Programm Laura Bassi 4.0
Eine Initiative der Nationalstiftung für Forschung, Technologie und Entwicklung (FTE)

Cyber Security Literacy and Dexterity Through Cyber Exercises

Final Report

Version 1.0

AIT Austrian Institute of Technology • Infraprotect • KSÖ Kompetenzzentrum Sicheres Österreich
Cybersecurity Austria • Fachhochschule Oberösterreich

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACSC	Austria Cybersecurity Challenge
AIT	AIT Austrian Institute of Technology GmbH
AK	Arbeiterkammer
AP	Arbeitspaket
APA	Animated pedagogical Agents
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CSA	Cybersecurity Austria
CTF	Capture the Flag
CÜ	Cyberübungen
DiFü	Digitaler Führerschein
DsiN	Deutschland sicher im Netz (Verein)
ECSC	European Cybersecurity Challenge
ENISA	European Union Agency for Cybersecurity
EPU	Ein-Personen-Unternehmen
FH OÖ	Fachhochschule Oberösterreich
FTI	Forschung, Technologie und Innovation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
INDUCE	Cybersecurity Literacy and Dexterity Through Cyber Exercises
IKT	Informations- und Kommunikationstechnologien
IFL	INFRAPROTECT® FUTURE LABS
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things, Internet der Dinge
IP	Internet Protocol
ISMS	Information Security Management System
IT	Informationstechnologie
KSÖ	Kompetenzzentrum Sicheres Österreich (Verein)
KMU	Klein und Mittleres Unternehmen
NATO	North Atlantic Treaty Organization oder Nordatlantikpakt
NIST	Nationales Institut für Standards und Technologie
NOC	Network Operations Center
ÖIAT	Österreichisches Institut für angewandte Telekommunikation
ÖRK	Österreichisches Rotes Kreuz
SOC	Security Operations Center
TZI	Themenzentrierte Interaktion
WLAN	Wireless Local Area Network
ZG	Zielgruppe

1 Einleitung

Das Projekt INDUCE („Cybersecurity Literacy and Dexterity Through Cyber Exercises“) wurde im Rahmen der FTI-Initiative „Laura Bassi 4.0“[1] ins Leben gerufen mit dem Ziel, Cybersicherheitskompetenzen und -fähigkeiten für eine breite Zielgruppe zugänglich zu machen. In einer zunehmend digitalisierten Welt, in der Informations- und Kommunikationstechnologien (IKT) allgegenwärtig sind, stellen Sicherheit und Privatsphäre zentrale Herausforderungen dar. Vor diesem Hintergrund hat sich INDUCE darauf fokussiert, existierende Cyberübungen durch den Einsatz von Diversitätsmanagement zu evaluieren und anzupassen. Dabei wurde besonderer Wert auf Chancengerechtigkeit und die Berücksichtigung von Diversitätsdimensionen wie Geschlecht, Alter und soziale Herkunft gelegt.

Im Rahmen des Projekts wurden innovative Konzepte, Methoden und Werkzeuge für Cyberübungen entwickelt, die in Future Labs mit potenziellen Zielgruppen getestet wurden. Diese Labs ermöglichten einen offenen Innovationsprozess, der es erlaubte, praxisorientierte Lösungsansätze für die Vermeidung, Erkennung und Eindämmung von Cybervorfällen zu erarbeiten. Ein wesentlicher Bestandteil des Projekts war zudem der Aufbau und die Förderung eines interdisziplinären Innovationsnetzwerkes, das den Wissenstransfer zwischen Wirtschaft, Behörden und Forschung unterstützte.

Die Ergebnisse des INDUCE-Projekts tragen langfristig zur Stärkung der Cybersicherheitskompetenzen in der Bevölkerung bei und erhöhen die Handlungsfähigkeit vielfältiger Zielgruppen in einer digitalen Gesellschaft. Mit der erfolgreichen Umsetzung der Projektziele leistet INDUCE einen bedeutenden Beitrag zur Förderung von Cybersicherheit und Chancengerechtigkeit im digitalen Raum.

Dieses Dokument bietet einen Überblick über die Ziele, den Hintergrund und die zentralen Aktivitäten des INDUCE-Projekts.

[1] https://www.ffg.at/laura-bassi-netzwerk-chancengerechte-zukunft

2 Aufbau und Struktur des Innovationsnetzwerkes

2.1 INDUCE-Ansatz

Das übergreifende Ziel des Projekts INDUCE ist, diversitätsgerechte Cyberübungen zu entwickeln. Dabei wird in erster Linie auf Erfahrungen des Konsortiums auf dem Gebiet der Cyber-Planspiele aufgebaut. Die im Projekt erarbeiteten Resultate sollen in einem breiten Netzwerk vorgestellt, getestet und evaluiert werden. Der Transfer von Know-how und Technologie ist daher einer der grundsätzlichen Bausteine der Vorgehensweise im INDUCE-Projekt. Es gilt, die Herausforderungen auf der Schnittstelle von Technologie und Diversität auf adäquate und umfassende Weise zu untersuchen und zu lösen.

Im Rahmen des vom Kompetenzzentrum Sicheres Österreich (KSÖ) zu verantwortenden Arbeitspakets 2 wird ein Innovationsnetzwerk für Cybersicherheitskompetenzen durch Cyberübungen aufgebaut und etabliert. Ausgehend von den bestehenden Netzwerken der Projektpartner*innen fördert die in diesem Sinne geplante Struktur den Austausch mit interessierten KMUs und weiteren Organisationen sowie die daraus erwachsenden Synergieeffekte. Die Entwicklung diversitätsgerechter Cyberübungen wird somit den Bedürfnissen und Realitäten verschiedener Organisationen aus Wirtschaft, Forschung und Behörden Rechnung tragen.

Im Einzelnen bietet das aufzubauende Innovationsnetzwerk folgende Vorteile:

- Know-how- und Technologietransfer im Bereich Cyberübungen,
- Erarbeitung von Strategien für Förderung von Cybersicherheitskompetenzen durch Cyberübungen,
- Erstellung eines Übungs- und Trainingskatalogs,
- Evaluierung von Diversitätsdimensionen im Bereich von Cyberübungen,
- Vernetzung von Wirtschaft, Behörden und Forschung.

2.2 Innovationsnetzwerk

2.2.1 Theoretischer Überblick

Um sich die grundsätzliche Funktion eines Innovationsnetzwerks zu vergegenwärtigen, wurde eine Literaturrecherche durchgeführt, aus der die folgenden Erkenntnisse hervorgingen.

2.2.1.1 Definition

Ein Innovationsnetzwerk wird definiert als:

- Zusammenschluss verschiedener Institutionen, wie Unternehmen, Universitäten, Forschungseinrichtungen etc. zu dem Zweck, die Innovationsrate zu erhöhen und neues technologisches Wissen zu verwerten.[2]

oder

- eine Organisationsform, um Innovationen innerhalb von Unternehmen oder unternehmensübergreifend schneller und effizienter umzusetzen.[3]

[2] Innovationsnetzwerke: Bedeutung und Funktionsweise – GRIN: https://www.grin.com/document/1781
[3] Quelle: Innovationsnetzwerk (innolytics.de): https://www.innolytics.de/innovationsnetzwerk/

2.2.1.2 Ziele

Funktionierende Innovationsnetzwerke erfüllen folgende Funktionen:

- unterstützen
  - den kontinuierlichen **Verbesserungsprozess**,
  - das **Ideenmanagement**,
  - das **Innovationsmanagement** eines Unternehmens;
- ergänzen den Innovationsprozess;
- sind fester Bestandteil einer **Innovationskultur**.[4]

2.2.1.3 Vorteile eines Innovationsnetzwerks

Ein Innovationsnetzwerk bietet einige Vorteile. Diese umfassen:

1. Steigerung der **Ideenvielfalt**
   a. unterschiedliche Sichtweisen in der Ideenfindung und Ideenentwicklung
   b. Inspirationen aus verschiedenen Perspektiven
   c. Überwindung des „Scheuklappenblickes“
2. Effizienzvorteile
   a. Netzwerk als ein agiler unterstützender Kreis, schnell verfügbare Ressourcen
   b. Innovationen schneller entwickelt und umgesetzt
3. Förderung der Innovationskultur
   a. aktuelles Wissen und aktuelle Trends werden durch Mitglieder des Netzwerks in die Organisation hineingetragen

2.2.1.4 Erfolgsfaktoren

Drei zentrale **Erfolgsfaktoren** für ein tragfähiges und zielführendes Innovationsnetzwerk sind:

1. **Stakeholdergruppen** zu identifizieren, die unsere Innovationsstrategie voranbringen,
2. einen digitalen oder physischen Raum als zentralen **Kontaktpunkt** zur Verfügung zu stellen,
3. aktiv mit dem Innovationsnetzwerk zusammenzuarbeiten und regelmäßig in **Kontakt** zu treten.[5]

2.2.2 Realisierte Maßnahmen

In Anlehnung an den theoretischen Rahmen sind im ersten Projektjahr die nachfolgend beschriebenen Ergebnisse zu verzeichnen.

Es wurde eigene Webseite für das INDUCE-Projekt als Vernetzungs- und Kooperationsplattform errichtet (https://induce.ait.ac.at/).

Es wird in Zukunft möglicherweise geplant werden, dass diversitätssensibles Awareness-Schulungsmaterialen auf der oben genannten Webseite zur Verfügung gestellt werden. Die ansprechend gestalteten Basics zur Cybersicherheit stellen den ersten Anknüpfungspunkt für die bisher an Cyberübungen nicht involvierten Zielgruppen. Dadurch soll das Interesse und die Motivation für die aktive Teilnahme an zukünftigen Cyber-Planspielen/Übungen entstehen. Im weiteren Verlauf des Projekts wird der Fokus verstärkt auf der praxisorientierten Fähigkeitsvermittlung liegen, die über die anfangs gestärkte Awareness hinausgeht.

[4] Quelle: Innovationsnetzwerk (innolytics.de): https://www.innolytics.de/innovationsnetzwerk/
[5] Quelle: Innovationsnetzwerk - KPMG Deutschland (home.kpmg)

Die eigene Projektwebseite, befüllt mit grundlegenden themenspezifischen Inhalten, stellt einerseits ein Angebot für die neuen Zielgruppen dar, andererseits eine Plattform für die Kontaktaufnahme zu potenziellen Netzwerkpartner*innen. Die beiden Stakeholdergruppen stehen somit in einem engen logischen Zusammenhang.

Der Etablierung des angestrebten Innovationsnetzwerks musste daher eine Zielgruppenanalyse vorangehen. Im Rahmen eines intensiven Austausches im Konsortium wurde eine Ist-Aufnahme in Bezug auf die Teilnehmer*innen der bisherigen Cyberübungen durchgeführt. Dafür wurden die angebotenen Cyberübungen detailliert analysiert und zugleich auf die Erfüllung oder Nichterfüllung von Diversitätskriterien geprüft. Es musste festgestellt werden, dass die bisher angebotenen Cyberübungen sich nur an die Managementebene von Unternehmen und Behörden oder IT-Sicherheitsexpert*innen der kritischen und strategischen Struktur und an die Cybersicherheits-Nachwuchstalente richteten. Dabei ist der Frauenanteil geringfügig und viele Teile der Bevölkerung nehmen an gar keinen Cyberübungen oder Planspielen teil. Angesichts der wachsenden Cyberkriminalität erscheint es daher dringend notwendig, für alle Bevölkerungsgruppen niederschwellige Möglichkeiten zu schaffen, eigene Cybersicherheitskompetenzen im Rahmen frei zugänglicher Cyberübungen zu überprüfen und zu stärken.

Als Folge dieser Erkenntnis einigte sich das Konsortium auf die neu angestrebten Zielgruppen (siehe Kapitel 5).

Die Heterogenität der in Betracht gezogenen Zielgruppen erfordert differenzierte Lösungsansätze bei der Entwicklung von diversitätssensiblen Cyberübungen. Die Ansprache der technikfernen Gruppen wird sich wesentlich von der Ansprache der angehenden Cybersicherheitsexpert*innen unterscheiden. Diese Diversität innerhalb der Zielgruppen soll sich ebenso in der Struktur des Innovationsnetzwerks widerspiegeln.

2.2.3 Struktur des Innovationsnetzwerks

Es wurden folgende mögliche Stakeholdergruppen für das Netzwerk identifiziert:

*2.2.3.1 Netzwerkpartner*innen nach definierten Zielgruppen*

Unternehmerinnen, Einzelunternehmerinnen / Juristinnen, Steuerberaterinnen, PR-Mitarbeiterinnen

- Frau in der Wirtschaft FiW (WKO) - www.wko.at/site/fiw-wien/
- EPU-Netzwerk (Wir sind 1 und trotzdem ganz schön viele) - www.wirsind1.at
- Sheconomy Wirtschaftsmagazin (das Netzwerk der Frauennetzwerke) - sheconomy.media/netzwerke/

Studentinnen, weibliche IT-Kräfte

- Femtec GmbH - www.femtec.org
- women@POI - das Frauennetzwerk von Porsche Informatik -
- www.porscheinformatik.com/it-frauennetzwerk-porsche-informatik
- FEMtech - Frauennetzwerk, das vom Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie betrieben wird - www.femtech.at
- Role Models: FEMtech Expertinnendatenbank[6]
- Frauen in der IT (confare.at), Confare Female IT-Mentoring (Think Tank Confare)
- Women in Informatics https://informatics.tuwien.ac.at/women-in-informatics/

[6] https://www.femtech.at/content/expertinnen-suche

- Innovatorinnen Club (früher: w-fFORTE) https://www.ffg.at/innovatorinnen

Jugendliche, Fokus: junge Frauen

- TheNewITGirls - www.thenewitgirls.com
- FIT – Frauen in die Technik (FIT Wien – NÖ – BGLD) https://fitwien.at/
- Think Tank CONFARE - führt eine Liste weiblicher Role Models für die IT-Branche aus dem DACH-Raum, um durch Mentor*innen und Vorbilder das Interesse an MINT-Fächern stärken https://confare.at/frauen-weiblicher-nachwuchs-fuer-die-it/
- BilundgsHub.Wien - Service der Bildungsdirektion für Wien https://bildungshub.wien/

2.2.3.2 Organisationen aus dem Bereich der Cybersicherheit

- CAST e.V. Competence Center for Applied Security Technology (Deutschland): Peer-Workshops und Vernetzungsmöglichkeit für Studierende (Nachwuchsförderpreis)
- TeleTrusT Bundesverband IT-Sicherheit e.V. (Regionalbüro für Österreich): Vernetzung mit deutschsprachigen Wirtschafts-Unternehmen im Security-Sektor
- ECSO: Arbeitsgruppe Women in Cybersecurity ECSO (European Cybersecurity Organisation) https://ecs-org.eu/initiatives/women4cyber-initiative

2.2.3.3 Organisationen aus dem Bereich Forschungsförderung

- FFG Österreichische Forschungsförderungsgesellschaft
- AWS Austria Wirtschaftsservice Gesellschaft mbH

2.2.3.4 Forschungsorganisationen

- FH St. Pölten
- Josef Ressel Forschungszentrum
- FH Technikum Wien
- TU Wien

2.2.3.5 Organisationen aus dem Bereich der Digitalen Bildung

- OCG Österreichische Computer Gesellschaft www.ocg.at
- GI Gesellschaft für Informatik e.V. (Deutschland, gi.de) als Publikationsforum und für Workshop-Teilnahmen
- IT-Cluster: regionale Vernetzung von IT-Unternehmen und IT-abhängigen Unternehmen, Veranstaltungen (auch für Laien) www.itcluster.at
- DigitalCityWien www.digitalcity.wien
- ICT Austria, Center for Business Technology - Verein für Österreichische IKT Unternehmen www.ictaustria.com
- A-SIT www.a-sit.at Zentrum für sichere Informationstechnologie – Austria
- Haus der Digitalisierung - Das virtuelle Haus der Digitalisierung (virtuelleshaus.at)

2.2.3.6 Niederschwellige autodidaktische Bildungsangebote

- www.fit4internet.at
- www.watchlist-internet.at
- www.saferinternet.at

2.2.4 Ausblick

Die zukünftigen Partner*innen des Innovationsnetzwerks werden zunächst mittels der Website auf das INDUCE-Projekt aufmerksam gemacht und zur Kooperation eingeladen. Angestrebt ist die ge-

genseitige Unterstützung bei einer niederschwelligen Gestaltung von Cybersicherheitsinhalten sowie eine gemeinsame Evaluierung der zu entwickelnden Cyberübungen und Planspielen für die breite Bevölkerung.

3 Netzwerkarbeit, Verbreitung der Ergebnisse und langfristige Erhaltung

Der Transfer von Know-how und Technologie ist einer der grundsätzlichen Bausteine der Vorgehensweise im INDUCE-Projekt. Daher wurden im zweiten und im dritten Projektjahr die Aktivitäten mit Außenwirkung verstärkt ins Visier genommen.

3.1 KSÖ-Aktivitäten 2022-2024

In den nächsten Kapiteln werden die realisierten Maßnahmen aufgelistet und beschrieben.

3.1.1 Teilnahme und Vortrag am 15. Forschungsforum der österreichischen Fachhochschulen (April 2022)

Am 15. Forschungsforum der österreichischen Fachhochschulen, das am 21. April 2022 stattfand, wurde das Projekt vorgestellt und auch erste Resultate präsentiert. In den nächsten Kapiteln werden Details der Teilnahme des INDUCE Projektes dargestellt.

3.1.1.1 „Cybersecurity Meets Equity“

Am 21. April 2022 haben das KSÖ und die Fachhochschule Oberösterreich (FH OÖ) am 15. Forschungsforum der österreichischen Fachhochschulen auf dem Campus Villach der FH Kärnten die ersten Ergebnisse des Projekts INDUCE präsentiert. Der Fokus des Vortrags lag auf der Methodologie der Analyse von Cyber-Spielen im Hinblick auf Diversitätsdimensionen und Chancengerechtigkeit. Denn die bewährten Formate von Cyber-Planspielen oder Cyber Ranges, deren namhaftes Beispiel das KSÖ Cybersecurity Planspiel darstellt, sollten nunmehr nicht nur für die kritische Infrastruktur und Behörden, sondern auch für technikferne und diverse Zielgruppen angeboten werden. Dies soll zur Stärkung der Cyberresilienz der breiten Bevölkerung Österreichs beitragen.

3.1.1.2 „Creating Impact“

Das Motto des diesjährigen Forschungsforums „Creating Impact – gemeinsam wirksam werden“ macht auf die Wichtigkeit von Kooperationen aufmerksam, die einerseits Non-Research-Organisationen einbeziehen, andererseits überregional oder generationenübergreifend wirken. So wird der Impact von Forschungsprojekten verstärkt und nachhaltig lösungsorientiert gestaltet.

Die Präsentation des Projekts INDUCE fand im Themenblock „Cross-border Cooperations“ statt, indem der Mehrwert grenzüberschreitender Projektpartnerschaften besonders hervorgehoben wurde. Dies trifft nämlich vollkommen auf das INDUCE-Konsortium zu, in dem sich Wissenschaftler*innen, IT-Spezialist*innen, Unternehmer*innen und Netzwerker*innen zusammenfanden, um die Digitalisierung in Österreich gerechter mitzugestalten.

3.1.1.3 Ausblick

Mit der Teilnahme am Forschungsforum der Fachhochschulen konnte das KSÖ von einem regen Austausch in der Forschungs-Community profitieren und viele neue Einblicke in die Zukunftsthemen gewinnen. Die Resonanz des Publikums auf die Präsentation des INDUCE-Projekts bestätigte die Bedeutsamkeit des Forschungsvorhabens und zeigte uns weitere Perspektiven auf Lösungsansätze für eine chancengerechte digitale Zukunft.

ABBILDUNG 1 TITELBILD FOLIE „CYBERSECURITY MEETS EQUITY"

3.1.2 Teilnahme der Gruppe „Gesellschaft" am KSÖ Planspiel (November 2022)

3.1.2.1 KSÖ Cyber-Planspiele

Das KSÖ veranstaltet regelmäßig Cyber-Planspiele, um die Zusammenarbeit von Unternehmen und Behörden bei Cyberangriffen zu trainieren und zu optimieren.

Die Erfahrung aus bisherigen KSÖ-Planspielen zeigte, dass sich diese in Bezug auf die Teilnehmenden stark auf die oberste Ebene staatlicher Organe und Behörden sowie auf die Ebene des Top-Managements und der Sicherheitsfachkräfte in großen Unternehmen der kritischen Infrastruktur fokussierten. Daraus resultierte die Tatsache, dass an diesen Übungen überwiegend männliche Personen mit einem starken Management- und Technikhintergrund aus Großunternehmen teilnahmen und Inhalt sowie Ablauf der Übungen prägten.

3.1.2.2 INDUCE-Ansatz

Das Projekt INDUCE soll dem KSÖ ermöglichen, das Format „KSÖ-Planspiel" auf Basis eines Diversitätsansatzes inklusiver zu gestalten. Dabei werden die Awareness und Ansprache von KMUs für deren Teilnahme an solchen Veranstaltungen substanziell gestärkt. Eine Erweiterung des Teilnehmendenkreises im Verlauf eines Cyber-Planspiels trägt nämlich dazu bei, dass die Realitäten von Gesellschaft und Wirtschaft in einem wesentlich höheren Ausmaß widergespiegelt werden. Dementsprechend wurde im Rahmen des Projekts INDUCE ein Versuch unternommen, das Format „KSÖ-Planspiel" inklusiver zu machen.

3.1.2.3 KSÖ-Planspiel BlackAUT 2022

Während des am 28. und 29. November 2022 veranstalteten KSÖ-Planspiels wurde in einer digitalen Simulationsumgebung ein Blackout-Szenario realitätsnah durchgespielt. Am Training nahmen neun Spieler*innen-Gruppen und mehrere Beobachter*innen teil, zum einen Sicherheitsakteure aus den Bereichen der kritischen Infrastruktur wie Energieversorgung, Telekommunikation, Mobilität, Finanzdienstleistungen, Gesundheitsversorgung, Lebensmittelversorgung, Logistik, zum anderen Vertreter*innen von Industrie, Behörden und relevanten Einsatzorganisationen.

