CLEMENTINE

Cybersecurity-Literacy in der wissEnsverMittlung dEr sekuNdarsTufe IN östErreich

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-Kybernet-Pass CS F&E Dienstleistungen (CS FED_2023)	**Status**	laufend
Projektstart	01.10.2024	**Projektende**	30.11.2025
Zeitraum	2024 - 2025	**Projektlaufzeit**	14 Monate
Keywords	Cybersecurity, digitale Kompetenz, Sekundarstufe II, Sensibilisierung		

Projektbeschreibung

Die Digitalisierung bildet eine wesentliche Grundlage für den Fortschritt hin zu einer zeitgemäßen Gesellschaft. Vor dem Hintergrund hoher Entwicklungsdynamiken im Bereich Cybersicherheit einerseits und in Vorausschau auf bevorstehende Durchbrüche weiterer emergenter und disruptiver Technologien gilt es, die Sensibilisierung der Gesellschaft für Cybersicherheit weiter voranzutreiben. Fehlendes Bewusstsein und Wissen für den Themenkomplex Cybersecurity stellen Unternehmen branchenübergreifend vor Herausforderungen. Ungefilterter Datenzugang und freizügiges Teilen von Daten und Inhalten im Internet bieten neue, einfach und rasch ausnutzbare Angriffsflächen für Cyberkriminelle. Dahingehend ist die Integration von Cybersicherheit in die schulische Bildung unerlässlich mit der Notwendigkeit, Bemühungen und Inhalte im Sinne der Cybersecurity-Kompetenzvermittlung als Vorbereitung auf den beruflichen Alltag voranzutreiben. Ausgehend von vorhandenen Maßnahmen und Initiativen zur Bewusstseinssteigerung für Cybersicherheit in Österreich (z.B. Digitale Grundbildung) wird in CLEMENTINE der Forschungsbedarf anhand folgender Ziele adressiert: Das Hauptziel ist die Entwicklung eines bildungspolitischen, gesellschaftlichen und sozio-technischen Ansatzes zur Vermittlung des Themenbereichs Cybersecurity für 14- bis 19- Jährige mit besonderem Bezug zum beruflichen Kompetenzerwerb und zum Arbeitsmarkt. Dies wird durch die folgenden drei Teilziele erreicht.

Ziel 1: Erlangung eines strukturierten Überblicks über wesentliche Akteur:innen für die Vermittlung von Cybersecurity-Kompetenzen in der Sekundarstufe II in Österreich: In CLEMENTINE werden strukturiert relevante Akteur:innen aus dem Bildungssektor in Österreich (Bildungsanbieter: innen, Bildungsdirektion, Schuldirektionen, Interessensvertretungen, Verbände, etc.) eruiert und ein Überblick über die relevanten Player geschaffen. Die Übersicht liefert die Basis zur Schaffung von Vernetzungs- und Kommunikationsstrukturen zwischen Akteur:innen zur Unterstützung des bildungspolitischen und schulpädagogischen Diskurses bei der Konzipierung von Maßnahmen für eine schulübergreifende Cybersecurity-Kompetenzvermittlung für 14-19-Jährige in Österreich.

Ziel 2: Identifikation arbeitsbezogener Cybersecurity Themen und Anknüpfungspunkte in Lehrplänen und Schulmaterialien der Sekundarstufe II in Österreich: Erforderlichen Kompetenzen hinsichtlich Cybersecurity aus Arbeitsmarktsicht exemplarisch für die Branchen Banken, Energie, Handel werden erhoben, Zudem werden Lehrpläne und Schulmaterialen

gesichtet. Auf Basis dessen und ausgehend von allgemein relevanten Themen (z.B. Phishing, Umgang mit Cyber-Sicherheit-Tools, Malware, Netzwerk-Sicherheit) werden konkrete Cybersecurity-Themengebiete identifiziert.

Ziel 3: Erarbeitung von exemplarischen didaktischen Konzepten zur Vermittlung von Cybersecurity Themen sowie deren Anknüpfungspunkte im Unterricht im Bereich der Sekundarstufe II in Österreich: Auf Basis der Analyse von Lehrplänen und -materialien sowie ausgehend vom wissenschaftlichen Stand der Forschung werden beispielhafte, didaktische Grundlagen für Vermittlungsformate einer im Vorfeld definierten Auswahl an Schultypen (z.B. AHS, BMHS, HTL) sowie Lehr- und Lernkontexte (z.B. Einsatz digitaler Medien, Methoden) erarbeitet. Dabei wird darauf geachtet, dass die vorgeschlagenen Konzeptskizzen an didaktische Vorgaben der vorhandenen Formate (Digitale Grundbildung, etc.) anknüpfen. Außerdem werden Chancen und Grenzen von Integrationsmöglichkeiten sowie Potenziale zur Adaptierbarkeit der Lehrinhalte erörtert, da der Bereich Cybersecurity im Besonderen einem ständigen Wandel unterliegt, bedingt durch immer neue technische Errungenschaften (z.B. KI) und neuartige Möglichkeiten von Cyberangriffen.

Die Ziele werden durch Desk Research (Aktuer:innen, Lehrmaterialien und didaktischen Konzepte), durch Interviews mit Experti:innen, Fokusgruppen mit Schüler:innen, Arbeitsgruppen und Stakeholder:innen Workshops erarbeitet.

Abstract

The digitization forms an essential basis for progress towards a contemporary society. Against the backdrop of high development dynamics in the field of cybersecurity on the one hand, and in anticipation of upcoming breakthroughs in other emerging and disruptive technologies, it is crucial to further advance society's awareness of cybersecurity. Lack of awareness and knowledge regarding the complex topic of cybersecurity pose challenges to companies across industries. Unfiltered data access and unrestricted sharing of data and content on the internet offer new, easily and rapidly exploitable attack surfaces for cybercriminals. Therefore, the integration of cybersecurity into school education is essential, with the need to advance efforts and content in terms of cybersecurity competence as preparation for professional life.
Based on existing initiatives to increase awareness of cybersecurity at schools (e.g., Digital Basic Education), CLEMENTINE addresses research needs through the following objectives:

Main Objective: Developing an educational, societal, and socio-technical approach to educate the topic of cybersecurity to 14- to 19-year-olds with a particular emphasis on vocational competency acquisition and the job market. This is achieved through the following three sub-goals.

Objective 1: Obtaining a structured overview of key actors in the field of cybersecurity competencies in upper secondary education in Austria. In CLEMENTINE, relevant actors from the education sector in Austria (educational providers, educational authorities, school administrations, interest groups, associations, etc.) are systematically identified, and an overview of the relevant players is created. This overview serves as the basis for establishing networking and communication structures between actors to support educational policy and pedagogical discourse in the design of measures for cross-school cybersecurity competence for 14-19-year-olds in Austria.

Objective 2: Identification of work-related cybersecurity topics and connection points in curricula and teaching materials of upper secondary education in Austria. Necessary competencies regarding cybersecurity from the labor market perspective, exemplarily for the banking, energy, and trade sectors, are surveyed. Additionally, curricula and teaching materials are

reviewed. Based on this and starting from generally relevant topics (e.g., phishing, handling cybersecurity tools, malware, network security), specific cybersecurity topic areas are identified.

Objective 3: Development of exemplary didactic concepts for imparting cybersecurity topics and their connection points in teaching in the field of upper secondary education in Austria. Based on the analysis of curricula and teaching materials and starting from the scientific state of research, exemplary didactic foundations for teaching formats of a pre-defined selection of school types (e.g., general secondary schools, vocational schools, technical schools) as well as teaching and learning contexts (e.g., use of digital media, methods) are developed. It is ensured that the proposed concept sketches align with the didactic requirements of existing formats (Digital Basic Education, etc.). Furthermore, opportunities and limitations of integration possibilities as well as potentials for adaptability of teaching content are discussed, as the field of cybersecurity, in particular, is subject to constant change, driven by ever-new technical advancements (e.g., AI) and novel possibilities of cyberattacks.

The objectives are developed through desk research (actors, teaching materials, and didactic concepts) as well as through interviews with experts, focus groups with students, working groups, and stakeholder workshops.

Endberichtkurzfassung

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 in folgenden Kategorien erstellt: Wissensvermittlung im Bildungsbereich, kommerzielle Wissensvermittlung, Forschung, Interessensvertretungen, Vereine, Initiativen sowie öffentliche Verwaltung. 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 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 vor. 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 acht Haupterkenntnisse umfassen 1) das heterogene Wissen und die Lücken im Cybersecurity-Wissen bei Jugendlichen, 2) die Herausforderungen bei der Aus- und Weiterbildung von Lehrkräften hinsichtlich Cybersecurity-Thematiken, 3) das hochdynamische und zunehmend komplexere Themenfeld Cybersecurity im Kontrast zu den relativ starren Rahmenbedingungen im Schulsystem, 4) pädagogische Ansätze für die Cybersecurity-Vermittlung, 5) das Lehrplan-Dilemma und die Frage nach Erreichung von einheitlichen Standards in der Cybersecurity-Bildung, 6) Chancen und Möglichkeiten bei den aktuellen Lehrplan-Reformen, 7) die Notwendigkeit kuratierter, praxisnaher Lehrmaterialien und 8) die Berücksichtigung von Gender, Diversität und Inklusion in der Vermittlung von CS-Kompetenzen.

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 in den Lehrplänen zu verankern. Gleichzeitig sollte langfristig eine Plattform geschaffen werden, um die sich stark verändernden Themenfelder im Bereich Cybersecurity in den schulischen Bereich zu überführen und so die Cybersecurity-Ausbildung aktuell zu halten — sowohl in Form kuratierter, innovativer Lehrmaterialien als auch durch vertieften Austausch zwischen Schulen und Stakeholder:innen aus der Praxis.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Österreichisches Institut für angewandte Telekommunikation
- Bundesministerium für Bildung