INDUCE

Cyber Security Literacy And Dexterity through Cyber Exercises

Programm / Ausschreibung	Laura Bassi 4.0, Laura Bassi 4.0, Laura Bassi NATS 2018	**Status**	abgeschlossen
Projektstart	01.04.2021	**Projektende**	31.08.2024
Zeitraum	2021 - 2024	**Projektlaufzeit**	41 Monate
Keywords	Cybersicherheit, Cyber-Übungen, Diversität		

Projektbeschreibung

Sicherheit und Privatsphäre sind wichtige Aspekte im Zuge der Digitalisierung und Vernetzung von Informations- und Kommunikationstechnologien (IKT). In den letzten Jahren wurden eine Vielzahl an verschiedenen Übungen entwickelt, die spezifisch Cybersicherheitskompetenzen und -fähigkeiten abfragen, erweitern und fördern. Zu diesen Übungen zählen unter anderem Table-Top-Übungen, die oftmals Awareness und Verständnis für die Thematik fördern oder technische Cyber-Übungen, die durch die Unterstützung von technischen Simulationen technische Fähigkei-ten oder Kenntnisse im Bereich Informationssicherheit fördern. Etablierte Übungen sind derzeit bereits z.B. im Bereich Informationssicherheit, im akademischen Bereich, in Netzwerken und Inno-vationshubs, in Organisationen, die bereits Cybersicherheitskompetenzen in diesem Bereich auf-bauen bzw. aufgebaut haben, zu finden. Beispiele sind z.B. die Austria Cyber Security Challenge oder das KSÖ Planspiel. Derzeit ist der Personenkreis, der an Übungen teilnimmt sehr limitiert. Bei-spielsweise nehmen Frauen nur im einstelligen Prozentbereich an technischen Cyber-Übungen teil. Diese praxis-orientierten Übungen wären jedoch auch für weitere Zielgruppen wichtig, damit eine breitere und kritischere Masse an Personen und Organisationen mit den digitalen Herausfor-derungen umgehen lernt, versteht und lösungsorientierte Ansätze zur Vermeidung, Erkennung und Eindämmung von Cybervorfällen in der täglichen Praxis anwenden kann.
Das Projekt INDUCE zielt darauf ab existierende Cyber-Übungen auf Chancengerechtigkeit für ver-schiedene Zielgruppen unter Einbezug verschiedener Diversitätsdimensionen (z.B. Gender, Alter und soziale Herkunft) evaluiert werden und aufbauend darauf Cyber-Szenarien, Algorithmen und Technologien neu entwickelt, erweitert bzw. adaptiert. Diese Entwicklungen werden durch den Aufbau eines interdisziplinären Innovationsnetzwerkes für Wirtschaft, Behörden und Forschung ergänzt und dadurch ein Wissens- und Technologietransfer unterstützt. Im Rahmen des Projektes werden vier zentrale Bausteine durchgeführt: Öffnung und Erweiterung von Cyber-Übungen für neue Zielgruppen mittels Vielfaltsmanagement, Entwicklung von diversitätssensiblen Cyber-Szenarien, Algorithmen und Technologien für Cyber-Übungen, den Aufbau und die Förderung ei-nes Innovationsnetzwerkes für Cyber-Übungen und die Umsetzung und Evaluierung für verschie-dene Zielgruppen mit Hilfe von Future Labs. Mit INDUCE können langfristig Cybersicherheitskom-petenzen für die Bevölkerung aufgebaut und weiterentwickelt werden, die im Zuge der Digitalisie-rung zur Handlungsfähigkeit vielfältiger Zielgruppen in einer digitalen Gesellschaft beitragen.

Abstract

Security and privacy are important aspects of the digitization and networking of information and communication technologies (ICT). In recent years, a large number of different exercises have been developed that specifically test, expand and promote cybersecurity skills and abilities. These exercises include table-top exercises, which often promote awareness and understanding of the topic, or technical cyber-exercises, which promote technical skills or knowledge in the field of information security by supporting technical simulations. Established exercises can already be found in the field of information security, in academia, in networks and innovation hubs, in organizations that are already building or have already built up cyber security competencies. Examples are e.g. the Austria Cyber Security Challenge or the KSÖ business game. Currently, the number of people participating in exercises is very limited. For example, women only take part in technical cyber exercises in the single-digit percentage range. However, these practice-oriented exercises would also be important for a number of target groups, so that a broader and more critical mass of people and organizations can learn to deal with the digital challenges, understand them and apply solution-oriented approaches to prevent, detect and contain cyber incidents in daily practice.
The INDUCE project aims to evaluate existing cyber-exercises on equal opportunities for different target groups, taking into account different diversity dimensions (e.g. gender, age and social back-ground) and to develop, extend and adapt cyber-scenarios, algorithms and technologies. These developments are complemented by the establishment of an interdisciplinary innovation network for business, public authorities and research, thus supporting knowledge and technology transfer. Within the project, four central modules are being implemented: Opening and expansion of cyber-exercises for new target groups by means of diversity management, development of diversity-sensitive cyber-scenarios, algorithms and technologies for cyber-exercises, the establishment and promotion of an innovation network for cyber-exercises and the implementation and evaluation for different target groups with the help of Future Labs. With INDUCE, cyber security competencies for the population can be established and developed in the long term, which in the course of digi-talization contribute to the empowerment of diverse target groups to act in a digital society.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Cyber Security Austria - Verein zur Förderung der digitalen Sicherheit, abgekürzt: CSA
- Kompetenzzentrum Sicheres Österreich (KSÖ)
- Infraprotect Gesellschaft für Risikoanalyse, Notfall- und Krisenmanagement GmbH
- FH OÖ Forschungs & Entwicklungs GmbH