Erstmals war auch die Gruppe „Gesellschaft“ Teil des Trainings und konnte gleichberechtigt mit den angestammten Teilnehmenden zur Definition effektiver Schutzmaßnahmen im Falle eines Blackouts beitragen. Denn aufgrund der immer stärkeren Verflechtung und gegenseitiger Abhängigkeit verschiedener digitaler Systeme erscheint es auch immer relevanter, bei einer Krisenbewältigung die Positionen und Bedürfnisse aller Bevölkerungsteile zu berücksichtigen. Somit konnte die Perspektive von Entscheider*innen in einem Ernstfall mit jener der am meisten Betroffenen abgeglichen und angepasst werden. Von besonderer Bedeutung zeigte sich dabei die Problematik der erschwerten Kommunikation zwischen den beteiligten Sektoren, den politisch Verantwortlichen und der Bevölkerung.

3.1.2.4 Erkenntnisse

Die erstmalige Integration einer neuen Gruppe trug nicht nur zu feinen ausdifferenzierten Ergebnissen des Trainings bei, sondern zeigte auch, mit welchen Herausforderungen organisatorischer, inhaltlicher wie auch technischer Natur solch eine diversitätsgerechte Gestaltung eines Planspiels einhergeht. Im Folgenden wird auf die Learnings des Blackout-Planspiels eingegangen.

In inhaltlicher Hinsicht zeigte sich eine klare Abgrenzung zwischen den verschiedenen gesellschaftlichen Rollen der Bevölkerungsvertreter*innen schwierig. Bei der Entwicklung des Spielszenarios wurde nämlich nicht ausreichend berücksichtigt, dass die Teilnehmenden der Gruppe „Gesellschaft“ nicht nur als vom Ernstfall betroffene Privatpersonen auftreten, sondern auch ein bestimmtes berufliches Selbstbild haben. Dies führte zur Unklarheit, in welcher Rolle und folglich aus welcher Perspektive sie die Aufgaben zu lösen hatten.

In der Gruppe waren folgende Berufe vertreten: Feuerwehrmann, Forscherin, Unternehmerin (Marketing-Agentur), Gebäudetechniker, Abteilungsleiterin beim Österreichischen Roten Kreuz und ein IT-Unternehmer als Vertreter der Wirtschaftskammer „Stabstelle Krisenmanagement und Sicherheitsvorsorge“. Im Gegensatz zu den weiteren acht Gruppen hatte diese im Krisenfall keine Entscheidungsbefugnisse wie etwa Vertreter*innen der kritischen Infrastruktur oder von Behörden, deren Aufgaben einen gesamtgesellschaftlichen Ansatz verfolgten. Daher nahmen sich die Mitglieder der Gruppe „Gesellschaft“ als Handelnde in Doppelrolle wahr, nämlich als betroffene Privatpersonen und als Berufstätige. Die Inhalte der Injects trugen nicht zu einer klaren Trennung zwischen diesen Rollen bei, denn sie betrafen u.a. folgende Themen: mobile Pflege, Bildungseinrichtungen und Gebäudetechnik. Dadurch schwankten die Spieler*innen zwischen der Betrachtung privater Herausforderungen (Kinderbetreuung, Angehörigenbetreuung, Eigenversorgung) und der Entwicklung von Krisenplänen (Feuerwehr, ÖRK usw.). Diese Herausforderung wurde insbesondere bei frauendominierten Berufsfeldern sichtbar, wie z. B. in der mobilen Pflege oder allgemein im Sozial- und Bildungsbereich, wo die Arbeitszeiten oft nicht regelmäßig sind und die Arbeitsvorbereitung teilweise zuhause stattfindet. Die Berufsrealität sieht hier also anders als bei Beamten*innen oder Angestellten aus, bei denen die Trennlinie viel klarer ist, somit auch die Rollenzuteilung bei der Aufgabenlösung. Zu beachten ist ebenfalls eine Besonderheit bei der Ausstattung von Kleinunternehmer*innen mit digitalen Geräten: Oft sind es keine getrennten Computer für Privates und Berufliches, was sich ebenfalls auf die Verhaltensmuster und Krisenbewältigungsstrategien dieser Gruppe auswirken kann.

In organisatorischer Hinsicht gelang es in diesem ersten diversitätsgerecht gestalteten Planspiel noch nicht ausreichend, die Vielfalt der gesellschaftlichen Realität vollständig widerzuspiegeln. Bei künftigen Cyber-Planspielen könnten demnach auch andere Alters- und Bevölkerungsgruppen miteinbezogen werden, z. B. Senioren*innen, Studierende, Beeinträchtigte, Migrant*innen. Vorerst gelang es nur, Personen der arbeitenden Bevölkerung, die abseits der strikt kritischen Infrastruktur tätig sind, für die Teilnahme zu gewinnen. Zu einem weiteren Erkenntnisgewinn würde auch die Einladung zusätzlicher gesellschaftlicher Institutionen wie etwa Bildungseinrichtungen oder Medien beitragen. Somit ist eine stärkere Erweiterung des Teilnehmer*innenkreises zu empfehlen. Was den Frauenanteil betrifft, waren insgesamt unter 74 spielenden Teilnehmenden 14 Frauen, d. h. knapp 19%. In der Gruppe „Gesellschaft" betrug der Frauenanteil 50%. Aus dem Feedback zum Planspiel ging hervor, dass die männlichen und die weiblichen Spielenden in dieser Gruppe gleichberechtigt zur Lösung der Aufgaben beitrugen. Der Trend zur Erhöhung der Frauenquote an Cyber-Planspielen gilt es daher fortzusetzen.

In technischer Hinsicht wurde die Gruppe „Gesellschaft" noch nicht ausreichend in die Nutzung der digitalen Simulationsumgebung eingeführt. Dies hätte den Bevölkerungsvertreter*innen ermöglicht, sich die Kaskadeneffekte einer Krise stärker zu vergegenwärtigen. Somit ist auch diesbezüglich ein Verbesserungspotenzial bei der Gestaltung künftiger Cyber-Planspiele festzustellen.

3.1.2.5 Ergebnisse der Feedback-Umfrage

Im Zeitraum 21.12.2022 – 22.01.2023 wurde unter den Teilnehmenden des Planspiels eine Feedback-Umfrage durchgeführt. Frage 2.5 bezog sich auf den Erkenntnis-Mehrwert und lautete:

> *Inwieweit hat die Teilnahme von Vertreter*innen der breiten Gesellschaft zum Erkenntnis-Mehrwert aus dem Planspiel beigetragen?*

Laut den Ergebnissen trug die Teilnahme von Vertreter*innen der breiten Gesellschaft für **65%** der Befragten zu einem **bedeutenden** Erkenntnis-Mehrwert bei, **15%** erachteten die Teilnahme als **entscheidend** und nur **20%** konstatierten einen **geringfügigen** Erkenntnis-Gewinn.

3.1.2.6 Fazit

Die Teilnahme der Bevölkerungsvertreter*innen am KSÖ-Planspiel 2022 trug zweifelsohne dazu bei, dass der Fokus bei der trainierten Krisenbewältigung stärker auf den **Faktor Mensch** verschoben wurde. Es wurde deutlich, dass bei einem **Zusammenbruch digitaler Systeme** nicht nur deren Wiederherstellung im Vordergrund stehen sollte, sondern auch die **Vielfalt der gesellschaftlichen Rollen** von Beteiligten und Betroffenen berücksichtigt werden muss. Gerade im immer noch **frauendominierten** Pflege- oder Versorgungsbereich vermengen sich die berufsbezogenen und die rein privaten Aufgaben, demnach ist eine klare Trennung zwischen den beiden Lebensbereichen schwierig. Dieser Erkenntnis soll daher in den künftigen Cyber-Planspielen verstärkt Rechnung getragen werden.

Die im KSÖ-Blackout-Planspiel 2022 erprobte Öffnung des Planspiel-Formats für eine breitere Zielgruppe verbessert die Chancengleichheit und Diversität in den zukünftigen Veranstaltungen dieser Art. Denn die Bewältigung einer Krise erfordert **einen gesamtgesellschaftlichen Einsatz**. Daher gilt es auch in den realitätsabbildenden Cyberübungen alle Diversitätsdimensionen mit einzubeziehen.

ABBILDUNG 2 TEILNEHMENDE „GESELLSCHAFT“ KSÖ BLACKAUT PLANSPIEL 2022

3.1.3 KSÖ-Planspiel 2023

Im darauffolgenden Jahr wurde bei der Planung und Organisation des KSÖ-Planspiels erneut versucht, die Vertreter*innen der Bevölkerung einzubeziehen.

Das bereits sechste KSÖ-Planspiel – diesmal unter dem Namen „CLUEDO“ – wurde am 13. und 14. November 2023 gemeinsam mit dem AIT im Haus der Digitalisierung in Tulln veranstaltet.

Nach dem fiktiven Szenario wurde die Versorgungsinfrastruktur der österreichischen Wirtschaft und die wichtigen, voneinander abhängigen Lieferketten angegriffen. Die teilnehmenden Vertreter*innen österreichischer Unternehmen und Behörden trainierten diesen Cyberangriff auf Staat, Wirtschaft und Gesellschaft in einer modernen digitalen Simulationsumgebung.

Gegen die massiven sektorenübergreifenden Auswirkungen der eingeschleusten Schadstoffware kämpften fünf Teams. Diese setzten sich aus Cybersicherheitsexpert*innen aus IT-Fachabteilungen, Behördenvertreter*innen und Unternehmer*innen aus den betroffenen Wirtschaftsbranchen zusammen. Durch die realitätsnahe Konfrontation mit dem Angriff konnten die bestehenden Sicherheitsmaßnahmen und Kommunikationskanäle erprobt und evaluiert werden.

Ein weiteres wichtiges Ziel des Planspiels war, die teilnehmenden Organisationen auf die Umsetzung der NIS2-Richtlinie vorzubereiten. Da dieser Bereich nicht direkt die breite Bevölkerung betrifft, gestaltete sich eine diversitätsgerechte Einbeziehung der Gesellschaftsvertreter*innen schwierig. Das Szenario spielte sich eher im organisationalen als im interpersonellen Kontext ab, daher waren die Inhalte der Übung kein adäquates Übungs- und Erfahrungsfeld für die breite Bevölkerung. Es ging grundsätzlich um Teile der kritischen Infrastruktur, deren Resilienz für alle Bürger*innen existenziell ist, aber nur von den jeweiligen Verantwortlichen geschützt und im Ernstfall wiederhergestellt werden kann.

Solch eine Schwerpunktsetzung wirkte sich auf die Diversität der teilnehmenden Personen aus. In den Spieler*innenteams befanden sich unter 41 Personen lediglich drei Frauen, und unter 46 Beobachter*innen nur vier. Dies zeigt, dass es nach wie vor nicht automatisch gelingt, ohne zielgerichtete Maßnahmen zur Stärkung der Diversität unter den Teilnehmenden mehr weibliche Interessierte zu gewinnen. In dieser Hinsicht erscheint es notwendig, diverse Gruppen unbedingt explizit anzusprechen.

Die INDUCE-Projektpartner*innen waren am Planspiel als stille Beobachter*innen anwesend. Das ganze Team kam zur Schlussfolgerung, dass die Diversität im Bereich der Cybersecurity nur mit dezidierten Anstrengungen möglich ist.

ABBILDUNG 3 INDUCE PROJEKTTEAM BEIM KSÖ-PLANSPIEL 2023

3.1.4 Awareness-Kampagne für EPU und KMU „Cybersecurity-Tipps“ in Kooperation mit der Wirtschaftskammer Wien (2023)

Währen der Arbeit an dem Projekt kam die Idee auf, wie man am besten EPUs und KMUs erreichen könnte. Da wurden wir darauf aufmerksam gemacht, dass die WKO ihren Mitgliedern regelmäßig Newsletter zukommen lässt. Da das KSÖ mit der WKO gut vernetzt ist, wurde dieser Schritt weiterverfolgt und kam auch zu einem positiven Schluss indem über mehrere Newsletter hinweg insgesamt 29 Tipps und ein Gewinnspiel (Tipp 24) ausgeschickt wurden.

3.1.4.1 Eckpunkte des Vorhabens

Die Cybersecurity-Tipps erschienen unter dem Leitspruch „Kurz.Verständlich.Sicher“ auf der Landingpage der Wirtschaftskammer Wien CYBER-TIPPS - WKO.at. Da diese Seite nicht mehr erreichbar ist, ist eine Zusammenfassung aller Tipps auf der INDUCE Homepage[7] und auch im Anhang unter Kapitel 12.1 zu finden.

- Zielgruppe: Kleinst-/Einzelunternehmen, die keine IT-Dienstleister*innen beschäftigen
- Ziel: Basiskenntnisse zur Cybersicherheit vermitteln, einen sanften Einstieg in die Thematik ermöglichen
- Methode (gemäß den im ersten Projektjahr erarbeiteten Handlungsempfehlungen):
  - Ultrakurze Lerneinheiten, die sich in den Geschäftsalltag einfach integrieren lassen
  - jeweils nur eine Botschaft
  - angepasste Sprache – Fachbegriffe möglichst einfach erklärt (z. B. *Malware* als *bösartige Programme*)
  - Verweise auf Cyberübungen zur Stärkung der Handlungskompetenz
  - Verweise auf niederschwellige weiterführende Quellen (z. B. auf aktuelle Betrugswarnungen der WKO oder von Watchlist Internet)
- Mehrwert für Unternehmer*innen:
  - Wissenserwerb für Eigenbedarf

[7] https://induce.ait.ac.at/induce-cybersecurity-tipps/

- im Cybernotfall eine bessere Kommunikationsbasis in Kontakten mit IT-Dienstleister*innen (Kommunikation auf Augenhöhe)
- Verinnerlichung der digitalen Gefahren

Mit dieser Kampagne wurde das im ersten Projektjahr entwickelte Vorhaben umgesetzt. Hier der einschlägige Auszug aus Kapitel 2.2.2:

> *„Demnächst entsteht diversitätssensibles Awareness-Schulungsmaterial, das auf der (…) Webseite zur Verfügung gestellt wird. Die ansprechend gestalteten Basics zur Cybersicherheit stellen den ersten Anknüpfungspunkt für die bisher an Cyberübungen nicht involvierten Zielgruppen. Dadurch soll das Interesse und die Motivation für die aktive Teilnahme an zukünftigen Cyber-Planspielen/Übungen entstehen. Im weiteren Verlauf des Projekts wird der Fokus verstärkt auf der praxisorientierten Fähigkeitsvermittlung liegen, die über die anfangs gestärkte Awareness hinausgeht.“*

3.1.4.2 Hintergrund

Die Kampagne setzte sich zum Ziel, die Wissensdefizite und Unsicherheiten im Umgang mit digitalen Technologien auf eine ansprechende Art und Weise auszugleichen. Es galt zu berücksichtigen, dass die digitalen Gefahren bei vielen Anwender*innen ambivalent bewertet werden. Nach den Recherchen der FH OÖ praktiziert man einerseits z. B. sorgloses Surfen im öffentlichen Raum, andererseits schenkt man viel Aufmerksamkeit den Datenschutzmaßnahmen. Eine kontinuierliche Auseinandersetzung mit der Cybersicherheit ist noch nicht zur Routine geworden. Die Thematik gilt womöglich als komplex, schwer verständlich und den IT-Experten*innen vorbehalten. Die bisherigen Lern- und Übungsangebote richten sich nicht an die breite Zivilgesellschaft, sondern einerseits in Form großangelegter Cyber-Planspiele an Akteure aus Behörden und Großunternehmen der kritischen Infrastruktur, andererseits an bestimmte Altersgruppen wie Jugendliche (z. B. saferinternet.at) oder Senioren*innen (digitalseniorinnen.at). Selten werden den diversen Zielgruppen handlungsorientierte und interaktive Cyberübungen angeboten. Die Inhalte erscheinen vorwiegend in Form von Texten, deren Anzahl, Länge und Informationsdichte technikferne Empfänger*innen überfordern könnten. Oft werden mehrere Empfehlungen und eine Reihe wichtiger Informationen in einem Text untergebracht. Die Umsetzung der so vermittelten Inhalte erfordert ein größeres Zeitfenster und wird daher auf später verschoben oder gar nicht mehr aufgenommen.

Daher konnte bei der Verfassung und Gestaltung der Cybersecurity-Tipps eine grundsätzliche Herausforderung identifiziert werden, und zwar eine möglichst sinnvolle Reduzierung der Inhalte auf tatsächlich Brauchbares in der unternehmerischen Realität der Zielgruppe. Die Texte sind kurz, in einer verständlichen Sprache verfasst und um Hinweise zu praktischen Übungen ergänzt. Ein Text behandelt nur ein konkretes Thema, wobei auf Nebenaspekte, zusätzliche Ergänzungen und Verweise strikt verzichtet wird. Im Vordergrund stehen stets die Einfachheit und der Realitätsbezug.

3.1.4.3 Synergieeffekte

Ein weiterer positiver Nebeneffekt der Kampagne war die Förderung der Innovationskultur innerhalb des INDUCE-Konsortiums. Bei der Entwicklung der Inhalte kamen die im Kapitel 2.2 genannten Vorteile eines Innovationsnetzwerks zum Tragen:

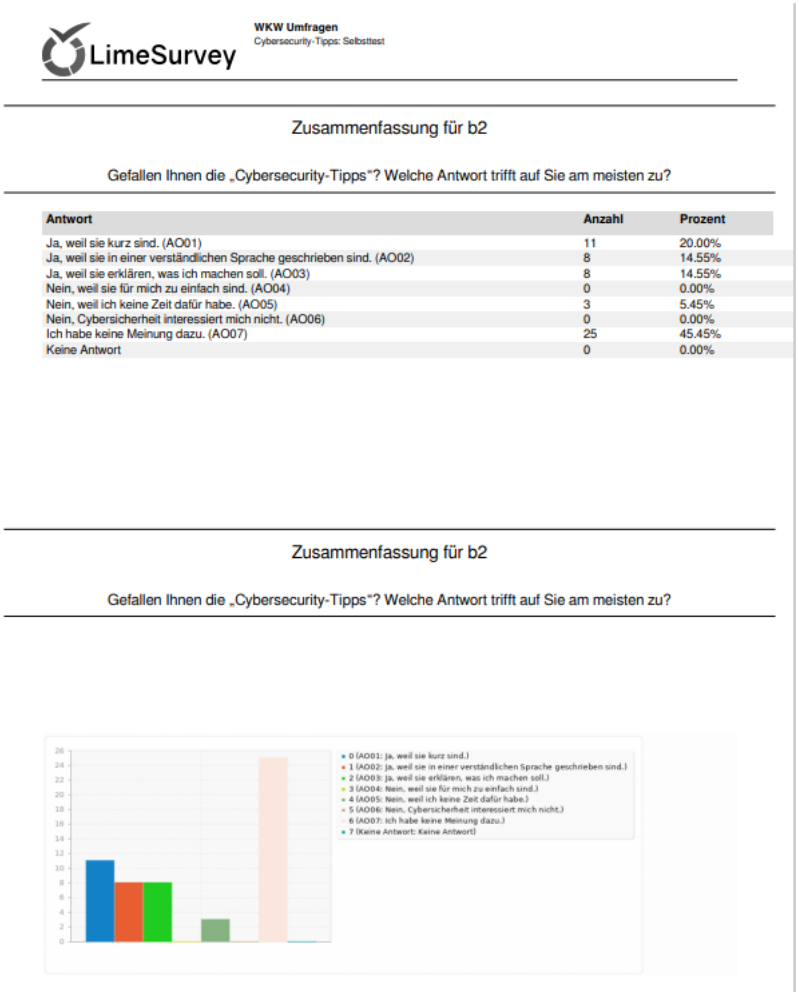
- Steigerung der Ideenvielfalt durch die Einbeziehungen unterschiedlicher Sichtweisen und Inspirationen in der Ideenentwicklung (IT, Diversitätsforschung),
- Effizienzvorteile durch agile Unterstützung und schnell verfügbare Ressourcen der Konsortiumsmitglieder,
- Förderung der Innovationskultur durch Berücksichtigung aktuellen Wissens und aktueller Trends in den Bereichen der Cybersicherheit und der Diversitätsforschung.

In diesem Sinne verknüpfte das KSÖ bei der Erarbeitung der Newsletter-Inhalte in einem diversitätsgerechten Zusammenhang die Expertise einerseits der IT-Spezialisierten, andererseits der diversitätsforschenden Konsortiumspartner*innen, was das Netzwerk innerhalb des Konsortiums maßgeblich verstärkte.

3.1.4.4 Feedback

Um zu eruieren, ob bei der Vermittlung der Grundkenntnisse im Bereich der Cybersicherheit die richtigen Methoden identifiziert wurden und wie sich die einzelnen Faktoren priorisieren lassen (kurz gehaltener zeitlicher Rahmen, die angepasste Sprache, praktische Übungen), wurde unter den Abonnenten*innen des WKW-Newsletters ein Selbsttest mit integrierter Feedback-Umfrage durchgeführt.

An der Umfrage nahmen 55 Personen teil, die sich neben Beantwortung einiger fachlicher Wissensfragen auch zum Mehrwert der Newsletter-Aktion geäußert haben. Hier die Auswertung:



LimeSurvey

WKW Umfragen
Cybersecurity-Tipps: Selbsttest

Zusammenfassung für b2

Gefallen Ihnen die „Cybersecurity-Tipps"? Welche Antwort trifft auf Sie am meisten zu?

Antwort	Anzahl	Prozent
Ja, weil sie kurz sind. (AO01)	11	20.00%
Ja, weil sie in einer verständlichen Sprache geschrieben sind. (AO02)	8	14.55%
Ja, weil sie erklären, was ich machen soll. (AO03)	8	14.55%
Nein, weil sie für mich zu einfach sind. (AO04)	0	0.00%
Nein, weil ich keine Zeit dafür habe. (AO05)	3	5.45%
Nein, Cybersicherheit interessiert mich nicht. (AO06)	0	0.00%
Ich habe keine Meinung dazu. (AO07)	25	45.45%
Keine Antwort	0	0.00%

Zusammenfassung für b2

Gefallen Ihnen die „Cybersecurity-Tipps"? Welche Antwort trifft auf Sie am meisten zu?

ABBILDUNG 4 AUSWERTUNG LIMESURVEY

Die Ergebnisse zeigen, dass die meisten Abonnent*innen die Kürze der Beiträge schätzten. Somit bestätigte sich eine der INDUCE-Hypothesen, dass das viele Informationsmaterial, das in den Medien zugänglich ist, als überladen und abschreckend wirkt. Die ganze Umfrage kann im Anhang (Kapitel 12.3) eingesehen werden.

3.1.4.5 Ausblick

Die Kampagne umfasste insgesamt 30 Newsletter-Kurzbeiträge. Die Inhalte werden auf der Projektwebsite zur Verfügung gestellt, damit die Wirkung der INDUCE-Aktivitäten über die Projektdauer hinaus nachhaltig bleibt[7].

Weiters wird beim KSÖ im Rahmen der Erarbeitung der Maßnahmen zur Projektnachhaltigkeit ein Format für regelmäßig anzubietende Cyber-Simulationsspiele mit niederschwelligen Inhalten entwickelt. Dabei sollen die beim INDUCE-Projekt erprobten Vorgehensweisen Anwendung finden. Die aktuellen Cyberbedrohungen sind demnach so darzustellen, dass die technik-fernen Teilnehmenden nicht überfordert werden und in einer diversitätsgerechten Form interaktiv ihre Resilienz im Umgang mit Cybersicherheit stärken.

3.1.5 Erstellung eines Katalogs für Cyberübungen

Die vorstehend beschriebene Kampagne „Cybersecurity-Tipps“ für EPU und KMU (siehe Kapitel 3.1.4) verfolgte das Ziel, die Cybersecurity-Inhalte nicht nur als Informationen zur Verfügung zu stellen, sondern sie auch um passende Übungen zu ergänzen. Dadurch erhielten die Abonnent*innen des Newsletters die Möglichkeit, ihre theoretischen Kenntnisse zumindest in ganz einfachen Übungen zu festigen. Es galt den Fokus auf eine **praxisorientierte Fähigkeitsvermittlung** zu verschieben. Die gestärkte Awareness wurde aktiv in der Praxis angewendet.

Hierfür wurde **das frei zugängliche Angebot an spielbasiertem Lernmaterial** zum Aufbau digitaler Kompetenzen untersucht. Es handelte sich dabei um diversitätsgerecht konzipierte Übungen, die für nicht fachspezifische und technikferne Gruppen geeignet sind.

Es wurden folgende Quellen für niederschwellige Übungen identifiziert:

- Cybersecurity Quiz (ovosplay.com)[8]
- Unsere Online-Quiz | Bottom-Up (dsin-berufsschulen.de)[9]
- Spiele – BAKgame[10]
- Lernzentrale | Digitalführerschein (DiFü) (xn--dif-joa.de)[11]
- DsiN-Computercheck - Starten (computercheck24.com) [12]
- DsiN-Computercheck - Aktuelle Downloads (computercheck24.com)[13]
- Onlinebetrug Simulator AKNÖ[14]
- Schnitzeljagd: Fake News - saferinternet.at[15]

Die Übungen wurden intern ausprobiert und auf ihre diversitätsgerechte Einfachheit und Praxistauglichkeit geprüft. Die in einem Katalog versammelten Quellen wurden für Interessierte auf der Projektwebsite[16] zur Verfügung gestellt. Der Katalog im Detail ist in Kapitel 4 anzusehen.

Bei jedem der Cybersecurity-Tipps, die im Newsletter der Wirtschaftskammer erschienen, stand – falls im Hinblick auf das behandelte Thema möglich – eine Übungsempfehlung. Es wurde dabei nicht auf die ganze Website verwiesen, sondern auf deren passende Bereiche oder gar auf einzelne Übungen. Angestrebt war damit die praktische Umsetzung der Cybersecurity-Inhalte.

[8] https://cybersecurityquiz.app.ovosplay.com/#/login
[9] https://www.dsin-berufsschulen.de/unsere-online-quiz
[10] https://www.bakgame.de/spiele/
[11] https://difue.de/lernzentrale/
[12] https://www.computercheck24.com/visor_server_1/dsin30/de/showAudit.action
[13] https://www.computercheck24.com/visor_server_1/dsin30/de/downloadlinks.page
[14] https://onlinebetrug.aknoe.at/
[15] https://www.saferinternet.at/quiz/schnitzeljagd-fake-news/
[16] https://induce.ait.ac.at/katalog-einfacher-cyber-ubungen/

Die **Kombination niederschwelliger Texte und Übungsempfehlungen** sollte der Zielgruppe nicht nur einen sanften Einstieg in die Thematik ermöglichen, sondern sie auch zur regelmäßigen Auseinandersetzung mit der Cybersicherheit motivieren. Dies war bisher für EPU/KMU mit Einstiegshürden und Hemmschwellen verbunden. Im Rahmen der Kampagne mit der Wirtschaftskammer Wien konnten diese Hürden allmählich abgebaut werden, indem die Einzel- und Kleinunternehmer*innen den Übungsempfehlungen folgten und sich dadurch die praktische Dimension der Cybersecurity vergegenwärtigten.

Wenn dieser Perspektivwechsel – von einer Auffassung der Cybersicherheit als eines schwierigen und technik-lastigen Themas zum alltagsintegrierten und vertrauten Umgang mit Digitalität – gelingt, wird voraussichtlich auch der Wille zur Teilnahme unterrepräsentierter Gruppen an Cyber-Planspielen/Übungen steigen. Langfristig soll sich ein Teilnehmendenfeld von EPU/KMUs etablieren, das regelmäßig an Cyberübungen teilnimmt. Solche Entwicklung wird zur Erhöhung der Chancengerechtigkeit und Stärkung der Handlungsfähigkeit breiter Bevölkerungsteile in einer digitalen Gesellschaft beitragen.

3.1.6 Fortsetzung der Netzwerk-Erweiterung

3.1.6.1 Innovationsnetzwerk

Die in Kooperation mit der Wirtschaftskammer Wien umgesetzte Kampagne „Cybersecurity-Tipps“ gab dem Projektkonsortium Anlass, sich mit dem vorhandenen Angebot der für die Öffentlichkeit zugänglichen Cyberübungen auseinanderzusetzen und sie auf ihre diversitätsgerechte Niederschwelligkeit zu prüfen. Daraus resultierten weitere Überlegungen, welche Faktoren sich auf die Chancengerechtigkeit in der Vermittlung von Cybersecurity-Inhalten konkret auswirken. Dies begünstigte den **Wissenstransfer** innerhalb des im ersten Projektjahr entwickelten Innovationsnetzwerks. Einerseits wurde eruiert und praxisbezogen evaluiert, welche **Netzwerkpartner*innen** eindeutig niederschwellige und somit für diverse Zielgruppen geeignete Cyberübungen anbieten. Andererseits konnten weitere **Handlungsempfehlungen** für die Gestaltung von Cyberübungen ausgearbeitet werden.

Folglich wurden die dem INDUCE-Ansatz entsprechenden Netzwerkpartner*innen kontaktiert und zum Austausch eingeladen. Somit erweiterte sich das aufzubauende Innovationsnetzwerk um folgende **Organisationen**, die niederschwellig gestaltete Lerninhalte und Übungen zur Cybersecurity bieten:

3.1.6.1.1 Vereine

- fit4internet: www.fit4internet.at
- ÖIAT (Österreichisches Institut für angewandte Telekommunikation), Projekte: www.watchlist-internet.at, www.saferinternet.at
- Deutschland sicher im Netz e.V. DsiN: https://www.sicher-im-netz.de/ueber-uns
- Technische Akademie für berufliche Bildung Schwäbisch Gmünd e.V.: https://www.technische-akademie.de/

3.1.6.1.2 Forschung

- Forschungsgruppe Security & Privacy, Fakultät für Informatik, Universität Wien (Entwicklung des Onlinebetrug-Simulators): https://sec.cs.univie.ac.at/

3.1.6.1.3 Wirtschaft, WKO

Der im Bereich der Cybersecurity unterrepräsentierten Gruppe von Einzel- und Kleinunternehmer*innen wurde im Rahmen des INDUCE-Projekts in enger Kooperation mit der Wirtschaftskammer Wien Folgendes angeboten:

- Niederschwellige Cybersecurity-Tipps, verbreitet mit dem wöchentlichen Newsletter der Wirtschaftskammer Wien (siehe Kapitel 12.1),
- Katalog von Cyberübungen auf der Projektwebseite[17]

Das INDUCE-Angebot erreichte in erster Linie Mitglieder des EPU-Netzwerks und des Netzwerks „Frau in der Wirtschaft".

3.1.6.1.4 Behörden

Die Teilnahme der Gruppe „Gesellschaft" am 2022 veranstalteten KSÖ-Planspiel ermöglichte einen interdisziplinären Austausch mit Vertreter*innen der teilnehmenden **Behörden**, u.a. Bundesministerium für Inneres (BMI) oder Bundesministerium für Landesverteidigung (BMLV).

3.1.6.1.5 IKT-Sicherheitsportal

Im Rahmen der Vernetzung wurde das Projekt INDUCE auf dem **IKT-Sicherheitsportal** www.onlinesicherheit.gv.at als eine der IT-Notfall- und Krisenübungen genannt[18]. Gemäß den Angaben auf der betreffenden Website ist das IKT-Sicherheitsportal eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt.

> *„Die Initiative verfolgt als strategische Maßnahme der* Nationalen IKT-Sicherheitsstrategie[19] *und der* Österreichischen Strategie für Cyber Sicherheit[20] *das Ziel, durch Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie durch Bereitstellung zielgruppenspezifischer Handlungsempfehlungen die IKT- und Cyber-Sicherheitskultur in Österreich zu fördern und nachhaltig zu stärken."*

3.1.6.2 Netzwerk Laura Bassi 4.0 – Digitalisierung und Chancengerechtigkeit

Die Aktivitäten und das Angebot des INDUCE-Projekts wurden auch in der LinkedIn-Gruppe des Netzwerkes Laura Bassi 4.0 kommuniziert.

> *„Das Netzwerk richtet sich an ProjektnehmerInnen der Laura Bassi 4.0 Forschungsprojekte, ExpertInnen im Bereich „Digitalisierung und Chancengerechtigkeit", UnternehmensvertreterInnen, ProgrammanagerInnen aus der Forschungs- und Entwicklungsförderung und ProjektnehmerInnen sowie alle interessierten Personen, die sich mit diesen Themen beschäftigen."*[21]

Die Teilnahme an Netzwerktreffen ermöglichte den Projektpartner*innen einerseits einem interessierten Publikum den INDUCE-Ansatz vorzustellen, andererseits durch regen Austausch mit den Netzwerkteilnehmenden Inspiration und Ideen für weitere Aktivitäten zu gewinnen. Das INDUCE-Team war an folgenden Netzwerktreffen vertreten:

- 16.11.2021 (online)
- 23.06.2022 (ganztägig, Koreakulturhaus Wien)
- 25.01.2023 (ganztägig, Impact Hub Wien)

[17] https://induce.ait.ac.at/katalog-einfacher-cyber-ubungen/
[18] https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/IT-Notfall-und-Krisenuebungen/INDUCE.html
[19] https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Koordination-und-Strategie/Nationale-IKT-Sicherheitsstrategie.html
[20] https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Koordination-und-Strategie/Oesterreichische-Strategie-fuer-Cyber-Sicherheit-OeSCS.html
[21] https://www.oegut.at/de/projekte/gender/laura-bassi-netzwerk-digitalisierung.php

ABBILDUNG 5 INDUCE AM LAURA BASSI NETZWERKTREFFEN, 23.06.2022

ABBILDUNG 6 INDUCE AM LAURA BASSI NETZWERKTREFFEN, 25.01.2023

3.1.6.3 Netzwerken am eDay der Wirtschaftskammer Österreich

Die Veranstaltung „eDAY“ findet jährlich statt und gehört zu den größten E-Business-Events Österreichs. An diesem Tag bringt die Wirtschaftskammer Österreich diverse KMU-relevante Akteur*innen zusammen und bietet ihnen eine Plattform für Austausch zu den aktuellen Themen im Bereich der Digitalisierung, Innovation und aktueller Zukunftsthemen.

Das Thema Cybersicherheit durchzieht jede Edition der Veranstaltung, daher ließen sich die Vertreter*innen des INDUCE-Projektteams vor Ort oder per Livestream von vielfältigen Perspektiven und aktuellen Trends inspirieren. Im Jahr 2022 lautete das Thema „Mit Digitalisierung und Nachhaltigkeit zu mehr Wachstum und Klimaschutz“, im Jahr 2023 „Künstliche Intelligenz als Chance sehen und nutzen“.

3.1.7 Netzwerkveranstaltungen – Teilnahme und Organisation

Um eine breite Wissensverteilung zu ermöglichen, wurden im Rahmen des Projekts Netzwerkveranstaltungen organisiert. Dabei handelte es sich in erster Linie um die Vorstellung der Projektergebnisse sowie um die Anregung einer Diskussion, ob die erforschten Maßnahmen in ausreichendem Maße direkte Effekte auf die neuen Zielgruppen haben und ob deren Bereitschaft zur Teilnahme an Cyberübungen gesteigert werden konnte.

Die allerersten Projektresultate wurden am Anfang des zweiten Projektjahres von FH OÖ und KSÖ am 15. Forschungsforum der österreichischen Fachhochschulen auf dem Campus Villach der FH Kärnten vorgestellt (siehe Pkt. 2.1).

Die Vernetzung mit relevanten Behörden und Vertreter*innen der kritischen Infrastruktur erfolgte im Rahmen des KSÖ-Planspiels (siehe Pkt. 2.2).

Um das Innovationsnetzwerk über aktuelle Entwicklungen und Resultate zu informieren und den Netzwerk-Teilnehmenden einen Erkenntnisaustausch zu ermöglichen, fand am 16. Mai 2023 ein Netzwerktreffen statt. Es war eine Diskussion- und Inspirationsrunde zum Thema „Durch Cyberübungen zur Handlungsfähigkeit“. Eine geeignete Räumlichkeit dafür wurde von der Wirtschaftskammer Österreich zur Verfügung gestellt. Außer den Projektpartner*innen (KSÖ, AIT, FH OÖ, Cybersecurity Austria und Infraprotect) nahmen an der Veranstaltung fit4internet (Frau Ulrike Domany-Funtan) und Universität Wien, Forschungsgruppe Security & Privacy (Herr Sebastian Schrittwieser) teil. Eingeladen war auch ÖIAT (watchlist.internet) und die Wirtschaftskammer Österreich. Die Vertreterinnen dieser Organisationen mussten jedoch ihre Teilnahme kurzfristig absagen. Die Teilnehmenden tauschten sich über ihre vielfältigen Aktivitäten aus. Eine anschließende rege Diskussion betraf u.a. folgende Themen: handlungsorientierte Stärkung der Cybersicherheitskompetenzen, diversitätssensible Ansätze, die größten Herausforderungen in diesem Bereich.

3.2 Netzwerk – Zusammenfassung

Im Zuge der oben genannten Aktivitäten wurde ein Innovationsnetzwerk für langfristigen Wissens- und Technologietransfer etabliert. Es wurden die ersten Kontakte zwischen den Netzwerk-Teilnehmenden aufgenommen wie auch die gemeinsamen Ziele und Tätigkeitsfelder definiert. Dies legte den Grundstock für weiteres Networking. Die Mitglieder des Netzwerks erhielten die Möglichkeit, sich über aktuelle Entwicklungen und Resultate ihrer Aktivitäten zu informieren oder zu Veranstaltungen einzuladen. Im Rahmen der Sensibilisierung für Diversitätsaspekte beachtete das Netzwerk stets ein geschlechterspezifisch ausgewogenes Verhältnis von Teilnehmenden sowie diversitätssensible Sprache bei Einladungen oder Ankündigungen von Veranstaltungen.

Die im ersten Projektjahr identifizierten möglichen Stakeholdergruppen für das Innovationsnetzwerk wurden im weiteren Verlauf des Projekts zum Wissens- und Technologietransfer animiert und

vernetzt. Somit konnten unterschiedliche Sichtweisen in der Ideenfindung und Ideenentwicklung berücksichtigt werden. Das INDUCE-Innovationsnetzwerk wurde zum agilen unterstützenden Kreis mit vielfältigen Ressourcen.

3.3 Ausblick – Nachhaltigkeit des Netzwerks

Das Netzwerk bleibt langfristig und über das Projektende hinaus erhalten und gelebt. Die Inhalte rund um die Cyberübungen und Planspiele bleiben auf der Projektseite abrufbar. Auch die niederschwellig verfassten Cybersecurity-Tipps und ein Katalog von diversitätsgerechten Cyberübungen stehen dauerhaft zur Verfügung. Die im Laufe des Projekts vernetzten Organisationen werden in Kontakt bleiben und das Thema Cyberübungen und Planspiele im Sinne der digitalen Chancengleichheit gemeinsam vorantreiben.

Beim KSÖ wird das Format von niederschwelligen diversitätsgerechten Cyber-Planspielen aufgenommen und in Form von Cybersimulationen für KMUs fortgesetzt. Darin zeigt sich der Mehrwert der Forschungsarbeit im Rahmen des INDUCE-Projekts.

3.4 Zusammenfassendes Fazit

Zusammenfassend lässt sich feststellen, dass das angestrebte Innovationsnetzwerk erfolgreich aufgebaut wurde. Die Zusammenarbeit findet im Rahmen einer gemeinsamen Webpräsenz statt, die als Kooperationsplattform fungiert. Im Rahmen der Aktivitäten mit der Wirtschaftskammer Österreich wurde das Netzwerk für interessierte KMUs geöffnet. Ein Katalog für Cyberübungen steht auf der Projektwebseite zur Verfügung. Zugleich wurde die Nachhaltigkeit und Erhaltung des Netzwerks über das Projekt hinaus spezifiziert und gesichert. Durch die Organisation von eigenen Veranstaltungen sowie die Teilnahme an den Veranstaltungen der Netzwerk-Teilnehmenden wie auch den öffentlichen KMU-spezifischen Konferenzen kam es zu einem intensiven Austausch und Know-how-Transfer zwischen Wirtschaft, Forschung und Behörden. Die Projektergebnisse wurden über diverse Publikationskanäle veröffentlicht.

4 Katalog für Cyberübungen

Theoretisches Grundwissen zur Cybersicherheit macht Sie noch nicht cybersicher. Diese Kenntnisse müssen Ihnen in Fleisch und Blut übergehen. Um dies zu erreichen, können Sie Übungen machen, die wir im Folgenden auflisten.

Dieses spielbasierte Lernmaterial ist frei zugänglich und auch für Personen geeignet, die sich für Technik nur bedingt interessieren. Auf eine unterhaltsame und angenehme Art und Weise können Sie Ihre Cybersicherheits-Kompetenzen aufbauen und festigen. Sie werden sich immer besser auskennen, welche digitalen Gefahren es gibt und wie Sie damit souverän umgehen. Um Ihr Können zu perfektionieren, können Sie auch an Cyber-Planspielen oder Cyber-Workshops teilnehmen.

4.1 „Cybersecurity Quiz"

www.cybersecurityquiz.at

Zielgruppe	alle ab 15
Zugang	über Website, Android oder iOS eine unkomplizierte Registrierung notwendig
Inhalte	technische Bedrohungen, sich vor Betrug schützen, Datenschutz, Cyber-Mobbing, Fake-News, Smartphone, Kinder sicher im Netz, Einkaufen im Internet, Urheberrecht, Home-Office
Aufbau	10 Module Jedes Modul umfasst mehrere Themen. Ein Thema besteht meistens aus zwei Teilen: Einführung und Szenarien. Die Inhalte kann man „entdecken" und „üben".

4.2 Unser Online-Quiz | Bottom-Up

dsin-berufsschulen.de

Zielgruppe	Mitarbeiter*innen von KMU, insbesondere künftige Mitarbeiter*innen (Berufsschüler*innen, Lehrlinge)
Zugang	Internet, mit oder ohne Registrierung
Inhalte	Grundeinstellungen für einen sicheren Arbeitsplatz Sichere digitale Kommunikation Datensicherung und Notfallplanung Mobile und private Endgeräte am Arbeitsplatz

	Cloud-Dienste und Datenschutz in Unternehmen Soziale Medien im Unternehmen nutzen – aber sicher! IT-Sicherheit für Leitende in kleinen und mittleren Unternehmen
Aufbau	6 Lerneinheiten, jeweils ein Online-Quiz als Wissens-Check zum Spielen

4.3 Spiele – BAKgame

https://www.bakgame.de/spiele/

Zielgruppe	kleine und mittlere Unternehmen
Zugang	ohne Registrierung
Inhalte	Lernspiele (Gamification): Phishing-Quiz, Password-Game, SecurityCards, ThreatAttack
Aufbau	4 Lernspiele

4.4 Lernzentrale | Digitalführerschein (DiFü)

https://difü.de/digitalfuehrerschein/lernzentrale/

Zielgruppe	alle ab 14
Zugang	mit oder ohne Registrierung
Inhalte	Geräte & Tools, Internet, Kommunikation, Datenwelt, Gefahrenschutz, Technologiealltag
Aufbau	Lernzentrale mit 2 Kontexten: privater und beruflicher Kontext, jeweils 3 Level, jeweils 6 Themenbereiche, die 4-6 Lerneinheiten zu unterschiedlichen Schwerpunkten enthalten, jeder Schwerpunkt umfasst kurz gehaltene Lerninhalte und den Teil „Mein Wissen üben“, am Ende jedes Bereichs eine optionale Teilprüfung

4.5 DsiN-Computercheck

https://www.computercheck24.com/visor_server_1/dsin30/de/showAudit.action

Zielgruppe	alle Benutzer*innen
Zugang	ohne Registrierung
Inhalte	Computercheck und nützliche Verweise auf Programme und Internetseiten zum Thema Sicherheit
Aufbau	Computercheck: den Startknopf drücken, um Ihren Computer auf veraltete Software und damit verbundene Sicherheitslücken hin zu überprüfen – Anzeige durch ein Ampelsystem (für Mobilgeräte – Start mit einem QR-Code) Downloads mit Schritt-für-Schritt-Anleitungen: Aktualisierungen für Multimedia-Programme, Antiviren-Programme, Firewall-Programme, Internet-Browser, Betriebssystem-Aktualisierungen, weitere kostenlose Programme Tipps rund um das Thema IT-Sicherheit – kurze Texte und Schritt-für-Schritt-Anleitungen

4.6 Onlinebetrug der AK Niederösterreich

https://onlinebetrug.aknoe.at/

Zielgruppe	alle
Zugang	Internet, Anmeldung mit E-Mail-Adresse
Inhalte	simulierte Phishing-Nachrichten und weiterführende Informationen zur Erkennung verdächtiger Nachrichten
Aufbau	Eintrag und Bestätigung Ihrer E-Mail-Adresse Information über den Ablauf des Trainings simulierte Trainings-Nachrichten per E-Mail, nicht gekennzeichnet Nachricht über das Ende des Trainings

4.7 Diversität und Chancengerechtigkeit

Das Arbeitspaket 3 sieht die literaturgestützte, diversitätssensible Analyse von Cyberübungen vor, sowie die Ausarbeitung von Handlungsempfehlungen und Maßnahmen zur Erschließung neuer Zielgruppen und zur Erweiterung oder Anpassung bestehender Cyberübungen an diese Nutzer*innen.

Das Arbeitspaket 3 lässt sich gemäß Projektbeschreibung[22] unter Ziel 1 und Ziel 2 einordnen.

[22] Vgl. AIT Austrian Insititute of Technology. (2020). Cybersecurity Literacy and Dexterity Through Cyber Exercises. Projektbeschreibung für Förderungsansuchen des Programms Laura Bassi 4.0. 2. Ausschreibung. Wien: 2020, S. 23ff. https://www.ffg.at/laura-bassi-4.0-2-ausschreibung (zuletzt aufgerufen am 11.01.2022).

Ziel 1 verfolgt die **Entwicklung von diversitätssensiblen Cyberszenarien und Technologien in Cyberübungen.** Dazu ist die Untersuchung der Gestaltung und Umsetzung von Cyberübungen (CÜ) erforderlich. Insbesondere sollen verschiedene Arten (z.B. handlungs- oder diskussionsbasiert) von CÜ auf Inhalte und deren Aufbau für verschiedene Zielgruppen (ZG) in Bezug auf Chancengerechtigkeit und Diversitätsdimensionen analysiert werden. Dabei sollen nicht nur technische, sondern auch organisatorische Prozesse in den Blick genommen werden.
Ziel 2 strebt den Zugang zu praxisorientierten Cybersicherheitskompetenzen und -fähigkeiten für verschiedene ZG an. Für die Entwicklung von **ZG-spezifischen Designs der Lehr- und Lerninhalte** stehen die Leitfragen „Welche Maßnahmen müssen nicht nur bezüglich Cyberszenarien, Technologien, Methodik und Didaktik getroffen werden, sondern auch für die Organisation von CÜ?“ und „Wie können unterrepräsentierte Zielgruppen sukzessive an das Thema Cybersicherheitskompetenz und -fähigkeiten durch Cyberübungen herangeführt werden?“[23] im Fokus der Untersuchungen.
Die erwarteten Resultate konnten gemäß den Projektanforderungen erfüllt werden:

- **umfassende Analyse von Literatur und aktuellen Cyberübungen unter dem Aspekt der Diversität und Chancengerechtigkeit** (D3.1; T3.1: Diversitätsdimensionen in Cyberübungen)
  - Im 1. Projektjahr erfolgt eine ausführliche Literaturrecherche zur Ermittlung des wissenschaftlichen Status Quo sowie zur Identifikation von Analysekategorien, die im weiteren Projektverlauf entsprechend den Bedürfnissen angepasst, erweitert und verfeinert werden
  - Table-Top-Recherche, Expert*innen-Interviews sowie leitfadengestützte Selbstbeschreibungen ergänzen die einführende Untersuchung der von den Konsortialpartner*innen angebotenen Cyberübungen. Eine detaillierte diversitätssensible Analyse des Teilnehmer*innenfeldes ist aufgrund fehlenden Datenmaterials nicht möglich.
  - Im 2. und 3. Projektjahr werden Table-Top- und Literaturrecherche kontinuierlich und bedarfsorientiert weitergeführt.
  - **Instrumente**: Table-Top- und Literaturrecherche, Expert*innen-Interviews, leitfaden-gestützte Selbstbeschreibung
- **strukturierte Analysen von verschiedenen Arten von CÜ und deren Auflistung nach potenziellen Zielgruppen** (D3.2; T3.2: Analyse von CÜ unter der Berücksichtigung von Diversität und Chancengerechtigkeit; T3.3: Aktuelle und künftige Zielgruppen in CÜ)
  - Im 1. Projektjahr werden mittels Expert*innen- und Fokusgruppeninterviews die verschiedenen Übungsformate genauer unter die Lupe genommen, so dass konkrete neue Zielgruppen für jede Konsortial-Organisation identifiziert werden können.
  - Die Erkenntnisse der Literaturrecherche fließen im 1. und 2. Projektjahr in die Entwicklung und/ oder Anpassung verschiedener Analyse-Instrumente, um die verschiedenen Arten von Cyberübungen untersuchen zu können.
  - Entsprechend erfolgt die Analyse von verschiedenen Arten von Cyberübungen im zweiten Projektabschnitt mittels eines Mixed-Method-Ansatzes, der die jeweiligen Rahmenbedingungen der Übungsformate berücksichtigt.
  - Dort, wo möglich, wird die Zusammensetzung der Übungs-Teilnehmer*innen auf ihre Diversitäts-Dimensionen hin untersucht.
  - Ebenso werden die Übungsformate mithilfe der entsprechenden Instrumente im Hinblick auf Diversitätsaspekte analysiert, um daraus Handlungsempfehlungen zu generieren.

[23] Vgl. AIT (2020), S. 24.

  - Im 3. Projektjahr wurde die Analyse von Cyberübungsformaten bedarfsorientiert weitergeführt und ergänzt.

  - **Instrumente**: Fokusgruppen- und Expert*innen-Interviews, Teilnehmer*innen-Fragebogen, Heuristik, Beobachtungsleitfaden

- **Handlungsempfehlungen für chancengerechte CÜ für Organisator*innen** (D3.3; T3.4 Handlungsoptionen und Empfehlungen für Organisator*innen und KMUs; D2.3 Handlungsempfehlungen für den Zugang von KMUs zu CÜ und niedrige Nutzungsbarrieren)

  - Im 1. Projektjahr erfolgen mehrere **Sensibilisierungs-Workshops** zum Thema „Zielgruppen-Ansprache“. Anhand von **Best Practices** werden erste Handlungsempfehlungen, wie neue Zielgruppen angesprochen, gefunden und interessiert werden können, formuliert. Ergänzt werden diese Empfehlungen durch einen Überblick **diversitätssensibler didaktischer Ansätze,** die nicht-traditionelle Zielgruppen fokussieren.

  - Die im 1. Projektjahr erarbeiteten Maßnahmen werden im 2. Jahr weiter ausgearbeitet und als **Handlungsempfehlungen für die diversitätssensible Gestaltung, Erweiterung oder Adaption von Cyberübungen** für Organisator*innen und Entwickler*innen von Cyberübungen zusammengestellt. Diese umfassen u.a. die **Ansprache** der Zielgruppen, mögliche **Themen**, **Design-Methoden** sowie hilfreiche **didaktische Konzepte**. Darüber hinaus werden konkrete, **zielgruppenspezifische Empfehlungen** formuliert, die sowohl die Ausgestaltung der Übungsformate selbst betreffen als auch die Organisation und Disseminationskanäle mit einbeziehen.

  - Die **Analyse der Disseminationskanäle** erfolgt primär im 3. Projektjahr, so dass deren Ergebnisse entsprechend in die Handlungsempfehlungen eingeflochten werden.

  - **Instrumente:** Literatur- und ggf. Online-Recherche, Best Practices, Heuristik

Anmerkung: Zwischen den einzelnen Deliverables können keine scharfen Trennlinien gezogen werden. Vielmehr gestalten sich die Übergänge fließend, da sich immer wieder Fortführungen und Rückkopplungen im Hinblick auf die zu erfüllenden Deliverables als notwendig erweisen. Dies ist zum einen darauf zurückzuführen, dass das AP der FH OÖ ein übergreifendes, alle Projektabschnitte betreffendes ist. Zum anderen liegt der Grund darin, dass aufgrund der Covid-19-Pandemie und der damit verbundenen Beschränkungen über lange Zeit keine Präsenz-Veranstaltungen, Teilnehmer*innen-Befragungen, Vorort-Beobachtungen und Untersuchungen von aktuellen Cyberübungen nur mit starken Verzögerungen durchgeführt werden können.

4.8 State of the Art

Im Sinne des Projektplanes wurde die Vorgabe für den ersten Meilenstein erfüllt. Dieser umfasst den Abschluss der State-of-the-Art-Analyse inklusive einer ersten Analyse von Cyberübungen im Hinblick auf Diversitäts-Dimensionen sowie der Vorstellung erster Maßnahmen im Konsortium. (vgl. AIT, 2020, S. 29, 33f.).

4.8.1 Cybersecurity und Diversity

Die digitale Transformation bringt gesamtgesellschaftliche Veränderungen und Herausforderungen mit sich, auf die Wirtschaft, Wissenschaft und Politik gleichsam reagieren müssen. Diese Herausforderungen wachsen, denn mit zunehmender Vernetzung steigt auch die Gefahr der „digitalen Ungleichheit“ (Reidl et al., 2020, S. 6), weil Teilnahme- und Gestaltungsmöglichkeiten sowie das Nutzungsverhalten nicht gleich verteilt sind. So verweist die Europäische Kommission darauf, dass trotz eines verstärkten Bewusstseins bisher eine umfassende Inklusion von Frauen im IKT-Sektor

noch nicht realisiert wurde und Frauen in diesem Bereich unterrepräsentiert sind, insbesondere in Entscheidungspositionen. Um langfristiges Wachstum und ökonomische Nachhaltigkeit in Europa zu ermöglichen und aufrecht zu erhalten, ist daher insbesondere die aktive Teilnahme von Frauen im IKT-Sektor unerlässlich (European Commission, 2013, S. 10). Untersuchungen (Bath, 2009; Reidl et al., S. 2020) zeigen zudem, dass die Bedürfnisse und Erfahrungen großer Bevölkerungsteile in der Entwicklung digitaler Produkte nicht berücksichtigt werden, weil unbewusst die Vorstellungen und Werte derjenigen, die solche Technologien entwickeln, in diese mit eingeschrieben werden. Um Digitalisierung erfolgreich zu gestalten, ist es daher unablässig, die potenziellen Nutzer*innen und Anwender*innen mit in den Blick zu nehmen, ihre Vielfältigkeit zu berücksichtigen und gemeinsam mit ihnen der Reproduktion von bestehenden Ungleichheiten und stereotypen Vorstellungen entgegenzutreten.

Die immer stärker erforderliche kompetente Nutzung digitaler Systeme sowohl im privaten als auch im beruflichen Umfeld rückt Cybersecurity als Schlüsselkompetenz immer mehr in den Mittelpunkt. Eine Methode, um Cybersicherheitskompetenzen zu vermitteln, sind digitale Spiele, denn Spielen ist eine weitverbreitete Aktivität, unabhängig von Geschlecht, Ethnie, Alter oder sozialem Status (Duggan, 2015, S. 6-7). Zudem kann Spiel-basiertes Lernen Spielende effektiv für neue Themenbereiche interessieren und sie darin einführen (Ketelhut, 2007, S. 108). Insbesondere spielerische Events wie Hackathons und Capture-the-Flag-Veranstaltungen sollen Interesse für das Thema Cybersicherheit wecken. Allerdings zeigt sich, dass solche Veranstaltungen Schwierigkeiten haben, Personen zu erreichen, die nicht den aktuellen Cybersicherheitsarbeitskräften entsprechen (Tobey et al., 2014, S. 56). Auch die Erfahrung des INDUCE-Konsortiums bestätigt, dass insbesondere Frauen nur im einstelligen Prozentbereich an Cyberübungen teilnehmen. Untersuchungen zur Repräsentation von Geschlecht und Ethnie in Cybersicherheitsspielen (Coenraad et al., 2020, S. 601) zeigen zudem, dass die Darstellung von Cybersicherheitsexpert*innen zum großen Teil die aktuelle Demographie und Stereotype der Cybersicherheitsarbeitskräfte als weiß und Männer-dominiert verstärken. Hier kann eine stärkere Präsenz und Wahrnehmung von Frauen und anderen unterrepräsentierten Gruppen deren Partizipation im Cybersecurity-Feld steigern (Coenraad et al., 2020, S. 605). Ein potenzielles Instrument, um eine stärkere Beschäftigung bisher unterrepräsentierter Gruppen in diesem Feld zu erreichen, ist zudem die Wahl der Repräsentation im Spiel. Untersuchungen (Birk et al., 2016, S. 2991) zeigen, dass die Möglichkeit, Avatare zu kreieren, die zur Identität der Spielenden passen, die intrinsische Motivation zum Spielen deutlich erhöhen. Eine dritte Möglichkeit, eine vielfältigere Gruppe anzusprechen, bietet die Betonung der bisher durch die starke Fokussierung der technischen Aspekte vernachlässigten sozioökonomischen Dimensionen des Cybersecurity-Feldes (Corneliussen, 2020, S. 1).

Das Projekt INDUCE (Cybersecurity Literacy And Dexterity through Cyber Exercises) (AIT, 2020, S. 1) zielt darauf, Cyberübungen als Instrument zur Vermittlung von Cybersicherheitskompetenzen einer breiteren Zielgruppe zu öffnen, um den bislang stark eingeschränkten Teilnehmer*innenkreis zu erweitern. Um dies zu erreichen, werden aktuell angebotene Cyberübungen des Konsortiums im Hinblick auf Diversitätsdimensionen und Chancengerechtigkeit[24] bewertet. Dabei kommt dem HEAD Wheel (Gaisch & Aichinger, 2016; Gaisch et al., 2019) als Sensibilisierungs- und Analyseinstrument eine entscheidende Rolle zu. Aufgrund seiner Struktur und Intersektionalität eröffnet es Akteur*innen unterschiedliche Zugänge über verschiedene Segmente, um, ausgehend von dieser Position, Sensitivität für weitere diversitätsrelevante Themen zu entwickeln. Zusätzlich werden bereits beschriebene Analysekategorien für digitale beziehungsweise Cybersecurity-Spiele (Clark et al., 2016, S. 95-98; Coenraad et al., 2020, S. 592) und Aspekte für informatische Artefakte (Bath

[24] „Equal opportunity: the absence of barriers to economic, political and social participation on the ground of sex. Such barriers are often indirect, difficult to discern and caused by structural phenomena and social represenations which have proved particularly resistant to change. Equal opportunities […] is founded on the rationale that a whole range of actions are necessary to redress deep-seated sex and gender-based inequities […]", European Commission, 2013, S.8.

2009, S. 301) herangezogen und nach Bedarf adaptiert, um die Cyberübungen zu evaluieren. Mithilfe von Fokusgruppeninterviews und Stakeholder*innenanalysen werden die Bedürfnisse potenzieller Zielgruppen ermittelt und mit den bestehenden Formaten verglichen. Die State-of-the-Art- und Zielgruppenanalyse wird durch eine entsprechende wissenschaftliche Literaturrecherche ergänzt und unterstützt. Auf Basis dieser Evaluation und Analyse werden Maßnahmen und Handlungsempfehlungen entwickelt, um die bestehenden Cyberübungen zu erweitern, umzugestalten oder neue Übungen zu entwerfen. Die erarbeiteten Konzepte, Methoden und Werkzeuge werden anschließend mit potenziellen neuen Zielgruppen in Future Labs getestet. Um das Feld der aktuellen Nutzer*innen zu erweitern und bisher unterrepräsentierte Gruppen zu adressieren, werden zudem bisherige Marketing- und Disseminationsstrategien evaluiert und adaptiert (AIT, 2020, S. 33f., 36f.).

4.8.2 Aktuelle Übungen des Konsortiums (Übersicht)

4.8.2.1 Austria Cybersecurity Challenge (ACSC)

Die Cybersecurity Austria (CSA)[25] ist Inhaberin und Herausgeberin des IT Security Hub und bietet die „Hacking"-Wettbewerbe ACSC (Austria Cybersecurity Challenge), ECSC (European Cybersecurity Challenge) sowie den openECSC. Die CSA wird in der Durchführung des Wettbewerbs vom Bundesheer und anderen Behörden unterstützt. Ziel der Veranstaltung ist das Bewusstsein für IT-Security zu schärfen, IT-Security-Talente zu entdecken und zu fördern, sowie das Thema Cyber-Security in den Schulen und der Gesellschaft zu verankern. Herausragende Schulen, Fachhochschulen oder Universitäten werden im Rahmen dieser Veranstaltung prämiert. Dabei wird auch ein besonderer Fokus auf die Sensibilisierung und Ausbildung von Lehrenden gelegt, um durch diese Multiplikator*innen auch mehr Schüler*innen anzusprechen.

Die aktuell angesprochenen Zielgruppen sind primär talentierte Lehrlinge, Schüler und Studenten [sic!][26] mit Interessenschwerpunkt Cybersecurity. Neben Ausbildungsstätten wie HTLs, AHS mit Informatikschwerpunkten, FHs und Universitäten werden in der offenen Klasse auch Behörden, Unternehmen sowie alle Security-interessierten Vertreter*innen der Gesellschaft angesprochen. Eine spezielle Zielgruppe stellt die Medienlandschaft als Kommunikationsmultiplikatorin dar. Die Ansprache der Zielgruppen erfolgt über aktive Pressearbeit, Einladungen, Promoter*innen, Aktivierung ehemaliger Teilnehmer*innen, Social-Media-Kanäle sowie durch Mailing via Bundesministerium für Bildung, Wissenschaft und Forschung.

Der Zugang zu den Übungen ist grundsätzlich frei und kostenlos, erfordert jedoch eine Anmeldung auf der online Plattform „HackingLab", über die sowohl die Qualifikation als auch die Finale der einzelnen Bewerbe abgewickelt werden. Schulklassen können zudem durch ihre Lehrkräfte angemeldet werden.

Die Plattform bietet drei Cyberübungsstufen, „Beginner", „Advanced" und „Expert", an. Die Trainings- und Ausbildungsübungen können ohne spezielle Vorkenntnisse absolviert werden. Die dritte Stufe umfasst die Qualifikationsphase für die Austria Cybersecurity Challenge und erfordert vertiefte Kenntnisse und Fähigkeiten unter anderem aus den Bereichen Netzwerk, Programmierung, Verschlüsselung und Datenbanken. Die Aufgaben unterschiedlicher Schwierigkeitsgrade stammen aus den Bereichen WebSecurity, Kryptographie oder Handy-Sicherheit und können über einen Zeitraum von zwei bis drei Wochen bearbeitet werden. Die zehn besten 5er oder 2er-Teams qualifizieren sich für das Finale, das sich über vier Tage erstreckt und während der IKT-Sicherheitskonferenz stattfindet. Die Qualifikationsphase erfolgt im Einzelspieler*innenmodus und verwendet

[25] https://www.cybersecurityaustria.at, letzter Aufruf: 29.11.2024.
[26] https://verbotengut.at/anmeldung, letzter Aufruf: 29.11.2024.

ausschließlich den Spieltyp Jeopardy, die Final-Bewerbe im Teammodus umfassen zusätzlich Attack&Defense (CTF) und Hackingbox (virtueller Escape Room). Teilnehmer*innen des ACSC werden neben ihren Lehrkräften im Rahmen des Center of Excellence zusätzlich durch Mentor*innen betreut.

Die CSA attestiert, dass der Frauenanteil bei diesen Veranstaltungen sehr gering ist und nur bei etwa 4-6% liegt und verweist auf die skandinavischen Länder Norwegen und Schweden, die bei solchen Veranstaltungen Frauenanteile von über 10% verzeichnen. Daraus ergibt sich das Problem, dass teilnehmende Frauen nur wahrgenommen werden, weil sie weiblich sind und nicht, weil sie gute Leistungen bringen. Im Rahmen des INDUCE Projektes sollen die Wettbewerbe diversitätssensibel gestaltet und angepasste Kommunikationsmittel entwickelt werden, die insbesondere Mädchen und junge Frauen ansprechen und zur Teilnahme an Cyberwettbewerben motivieren.

4.8.2.2 INFRAPROTECT® Planspiele

INFRAPROTECT®[27] hält verschiedene Übungstypen vor, die darauf ausgerichtet sind, Handlungswissen, technisches Wissen oder individuelle Fähigkeiten auszubilden oder zu verbessern. Die Übungstypen umfassen dabei Funktionstests, Kommunikationsübungen (sowohl technisch als auch organisatorisch ausgerichtet), Plan Reviews, Planbesprechungen (vom Basistraining bis zum Erlernen individueller Fähig- und Fertigkeiten), Stabsübungen (als Situationstraining ohne Stressfaktoren), Stabsrahmenübungen (als Krisenmanagementübungen, unter Stress, sowohl angekündigt als auch unangekündigt), Krisenkommunikationsübungen und Vollübungen.

Aktuell werden folgende Zielgruppen adressiert: Führungskräfte auf der Managementebene (Störung-, Notfall- und Krisenmanagement), IT-Fachpersonal (CISO, ISMS, Administrator*innen, Content-Team-Leader*innen, Ingenieur*innen), Jurist*innen, Corporate Communication und Behördenvertreter*innen. Die Zielgruppenansprache erfolgt zum überwiegenden Teil durch Kund*innenempfehlungen, daneben wird das Übungsangebot über die Homepage sowie den vierteljährlichen Newsletter verbreitet.

Die Übungen werden ausschließlich im Auftrag der Kund*innen abgewickelt. Die Teilnehmer*innen werden dazu in Abstimmung und auf Vorschlag von INFRAPROTECT® vor dem Hintergrund des Übungszieles ausgewählt. Dadurch ist der Zugang zu den Übungen nur im Rahmen des Dienstes möglich.

Ziel und Übungszweck werden gemäß dem INFRAPROTECT® Reifegradmodell im Vorfeld abgestimmt. Das Modell gliedert die Vorkenntnisse anhand von technischen, prozessualen und individuellen Basiskriterien, die je nach Übungsziel, Übungszweck und Übungskomplexität stark variieren können. In jeder Übungstype befinden sich Mitarbeiter*innen von INFRAPROTECT® in der Übungsleitung, mitunter auch als Übungsbeobachter*innen vor Ort.

Hauptziel der Übungen ist das Erleben einer „Realsituation“ und die Erarbeitung und Optimierung der vordefinierten Handlungsabläufe zur Ereignisbewältigung. Dazu soll der Umgang mit der relevanten Technik trainiert, organisationale Abläufe einstudiert und die handelnden Personen mit den notwendigen Fähigkeiten ausgerüstet werden, um auf Krisensituationen angemessen reagieren zu können. Es werden daher sowohl technische Aspekte als auch Managementskills vermittelt und eingeübt. Die meist drei-phasigen Übungen bieten den Teilnehmer*innen Situationsbeschreibungen, anhand derer sie sich entlang von vordefinierten Handlungsabläufen iterativ und interdisziplinär einer „Lösung“ und Bewältigung der Situation nähern müssen. Für alle Übungstypen werden Drehbücher mit kurzen Situationsdarstellungen erarbeitet, die von den Teilnehmer*innen interpretiert und daraus Handlungsoptionen abgeleitet werden müssen. Primär werden die Reaktionen auf die verschiedensten Bedrohungen eingeübt und vorbereitet. Die Grundstruktur der Übungen bilden

[27] https://infraprotect.com, letzter Aufruf: 16.03.2022.

Szenarien, welche die Vertraulichkeit, Integrität oder Verfügbarkeit der IT-Systeme kompromittieren.

INFRAPROTECT® verweist darauf, dass der Frauenanteil je nach Übung und teilnehmenden Unternehmen variiert. Beispielsweise liegt der Frauenanteil bei juristischen Aspekten bei 50% oder darüber. Im Rahmen des INDUCE Projektes sollen neue Formate (wie z.B. Self-Assessment-Tests) und Methoden (z.B. Gamification) entwickelt werden, die neben den aktuell angesprochenen Unternehmen insbesondere klein- und mittelständische Unternehmen (KMUs) ansprechen, aber auch gezielt Frauen und auch ältere Personen adressieren.

4.8.2.3 KSÖ Planspiele

Das Kompetenzzentrum Sicheres Österreich[28] bietet Planspiele, die jedes Jahr unter einem neuen Schwerpunktthema und Szenario stehen und sich an Mitarbeiter*innen aus den Bereichen der kritischen Infrastruktur, Wirtschaft, Behörden, Medien oder Wissenschaft richten. Die Planspiele thematisieren dabei gesamtgesellschaftliche Cyberbedrohungsszenarien wie z.B. Ausfall des Internets in ganz Österreich, Datendiebstahl, Cybererpressung in Unternehmen der kritischen Infrastruktur, Terrorbedrohung, Erprobung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) oder Angriffe auf ein Pharmaunternehmen mit Schlüsselfunktion in der Bekämpfung der Pandemie.

Über die letzten Jahre ist dabei eine stetige Zunahme der teilnehmenden Unternehmen zu verzeichnen: Waren es 2014 noch zwölf Organisationen, meldeten sich 2017 bereits 32 Organisationen für diese Übungen an. Die Szenarien der Übungen folgen stets einem übergreifenden Thema. So wurde 2012 ein Internetkollaps fingiert, 2014 lag der Schwerpunkt des Szenarios bei den Themen Datendiebstahl, Cybererpressung und terroristische Gegner*innen, 2016 wurde das Planspiel auf die Erprobung der EU-Richtlinie zur NIS ausgerichtet und 2017, zur Zeit der EU-Ratspräsidentschaft Österreichs, war das Szenario eine Terrorbedrohung kritischer Infrastrukturen.

Ziel der Planspiele ist die Bewältigung realistischer Probleme. Dazu werden den Teilnehmer*innen komplexe Fragestellungen gestellt, die sie unter Zeitdruck gemeinsam und koordiniert, unter Einbeziehung verschiedener Organisationsebenen, erfüllen müssen. Im Fokus dieser Übungen steht dabei die Praxistauglichkeit des Trainings, die Bewusstseinsschärfung, sowie das Einstudieren von Handlungsabläufen.

In der Durchführung der Übungen greift das KSÖ auf bestehende Formate, wie sie z.B. das AIT anbietet, zurück.

Das Kompetenzzentrum Sicheres Österreich bemerkt, dass Frauen in den angebotenen Planspielen unterrepräsentiert sind und verweist darauf, dass diese, oft als Einzelunternehmerinnen tätig, nicht genug informiert sind. Aus diesem Grund zielt das KSÖ im Rahmen des INDUCE Projektes auf die Erweiterung der bisherigen Zielgruppe in Richtung Klein- und Kleinstunternehmerinnen, indem, auch über neu zu erschließende Kanäle (wie die INDUCE Innovationsplattform), neue, handlungsorientierte Formate (wie z.B. Sensibilisierungs- und Praxisworkshops) angeboten werden, die, unter Verwendung diversitätssensibler Methoden, auch Personen mit (unter)durchschnittlichen technischen Skills ansprechen und schulen.

[28] https://kompetenzzentrum-sicheres-oesterreich.at, letzter Aufruf: 13.06.2024.

4.8.2.4 AIT Cyber Range Planspiele

Das AIT (AIT Austrian Institute of Technology GmbH)[29] bietet eine virtuelle Umgebung (Cyber Range[30]), um kritische Infrastrukturen zu simulieren. In dieser sicheren Umgebung können verschiedene Testformate durchgeführt werden, die entweder den strategischen oder den technischen Umgang mit kritischen Situationen im Bereich Cybersicherheit fokussieren und von der Bewusstseinsbildung bis hin zu spezifischen Maßnahmen im Fall einer Bedrohung reichen.

Technische Übungen sind kollaborative Übungen mit unterschiedlichen Aufgabenstellungen und unterschiedlichen Schwierigkeitsgraden. Sie zielen auf die Erkennung von und die Reaktion auf Cyberangriffe und trainieren in diesem Zusammenhang den Umgang mit der notwendigen Technik, den Werkzeugen und der Infrastruktur. Die vermittelten Praktiken umfassen aktive und passive Verteidigungsmaßnahmen sowie pre- und post mortem-Analysen. Dies wird mit einer virtuellen Infrastruktur erreicht, die stark auf kollaborative Zusammenarbeit setzt. Weiter können die Prozesse des Krisen- und Notfallmanagements sowie die Incident-Response-Prozesse geübt und evaluiert werden. Übungen dieser Art adressieren insbesondere Personal aus den Bereichen IT, SOC und NOC, CIO, CISO, dem Incident Response Team sowie dem Krisen- und Notfall-Management.

Strategische Übungen wiederum fokussieren die Herausforderung, bestimmte Szenarien zu bewältigen, von der Entscheidungsfindung, über die Kommunikation bis zum Management, oder die Erprobung von Strukturen und Prozessen. Hierfür werden neben allgemeinem Personal insbesondere Mitarbeiter*innen aus der Managementebene sowie dem IT- und Sicherheitspersonal angesprochen. Die Thematik Cybersicherheit wird in strategischen Übungen mittels eines holistischen Blicks vermittelt. Die Teilnehmer*innen sollen ihr Wissen aus den unterschiedlichen Disziplinen einbringen, um Lösungsansätze zu generieren. Meist werden diese Übungen als interaktives kollaboratives Quiz durchgeführt, mit dezidierten Aufgabenstellungen und Prozessen. Im Vordergrund dieses Übungstyps steht die Bewusstseinsbildung für die Herausforderungen der IT und der Cybersicherheit sowie die sichere Durchführung von Prozessen.

Die Übungen gliedern sich in die Abschnitte der Vorbereitung, Planung, Durchführung und Evaluierung und zielen in der Ausgestaltung der unterschiedlichen Angriffsszenarien stets auf den Lerneffekt der Teilnehmenden ab. Diese werden in Absprache und unter Einbeziehung des*der Auftraggebers*in entwickelt, um die Szenarien den jeweiligen Gegebenheiten anzupassen. Während der Durchführung stehen Mitarbeiter*innen des AIT den Teilnehmer*innen zur Verfügung, um Unterstützung anzubieten oder Hilfestellungen zu geben.

Der Zugang zu den Übungen erfolgt entweder über das auftraggebende Unternehmen oder im Rahmen eines Konferenzvortrages, bei dem die Konferenzteilnehmer*innen je nach Platzverfügbarkeit teilnehmen können. Die aktuelle Ansprache der Zielgruppen erfolgt über die Cyber Range- und AIT-Webseite, Publikationen, Consulting, nationale und internationale Projekte sowie über die Arbeitgeber*innen.

Die Cyber Range versteht sich als Bildungsangebot sowohl für Lehrende als auch für Lernende, um die Aus- und Weiterbildung im Cybersecurity-Bereich zu fördern, das Bewusstsein für die Thematik zu erhöhen, sowie die individuellen Fähigkeiten zu verbessern. Das Angebot des AIT adressiert grundsätzlich alle Mitarbeiter*innen eines Unternehmens, verzeichnet allerdings in unternehmensbezogenen Übungen einen Frauenanteil von weniger als 10%, oft nehmen keine Frauen teil. Eine Abhilfe dieses Umstandes verspricht man sich durch die Einbeziehung von Diversitätsaspekten (z.B. in der Ausrichtung auf neue Zielgruppen, veränderte Kommunikation, aber auch in der Neugestaltung insbesondere der technischen Übungen) im Rahmen des INDUCE Projektes.

[29] https://www.ait.ac.at, letzter Aufruf: 13.06.2024.
[30] https://cyberrange.at/, letzter Aufruf: 21.06.2024

4.9 Analyse der Übungen

Die Analyse der Cyberübungen konzentriert sich auf zwei Schwerpunkte:

- **Ansprache und Kommunikation** im Vorfeld der Cyberübung (Werbung): Wird die angedachte Zielgruppe sprachlich und grafisch angesprochen und dargestellt?

Innerhalb des ersten Projektjahres ergehen von Seiten der FH OÖ mehrere Sensibilisierungworkshops, die sich mit den Themen Zielgruppenansprache und Kommunikation beschäftigen (siehe Kapitel 4.10). Zusätzlich bietet die FH OÖ konkrete Hilfestellung bei Fragen bezüglich der Gestaltung aktueller Internetauftritte oder Veranstaltungsposter (bspw. für den Hacking-Event ACSC). Im weiteren Projektverlauf ewerden durch eine Erweiterung oder Adaptierung der Marketing- und Disseminationsstrategie, auch unter Verwendung neuer Kommunikationskanäle, gezielt bisher unterrepräsentierte Gruppen adressiert (AIT, 2020, S. 34).

- **Gestaltung** der Cyberübungen: Lassen sich in der technischen/ grafischen/ sprachlichen Gestaltung der Cyberübungen Hinweise auf I-Methodology/ eingeschriebene Stereotype/ algorithmische Verzerrungen finden, die zur Vergeschlechtlichung oder Ungleichheit der Produkte führen?

Der Begriff „**I-Methodology**“ verweist auf das Phänomen, dass bereits während des Entwicklungsprozesses unbewusst Ungleichheit beziehungsweise eine Vergeschlechtlichung digitaler Produkte erzeugt wird. Dies geschieht, wenn Technikgestalter*innen ihre eigenen Kompetenzen, Interessen und Nutzungsweisen als repräsentativ für alle Nutzer*innen halten und eigene Erfahrungen, Werte und Vorstellungen unbewusst in das Produkt mit einfließen lassen. Dadurch werden nur bestimmte Bedürfnisse berücksichtigt, andere Lebensperspektiven, Interessen und Fähigkeiten dagegen werden nicht wahrgenommen. Das Erscheinungsbild und die Funktionsweise der Technologie wird so insbesondere durch homogene Entwicklungsteams einseitig beeinflusst und kann zur erschwerten oder eingeschränkten Verwendung sowie zum Ausschluss von der Technologie aufgrund von Geschlecht, Alter, Herkunft, anderen Kompetenzen und Präferenzen oder anderen Lebensumständen führen. Werden unbewusst getroffene Vorannahmen nicht hinterfragt, kann dies zur Fortschreibung bestehender Ungleichheiten führen. Insbesondere **stereotype Vorstellungen** und Rollenbilder müssen in diesem Zusammenhang aufgedeckt werden, da diese nicht nur in die Technologieentwicklung mit eingehen, sondern, durch deren **Einschreibung in die Algorithmen**, bestehende Ungleichheiten zusätzlich verstärken und/oder zur Verzerrung der Daten führen. (vgl. Bath, 2009; Reidl et al., 2020)

Für die Analyse der Cyberübungen werden daher bereits beschriebene Kategorien (Clark et al., 2016, S. 95-98; Coenraad et al., 2020, S. 592) herangezogen und entsprechend den Fragestellungen von INDUCE im Laufe des Projektes angepasst, erweitert und verfeinert. Die Analyse erfolgt auf Basis schriftlicher Beschreibung und Vorführung der Übungen von Seiten der Projektpartner*innen sowie den Interviewergebnissen (s. Kapitel 4.10). Mit Hilfe dieser Analyse werden im nächsten Projektabschnitt Hürden und Hemmnisse in der Ansprache und Gestaltung identifiziert, die es potenziellen Nutzer*innen erschweren, die Übungen zu nutzen. Zudem werden Maßnahmen und Handlungsempfehlungen formuliert sowie Methoden vorgestellt, um die vorhandenen Übungen zu erweitern, anzupassen oder neue Übungen zu erstellen, so dass die anvisierten Zielgruppen erreicht und angesprochen werden und die gewünschten Lerneffekte erzielt werden können.

Die Analysekategorien gestalten sich wie folgt:

Basisinformationen:

- Spielname
- Link und Quelle
- Organisation/ Hersteller*in/ Besitzer*in

- Publikationsdatum
- Kosten
- Zielgruppe
- Spieldauer
- Anzahl der Sitzungen

Organisatorische Vorbereitung:

- Aktuell angesprochene Zielgruppe
- Aktuelle Ansprache der ZG (Werbung, Newsletter, Netzwerke)
- Zugang zur Übung (frei verfügbar, Anmeldung über Arbeitgeber*in, kostenpflichtige Anmeldung)
- Anbietende Plattform (mobil, Internet, PC)

Motivation

- Storybedingte Motivation
- Wettbewerb
- Kompetenzerwerb
- Unterhaltung
- Übung

Durchführung:

- Benötigte Vorkenntnisse
- Unterstützung durch Supporter*innen/ Trainer*innen/ Mentor*innen
- Technische Voraussetzungen
- Einzel- oder Teamteilnahme

Didaktischer/ Cybersecurity Inhalt:

- Lernziele: welche technischen/ praktischen Fähigkeiten werden erlernt?
- Lernziele: welche Kenntnisse über CS werden vermittelt?
- Spieltyp
- Variation der Spielaktionen

Spieler*innen/ Charaktere

- Spieler*innen-Rolle
- Geschlecht/ Ethnie/ Alter der Charaktere
- Rolle von Frauen, ethnischen Minderheiten, älteren Personen
- Anthropomorphismen
- Einsatz von APAs? (Animated pedagogical Agents)
- Einsatz von diversitätssensibler Sprache?

Organisatorische Nachbearbeitung/ Evaluation:

- Gibt es begleitende Programme, welche die Community stärken, vergrößern, Kontinuität sicherstellen?
- Stärken/ Schwächen des Angebots, gute Erfahrungen?
- Erweiterungspotential dieser Übung?
- Feedbackmöglichkeiten von Spieler*innen an Anbieter*innen?
- Messung des inhaltlichen und praktischen Lernerfolges?

4.10 Methodik der Zielgruppenanalyse

Die **State-of-the-Art-Zielgruppenanalyse** erfolgt in mehreren Schritten. Zunächst ergehen einige Sensibilisierungsworkshops, in denen, basierend auf bereits existierenden Studienergebnissen (Berg, 2020; Gaisch & Kerschbaumer, 2019; Gaisch & Rammer, 2018; Reidl et al., 2020; Seyda & Flake, 2019; Seifert & Schelling, 2015), **verschiedene Aspekte von Gleichstellung und Diversity** vorgestellt werden. In diesen Treffen wird das Problem behandelt, warum in der Informatik Frauen meist unterrepräsentiert sind. Hinderungsgründe wie stereotypes Denken, sozialisierte Rollenbilder oder fehlende Informationen werden dargestellt. Ebenso werden Erfolgsfaktoren, die hier entgegenwirken und die Informatik auch für Frauen attraktiver machen können, präsentiert. Dazu gehört zum Beispiel eine Imagekorrektur, welche die Breite der Möglichkeiten in der IT verdeutlicht, die Betonung der gesellschaftlichen, internationalen, interkulturellen und interdisziplinären Relevanz, ihre Anwendungsorientierung sowie Gestaltungsmöglichkeit. Es wird deutlich, dass weibliche Rollenvorbilder nötig sind, um Frauen in der Informatik mehr mediale Präsenz zu verleihen. Informelle Netzwerke können hier zusätzlich niedrigschwellig schnelle Kontaktaufnahmen ermöglichen.

Eine weitere **Sensibilisierung** erfolgt im Hinblick auf **gender- und diversitätssensible Versprachlichung** und Kontextualisierung sowie eine entsprechende **Zielgruppenansprache**. Gezeigt wird, wie potenzielle neue Zielgruppen durch Einbindung derselben in Wort, Bild und Schrift angesprochen, gefunden und interessiert werden. Weitere Diversitätsaspekte kommen in der Thematisierung von **Rassismus/Sexismus und Exklusion** zum Ausdruck. Hier erfolgen beispielhaft Hinweise darauf, wie unreflektierte Datensätze (ungewollt) Stereotype reproduzieren und rassistische Zuordnungen ermöglichen, selbstfahrende Autos Rollstuhlfahrer*innen nicht erkennen, Spracherkennungssoftware keine Frauenstimmen oder Antischummelsoftware keine schwarzen Studierenden erkennt, oder dass Mediennutzer*innen mit Lernschwierigkeiten von digitaler Exklusion betroffen sind. Auch die Generation 65+ ist vermehrt digital unterwegs und wünscht sich mehr Schutz und Hilfsangebote.

Eine erste **Analyse von Diversitätsdimensionen im Hinblick auf mögliche Zielgruppen** greift die Überlegung auf, ob anhand von polizeilichen Kriminalitätsstatistiken (Kriminalitätsbericht, 2019; Polizeiliche Kriminalstatistik, 2021) und Cybercrime-Lageberichten (Cybercrime Report, 2019; Cybercrime Bundeslagebild, 2019) Opfergruppierungen bezüglich Alter und Geschlecht möglich sind und welche Delikte dabei im Vordergrund stehen, um eventuell gezielt bestimmte Gruppen vor bestimmten Delikten zu schützen. Der Ansatz verdeutlicht die Handlungsnotwendigkeit, Cybersicherheitskompetenzen breiter in der Bevölkerung zu verankern, da ein kontinuierlicher Anstieg von Cybercrime-Delikten zu verzeichnen ist (Cybercrime Report, 2019, S. 14). Allerdings verweisen Kriminalitätsstatistiken darauf, dass gerade im Bereich der Internetkriminalität die Dunkelziffer besonders hoch ist (Cybercrime Report, 2019, S. 17). Dies und die fehlende Opferstatistik erschwert die Zuordnung von möglichen Opfergruppen auf bestimmte Cybercrime-Delikte.

Basierend auf einer **Table-Top-Recherche** erfolgt ein Überblick über die angebotenen Cyberübungen der Projektpartner*innen, deren Zielgruppen und Trainingsmethoden (siehe Kapitel 4.9). Diese zeigt, dass die vorhandenen Cyberübungen primär Akteur*innen in Behörden, Unternehmen sowie in der kritischen Infrastruktur adressieren. **Cybersecurity als „gesamtgesellschaftliche Herausforderung“** (Cybercrime Bundeslagebild, 2020, S. 54) allerdings wird dadurch nicht abgebildet. Alternative Angebote, die sich an die Zivilgesellschaft richten, existieren zwar, greifen zum Zweck der Wissensvermittlung und Befähigung allerdings nicht auf das Instrument der Cyberübungen zurück. Es wird deutlich, dass es mehrerer Kanäle bedarf, um über Risiken, Gefahren und Gegenmaßnahmen aufzuklären und entsprechende Kompetenzen zu vermitteln. Die Heterogenität der möglichen Zielgruppen lässt dabei keine Einheitslösung zu. Passgenaue Regelungen und Lösungsansätze zur Verbesserung der Informationssicherheit sind erforderlich. Das Konsortium kommt zu dem Schluss, dass der opferzentrierte Ansatz im vorliegenden Zusammenhang nicht

zielführend ist. Die Zuordnung von Opfergruppierungen und Cybercrime-Delikten ist nur schwierig zu realisieren, da beispielsweise für Österreich eine gezielte Opferabfrage beim Bundeskriminalamt nötig ist. Zudem ist die Aussagekraft einer solchen Abfrage aufgrund der hohen Dunkelziffer von Cybercrime-Delikten zweifelhaft. Sollten dennoch Schwachpunkte bestimmter Gruppen herausgefunden werden, wird die Gefahr der Stigmatisierung von den Projektpartner*innen als hoch eingeschätzt. Aus diesen Gründen wird der opferzentrierte Ansatz nicht weiterverfolgt.

Das Ergebnis der State-of-the-Art-Analyse bestätigt die geringe Teilnahmerate von Frauen an Cyberübungen und kann auf die fehlende Adressierung, Ansprache und Berücksichtigung dieser Zielgruppe und deren Bedürfnisse zurückgeführt werden. Infolgedessen richtet sich der Fokus darauf, Möglichkeiten auszuloten, neue Zielgruppen, insbesondere weibliche, zu erschließen.

Von Seiten der FH OÖ ergeht der Vorschlag, **„Frauen in allen Lebenslagen“** als übergeordnete neue Zielgruppen zu avisieren, da dieser Titel sowohl die angestrebten diversitätssensiblen Aspekte Geschlecht, Alter (Mädchen, junge Frauen, Wiedereinsteigerinnen, Seniorinnen) und soziale Herkunft (Migrationshintergrund, bildungsferne Schichten, Cybersecurity ferne Berufe…) umgreift, als auch die kognitive und fachliche Diversität abdeckt. Der Vorschlag wird von den Projektpartner*innen angenommen.

Vor diesem Hintergrund erfolgt von Seiten der FH OÖ eine Zusammenfassung des aktuellen Standes und ein Ausblick auf mögliche, neu zu erschließende Zielgruppen der jeweiligen beteiligten Organisationen sowie Vorschläge, diese Zielgruppen zu erreichen. Ergänzt wird die Veranstaltung durch eine Sensibilisierung der Projektpartner*innen hinsichtlich der Ansprache dieser neuen, übergeordneten Zielgruppe. **Best-Practice-Beispiele** veranschaulichen Möglichkeiten, die sich hier bieten. Konkret geht es um Fragen, wie potenzielle neue Zielgruppen angesprochen, gefunden und interessiert werden können. Betont wird die Notwendigkeit, die Zielgruppe in ihrer jeweiligen Lebensrealität abzuholen, den persönlichen Nutzen und Mehrwert von Cybersicherheit deutlich zu machen, Ängste abzubauen, sowie ausreichend Informationen und Vernetzungsmöglichkeiten zu bieten. Wichtig sind niedrigschwellige Angebote, die auch Menschen motivieren, sich auf das Cybersecurity-Thema einzulassen, die nicht über ausgeprägte informationstechnische Kenntnisse und Fähigkeiten verfügen. Weibliche **Role Models** sowie die **sprachliche und grafische Berücksichtigung** aller Geschlechter und diverser Gruppen fördert zudem die verstärkte Wahrnehmung von Frauen in diesem Umfeld und trägt, ebenso wie die Begriffswahl, zur Motivation neuer Zielgruppen bei, sich mit Cybersecurity auseinander zu setzen.

Ergänzend wird der **Einsatz diversitätssensibler didaktischer Ansätze** (vgl. Leicht-Scholten & Schroeder, 2014) behandelt, die nicht-traditionelle Zielgruppen fokussieren. Zusätzlich wird dem Konsortium das **Forschungsdesign „Fokusgruppeninterviews“** (vgl. Mayerhofer 2009) vorgestellt, mit dessen Hilfe neue Zielgruppen erschlossen werden können. Ein 10-stufiger Leitfaden zur Orientierung wird an die Hand gegeben und stellt sich wie folgt dar:

1. Problem definieren
2. Forschungsfrage formulieren
3. Gruppe bestimmen (purpose sampling); ideal für eine qualitative Forschung sind sechs bis acht Personen; im besten Fall drei Interviews
4. Moderator*in schulen (keine Suggestivfragen, Narrativ zulassen, keine Unterbrechungen…)
5. Semi-strukturierten Leitfaden erstellen; primär offene Fragen; keine Suggestivfragen
6. Mittels Pretests anpassen (ein bis zwei Personen)
7. Erhebungsphase: Fokusgruppeninterview durchführen
8. Auswerten (z.B.: qualitative Inhaltsanalyse (Mayring, 1991); thematic analysis (Braun & Clarke, 2013))
9. Ergebnisse zusammenführen

10. Schlussfolgerungen ableiten

Die Konsortialpartner*innen werden ermutigt, die theoretischen und praktischen Handreichungen zu nutzen und ihre Vorstellungen bezüglich künftiger neuer Zielgruppen zu konkretisieren. Auf Wunsch der Beteiligten wird eine Excel-Tabelle (siehe Anhang 12.6) erstellt, um die Rahmenbedingungen der aktuell verwendeten Cyberübungen (Name der Übung, angesprochene Zielgruppe, aktuelle Ansprache, Kontext/ Setting, verwendete Methodik und Didaktik) sowie deren Adaption oder Erweiterung zu verschriftlichen.

Erweitert wird die Zielgruppenanalyse mit Hilfe von semistrukturierten qualitativen **Expert*innen- und Fokusgruppeninterviews** mit den beteiligten Projektpartner*innen. Die semistrukturierten, leitfadengestützten Interviews folgen dem Forschungsdesign von Braun & Clarke, 2013, und wurden in der Zeit vom 13. Dezember 2021 bis 18. Januar 2022 von der FH OÖ durchgeführt. Die Anzahl der befragten Personen pro Interview liegt bei eins bis drei, die Dauer der Interviews beträgt etwa eine Stunde, in einem Fall eine Stunde und 50 Minuten. Die Interviews dienen der Realisierung mehrerer Ziele. Einerseits soll der Fortschritt des Projektes intern evaluiert werden. Zudem strebt die FH OÖ an, die angebotenen Cyberübungen näher kennenzulernen, um die bisher erarbeiteten Analysekategorien für die Übungsevaluierung im nächsten Projektabschnitt zu verfeinern (siehe Kapitel 4.9) und die geplante Vorführung konkreter Übungen vorzubereiten. Drittens dienen die Interviews der konkreteren Ausgestaltung neuer Zielgruppen. Die Interviews werden entsprechend der genannten Fragestellungen kodiert und nach Braun & Clarke, 2013, mittels thematischer Analyse ausgewertet.

4.11 Ergebnis der Zielgruppenanalyse

Im bisherigen Projektverlauf lassen sich für die neu zu erschließenden Zielgruppen drei größere Gruppen identifizieren, die von den Projektpartner*innen verstärkt in den Blick genommen werden (siehe Deliverable D2.1: Kooperationsplattform und Struktur des Innovationsnetzwerkes):

- Unternehmerinnen von KMUs, Einzelunternehmerinnen (EPUs); Dienstleistung, Handwerk, PR
- Studentinnen und weibliche IT-Kräfte
- Jugendliche und junge Frauen

4.11.1 KSÖ

- **Name/ Bezeichnung der aktuellen Cyberübung**: KSÖ-Sicherheits-Planspiel
- **Aktuell angesprochene Zielgruppe(n)**: Behörden, Vertreter*innen der kritischen Infrastruktur, CERTs, Wissenschaftsvertreter*innen, Interessenvertretungen, Medienvertreter*innen
- **Zu erweiternde/ neu zu erschließender Zielgruppe(n)**: Klein- und Kleinst-Unternehmer*innen (EPUs), insbesondere aus den Bereichen Gewerbe und Handwerk, Information und Consulting, Tourismus
- **Maßnahmen zur Erschließung dieser Zielgruppen:** Überblicksrecherche zum vorhandenen Angebot im Bereich der Cybersicherheit; Vorbereitung eines niederschwelligen Awareness-Programms für Klein- und Kleinstunternehmer*innen als Fundament für Praxis-Workshops
- **Aktuelle Zielgruppenansprache:** das aktuelle Angebot (themenspezifische Webseite, Webinare und Vorträge) richtet sich an Personen, die ohnehin motiviert sind, sich mit dem Thema Cybersicherheit auseinander zu setzen. Personen mit Berührungsängsten in Bezug auf IT-Sicherheit benötigen niederschwellige und handlungsorientierte Angebote.

- **Adaptierte/ erweiterte Zielgruppenansprache:** Sensibilisierung und Aktivierung über folgende Kanäle: Newsletter der Wirtschaftskammer, insbesondere: Frau in der Wirtschaft[31], Ausschuss für Ein-Personen-Unternehmen[32], EPU-Plattform "Wir sind 1 und trotzdem ganz schön viele"[33]; KSÖ-Präsenz bei verschiedenen Veranstaltungen zwecks Erweiterung der Zielgruppen
- **Kontext/ Setting aktuelle Cyberübungen:** gesamtgesellschaftliche Cyberbedrohungsszenarien wie z.B. Ausfall des Internets in ganz Österreich, Datendiebstahl, Cybererpressung in Unternehmen der kritischen Infrastruktur, Terrorbedrohung, Erprobung der EU-Richtlinie zur Netzwerk- und Informationssicherheit, Angriff auf ein Pharmaunternehmen mit Schlüsselfunktion in der Bekämpfung der Pandemie
- **Adaptierter/ diversitäts-sensibler Kontext:** Fokus auf Cybersicherheit und Cyberrisiken in einem Klein-/Kleinstunternehmen, Berücksichtigung von (unter)durchschnittlich ausgeprägten technischen Skills der Unternehmer*innen, Sensibilisierung für die Problematik im Vorfeld der praktischen Cyberübungen
- **Methodik/ Didaktik der aktuellen Cyberübungen**: Training in einer IT-Simulationsumgebung, der „AIT Cyber Range“, mit mehreren Spieler*innengruppen
- **Adaptierte/ erweiterte Methodik/ Didaktik:** Microlearning, Storytelling, Emotionalisierung der Lerninhalte, humoristischer Ansatz, handlungsorientierte Aktivierung

4.11.2 Infraprotect

- **Name/ Bezeichnung der aktuellen Cyberübung:** Cybersecurity ANOBLACK (Stabsrahmenübung); Cyberplanspiel; Cybertrain (Planbesprechungen); Cyberplan (Ausplanungen von Cyberübungen); Cybertrue (Vollübung bis hin zu tatsächlichen Abschaltungen/Umschaltungen); Cyberworld – Atlantica (Stabsrahmenübungen über mehrere Kontinente und Zeitzonen hinweg)
- **Aktuell angesprochene Zielgruppe(n):** Führungskräfte auf Management-Ebene (Störungs-, Notfall-, Krisenmanagement), IT-Fachpersonal (CISO; ISMS; Administrator*innen, Content-Team-Leader, Ingenieur*innen); Jurist*innen, Corporate Communication, Behörden
- **Zu erweiternde/ neu zu erschließender Zielgruppe(n):** Klein- und Mittelständische Unternehmen (KMUs) aus den Bereichen Handwerk, Dienstleistung, Tourismus, Gewerbe
- **Maßnahmen zur Erschließung neuer Zielgruppen:** Vernetzung via WKO, Interviews, Awarenessschulung (Self-Assessment)
- **Aktuelle Zielgruppenansprache:** Homepage, Newsletter, Kund*innen-Empfehlung
- **Adaptierte/ erweiterte Zielgruppenansprache:** Einstieg via Fragenkatalog, Newsletter mit einfachen Tipps und Tricks, App
- **Kontext/ Setting der aktuellen Cyberübung:** Im Vordergrund steht die Vermittlung des Zusammenwirkens zwischen Technik und Mensch. Es werden in der Regel drei Phasen abgebildet, die durch Situationsbeschreibungen den Teilnehmer*innen aufbereitet werden. Die Teilnehmer*innen haben sich dann entlang von vordefinierten Handlungsabläufen iterativ und interdisziplinär einer „Lösung“ und Bewältigung der Situation zu näheren. Je nach Übungszweck kann es mehrere Iterationen geben, die Was-Wäre-Wenn Fragestellungen erlauben. Grundhaltung dabei ist, dass durch Handeln Handlungswissen und damit Erfahrungen im Spiel gesammelt werden, um besser auf Realfälle vorbereitet zu sein.
- **Adaptierter, diversitäts-sensibler Kontext**: Altersgruppe 50+ mitbedenken
- **Methodik/ Didaktik der aktuellen Cyberübungen:** gemäß NATO-Training Exercise Directive, Didaktisches Achteck; 5 Grundelemente der Erwachsenen Aus- und Fortbildung (Anschaulichkeit, Mitarbeit, Zeitgemäßheit, Vergessenssicherung, Wirklichkeitsnähe); Erfahrungswissensvermittlung

[31] https://www.wko.at/dienststelle/15342 [18.06.2024]
[32] https://www.wko.at/epu/ein-personen-unternehmen [18.06.2024]
[33] https://www.wirsind1.at/ [18.06.2024]

- **Adaptierte/ erweiterte Methodik/ Didaktik:** Gaming, geleitete Trainings, unterstützt durch entsprechende KPIs

4.11.3 AIT

- **Name/ Bezeichnung der aktuellen Cyberübung:** 1) Cyber Sicherheitsplanspiel (Technische Cyber Übung); 2) Strategische Cyber Sicherheitsplanspiele (Strategische Übung)
- **aktuell angesprochene Zielgruppe(n):** In den technischen Übungen werden vom AIT folgende Zielgruppen adressiert: IT-Personal, SOC- und NOC-Teams; Incident Response Team; CIO, CISO, Krisen- und Notfall-Management; In den strategischen Übungen werden vom AIT folgende Personengruppen hauptsächlich adressiert: Management in allen Bereichen; allgemeines Personal; IT- und Sicherheitspersonal
- **zu erweiternde/ neu zu erschließende Zielgruppe(n):** Berufstätige, Studierende, Arbeitnehmer*innen, die im IT-Umfeld aktiv sind und noch nicht über genügend IT-Sicherheitswissen verfügen; Fokus auf ZG Frauen, weil diese bisher nicht angesprochen wurden.**Maßnahmen zur Erschließung neuer Zielgruppen:**
  1. Schritt: schriftliche qualitative Umfrage via Internet-Fragebogen (Hoffnung: Kontakte zu potenziellen Interviewpartner*innen);
  2. Schritt: Interviews mit Frauen, die bereits an Übungen teilgenommen haben oder mit einer gemischten Gruppe;
  3: Intensivierung der Forschungsprojekte und stärkere Verfügbarmachung der Planspiele für eine breitere Zielgruppe;
- **aktuelle Zielgruppenansprache:** (Cyber Range und AIT) Webseite, Publikationen in den Themenbereichen Cybersicherheit, Operational Technologies und Bildung, Consulting und nationale und internationale Projekte, Vermittlung via Arbeitgeber*innen (CISO)
- **adaptierte/ erweiterte Zielgruppenansprache:** evtl. Einladung zu offenen Planspielen
- **Kontext/Setting aktuelle Cyberübung:** Bei Strategischen Übungen wird die Thematik Cybersicherheit mittels eines holistischen Bildes an die Teilnehmer*innen vermittelt. So sollen diese im Rahmen der Übung Wissen aus den unterschiedlichen Disziplinen einbringen, um Lösungsansätze zu generieren. Bei den technischen Übungen arbeiten die Teilnehmer*innen mittelbar an den Bedrohungen und sollen so ein Bewusstsein der Cybersicherheitsherausforderungen im digitalen Raum aufbauen.
- **adaptierter, diversitäts-sensibler Kontext:** Simulationen sollen variabler gestaltet und an die jeweiligen ZG angepasst werden (Umfrage: welche Szenarien "passen" zu welchen Zielgruppen?)
- **Methodik/ Didaktik aktuelle Cyberübungen**: (interaktive) Schulungen:
  - strategische Übungen: angeleitet von Moderator*in mit anschließender Gruppendiskussion
  - technische Übungen: Team erarbeitet sich selbständig die Lösungen, Spielleiter*in ist anwesend; Planspiele: Awareness-Schulung;
  - Grundlage: Didaktisches Achteck sowie Kombination unterschiedlicher Ansätze (problembasierter, Kommunikations-orientierter, Multi-Perspektiven-orientierter, Wissensbasierter, Zeitbasierter, Szenario-basierter und Problem-orientierter Ansatz; evtl. erweitert durch experimentellen und Fakten-basierten Ansatz sowie herkunftsorientierter/ kultureller Ansatz)
- **adaptierte/ erweiterte Methodik/ Didaktik:** strategische Übungen:
  (1) haben sich bewährt (Ziel: Awareness); technische Übungen
  (2): evtl. kürzen, um "Neue" nicht abzuschrecken; Unterstützung und Support sind dabei besonders wichtig

4.11.4 CSA

- **Name/ Bezeichnung der aktuellen Cyberübung:** ACSC – Austria Cybersecurity Challenge, ECSC – European Cybersecurity Challenge, openECSC

- **aktuell angesprochene Zielgruppe(n):** primär: Cybersecurity-Talente; sekundär: Wirtschaft, Ausbildungsstätten, Lehrkräfte, Medien
- **zu erweiternde/ neu zu erschließende Zielgruppe(n):** offene Klasse: Menschen, die bereits im Berufsleben stehen oder älter sind; Universitäten/ Schulen (hier insb. Lehrer*innen; neben HTLs, vor allem neuer Fokus auf AHS mit Schwerpunkt Informatik/ Firmen/ Behörden); Frauen und Mädchen
- **Maßnahmen zur Erschließung neuer Zielgruppen:** Verstärkung im Lehrer*innen-Ausbildungs-Modell; Multiplikator*innen-getrieben/ niedrigschwellige Zugänge via Quizz-Duell-App; Entwicklung einer Internet-Lösung zum Sprung Hacking Lab; Definition des NTL nationalen Trainingslagers mit Schwerpunkt Entwicklung von Zielgruppen-orientierten Trainingsinhalten/ Customer journey: Wie sehen Frauen Security?
- **aktuelle Zielgruppenansprache:** Aktive Pressearbeit; bilaterale Gespräche/Einladungen mit/ an Department-Leitung von Schulen und Hochschulen sowie mit unterstützenden Medien und Unternehmen; Aufbau dezentraler Zellen als aktive Promoter*innen in den jeweiligen Schulen/Hochschulen; Aktivierung der Teilnehmer*innen sowie der Mitglieder des Center of Excellence; Mailing via Bundesministerium für Bildung, Wissenschaft und Forschung an über 2000 Schulen in Österreich; Kommunikation der Challenge auch via IKT-Sicherheitskonferenz des BMLVS; Online-Vermarktung der Challenge via Social Media und Webauftritt der Cybersecurity Challenge. (www.verbotengut.at)
- **adaptierte/ erweiterte Zielgruppenansprache:** Mundpropaganda-Modell und Affiliate-Programm für Teilnehmer*innen und Interessierte. Die ACSC erreicht durchschnittlich rund 600 Sicherheitsinteressierte und liegt mit etwa 100 Presseclippings/ Jahr erfolgreich auf Kurs (orf.on, standard, futurzone...), auch 2-3 Fernsehclips (ZIB) und Radiobeiträge (Morgenjournal, Nachrichten Ö3) ermöglichen relativ hohe Reichweiten; der online Auftritt "verbotengut" erreicht rund 30k unique visitors, die ECSC.eu rund 90k
- **Kontext/Setting der aktuellen Cyberübung:** Es gibt keine übergeordneten „Themen“ – es gibt keine Story rund um die Bewerbe – die Aufträge für die Jeopardy-challenges ergeben sich aus ihren Aufgabenstellungen und folgen hier keinem Drehbuch, das ein aufeinander abgestimmtes oder challenge-by-challenges Konzept vorsehen würde
- **adaptierter, diversitäts-sensibler Kontext:** Challenges diversitätssensibler erstellen und andere Zielgruppen erreichen sowie die Information über die Challenges an sich zur Thematisierung/Sensibilisierung des Bereiches nutzen; Möglichkeit, auch Umfragen auf Landing Pages einzubauen, um nähere Informationen über Nutzer*innenverhalten sowie Selbsteinschätzungen abzufragen
- **Methodik/ Didaktik aktuelle Cyberübungen:** Motivation der Teilnehmer*innen ergibt sich aus dem Wunsch sich für das Finale zu qualifizieren; gewertet wird nach Punkten, je nach Aufgaben-Kategorie leicht/mittel/schwer mit 10/20/30 Punkten; additiv gibt es ein Write-Up (Beschreibung des Lösungsweges, aber auch der Prävention des durchgeführten Angriffs sind abzuliefern, um die volle Punktezahl erlangen zu können); bei Punkte-Gleichstand entscheidet der Time-Stamp - also der Zeitpunkt der eingereichten Lösung (wer war schneller); die Finale sehen ein ähnliches Scoring-Modell vor - jenes Team mit den meisten Punkten entscheidet den Bewerb für sich.
- **adaptierte/ erweiterte Methodik/ Didaktik:** Autodidakt*innen, Schulen/Hochschulen (Lehrbetrieb), CTF-Communities, Rolemodels (derzeit nur männliche), Lehrlingsausbildungsbereiche - primär via HackingLab-Plattform zu den jeweiligen Security-Schwerpunkten
- **Motivation/ Hintergrund:** Fachkräftemangel ist für Europas Wirtschaft und Gesellschaften zum spürbaren Problem geworden – dies gilt ins besonders auch für IKT-Sicherheitsfachkräfte. Eine Reihe nationaler Bewerbe versucht dieser Entwicklung mit der Durchführung lokaler Challenges konkrete Maßnahmen entgegenzusetzen

5 Aktuelle und potentielle Zielgruppen für Cyberübungen

5.1 Einleitung

Ziel 1: Entwicklung von diversitätssensiblen Cyberszenarien und Technologien in CÜ:

Gefordert wird die Untersuchung der Gestaltung und Umsetzung von Cyberübungen (CÜ). Insbesondere werden verschiedene Arten (z.B. handlungs- oder diskussionsbasiert) von CÜ auf Inhalte und deren Aufbau für verschiedene Zielgruppen (ZG) analysiert. Zudem werden nicht nur technische, sondern auch organisatorische Prozesse in Bezug auf Chancengerechtigkeit und Diversitätsdimensionen untersucht.

Ziel 2: Zugang zu praxisorientierten Cybersicherheitskompetenzen und -fähigkeiten für verschiedene ZG ermöglichen

Leitfragen:

> „Welche Maßnahmen müssen nicht nur bezüglich Cyberszenarien, Technologien, Methodik und Didaktik getroffen werden, sondern auch für die Organisation von CÜ?“
>
> „Wie können unterrepräsentierte Zielgruppen sukzessive an das Thema Cybersicherheitskompetenz und -fähigkeiten durch Cyberübungen herangeführt werden?“[34]

Ziel: ZG-spezifisches Design der Lehr- und Lerninhalte

Erwartete Resultate:

- Eine umfassende Analyse von Literatur und aktuellen Cyberübungen unter dem Aspekt der Diversität und Chancengerechtigkeit:

Die bereits im ersten Projektabschnitt erfolgte ausführliche Literaturrecherche wird kontinuierlich und bedarfsorientiert weitergeführt (siehe Kapitel 4.8).

- Die Cyberübungen werden entlang demografischer, kognitiver, fachlicher, funktionaler und institutioneller Aspekte analysiert und mittels eines (de-)konstruktiven und intersektionalen Verständnis von Geschlecht und Differenz didaktisch angereichert und aufbereitet

Strukturierte Analysen von verschiedenen Arten von CÜ und deren Auflistung nach potenziellen Zielgruppen (siehe Kapitel 4.9):

- Mittels Fokusgruppeninterviews und Stakeholder*innenanalysen werden die Bedürfnisse der Zielgruppen erhoben und mit dem aktuellen Format der Cyberübungen verglichen. Die Empfehlungen fließen in das didaktische Design ein und werden auf die Bedürfnisse und Interessenslagen der jeweiligen Gruppe abgestimmt.
- Um das Feld der aktuellen Nutzer*innengruppe zu erweitern, wird daran gedacht, gezielt unterrepräsentierte Gruppen zu adressieren. Diese umfassen primär die Kategorien Gender, Alter und soziale Herkunft. Dabei werden auch die Marketing- und Disseminationsstrategie betrachtet und ggf. adaptiert.

[34] Projektbeschreibung INDUCE, S. 24.

Instrumente: Fokusgruppen- und Expert*innen-Interviews, Teilnehmer*innen-Fragebogen, Heuristik, Beobachtungsleitfaden

- Handlungsempfehlungen für chancengerechte CÜ für Organisator*innen (D3.3; T3.4 Handlungsoptionen und Empfehlungen für Organisator*innen und KMUs; D2.3 Handlungsempfehlungen für den Zugang von KMUs zu CÜ und niedrige Nutzungsbarrieren) (siehe Kapitel 2.3)
- Eine grundlegende Analyse der Disseminationskanäle und ggf. eine Anpassung an neue unterrepräsentierte Gruppen. Hier sollen Medien (z.B. soziale Medien) genutzt werden, die für diese Gruppen relevant sind.

Jede Cyberübung sollte mit einem zielgruppenspezifischen didaktischen Design angereichert werden.

Instrumente: Literatur- und ggf. Online-Recherche, Reflexions-Sheets

Anmerkung: Zwischen den einzelnen Deliverables können keine scharfen Trennlinien gezogen werden. Vielmehr gestalten sich die Übergänge fließend, da sich sowohl Fortführungen und Rückkopplungen im Hinblick auf D3.1 (State of the Art- und Zielgruppenanalyse) als auch Vorgriffe auf D 3.3 (Handlungsempfehlungen und Maßnahmen für diversitätssensible Cyberübungen) als notwendig erweisen. Dies ist zum einen darauf zurückzuführen, dass das AP der FH OÖ ein übergreifendes, alle Projektabschnitte Betreffendes ist. Zum anderen liegt der Grund darin, dass aufgrund der Covid-19-Pandemie und der damit verbundenen Beschränkungen über lange Zeit keine Präsenzveranstaltungen, Teilnehmer*innenbefragungen, Vorort-Beobachtungen und Untersuchungen von aktuellen Cyberübungen nur mit starken Verzögerungen durchgeführt werden konnten.

5.2 Literaturrecherche

Diversity-Dimensionen können helfen, mögliche Zielgruppen zu identifizieren und dienen als modellhafte Einteilung dazu, Ungleichheiten zu erkennen. Während die inneren (im HEAD-Wheel die demografischen) Dimensionen (Alter, Geschlecht, sexuelle Orientierung, geistige und körperliche Fähigkeiten, nationale Herkunft/Ethnie, soziale Herkunft sowie Religion oder Weltanschauung) weitgehend unveränderlich und in der gesamten EU gesetzlich vor Diskriminierung geschützt sind, können sich die äußeren (wie zum Beispiel Familienstand, Einkommen, Ausbildung oder Berufserfahrung) und die kognitiven, institutionellen, funktionalen und disziplinären (vgl. Gaisch, Preymann & Aichinger 2018) Dimensionen im Laufe eines Lebens verändern. Grundsätzlich vereint eine Person eine Vielzahl unterschiedlicher und unterschiedlich stark kombinierter Dimensionen in sich, die kontextabhängig unterschiedlich große Bedeutung haben. (vgl. Erharter 2013: GUT Teil A, S. 7ff; Erharter 2014, S. 45ff)

Erharter (2014, S. 45ff; 2015) verweist in diesem Zusammenhang darauf, dass Unterschiede, die für die Entwicklung von Nutzer*innen-orientierten IKT-Anwendungen eine Rolle spielen, weniger durch das Geschlecht selbst als vielmehr durch unterschiedliche Lebensrealitäten zustande kommen. Aus diesem Grund sollten den bestehenden inneren Diversitätsdimensionen drei weitere hinzugefügt werden, um die Lebensrealitäten und Einstellungen der potenziellen Nutzer*innen abzubilden und diese im Vorfeld von Entwicklungen in qualitativen Studien zu erheben. Die erste zusätzliche, weitgehend durch die Lebensumstände der Nutzer*innen geprägte, Dimension ist die der **raum-zeitlichen Rahmenbedingungen und Wege** der potenziellen Nutzer*innen. Eine weitere zuzufügende Dimension ist die der **Werthaltungen und Einstellungen gegenüber der Technik**, die insbesondere durch Sozialisationsprozesse geprägt werden. Die dritte Dimension ist die der **Technikerfahrung und des Technikwissen** und wird wesentlich durch die berufliche Biografie geprägt. Für die Erhebung quantitativer Studien empfiehlt Erharter auf das Clustering entlang von inneren Diversitätsdimensionen zu verzichten, um eine unbewusste Verstärkung von Stereotypen

zu vermeiden, und stattdessen ein Clustering entlang von Faktoren vorzunehmen, die sich aus der Studie selbst ergeben oder Merkmale zu wählen, die weniger stark Stereotypen unterliegen, wie zum Beispiel ein Clustering nach unterschiedlichem Nutzungsverhalten.

Die Erkenntnisse der Literaturrecherche werden für das INDUCE Projekt nutzbar gemacht und fließen in den Entwurf eines **Gender-Erhebungsbogens** ein, mit dessen Hilfe die Verteilung unterschiedlicher Diversitätsdimensionen innerhalb der aktuellen und potenziellen neuen Zielgruppen ermittelt werden sollen. Die Erhebungen werden, wie von Erharter empfohlen, anwendungsorientiert durchgeführt, das heißt sie erfolgen (unter Beratung durch die FH OÖ) im Hinblick auf unterschiedliche, durch die Lebens- und Arbeitsrealitäten geprägte Nutzungs- und, in diesem Zusammenhang von den Konsortialpartner*innen zur Verfügung gestellte, Angebotskontexte. (siehe Kapitel 2.2).

Im Kern werden folgende Dimensionen erhoben beziehungsweise betrachtet (vgl. Erharter 2013: GUT Teil A, S. 9f):

- **Geschlecht**: Ausgewiesenes Ziel des INDUCE Projektes ist es, den nachweislich geringen Frauenanteil an Cyberübungen zu erhöhen. Dazu ist es erforderlich, die aktuellen und neu entworfenen Übungen insbesondere auf ihre Geschlechterverteilung hin zu analysieren und Verbesserungspotential aufzudecken beziehungsweise zu dokumentieren. Diese Dimension spielt im INDUCE-Zusammenhang insbesondere bei der verbalen und bildsprachlichen Gestaltung von Cyberübungen eine bedeutende Rolle.
- **Alter**: Erharter verweist hier im Zusammenhang mit zu entwickelnden Apps oder Websites auf im Alter nachlassende physische Fähigkeiten. Es ist zu erwarten, dass unterschiedliche Altersgruppen unterschiedliche Erfahrungen, Kompetenzen und Hintergrundwissen im Umgang mit der Informationstechnologie und hier insbesondere mit Cybersicherheit aufweisen. Ein Monitoring der erreichten Altersgruppen in aktuellen und neu entwickelten oder angepassten Cyberübungen dokumentiert die angestrebte Erweiterung in dieser Dimension.
- **Bildungshintergrund**: Dieser wird anhand des Schulabschlusses der befragten Person sowie der beiden Elternteile ermittelt und dient dazu, die aktuell erreichte Zielgruppe auch in dieser Dimension zu erweitern.
- **derzeitige Tätigkeit**: hier wird die aktuelle Ausbildungs- oder berufliche Tätigkeit erfragt. Erharter weist darauf hin, dass das Tätigkeitsfeld die Lebensrealität der Menschen, im Alltag und in der Freizeit, stark prägt und die Erwartungen und Ansprüche an technische Produkte beeinflusst. Personen, die im beruflichen Kontext häufig den Computer nutzen, erwerben implizit Wissen, sammeln Erfahrungen und sind mit Funktionalitäten vertraut. Dieses Hintergrundwissen fehlt Menschen, die beruflich (oder im Ausbildungsverhältnis) gar nicht oder kaum IT-Technologien einsetzen.
- **Einstellung zu und Erfahrung mit Informationstechnologie**: in diesen, von Erharter empfohlenen zusätzlichen Dimensionen, werden sowohl die technischen Vorerfahrungen und Kompetenzen als auch die grundlegende Motivation, sich mit (sicherheits-)technischen Fragestellungen zu beschäftigen, erfragt. Diese beiden Dimensionen spielen im INDUCE-Kontext eine bedeutsame Rolle im Hinblick auf die Nutzer*innen-angepasste Entwicklung von Cyberübungen und die Vermeidung von I-Methodology.

Mit Hilfe der erweiterten Literaturrecherche können zudem die auf der bisherigen Recherche (Coenraad et al. 2020, Bath 2009 und Reidl et al. 2020) aufbauenden Analysekategorien (siehe Kapitel 5) für INDUCE-Zwecke erweitert und die Möglichkeiten verbessert werden, bestehende und neu entwickelte oder angepasste **Cyberübungen im Hinblick auf Diversität und Chancengerechtigkeit** zu untersuchen und Differenzen zwischen dem angebotenen Format und dem angesprochenen Zielpublikum offen zu legen. Entwickelt wird ein heuristisches Instrument, mit dessen

Hilfe verschiedene Teilaspekte von Cyberübungen betrachtet und bewertet werden können. Dieses wird im Laufe des Projektes angepasst und verfeinert. Ziel ist, auf Basis dieser Heuristik ein **Reflexions- und Evaluationsinstrument** zu erarbeiten, das Entwickler*innen und Organisator*innen von Cyberübungen zur Verfügung gestellt werden kann.

Die **Heuristik** beinhaltet folgende Teilaspekte:

- Inhalt der Übung
- Bilder
- Charaktere/ Rollen
- Sprache und Texte
- Organisatorische Vorbereitung
- Durchführung
- Organisatorische Nachbearbeitung/ Evaluation

5.3 Strukturierte Analyse von verschiedenen Arten von Cyberübungen und deren Auflistung nach potenziellen Zielgruppen

5.3.1 Methodische Reflexion

Die unterschiedlichen Übungsangebote der Konsortialpartner*innen sowie die von ihnen jeweils fokussierten neuen Zielgruppen erfordern einen **Mixed-Method-Ansatz** (vgl. Flick 2009), bei dem, angepasst an den jeweiligen Nutzungskontext, entsprechende Untersuchungsmethoden entwickelt und auf die jeweiligen Bedingungen abgestimmt werden müssen. So zeigt sich beispielsweise, dass die Übungsformate der CSA aufgrund der starken technischen Ausrichtung kaum Möglichkeiten einer sprachlichen oder inhaltlichen Gender-sensiblen Gestaltung bieten. Da zudem das ausgewiesene Ziel der Hackathons darin liegt, IT-Security-Talente zu identifizieren und zu fördern, kann das Niveau der Aufgaben nicht beliebig herabgesetzt werden. Aus diesem Grund muss hier der Fokus darauf gerichtet werden, Rekrutierungsmaßnahmen zu verbessern, um unter den Teilnehmer*innen mehr Diversität zu erreichen. Daher kommen in diesem Zusammenhang vermehrt quantitative und qualitative Erhebungsmethoden (Braun & Clarke 2013, Flick 2009) zum Einsatz, um, durch Befragungen der Teilnehmer*innen und Coaches während der ECSC-Veranstaltung den Status Quo sowie Ansatzmöglichkeiten zu ermitteln, wie in Zukunft eine breitere Diversität unter den Teilnehmer*innen erreicht werden kann. Es zeigt sich einerseits, dass unter den teilnehmenden Ländern ein großes Interesse an den Ergebnissen dieser Untersuchungen besteht, andererseits, dass der Auswahlprozess der ECSC-Teilnehmer*innen bereits wissenschaftliche Aufmerksamkeit geweckt hat und im Hinblick auf die Trainings- und Auswahlmodalitäten untersucht wird (vgl. Yamin et al. 2021 und 2022; ENISA 2021). Hier kann INDUCE mit seinen Ergebnissen anknüpfen und mit der Auswertung der durchgeführten Studie weitere Erkenntnisse liefern.

Eine weitere Schwierigkeit besteht darin, dass bei vielen Cybersecurity-Übungen die anbietenden Organisationen kaum Einfluss auf die Zusammensetzung der Teilnehmenden haben, weil häufig die Anmeldungen über die Arbeitgeber*innen erfolgen. Daher muss auf andere Möglichkeiten zurückgegriffen werden, neue Zielgruppen zu erschließen. So werden neue Angebote für spezielle Zielgruppen geschaffen (AIT, KSÖ-Newsletter), vorhandene Angebote werden um die Teilnahme spezieller Gruppen erweitert (KSÖ-Planspiel) oder der Fokus wird daraufgelegt, teilnehmende, unterrepräsentierte Gruppen zu stärken und für eine erneute Teilnahme zu motivieren (INFRAPROTECT®).

5.3.2 Analyse des Teilnehmer*innenfeldes

Die Konsortialpartner*innen werden gebeten, so weit als möglich, die Geschlechterverteilung im Teilnehmer*innenfeld bei bisherigen Übungen als Vergleichsfolie zu ermitteln. Zudem werden, aufbauend auf den unter Kapitel 5.2 aufgelisteten Genderdimensionen, im Konsortium unter Federführung der FH OÖ Übungs- und Kontextabhängige Teilnehmer*innen-Fragebögen, Leitfadeninterviews sowie Beobachtungsleitfäden erarbeitet, die von den Konsortialpartner*innen im Rahmen der jeweiligen Übungsformate zur Untersuchung des Teilnehmer*innenfeldes eingesetzt werden können.

5.3.2.1 AIT

Neue Zielgruppe: (primär weibliche) Berufstätige, die IKT für ihren Arbeitsalltag verwenden, aber nicht genügend IT-Sicherheitswissen und -bewusstsein aufweisen

Untersuchungsgegenstand: neu entwickeltes strategisches Cyberplanspiel: Lehrer*innenzimmer/ Home Office-Szenario

Untersuchungsinstrument: Standardisierter Fragebogen mit geschlossenen und ein (oder drei) offenen Frage(n) (drei Fragen, wenn die Evaluationsfragen hinzugenommen werden)

- **Stichprobe**: Teilnehmer*innen des Planspiels
- **Inhalt**: Erhebung von Genderdimensionen (Geschlecht, Alter, Bildungshintergrund, derzeitige Beschäftigung), IT-Wissen und -Affinität, Wissen über Planspiele, (Evaluierung des Planspiels)
- **Ziel der Erhebung**: Erfassung der Genderdimensionen in der angesprochenen Zielgruppe, Erfassung des Vorwissens und Sensibilisierungsgrades in Bezug auf IT(-Sicherheit), Anregungen für weitere mögliche Szenarien, Usability-Test des neu entwickelten Planspiels
- **Auswertung**: statistische Auswertung, Kodierung und Kategorisierung (falls nötig)

5.3.2.2 Cybersecurity Austria

Neue Zielgruppe: Steigerung der weiblichen Teilnehmenden an den Wettbewerben

Untersuchungsgegenstand: ACSC- und ECSC-Wettbewerb: Es werden zwei Untersuchungsformate entwickelt:

Untersuchungsinstrument 1: Leitfadeninterview (Vor-Ort-Befragung durch INDUCE-Projektmitarbeiter*innen): geschlossenes, halboffenes und offenes Antwortformat

- **Stichprobe**: Team-Coaches der teilnehmenden Länder am ECSC-Finale
- **Inhalt**: Erhebung in Bezug auf Organisation, Teilnehmer*innen, Werbung und Teilnehmendenrekrutierung, Teamzusammensetzung sowie Maßnahmen zur Förderung von Diversität
- **Ziel**: Erhebung und Vergleich der nationalen Anstrengungen zur Steigerung der Diversität innerhalb der Teams im Hinblick auf Best-Practice-Beispiele und Verbesserungsmöglichkeiten
- **Auswertung** (noch in Ausarbeitung): statistische Auswertung, Kodierung und Kategorisierung

Untersuchungsinstrument 2: Online-Teilnehmer*innen-Fragebogen (vorab ausgeschickt): geschlossenes, halboffenes und offenes Antwortformat

- **Stichprobe**: Teilnehmer*innen ECSC-Finale

- **Inhalt**: Erfassung der Genderdimensionen in der teilnehmenden Gruppe (Geschlecht, Alter, Bildungshintergrund, derzeitige Tätigkeit), IT-Security-Hintergrund und -Ausbildung, Motivation zur Teilnahme, Stellenwert der IT-Security, Vorbilder und Unterstützungsmöglichkeiten
- **Ziel**: Erfassung der Teamzusammensetzungen innerhalb verschiedener nationaler Teams, Vergleich von unterschiedlichen Motivationslagen, Unterstützungsangeboten und Anstrengungen zur Förderung der Diversität im Hinblick auf best-practice-Beispiele und Verbesserungsmöglichkeiten
- **Auswertung**: statistische Auswertung; Kodierung und Kategorisierung

5.3.2.3 INFRAPROTECT®

Neue Zielgruppe: Erweiterung des Angebots für KMU, Förderung und Stärkung teilnehmender Frauen

Bei einer intern von INFRAPROTECT® durchgeführten Analyse der Übungen der letzten acht Jahre zeigt sich folgendes Bild: Der Frauenanteil unter den Übungsteilnehmenden mit Cybersecurity-Bezug lag bei etwa 22%, die Hälfte unterstützte dabei aber überwiegend im Support-Bereich. Als Fachfunktion im Krisenstab agierten nur etwa 10% der Teilnehmerinnen. Dennoch steigt der Prozentsatz stetig und tendiert aktuell zu 25%. Diese positive Entwicklung ist auch beim Frauenanteil der Leitungsfunktionen zu beobachten.

Als anbietende Organisation von Krisenübungen hat INFRAPROTECT® wenig Einfluss auf die Zusammensetzung und Auswahl der teilnehmenden Personen. Zwar steigt die Teilnahmerate von Frauen in den vergangenen Jahren stetig, liegt aber insbesondere in den Fach- und Leitungsfunktionen nach wie vor weit hinter dem Anteil männlicher Teilnehmer zurück. Eine mögliche Einflussnahme in Bezug auf eine Erhöhung des Frauenanteils liegt daher erst in der Übungssituation selbst. Ziel ist es, teilnehmende Frauen zu stärken und für eine erneute Teilnahme zu motivieren. Dazu gilt es zu eruieren, ob es Unterschiede im Führungsstil und hier insbesondere in der Kommunikation von Männern und Frauen gibt und wie diese Erkenntnisse zukünftig für die Übungsgestaltung genutzt werden können. Das von INFRAPROTECT® angebotene interaktive Seilspiel bietet eine Möglichkeit, diese Fragen anhand einer künstlich konstruierten Situation zu untersuchen (Siehe Kapitel 5.3.3.3).

5.3.2.4 KSÖ

Neue Zielgruppe: Klein- und Kleinstunternehmer*innen, insbesondere Gewerbe und Handwerk, Information und Consulting, Tourismus

Durch die Kooperation mit der WKO und der Konzeption des Newsletters konnten viele zielgruppenzugehörige Personen sowohl erstmalig als auch gut erreicht werden. Die Rückmeldungen zu den Newslettern sind auch durchwegs positiv (vgl. Bericht des KSÖ).

5.3.3 Handlungsempfehlungen und Maßnahmen für diversitätssensible Cyberübungen

Die im Kapitel 5.2 bereits dargestellten Erkenntnisse der Literaturrecherche in Bezug auf De-Gendering informatischer Artefakte, digitale Ungleichheit, I-Methodology, partizipative Designmethoden (Bath 2009; Coenraad et al; 2020, Reidl et al 2020) werden mit Erkenntnissen zu inklusiver Didaktik (Leicht-Scholten & Schroeder, 2014) ergänzt, gebündelt und als konkrete **Handlungsempfehlungen für die diversitätssensible Gestaltung, Erweiterung oder Adaption von Cyberübungen** den Konsortialpartner*innen vorgestellt. Diese umfassen verschiedene Bereiche, wie die **Ansprache** der Zielgruppen (z.B. sprachliche und grafische Berücksichtigung der Zielgruppe, niedrigschwellige Zugänge, Einbeziehung von entsprechenden Role Models), mögliche **Themen** (z.B.

Multidisziplinarität des Cybersecurity-Feldes betonen und sozioökonomische Dimensionen mit einbeziehen, Themen aus der unmittelbaren Arbeits- und Lebenswelt aufgreifen), **Designmethoden** (wie z.B. partizipative und Nutzer*innen-orientiertes Design) sowie hilfreiche **didaktische Konzepte** (z.B. Persona-Effekte ausnutzen, stärkere Repräsentation von nicht-traditionellen Gruppen, interaktive Methoden, Hilfs- und Beratungsangebote, Praxisorientierung und Anwendungsbezug, gestaffelte Level).

Insbesondere werden die Partner*innen auf die Gefahren einer (Re-)Produktion von Ungleichheit im Technikgestaltungsprozess hingewiesen und dahingehend sensibilisiert. Der Begriff „**Digitale Ungleichheit**“ (Reidl et al., 2020, S. 6) beschreibt die Tatsache, dass nicht alle Menschen die Potenziale und Chancen der Digitalisierung nutzen können oder wollen. Daraus allerdings resultieren Wissensdefizite, Kostennachteile oder schlechtere Chancen am Arbeitsmarkt. Die Gründe für die unterschiedliche Nutzung der IKT-Technologien sind mannigfaltig, wie z.B. fehlender oder unzureichender Zugang zur Technologie, mangelnde Kompetenzen oder ungleiche Möglichkeiten, an der Gestaltung mitzuwirken. INDUCE fokussiert in diesem Zusammenhang den Aspekt der Technikgestaltung. Hier spielt neben der unreflektierten Einschreibung von stereotypen Vorstellungen, aus der wiederum technische Produkte hervorgehen, die bestehende Rollenbilder und Stereotype fortschreiben oder durch ihre Einschreibung in Algorithmen zu verzerrten Daten oder falschen Rückschlüssen führen, vor allem das Problem der **I-Methodology** eine große Rolle. Hierbei gehen Technikgestalter*innen im Entwicklungsprozess von ihren eigenen Kompetenzen, Interessen und Nutzungsweisen aus und lassen ihre Erfahrungen, Werte und Vorstellungen (unbewusst), als repräsentativ für alle in das Produkt mit einfließen. Bleibt eine solche Herangehensweise unreflektiert, können sich bestehende Ungleichheiten weiter fortschreiben, indem nur bestimmte Bedürfnisse berücksichtigt, während andere Perspektiven, Interessen oder Fähigkeiten nicht wahrgenommen werden. Auf diese Weise können Menschen aufgrund ihres Geschlechts, Alters, ihrer Herkunft, Kompetenzen oder Präferenzen oder ihrer differierenden Lebensumstände von der Nutzung der Produkte ausgeschlossen werden oder ihnen steht die Nutzung der Produkte nur eingeschränkt oder unter erschwerten Bedingungen zur Verfügung. Solche Ungleichheiten sollen im Zuge des Projekts aufgedeckt und durch Neu- oder Umgestaltung der Übungen vermieden werden.

5.3.3.1 AIT

Das AIT entwirft ein neues strategisches Planspiel (Lehrer*innen-Szenario), das die Zielgruppenerweiterung auf (primär weibliche) Berufstätige, die Informationstechnologie für ihren Arbeitsalltag verwenden, aber nicht genügend IT-Sicherheitswissen aufweisen. Fokussiert wird insbesondere die Berufsgruppe der Lehrenden, da sie als potenzielle Multiplikator*innen fungieren können, sowie weibliche Arbeitnehmende aus dem IT-Umfeld und weibliche Studierende. Vorgestellt wird das im Rahmen einer Lehrer*innen-Fortbildung durchgeführte Cybersicherheits-Planspiel, das das gemeinsame Vorhandensein beruflicher und privater Daten auf einem Gerät in den Fokus nimmt, wie es insbesondere seit dem durch die Covid-19-Pandemie ermöglichten „Home Office“ üblich geworden ist.

Die Änderungen gegenüber vorherigen Formaten des AIT sind in mehreren Bereichen zu finden. In der vorgestellten Übung wird der vermittelte Inhalt stark auf die adressierte Zielgruppe zugeschnitten, auch die Dauer wird deutlich gekürzt, so dass die Übung insgesamt (Durchführung und Nachbesprechung) etwa 60 Minuten umfasst. Um die neue, nicht traditionelle, Zielgruppe zu erreichen, wird das Planspiel als Workshop-Format konzipiert und im Rahmen einer Fortbildungsveranstaltung (e-education in Linz am 10.11.2022) kostenlos angeboten.

Von den im Rahmen des INDUCE-Projektes bisher erarbeiteten Handlungsempfehlungen fließen folgende in das Design der Übung mit ein:

- Scenario-based Design

- Value sensitive Design (gender-sensible Sprache und Abbildungen)
- Sprachliche und grafische Berücksichtigung der Zielgruppe
- Niedrigschwelliger Zugang
- Partizipatives Design
- Praxis-/ Anwendungsbezug
- Feedback-Möglichkeit
- Gamification/ aktivierende Lernmethode
- Fachausdrücke vermeiden oder erklären
- Förderung von Teamwork
- Awareness schaffen (ZG-spezifische Themen)
- Leichter Zugang zur Übung (keine oder einfache technische Ausrüstung, gratis Angebot, kurze Dauer)
- Abstimmung der Aufgabenformate auf Verständnis- und Handlungshorizont der ZG
- Hilfs-/ Beratungs-/ Feedback-Angebot

Analyse-Instrument: Heuristik

Das betrachtete Planspiel verfolgt eine **strategische Perspektive** und dient in erster Linie der **Awareness-Schulung für Cybersicherheitsgefahren**. Die Ablaufart ist primär diskussions-, weniger handlungsorientiert. Zur Durchführung wird eine **interaktive, dynamische Abstimmungsmöglichkeit via Mentimeter** [35] angeboten. Die Teilnehmer*innen können sich in der Gruppe beraten, wie auf die dargestellten Situationen reagiert werden kann, wählen dann aber einzeln ihre jeweils präferierte Reaktion. Die Abstimmungsergebnisse werden unmittelbar darauf angezeigt. Das Planspiel bietet keine konkreten Handlungsanweisungen, allerdings werden Fragen, die sich unmittelbar im Rahmen der Diskussionen ergeben, in der abschließenden Reflexionsrunde bestmöglich von den Veranstalter*innen beantwortet.

Nach einer kurzen Einführung, die unverkrampft das Thema eines normalen Lehrer*innentages eröffnet und eine erste Anwendung der Abstimmungsgeräte ermöglicht, werden drei kurze Szenarien präsentiert, die jeweils die Verletzung eines der drei Sicherheitsziele der Informatik behandeln.

Das Thema „**Verfügbarkeit**“ wird anhand eines Ransomware-Angriffes simuliert, bei dem alle Daten am Laptop verschlüsselt und auf diese nicht mehr zugegriffen werden kann. In der Folge werden sensible Daten der Schüler*innen im Internet veröffentlicht, sodass hier die „**Vertraulichkeit**“ verletzt wird. Abschließend wird in der Simulation gezeigt, dass im Namen der Lehrer*innen E-Mails an die Eltern verschickt werden, um mit Geld die Noten ihrer Kinder aufzubessern. Hier liegt eine Verletzung der „**Integrität**“ vor. Die Teilnehmer*innen des Workshops werden im Verlauf der Simulation dazu aufgefordert, unter vorgegebenen Reaktionen auf die jeweils neue Situation, eine auszuwählen.

Im Hinblick auf die **Inhalte, Nutzungskontexte und Aufgabenstellungen** des Planspiels kann eine **Übereinstimmung mit dem Horizont der Zielgruppe** attestiert werden. Dies wird auch durch rege Diskussionen, Nachfragen und Weiterbildungswünsche der Teilnehmenden im Anschluss an die Veranstaltung bestätigt.

Die Abbildungen des Planspiels weisen, soweit möglich, eine **gender-sensible Darstellung** auf. Die Bilder sind häufig gegenständlich (z.B. Schreibtisch, Telefon, Stifte), abstrakt (Binärcode) oder

[35] Leitner, M. (2023). A Scenario-Driven Cybersecurity Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned. International Conference on Information Systems Security and Privacy (ICISSP).

zeigen Tätigkeiten (auf einem Tablet, Laptop o.Ä. tippende Hände). Von fünf Darstellungen einer Hand lassen sich drei einer Frau und zwei einem Mann zuordnen. Variationen in Bezug auf Alter oder visuell fremdländische Herkunft werden hier allerdings nicht berücksichtigt. Insbesondere die gegenständlichen Abbildungen weisen Accessoires auf, die auf weibliche Nutzerinnen schließen lassen.

In den Texten, die das Szenario beschreiben, wird durchgängig eine **gender-sensible Sprache** sowie die inklusive Wir-Form verwendet. In den Spiel- beziehungsweise Entscheidungssituationen werden die Teilnehmenden direkt angesprochen und zu einer Reaktion aufgefordert, während die zu wählenden Entscheidungen aus der Ich-Perspektive dargestellt werden. Da die Texte jeweils nur kurze Situationsbeschreibungen liefern, beziehungsweise zu einer Reaktion auffordern, kann hier keine Einschätzung im Hinblick auf darin transportierte Werthaltungen gemacht werden.

Da die Teilnahme an der Übung **keine Vorkenntnisse** erfordert und sich in erster Linie an Personen richtet, die einen geringen Kenntnisstand in Bezug auf Cybersicherheit aufweisen, ist es im Rahmen dieser Sensibilisierungsschulung besonders wichtig, die Sicherheitsziele der Informatik als **Fachausdrücke** einzuführen und zu erklären. Der **niedrigschwellige Zugang** wird zudem dadurch erreicht, dass das Planspiel als **kostenloses Workshop-Angebot** im Rahmen einer umfassenderen Veranstaltung besucht werden kann. Die Teilnehmenden benötigen keine technische Ausrüstung, die erforderlichen Abstimmungsgeräte werden von der durchführenden Organisation zur Verfügung gestellt.

Im Anschluss an die etwa 25-minütige Übung erfolgt eine etwa 30-minütige **Reflexionsrunde**, in der die Teilnehmenden Feedback geben, Fragen stellen und gemeinsam diskutieren können.

Es zeigt sich, dass das bereits im Juni 2022 durchgeführte Planspiel unter dem Thema „Home Office“ eine gute Grundlage bietet und leicht auf unterschiedliche Zielgruppen angepasst werden kann. Im Mittelpunkt dieses Szenarios steht die gleichzeitige Nutzung eines Gerätes für berufliche und private Zwecke und die sich daraus ergebenden Schwierigkeiten. Insbesondere die gemeinsame, globale Erfahrung der Covid-19-Pandemie hat diesen Sicherheitsaspekt branchenübergreifend verstärkt in den Aufmerksamkeitsfokus gerückt und stellt so einen Anknüpfungspunkt für die sichere Nutzung von Informationstechnologien dar.

5.3.3.2 Cybersecurity Austria

Inhalt und beispielhafte Aufgabenstellungen in der Qualifikationsphase wurden den Mitarbeiterinnen der FH OÖ während eines Experteninterviews im Januar 2022 präsentiert. Es zeigte sich, dass Übungsformate aufgrund der starken technischen Ausrichtung kaum Möglichkeiten aufweisen, Gender-sensible Sprache, Texte oder Bilder zu verwenden und so durch eine verstärkte Sichtbarmachung bisher unterrepräsentierter Gruppen besser anzusprechen.

Da zudem das ausgewiesene Ziel solcher Hackathons darin liegt, IT-Security-Talente zu identifizieren und zu fördern, kann das Niveau der Übungen nicht beliebig herabgesetzt werden, um Teilnehmer*innen mit weniger ausgeprägten IT-Security-Kenntnissen zu gewinnen.
Aus diesem Grund richtet sich der Fokus darauf, wie Rekrutierungs-, Unterstützungs- und Trainingsmaßnahmen zu verbessern sind, um mehr Diversität unter den Teilnehmer*innen zu erreichen. Als besondere Herausforderung stellt sich in diesem Zusammenhang der Übergang beziehungsweise die weiterführende Qualifizierung im Bereich IT-Security von Einstiegsübungen, wie sie beispielsweise im „Cybersecurity Quiz“[36] (siehe Kapitel 5.3.3.4.2) angeboten werden, bis zur Teilnahme an der Qualifikationsphase des Wettbewerbs dar.

[36] https://ovosplay.com/cybersecurity-quiz; www.saferinternet.at/news-detail/neu-cyber-security-quiz/

5.3.3.3 INFRAPROTECT®

Erarbeitung eines **Beobachtungsleitfadens** (vgl. Flick 2009) für das Interaktionsspiel der INFRAPROTECT®

- Vorab: **Expert*innen-Interview** (04.10.2022, 11:00-11:20 mit Judith Welzl und Oliver Decker) zur Erhebung und Generalisierung von Ablauf und Erkenntnisziel des Spiels
- Erkenntnisziel des Spiels:
  - Wie einfach muss Kommunikation gestaltet sein, damit alle die Botschaften/ Kommandos verstehen, die gegeben werden?
  - Wie funktioniert die Einordnung in eine unbekannte Gruppe/ die Unterordnung unter eine Führungsperson (insbesondere bei Krisenstabübungen interessant)?
  - Wie schwierig ist es, wenn der wichtige Sehsinn wegfällt, trotzdem alle relevanten Informationen mitzubekommen?
  - Wie kommt die Gruppe zur Lösung? Kann sie eine Lösung präsentieren?
  - Wie inklusiv werden die Botschaften formuliert?
- Beobachtung: teil-standardisierte Beobachtung:
  - offene, nicht-teilnehmende Beobachtung
  - künstliche Situation: Teilnehmer*innen des INFRAPROTECT®-Seilspiels
  - Dokumentation: Video-Aufzeichnung
- Beobachtungsleitfaden: Ereignisstichproben zu
  - Verteilung Männer/ Frauen?
  - Häufigkeit der Handlungsvorschläge von Männern/ Frauen?
  - Häufigkeit der Kommandos von Männern/ Frauen?
  - Häufigkeit opponierender (Ja, aber…) Beiträge von Männern/ Frauen?
  - Häufigkeit kontraproduktiver Beiträge von Männern/ Frauen?
  - Häufigkeit unterstützender Beiträge von Männern/ Frauen?
  - Anzahl aktiver/ passiver Teilnehmer*innen? M/F-Verteilung?
  - Führungsperson: m/w?
  - Führungsperson:
    - Autoritär: gibt Kommandos, lässt sich nicht reinreden
    - Souverän: leitet die Gruppe mit klaren Kommandos, ist aber offen für konstruktive Einwände
    - Unsicher: macht zögerlich Vorschläge, ist aber froh, wenn Gruppenmitglieder Hinweise geben, und schließt sich diesen an
    - gibt Leitungsposition ab
- Nachbesprechung:
  - Offene Feedbackrunde im Hinblick auf subjektives Empfinden, Verständnis und Ausführung der Kommandos, Interaktion
  - Videovorführung: Differenz zwischen subjektivem Empfinden und Realität
  - Fragen/ Ergänzungen/Verbesserungen von Seiten der Teilnehmer*innen
  - Mögliche zusätzliche Fragen:
    - Setting/ Spiel bekannt?
    - Teammitglieder bekannt?
    - Selbstbezeichnung der eingenommenen Rolle?
    - Zufrieden mit den eigenen Entscheidungen?

- Würden Sie bei einem erneuten Spiel wieder so entscheiden/ wieder die gleiche Rolle einnehmen?

5.3.3.4 KSÖ

Das Kompetenzzentrum Sicheres Österreich erweitert das bisherige Angebot in zwei Richtungen, um Cybersicherheitsthemen breiter in der Bevölkerung zu verankern. Einerseits wird das bisherige Format des umfassenden Planspiels um eine weitere Gruppe aus der Gesellschaft ergänzt. Dieses Format, die Einbeziehung der Bevölkerung in die Simulation eines großflächigen Blackouts, wurde im November 2022 unter Teilnahme einer Mitarbeiterin der FH OÖ zum ersten Mal erprobt.

Zusätzlich wird ein neues Übungskonzept entworfen, das sich an die Zielgruppe der Klein- und Kleinstunternehmen sowie EPUs richtet. Für diese Zielgruppe werden von Seiten der FH OÖ, unter Rückbezug auf die erarbeiteten Handlungsempfehlungen und unter Verwendung der Heuristik als Analyse-Instrument, die zu berücksichtigenden Zielvorgaben zusammengefasst sowie ein best-practice-Beispiel beschrieben.

5.3.3.4.1 Planspiel 2022 BlackAUT

Im Rahmen der Erweiterung des Planspiels[37] um eine Gruppe aus der Gesellschaft nimmt eine Mitarbeiterin der FH OÖ am Spiel teil. Ziel dieser Teilnahme ist einerseits das Kennenlernen des Planspielkonzepts sowie ein erstes Feedback aus Sicht der teilnehmenden Bevölkerungsgruppe im Rahmen einer informellen Beobachtung.

Die Gruppe der **„Tischgesellschaft“** setzt sich aus neun Personen, sechs Männer und drei Frauen, aus verschiedenen Berufssparten (IT-Abteilung Staatsunternehmen, Krisenmanagement WKO, Krisenmanagement Feuerwehr, Dachverband ÖRK, Gebäudemanagement, Marketing) zusammen. Das behandelte Szenario umfasst einen flächendeckenden, länderübergreifenden Stromausfall (**Blackout)** über mehrere Tage.

Nach der Teilnahme am Planspiel lassen sich Erkenntnisse auf verschiedenen Ebenen identifizieren.

Der **persönliche** Erkenntnisgewinn betrifft Maßnahmen, die von Einzelpersonen getroffen werden können, um sich auf eine solche Situation vorzubereiten. Dieser deckt sich mit den Erkenntnissen, welche die weiteren Teilnehmenden der „Tischgesellschaft“ formulieren. Auch hier dominiert das Fazit, sich mehr Gedanken über einen Blackout zu machen und dahingehende Absprachen in der Familie zu treffen beziehungsweise da, wo es möglich ist, vorzusorgen. Des Weiteren werden die Teilnehmenden versuchen, die neu gewonnenen Erkenntnisse in ihren beruflichen Alltag mit einfließen zu lassen.

Der von Seiten der FH OÖ identifizierte Erkenntnisgewinn durch die Beteiligung der Bevölkerung **für die Veranstalter*innen** liegt darin, dass diese Gruppe den Faktor „Mensch“ deutlicher in den Fokus rückt. Neben den Fragen, Sorgen und Nöten, welche die einfache Bevölkerung in einer solchen Situation beschäftigen (Sorge um Kinder, Wasser, Lebensmittel, Wärme, Information und Sicherheit) wird im Spiel deutlich, dass die Ressource der Mitarbeiter*innen ebenfalls eine kritische ist, da diese oftmals Familienväter und -mütter sind, die sich in Krisen- und Notsituationen zuerst um ihre Familie kümmern wollen. Insbesondere im Pflege- und Nahversorgungsbereich arbeiten viele Frauen, die zu Hause Betreuungspflichten haben und im Krisenfall als Mitarbeiterinnen eventuell nicht zur Verfügung stehen.

Die Erkenntnisse im Bereich **Diversität** sind vielschichtig. Grundsätzlich kann die Einbeziehung der Bevölkerung aus Sicht der FH OÖ im Rahmen des INDUCE Projektes positiv bewertet werden.

[37] https://kompetenzzentrum-sicheres-oesterreich.at/ksoe-blackout-planspiel-endergebnisse/

So konnten auf diese Weise nicht nur die Ziele des Projektes bekannt gemacht, sondern auch in Erfahrung gebracht werden, dass die Absicht, die Bevölkerung im Bereich Cybersecurity zu sensibilisieren und dahingehende Kompetenzen zu vermitteln, von Seiten dieser Gruppe als sehr sinnvoll und notwendig erachtet wird. Auch zeigt sich, dass innerhalb der Bevölkerungsgruppe trotz eines Übergewichts der männlichen Beteiligten (zwei Drittell der Beteiligten) keine Dominanz in den Entscheidungsfindungen und der Bereitschaft zur Präsentation der Ergebnisse zu verzeichnen war, sondern diese eher als ausgeglichen bewertet werden.

Allerdings kann auf Seiten der Veranstalter*innen ein noch unklar formuliertes **Erkenntnisinteresse** identifiziert werden. Liegt das Erkenntnisinteresse auf der Sichtweise und den Reaktionen der Bevölkerung, sollte über eine diversere/ inklusivere Zusammensetzung der Gesellschaftsgruppe nachgedacht werden. Im beschriebenen Spiel waren die Spieler*innen der „Tischgesellschaft“ ausnahmslos Berufstätige im Alter zwischen (etwa) 40-55 Jahren. Zusätzliche Diversität kann hier erreicht werden, indem weitere Gruppen wie zum Beispiel Studierende und Senior*innen sowie beeinträchtigte Personen und Migrant*innen eingeladen werden.

Liegt das Erkenntnisinteresse der Einbeziehung der Bevölkerung darin, diese zu befähigen, auf eine solche Krisensituation zu reagieren, sollten gezielt (Entscheidungs-)Vertreter*innen unterschiedlicher Berufssparten (Handwerk, Medien, Bildung) aus der Bevölkerung teilnehmen, um als Multiplikator*innen in ihren Bereich hineinzuwirken. Auch eine gesonderte Veranstaltung kann hier eine Lösung sein.

Weitere Erkenntnisse lassen sich im **organisatorischen Bereich** ausmachen. Hier wäre eine etwaige vorherige Einweisung der Bevölkerungsgruppe aus zwei Gründen in Erwägung zu ziehen. Einerseits herrschte Unklarheit darüber, was genau von der Bevölkerungsgruppe erwartet wird. Zu reflektieren wäre hier, ob die Teilnehmer*innen als Privatpersonen oder als Vertreter*innen ihrer jeweiligen Organisation auftreten. Da bei den Teilnehmer*innen der Bevölkerungsgruppe Privates und Öffentliches (Beruf, Verein, Interessenvertretung) mitunter stark verschmilzt, kann es zu Komplikationen in der Entscheidungsfindung kommen. Zusätzlich wurde deutlich, dass die Teilnehmer*innen die steuernde Simulation des AIT nicht wahrgenommen und in ihre Entscheidungen eingebunden haben.

5.3.3.4.2 Neues Übungskonzept

Neue Zielgruppe:

- Klein- und Kleinstunternehmer*innen, EPU, insbesondere in Gewerbe und Handwerk, Information und Consulting
- Insbesondere Klein- und Kleinstunternehmen, die finanziell nicht in der Lage sind, Fachpersonal zu beschäftigen, das für IT-Sicherheit im Unternehmen sorgt
- Personen, die einerseits Berührungsängste in Bezug auf IT-Themen haben oder denen bisher ein Bewusstsein über die Bedeutung von digitaler Sicherheit für ihr eigenes Unternehmen fehlt
- Es wird davon ausgegangen, dass die angesprochenen Nutzer*innen wenige bis gar keine Kenntnisse in diesem Bereich haben

Ziel der Übungen:

- Sensibilisierung für Sicherheitsthemen im (unternehmerischen) Umgang mit dem Internet
- Vermittlung von Basiskompetenzen, mit denen eine grundlegende IT-Sicherheit für das eigene Unternehmen aufgebaut werden kann

Anforderungen/ Requirements an die Übungen:

- Fokus auf Cybersicherheit und Cyber-Risiken in Klein- und Kleinstunternehmen
    - Sensibilisierung für mögliche Gefahren
    - Handlungsorientierte Übungen mit Praxisbezug, unmittelbare Umsetzung des Gelernten
- Nützliche Links/ Hinweise, wo zusätzliche Informationen/ Beratung/ Hilfestellung gefunden werden kann
- Niedrigschwelliger Zugang, Übungen müssen auch ohne Vorkenntnisse durchführbar sein
- Kleinformatige Übungen, welche die knappen Zeitressourcen der Zielgruppen berücksichtigen
- Gendergerechte, stereotypenfreie Sprache/ Darstellungen
- Einfache Sprache, Erklärung/ Vermeidung von Fachausdrücken
- Einfacher Zugang zur Übung
    - leicht auffindbar
    - technische Standardausrüstung
    - Gratis Angebot
- Inhalte und Beispiele müssen dem Nutzungskontext der Anwender*innen entsprechen

5.3.4 Best Practice-Beispiel „Cybersecurity Quiz"

Analyse-Instrument: Heuristik

Das Cybersecurity Quiz[38] von ovosplay erfüllt Großteils die Anforderungen, die das KSÖ an Cyberübungen für die neue Zielgruppe stellt. Das Angebot richtet sich an „alle Lernmotivierten ab dem Jugendlichenalter", kurz, Personen aus dem privaten und beruflichen Basisanwendungsbereich. Das **Ziel** des Quizzes umfasst sowohl die **Sensibilisierung** (awareness) für, als auch die **Vermeidung** (prevention), **Erkennung** (detection) und **Eindämmung** (containment) von Cyberrisiken.

Der **Zugang** zum Cybersecurity Quiz kann zum großen Teil als „**niedrigschwellig**" bezeichnet werden. Das Quiz kann über alle gängigen Smartphone-Betriebssysteme (Android, iOS) oder auch über Web erreicht werden. Es bedarf nur einer **minimalen technischen Ausrüstung** zur Durchführung der Übungen (Smartphone, Tablet, Notebook oder PC mit Internetzugang). Der niedrigschwellige Zugang bezieht sich zudem darauf, dass die Nutzer*innen **keine Vorkenntnisse** mitbringen müssen. Vielmehr wird der*die Leser*in der Website angespornt, das eigene Wissen im Bereich Datenschutz, Internetbetrug & Co. zu testen und ermutigt, die eigenen Kompetenzen zum Thema Internetsicherheit zu stärken. