizenzverträge** angesprochen. Dies deckt **grundlegende Aspekte ab**, jedoch ist eine umfassende und direkt auf IT-Sicherheit ausgerichtete

Behandlung der relevanten Rechtsgrundlagen und Normen (wie DSGVO im Detail oder IT-Sicherheitsgesetz) **nicht explizit** dargelegt.

Der Lehrplan für Mechatronik vermittelt **Grundlagen in verschiedenen informationstechnischen Bereichen**, die auch für die Cybersecurity relevant sind. Jedoch werden die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells **nicht systematisch und explizit aus der Perspektive der Cybersecurity** behandelt. Viele Aspekte werden implizit oder in einem anderen Kontext (z.B. Datenschutz im allgemeinen Rechtsrahmen) angesprochen, aber eine dedizierte Cybersecurity-Grundbildung, die Motivation und persönliche Sicherheit umfassend abdeckt, ist im vorliegenden Lehrplan **nicht explizit verankert**.

5.5.10 Informatik und Informationssysteme

Der Gegenstand "Informatik und Informationssysteme" wird in allen **Wirtschaftsingenieur (WI)-Lehrplänen** (Rohstoff- und Energietechnik, Bekleidungstechnik, Betriebsinformatik, Holztechnik, Logistik, Maschinenbau, Technisches Management, Produktmanagement Futuretecs, Informationstechnologie und Smart Production) verwendet.

Die Anpassung und Verankerung von **Cybersecurity-Inhalten** in den Lehrplänen zeigt jedoch eine zweigspezifische Gewichtung, wobei fundamentale Aspekte in allen Fachrichtungen als Basis vorhanden sind, während spezielle IT-nahe Ausbildungen deutlich tiefergehende Kompetenzen vermitteln.

5.5.10.1 Lehrplananpassungen

Basierend auf den Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells, sollte der Lehrstoff im Fach **„Informatik und Informationssysteme"** in den **ersten beiden Jahrgängen (1. und 2. Jahrgang), entsprechend dem 1. bis 4. Semester**, explizit um folgende Inhalte ergänzt werden:

1. Jahrgang - 1. und 2. Semester:

Pflichtfach „Informatik und Informationssysteme":

- **Einführung in die Informationssicherheit:** Warum ist IT-Sicherheit wichtig? [Nicht explizit im Lehrstoff der frühen Jahre genannt].
- **Grundlegende Schutzziele:** Explizite Nennung und einfaches Verständnis von **Vertraulichkeit, Integrität und Verfügbarkeit** als Kernziele der Sicherheit im digitalen Raum [Nicht explizit im Lehrstoff der frühen Jahre genannt].
- **Erste Schritte zur Bedrohungserkennung:** Bewusstsein für gängige Bedrohungen auf Anwenderebene (z.B. Viren, Malware – einfache Definition) [Virenschutz ist teilweise implizit oder später genannt].
- **Basis-Schutzmaßnahmen für Anwender:**
  - Die Bedeutung und das Prinzip **sicherer Passwörter** [Nicht explizit im Lehrstoff der frühen Jahre genannt].
  - Verantwortungsvoller Umgang mit Informationen und digitalen Medien [Grundlagen der IT-Nutzung sind genannt].
  - Einfaches Verständnis von Software-Updates und deren Notwendigkeit [Updates sind teilweise genannt].
- **Grundlagen des Umgangs mit Daten:**
  - Wichtigkeit des **regelmäßigen Speicherns** von Daten.
  - Das Prinzip der **Datensicherung (Backup)**: Warum macht man Backups? [Datensicherung ist teilweise genannt, z.B. im 2. Jahrgang Werkstätte bei WI Betriebsinformatik].
- **Grundlegende rechtliche und gesellschaftliche Aspekte:**
  - Einführung in das Konzept des **Datenschutzes** und den verantwortungsvollen Umgang mit eigenen und fremden Daten im digitalen Raum [Grundlagen des DSG/TKG oder DSGVO-Details sind oft erst später genannt].
  - Die Bedeutung von **Urheberrecht** und die verantwortungsvolle Nutzung digitaler Inhalte [Urheberrecht ist teilweise genannt, aber oft im Kontext von Wirtschaftsrecht].
  - Basis-Verständnis von **Netiquette** und ethischem Verhalten online [Nicht explizit im Lehrstoff genannt].

2. Jahrgang - 3. und 4. Semester:

Pflichtfach „Informatik und Informationssysteme":

- **Erweiterte Bedrohungserkennung:** Explizite Nennung und Erkennung von Bedrohungen wie **Phishing, Social Engineering, Ransomware** [Nicht explizit im Lehrstoff der frühen Jahre genannt].
- **Detailliertere Schutzmaßnahmen für Anwender:innen:**
  - Methoden zur sicheren **Passwortverwaltung** (z.B. Passwort-Manager) [Nicht explizit im Lehrstoff der frühen Jahre genannt].
  - Verständnis und Nutzung der **Multi-Faktor-Authentifizierung (MFA)** [Nicht explizit im Lehrstoff der frühen Jahre genannt].
  - Sicheres Surfen: Erkennen von **sicheren Verbindungen (HTTPS)** [Nicht explizit im Lehrstoff der frühen Jahre genannt] und Risiken unsicherer Webseiten.
  - Sicherer Umgang mit E-Mails und Dateianhängen [Nicht explizit im Lehrstoff der frühen Jahre genannt].
  - Grundprinzipien von Firewalls aus Anwender:innensicht [Updates und Virenschutz sind teilweise genannt z.B.].
- **Datensicherung und Wiederherstellung (Vertiefung):**
  - Verschiedene **Medien für Backups**.
  - Grundlegende **Strategien zur Wiederherstellung** von Daten nach einem Datenverlust [Nicht explizit als Lehrstoff aufgeführt in den frühen Jahren].
- **Datenschutz (Vertiefung auf Anwenderebene):**
  - Grundlagen der **Datenschutz-Grundverordnung (DSGVO)** bezogen auf die Rechte der Nutzer:innen und den Umgang mit deren Daten [Grundlagen des DSG/TKG sind teilweise genannt, DSGVO-Details oft erst später oder nicht explizit in der Informatik.
  - Umgang mit persönlichen Daten in Sozialen Medien und Online-Diensten [Nicht explizit im Lehrstoff genannt].
- **Sicherheit im Netzwerk (Grundlagen für Anwender:innen):**
  - Risiken der Nutzung **öffentlicher WLANs** [Nicht explizit im Lehrstoff genannt].
  - Einfaches Verständnis von **VPN (Virtual Private Network)** und dessen Nutzen für sichere Verbindungen [Nicht explizit im Lehrstoff genannt].
  - Sicheres Teilen von Dateien in Netzwerken.
- **Rechtliche und gesellschaftliche Aspekte:**
  - Konsequenzen von Urheberrechtsverletzungen.
  - Unterschiedliche Arten von Software-Lizenzen (Open Source vs. kommerziell).
  - Konzept des „digitalen Fußabdrucks“ und Online-Reputation [Nicht explizit im Lehrstoff genannt].

Die Aufnahme dieser expliziten Lernziele und Lehrstoffinhalte in den Lehrplänen für die ersten beiden Jahrgänge (1.-4. Semester) im Rahmen des einführenden IT-Gegenstandes würde eine klare Abdeckung der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells sicherstellen, was für alle Wirtschaftsingenieur-Fachrichtungen als Grundlage notwendig ist.

5.5.10.2 Zusammenfassende Analyse

Der Gegenstand „Informatik und Informationssysteme“ oder ähnliche Bezeichnungen wie „Angewandte Informatik“, „Netzwerke und Embedded Software“, „Systemkonzeption, Sicherheit und IT-Recht“ findet sich in den vorliegenden Auszügen aller Wirtschaftsingenieurlehrpläne, wenn auch mit unterschiedlicher Ausgestaltung und Tiefe.

Gemeinsamkeiten hinsichtlich Cybersecurity-relevanter Inhalte ist in fast allen Wirtschaftsingenieurlehrplänen im Rahmen des Pflichtgegenstandes „Angewandte Informatik“ oder „Informatik und Informationssysteme" im ersten oder zweiten Jahrgang verankert:

- **Datensicherheit Grundlagen:** Die meisten Lehrpläne listen explizit **„Datensicherheit“** als Lehrstoff im Bereich Angewandte Informatik auf. Dieser Lehrstoff umfasst typischerweise **Virenschutz, Firewalls, Updates, Service Packs und Digitale Signatur**. Die Bildungs- und Lehraufgabe in diesem Bereich zielt darauf ab, dass die Absolventinnen und Absolventen Richtlinien des Datenschutzes und der Datensicherheit berücksichtigen können.
- **Rechtliche und gesellschaftliche Aspekte:** Alle vorgelegten Lehrpläne der Wirtschaftsingenieure enthalten im Bereich Angewandte Informatik oder Informatik und Informationssysteme das Thema **„rechtliche und gesellschaftliche Aspekte“** im Umfeld der Informationstechnologie. Der Lehrstoff nennt dabei **Grundsätze des Datenschutz- und Telekommunikationsgesetzes**, die Bedeutung des Urheberrechts, Copyright und Lizenzverträge. Auch im Bereich Wirtschafts- und Steuerrecht, der in allen WI-Lehrplänen vorkommt, ist die Fähigkeit genannt, festzustellen, ob Internetauftritte den rechtlichen Vorgaben entsprechen. Dies entspricht Aspekten der **Stufen 1 und 2**, insbesondere den rechtlichen Grundlagen.

- **Netzwerkgrundlagen mit Sicherheitsaspekt:** Die Nutzung von Netzwerkressourcen und das Benennen/Einsetzen von Netzwerkkomponenten sowie die Identifizierung von Problemen im Netzwerk sind Teil des Lehrplans im Bereich Angewandte Informatik in höheren Jahrgängen (z.B. 6. Semester/3. oder 4. Jahrgang). Der Lehrstoff zum Thema Netzwerke listet dabei explizit **"Sicherheit"** als Unterpunkt auf, was ein Bewusstsein für dieses Thema schafft, auch wenn die Tiefe variieren kann.
- **Umgang mit Daten:** Grundlegende Fähigkeiten im Umgang mit Daten, Datenverwaltung und Datensicherung werden in den ersten Jahrgängen gelehrt. Dies ist eine Basis für die Datensicherheit.
- **Praktische Sicherheitsaspekte:** Im Rahmen von Laborbetrieb und Werkstätten in verschiedenen Disziplinen werden allgemeine Sicherheitsvorschriften und Sicherheitsunterweisungen behandelt. Obwohl dies nicht primär *Cyber*-Sicherheit ist, gehört es zum breiteren Sicherheitsverständnis in technischen Berufen.

Diese Gemeinsamkeiten entsprechen im Wesentlichen den Inhalten der **Stufen 1 und 2** des CLEMENTINE-6-Stufen-Modells, die als allgemeine Kompetenzstufen für alle Schultypen der Sekundarstufe II gelten. Dazu gehören Grundbegriffe der Datensicherheit, Umgang mit Daten, sowie tiefergehende Awareness für rechtliche Rahmenbedingungen (DSGVO etc.) und grundlegende Netzwerksicherheitstools.

Alle vorgelegten Wirtschaftsingenieurlehrpläne teilen ein grundlegendes Curriculum im Bereich „Informatik und Informationssysteme“, dass die Basiselemente der IT-Nutzung, Datenverwaltung, grundlegende Datensicherheit (Virenschutz, Firewalls, Updates) und die relevanten rechtlichen und gesellschaftlichen Rahmenbedingungen (Datenschutz, Urheberrecht) abdeckt. Diese Inhalte entsprechen im Wesentlichen der notwendigen **Grundlagen- und Awareness-Stufe.**

Eine signifikant **tiefere und technischere Behandlung** von Cybersecurity-Themen findet sich jedoch spezifisch in den Lehrplänen der **Wirtschaftsingenieure – Betriebsinformatik** und insbesondere der **Wirtschaftsingenieure – Informationstechnologie und Smart Production**. Diese Lehrpläne integrieren dedizierte Bereiche zur Netzwerksicherheit, Kryptografie, Systemkonzeption mit Sicherheitsaspekten, Datenschutzkonzepten und sogar explizite Themen wie Bedrohungen, Angriffe und Angriffsszenarien.

Dies positioniert diese beiden Fachrichtungen klar auf einer höheren Stufe der Cybersecurity-Kompetenz (Teile von **Stufe 3 und Ansätze von Stufe 4** im CLEMENTINE-6-Stufen-Modell) im Vergleich zu den anderen hier analysierten Wirtschaftsingenieur-Lehrplänen, die sich stärker auf die Anwendung von IT in ihrem jeweiligen Fachgebiet konzentrieren und die Cybersecurity-Inhalte auf einer fundamentaleren Ebene behandeln.

5.5.11 Informatik, Projekt und Qualitätsmanagement

Der Gegenstand „Informatik, Projekt und Qualitätsmanagement“ wird ausschließlich im Lehrplan **Material- und Umwelttechnologie** verwendet.

Der Lehrplan für Material- und Umwelttechnologie vermittelt im Rahmen des Fachs „Informatik, Projekt und Qualitätsmanagement“ vor allem im Bereich „Angewandte Informatik“ grundlegende Konzepte der IT-Sicherheit und des verantwortungsvollen Umgangs mit Daten. Diese Inhalte legen eine Basis, die mit den Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells angepasst werden müssen.

5.5.11.1 Lehrplananpassungen

Das Einfügen der fehlenden Inhalte aus Stufe 1 und 2 bedeuten primär eine **Stärkung der Grundlagen in Cybersecurity-Awareness und persönlicher IT-Sicherheit** für alle Schüler:innen der Material- und Umwelttechnologie. Diese Inhalte passen gut in das bestehende Fach **„Informatik, Projekt- und Qualitätsmanagement“**, insbesondere in die Abschnitte zur Angewandten Informatik. Angesichts dessen, dass Stufe 1 und 2 des CLEMENTINE-6-Stufen-Modells als „allgemeine Kompetenzstufen“ konzipiert sind, wäre eine Integration in den **1. und 2. Jahrgang** dieses Fachs am sinnvollsten.

1. Jahrgang - 1. und 2. Semester:

Pflichtfach "Informatik, Projekt- und Qualitätsmanagement" – Bereich Angewandte Informatik:

- **Vertiefung Datensicherheit/Grundverständnis:** Grundlegende Bedrohungsarten (Viren, Würmer, Phishing – Fokus: Erkennung und Vermeidung). Einfache Fallbeispiele zu Identitätsdiebstahl und Social Engineering. Bedeutung sicherer Passwörter und einfacher Schutzmaßnahmen.
- **Grundlagen Notfallverhalten:** Wer ist Ansprechpartner bei IT-Problemen? Basis-Verhalten bei Verdacht auf Infektion.

- **Grundlagen Recht:** Wiederholung/Verankerung der bereits genannten „gesetzlichen Rahmenbedingungen“ im Kontext des Umgangs mit Daten und den besprochenen Bedrohungen.
- **Zusätzliche Bildungs- und Lehraufgaben (Fähigkeiten):**
  - Einfache Bedrohungen erkennen und grundlegende Schutzmaßnahmen anwenden.
  - Sicheres Verhalten im digitalen Raum demonstrieren (Passwortmanagement, Umgang mit E-Mails/Links).
  - Grundlegendes Verhalten im Falle eines IT-Sicherheitsproblems beschreiben.

2. Jahrgang - 3. und 4. Semester:

Pflichtfach „Informatik, Projekt- und Qualitätsmanagement“ – Bereich Angewandte Informatik:

- **Persönliche Sicherheit:** Absicherung privater Geräte und Online-Konten, sicheres Surfen, digitale Fußabdrücke.
- **Grundlagen Vertraulichkeit/Integrität:** Einfache, nicht-technische Erklärung von Verschlüsselung (Warum brauche ich sie? Was macht sie?) und Hash-Funktionen (Was ist ein digitaler Fingerabdruck?). Kontext: E-Mail-Sicherheit (Signatur vs. Verschlüsselung), sichere Verbindungen (HTTPS - sehr grundlegend).
- **Vertiefung Recht/Normen:** Konkretere Beispiele zu rechtlichen Implikationen von Datennutzung und Internetverhalten (z.B. Filesharing, Cybermobbing, Urheberrecht - wo relevant für Endnutzer). Bezug zu Normen wie ISO 27001 (sehr grundlegend: Was sind Informationssicherheits-Managementsysteme, warum sind sie wichtig?).
- **Zusätzliche Bildungs- und Lehraufgaben (Fähigkeiten):**
  - Maßnahmen zur Erhöhung der persönlichen IT-Sicherheit im Alltag anwenden.
  - Die grundlegende Funktionsweise von Verschlüsselung und Hashing erklären (ohne technische Details).
  - Die Bedeutung rechtlicher und normativer Vorgaben für den Umgang mit IT verstehen und erklären.

3. Jahrgang - 5. und 6. Semester:

Pflichtfach „Informatik, Projekt- und Qualitätsmanagement“ – Bereich Angewandte Informatik:

In diesem Jahrgang wird Netzwerksicherheit („Sicherheit“ unter Lehrstoff Netzwerke) eingeführt. Dies wäre ein Ort, um die Stufe 1 und 2 Inhalte **anzuwenden und zu vertiefen**, z.B. durch das Erkennen von Bedrohungen im Netzwerk-Kontext oder die Anwendung rechtlicher Aspekte auf Netzwerke. Die Hauptintegration der fehlenden Stufe 1 & 2 Inhalte sollte jedoch in den Jahrgängen 1 und 2 erfolgen, um die Grundlage frühzeitig zu schaffen.

Die Integration dieser Inhalte erfordert möglicherweise eine **Neugewichtung** innerhalb **der bestehenden Stunden** im Fach „Informatik, Projekt- und Qualitätsmanagement“. Da es sich bei den fehlenden Inhalten von Stufe 1 und 2 überwiegend um theoretische/Awareness-Themen handelt, könnte dies im Rahmen der vorhandenen Stunden (2 Wochenstunden pro Semester im 1. und 2. Jahrgang) umsetzbar sein, erfordert aber eine sorgfältige didaktische Planung.

Es würde das fachbezogene **Qualifikationsprofil** der Absolvent:innen im Bereich „Angewandte Informatik“ erweitern, indem nicht nur die Nutzung von IT-Systemen, sondern auch deren sichere und rechtskonforme Anwendung betont wird.

Zusammenfassend lässt sich sagen, dass der vorliegende Lehrplan im Fach „Informatik, Projekt- und Qualitätsmanagement“ einige Aspekte von Stufe 1 (Datensicherheit, rechtliche Rahmenbedingungen) und Stufe 2 (rechtliche Rahmenbedingungen) bereits abdeckt. Wesentliche, insbesondere motivational und Awareness-bezogene Inhalte aus Stufe 1 sowie persönliche Sicherheit und grundlegende technische Konzepte (Verschlüsselung/Hashing) aus Stufe 2 fehlen jedoch explizit.

Das Einfügen dieser fehlenden Teile in den 1. und 2. Jahrgang würde das Fundament für Cybersecurity-Kompetenzen gemäß dem CLEMENTINE-6-Stufen-Modell legen und die Schüler:innen besser auf die Herausforderungen der digitalen Welt vorbereiten, ohne dass dies voraussichtlich massive strukturelle Änderungen oder Stundenaufstockungen erfordern würde, sondern eher eine Neuausrichtung und Konkretisierung bestehender Lehrstoffbereiche.

5.5.11.2 Zusammenfassende Analyse

Im Lehrplan für Material- und Umwelttechnologie, Gegenstand „Informatik, Projekt- und Qualitätsmanagement“, finden sich folgende relevante Punkte in den frühen Jahrgängen. Ein grundlegendes Verständnis für Datenhandling, rechtliche Rahmenbedingungen und Normen ist vorhanden. Wichtige Themen zur Motivation und Bewusstseinsbildung, wie Bedrohungsarten, Angriffsmuster, Social Engineering und Notfallverhalten, fehlen weitgehend oder werden nur allgemein erwähnt. Konzepte zur persönlichen Sicherheit sowie die nicht-technische Erklärung von Verschlüsselung und Hashing werden jedoch nicht explizit genannt.

1. Jahrgang - 1. und 2. Semester:

Stufe 1: Allgemeine Einführung & Motivation:

- Der Punkt „**Das richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten**“ wird explizit durch den Lehrstoff „Datensicherheit“ und die genannte Fähigkeit abgedeckt.
- Auch das technologische Grundverständnis ist durch die generellen Inhalte des Gegenstands (Hardware, Betriebssysteme, Anwendungen) im Bereich Angewandte Informatik implizit vorhanden.
- **Das Erkennen von Risiken und Reaktionsgrundsätze** ist in den frühen Jahrgängen **nicht explizit** als Lehrstoff oder Fähigkeit aufgeführt.
- Die spezifischen Themen der **„Motivation zur Sicherheit“** wie Schadsoftware, Hacker, Identitätsdiebstahl, konkrete Bedrohungen/Angriffsvektoren, Social Engineering oder Verhalten im Notfall sind in diesem Abschnitt des Lehrplans **nicht genannt**.
- Der Schutz personenbezogener Daten wird zwar im 1. Jahrgang im Zusammenhang mit gesetzlichen Rahmenbedingungen erwähnt, aber die tiefergehenden Aspekte der Bedrohungen und Angriffsvektoren fehlen.

2. Jahrgang - 3. und 4. Semester:

- Im 4. Semester: Lehrstoff „**rechtliche und gesellschaftliche Aspekte im Umfeld der Informationstechnik**“.

3. Jahrgang - 5. und 6. Semester:

- **Im 6. Semester:** Bildungs- und Lehraufgabe: Fähigkeit, „**im Netzwerk auftretende Probleme identifizieren**“ zu können. Lehrstoff: „Netzwerke (Komponenten und Protokolle, Adressierung, Netzwerkdienste, **Sicherheit**)“.

Zusammenfassende Bewertung Stufe 1: Grundlegendes Verständnis des Umgangs mit Daten und rechtliche Rahmenbedingungen sind vorhanden. Die umfassenden, zur **Motivation und Bewusstseinsbildung** essenziellen Themen wie Bedrohungsarten, Angriffsmuster (auch grundlegend), Social Engineering und konkretes Verhalten im Notfall sind im Fach „Informatik, Projekt- und Qualitätsmanagement“ in den frühen Jahren **weitgehend fehlend oder nur sehr allgemein angedeutet**.

Stufe 2: „Exploratory“ - Tiefergehende Awareness

1. Jahrgang - 1. und 2. Semester:

- Dies deckt die rechtlichen Rahmenbedingungen von Stufe 2 ab. Persönliche Sicherheit sowie Grundlagen von Verschlüsselung/Hashing sind **nicht erwähnt**.

2. Jahrgang - 3. und 4. Semester:

- Im 4. Semester Lehrstoff „rechtliche und gesellschaftliche Aspekte im Umfeld der Informationstechnik“. Das *v*erstärkt die Abdeckung der rechtlichen Rahmenbedingungen. Persönliche Sicherheit sowie Grundlagen von Verschlüsselung/Hashing sind **nicht erwähnt**.

3. Jahrgang - 5. und 6. Semester:

- Keine expliziten Inhalte von Stufe 2 (außer eventuell sehr indirekt über Netzwerksicherheit) werden in diesem Jahrgang für dieses Fach aufgeführt.

Zusammenfassende Bewertung Stufe 2: Die **rechtlichen Rahmenbedingungen und Normen** sind im Lehrplan des Faches „Informatik, Projekt- und Qualitätsmanagement“ in den frühen Jahren solide verankert. Die Konzepte der **persönlichen Sicherheit** und die grundlegende, nicht-technische Erklärung von **Verschlüsselung und Hashing** sind in den vorliegenden Auszügen **nicht explizit genannt**.

5.6 Mittlere technische gewerbliche und kunstgewerbliche Fachschulen

Fachschulen im technischen, gewerblichen und kunstgewerblichen Bereich zeichnen sich durch eine praxisorientierte Ausbildung aus, die gezielt auf den unmittelbaren Einstieg in das Berufsleben vorbereitet. Im Zentrum steht die Vermittlung anwendungsbezogener Kompetenzen, die den aktuellen Anforderungen der Wirtschaft entsprechen. Im Unterschied zur *Angewandten Informatik* an Höheren Lehranstalten, die ein breit gefächertes Curriculum mit vertieften Kenntnissen in Programmierung und Datenbanktechnologien bietet und damit universitätsnahe Qualifikationen schafft, konzentrieren sich Fachschulen auf die fundierte Vermittlung grundlegender Inhalte. Dieses solide Fundament befähigt Absolvent:innen zu qualifizierten Tätigkeiten im Berufsalltag und bietet zugleich Anschlussmöglichkeiten für weiterführende Ausbildungen.

Die Vielfalt technischer, gewerblicher und kunstgewerblicher Fachrichtungen spiegelt sich in insgesamt 28 unterschiedlichen Lehrplänen wider:

- In 25 dieser Lehrpläne ist die digitale Grundbildung – ähnlich wie in der höheren Ausbildung – über den Gegenstand *Angewandte Informatik* gemäß *Anlage 1* der Fachschulen hinsichtlich Umfangs und Inhalt verbindlich geregelt.
- In den drei übrigen Fachrichtungen – *Elektronik und technische Informatik*, *Informationstechnik* sowie *Informationstechnik für blinde und sehbehinderte Menschen* – verteilt sich die digitale Grundbildung naturgemäß auf mehrere fachspezifischen Unterrichtsgegenstände.

Cybersecurity nimmt auch im Fachschulbereich eine zentrale Rolle ein – aus folgenden Gründen:

- **Berufliche Relevanz**: Absolvent:innen arbeiten häufig in Bereichen, in denen digitale Steuerungssysteme, Netzwerke und vernetzte Geräte zum Arbeitsalltag gehören. Der sichere und verantwortungsvolle Umgang mit diesen Technologien ist essenziell, um Sicherheitsrisiken frühzeitig zu erkennen und proaktiv zu vermeiden.
- **Menschliches Verhalten als Risikofaktor**: Ein Großteil sicherheitsrelevanter Vorfälle ist auf menschliches Fehlverhalten zurückzuführen. Fachkräfte im technischen Bereich benötigen daher ein geschärftes Bewusstsein für digitale Gefahren, etwa im Umgang mit Passwörtern, Social Engineering oder Phishing-Versuchen.
- **Langfristige Anschlussfähigkeit**: Die Fähigkeit, sich in einem zunehmend digitalisierten Arbeitsumfeld weiterzuentwickeln, gewinnt an Bedeutung. Grundlegende Kenntnisse im Bereich IT-Sicherheit bilden die Basis, um sich auch später neuen Anforderungen – wie z. B. in Smart Maintenance oder digitaler Logistik – kompetent stellen zu können.
- **Verantwortung im beruflichen Alltag**: Viele Fachschulabsolventen übernehmen in kleinen und mittleren Betrieben Schlüsselrollen oder gründen eigene Unternehmen. IT-Sicherheit ist hierbei nicht nur ein technisches, sondern auch ein unternehmerisches und gesellschaftliches Anliegen.

Insgesamt ist davon auszugehen, dass in den bestehenden Lehrplänen bereits grundlegende Aspekte der Cybersecurity implizit verankert sind. Um jedoch eine gezielte Kompetenzentwicklung im Sinne des CLEMENTINE-6-Stufen-Modells zu gewährleisten, sollten ausgewählte Begrifflichkeiten und Inhalte explizit ergänzt werden.

Die folgende Abbildung zeigt eine Übersicht der Lehrpläne für technische, gewerbliche und kunstgewerbliche Fachschulen:

Lehrpläne der technischen, gewerblichen und kunstgewerblichen Fachschulen 2016 - BGBl. II Nr. 240/2016 idgF[28]

28 Lehrplaene_der_technischen_gewerblichen_und_kunstgewerblichen_Fachschulen_2016_Stand_14_09_2021_0738377e0a.pdf

Anlage	Fachrichtung	Cybersecurity Zielgegenstand	1	2	3	4
1	Anlage 1					
1.1	Bautechnik	**Angewandte Informatik**	2	2		
1.2	Bildhauerei	**Angewandte Informatik**	2	2		
1.3	Büchsenmacher	**Angewandte Informatik**	2	2		
1.4	Chemie	**Angewandte Informatik**	2	2		
1.5	Chemische Technologie	**Angewandte Informatik**	2	2		
1.6	Drechsler	**Angewandte Informatik**	2	2		
1.7	Elektronik und technische Informatik	Diverse Gegenstände	-	-	-	-
1.8	Elektrotechnik	**Angewandte Informatik**	2	2		
1.9	Flugtechnik	**Angewandte Informatik**	2	2		
1.10	Gebäudetechnik	**Angewandte Informatik**	2	2		
1.11	Glastechnik und Gestaltung	**Angewandte Informatik**	2	2		
1.12	Holzwirtschaft	**Angewandte Informatik**	2	2		
1.13	Informationstechnik	Diverse Gegenstände	-	-	-	-
1.14	Informationstechnik für blinde und sehbehinderte Menschen	Diverse Gegenstände	-	-	-	-
1.15	Keramik und Ofenbau	**Angewandte Informatik**	2	2		
1.16	Korb- und Möbelflechterei für blinde und sehbehinderte Menschen	**Angewandte Informatik**	2	2		
1.17	Lederdesign	**Angewandte Informatik**	2	2		
1.18	Malerei und Gestaltung	**Angewandte Informatik**	2	2		
1.19	Maschinenbau	**Angewandte Informatik**	2	2		
1.20	Maschinenbau für blinde und sehbehinderte Menschen	**Angewandte Informatik**	2	2		
1.21	Mechatronik	**Angewandte Informatik**	2	2		
1.22	Mediengestaltung und digitale Druckproduktion	**Angewandte Informatik**	2	2		
1.23	Präzisions- und Uhrentechnik	**Angewandte Informatik**	2	2		
1.24	Steintechnik und Steingestaltung	**Angewandte Informatik**	2	2		
1.25	Streich- und Saiteninstrumentenerzeugung	**Angewandte Informatik**	2	2		
1.26	Tischlerei	**Angewandte Informatik**	2	2		
1.27	Vergolden und Schriftdesign	**Angewandte Informatik**	2	2		
1.28	Weberei für blinde und sehbehinderte Menschen	**Angewandte Informatik**	2	2		

Tabelle 8: Lehrpläne der Höheren technischen und gewerblichen Lehranstalten (einschließlich der kunstgew. Lehranstalten) - 2015 – BGBl. II Nr. 262/2015 idgF

5.6.1 Angewandte Informatik – Fachschule

Der Gegenstand „Angewandte Informatik“ ist auch in Fachschulen über die Anlage 1 geregelt und findet in 25 der 28 Lehrpläne technischer, gewerblicher und kunstgewerblicher Fachschulen Anwendung (siehe Abbildung 2).

Analog zur Struktur der Lehrpläne in Höheren und Mittleren technischen sowie gewerblichen Lehranstalten definiert die Anlage 1 mehrere allgemein gültige Unterrichtsgegenstände für unterschiedliche Ausbildungsrichtungen. Der Bereich *Angewandte Informatik* bildet dabei die Grundlage für eine einheitliche Vermittlung digitaler Basiskompetenzen.

Die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells fließen insofern bereits ein, als grundlegende IT-Kenntnisse sowie ein verantwortungsvoller Umgang mit Daten in verschiedenen Pflichtgegenständen vermittelt werden.

Ein darauf aufbauender Vorschlag sieht vor, diese Inhalte schrittweise in den Gegenstand *Angewandte Informatik* der ersten beiden Jahrgänge zu integrieren. Zusätzlich können sprachliche Fächer zur Sensibilisierung für Kommunikationssicherheit beitragen, während der Unterricht in *Sozialer und personaler Kompetenz* angemessene Verhaltensweisen und Reaktionsmuster stärken kann.

Wesentlich ist dabei, dass der technische Anspruch der Cybersecurity-Inhalte in diesen frühen Stufen bewusst niedrig gehalten wird – mit dem Ziel, grundlegendes Verständnis zu fördern und nachhaltiges Interesse zu wecken.

5.6.1.1 Lehrplanergänzungen

1. Jahrgang - 1. Semester:

Bereich Informatiksysteme, Mensch und Gesellschaft:

Lehrstoff: Hardwarekomponenten & Betriebssysteme

- **Technologisches Grundverständnis**: Vertiefung des Verständnisses für den grundlegenden Aufbau und die Funktionsweise moderner Computersysteme (z.B. Zusammenspiel von Soft- und Hardware, verschiedene Computerarten wie Supercomputer oder Embedded Systems).
- **Gerätesicherheit (Basis)**: Praktische Maßnahmen zur Sicherung des eigenen Geräts, wie das Einrichten eines Sperrbildschirms mit Kennwörtern, die Bedeutung regelmäßiger Abmeldung/Sperren des Geräts und das Konzept eines „Clean Desktops“.
- **Software-Aktualisierung**: Vermittlung der Notwendigkeit und Vorteile von regelmäßigen Software-Updates und Sicherheits-Patches; Einführung in das Konzept von „0-Day-Exploits“ auf einem grundlegenden Niveau.

Lehrstoff: Datensicherung

- **Schadsoftware und Grundbegriffe**: Neben „Virenschutz“, explizite Definitionen von „Malware“ und „Antivirus“.
- **Datenspuren und Datenschutz**: Bewusstseinsbildung über die digitalen Spuren, die im Internet hinterlassen werden, und das richtige Verhalten im Umgang mit (insbesondere personenbezogenen) Daten.

Bereich Publikation und Kommunikation im Web

Lehrstoff: Publikation und Kommunikation im Web

- **Erkennung von Angriffen**: Einführung in die Erkennung und Vermeidung klassischer „persönlicher“ Angriffe, wie z.B. „Phishing“ und „Cybermobbing“. Praktische Hinweise zur Analyse einfacher Mail-Header und URLs, um die Herkunft von Spam-/Phishing-E-Mails festzustellen.
- **Privatsphäre online**: Sensibilisierung für den Schutz der Privatsphäre und persönlichen Daten in Online-Spielen und Chatrooms.
- **Sichere Datenverwaltung**: Betonung des sicheren Verwaltens und Weitergebens von Daten, insbesondere bei der Nutzung von Cloud-Diensten.

1. Lehrgang - 2. Semester:

Bereich Informatiksysteme, Mensch und Gesellschaft

Lehrstoff: Rechtliche und gesellschaftliche Aspekte

- **Vertiefung der Rechtsgrundlagen**: Ergänzung der „Grundsätze des Datenschutz- und Telekommunikationsgesetzes“ um eine explizite Nennung und Erläuterung der „DSGVO“ und grundlegende Aspekte des „IT-Rechts/StGB“ in Bezug auf IT-Sicherheit in Österreich und Europa.
- **Identität und Verantwortung**: Vertiefung der Konzepte von „digitaler Identität“ und der Wichtigkeit von „Identität und Verantwortlichkeit“ im digitalen Raum, um Handlungen und Daten bestimmten Personen zuordnen zu können.
- **Grundlagen Angriffsvektoren**: Einführung in spezifische Bedrohungen wie „Identitätsdiebstahl“, „Social Engineering“ und „Ransomware“.
- **Reaktion im Notfall**: Grundsätzliche Verhaltensregeln für den Notfall: wie man richtig reagiert, Ansprechpartner kennt und die Beseitigung von Infektionen initiiert.

Lehrstoff: Netzwerke

- **Sicheres Netzwerkverhalten**: Vermittlung von Risiken und sicherem Verhalten beim Zugang und der Nutzung in öffentlichen Netzen, öffentlichen WLANs und privaten Netzwerken.

2. Jahrgang - 3. Semester:

Bereich Informatiksysteme, Mensch und Gesellschaft

Lehrstoff: Datensicherung (Vertiefung)

- **Praktische Datensicherung**: Konkrete Übungen zum Anlegen von Backups und zur Wiederherstellung von Daten.
- **Datenträgerverschlüsselung**: Kennenlernen und grundlegende Anwendung von Datenträgerverschlüsselung, z.B. für USB-Sticks.
- **Sicheres Löschen**: Methoden und Bewusstsein für das sichere Entsorgen von Dokumenten und Datenträgern.
- **Virenscanner**: Praktische Konfiguration und effektiver Einsatz von Virenscannern.

Lehrstoff: Netzwerke & Publikation und Kommunikation im Web

- **Grundlagen Verschlüsselung**: Einführung in die Funktionsweise von Verschlüsselung und Hashfunktionen (ohne technische Tiefe).
- **Sichere Kommunikationskanäle**: Die Bedeutung von HTTPS und Zertifikaten für sichere Verbindungen im Internet.
- **Sichere Authentifizierung**: Vorstellung sicherer Authentifizierungsmethoden wie Mehrfaktorauthentifizierung (MFA) und Password Safes.
- **Persönliche Firewalls**: Der Zweck und der grundlegende Einsatz persönlicher Firewalls.
- **Dateianalyse**: Erkennen und Bewerten potenziell bösartiger Dateianhänge anhand ihrer Endungen.

Neuer Lehrstoff-Aspekt (oder unter „Rechtliche und gesellschaftliche Aspekte“)

- Digitale Signatur: Grundlagen der digitalen Signatur (asynchrone Verschlüsselung mit Public und Private Key) und der elektronischen Signatur (z.B. „Handysignatur“), sowie deren Anwendungsbereiche und Funktionsabläufe.

2. Jahrgang - 4. Semester:

Bereich Informatiksysteme, Mensch und Gesellschaft

Lehrstoff: Gesellschaftliche Auswirkungen der Informationstechnologie

- **Vertiefende Angriffsvektoren**: Detailliertere Betrachtung von Angriffen wie „Botnetze“, „Mobiltelefon als lohnendes Angriffsziel“ und „DOS/DDOS“. Diskussion, ob man einer App vertrauen kann, mit Beispielen wie „Android Hardening guides“.

- **Cybercrime**: Überblick über aktuelle Formen der Internetkriminalität, ggf. unter Bezugnahme auf aktuelle Berichte (z.B. ENISA Top 15 Thread Landscape, Europol IOCTA).
- **Smart Devices und Suchmaschinen**: Anwendungsfelder und Sicherheitsaspekte von Smartwatches, Sprachassistenten (wie Alexa) und spezialisierten Suchmaschinen (wie Shodan).
- **Grundlagen technischer Sicherheitsstrategien**: Einführung in Konzepte wie Sicherheitsmanagement und -systeme (inklusive Sicherheitsstrategien), Grundschutz nach BSI, einfache Netzwerksicherheitstools, Anonymisierungsdienste, Logfiles, Sandboxing und virtuelle Maschinen.
- **Ethik in der IT-Sicherheit**: Vertiefende Diskussion über die Rolle von „guten Hackern“ und „bösen Crackern“ (Ethical Hacking) sowie das „Defender’s Dilemma“, um die ethische Verantwortung in IT-Berufen zu stärken.

5.6.1.2 Zusammenfassende Analyse

Die „Angewandte Informatik“ im bestehenden Lehrplan legt den Schwerpunkt auf die sichere und kompetente Anwendung moderner Informationstechnologien im beruflichen Alltag und die Teilnahme an der vernetzten Gesellschaft. Sie deckt grundlegende IT-Kompetenzen ab, wie das Kennen von Hardware-Komponenten, die Nutzung von Betriebssystemen, Netzwerken, Datensicherung und die Berücksichtigung gesetzlicher Rahmenbedingungen.

Das CLEMENTINE-6-Stufen-Modell, insbesondere seine Stufen 1 und 2, führt jedoch eine wesentlich umfassendere, detailliertere und proaktivere Auseinandersetzung mit dem Thema Cybersecurity ein. Es geht weit über das bloße „sichere Anwenden“ hinaus und zielt darauf ab, ein tiefes Bewusstsein für die digitale Bedrohungslandschaft, das menschliche Verhalten als Sicherheitsfaktor, konkrete Schutzmaßnahmen, rechtliche Implikationen und spezifische Angriffsmuster zu schaffen.

Die Analyse zeigt, dass der Lehrplan „Angewandte Informatik“ viele der spezifischen Cybersecurity-Inhalte entweder nicht oder nur sehr oberflächlich behandelt, insbesondere in den Bereichen Bedrohungsszenarien, technische Schutzmechanismen, fortgeschrittene Datenverarbeitungssicherheit und die explizite Auseinandersetzung mit rechtlichen und verhaltensbezogenen Aspekten der Cybersecurity.

Die Veränderungen im CLEMENTINE-6-Stufen-Modell stellen somit eine deutliche Vertiefung und Aktualisierung der Cybersecurity-Bildung dar, die über die derzeitigen Inhalte der „Angewandten Informatik“ hinausgeht.

5.6.2 Lehrplan Fachschule Elektrotechnik und technische Informatik

5.6.2.1 Lehrplanergänzungen

Der Lehrplan der „Fachschule für Elektronik und Technische Informatik“ berücksichtigt die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells, insbesondere deren technische und anwendungsbezogene Aspekte, wenn auch oft mit einem stärkeren Fokus auf technische Umsetzung und Funktionalität als auf die reine Bewusstseinsbildung oder spezifische Verhaltensweisen.

1. Jahrgang - 1. und 2. Semester:

Pflichtfach: Computer- und Netzwerktechnik

- **Sicherung des Grundverständnisses aus Sekundarstufe I:** Explizite Behandlung des „richtigen Verhaltens im Umgang mit (vor allem personenbezogenen) Daten“ im digitalen Alltag und die Sensibilisierung für den Wert dieser Daten. Einführung in das Erkennen einfacher Risiken (z.B. ungewöhnliche Pop-ups, verdächtige E-Mails) und grundlegende Reaktionsgrundsätze bei Auffälligkeiten.
- **Motivation zur Sicherheit:** Vorstellung von realen, einfachen Fallbeispielen zu Schadsoftware (z.B. Viren, Phishing) zur Veranschaulichung potenzieller Bedrohungen und deren Auswirkungen. Diskussion über die Rollen von „guten Hackern“ (Ethical Hacking) und „bösen Crackern“ zur Motivation für IT-Sicherheit. Einführung in Social Engineering als menschlicher Angriffsvektor.
- **Grundbegriffe:** Vermittlung grundlegender Cybersecurity-Begriffe wie Antivirus, Malware, Phishing, Cybermobbing. Einführung in erste Strategien der Datensicherheit und das Konzept der digitalen Identität.
- **Über den Umgang mit Daten im Internet:** Praktische Hinweise zum Erkennen und Vermeiden klassischer „persönlicher“ Angriffe. Grundlagen zum Umgang mit Dateianhängen (Attachments) und der Identifizierung potenziell „bösartiger“ Dateiendungen. Überblick über die Entstehung von

„Datenspuren im Internet“ und deren Implikationen. Basismaßnahmen zur Sicherung des eigenen Gerätes (z.B. einfache Bildschirmsperre, Passwörter).
- **Sicherheitsempfehlungen:** Einführung grundlegender Verhaltensrichtlinien für digitale Sicherheit (z.B. sicheres Abmelden von Diensten, „Clean Desktop Policy“). Betonung der Bedeutung von Sperrbildschirmen mit Kennwörtern und der Notwendigkeit regelmäßiger Updates für Software und Betriebssysteme.
- **Bedrohungsszenarien:** Erste Schritte zur Frage „Was tun im Notfall?“ – Fokus auf richtiges Reagieren bei ersten Anzeichen eines Vorfalls und das Wissen um Ansprechpartner.

2. Jahrgang - 3. und 4. Semester:

Pflichtfach: Computer- und Netzwerktechnik

- **Über den Umgang mit Daten im Internet:** Vertiefung des sicheren Verwaltens und Weitergebens von Daten (z.B. bewusster Umgang mit Cloudspeichern). Einführung in Methoden des sicheren Löschens von Daten (konzeptionell).
- **Sicherheitsempfehlungen:** Detailliertere Betrachtung der Bedeutung von Kennwörtern (Komplexität, Länge) und das Konzept von Rainbowtables zur Veranschaulichung der Angreifbarkeit schwacher Passwörter. Spezifisches Verhalten in öffentlichen Netzen (z.B. öffentlichen WLANs) versus privaten Netzen.
- **Vertraulichkeit und Integrität:** Konzeptionelles Verständnis der Funktionsweise von Verschlüsselung und Hashfunktionen, *ohne* technische Implementierungstiefe. Fokus auf deren Rolle zur Sicherstellung von Vertraulichkeit und Integrität von Daten.
- **Über den Umgang mit Daten II:** Konzepte und Best Practices für das Anlegen von Backups und die Wiederherstellung von Daten. Einführung in die Notwendigkeit und Methoden des sicheren Entsorgens von Dokumenten und Datenträgern. Installation, Konfiguration und Einsatz von Virenscannern.

Pflichtfach: Unternehmensführung

- **Rechtsgrundlagen:** Einführung in die rechtlichen Gegebenheiten in Österreich und Europa im Kontext der IT-Sicherheit. Explizite Behandlung der Grundzüge der DSGVO (Datenschutz-Grundverordnung), relevanter Passagen aus dem Strafgesetzbuch (StGB) im Bereich Cyberkriminalität und grundlegendes IT-Recht.

3. Jahrgang - 5. und 6. Semester:

Pflichtfach: Computer- und Netzwerktechnik

- **Sichere Kommunikation:** Verständnis zur Herstellung sicherer Verbindungen zum Arbeitsplatznetzwerk (konzeptionell, z.B. VPN). Konfiguration und Einsatz von persönlichen Firewalls. Benennen von sicheren Authentifizierungsmethoden (z.B. NIST Guidelines, Password Safes, Mehrfaktorauthentifizierung (MFA)) und sichere Kommunikationskanäle (z.B. HTTPS und Zertifikate).
- **Technische Umsetzungsstrategien:** Überblick über Sicherheitsmanagement und -systeme, einschließlich grundlegender Sicherheitsstrategien. Einführung in einfache Netzwerksicherheitstools und deren Bedienung. Konzepte von Anonymisierungsdiensten (z.B. VPN, Tor) und deren Einsatzmöglichkeiten. Bedeutung von Logfiles für die Sicherheit und erste Schritte zur Interpretation einfacher Log-Einträge. Einführung in Sandboxing und virtuelle Maschinen als Sicherheitsmechanismen.
- **Angriffsvektoren:** Explizite Vorstellung von Angriffsvektoren wie Ransomware, Botnetze und DOS/DDOS (ohne technische Implementierungstiefe). Diskussion über deren Funktionsweise und Auswirkungen.

Pflichtfach: Kommunikationselektronik

- **Smart Devices:** Diskussion der Anwendungsfelder und spezifischer Sicherheitsimplikationen von Smartwatches, Sprachassistenten (Alexa) und anderen IoT-Geräten im Kontext der Kommunikationselektronik. Sensibilisierung durch die Einführung in spezifische Suchmaschinen für IoT-Geräte (z.B. Shodan) zur Illustration der Sichtbarkeit von Geräten im Internet.
- **Softwaretechnik** (Übungen in EDV) (Kann auch im Laboratorium oder in Projektarbeiten integriert werden, da in der 3. Klasse in der Stundentafel I.2 kein expliziter Lehrstoff für Softwaretechnik mehr ausgewiesen ist.)

- **Angriffsvektoren:** Vertiefung der Sicherheit von Mobiltelefonen als Angriffsziel. Kriterien zur Beurteilung der Vertrauenswürdigkeit von Apps und grundlegende Tipps zur Härtung mobiler Geräte (z.B. basierend auf einem „Android Hardening Guide“). Überblick über die „6 Stufen eines Angriffs“ (z.B. Reconnaissance, Gaining Access, Maintaining Access) zur Systematisierung des Verständnisses von Bedrohungsszenarien.

4. Jahrgang - 7. und 8. Semester:

Pflichtfach: Computer- und Netzwerktechnik

- **Digitale Bürgerkarte:** Vertiefte Behandlung der digitalen Signatur (asynchrone Verschlüsselung mit Public und Private Key). Verständnis, wie digitale Signaturen überprüft und angewendet werden. Erläuterung der Funktionsabläufe elektronischer Signaturen (z.B. „Handysignatur“).
- **Angriffsvektoren:** Einführung in das breitere Feld der Cyberkriminalität („Cybercrime“), einschließlich der Rolle relevanter Organisationen wie ENISA und Europol (IOCTA). Beispiele für „Defacements“ und die Bedeutung von „Reconnaissance“-Aktivitäten als Angriffsphase.

Pflichtfach: Laboratorium

- Praktische Übungen zur Anwendung der Sicherheitsempfehlungen: Sichere Konfiguration einfacher Netzwerke oder Betriebssysteme, einfache Backup-Strategien umsetzen.
- Simulation von Phishing-Angriffen und Analyse von Mail-Headern/URLs zur Herkunftsbestimmung von Spam/Phishing.
- Analyse von bereitgestellten Logfiles zur Erkennung einfacher Anomalien oder verdächtiger Aktivitäten.
- Demonstration von Social Engineering Taktiken und Reaktionstrainings in sicheren Umgebungen.
- Grundlegender Umgang mit Virenscannern und persönlichen Firewalls zur Systemhärtung.

Innerhalb der jeweiligen Ausbildungsschwerpunkte (z.B. „Computer- und Informationstechnik“, wo Dienste und Sicherheitssysteme installiert und konfiguriert werden), sollten die Awareness-Themen direkt in die technische Umsetzung einfließen. Beispielsweise die Implementierung von Systemen unter Berücksichtigung von „Least Privileges“ oder „Gerätehärtung“ als praktische Anwendung der in Stufe 1 und 2 erarbeiteten Prinzipien.

5.6.2.2 Zusammenfassende Analyse

Im aktuellen Lehrplan für *Elektrotechnik und Technische Informatik* sind mehrere Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells entweder nicht explizit verankert oder werden lediglich oberflächlich bzw. in technisch-abstrakter Form behandelt – ohne dabei gezielt auf die Bewusstseinsbildung oder konkrete Verhaltensdimensionen im Bereich der Cybersecurity einzugehen.

Die Cybersecurity-Initiative verfolgt hingegen einen deutlich praxisnäheren und differenzierteren Zugang: Sie fordert eine intensivere Auseinandersetzung mit sicherheitsrelevanten Themen bereits auf den unteren Kompetenzstufen – über grundlegendes IT-Wissen und technische Basiskompetenzen hinaus. Dabei stehen insbesondere die Sensibilisierung für digitale Bedrohungsszenarien, klar formulierte Verhaltensrichtlinien sowie die Einbettung rechtlicher Rahmenbedingungen aus einer Cybersecurity-Perspektive im Vordergrund.

5.6.3 Lehrplan Fachschule Informationstechnologie

Im Bereich „Informationssysteme und IT-Sicherheit“ des Lehrplans lernen die Schüler:innen , Bedrohungen und Angriffsvektoren zu benennen, Grundbegriffe der Datensicherheit zu kennen, grundlegende Schutzmechanismen anzuwenden, Authentifizierungsmethoden zu verstehen und wichtige Faktoren für Datensicherheit zu kennen sowie grundlegende IT-Sicherheitstools einzusetzen. Dazu gehören auch Anwendungssicherheit, Verschlüsselungswerkzeuge, Schutz vor Schadsoftware, digitale Identität und Signaturen sowie rechtliche Grundlagen. Im Bereich "Netzwerksicherheit" lernen sie, Gefahrenszenarien zu identifizieren, Absicherungsmaßnahmen für Server- und Netzwerksysteme zu konfigurieren und Verschlüsselungsmethoden anzuwenden.

5.6.3.1 Lehrplanergänzungen

Die folgende Integration der Cybersecurity Inhalte konzentriert sich hauptsächlich auf den Pflichtgegenstand **„Informationssysteme und IT-Sicherheit“** sowie relevante Ergänzungen in **„Systemtechnik“** und **„Netzwerktechnik“**.

1. Jahrgang - 1. Semester:

Pflichtfach: Informationssysteme und IT-Sicherheit

- **Bereich IT-Sicherheit:** Bedrohungen und Angriffsvektoren benennen; die Grundbegriffe der Datensicherheit benennen; das Spannungsfeld zwischen Sicherheit und Privatsphäre erkennen. Lehrstoff: Bedrohungen, Angriffsvektoren, Schutz personenbezogener Daten, Grundbegriffe der Datensicherheit.
- **Bewusstseinsbildung:** Ergänzung um die explizite Nutzung von Video-Fallbeispielen und die Vorstellung von Bedrohungen wie **Keyloggern** als konkretes Beispiel für Schadsoftware.
- Diskussion der Konzepte von **„Gute Hacker – Böse Cracker?“** und **Ethical Hacking** zur Kontextualisierung von IT-Sicherheit.
- Einführung und Erklärung von **Social Engineering** als psychologische Angriffsmethode.
- Konkrete Definition und Beispiele von **Identitätsdiebstahl**.
- Betonung der **Auswirkungen und Eskalationsszenarien** von Sicherheitsvorfällen.
- Spezifizierung von **Phishing** als einen zentralen Angriffsvektor und Grundbegriff.
- Einführung des Begriffs **Cybermobbing** im Rahmen des verantwortungsvollen Umgangs mit sozialen Medien.
- Erläuterung des konzeptionellen **„Defender’s Dilemma“** zur Verdeutlichung der Herausforderung der IT-Sicherheit.
- Anleitung zur **Analyse von Mail-Headern und URLs**, um Spam- oder Phishing-Mails eindeutig zu identifizieren.
- Regeln und Bewusstsein für den Umgang mit **Attachments und Dateiendungen**, insbesondere potenziell „bösartigen“ Dateien.
- Detailliertere Auseinandersetzung mit **Datenspuren im Internet** und wie diese entstehen und reduziert werden können.
- Grundlagen des **sicheren Löschens von Daten** von Datenträgern.
- Explizite **Verhaltensrichtlinien** wie das „Abmelden/Sperren des Gerätes“, die Praxis eines „Clean Desktop“ und die obligatorische Verwendung eines **Sperrbildschirms mit Kennwörtern**.
- Einführung des Prinzips der **„Least Privileges“** (geringste Berechtigungen).

1. Jahrgang - 2. Semester:

Pflichtfach: Informationssysteme und IT-Sicherheit

- Anleitung zum **sicheren Verwalten und Weitergeben von Daten**, inklusive der sicheren Nutzung von **Cloudspeichern**.
- Umfassende Maßnahmen zum **Sichern des eigenen Geräts**.
- Erläuterung der Sicherheitskompromittierung durch **externe Geräte** (z.B. **Rubberducky, USB-Killer**).
- Ergänzung weiterer Angriffsmethoden für Informationsweitergabe: **Whaling und Gophish**.
- Etablierung von **Reaktionsgrundsätzen für Notfälle** („Was tun im Notfall? Richtig reagieren, Ansprechpartner kennen, Infektionsbeseitigung initiieren“). Dies ist ein wesentlicher operativer Aspekt, der aktuell fehlt.
- Einfache Erklärung, **wie Verschlüsselung funktioniert** (ohne technische Tiefe). Dies ergänzt die spätere praktische Anwendung.
- Einfache Erklärung, **wie eine Hashfunktion funktioniert** (ohne technische Tiefe). Dies bildet eine Grundlage für das Verständnis von Integrität und Signaturen.
- Praktische Anweisung zum **sicheren Entsorgen von Dokumenten und Datenträgern**.
- Konfiguration und effektiver Einsatz von **Virenscannern**.
- **Sichere Kommunikation (Voreinführung):**
- Grundlagen von **HTTPS und Zertifikaten** als sichere Kommunikationskanäle.

2. Jahrgang - 3. Semester:

Pflichtfach: Informationssysteme und IT-Sicherheit

- Detaillierung der **Bedeutung von Kennwörtern** hinsichtlich Komplexität und Länge, und Erklärung von **Rainbowtables**.
- Einführung in **Mobile Device Management (MDM)**, einschließlich der Funktion der "Fernlöschung".

Konkrete sichere **Authentifizierungsmethoden** wie **NIST Guidelines** für Passwörter, die Nutzung von **Password Safes** und die Implementierung von **Mehrfaktorauthentifizierung (MFA)**.

Pflichtfach: Systemtechnik

- Einführung von **BIOS-Kennwörtern** und dem Konzept eines **sicheren Bootprozesses**. (Kann hier oder bereits in der 1. Klasse vertieft werden, je nach technischer Tiefe).

2. Jahrgang - 4. Semester:

Pflichtfach: Informationssysteme und IT-Sicherheit

- Konkrete Anwendungsbeispiele wie die **Elektronische Signatur ("Handysignatur")** und deren Funktionsabläufe.
- Explizite Benennung und Erläuterung der **rechtlichen Gegebenheiten in Österreich und Europa**, insbesondere **IT-Recht, Strafgesetzbuch (StGB) und DSGVO**. (Der aktuelle Lehrplan nennt nur "rechtliche Rahmenbedingungen").
- Einführung in **Sicherheitsmanagement und -systeme**, einschließlich allgemeiner Sicherheitsstrategien.
- Vorstellung des **Grundschutzes nach BSI** als etabliertes Sicherheitskonzept.
- Erklärung von **Anonymisierungsdiensten**.
- Grundlagen von **Logfiles** als Werkzeug zur Überwachung und Fehleranalyse.
- Das Konzept von **Sandboxing** und der Einsatz von **Virtuellen Maschinen** als Sicherheitsstrategie.
- Spezifische Bedrohungen wie **Ransomware und Botnetze**.
- Das **Mobiltelefon als "lohnendes" Angriffsziel** und die kritische Frage: **"Vertraue ich einer App?"** (z.B. Android Hardening Guide).
- Erklärung von **Denial-of-Service (DOS) und Distributed Denial-of-Service (DDOS)** Angriffen.
- Überblick über **Cybercrime** basierend auf relevanten Berichten (z.B. ENISA Top 15 Threat Landscape, Europol IOCTA).
- Weitere Angriffstypen wie **Defacements** und **Reconnaissance**.

Pflichtfach: Netzwerktechnik

- verschiedene **Netzwerkkomponenten** anschließen und konfigurieren.
- Verhaltensregeln für die Nutzung von Netzen, insbesondere das **Verhalten in öffentlichen Netzen, öffentlichen WLANs und privaten Netzen**.

3. Jahrgang - 5. Semester:

Pflichtfach: Informationssysteme und IT-Sicherheit

- Diskussion der Sicherheitsaspekte von **Smartwatches und smarten Sprachassistenten (z.B. Alexa)**.
- Vorstellung von **Shodan** als spezialisierte Suchmaschine zur Identifizierung und Analyse vernetzter Geräte.

Pflichtfach: Netzwerktechnik

- Der Einsatz von **persönlichen Firewalls** (ergänzend zu Server- und Netzwerk-Firewalls).
- Nennung und exemplarische Bedienung von **einfachen Netzwerksicherheitstools**.

Das Fach "Informationssysteme und IT-Sicherheit" ist bereits als Pflichtgegenstand mit 21 Semesterwochenstunden über die 3,5 Jahre verteilt enthalten. Die Vermittlung der IT-Sicherheit ist explizit als ein wichtiges Bildungsziel dieses Lehrplans aufgeführt. Absolvent:innen sollen unter anderem praktische Tätigkeiten im Bereich der IT-Sicherheit ausführen und informationstechnische Problemstellungen analysieren, Lösungen erarbeiten und umsetzen können.

5.6.3.2 Zusammenfassende Analyse

Der Lehrplan der Fachschule für Informationstechnik stellt eine solide Grundlage in der IT-Sicherheit und Kernkompetenzen wie das Benennen von Bedrohungen, Angriffsvektoren und Grundbegriffen der Datensicherheit dar, es fehlen jedoch die detaillierten und auf Bewusstseinsbildung ausgerichteten Inhalte des CLEMENTINE-6-Stufen-Modells. Insbesondere fehlen im Lehrplan spezifische Lerninhalte zu nuancierten

Verhaltensrichtlinien für den Umgang mit Daten und in digitalen Umgebungen (wie "Clean Desktop" oder Verhalten in öffentlichen WLANs), detaillierte Fallbeispiele und explizite Nennungen moderner, spezifischer Bedrohungsarten wie "Social Engineering", "Phishing" oder "Ransomware" auf dieser grundlegenden Ebene.

Die dargestellten "Veränderungen" sind somit weniger eine *Reform* des gesamten Lehrplans als vielmehr eine detaillierte **Strukturierung und Konkretisierung der Cybersecurity-Inhalte** innerhalb der Sekundarstufe II, die darauf abzielt, diese umfassend in den bestehenden und zukünftigen Lehrplänen zu verankern und die Kompetenzvermittlung zu schärfen.

5.6.4 Lehrplan Fachschule Informationstechnologie für blinde und sehbehinderte Menschen

Der Lehrplan für blinde und sehbehinderte Menschen unterscheidet sich vom allgemeinen Lehrplan für Informationstechnologie nicht nur durch spezielle Unterrichtsfächer und angepasste Stundentafeln, sondern vor allem durch eine ganzheitlich ausgerichtete Didaktik, die gezielt auf die besonderen Bedürfnisse dieser Schüler:innen eingeht und ihnen somit eine gleichwertige Ausbildung im Bereich der Informationstechnik ermöglicht.

5.6.4.1 Lehrplanergänzungen

Die Vorschläge zielen darauf ab, die allgemeine Sensibilisierung und das tiefergehende Bewusstsein für IT-Sicherheit (Awareness) gemäß dem CLEMENTINE-6-Stufen-Modell zu stärken, indem konkrete Verhaltensrichtlinien, detailliertere Bedrohungsszenarien und konzeptionelle Grundlagen explizit in den Lehrstoff integriert werden.

Um die Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells explizit in den vorliegenden Lehrplan der Fachschule für Informationstechnik für blinde und sehbehinderte Menschen zu integrieren, sind folgende Ergänzungen in den jeweiligen Jahrgängen, Semestern und Gegenständen vorgeschlagen:

1. Jahrgang - 1. Semester

Pflichtfach: Informationssysteme und IT-Sicherheit

- **Motivation zur Sicherheit:** Bewusstseinsbildung (Fallbeispiele, Keylogger), Ethical Hacking vs. Cracker, Identitätsdiebstahl.
- **Grundbegriffe:** Phishing.
- **Umgang mit Daten im Internet:** Datenspuren im Internet, Daten sicher löschen.
- **Sicherheitsempfehlungen:** Verhaltensrichtlinien (Abmeldung/Sperren, Clean Desktop).

1. Jahrgang - 2. Semester

Pflichtfach: Informationssysteme und IT-Sicherheit

- **Motivation zur Sicherheit:** Social Engineering.
- **Grundbegriffe:** Cybermobbing, Defender’s Dilemma.
- **Umgang mit Daten im Internet:** E-Mail-Header und URLs analysieren.
- **Sicherheitsempfehlungen:** Updates und Patches, 0-Day-Exploits, BIOS-Kennwörter, sicherer Bootprozess, Bedeutung von Kennwörtern (Komplexität, Länge), Rainbowtable, Mobile Device Management (Fernlöschung), Least Privileges, Verhalten in öffentlichen / privaten Netzen, Privatsphäre in Spielen und Chatrooms.
- **Bedrohungsszenarien:** Sicherheitskompromittierung durch externe Geräte (Rubberducky, USB-Killer), Angriffsmethoden für Informationsweitergabe (Whaling, Gophish), Notfallreaktion (richtig reagieren, Ansprechpartner, Infektionsbeseitigung initiieren).

2. Jahrgang - 3. Semester (Modul 3)

Pflichtfach: Informationssysteme und IT-Sicherheit

- **Vertiefung der IT-Sicherheit:** Vertraulichkeit und Integrität (Verschlüsselung, Hashfunktion – ohne technische Tiefe).
- **Umgang mit Daten II:** Sicheres Entsorgen von Dokumenten/Datenträgern.
- **Sichere Kommunikation:** Sichere Authentifizierungsmethoden (NIST Guidelines, Password Safes, Mehrfaktorauthentifizierung).

Pflichtfach: Netzwerktechnik

- **Sichere Kommunikation:** Einführung in persönliche Firewalls.
- **Sichere Kommunikation:** Vertiefung der sicheren Verbindung zum Arbeitsplatznetzwerk (z.B. VPN, FIDO, MFA, HTTPS, Zertifikate).

2. Jahrgang - 4. Semester

Pflichtfach: Informationssysteme und IT-Sicherheit

- **Digitale Bürgerkarte:** Elektronische Signaturen (Handysignatur), Funktionsabläufe.
- **Smart Devices:** Anwendungsfelder von spezifischen Devices (Smartwatches, Alexa), Spezifische Suchmaschinen (Shodan).
- **Rechtsgrundlagen:** Rechtliche Gegebenheiten in Österreich und Europa (IT-Recht, StGB, DSGVO).
- **Technische Umsetzungsstrategien:** BSI-Grundschutz, Anonymisierungsdienste, Logfiles, Sandboxing – Virtuelle Maschinen.
- **Angriffsvektoren:** Ransomware, Botnetze, Mobiltelefon als Angriffsziel (Vertrauen einer App/Android Hardening), DOS/DDOS, Cybercrime (Enisa, Europol IOCTA), Defacements, Reconnaissance, 6 Stufen eines Angriffs.

Pflichtfach: Unternehmensführung

- **Sicherheitsmanagement:** Sicherheitsmanagement und -systeme, Sicherheitsstrategien, Grundschutz nach BSI.

3. Jahrgang

Die Inhalte des 3. Jahrgangs wurden bereits im 2. Jahrgang des Fachgegenstandes "Informationssysteme und IT-Sicherheit" umfassend integriert, um eine frühere und breitere Behandlung der grundlegenden Aspekte der Stufen 1 und 2 zu gewährleisten, insbesondere da die Fachschule 3,5 Jahre dauert und die Grundlagen frühzeitig gelegt werden sollen.

Bei der Integration dieser Inhalte muss der Lehrplan die bereits vorhandenen didaktischen Grundsätze berücksichtigen, die auf die besonderen Bedürfnisse blinder und sehbehinderter Schülerinnen und Schüler eingehen. Dies bedeutet, dass die Vermittlung des Lehrstoffs durch verstärkten Einsatz von auditiven, haptischen und verbalen Medien erfolgen sollte. Konzepte, die stark auf visuelle Wahrnehmung angewiesen sind (z.B. "E-Mail-Header analysieren" oder "Reconnaissance"), müssen entsprechend angepasst und durch blindengerechte Modelle, taktile Darstellungen oder detaillierte verbale Beschreibungen und praktische Übungen mit geeigneten assistierenden Technologien zugänglich gemacht werden. Auch ist der erhöhte Zeitaufwand für die Erarbeitung des Lehrstoffs zu berücksichtigen. Es ist entscheidend, dass die neuen Inhalte nicht nur theoretisch vermittelt, sondern auch praktisch erfahrbar gemacht werden, wo immer dies möglich ist, um die "Kooperationsfähigkeit, die gedankliche Mobilität sowie die Auseinandersetzung mit dem sozialen, ökonomischen und ökologischen Umfeld" zu fördern.

5.6.4.2 Zusammenfassende Analyse

Es gilt auch für den Lehrplan der Fachschule für Informationstechnik für blinde und sehbehinderte Menschen ein solides Fundament in IT-Sicherheit zu sein. Zentrale Konzepte wie Bedrohungsszenarien, Angriffsformen und Grundbegriffe der Datensicherheit sind verankert. Was jedoch fehlt, sind die bewusstseinsbildenden, praxisnahen Inhalte der Stufen 1 und 2 des CLEMENTINE-6-Stufen-Modells – darunter konkrete Verhaltensrichtlinien (z. B. „Clean Desktop“), Fallbeispiele und der explizite Umgang mit Phänomenen wie *Phishing* oder *Ransomware*.

Die vorgeschlagenen Ergänzungen verstehen sich somit nicht als Reform, sondern als gezielte Schärfung und Strukturierung bestehender Inhalte, um Cybersecurity-Kompetenzen umfassend und nachhaltig in der Sekundarstufe II zu verankern.

Hinsichtlich der didaktischen Prinzipien berücksichtigt der Lehrplan für blinde und sehbehinderte Schülerinnen und Schüler die besonderen Anforderungen eingeschränkter oder fehlender visueller Wahrnehmung. Unterrichtsmaterialien sind in Brailleschrift, digital zugänglich oder als tastbare Grafiken bereitzustellen. Dabei kommt einer verstärkten Einbindung aller Sinne – insbesondere Tasten, Spüren, Fühlen und Hören – besondere Bedeutung zu. Der Computer fungiert als zentrale Kommunikationsschnittstelle, deren effektiver

Einsatz sowie die kontinuierliche Anpassung assistierender Technologien als unverzichtbare Voraussetzung für eine gleichwertige Teilhabe am Unterricht gelten.

6 Didaktische Ansätze zur Vermittlung von Cybersecurity in der Sekundarstufe II

6.1 Existierende Ansätze: Bestehende Initiativen zur Vermittlung von Cybersecurity

In der Vergangenheit dominierte häufig die Vorstellung, dass der Mensch das schwächste Glied in der Sicherheitskette darstellt (Deterding et al., 2011b). Dieses Bild wandelt sich derzeit. Im Gegensatz zum schwächsten Glied wird der Mensch zunehmend als zentrale Schutzinstanz verstanden – als eine Art „*menschliche Firewall*“. Diese veränderte Sichtweise beeinflusst auch die Gestaltung von Vermittlungsangeboten im Bereich Cybersecurity.

Traditionelle E-Learning-Formate wurden als wenig ansprechend oder motivierend erlebt. Um Lerninhalte besser zugänglich und wirksamer zu gestalten, wurde daher zunehmend auf Gamification gesetzt – mit dem Ziel, Lernprozesse interaktiver, lebensnaher und unterhaltsamer zu gestalten. Spielerische Elemente können helfen, komplexe Inhalte greifbarer zu machen und die aktive Auseinandersetzung mit sicherheitsrelevanten Themen zu fördern (Deterding et al., 2011a). Jedoch auch dieses Modell greift zu kurz, weil die Langfristigkeit der Effekte oft nicht gegeben ist (Hamari et al., 2014). Daher rückt der Aufbau einer sogenannten „Security-Kultur“ in den Fokus. Eine solche Kultur zeichnet sich dadurch aus, dass beteiligte Akteur:innen befähigt (empowered) sind, ein grundlegendes Systemverständnis zu besitzen, sich der Konsequenzen ihres Handelns bewusst sind und Verantwortung füreinander übernehmen. Ziel ist es, ein Bewusstsein zu schaffen, das über bloße Wissensvermittlung hinausgeht – hin zu einer reflektierten, sicherheitsbewussten Haltung im digitalen Raum durch eine Vielzahl von Akteur:innen (siehe Abbildung 10).

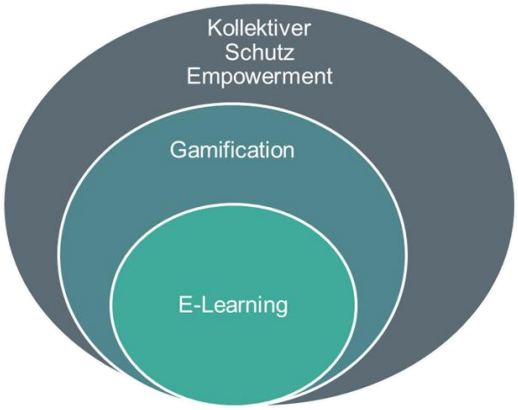

Abbildung 10: Vermittlungsformate von Cybersecurity Themen

Auf Basis aktueller Trends und Bemühungen im Bereich der Cybersecurity-Vermittlung lässt sich eine Vielzahl an Initiativen identifizieren, die sich gezielt an Kinder und Jugendliche richten. Diese Initiativen verfolgen unterschiedliche pädagogische Ansätze – von gamifizierten Formaten über schulische Projekte bis hin zu Workshop-Angeboten **und online Tools und Plattformen** – und spiegeln eine wachsende Vielfalt an Methoden und Zugängen wider. In der folgenden Tabelle 9 haben wir Angebote zusammengefasst. Die Übersicht umfasst Programme aus Österreich sowie international relevante Initiativen, etwa aus Deutschland, den USA und den Niederlanden. Eine weitere Idee wurde im Rahmen der Interviews formuliert:

Vermittlung von Cybersecurity Inhalten als Krimi/True Crime – Lernen durch Spannung

Zur Vermittlung von Cybersecurity-Inhalten wurde im Interview das Potenzial von Krimi- und True-Crime-Formaten hervorgehoben (aufgrund der Erfahrung in den Vorträgen zu dieser Thematik). Anstatt mit rein technischen Grundlagen wie Binärrechnung zu starten, könne man Jugendliche stärker erreichen, wenn man reale Angriffsszenarien als spannende Geschichten aufbereitet – etwa das „Jagen von Hackern“. Solche Geschichten sind spannend und erzeugen hohe Aufmerksamkeit. Gleichzeitig wurde auf die pädagogische Verantwortung hingewiesen: Die Darstellung muss sorgfältig erfolgen, um nicht die Faszination für die Täterseite zu fördern – etwa durch Anekdoten über das Darknet, die unerwünschte Neugier wecken können.

Tabelle 9: Liste von Cybersecurity Vermittlungsangeboten

Name	Beschreibung
Gamifizierte Cybersecurity Spiele für die Zielgruppe Kinder und Jugendliche	
HackShield	HackShield ist ein spielerisches Lernangebot für Kinder von 8 bis 12 Jahren, bei dem sie durch das Lösen von Rätseln und das Beantworten von Fragen zu sogenannten Cyber Agents ausgebildet werden. Sie lernen dabei, sich selbst und ihr Umfeld – wie Freund:innen, Eltern oder Großeltern – vor Online-Gefahren zu schützen. Das Spiel ist webbasiert, weltweit verfügbar (bereits über 350.000 Teilnehmende) und eignet sich durch begleitende Unterrichtsmaterialien sowie einen Lehrkräfte-Account besonders gut für den Einsatz im Schulunterricht. Entwickelt wurde es von der niederländischen Organisation JoinHackShield. (https://nl.joinhackshield.com/en).
Cyber Castle Challenge	Cyber Castle Challenge ist ein Minecraft-basiertes Lernspiel für Kinder und Jugendliche ab 12 Jahren, das vom australischen Questacon entwickelt wurde. In vier Spiellevels verteidigen die Spieler:innen ihr Cyber-Schloss gegen angreifende Cyber-Füchse und schützen die dort lebenden Hühner. Dabei lernen sie spielerisch grundlegende Konzepte der IT-Sicherheit – etwa durch Identitätsprüfungen, Verteidigungsmechanismen und das Management digitaler Zugänge. Das Spiel kann auf PC, Laptop oder Tablet gespielt werden. Ergänzende Unterrichtsmaterialien stehen online zur Verfügung, um die „Cyber Castle Challenge“ im Schulunterricht einzusetzen. (https://education.minecraft.net/en-us/lessons/cyber-castle-challenge).
Cybersecurity Quiz	Etwas erfahrenere Kinder und Jugendliche ab etwa 14 Jahren können mit dem Cybersecurity Quiz ihre Kenntnisse zur Onlinesicherheit spielerisch testen und vertiefen. In Quizduellen treten sie gegeneinander an und beantworten Fragen zu Themen wie Cyberbedrohungen, Online-Betrug, Datenschutz und Cybermobbing. Das Quiz eignet sich dabei nicht nur für Jugendliche, sondern auch für Erwachsene. Es steht sowohl als Desktop-Anwendung als auch als mobile App für Android und iOS zur Verfügung. Entwickelt wurde das Angebot von ÖIAT in Kooperation mit ovos play und SBA Research (AT) und ist in deutscher und englischer Sprache verfügbar (https://ovosplay.com/cybersecurity-quiz).
Jakob und die Cybermights	Die Cybermights ist ein interaktives Abenteuerspiel für Kinder ab 10 Jahren, in dem die Spieler:innen den Schüler Jakob an seinem ersten Tag an einer neuen Schule begleiten. Als ein gefälschtes Online-Profil seiner Mitschülerin Nicole für Aufregung sorgt, begeben sich die Spieler:innen gemeinsam mit Jakob auf Spurensuche, um den Vorfall aufzuklären. Im Verlauf des Spiels erhalten sie Nachrichten, die sich mit Themen wie Cybermobbing, Fake-Accounts, Spam und Internetsicherheit befassen. Das Spiel vermittelt auf spielerische Weise zentrale Aspekte der digitalen Sicherheit und fördert Medienkompetenz durch aktives Mitdenken und Interaktion. Entwickelt wurde es von mmc games (DE). (https://die-cybermights.de/)
Spoofy	Spoofy richtet sich an Kinder ab 6 Jahren und lädt sie ein, fünf verschiedene Welten zu entdecken: Schule, Park, Omas Haus, Geburtstagsparty und Straße. In diesen Umgebungen begegnen sie digitalen Gefahren und Herausforderungen – von respektvoller Online-Kommunikation und dem Umgang mit Freundschaftsanfragen bis hin zu sicheren Passwörtern, Spam-Mails und Internet-Betrug. Das Spiel ist als Desktop-Anwendung sowie als mobile App für Android und iOS verfügbar und wurde von CGI Eesti aus Estland entwickelt. (https://spoofy.ee/en)

Escape Fake	Escape Fake ist ein kostenloses Augmented-Reality-Spiel für 12- bis 18-Jährige. Die Spieler:innen durchlaufen einen digitalen Escape Room, in dem sie Fake News entlarven müssen, um die Zukunft zu retten – mit thematischen Bezügen zu Internetbetrug. Das Angebot umfasst zudem ein Toolkit und einen begleitenden MOOC (Massive Open Online Course) für Pädagog:innen. Entwickelt von der Polycular GmbH aus Österreich. (https://escapefake.org/de/)
CyberXscape	CyberXscape ist ein digitales Escape-Game für 12- bis 18-Jährige. Die Spieler:innen müssen Sicherheitslücken schnell aufdecken und dabei ihre Kompetenzen im Bereich Cybersecurity stärken. In der aktuellen Version liegt der Fokus auf Themen wie Passwörter, ungesperrte Geräte und sensible Daten. Entwickelt von der Polycular GmbH aus Österreich. (https://cyber-x-scape.at)
„Wo ist Goldi? – Sicher Surfen im Netz“	Wo ist Goldi? ist ein Abenteuerspiel für Kinder ab 8 Jahren, in dem sie digitale Gefahren wie Cybermobbing und Fake News kennenlernen. Die Spieler:innen schlüpfen in die Rolle eines Schulkindes und lösen in fünf Episoden verschiedene digitale Rätsel, während sie nach dem Klassen-Goldfisch suchen. Dabei testen sie spielerisch ihr Medienwissen. Entwickelt vom Bayerischen Staatsministerium für Digitales, ist das Spiel als mobile App für Android und iOS verfügbar. (https://www.stmd.bayern.de/themen/wo-ist-goldi)
Interland	Interland richtet sich an Kinder ab 7 Jahren und bietet vier verschiedene Spielwelten, in denen sie lernen, sich gegen Hacker, Phishing-Angriffe und Cybermobbing zu schützen. Das Spiel ist Teil des „Be Internet Awesome“-Programms von Google, das digitale Kompetenzen vermittelt und zusätzlich kostenfreie Materialien für Eltern und Lehrkräfte bereitstellt. „Interland“ ist als Webbrowser-Spiel verfügbar. (https://beinternetlegends.withgoogle.com/en_ie/interland)
„Digital? Sicher!“	Das vom Land Steiermark finanzierte Projekt „Digital? Sicher!“ richtete sich an Jugendliche der 9. bis 13. Schulstufe und verfolgte das Ziel, das Bewusstsein für Cybersecurity und einen verantwortungsvollen Umgang mit Daten zu stärken. Im Zentrum des Projekts stand die Entwicklung und Evaluation einer spielerischen Lern-App, die auf dem Prinzip des Serious Gaming basiert. Ergänzt wurde das Angebot durch praxisnahe Fallbeispiele aus der steirischen Wirtschaft, um die Relevanz der Inhalte im Alltag der Jugendlichen zu verdeutlichen. Die Lerninhalte gliederten sich in fünf Module: Erstellung eines sicheren Accounts, Privatsphäre, Datafication, Cyberangriffe sowie Reflexion und Nachbearbeitung. (https://www.digitalekompetenzen.gv.at/Good-Practice/Good-Practice/Good-Practice-2.html)
CyberSprinters	CyberSprinters ist ein interaktives Lernspiel für Kinder im Alter von 7 bis 11 Jahren, das vom britischen National Cybersecurity Centre (UK) entwickelt wurde. In verschiedenen, spielerisch gestalteten Herausforderungen – etwa als Rätsel oder Bingo-Spiel – lernen Kinder grundlegende Sicherheitspraktiken wie das Erstellen sicherer Passwörter, das Erkennen von Phishing-Mails oder den Umgang mit Zwei-Faktor-Authentifizierung. Das Spiel ist webbasiert und kostenlos verfügbar und eignet sich besonders für den Einsatz im Schulunterricht. (https://www.ncsc.gov.uk/collection/cybersprinters).

Challenges bzw. Wettbewerbe

Cybersecurity Challenge Austria	Nationale Hacking-Challenge von CSA (Cybersecurity Austria) für Schüler:innen und Studierende ab 14 Jahren, mit Vorrunden und Finalbewerben. Ein Programm, um Jugendliche früh für das Thema Hacking zu begeistern. Hier werden auch vor allem Lehrkräfte miteinbezogen, die einen Multiplikatoreffekt haben (https://verbotengut.at).
Online-Plattformen, Simulationen oder Tools für Cybersecurity Trainings für Schulen bzw. Schüler:innen	
HackTheBox	Online-Plattform mit realitätsnahen Hacking-Simulationen in virtuellen Maschinen zur spielerischen Förderung von Hacking-Kompetenzen (https://www.hackthebox.com)
TryHackMe	Interaktive, geführte Lernplattform für Hacking- und Sicherheitsgrundlagen mit Gamification-Elementen (https://tryhackme.com).
Hacking Lab	Schweizer Plattform zur Schulung von IT-Sicherheitskompetenzen durch virtuelle Übungen (https://hacking-lab.com).
Hacker School	Die Hacker School in Deutschland will Kinder und Jugendliche für das Programmieren begeistern. Verschiedene Programmiersprachen (Python, JavaScript, HTML, CSS, Scratch) können erlernt werden. Es kann auch gelernt werden Roboter zu programmieren. Die Kurse werden sowohl online als auch vor Ort in Schulen durchgeführt. Die Angebote sind für Schulen kostenlos (https://hacker-school.de).
Hack the box	Hack The Box ist eine internationale Plattform (aus UK), die praxisnahe Cybersecurity-Trainings in Form von virtuellen Maschinen, Challenges und gamifizierten Lernpfaden anbietet. Besonders im Bereich der HTLs in Österreich wird Hack The Box häufig genutzt, da viele Angebote kostenlos zugänglich sind. Die Plattform bietet hochwertige Tutorials und Trainingsmöglichkeiten – vom Einstieg bis zum fortgeschrittenen Niveau – und eignet sich besonders für den schulischen Einsatz im Bereich der Cybersecurity. (https://www.hackthebox.com/)
Vorsicht, Falle!	Watchlist Internet aus Österreich bietet für Schulen ein Präventionstool gegen Internetbetrug an: Simulierte Onlinefallen – etwa Phishing-Mails, Fake-Shops oder gefälschte Investmentplattformen – sensibilisieren Schüler:innen auf realitätsnahe Weise für Betrugsgefahren im Netz. Die Fallen können über soziale Kanäle an Freund:innen oder Bekannte weitergeleitet werden. Wer darauf hereinfällt, erleidet keinen echten Schaden, sondern wird rechtzeitig informiert und erhält Hinweise sowie Tipps zum sicheren Umgang. (https://www.watchlist-internet.at/vorsicht-falle)
Workshops und Kurse	
Saferinternet.at	Saferinternet.at ist die zentrale österreichische Anlaufstelle für Fragen rund um den sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien. Als nationaler Partner im Safer-Internet-Netzwerk der Europäischen Union richtet sich das Angebot insbesondere an Kinder, Jugendliche, Eltern sowie Lehrende. Für junge Menschen ab etwa 10 Jahren werden spezifische Cybersecurity-Workshops angeboten. Darüber hinaus finden sich auf der Website umfangreiche, didaktisch aufbereitete Unterrichtsmaterialien – beispielsweise zu Internetbetrug – zur Unterstützung von Lehrkräften im Schulalltag. Für Jugendliche selbst bietet Saferinternet.at zielgruppengerechte Informationen, Tipps und Tools zum sicheren Umgang mit Handy und Internet – unter anderem in Form von Schnitzeljagden, Quizzes, Social-Media-Formaten und Flyern. Die

	behandelten Themen reichen von Cybermobbing über Fake News und Influencer-Kultur bis hin zum verantwortungsvollen Umgang mit digitalen Geräten. (https://www.saferinternet.at/zielgruppen/jugendliche)
UNDER 18	Das polizeiliche Präventionsprogramm „UNDER 18“ richtet sich an Jugendliche zwischen 13 und 17 Jahren und thematisiert im schulischen Setting zentrale Online-Gefahren wie Cybermobbing, Sextorsion und Grooming. Es ermöglicht eine altersgerechte Auseinandersetzung mit digitalen Risiken in einem geschützten Rahmen. Ergänzt wird das Angebot durch Materialien für Lehrkräfte und Elternabende, um auch das Umfeld der Jugendlichen einzubinden. Bereits ab zehn Jahren setzt das Teilprojekt „Click & Check“ an und fördert den verantwortungsvollen Umgang mit digitalen Medien. (https://www.bundeskriminalamt.at/205/start.aspx)
Digitale Lernwerkstatt	Die Digitale Lernwerkstatt ist ein frei zugängliches Online-Angebot, das grundlegendes Hintergrundwissen zur Digitalisierung vermittelt – interaktiv, niederschwellig und vollständig digital. Die Plattform richtet sich an Lehrende, Schüler:innen und alle Interessierten und stellt eine Vielzahl an Onlinekursen sowie begleitenden Unterrichtsmaterialien bereit. Ziel ist es, zentrale Zusammenhänge der digitalen Welt verständlich und praxisnah zu vermitteln. (https://de.digitale-lernwerkstatt.com/home)
Epicenter Academy	Das Workshopangebot „Digitale Selbstverteidigung für Schüler:innen“ der epicenter.academy GmbH (AT) richtet sich an Jugendliche ab 12 Jahren in der Sekundarstufe I, II sowie in Berufsschulen. In zielgruppenspezifischen Workshops vermitteln eigens ausgebildete Trainer:innen praxisnahe Kompetenzen für den sicheren Umgang mit digitalen Technologien und zur Stärkung der digitalen Selbstbestimmung. (https://epicenter.academy/workshops/workshops-schulen)
ECDL/ICDL Führerschein	Der ICDL (International Certification of Digital Literacy) ist eine zertifizierte digitale Zusatzausbildung, die ab der 1. Oberstufe (ab etwa 10 Jahren) angeboten wird und ein eigenes Modul zur Cybersecurity umfasst. Dieses Modul unterstützt Schüler:innen dabei, ein fundiertes Verständnis für digitale Sicherheit zu entwickeln. Der ICDL wird von der OCG (Österreichische Computer Gesellschaft) getragen und deckt die Inhalte des österreichischen Lehrplans zur Digitalen Grundbildung nahezu vollständig ab – und geht in vielen Bereichen darüber hinaus. Durch den modularen Aufbau kann der ICDL flexibel in den Unterricht integriert werden und bildet in zahlreichen Schulen bereits die Grundlage für den IT-Unterricht. Das Programm richtet sich an Lehrkräfte, Eltern und Schüler:innen und fördert selbstbestimmtes, kompetentes Lernen im digitalen Raum. (https://www.icdl.at/icdlschulen)
CAP.	CAP. bietet eine umfassende Ausbildung im Bereich Cybersecurity, die Jugendliche parallel zur AHS absolvieren können. Die Ausbildung erstreckt sich über insgesamt neun Semester. In den ersten beiden Semestern werden grundlegende Inhalte vermittelt, einschließlich sozialer und persönlicher Kompetenzen sowie Projektmanagement. Ab dem dritten Semester (ab der 6. AHS-Klasse, also in der Oberstufe) vertiefen die Teilnehmer:innen ihre Kenntnisse im Rahmen des sogenannten "Cyberprofessional"-Tracks. Den Abschluss bildet eine rund eineinhalbjährige Projektarbeit, die mit einer Präsentation vor einer Kommission endet. Nach erfolgreichem Abschluss erhalten die Jugendlichen einen anerkannten Lehrabschluss im Bereich Cybersecurity. (https://www.cap-ausbildung.eu/leistungen/cybersecurity/)

Cybersecurity Trainingsangebote für Unternehmen (Auswahl[29])

Fortress vs. Hackers	Das gamifizierte IT-Security- und Awareness-Planspiel der nextbeststep GmbH (AT) vermittelt spielerisch Grundlagen der Cybersecurity mit Fokus auf menschliches Verhalten. In Gruppen aufgeteilt in „Hacker“ und „Sicherheitsmanagement“, analysieren die Teilnehmenden alltagsnahe Szenarien, bewerten Risiken, entwickeln Strategien und setzen Ressourcen gezielt ein. (https://www.nextbeststep.at/produkte/fortress-vs-hackers)
Deepspace-Danger	Deepspace Danger ist ein gamifiziertes Lernspiel zur Security Awareness für Mitarbeitende, entwickelt von Infosec (US). In einer futuristischen Weltraumumgebung übernehmen Spielende die Verantwortung für einen KI-Computer mit sensiblen Daten. Die Handlung wird durch animierte Videos erzählt, die durch Multiple-Choice-Fragen ergänzt werden. (https://www.infosecinstitute.com/iq/content-library/deep-space-cybersecurity-game/)
Cybersecurity E-Learning	Das Cybersecurity E-Learning von SoSafe (DE) bietet ein interaktives Lernerlebnis für Mitarbeitende. Durch gamifizierte Module werden sichere Verhaltensweisen spielerisch gefestigt – mit dem Ziel, die gesamte Organisation wirksam vor Cyberbedrohungen zu schützen. (https://sosafe-awareness.com/)
Cyberplanspiel	Seit 2012 veranstaltet das Kompetenzzentrum Sicheres Österreich (KSÖ) regelmäßig Cyber-Planspiele, bei denen Behörden und Wirtschaftsvertreter fiktive, realistische Cyberangriffe bewältigen. Ziel ist es, interne Krisenprozesse und die organisationsübergreifende Zusammenarbeit zu testen. Das DACH-Planspiel 2021 wurde gemeinsam mit dem BKA, BMI, BMLV, BMF und internationalen Partnern (NCSC, BSI) durchgeführt. Die technische Grundlage bildete die „AIT CyberRange“ als Simulationsumgebung. (https://kompetenzzentrum-sicheres-oesterreich.at/2024/08/21/ksoe-ait-und-das-haus-der-digitalisierung-veranstalteten-cybersicherheitstraining-fuer-die-oesterreichische-wirtschaft)
baksecure	In diesem Lernspiel schlüpfen die Spielenden in die Rolle der Geschäftsleitung eines fiktiven Unternehmens und müssen Cybersecurity-Maßnahmen wie Backups, Schulungen oder Passwortrichtlinien strategisch einsetzen – und gleichzeitig den laufenden Betrieb am Laufen halten. Herausforderungen wie Lieferengpässe oder Maschinenausfälle erschweren den Alltag zusätzlich. Immer wieder treten Cyberangriffe auf, die abgewehrt werden müssen. Entwickelt von der Technischen Akademie für berufliche Bildung Schwäbisch Gmünd. (https://baksecure.de/spiele)

[29] Es gibt zahlreiche Spiele für die Zielgruppe Unternehmen, um Themen rund um Cybersecurity im Rahmen von organisationaler Weiterbildung zu vermitteln. In diesem Bericht wird eine Auswahl an möglichst unterschiedlichen Ansätzen gelistet.

7 Digitale Medien in der schulischen Cyber-Sicherheitsbildung: Eine didaktische Analyse von Wirksamkeit und Praktikabilität

Die Vermittlung von Cybersicherheit in Schulen gewinnt zunehmend an Bedeutung, da Kinder und Jugendliche früh mit digitalen Medien in Kontakt kommen. Ein erfolgreicher Cyber-Sicherheitsunterricht erfordert geeignete Lehrmittel, konkrete Unterrichtskonzepte zu relevanten Themen, fundierte didaktische Ansätze sowie eine klare Einteilung digitaler Bildungsmedien. Im Folgenden werden digitale Lehrmittel und Plattformen vorgestellt, beispielhafte Unterrichtseinheiten skizziert, didaktische Modelle diskutiert und eine Klassifikation digitaler Medien für Cybersicherheit-Themen erläutert – ergänzt durch Beispiele aus dem deutschsprachigen Raum und internationalen Bildungsprogrammen.

7.1 Einleitung: Cyber-Sicherheit als Schlüsselkompetenz im 21. Jahrhundert

7.1.1 Die Dringlichkeit der Cyber-Sicherheitsbildung

Die fortschreitende Digitalisierung aller Lebensbereiche hat auch die Bildungslandschaft fundamental verändert. Vor diesem Hintergrund ist die Vermittlung von Cyber-Sicherheitskompetenzen keine optionale Ergänzung des Informatikunterrichts und der digitalen Bildung. Es geht nicht mehr nur darum, auf einen externen, unaufhaltsamen Prozess der Digitalisierung zu reagieren, sondern darum, diesen aktiv und sicher zu gestalten. Ziel der schulischen Bildung muss es sein, Kinder und Jugendliche zu stärken und sie zu befähigen, Daten, das Internet und digitale Technologien verantwortungsbewusst, kritisch und sicher zu nutzen (Bundesministerium für Bildung, 2025b; Bundesministerium für Finanzen, n.d.)

Die zentrale Prämisse einer modernen Cyber-Sicherheitsbildung im schulischen Kontext geht dabei über rein technische Schutzmaßnahmen hinaus. Während Firewalls, Antivirenprogramme und sichere Netzwerkkonfigurationen die unverzichtbare Basis bilden, zeigt die Realität, dass die größte Schwachstelle oft nicht die Technologie, sondern der Mensch ist (Bartels, 2023). Angreifer:innen zielen bewusst auf menschliche Faktoren wie Neugier, Hilfsbereitschaft oder Angst ab, um durch Social Engineering und Phishing-Angriffe in Systeme einzudringen. Daraus leitet sich ein fundamentaler pädagogischer Leitsatz ab: Das primäre Ziel der Cyber-Sicherheitsbildung ist die Stärkung der „menschlichen Firewall“ (Mühlenbeck 2025). Es geht in der Allgemeinbildung weniger darum, jede:n Schüler:in zu eine:r IT-Expert:in auszubilden, als vielmehr darum, eine Kultur der Achtsamkeit und ein kritisches, sicherheitsbewusstes Denken zu kultivieren. Die Wirksamkeit digitaler Bildungsmedien muss sich daher daran messen lassen, inwieweit sie nicht nur Wissen vermitteln, sondern nachhaltig das Verhalten prägen und die Urteilsfähigkeit der Lernenden stärken (Brüggen et al., 2019; Foisy, 2024; Gulyamov et al., 2024).

7.1.2 Definition zentraler Lernziele und Kompetenzbereiche

Um digitale Medien zielgerichtet auswählen und bewerten zu können, bedarf es einer klaren Definition der zu fördernden Kompetenzen. Diese lassen sich in drei ineinandergreifende Bereiche gliedern, die gemeinsam das Fundament für eine umfassende digitale Souveränität bilden (Zhilisbayev, 2023).

Fachkompetenz: Dieser Bereich umfasst das grundlegende Wissen über die digitale Welt und ihre Bedrohungen. Schüler:innen sollen die zentralen Begriffe, Prinzipien und Mechanismen der Cyber-Sicherheit verstehen. Dazu gehört das Wissen über die Funktionsweise und Erkennung von Phishing-Mails, Malware (Viren, Trojaner, Ransomware) und Social-Engineering-Taktiken. Sie lernen, was ein sicheres Passwort ausmacht und warum Passwort-Manager sinnvolle Werkzeuge sind. Ein weiterer Kernpunkt ist das Verständnis für die grundlegenden Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit von Daten – sowie die Relevanz gesetzlicher Regelungen wie der Datenschutz-Grundverordnung (DSGVO). Die Lernenden sollen die Motivationen von Cyberkriminellen ebenso nachvollziehen können wie die Aufgaben von Sicherheitsexperten.

Medienkompetenz: Aufbauend auf der Fachkompetenz zielt die Medienkompetenz auf die Fähigkeit zur kritischen Reflexion und Anwendung ab (Baacke, 1997; Schirmer et al., 2024; Schüller et al., 2021). Es geht darum, Informationsquellen im Internet kritisch zu hinterfragen und Manipulationsstrategien wie Fake News, Deepfakes oder Clickbait zu erkennen. Die Schüler:innen entwickeln ein Bewusstsein für den Wert und die Schutzwürdigkeit ihrer persönlichen Daten und lernen, die Konsequenzen der Preisgabe von

Informationen in sozialen Netzwerken oder Apps abzuschätzen. Diese Kompetenz befähigt sie, nicht nur Regeln zu befolgen, sondern die Notwendigkeit von Sicherheitsmaßnahmen zu verstehen und ihr eigenes digitales Verhalten bewusst zu steuern.

Sozialkompetenz: Cyber-Sicherheit ist keine rein individuelle Angelegenheit, sondern hat eine starke soziale Dimension. Die Förderung der Sozialkompetenz zielt auf einen verantwortungsbewussten und respektvollen Umgang in der digitalen Kommunikation ab. Dazu gehört die Einhaltung einer „Netiquette“ und das Verständnis für die gravierenden Auswirkungen von Cyber-Mobbing. Die Schüler:innen lernen die Tragweite von Cyberangriffen nicht nur für sich selbst, sondern auch für Unternehmen, die Gesellschaft und staatliche Institutionen einzuschätzen. Sie werden ermutigt, ihr Wissen zu teilen und sich gegenseitig zu unterstützen, um ein sichereres digitales Umfeld für alle zu schaffen.

Fachkompetenz, Medienkompetenz und Sozialkompetenz lassen sich sehr gut auf die didaktischen Modelle des Dagstuhl-Dreiecks und des Frankfurt-Dreiecks abbilden, welche die informatische bzw. digitale Bildung strukturieren (Schirmer et al., 2024; Schüller et al., 2021):

- **Fachkompetenz** entspricht der technologischen und anwendungsorientierten Perspektive des Dreiecks und umfasst das grundlegende Wissen über digitale Systeme und deren sichere Nutzung.
- **Medienkompetenz** verbindet die Anwendungs- und die soziokulturelle Perspektive, indem sie den kritischen Umgang mit Informationen und die Reflexion des eigenen digitalen Verhaltens in den Mittelpunkt stellt.
- **Sozialkompetenz** ist fest in der soziokulturellen Perspektive verankert und konzentriert sich auf verantwortungsvolle digitale Interaktion und das Verständnis für gesellschaftliche Auswirkungen.

7.2 Didaktische Grundlagen und Klassifikation digitaler Bildungsmedien

Die Auswahl geeigneter digitaler Medien für die Cyber-Sicherheitsbildung erfordert einen strukturierten Analyserahmen, der über rein technische Merkmale hinausgeht und die pädagogische Eignung in den Mittelpunkt stellt. Auf Basis dieses Rahmens lässt sich eine Klassifikation von Medienformaten entwickeln, die Lehrkräften als Orientierung für eine didaktisch sinnvolle Unterrichtsgestaltung dienen kann.

7.2.1 Analyserahmen für digitale Bildungsmedien

Um die Wirksamkeit und Praktikabilität digitaler Medien zu bewerten, werden folgende didaktische Kriterien herangezogen, die sich aus der Analyse der Forschungsliteratur ableiten (Brägger & Rolff, 2024; Seidel & Krapp, 2014):

- **Interaktivität**: Dieses Kriterium beschreibt das Ausmaß, in dem ein Medium den Lernenden aktive Eingriffe und Entscheidungen ermöglicht, die über eine simple Navigation hinausgehen. Echte Interaktivität fördert das Engagement, indem sie die Lernenden von passiven Konsumenten zu aktiven Teilnehmern macht, die Probleme lösen und auf simulierte Ereignisse reagieren.
- **Adaptivität**: Adaptive Lernmedien können ihre Inhalte, Aufgaben oder den Schwierigkeitsgrad an die individuellen Leistungen und Bedürfnisse der Lernenden anpassen. Ein solches System kann beispielsweise einem Schüler, der Schwierigkeiten bei der Erkennung von Phishing-Merkmalen zeigt, gezielt zusätzliche Übungen anbieten, während ein fortgeschrittener Lernender anspruchsvollere Szenarien erhält. Dies ermöglicht eine hochgradig individualisierte Förderung (Knogler, M. et al., 2018).
- **Multimedialität & Anschaulichkeit:** Die Fähigkeit, komplexe und oft abstrakte Konzepte der Cyber-Sicherheit durch die sinnvolle Verknüpfung verschiedener medialer Formate (Text, Bild, Audio, Video, Animation, Simulation) verständlich zu machen, ist ein entscheidender Vorteil digitaler Medien. Ein gut gestaltetes Erklärvideo kann die Funktionsweise eines Trojaners anschaulicher vermitteln als reiner Text.
- **Kollaborationspotenzial**: Einige Medienformate sind explizit darauf ausgelegt, die Zusammenarbeit zwischen Schüler:innen zu fördern. Gemeinsames Lösen von Rätseln, Diskussionen über ethische Dilemmata oder die kollaborative Arbeit an einem Sicherheitsprojekt stärken nicht nur die Sozialkompetenz, sondern auch das tiefere Verständnis durch den Austausch von Perspektiven.

- **Feedback-Mechanismen**: Die Qualität des Feedbacks ist für den Lernerfolg von zentraler Bedeutung. Es gibt laut Hattie (Zierer et al., 2015) Feedback, das auf Aufgabenebene gegeben werden kann, Feedback auf Prozessebene, Feedback auf Selbstregulationsebene und Feedback auf Selbstebene. Feedback auf der Ebene der Aufgabe wird in diesem Kontext hervorgehoben und von der Frage geleitet „Wie gut wurde eine Aufgabe verstanden bzw. erledigt?“ Idealerweise ist das Feedback unmittelbar, konstruktiv und handlungsorientiert. Digitale Lernmedien ermöglichen automatisiertes und differenziertes Feedback sowie ein Fortschrittsmonitoring.
- **Problem- und Handlungsorientierung**: Besonders wirksame Lernmedien konfrontieren die Lernenden mit authentischen, lebensnahen Problemstellungen und ermöglichen es ihnen, reale Handlungsstrategien in einer sicheren, geschützten Umgebung zu erproben. Dies unterstützt den Transfer von theoretischem Wissen in praktisches Können und stärkt die Handlungssicherheit im Ernstfall (McGettrick, 2013).

7.2.2 Klassifikation der Medienformate

Basierend auf dem Grad der Interaktivität und der Komplexität der Lernanforderung lassen sich die für die Cyber-Sicherheitsbildung relevanten digitalen Medien in vier Hauptkategorien einteilen. Diese Kategorien stellen eine aufsteigende Skala dar, die von der reinen Informationsaufnahme bis zur aktiven, strategischen Problemlösung reicht (Gulyamov et al., 2024).

- **Kategorie 1: Informations-, Präsentations- und Visualisierungsmedien**: Diese Medien dienen primär dem Transfer von Faktenwissen und der Sensibilisierung für grundlegende Themen. Sie sind oft der Einstiegspunkt in ein neues Thema und zeichnen sich durch eine geringe Interaktivität aus (Young et al., 2024).
  - **Beispiele**: Erklärvideos zu Themen wie Phishing oder sicheren Passwörtern, interaktive PDF-Arbeitsblätter, digitale Poster und Infografiken, Präsentationsfolien für den Lehrkräftevortrag sowie Karikaturen, die als Impuls für Diskussionen dienen.
- **Kategorie 2: Strukturierte Lernumgebungen**: Hierbei handelt es sich um in sich geschlossene digitale Kurse, die Lernende durch einen vordefinierten, sequenziellen Lernpfad führen. Sie kombinieren oft verschiedene Medienformate aus Kategorie 1 und reichern diese mit einfachen interaktiven Elementen an (Arsenovych et al., 2024).
  - **Beispiele**: Online-Kurse und MOOCs (Massive Open Online Courses) von Anbietern wie Cisco Networking Academy[30], Saferinternet.at[31], internet-abc[32] oder kommerziellen Plattformen wie Lehrer-Online[33] und Future Learn[34]. Diese Kurse umfassen typischerweise Lektionen mit Videos, Texten und abschließenden Quiz zur Wissensüberprüfung.
- **Kategorie 3**: **Gamifizierte Anwendungen und „Serious Games“**: Diese Kategorie nutzt spielerische Elemente (Gamification), um die Motivation, das Engagement und den Lernerfolg zu steigern. Der Fokus liegt auf aktivem Lernen durch Interaktion in einem spielerischen Kontext (Jin et al., 2018; Videnovik et al., 2025).
  - **Beispiele**: Interaktive Quizz und Wissens-Duelle, narrative Abenteuerspiele („Serious Games“) wie „Wo ist Goldi?“[35] oder „HackShield“[36], sowie themenspezifische Minispiele wie der „Phishing Master“[37] zum Erkennen gefälschter E-Mails.
- **Kategorie 4**: Immersive und komplexe Simulationen: Dies ist die höchste Stufe des interaktiven Lernens. Diese Medien bilden komplexe Systeme und Szenarien realitätsnah ab und fordern von den

[30] Online-Kurs Cyber-Sicherheit: https://www.lehrer-online.de/unterricht/sekundarstufen/naturwissenschaften/informatik/unterrichtseinheit/ue/online-kurs-cyber-sicherheit/
[31] Saferinternet.at: https://www.saferinternet.at/
[32] Internet-abc: https://www.internet-abc.de/lehrkraefte/lernmodule/
[33] Lehrer-Online: https://www.lehrer-online.de/
[34] Future-Learn: https://training.safetyculture.com/blog/de/12-kostenlose-cybersecurity-kurse/
[35] Cybersicherheit für Kinder: Die besten interaktiven Online-Spiele - Onlinesicherheit, https://www.onlinesicherheit.gv.at/Services/News/Cybersicherheit-Onlinespiele-Kinder.html
[36] So macht Cybersicherheit Spaß!: https://hackshieldgame.com
[37] Die Macht der Mini-Spiele - Cybersecurity Awareness Playbook: https://phishing-master.secuso.org/ Phishing Master

Lernenden strategische Entscheidungen und die Anwendung von Wissen unter Druck. (Corradini, 2020)

- **Beispiele**: Phishing-Simulationen, bei denen realistische Phishing-Mails an Lernende gesendet werden, um deren Reaktion zu testen und zu schulen; Krisensimulationen wie „Cyber-Escape-Rooms“[38] die eine team-basierte Reaktion auf einen Cyberangriff erfordern; Netzwerksimulationen wie „Filius“[39]; sowie hochtechnische „Capture the Flag“ (CTF) Wettbewerbe, die sich auf das Lösen komplexer Sicherheitsrätsel konzentrieren.

7.3 Analyse ausgewählter Medienformate und ihrer didaktischen Potenziale

Die folgende Analyse untersucht die vier Medienkategorien detailliert hinsichtlich ihrer didaktischen Potenziale, ihrer nachgewiesenen oder postulierten Wirksamkeit und ihrer Praktikabilität für den Einsatz im schulischen Alltag[40].

7.3.1 Kategorie 1 & 2: Online-Kurse und strukturierte Lernumgebungen

Medien dieser beiden Kategorien bilden das Fundament der Wissensvermittlung in der Cyber-Sicherheitsbildung. Online-Kurse, MOOCs und Sammlungen von digitalen Arbeitsmaterialien sind darauf ausgelegt, Lernenden einen systematischen und umfassenden Überblick über ein Themenfeld zu geben.

Analyse: Der große Vorteil dieser Formate liegt in ihrer Fähigkeit, ein breites Spektrum an Inhalten strukturiert und kohärent zu präsentieren. Plattformen wie die Cisco Networking Academy bieten umfassende Kurse an, die von den Grundlagen der Datentypen und ihrer Schutzwürdigkeit bis hin zu komplexen Angriffsmethoden und den rechtlichen Rahmenbedingungen reichen. Diese Kurse sind oft modular aufgebaut, was den Lernenden ermöglicht, in ihrem eigenen Tempo zu arbeiten. Angebote wie die MOOCs von Saferinternet.at erweitern den Fokus auf verwandte Themen der „Digital Citizenship“, wie den Umgang mit Fake News, Hassrede und Verschwörungserzählungen, und schlagen so eine wichtige Brücke zwischen technischer Sicherheit und gesellschaftlicher Medienkompetenz.

Wirksamkeit: Die Effektivität dieser Medien liegt primär in der Bereitstellung von zugänglichem und gut organisiertem Faktenwissen. Sie eignen sich hervorragend, um eine gemeinsame Wissensbasis in einer Lerngruppe zu schaffen. Die integrierten Quizze und Lernkontrollen am Ende jedes Moduls helfen dabei, das Gelernte zu festigen und den eigenen Lernfortschritt zu überprüfen. Die entscheidende Schwäche liegt jedoch in der oft passiven Natur des Lernens. Das reine Konsumieren von Videos und Texten führt nicht zwangsläufig zu einer tiefgreifenden Verhaltensänderung oder zur Fähigkeit, das Wissen in neuen, unbekannten Situationen anzuwenden (Young et al., 2024). Ohne eine Ergänzung durch praktische und kollaborative Anwendungsaufgaben besteht die Gefahr, dass das erworbene Wissen träge bleibt und die langfristige Motivation der Lernenden nachlässt.

Praktikabilität: Die Praktikabilität dieser Medienformate ist als sehr hoch einzustufen. Viele hochwertige Kurse und Materialien werden von öffentlichen Stellen (z. B. BSI, Saferinternet.at) oder im Rahmen von Bildungsinitiativen (z. B. Cisco, Internet abc) kostenlos angeboten. Da sie in der Regel webbasiert sind, benötigen sie lediglich einen Computer oder ein Tablet mit Internetzugang, was sie ideal für den Einsatz im Präsenzunterricht, aber auch für Blended-Learning-Szenarien macht. Die größte Herausforderung für Lehrkräfte besteht darin, die Schülerinnen und Schüler zur selbstständigen und kontinuierlichen Bearbeitung der Kurse zu motivieren und die Inhalte durch weiterführende Diskussionen und praktische Übungen im Unterricht zu vertiefen.

[38] Escape-Room: https://www.onlinesicherheit.gv.at/Services/News/Cyber-Escape-Room.html
[39] Filius: https://www.lernsoftware-filius.de/
[40] Beispiel dafür finden Sie in der Materialsammlung Padlet Cyber Security: https://padlet.com/eis/cyber-security-vl5hxe5kxinv97zt

7.3.2 Kategorie 3: Gamification und „Serious Games“ – Der spielerische Weg zur Security Awareness

Gamifizierte Anwendungen und „Serious Games“ stellen einen Paradigmenwechsel von der reinen Wissensvermittlung hin zum erfahrungsbasierten und motivationsgesteuerten Lernen dar. Sie nutzen gezielt psychologische Mechanismen, um Lernprozesse effektiver und nachhaltiger zu gestalten.

Didaktische Wirkmechanismen: Der Erfolg von Gamification beruht nicht allein auf dem Faktor „Spaß“. Vielmehr werden grundlegende menschliche Bedürfnisse und Anliegen angesprochen, um das Lernen zu fördern (Jin et al., 2018; Moore, 2025; Videnovik et al., 2025).

- **Motivation und Engagement**: Elemente wie Punkte, Abzeichen (Badges) und Ranglisten (Leaderboards) visualisieren den Lernfortschritt und befriedigen das Bedürfnis nach sichtbarer Entwicklung, sozialer Anerkennung und Wettbewerb. Eine narrative Einbettung, also das Erzählen einer Geschichte, in die die Lernaufgaben integriert sind, schafft einen emotionalen Bezug und macht die Lerninhalte einprägsamer.
- **Aktives Lernen und Feedback**: Im Gegensatz zu passiven Lernformen fordern Spiele eine kontinuierliche aktive Teilnahme. Die Lernenden müssen Entscheidungen treffen, Rätsel lösen und auf Ereignisse reagieren. Dabei erhalten sie unmittelbares Feedback auf ihre Aktionen. Dieser Zyklus aus Aktion, Konsequenz und Feedback ermöglicht ein effektives Lernen durch Versuch und Irrtum in einer risikofreien Umgebung (Hoxhunt, 2025).
- **Verhaltensänderung**: Das übergeordnete Ziel ist die Automatisierung sicherer Verhaltensweisen. Anstelle einer langen, einmaligen Schulung setzen effektive gamifizierte Ansätze auf häufige, kurze „Mikro-Herausforderungen“ (Moore, 2025). Diese regelmäßige Wiederholung in variierenden Kontexten hilft, sichere Reaktionsmuster zu verinnerlichen, ohne dass Ermüdung oder Langeweile aufkommt.

Evaluation der Wirksamkeit: Die Forschung liefert zunehmend Belege für die Wirksamkeit von spielbasierten Ansätzen. Studien zeigen, dass „Game-Based Learning“ sehr effektiv für das Bewusstseinstraining sein kann und das Interesse an Cyber-Sicherheitsthemen steigert (Jin et al., 2018). In Evaluationen konnten bei Schülerinnen und Schülern signifikant höhere Wissensstände in Post-Tests im Vergleich zu Pre-Tests nachgewiesen werden (Hill et al., 2020; Videnovik et al., 2025). Die Wirksamkeit ist jedoch kein Selbstläufer. Sie hängt entscheidend von der Qualität des Spieldesigns ab. Ein Spiel, das didaktisch überfrachtet ist oder dessen Spielmechanik keinen Spaß macht, wird seine Ziele verfehlen. Ebenso kann eine schlechte Balance zwischen Lerninhalt und Spielelementen dazu führen, dass die Lernenden zwar das Spiel spielen, aber keinen Transfer der Lerninhalte in die Realität vollziehen. Einige Studien deuten zudem darauf hin, dass spielerische Ansätze das Interesse von Jungen und Mädchen an einer späteren Karriere in der Cyber-Sicherheit unterschiedlich stark beeinflussen können, was bei der Konzeption von Bildungsangeboten berücksichtigt werden sollte (Jin et al., 2018).

Praktikabilität: Das Angebot in dieser Kategorie ist außerordentlich breit und vielfältig, was die Praktikabilität für Schulen erhöht. Es reicht von sehr einfachen, kostenlosen und schnell einsetzbaren Werkzeugen bis hin zu aufwendig produzierten, professionellen Lernspielen. Lehrkräfte können mit Tools wie wordwall.net[41] oder QuizAcademy[42] (einer datenschutzfreundlichen Alternative zu Kahoot![43]) mit geringem Aufwand eigene Quiz, Zuordnungsspiele oder kleine Gameshows erstellen und so bestehende Unterrichtsinhalte spielerisch aufbereiten. Gleichzeitig gibt es eine wachsende Zahl an kostenlosen, webbasierten oder als App verfügbaren „Serious Games“, die speziell für die Cyber-Sicherheitsbildung entwickelt wurden und ohne große technische Hürden im Unterricht eingesetzt werden können (Jin et al., 2018).

[41] Wordwall: https://wordwall.net/
[42] QuizAcademy: https://quizacademy.de/
[43] Kahoot: https://kahoot.com/de/

Die folgende Tabelle bietet eine vergleichende Übersicht über einige repräsentative „Serious Games“, um Lehrkräften die Auswahl eines für ihre spezifischen Bedürfnisse geeigneten Mediums zu erleichtern. Die Beschreibungen der Games sind bitte der Tabelle 9 oben zu entnehmen:

Tabelle 10: Übersicht Serious Games

Spiel/Anwendung	Zielgruppe	Didaktischer Ansatz	Link
Wo ist Goldi?	Ab 8 Jahren	Narratives Point-and-Click-Abenteuerspiel, Problemlösung, Dialoge	https://www.schule.at/tools-apps/details/wo-ist-goldi
Interland	Ab 7 Jahren	Vier verschiedene Minispiele in einer Abenteuerwelt, Jump'n'Run, Puzzle	https://beinternetawesome.withgoogle.com/en_us/interland/
HackShield	8-12 Jahre	Spieler werden zu "Cyber Agents", lösen Rätsel und beantworten Fragen in verschiedenen Levels	https://global.joinhackshield.com/de
CyberSprinters	7-11 Jahre	Endlos-Runner-Spiel, bei dem Hindernissen (Cyber-Bedrohungen) ausgewichen und Power-ups (Sicherheitsmaßnahmen) gesammelt werden	https://pshe-association.org.uk/resource/cyberchoices
Cyber Security Quiz	Ab 14 Jahren	Wissensquiz im Duell-Format gegen andere Spieler oder im Einzelspielermodus	https://www.guetesiegel-lernapps.at/lern-apps/cyber-security-quiz
Phishing Master / PhishingQuiz	Sekundarstufe	Spieler müssen in kurzer Zeit entscheiden, ob eine E-Mail echt oder ein Phishing-Versuch ist	https://phishing-master.secuso.org/

7.3.3 Kategorie 4: Interaktive und komplexe Simulationen

Diese Kategorie umfasst die anspruchsvollsten digitalen Lernmedien, die auf die Entwicklung fortgeschrittener, praktischer Fähigkeiten und strategischer Kompetenzen abzielen. Sie repräsentieren anspruchsvolle Formen des handlungsorientierten Lernens.

Analyse:

- **Phishing-Simulationen**: Diese Werkzeuge, wie die Seite „Phishen Impossible“[44], gehen über das theoretische Wissen hinaus, indem sie die Lernenden mit realistischen, aber ungefährlichen Phishing-E-Mails konfrontieren. Der Lerneffekt entsteht durch die direkte Erfahrung und das unmittelbare Feedback, wenn ein Nutzer auf eine simulierte Bedrohung hereinfällt (O’Hara, 2025; Schrittwieser, 2025). Solche Simulationen sind ein Kernbestandteil moderner Security-Awareness-Programme in Unternehmen, da sie die Fähigkeit, echte Angriffe zu erkennen und zu melden, nachweislich verbessern (Rizzoni et al., 2022).
- **Krisensimulationen („Tabletop Exercises“)**: Diese Simulationen, wie das „Game of Threats“[45] von PwC, modellieren den gesamten Ablauf eines schwerwiegenden Sicherheitsvorfalls. Anstatt nur die Reaktion eines Einzelnen zu testen, fordern sie Teams (z. B. bestehend aus Schulleitung, IT-Verantwortlichen und Lehrkräften) heraus, unter Druck zu kommunizieren, Entscheidungen zu treffen und koordinierte Gegenmaßnahmen einzuleiten. Sie decken Schwachstellen in Notfallplänen und Kommunikationsketten auf.
- **“Capture the Flag“ (CTF) Wettbewerbe**: CTFs sind kompetitive, oft teambasierte Herausforderungen, bei denen die Teilnehmenden komplexe Aufgaben aus verschiedenen

[44] Phishen Impossible: https://www.phishen-impossible.at/
[45] Game of Threats: https://www.pwc.ch/de/dienstleistungen/consulting/cybersecurity/game-of-threats.html

Bereichen der IT-Sicherheit lösen müssen, z. B. das Entschlüsseln von Nachrichten (Kryptographie), das Analysieren von Schadsoftware (Reverse Engineering) oder das Finden von Schwachstellen in Webanwendungen. Sie sind ein etabliertes Format in der Ausbildung von IT-Sicherheitsprofis und eignen sich hervorragend, um Talente zu identifizieren und zu fördern.

Wirksamkeit: Die Wirksamkeit dieser Formate zur Entwicklung anwendungsbereiter Fertigkeiten ist hoch. Phishing-Simulationen führen in der Praxis zu einer signifikanten Reduzierung der Klickraten auf bösartige Links und zu einer Erhöhung der Melderate verdächtiger E-Mails. Krisensimulationen bieten unschätzbare Einblicke in die organisatorische Resilienz und bereiten Entscheidungsträger auf den Ernstfall vor. CTFs sind der Goldstandard für das Training technischer Fähigkeiten und des „Hacker-Mindsets“, das für die Verteidigung von Systemen notwendig ist (Huitema & Wong, 2025).

Praktikabilität: Hier liegt die größte Hürde für den breiten Einsatz in Schulen. Komplexe Krisensimulationen und CTFs sind in der Regel auf fortgeschrittene Schüler der Sekundarstufe II, Studierende oder Fachkräfte ausgerichtet. Sie erfordern eine erhebliche technische Vorbereitung und eine intensive Betreuung durch fachkundige Lehrkräfte oder externe Mentoren. Viele der professionellen Simulations-Tools sind kommerzielle Produkte und mit hohen Kosten verbunden. Auch Phishing-Simulationen, obwohl konzeptionell einfacher, bedürfen einer sorgfältigen didaktischen Planung. Werden sie unsensibel eingesetzt, können sie bei Schülerinnen und Schülern zu Verunsicherung, Demotivation oder einem Gefühl des Bloßgestellt Werdens führen, was dem Lernziel entgegenwirkt (O’Hara, 2025).

Die vorgestellten Medienkategorien sollten nicht als isolierte Alternativen betrachtet werden. Vielmehr bilden sie die Bausteine für einen didaktisch sinnvollen, gestuften Lernprozess. Lernende können kaum an einer komplexen Phishing-Simulation (Kategorie 4) erfolgreich teilnehmen, ohne zuvor ein grundlegendes Verständnis von Phishing entwickelt zu haben (Kategorie 1 oder 2). Ein „Serious Game“ (Kategorie 3) kann hier als motivierende Brücke dienen, indem es das erworbene Grundlagenwissen in einem interaktiven, problemorientierten Kontext zur Anwendung bringt. Ein effektiver Lehrplan sollte das Lernen daher schrittweise aufbauen (Scaffolding), indem er die Medienformate kombiniert. Eine Unterrichtseinheit zum Thema Phishing könnte beispielsweise mit einem kurzen Erklärvideo des BSI (Kategorie 1) beginnen, das Wissen durch ein interaktives Spiel wie den „Phishing Master“ (Kategorie 3) festigen und in einer moderierten, klassenbasierten Analyse verschiedener E-Mail-Beispiele (eine pädagogisch angepasste Form der Simulation aus Kategorie 4) münden. Dieser Ansatz einer didaktischen Progression bietet eine klare, praktikable und pädagogisch fundierte Struktur für die Unterrichtsgestaltung.

7.4 Evaluation der Praktikabilität: Herausforderungen und Erfolgsfaktoren der Implementierung

Die didaktische Eignung eines digitalen Mediums ist nur eine Seite der Medaille. Für einen erfolgreichen und nachhaltigen Einsatz im Schulalltag muss auch seine Praktikabilität gegeben sein. Die Implementierung von Cyber-Sicherheitsbildung steht und fällt mit den technischen, personellen und curricularen Rahmenbedingungen an den Schulen.

7.4.1 Technische und infrastrukturelle Voraussetzungen

Die grundlegendste Voraussetzung für den Einsatz digitaler Bildungsmedien ist eine funktionierende technische Infrastruktur. Dies umfasst eine stabile und ausreichend schnelle Internetverbindung, die Verfügbarkeit von Endgeräten für die Schülerinnen und Schüler (z. B. Tablets, Laptops oder PC-Arbeitsplätze) sowie eine professionell administrierte Netzwerkinfrastruktur. Zwar sind viele der vorgestellten Tools webbasiert und stellen keine hohen Anforderungen an die Hardware, doch die Realität an Schulen ist oft von einer heterogenen und teilweise veralteten Ausstattung geprägt. Initiativen wie der „Digitale Schule“ zielen darauf ab, diese Defizite zu beheben, doch die Umsetzung verläuft oft schleppend und wird durch komplexe Antragsverfahren erschwert (Bundesministerium für Bildung, 2025a). Schulen benötigen daher nicht nur die finanziellen Mittel für die Anschaffung, sondern auch nachhaltige Konzepte für Wartung, Support und die Verwaltung der Geräte (z. B. über ein Mobile Device Management, MDM).

7.4.2 Die Rolle der Lehrkräfte: Das Nadelöhr des Erfolgs

Selbst bei perfekter technischer Ausstattung sind es die Lehrkräfte, die den entscheidenden Faktor für den Erfolg digital gestützter Bildungsprozesse darstellen. Ihre Rolle ist jedoch mit erheblichen Herausforderungen verbunden.

Kompetenzanforderungen: Lehrkräfte müssen keine ausgebildeten Cyber-Sicherheitsexperten sein. Sie benötigen jedoch solide digitale Grundkompetenzen, ein Verständnis für die zentralen Sicherheitsrisiken und Schutzmaßnahmen sowie die Fähigkeit, die eingesetzten digitalen Werkzeuge souverän zu bedienen. Darüber hinaus ist eine hohe medienpädagogische Kompetenz gefordert: Sie müssen in der Lage sein, Lernprozesse anzuleiten, Schülerinnen und Schüler zu einer kritischen Reflexion ihres Medienkonsums zu ermutigen und einen sicheren und angstfreien Lernraum zu schaffen, in dem auch Fehler als Lernchancen begriffen werden. Dies schließt auch das Wissen um datenschutzrechtliche und ethische Aspekte beim Einsatz digitaler Tools mit ein.

Unterstützungsbedarf: Die Realität zeigt, dass sich viele Lehrkräfte von der schnellen technologischen Entwicklung und den damit verbundenen neuen Anforderungen überfordert fühlen. Um die Potenziale digitaler Medien für die Cyber-Sicherheitsbildung heben zu können, benötigen sie umfassende Unterstützung. Dies beginnt bei qualitativ hochwertigen und didaktisch aufbereiteten Unterrichtsmaterialien, die direkt im Unterricht einsetzbar sind. Essenziell ist zudem ein verlässlicher technischer Support durch IT-Administratoren, der die Lehrkräfte von technischen Problemen entlastet. Der wichtigste Hebel ist jedoch eine effektive und kontinuierliche Fort- und Weiterbildung. Angebote wie der Selbstlernkurs zur IT-Sicherheit für Lehrkräfte der ALP Dillingen oder iMOOX Kurse zu Cyber Security[46] im Bildungsbereich sind wichtige, niederschwellige Bausteine, um eine breite Basis an Sensibilisierung und Wissen zu schaffen. Diese müssen jedoch durch praxisorientierte Workshops ergänzt werden, in denen der konkrete Einsatz der Tools im Unterricht geübt wird.

7.4.3 Strategien zur curricularen Integration

Die Verankerung der Cyber-Sicherheitsbildung im Schulalltag erfordert eine strategische curriculare Planung. Dabei stehen grundsätzlich zwei Ansätze zur Debatte, die sich nicht ausschließen, sondern ergänzen sollten.

Eigenständiges Fach vs. fächerübergreifend: Die Integration in ein eigenständiges Fach wie Informatik oder Digitale Grundbildung ermöglicht eine systematische, tiefgehende und kontinuierliche Behandlung der Themen. Dies stellt sicher, dass alle relevanten Aspekte kohärent vermittelt werden. Gleichzeitig ist ein fächerübergreifender Ansatz unerlässlich, um die Allgegenwart und Relevanz von Cyber-Sicherheit zu verdeutlichen. Die Analyse von Fake News im Politik- oder Geschichtsunterricht, die Diskussion von Bildrechten im Kunstunterricht oder die Behandlung von Datenschutz in den Sozialwissenschaften zeigt den Schülerinnen und Schülern, dass es sich nicht um ein isoliertes technisches Thema handelt, sondern um eine Kompetenz, die in allen Lebensbereichen relevant ist. Eine effektive Strategie kombiniert daher ein fest verankertes Grundlagenfach mit der konsequenten Thematisierung in anderen Fächern.

Die Implementierung von digitalen Medien und Lehrinhalten darf nicht als rein technische oder administrative Aufgabe missverstanden werden. Der Kauf von Lizenzen für ein Lernspiel oder die Installation eines Filtersystems allein schafft noch keine Sicherheit. Wenn eine Lehrkraft ihr Endgerät im Klassenzimmer unbeaufsichtigt und unversperrt zurücklässt oder wenn Schülerinnen und Schüler nicht verstehen, warum sie Passwörter nicht weitergeben sollten, werden selbst die besten technischen Werkzeuge wirkungslos. Die Einführung digitaler Medien muss daher Teil einer umfassenden, sozio-pädagogischen Strategie sein, die auf die Entwicklung einer gesamt-schulischen Sicherheitskultur abzielt. Es geht nicht nur darum, ein Werkzeug zu nutzen, sondern darum, eine Haltung zu etablieren. Dies erfordert klare und für alle verständliche Nutzungsrichtlinien, eine starke Vorbildfunktion der Schulleitung und der Lehrkräfte, die aktive Einbindung der Eltern und die Etablierung von Sicherheit als gemeinsamer Verantwortung aller Mitglieder der Schulgemeinschaft. Die in der Forschung beschriebenen „Best

[46] simooc | Safer Internet – das Internet in meinem Unterricht? Aber sicher! https://imoox.at/course/simooc2021

Practices“ – wie die verpflichtende Nutzung von Multi-Faktor-Authentifizierung (MFA), regelmäßige Schulungen für das gesamte Personal und klare Zugriffskontrollen – bilden das Fundament für diesen notwendigen kulturellen Wandel.

7.5 Synthese und Schlussfolgerungen

Die Analyse der digitalen Medien zur Vermittlung von Cyber-Sicherheit im schulischen Kontext zeigt ein breites Spektrum an Möglichkeiten, aber auch erhebliche Herausforderungen bei der praktischen Umsetzung. Um eine nachhaltige und wirksame Bildungsarbeit zu gewährleisten, bedarf es einer strategischen Auswahl der Medien sowie gezielter Maßnahmen auf allen Ebenen des Bildungssystems.

7.5.1 Zusammenfassende Bewertung

Es gibt nicht das eine perfekte digitale Medium. Die Eignung eines Formats hängt maßgeblich von der Altersstufe der Lernenden, den spezifischen Lernzielen und den vorhandenen Rahmenbedingungen ab.

- Eine Studie mit dem Titel „Shifting Security Left: A Guide to Cybersecurity Education for Children“ (Subramanian, 2024), die über einen Zeitraum von 18 Monaten durchgeführte wurde, analysierte den Bildungsfortschritt in drei Altersgruppen (7-10, 11-14 und 15-18 Jahre) zieht mehrere wichtige Schlußfolgerungen zur Wirksamkeit und Umsetzung der Rahmenbedingungen für die Cybersicherheitserziehung für junge Menschen:
- Grundschule (7-10 Jahre): Diese Gruppe zeigte besonders hohe Bindungsraten, wenn visuelle und interaktive Inhalte verwendet wurden.
- Mittelstufe (11-14 Jahre): Signifikante Verbesserungen der praktischen Sicherheitsfertigkeiten wurden bei Teilnehmenden dieser Altersgruppe beobachtet.
- Gymnasien (15-18 Jahre): Probanden haben bewiesen, dass sie fortgeschrittene Cybersicherheitskonzepte beherrschen.

Die Studie zeigt, dass die Bereitstellung altersgerechter Inhalte zusammen mit spielerischen Lernerfahrungen und konsequenter Einbindung der Familie das Bewusstsein für Cybersicherheit und die Verhaltensergebnisse deutlich verbessert.

Basierend auf den bisherigen Analysen lässt sich eine Empfehlung für den gestuften Einsatz der Medienkategorien entlang der schulischen Laufbahn ableiten:

- Grundschule (Primarstufe): Der Fokus sollte auf der spielerischen Sensibilisierung und dem Aufbau eines grundlegenden Problembewusstseins liegen. Hierfür eignen sich insbesondere narrative „Serious Games“ (Kategorie 3) wie „Wo ist Goldi?“, die komplexen Themen in altersgerechte Geschichten verpacken. Ergänzend können einfache Informationsmedien (Kategorie 1) wie kindgerechte Videos oder interaktive Poster eingesetzt werden, um grundlegende Verhaltensregeln (z. B. „Sprich mit deinen Eltern“, „Gib keine persönlichen Daten preis“) zu vermitteln.
- Sekundarstufe I (Klassen 5-10): In dieser Phase kann das Wissen systematisiert und vertieft werden. Strukturierte Lernumgebungen und Online-Kurse (Kategorie 2) bieten eine solide Grundlage für das Faktenwissen. Um die Motivation hochzuhalten und die Anwendung zu fördern, sollten diese mit anspruchsvolleren gamifizierten Anwendungen (Kategorie 3) wie Quiz-Duellen oder themenspezifischen Minispielen kombiniert werden. Zudem können hier erste, von Lehrkräften eng begleitete und moderierte Simulationen (Kategorie 4), wie die gemeinsame Analyse von Phishing-E-Mails, eingeführt werden.
- Sekundarstufe II (Oberstufe): Für ältere Schülerinnen und Schüler können fortgeschrittene und komplexere Medienformate genutzt werden. Umfassende Online-Kurse (Kategorie 2) können zur Vorbereitung auf ein Studium oder eine Ausbildung im IT-Bereich dienen. Komplexe Simulationen (Kategorie 4) wie „Capture the Flag“-Wettbewerbe oder Krisensimulationen eignen sich hervorragend, um tiefere technische Einblicke zu gewähren, strategisches Denken zu schulen und potenzielle Karrierewege in der Cyber-Sicherheit aufzuzeigen.

7.5.2 Ausblick: Die Rolle von KI und zukünftige Entwicklungen

Die Zukunft der digitalen Bildungsmedien wird maßgeblich von Entwicklungen im Bereich der Künstlichen Intelligenz (KI) geprägt sein. KI-Systeme bieten enorme Potenziale, um die hier analysierten Medienformate weiter zu verbessern. Intelligente tutorielle Systeme können Lernpfade hochgradig personalisieren, den Schwierigkeitsgrad von Aufgaben dynamisch an den Lernfortschritt anpassen und differenziertes, unmittelbares Feedback geben. KI kann Simulationen noch realistischer und interaktiver gestalten, indem sie auf die Aktionen der Lernenden unvorhersehbar und intelligent reagiert. (Moore, 2025)

Gleichzeitig bringt der Einsatz von KI neue Herausforderungen mit sich. Die Nutzung von KI-gestützten Lernsystemen wirft komplexe Fragen des Datenschutzes und der Datensicherheit auf, die sorgfältig bedacht werden müssen. (Happ, 2024) Zudem entwickelt sich auch die Gegenseite weiter: KI-generierte Phishing-E-Mails oder Deepfake-Videos werden immer überzeugender und schwerer zu erkennen sein. (BSI, 2025) Dies bedeutet, dass die Cyber-Sicherheitsbildung ein dynamisches Feld bleiben wird, das einer ständigen Anpassung und Weiterentwicklung von Inhalten und Methoden bedarf. Der Fokus muss sich daher zunehmend von der Vermittlung von Wissen über bekannte Bedrohungen hin zur Stärkung von übergeordneten Kompetenzen wie kritischem Denken, einer gesunden Skepsis und der Fähigkeit zur resilienten Anpassung an neue, unbekannte Herausforderungen verschieben.

7.5.3 Single Point of Truth (SPoT) - Mediensammlung und didaktische Anregungen für den Unterricht

Ein *Single Point of Truth* (SPoT) für schulische Unterlagen und Informationen ist entscheidend, um **Klarheit, Konsistenz und Verlässlichkeit** in der Cybersecurity-Ausbildung zu gewährleisten. Statt verstreuter Materialien und widersprüchlicher Quellen erhalten Lehrkräfte und Lernende einen zentralen, geprüften Zugang zu allen relevanten Inhalten. Anbei ein einfaches Beispiel für eine Sammlung an geprüften Materialien und Informationsquellen für den Unterricht in Form eines Padlets:

Link zum Padlet: https://padlet.com/eis/cyber-security-vl5hxe5kxinv97zt

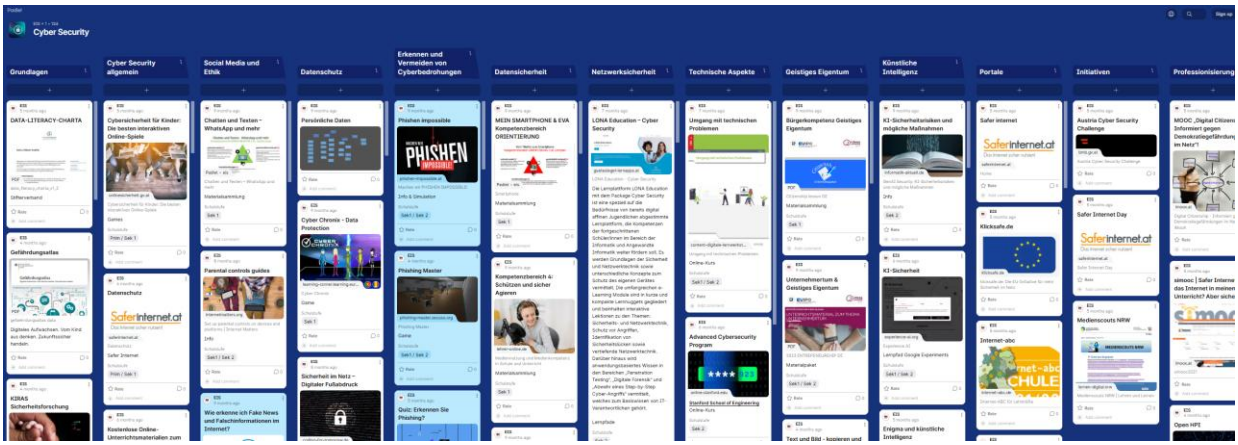

Abbildung 11: Padlet mit strukturierter Sammlung von Cybersecurity-Lehrmaterialien

Abbildung 11 zeigt einen Ausschnitt des Padlets, wo Cybersecurity-Lehrmaterialien nach Themen strukturiert gesammelt sind. Mit diesem einfachen Ansatz könnte man einen SPoT schaffen, der für Schulen nicht nur eine organisatorische Erleichterung, sondern eine **Grundvoraussetzung für wirksame und nachhaltige Cyber-Sicherheitsbildung** darstellt**.** Er schafft Klarheit, reduziert Fehlerquellen und stärkt das Vertrauen aller Beteiligten in die vermittelten Inhalte.

Damit die Inhalte stets aktuell bleiben, ist eine fortlaufende Kuratierung durch ein Expertenteam erforderlich, das Quellen kontinuierlich prüft und passgenau für den schulischen Bedarf auf der Informationsplattform bereitstellt.

8 Handlungsempfehlungen

Aus Basis der wichtigsten Ergebnisse und Erkenntnisse des Projekts CLEMENTINE werden Handlungsempfehlungen für Bildungspolitik, Schulleitung und Lehrkräfte sowie grundsätzliche Voraussetzungen für einen gelungene Cybersecurity-Kompetenzaufbau in der Sekundarstufe II abgeleitet.

8.1 Wissenslücken und Bildungsauftrag

Jugendliche verfügen über ein heterogenes, oft erfahrungsbasiertes Wissen zu Cybersecurity und Online-Betrug. Ein einheitliches Kompetenzniveau fehlt. Schulen tragen aktuell nur wenig zur Wissensvermittlung in diesem Bereich bei – unter anderem da ein Bekenntnis zur Integration von Cybersecurity-Themen in den Lehrplan genauso fehlt wie entsprechende Kenntnisse bei den Lehrenden oder ein vorgelebte Sicherheitskultur in vielen Schulen. Entsprechend groß ist der Wunsch vonseiten unterschiedlicher Stakeholder:innen den Begriff Cybersecurity curricular zu verankern.

8.1.1 Empfehlung für Bildungspolitik: Cybersecurity im Lehrplan

Implementierung von Cybersecurity-Inhalten in den bestehenden Lehrplänen - anhand des CLEMENTINE-6-Stufen-Modells - in folgenden Varianten:

1. Anpassung bestehender Gegenstände wie "Digitale Grundbildung", Angewandte Informatik", fachspezifischer Informatik-Gegenständen, usw. oder
2. Einführung einer eigenen, schulstufenübergreifend koordinierten Cybersecurity-Ausbildung in einem eigenen Gegenstand, mit Neuorientierung der angeschlossenen Informatik-Ausbildungen.

2a. Kernkompetenzen können in Form einer (oder mehrteiliger) Zertifizierung sichergestellt und standardisiert werden.

8.1.2 Empfehlung für Schulleitung: Cybersecurity als Haltung im Schulalltag

Cyber-Sicherheit sollte als strategisches Ziel im schulischen Leitbild verankert werden. Eine ganzheitliche Sicherheitskultur auf Basis gemeinsamer Verantwortung ist durch klare Nutzungsrichtlinien, technische Mindeststandards (z. B. verpflichtende Mehr-Faktor-Authentifizierung) und regelmäßige Sensibilisierungsmaßnahmen für alle Beteiligten (Lehrkräfte, Schüler:innen, Eltern) zu fördern.

8.1.3 Empfehlung für Lehrkräfte: Vorbilder gehen voraus

Elektronische Medien sollten didaktisch sinnvoll in den Unterricht integriert und durch klare Handlungsanleitungen für ihren verantwortungsvollen Gebrauch ergänzt werden. Eine gelebte Vorbildfunktion der Lehrenden im sicheren Umgang mit digitalen Technologien und Daten trägt wesentlich zur Wirksamkeit der Medienbildung bei und stärkt die digitale Kompetenz aller Beteiligten.

8.1.4 Zusätzliche Voraussetzungen: Bildung im digitalen Zeitalter

Die Schaffung geeigneter Rahmenbedingungen erfordert die Bereitstellung ausreichender Ressourcen für eine zeitgemäße technische Ausstattung, qualifizierten IT-Support sowie für die gezielte und kontinuierliche Fortbildung des pädagogischen Personals. Ergänzend sollten einheitliche und standardisierte Unterrichtsmaterialien entwickelt werden, um die Qualität und Konsistenz der digitalen Bildungsangebote zu sichern.

8.2 Wenn Lehrkräfte Nachhilfe brauchen

Eine Sicherheitskultur im Sinne der Cybersecurity ist in der Schule nicht vorhanden, insbesondere den Lehrkräften fehlen die entsprechenden systematisch vermittelten Kompetenzen. Didaktisch sind Schulungen zu Basiswissen gefordert, verknüpft mit unterschiedlichen Lernformaten wie Spielen, Awareness-Kampagnen mit Storytelling, Online-Kursen oder interaktive E-Learnings. Auch die Jugendlichen identifizierten einen Wissens- und Kompetenzmangel bei Lehrkräften und berichteten davon, dass Lehrkräfte entweder kein Interesse am Thema zeigen oder nicht über die ausreichenden fachlichen und didaktischen Kenntnisse verfügen, um das Thema in den Unterricht einzubringen.

8.2.1 Empfehlung für Bildungspolitik: Lehrkräfte mit Update

Die wirksame Vermittlung von Cyber-Sicherheit im schulischen Kontext setzt eine fundierte und praxisnahe Qualifizierung der Lehrkräfte voraus. Daher sollte die Didaktik der Cyber-Sicherheit als integraler Bestandteil in die Lehrkräfteaus- und -weiterbildung aufgenommen werden. Nur entsprechend ausgebildete Lehrpersonen sind in der Lage, das Thema fachlich kompetent und pädagogisch wirksam im Unterricht zu verankern (Gulyamov et al., 2024). Zur Umsetzung dieser Zielsetzung sind zwei zentrale Säulen zu etablieren:

1. Grundausbildung über Pädagogische Hochschulen (PH): Die Vermittlung von Cyber-Sicherheitskompetenzen sollte entweder durch eigenständige Studiengänge oder durch Schwerpunktsetzungen innerhalb bestehender Informatik-Ausbildungen im Bachelor- und Masterbereich erfolgen.
2. Gezielte und regelmäßige Weiterbildung für bereits tätige Lehrkräfte: Es bedarf strukturierter Programme zur berufsbegleitenden Fortbildung, die aktuelle Themen der Cybersecurity adressieren und eine Einschulung in ein standardisiertes Cybersecurity-Curriculum ermöglichen.

8.2.2 Empfehlung für Schulleitung: Digitale Sicherheit ist Führungsaufgabe

Die Schulleitung sollte die systematische Qualifizierung im Bereich Cyber-Sicherheit als strategisches Entwicklungsziel verankern und aktiv fördern. Dazu gehört die Integration entsprechender Inhalte in die schulinterne Fortbildungsplanung sowie die Unterstützung von Weiterbildungsmaßnahmen über Pädagogische Hochschulen. Es ist sicherzustellen, dass Lehrkräfte Zugang zu praxisnahen, standardisierten Schulungen erhalten, die sowohl technische Grundlagen als auch didaktische Umsetzungskompetenz vermitteln.

8.2.3 Empfehlung für Lehrkräfte: Vom Vorbild zur Vermittlung

Lehrkräfte sollten ihre digitale und didaktische Kompetenz im Bereich Cyber-Sicherheit regelmäßig weiterentwickeln, um das Thema fachlich fundiert und pädagogisch wirksam im Unterricht zu vermitteln. Dies umfasst die Teilnahme an gezielten Fortbildungsangeboten, die Reflexion der eigenen Medienpraxis sowie die aktive Mitgestaltung eines sicheren und verantwortungsvollen Umgangs mit digitalen Technologien im Schulkontext. Die Bereitschaft, als Vorbild zu agieren und Cyber-Sicherheit als Querschnittsthema in den Unterricht zu integrieren, trägt wesentlich zur Förderung der digitalen Mündigkeit der Schüler:innen bei.

8.2.4 Zusätzliche Voraussetzungen: Lehrkräfte brauchen mehr als Lehrpläne

Ergänzend sind entsprechende Ressourcen bereitzustellen – sowohl für die Entwicklung und Durchführung der Programme als auch für die technische und personelle Unterstützung. Eine systematische, standardisierte und praxisorientierte Lehrkräftequalifizierung ist der Schlüssel, um die bestehende Diskrepanz zwischen Lehrplanvorgaben und tatsächlicher Unterrichtspraxis nachhaltig zu überwinden. Damit Lehrkräfte geeignete Cybersecurity-Inhalte altersgerecht und curricular passend vermitteln können, müssen grundsätzlich einige infrastrukturelle Voraussetzungen gelten:

1. Zugang zu digitalen Endgeräten wie Tablets oder Laptops für Lehrkräfte und Schüler:innen
2. Stabile Internetverbindung in allen Unterrichtsräumen
3. Digitale Plattformen zur Bereitstellung und gemeinsamen Nutzung kuratierter Unterrichtsmaterialien
4. Technische Unterstützung durch IT-Fachkräfte oder Medienpädagog:innen
5. Fortbildungsangebote über schulinterne oder externe Lernmanagementsysteme

8.3 Cybersecurity schläft nicht

Cybersecurity ist ein hochdynamisches und zunehmend komplexes Themenfeld, dessen Entwicklungen das Bildungssystem strukturell herausfordern. Die Geschwindigkeit technologischer Veränderungen – insbesondere durch den Einsatz von KI – steht im Kontrast zu den vergleichsweise starren Rahmenbedingungen schulischer Strukturen. KI-gestützte Lernsysteme werfen neue Fragen zu

Datenschutz und Datensicherheit auf, während gleichzeitig Bedrohungen wie Deepfakes und KI-generierte Phishing-Mails zunehmen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2025; Happ et al., 2024).

Cyber-Sicherheitsbildung bleibt damit ein fortlaufender Anpassungsprozess, der flexible Inhalte und Methoden erfordert. Aus den Interviews geht hervor, dass traditionelle Fortbildungsformate mit dieser Dynamik kaum Schritt halten. Cybersecurity-Wissen ist kein statisches Wissen, sondern verlangt kontinuierliche Aktualisierung, Anwendung und Reflexion – jeder Bildungsansatz bildet daher nur eine Momentaufnahme.

8.3.1 Empfehlung für Bildungspolitik: Fachimpulse für digitale Bildung

Um der schnellen inhaltlichen Entwicklung im Bereich Cybersecurity gerecht zu werden, sollte ein dauerhaftes und allgemein verfügbares Unterstützungsformat etabliert werden, das für Lehrkräfte die Einbindung externer Expert:innen in den Unterricht ermöglicht. Fachleute bringen aktuelle Perspektiven, reale Bedrohungsszenarien und praxisnahe Impulse in die Schule. Damit solche Kooperationen wirksam und nachhaltig gelingen, sind klare organisatorische Rahmenbedingungen erforderlich.

8.3.2 Empfehlung für Schulleitung: Schule trifft Expertise

Zur Stärkung der Cyber-Sicherheitsbildung sollte die Einbindung externer Expert:innen aktiv gefördert werden. Dafür sind administrative Hürden zu reduzieren, lokale Kontakte zu Fachpersonen aufzubauen und nachhaltige Kooperationen mit einschlägigen Ausbildungsinstitutionen (z. B. FH, Universität, HTL), Unternehmen und Forschungseinrichtungen zu etablieren. So können aktuelle Inhalte praxisnah vermittelt und schulische Lernprozesse gezielt unterstützt werden.

8.3.3 Empfehlung für Lehrkräfte: Expertise trifft Urteilskraft

Die gezielte Einbindung externer Expert:innen ermöglicht praxisnahe Einblicke und unterstützt die didaktische Aufarbeitung aktueller Entwicklungen aus Wirtschaft, Schule und lokalem Umfeld. Ergänzend fördern fächerübergreifende Zusammenarbeit, kollegialer Austausch und die gemeinsame Nutzung bewährter Materialien die Qualität des Unterrichts. Dabei sollte sich der Fokus zunehmend von der reinen technischen Wissensvermittlung hin zur Stärkung überfachlicher Kompetenzen wie kritischem Denken, reflektierter Skepsis und resilienter Anpassungsfähigkeit gegenüber neuen, unbekannten Herausforderungen verschieben. (siehe multiperspektivische Erschließung entsprechend der Modelle des Dagstuhl-Dreiecks und Frankfurt-Dreiecks)

8.3.4 Zusätzliche Voraussetzung: Cybersicherheit sichtbar machen

Regierung, Zivilgesellschaft und Medien sollten öffentliche Kampagnen und Challenges zur Förderung der digitalen Kompetenz durchführen, um die Bedeutung der Cybersicherheitserziehung hervorzuheben und für das Thema zu sensibilisieren, insbesondere Eltern und Bildungsverantwortliche, die wichtige Akteure des Wandels sind.

8.4 Cybersecurity braucht Pädagogik

Zur Sicherstellung der wesentlichen Cybersecurity-Inhalte wird das aus dem 5-stufigen Kompetenzmodell des BMBWF entwickelte CLEMENTINE-6-Stufen-Modell verwendet. Es gewährleistet die Vermittlung der wesentlichen technischen Kerninhalte der Cybersecurity, bleibt jedoch in seiner Ausrichtung rein technisch. Für eine wirksame Bildungsarbeit bedarf es daher einer pädagogischen Ergänzung durch ganzheitliche Ansätze.

8.4.1 Empfehlung für Bildungspolitik: Cyberunterricht mit Tiefgang - Modell trifft Methode

Für die Integration von Cybersecurity-Inhalten in bestehende Lehrpläne empfiehlt sich die Anwendung des CLEMENTINE-6-Stufen-Modells sowie - in Anlehnung an die „Digitale Grundbildung“ der Sekundarstufe I - die Einbindung des Frankfurt-Dreiecks. Dieses pädagogische Modell ermöglicht die Verbindung gesellschaftlich-kultureller sowie methodisch-didaktischer Perspektiven und trägt dazu bei, sowohl die fachliche Tiefe als auch die persönliche Entwicklung der Lernenden ganzheitlich zu fördern.

8.4.2 Empfehlung für Schulleitung: Cyberkompetenz wirksam vermitteln

Schulleitende sollten ganzheitliche Lehransätze fest im Schulalltag verankern und Lehrkräfte gezielt in methodisch-didaktischen Kompetenzen fördern. Modelle wie das Frankfurt-Dreieck bieten dabei wertvolle Orientierung für eine reflektierte Unterrichtsgestaltung.

8.4.3 Empfehlung für Lehrkräfte: Cyberbildung Schritt für Schritt

Die Unterrichtsgestaltung sollte sich am Prinzip der didaktischen Progression orientieren. Dabei empfiehlt es sich, zunächst mit niedrigschwelligen, zielgruppenspezifischen und qualitativ hochwertigen Materialien zu arbeiten – etwa mit Erklärvideos des BSI oder Lernspielen von Saferinternet.at – um eine grundlegende Wissensbasis zu schaffen. Darauf aufbauend können schrittweise komplexere und anwendungsorientierte Methoden eingesetzt werden.

8.4.4 Zusätzliche Voraussetzung: Interdisziplinär zur Didaktik

Einrichtung einer interdisziplinären Expert:innengruppe mit dem Ziel, bestehende Modelle zu einem kohärenten, methodisch-didaktischen Lehrkonzept für die Cybersecurity-Bildung zu integrieren und weiterzuentwickeln.

8.5 Lehrplan-Dilemma

Lehrpläne bieten durch ihre Formulierung wertvolle pädagogische Freiräume, führen jedoch in der Praxis zu Unterschieden in der Umsetzung und Zielerreichung. Diese Unterschiede werden durch den teils unzureichenden Qualifikationsstand vieler Lehrkräfte – insbesondere im Umgang mit digitalen Medien und didaktischen Innovationen – weiter verstärkt. In der Folge entstehen deutliche Unterschiede in der Qualität und Vergleichbarkeit von Unterrichtsinhalten und Lernergebnissen zwischen Schulen.

8.5.1 Empfehlung für Bildungspolitik: Cyberunterricht mit Standard

Zur Sicherung einheitlicher Standards in der Cybersecurity-Bildung sollte ein schultypgerechtes, verbindliches Basis-Curriculum entwickelt werden, das zentrale Inhalte und Qualitätskriterien festlegt. Ergänzend empfiehlt sich die Einführung eines Zertifizierungsverfahrens, das erworbene Kompetenzen objektiv bestätigt und schulübergreifend vergleichbar macht. So wird sowohl die Qualität der Bildungsangebote als auch die Nachvollziehbarkeit der Lernergebnisse nachhaltig gestärkt.

8.5.2 Empfehlung für Schulleitung: Cyberbildung als Karrierebaustein

Die Zertifizierung im Bereich Cybersecurity sollte als qualifizierende Maßnahme klar kommuniziert und im schulischen Umfeld sichtbar gemacht werden. Ihre Relevanz für Bildung und Beruf sollte gegenüber Lernenden, Erziehungsberechtigten und dem Kollegium deutlich hervorgehoben werden, um das Bewusstsein für digitale Sicherheit zu stärken und die Akzeptanz im Schulalltag zu fördern.

8.5.3 Empfehlung für Lehrkräfte: Haltung der Lehrenden

Die Einführung und Umsetzung einer Zertifizierung im Bereich Cybersecurity sollte aktiv in den schulischen Alltag integriert werden. Lehrkräfte tragen dabei eine zentrale Verantwortung: Sie machen die Relevanz digitaler Sicherheit im Unterricht sichtbar, zeigen den Nutzen für die berufliche Zukunft der Lernenden auf und motivieren zur Teilnahme. Durch ihre Haltung, ihre Kommunikation und ihr pädagogisches Handeln stärken sie das Bewusstsein für digitale Sicherheit und verankern die Bedeutung dieser Qualifikation im schulischen wie gesellschaftlichen Kontext.

8.5.4 Zusätzliche Voraussetzung: Lehrkräfte stärken – Qualität sichern

Um die pädagogischen Freiräume von Lehrplänen sinnvoll zu nutzen und Qualitätsunterschiede zwischen Schulen zu verringern, braucht es eine fundierte Lehrekräfteausbildung, die digitale Medienkompetenz und didaktische Innovationsfähigkeit systematisch fördert. Ein schultypengerecht abgestimmtes PH-Ausbildungsmodell sollte daher praxisnah, reflexiv und interdisziplinär und österreichweit aufgebaut sein – mit festen Modulen zu digitaler Didaktik, Medienethik und adaptiver Unterrichtsgestaltung – um Lehrkräfte gezielt auf Cybersecurity vorzubereiten.

8.6 Lehrplan-Update als Chance

Die aktuelle Lehrplanreformen bieten eine kritische Integrationschance: Die Lehrpläne der 5. Klasse AHS und der HAK 2014 werden derzeit überarbeitet, und die HTL-Lehrpläne sollen modernisiert und vereinheitlicht werden.

8.6.1 Empfehlung für Bildungspolitik: Rahmen, Expertise, Diagnose

1) Curriculare Rahmenbedingungen schaffen: Entwickeln Sie schulstufenübergreifende verbindliche, aber flexible curriculare Leitlinien für die Cyber-Sicherheitsbildung, die sowohl eine Verankerung in einem Kernfach als auch fächerübergreifende Ansätze vorsehen (Mishra, 2024).

2) Die staatlichen Bildungsbehörden sollten Expert:innenarbeitsgruppen einrichten, um Cybersicherheits-standards und -rahmen zu formulieren, die auf ihren spezifischen Kontext zugeschnitten sind, und sicherstellen, dass die wichtigsten Wissens- und Kompetenzbereiche abgedeckt werden (Gulyamov et al., 2024).

3) Die Implementierung einer Cybersecurity-Kompetenzdiagnostik beim Eintritt in die Sekundarstufe II ist sinnvoll, um individuelle Förderbedarfe zu erkennen und gezielte Maßnahmen zur Niveaustabilisierung zu ermöglichen.

8.6.2 Empfehlung für Schulleitung: Fördern wo wir stehen

Mit dem Eintritt in die Sekundarstufe II empfiehlt sich – in Anlehnung an die gängige Praxis der Bildungsstandards- und Förderbedarfsdiagnostik – eine systematische Erhebung der Cybersecurity-Kompetenzen, die bei Bedarf in passgenaue Fördermaßnahmen zur Niveaustabilisierung münden sollte.

8.6.3 Empfehlung für Lehrkräfte: Cybersecurity mit Niveau

Ausgehend von der Erhebung der Cybersecurity-Kompetenzen ist eine schultypengerechte Förderung zum Ausgleich von Niveauunterschiede durchzuführen. Im Besonderen ist darauf zu achten, dass die wichtigsten Wissens- und Kompetenzbereiche abgedeckt sind - von technischer Sicherheit über Datenschutz bis hin zu ethischen Fragenstellungen.

8.6.4 Zusätzliche Voraussetzung: Cyberkompetenz und smarte Diagnostik

Für eine konsistente, schulstufen- und schultypenübergreifende Verankerung von Cybersecurity in den Lehrplänen bedarf es einer abgestimmten Koordination zwischen Lehrplanexpert:innen. Gleichzeitig sollte der Aufwand für automatisierte Diagnostik möglichst geringgehalten werden, um eine praktikable und nachhaltige Umsetzung im Schulalltag zu ermöglichen.

8.7 Bildung braucht Orientierung

Trotz der Fülle an frei verfügbaren Informationen zu Cybersecurity im Netz stellt die Auswahl geeigneter, didaktisch aufbereiteter Inhalte für den Unterricht eine erhebliche Herausforderung für Lehrkräfte dar – es fehlt an kuratierten, praxisnahen Materialien, die curricular anschlussfähig und altersgerecht sind.

8.7.1 Empfehlung für Bildungspolitik: Kuratiert und frei

Stellen Sie eine **kuratierte und qualitätsgesicherte Informations- und Materialplattform** (OER) bereit, die Lehrkräfte anhand einer fachlichen Leitlinie (Roadmap) bei der Auswahl geeigneter Inhalte unterstützt – inklusive gesicherter weiterführender Internetquellen, Lehrunterlagen, Unterrichtsbeispielen, Lernpfaden und Fortbildungsangeboten (siehe auch Kapitel 7.5.3).

8.7.2 Empfehlung für Schulleitung: Cybermaterial gezielt steuern

Schulleitungen sollten gezielt den Zugang zu altersgerechten und curricular passenden Materialien im Bereich Cybersecurity fördern. Dazu gehört die Unterstützung von Lehrkräften bei der Auswahl und Nutzung didaktisch aufbereiteter Inhalte sowie der Aufbau von Kooperationen mit Fachstellen und kollegialen Arbeitsgruppen, die solche Materialien bereitstellen.

8.7.3 Empfehlung für Lehrkräfte: Gemeinsam gestalten

Lehrkräfte sollten gezielt nach altersgerechten und curricular passenden Materialien im Bereich Cybersecurity suchen und dabei auf geprüfte, didaktisch aufbereitete Inhalte zurückgreifen. Der Austausch mit Kolleg:innen und die Nutzung von Fachplattformen kann helfen, praxisnahe Unterrichtseinheiten zu gestalten.

8.7.4 Zusätzliche Voraussetzungen: Freie Inhalte, klare Standards

Eine entsprechende Finanzierung und Förderung ist die Voraussetzung für die Entwicklung, Evaluation und Bereitstellung von qualitativ hochwertigen, kostenlosen und offenen digitalen Bildungsmedien (Open Educational Resources). Dies senkt die Hürden für Schulen und Lehrkräfte und sichert einen pädagogischen Qualitätsstandard (Macgilchrist, 2019).

8.8 Gender, Diversity und Inklusion - Cybergerechtigkeit beginnt im Klassenzimmer

Ein wiederkehrendes Thema in den durchgeführten Interviews waren geschlechtsspezifische Unterschiede beziehungsweise die (Un-)Gleichheit im Wissen und in der Vermittlung von Cybersecurity-Inhalten. Empirische Studien legen nahe, dass Frauen ihre Selbstwirksamkeit im Bereich der Cybersicherheit tendenziell niedriger einschätzen als Männer, was sich hemmend auf ihre Teilhabe und berufliche Orientierung in diesem Feld auswirken kann (Anwar et al., 2017). Vor diesem Hintergrund erscheint es bildungspolitisch und didaktisch geboten, geschlechtersensible Zugänge zu fördern, stereotype Rollenzuschreibungen kritisch zu reflektieren und insbesondere weibliche Vorbilder im Bereich der Cybersecurity sichtbar zu machen, um eine chancengerechte Teilhabe aller Geschlechter zu ermöglichen. Zudem ist es notwendig inklusive Materialien und pädagogische Ansätze zu verwenden um allen Menschen, insbesondere Menschen mit körperlichen oder kognitiven Einschränkungen, den Cybersecurity-Kompetenzerwerb zu ermöglichen beziehungsweise auf spezifische Cybersecurity-Gefahren für diese Menschen einzugehen.

8.8.1 Empfehlung für Bildungspolitik: Lehrpläne für alle

Gendersensible und inklusive Cybersecurity-Bildung sollte als integraler Bestandteil schulpolitischer Strategien verankert werden. Lehrpläne, Unterrichtsmaterialien und Fortbildungsangebote müssen Diversitätsaspekte systematisch mitdenken – etwa durch die Entwicklung von Formaten, die unterschiedliche Lernzugänge ermöglichen, wie sowohl wettbewerbsorientierte als auch kooperative Ansätze. Es ist schulpolitisch essenziell, dass alle Schüler:innen unabhängig von Geschlecht oder auch Ethnie beziehungsweise Beeinträchtigungen Zugang zu denselben Inhalten erhalten, weibliche Role Models sichtbar gemacht werden und geschlechtsspezifische Unterschiede – etwa bei Bedrohungsszenarien wie Deepfakes – berücksichtigt werden. Nur so kann eine chancengerechte, inklusive Cyberbildung entstehen, die stereotype Rollenzuschreibungen aufbricht und Selbstwirksamkeit alle Lernenden stärkt.

8.8.2 Empfehlung für Schulleitung: Inklusive Cyberkompetenz

Zur Förderung einer geschlechtersensiblen und diversitätsorientierten Vermittlung von Cybersecurity-Inhalten im schulischen Kontext sollten gezielt Initiativen zur Entwicklung entsprechender Fortbildungsangebote unterstützt werden. Dabei ist es zentral, bestehende geschlechtsspezifische Stereotype kritisch zu reflektieren und didaktisch zu durchbrechen. Diversitätsaspekte sind nicht nur in der Konzeption von Lehrformaten, sondern auch im schulischen Kollegium aktiv zu thematisieren – etwa durch strukturierte Diskussionsformate oder Sensibilisierungsmaßnahmen sowie auch bei aufkommenden Cybersecurity-Vorfällen in der Schule. Auch die visuelle und narrative Gestaltung von schulischen Werbematerialien zu Cybersecurity-Schwerpunkten sollte Vielfalt abbilden und vermeiden, ausschließlich männlich konnotierte Darstellungen zu reproduzieren. Die gezielte Einbindung weiblicher Role Models – sei es in Form von Lehrkräften, Expertinnen oder Forscherinnen – trägt wesentlich zur Sichtbarkeit und Identifikationsmöglichkeit bei und sollte bei der Auswahl externer Fachpersonen bewusst priorisiert werden. So kann ein inklusives Bildungsumfeld entstehen, das allen Schüler:innen chancengerechte Zugänge zu digitalen Kompetenzen eröffnet.

8.8.3 Empfehlung für Lehrkräfte: Vielfalt stärken, Vorbilder zeigen, Risiken benennen

Für eine chancengerechte Vermittlung von Cybersecurity-Inhalten im schulischen Kontext ist es zentral, vielfältige didaktische Zugänge zu ermöglichen, die unterschiedlichen Lernpräferenzen und sozialen Orientierungen Rechnung tragen – etwa durch die Kombination von wettbewerbsbasierten und kooperativen Lernformaten. Die gezielte Sichtbarmachung weiblicher Role Models, insbesondere von Expertinnen mit ausgewiesener Fachkompetenz in der Cybersicherheitsforschung und -entwicklung, kann dazu beitragen, geschlechtsspezifische Selbstwirksamkeitserwartungen positiv zu beeinflussen und Mädchen zur aktiven Auseinandersetzung mit dem Themenfeld zu ermutigen. Darüber hinaus sollte der Unterricht Raum für die kritische Reflexion und Diskussion geschlechtsspezifischer Bedrohungsszenarien bieten – etwa im Kontext von Deepfakes, die insbesondere Frauen und Mädchen in sexualisierter Form betreffen. Eine solche pädagogische Ausrichtung fördert nicht nur digitale Kompetenz, sondern auch ein Bewusstsein für strukturelle Ungleichheiten im digitalen Raum.

8.8.4 Zusätzliche Voraussetzungen: Cyberfairness versus digitale Ungleichheit

Für eine gerechte und diversitätssensible Cybersecurity-Bildung braucht es klare strukturelle Voraussetzungen: Lehrpläne und Fortbildungsangebote müssen Vielfalt und Geschlechtergerechtigkeit systematisch berücksichtigen, Unterrichtsmaterialien sollten unterschiedliche Zugänge – etwa kooperative und wettbewerbsorientierte Formate – ermöglichen, und weibliche Role Models sowie Expertinnen gezielt sichtbar gemacht werden. Lehrkräfte sind zu sensibilisieren für geschlechtsspezifische Bedrohungsszenarien wie Deepfakes, und schulische Öffentlichkeitsarbeit sollte Diversität aktiv mitdenken, etwa durch ausgewogene Darstellungen in Kommunikationsmedien. Nur durch diese abgestimmten Maßnahmen kann Cyberkompetenz chancengerecht vermittelt werden.

9 Zusammenfassung und Ausblick

Die fortschreitende Digitalisierung führt zu einer deutlichen Zunahme von Cyberangriffen. 2023 stieg die Zahl der Cyberangriffe auf Unternehmen um über 200% (Bundesministerium für Inneres, Bundeskriminalamt, 2024). Gleichzeitig professionalisieren sich Cyberkriminelle mittels generativer KI, Angriffe lassen sich dadurch schwerer erkennen. Zentraler Angriffsvektor ist der Menschen, die Förderung von Cybersecurity-Kompetenzen gewinnt zunehmend an Bedeutung– sowohl am Arbeitsmarkt als auch in der schulischen Bildung. Jugendliche zwischen 14- und 19 Jahren sind besonders relevant: Obwohl sie viel Zeit online verbringen, werden sie in Schulen bislang nur unzureichend auf digitale Gefahren vorbereitet.

Im Projekt CLEMENTINE wurden Ansätze entwickelt, um Cybersecurity-Kompetenzen systematisch in der Sekundarstufe II zu verankern. Auf Basis von Expert:innen-Interviews, Fokusgruppen mit Jugendlichen, einer Online-Befragung, Workshops mit Stakeholdern und Lehrplananalysen konnte ein umfassendes Bild des aktuellen Stands der Cybersecurity-Kompetenzen von Jugendlichen, deren Vermittlung im schulischen Kontext sowie der Anforderungen des Arbeitsmarkts im Bereich Cybersecurity erstellt werden.

So verfügen Jugendliche bereits über grundlegendes Wissen. Ein tiefergehendes Verständnis, das auch nachhaltig wirkt und zu einem sicheren Umgang mit digitalen Geräten und dem Internet führt, fehlt jedoch. Schulen tragen laut Schüler:innen, aber auch laut Expert:innen an der Schnittstellte Schule und Cybersecurity, bislang nur wenig zur Wissensvermittlung in diesem Bereich bei. Jugendliche schöpfen ihr Wissen überwiegend aus eigenen Erfahrungen. Entsprechend groß ist der Wunsch vonseiten verschiedener Stakeholder Cybersecurity stärker im Unterricht zu verankern.

Ein weiterer zentraler Befund betrifft die Rolle der Lehrkräfte: Häufig fehlt es an fachlicher Expertise, geeignete Weiterbildungsangebote sind rar. Doch insbesondere aufgrund der Dynamik und Schnelllebigkeit des Themenfelds sind kontinuierliche Fortbildungen zentral. Auch aus Sicht des Arbeitsmarkts wird dieser Bedarf bestätigt: Unternehmen sehen Social Engineering und Phishing als die größten Bedrohungen. Neben Basiskenntnissen zu den Vor- und Nachteilen der Digitalisierung, zum sicheren Umgang mit Daten und der Vermittlung eines kritischen Denkens hinsichtlich der Nutzung digitaler Geräte müssen auch Zukunftsthemen wie Künstliche Intelligenz oder Cloud-Sicherheit vermittelt werden.

Die Lehrplananalyse zeigt den aktuellen Stand zu aktuell vermittelten CS-Themenbereichen. Darauf aufbauend wurden Empfehlungen für Adaptierungen der Lehrpläne erarbeitet. Zudem wurden aktuelle pädagogische Konzepte im Bereich CS analysiert und ein Padlet mit Materialien zur Vermittlung von CS-Kompetenzen erstellt.

Aus den Ergebnissen lassen sich Handlungsempfehlungen für Bildungspolitik, Schulleitung und Lehrkräfte ableiten, die sowohl Basisvoraussetzungen im schulischen Kontext, Lehrkräftequalifizierungsansätze, Einbindung von externen Expert:innen und didaktische Aspekte umfassen. Im Zuge der aktuellen beziehungsweise anstehenden Lehrplanreformen sollten die Adaptierungsvorschläge auf Basis der Lehrplananalysen aufgegriffen werden, um Cybersecurity-Kompetenzen entsprechend im Lehrplan zu verankern.

Die Ergebnisse des Projekts liefern wichtige Grundlagen für darauf aufbauende Schritte und Maßnahmen: Aus der Erkenntnis, dass die Einbindung von externen Expert:innen gewünscht und wichtig ist, um dem hochdynamischen Feld der CS zu begegnen, sollten Schritte gesetzt werden, um einen Pool an Expert:innen bzw. Role Models zu erstellen, die im schulischen Kontext eingebunden werden können. Zudem ist es wichtig hier vor allem weibliche Expertinnen als Role Models für (junge) Frauen auf die Bühne zu holen, um das Interesse am Thema bei Schülerinnen aber auch Lehrerinnen zu forcieren.

Basierend auf den Lehrplananalysen können mit Lehrplan-Verantwortlichen in einem nächsten Schritt Details zu notwenigen Änderungen ausdefiniert werden. Zudem sollten nach der Erkenntnis, dass es keine geprüften Lehrmaterialien gibt, diese gesammelt bzw. erstellt, strukturiert und geprüft werden, um Lehrkräften die notwenigen Mittel für den CS-Unterricht gemäß Kompetenzlevel ihrer Schüler:innen zur Verfügung stellen zu können. Des Weiteren sollten nächste Schritte hin zu einer Zertifizierung von CS-Kompetenzen sowohl für Schüler:innen als auch für die Lehrkräfte - im Rahmen der Grundausbildung als auch Weiterbildung – gesetzt werden. Für all diese Maßnahmen müssen zudem Prozedere definiert werden, wie die Materialien und Kompetenzen aktuell gehalten werden können, um den schnellen Veränderungen im Bereich CS Schritt halten zu können.

Appendix: Das CEMENTINE-6-Stufen-Kompetenzmodell

Stufe 0: Grundlagen und Verhalten

Dieses Kapitel befasst sich mit der kritischen Schnittstelle von Kommunikationsanforderungen und Nutzerverhalten im Bereich der Cybersicherheit und greift dabei auf Schlüsselkonzepte aus den bereitgestellten 5-Stufen-Modells zurück. Es betont das menschliche Element bei der Aufrechterhaltung einer sicheren digitalen Umgebung:

0.1 Grundlagen eines Computers – sicherer Umgang mit digitalen Geräten:

- **Computerarten**: Überblick der verschiedenen Computerformen - vom Supercomputer bis zum Embedded System.
- **Grundlegende Funktionsweise**: Einfacher Aufbau aller moderner Computersysteme.
- **Funktionsabgrenzung**: Zusammenwirken von Soft- und Hardware. Nutzungsmöglichkeiten des Computers und Grenzen des Einsatzes.
- **Umfeld und Einbettung des Computers:** Datenaustausch zwischen Computern.

0.2 Kommunikationsbedürfnisse – sicheres Onlineverhalten:

- **Kollaboration und Ortsunabhängigkeit**: Unterstreicht die Notwendigkeit der Zusammenarbeit unabhängig vom physischen Standort.
- **Informationsaustausch:** Konzentriert sich auf die Notwendigkeit einer sicheren Datenverbreitung

0.3 Sicherheitsüberlegungen – Grundlagen der Cybersicherheit:

- **Perimetersicherheit**: Traditionelle Sicherheitsansätze, die eine definierte Grenze festlegen.
- **Zero Trust:** Ein Sicherheits-Framework, das auf dem Prinzip "niemals vertrauen, immer überprüfen" basiert und davon ausgeht, dass kein Benutzer oder Gerät standardmäßig vertrauenswürdig sein sollte.

0.3 Verhalten – Rechte und Pflichten im digitalen Raum:

- **Identität und Verantwortlichkeit**: Befasst sich mit der Wichtigkeit, Handlungen und Daten bestimmten Personen zuordnen zu können.
- **Anonymität**: Befasst sich mit Situationen, in denen die Identitäten der Benutzer maskiert oder unbekannt sind.
- **Bewusstsein**: Betont die Bedeutung des Verständnisses der Benutzer für Sicherheitsrisiken und Best Practices.
- **Verantwortung**: Betont die Notwendigkeit, dass die Benutzer die Verantwortung für ihre Handlungen und deren Auswirkungen auf die Sicherheit übernehmen.
- **Auswirkungen**: Diskutiert, wie sich das Nutzerverhalten auf die Gesellschaft und den Einzelnen auswirken kann.
- **Verhaltensrichtlinien**: Stellt einen Rahmen für sicheres und verantwortungsvolles Verhalten im digitalen Raum vor.

0.4 Fähigkeiten und Fertigkeiten – Verantwortung in der digitalen Gesellschaft:

- **Usability**: Konzentriert sich auf das Design von Systemen, die einfach zu bedienen sind.
- **Einfachheit**: Unterstreicht die Notwendigkeit einfacher und leicht verständlicher Sicherheitsmaßnahmen.
- **Geschwindigkeit**: Befasst sich mit der Effizienz von Sicherheitsprozessen.
- **Genauigkeit**: Betont die Bedeutung eines fehlerfreien Betriebs.
- **Interpretierbarkeit**: Unterstreicht die Notwendigkeit von Sicherheitsinformationen und Schnittstellen, die klar und eindeutig sind.

Die Konvergenz von Kommunikationsbedürfnissen und Nutzerverhalten ist ein kritischer Bereich innerhalb der Cybersicherheit. Die intensive vernetzte Kommunikation, verbunden mit menschlichem Verhalten bei der Nutzung von Informations- und Kommunikationstechnologie (IKT), erfordert ein hohes Maß an Bewusstsein für Verantwortung, mögliche Auswirkungen und Richtlinien für das Verhalten in der digitalen Welt.

Stufe1: Allgemeine Einführung & Motivation

Quelle: BMBWF: Abt. I/11a - Bundes-AG ITen IT-Sicherheit, Kompetenzebenen 1 – 5; Version März 2019
+ projektbezogene Anpassung mit Punkt 1.0, als Überleitung aus der Sekundarstufe I.

1.1 Grundlagen und Verhalten:

- Technologisches Grundverständnis.
- Das richtige Verhalten im Umgang mit (vor allem personenbezogenen) Daten.
- Das Erkennen von Risken und Reaktionsgrundsätze.

1.2 Motivation zur Sicherheit

- Bewusstseinsbildung: Video - Fallbeispiele, Keylogger.
- Schadsoftware.
- Gute Hacker – Böse Cracker?; Ethical Hacking.
- Identitätsdiebstahl.
- Bedrohungen, Angriffsvektoren, Auswirkungen und Eskalationsszenarien, Schutz personenbezogener Daten.
- Social Engineering.

1.3 Grundbegriffe

- Antivirus, Malware, Phishing.
- Cybermobbing.
- Grundbegriffe und Strategien der Datensicherheit.
- Digitale Identität.
- Defender’s Dilemma.

1.4 Über den Umgang mit Daten im Internet

- Klassische "persönliche" Angriffe erkennen und vermeiden
- Attachements – Dateiendungen (welche gibt es, welche können „bösartig“ sein).
- Mail - Header und URLs analysieren können, um die Herkunft von Spam-/Phishing-Mails als solche eindeutig feststellen zu können.
- Datenspuren im Internet.
- Daten sicher verwalten und weitergeben (z.B. Cloudspeicher verwenden).
- Daten sicher löschen.
- Das eigene Gerät sichern.

1.5 Sicherheitsempfehlungen

- Verhaltensrichtlinien (beispielsweise Abmeldung/Sperren, Clean Desktop…).
- Sperrbildschirm mit Kennwörtern.
- Updates und Patches; 0-Day-Exploits.
- Bioskennwörter–sicherer Bootprozess.
- Verhalten in öffentlichen Netzen / öffentlichen WLAN’s / privaten Netzen.
- Bedeutung von Kennwörtern (Komplexität, Länge), Rainbowtable.
- Mobile Device Management (beispielsweise „Fernlöschung“).
- Least Privileges.
- Privatsphäre in Spielen und Chatrooms.

1.6 Bedrohungsszenarien

- Sicherheitskompromittierung durch externe Geräte erklären (Rubberducky / Bashbunny, Autorun, USB-Killer).
- Angriffsmethoden für Informationsweitergabe: z.B. Phishing, Whaling, Gophish.
- Was tun im Notfall?
- Richtig reagieren.
- Ansprechpartner kennen.
- Infektionsbeseitigung initiieren.

Stufe 2: “Exploratory” - Tiefergehende Awareness für IT-anwendende Berufe, persönliche Sicherheit, rechtliche Rahmenbedingungen und Normen

Quelle: BMBWF: Abt. I/11a - Bundes-AG ITen IT-Sicherheit, Kompetenzebenen 1 – 5; Version März 2019

2.1 Vertraulichkeit und Integrität

- Wie funktioniert Verschlüsselung? (ohne technische Tiefe).
- Wie funktioniert eine Hashfunktion? (ohne technische Tiefe).

2.2 Über den Umgang mit Daten II

- Backup anlegen und Daten wiederherstellen.
- Datenträgerverschlüsselung kennen und benutzen.
- Sicheres Entsorgen von Dokumenten / Datenträgern.
- Virenscanner konfigurieren und einsetzen.

2.3 Sichere Kommunikation

- Sichere Verbindung zum Arbeitsplatznetzwerk herstellen.
- Persönliche Firewalls einsetzen.
- Sichere Authentifizierungsmethoden benennen (NIST Guidelines, Password Safes, Mehrfaktorauthentifizierung).
- Verschlüsselte Kommunikationskanäle wie z.B. HTTPS und Zertifikat.

2.4 Digitale Bürgerkarte

- Was ist eine Signatur? (asynchrone Verschlüsselung mit Public und Private Key).
- Digitale Signaturen überprüfen und anwenden.
- Elektronische Signaturen („Handysignatur“).
- Funktionsabläufe.

2.5 Smart Devices

- Anwendungsfelder von spezifischen Devices und Bedienhilfen, z.B. Smartwatches, Alexa.
- Spezifische Suchmaschinen, z.B. Shodan.

2.6 Rechtsgrundlagen

- Die rechtlichen Gegebenheiten in Österreich und Europa verstehen (IT-Recht/StGB/DSGVO).

2.7 Technische Umsetzungsstrategien

- Sicherheitsmanagement und -systeme kennen (inkl. Sicherheitsstrategien).
- Grundschutz nach BSI.
- Einfache Netzwerksicherheitstools nennen und bedienen
- Anonymisierungsdienste
- Logfiles
- Sandboxing – Virtuelle Maschinen

2.8 Angriffsvektoren

- Ransomware.
- Botnetze.
- Mobiltelefon als „lohnendes“ Angriffsziel?
- Vertraue ich einer App? (beispielsweise Android Hardening guide).
- DOS / DDOS.
- Cybercrime (ENISA Top 15 Thread Landscape, Europol IOCTA).
- Defacements.
- Reconnaissance.
- 6 Stufen eines Angriffs.

Stufe 3: “Foundational” - Netzwerk- Geräte - und Anwendungssicherheit, Sicherheitsmanagement

Quelle: BMBWF: Abt. I/11a - Bundes-AG ITen IT-Sicherheit, Kompetenzebenen 1 – 5; Version März 2019

3.1 Grundlagen der IT-Sicherheit

- Verschlüsselungs- und Hashing-Verfahren beschreiben und unterscheiden.
- Funktionsweise von aktiven Netzwerkkomponenten (Switches, Router, Firewall, APs, IDS-IPS).

3.2 Gerätesicherheit

- Unterschiedliche Betriebssysteme und Netzwerkkomponenten wie z.B. Microsoft Windows, Linux mittels Rechte-verwaltung und Authentifizierung gegen unberechtigte Zugriffe absichern.
- Reduktion der Angriffsfläche durch Abschaltung nicht benötigter Dienste (Gerätehärtung, etc.).
- Monitoring von Diensten/Prozessen. Erkennen unerwünschter oder mangelhaft konfigurierter Dienste / Prozesse.
- Konfiguration und Analyse von Betriebssystem-Ereignissen.
- Automatisierung von Administrationsabläufen mit Scripts - in diversen Programmiersprachen wie z.B. Bash, Powershell etc., für Angriffs- und Verteidigungszwecke (DDoS, Abfrage von Konten mit denen Dienste gestartet werden, etc.).
- Einsatz von Werkzeugen und Scripts zur Informationsbeschaffung von Endsystemen (Abfrage, ob ein besti mmter KBxxx installiert wurde, Benutzeranmeldungen die älter sind als 30 Tage, Aktivieren aller gesperrten Konten, welche Dienste laufen, etc.).

3.3 Netzwerksicherheit

- Analyse einfacher fundamentaler Protokolle (z.B. DHCP, HTTP, DNS, TCP/IP, ICMP und ARP mit Wireshark o.ä.).
- Gesicherte Verbindung zwischen Arbeitsplätzen konfigurieren (VPN, FIDO, MFA, HTTPS).
- Einsatz von Standardwerkzeugen für die Netzwerkanalyse (Bsp.: Nslookup, tracert, etc.).
- Einsatz von Scripts zur Informationsbeschaffung aus dem IT-Netzwerk (z.B. Syslog, Remote-Scannen).
- Grundlegende Anwendungsmöglichkeiten geeigneter Tools und Frameworks wie z.B. Kali, Hacking-Lab, Metasploit etc. um Hosts oder Netzwerke angreifen zu können.

3.4 Sicherheit von Daten und Webanwendungen

- Passende Technologien zur Absicherung von gespeicherten Daten anwenden (z.B.. Bitlocker).
- Verschlüsselungs- und Hashing-Verfahren einsetzen und anwenden.
- Webanwendungen nach Sicherheitslücken scannen und Analysedaten verstehen.
- Einsatz von Werkzeugen und Scripts zur Informationsbeschaffung von Webanwendungen.
- Kennenlernen von Programmierrichtlinien für sichere Webanwendungen (z.B.: ISO 25000, ÖNORM A7700, etc.).

3.5 Organisations-, Risiko- und Sicherheitsmanagement

- IT Security Strukturen in Österreich und Europa sowie deren Aufgaben erklären (Cyberstrategie der Bundesregierung; Cybersecurity Austria / Europol EC3, ENISA, ECSO).
- Sicherheitsmanagement und Sicherheitsprozesse erklären und einsetzen (ISMS/ISO 27001, Sicherheitsprozesse, Risikomanagement).
- Kennenlernen von Sicherheitsstandards wie z.B.: Schweizer IKT-Minimalstandard, BSI-Grundschutz.

Stufe 4: „Professional“ - Angriffsmuster und Verteidigungsmaßnahmen

Quelle: BMBWF: Abt. I/11a - Bundes-AG ITen IT-Sicherheit, Kompetenzebenen 1 – 5; Version März 2019

4.1 Sichere Softwareentwicklung

- Standards bei der Softwareentwicklung kennen und anwenden (z.B. NIST, Audits, Safety, etc.).
- Continuous Integration und Testing einsetzen.
- Verschlüsselungs- und Hashingverfahren in eigenen Programmen einsetzen und anwenden.
- Formale Verifikation von Software und Protokollen an einfachen Beispielen durchführen.
- Statische und dynamische Code Analysen an einfachen Beispielen durchführen (mögliche Buffer Overflows erkennen, Tools zum Auffinden von Memory Corruptions einsetzen, etc.).
- Schutzmaßnahmen kennen und anwenden (gegen Injections, etc.; Control Flow Integrity - CFI, Address Space Layout Randomization - ASLR, etc.).
- Finden von Schwachstellen mittels Fuzzing und Delta Debugging.

Sichere Webentwicklung:

- Standards bei der Webentwicklung kennen und anwenden (ISO 25000, ÖNORM A7700, etc.).
- Continuous Integration und Testing einsetzen.
- Verschlüsselungs- und Hashingverfahren in eigenen Programmen einsetzen und anwenden.
- Authentifizierungsmethoden bei Webanwendungen einsetzen.
- Web Application Security Angriffsvektoren kennen und Angriffe durchführen (OWASP Top 10).
- Eigene Anwendungen durch geeignete Gegenmaßnahmen schützen (WAF, etc.).

4.2 Angriffsmuster und Gegenmaßnahmen

- Hardwarebasierte Sicherheitslücken kennen (sidechannel Angriffe, rowhammer /meltdown /spectre /… kaiser defense - out of order execution).
- Exploits nutzen und metasploit Module anwenden.
- Penetration Testing planen, (im Labor) durchführen und dokumentieren (wie z.B. Kali, metasploit, etc.).
- Netzwerk-Angriffsvektoren kennen und Angriffe durchführen (dhcp, arp, ospf, dns, bgp, wlan, etc.).
- Geeignete Gegenmaßnahmen implementieren (IDS/IPS, Monitoring).

4.3 Monitoring und BigData

- Automatisierte Verfahren zur Informationsbeschaffung aus dem Netzwerk einsetzen (SIEM, Windows Event Forwarding, syslog, Proxylogs, etc.).
- Netzwerk-Angriffsvektoren erkennen (IDS, Monitoring).
- Werkzeuge zur Visualisierung von Daten einsetzen (ELK, etc.).
- Werkzeuge zur automatisierten Verhaltensanalyse und Anomalieerkennung einsetzen (AI, ELK, SIEM, etc.).

Stufe 5: „Excellence“ – Forensik und Softwaresicherheit

Quelle: BMBWF: Abt. I/11a - Bundes-AG ITen IT-Sicherheit, Kompetenzebenen 1 – 5; Version März 2019

5.1 Digitale Forensik

- Incident-Response Zyklus kennen und anhand von Fallbeispielen Schritte ableiten.
- **Phase 1** - laufendes System
  - Speicherdumps erstellen.
  - Beweismittel sicherstellen ("Prozessablauf", Festplattenabbilder erstellen, etc.).
- **Phase 2** - Offlineanalyse
  - Versteckte und verdächtige Prozesse finden (volatility, rekall, etc.).
  - Prozessartefakte (Netzwerkhandles, Filehandles, etc.) analysieren (Prozessexplorer, TCPView, lsof, netstat, etc.).
  - Dateisysteme, Logdateien analysieren (File Carving, MFT, Timestamps, Timeline Analyse).
  - Rechtliche Aspekte berücksichtigen (Behörden und Dritte einbeziehen, Meldepflichten, Datensch utz, etc.).
- **Phase 3** - Reporting
  - Angriffe nachvollziehen (Backtracking, Angriffsquellen, Timeline Analyse, etc.).
  - Dokumentation des Sachverhalts durchführen & "Lessons Learned" festhalten.

5.2 Reverse Engineering

- Dynamische Analyse von Software (tracing, etc.) mittels sandboxing (cuckoo, etc.) und anderen geeigneten Werkzeugen durchführen.
- Einfache statische Analysen durchführen (strings, FLOSS, etc.).
- Malware-Analyse anhand von einfachen Beispielen mit einem Debugger durchführen.
- Disassemblierung und/oder Deobfuscation von codierten Binärdateien oder Skripten durchführen (Debugger, Disassembler, etc.).

Literaturverzeichnis

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, *82*(2), 261.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on Cybersecurity social engineering: A literature review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE*, 62–68.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). *Gender difference and employees' cybersecurity behaviors*.

Arsenovych, L., Nikolaievsky, O., Skliarenko, O., Lytvynenko, L., & Kydriavskyi, I. (2024). Organization of Training with the Use of Digital Technologies for Ensuring Cybersecurity in the Educational Space. *WSEAS TRANSACTIONS ON COMPUTER RESEARCH*, *12*, 524–536. https://doi.org/10.37394/232018.2024.12.51

Baacke, D. (1997). *Medienpädagogik* (Vol. 1). Niemeyer.

Bacigalupo, M., Kampylis, P., Punie, Y., & Brande, G. (2016). *EntreComp: The entrepreneurship competence framework*. Publication Office of the European Union. https://eige.europa.eu/resources/lfna27939enn.pdf

Bartels, J. (2023). *Cyber-Sicherheit Schülerdaten in Gefahr* [Online Bericht]. https://www.business-wissen.net/articles/cyber-sicherheit-schuelerdaten-gefahr

Brägger, G., & Rolff, H.-G. (Eds). (2024). *Handbuch Lernen mit digitalen Medien: Wege der Transformation.* (3., aktualisierte und erweiterte Auflage). Beltz Verlagsgruppe.

Brečko, B., & Ferrari, A. (2016). *The digital competence framework for consumers* (EUR28133EN). Publications Office of the European Union. https://doi.org/10.2791/838886

Brüggen, N., Dreyer, S., Gebel, C., Lauber, A., Müller, R., & Stecher, S. (2019). *Gefährdungsatlas Digitales Aufwachsen. Vom Kind aus denken. Zukunftssicher handeln.* (p. 186). Bundesprüfstelle für jugendgefährdende Medien. https://www.bzkj.de/resource/blob/176416/2c81e8af0ea7cff94d1b688f360ba1d2/gefaehrdungsatlas-data.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2025). *Die Lage der IT-Sicherheit in Deutschland 2025*.

Bundeskanzleramt. (n.V.). *Cybersicherheit—Bundeskanzleramt Österreich*. Bundeskanzleramt. https://www.bundeskanzleramt.gv.at/themen/cybersicherheit.html

Bundesministerium für Bildung. (2025a). *Digitale Schule*. https://www.bmb.gv.at/Themen/schule/zrp/dibi.html

Bundesministerium für Bildung. (2025b). *Sicheres Internet für Schülerinnen und Schüler*. https://www.bmb.gv.at/Themen/schule/zrp/dibi/saferinternet.html

Bundesministerium für Finanzen. (n.d.). *CLEMENTINE – Cybersecurity-Literacy in der wissEnsverMittlung dEr sekuNdarsTufe IN östErreich*. Retrieved 3 October 2025, from https://www.kiras.at/gefoerderte-projekte/detail/clementine-cybersecurity-literacy-in-der-wissensvermittlung-der-sekundarstufe-in-oesterreich/

Bundesministerium für Inneres, Bundeskriminalamt. (2024). *Cybercrime-Report 2023*. https://www.bmi.gv.at/magazin/2024_07_08/01_Cybercrime_Report_2023.aspx

Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Publications Office of the European Union. https://doi.org/10.2760/38842

Cascio, W. F., & Montealegre, R. (2016). How Technology Is Changing Work and Organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, *3*(1), 349–375. https://doi.org/10.1146/annurev-orgpsych-041015-062352

Coeckelbergh, M. (2020). *AI Ethics*. MIT Press.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011a). From game design elements to gamefulness: Defining gamification. *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9–15.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011b). From game design elements to gamefulness: Defining" gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9–15.

European Commission. (2019). *The EU Cybersecurity Act*. 55.

European Union Agency for Cybersecurity. (2023). *Identifying emerging cybersecurity threats and challenges for 2030.* Publications Office. https://data.europa.eu/doi/10.2824/117542

Foisy, N. (2024, July 25). *Integrating Cybersecurity Education in the K-12 Curriculum*. https://www.compassitc.com/blog/integrating-cybersecurity-education-in-the-k-12-curriculum

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *17*, 4.

Gulyamov, S., Babaev, J., & Rakhmatov, U. (2024). Building Cybersecurity Culture in Education as Imperative for Youth to Thrive in Digital Society. *Uzbek Journal of Law and Digital Policy*, *2*(5), 1–10. https://doi.org/10.59022/ujldp.218

Hamari, J., Koivisto, J., & Sarsa, H. (2014). *Does gamification work? A literature review of empirical studies on gamification* (pp. 3025–3034). https://doi.org/10.1109/HICSS.2014.377

Happ, R., Kögler, K., Schmidt, J., & Egloffstein, M. (2024). Editorial. *Empirische Pädagogik*, *38*(1), 6–8. https://doi.org/10.62350/QVHQ3765

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based Cybersecurity training: Are serious games suitable for Cybersecurity training? *International Journal of Serious Games*, *3*(1), 53–61.

Hill, W., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020). A Survey of Serious Games for Cybersecurity Education and Training. *KSU Proceedings on Cybersecurity Education, Research and Practice*. https://digitalcommons.kennesaw.edu/ccerp/2020/Research/7

Hoxhunt. (2025, June 24). *Does Gamified Cyber Security Training Actually Work?* https://hoxhunt.com/blog/gamified-cyber-security-training

Huitema, D., & Wong, A. (2025). A Case Study in Gamification for a Cybersecurity Education Program: A Game for Cryptography. *arXiv Preprint arXiv:2502.06706*.

IBM. (n.V.). *What is Cybersecurity?* https://www.ibm.com/topics/cybersecurity

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158.

Knogler, M., Hetmanek, A., & CHU Research Group. (2018). *Adaptive Lernsoftware: Ein wirksames Mittel im Umgang mit Schülerdiversität?* (No. Kurzreview 21). www.clearinghouse-unterricht.de

KPMG Austria. (2023). *Cybersecurity in Österreich 2023. Österreichs Unternehmen im Umgang mit neuen Herausforderungen*. https://kpmg.com/at/de/home/insights/2023/05/cybersecurity-studie-2023.html

Macgilchrist, F. (2019). *Digitale Bildungsmedien im Diskurs: Wertesysteme, Wirkkraft und alternative Konzepte*. https://www.bpb.de/shop/zeitschriften/apuz/293124/digitale-bildungsmedien-im-diskurs/

McGettrick, A. (2013). Toward Effective Cybersecurity Education. *IEEE Security & Privacy*, *11*(6), 66–68. https://doi.org/10.1109/MSP.2013.155

Mishra, S. (2024). *Integrating Cybersecurity Education into the Curriculum: Best Practices and Implementation Challenges*. Department of Business management,Maharana Pratap Engineering College. https://www.researchgate.net/publication/383846506_Integrating_Cybersecurity_Education_into_the_Curriculum_Best_Practices_and_Implementation_Challenges#fullTextFileContent

Mits, K. (2023, May). *Cybercrime Report 2022: Lagebericht über die Entwicklung von Cybercrime, Bundesministerium für Inneres, Bundeskriminalamt*. https://www.bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf

Moore, M. (2025). *Bringing Gamification to Cyber Security Training*. https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. *Transactions on Edutainment*, *XV*, 93–107.

Mühlenbeck, F. (2025). *Whitepaper: Menschliche Firewall zum Schutz vor Cyberangriffen.*

Oberländer, M., Beinicke, A., & Bipp, T. (2020). Digital competencies: A review of the literature and applications in the workplace. *Computers & Education*, *146*, 103752, https://doi.org/10.1016/j.compedu.2019.103752

O'Hara, G. (2025, January 14). Phishing-Simulationen stärken das Cyber-Bewusstsein und die Abwehrkräfte. *Cyber Resilience Insights*. https://www.mimecast.com/de/blog/phishing-simulations-boost-cyber-awareness-and-defenses/

Olmstead, K., & Smith, A. (2017, March 22). What the Public Knows About Cybersecurity. *Pew Research Center*. https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

Pfleeger, C. P. (1997). *Security in computing* (2. ed). Prentice Hall.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

Redecker, C. (2017). European framework for the digital competence of educators: DigCompEdu. *JRC Research Reports JRC107466*. https://doi.org/10.2760/159770

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH*, *8*, 205520762210817. https://doi.org/10.1177/20552076221081716

Schirmer, K., Frieß, M., Missomelius, P., & Steiner, M. (2024). *Kommentar zum Fachlehrplan Digitale Grundbildung(Mittelschule/AHS-Unterstufe)*. https://www.paedagogikpaket.at/component/edocman/365-kommentar-zum-lehrplan-2/download.html?Itemid=0

Schrittwieser, S. (2025). Phishing-Simulation. *Das Cybersecurity Awareness Playbook*. https://www.watchlist-internet.at/warnungen-tipps/phishing-smishing-vishing/

Schüller, K., Koch, H., & Rampelt, F. (2021). Data-Literacy-Charta. *Berlin: Stifterverband.* *https://www.stifterverband.org/sites/default/files/data-literacy-charta_v1_1.pdf*

Seidel, T., & Krapp, A. (Eds). (2014). *Pädagogische Psychologie: Mit Online-Materialien zum Download* (6., vollständig überarbeitete Aufl). Beltz.

Statistik Austria. (2022). *IKT-Einsatz in Haushalten*. https://www.statistik.at/statistiken/forschung-innovation-digitalisierung/digitale-wirtschaft-und-gesellschaft/ikt-einsatz-in-haushalten

Tirtea, R. (2017). *ENISA overview of cybersecurity and related terminology*. 8.

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 223–228. https://doi.org/10.1109/PST.2016.7906931

Videnovik, M., Trajkovik, V., Vold, T., Kiønig, L. V., Bogdanova, A. M., & Filiposka, S. (2025). Using Peer-Learning and Game-Based Instruction for Achieving Long-Lasting Knowledge of Cybersecurity in Primary Schools. *IEEE Access*, *13*, 11679–11688. https://doi.org/10.1109/ACCESS.2024.3479921

Young, J., Farshadkhah, S., & Smith, T. (2024). Directing the eye: Enhancing cybersecurity education through media. In M. I. Hwang (Ed.), *Teaching Information Systems* (pp. 87–114). Edward Elgar Publishing. https://doi.org/10.4337/9781802205794.00011

Zhilisbayev, A. (2023, May 8). *Cybersecurity in der Schule: Ein nachhaltiger Umgang*. https://www.wirmachendigitalisierungeinfach.de/bildung/cybersecurity-in-der-schule/

Zierer, K., Busse, V., Wernke, S., & Otterspeer, L. (2015). Feedback in der Schule—Forschungsergebnisse. In *Handbuch Feedback in der Schule* (pp. 31–50). Beltz.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.

Abbildungsverzeichnis

Tabellenverzeichnis

Kontakt

AIT Austrian Institute of Technology GmbH

Giefinggasse 4, 1210 Wien

www.ait.ac.at

Beatrix Wais-Zechmann

Tel +43 (0) 50550-4574

beatrix.wais-zechmann@ait.ac.at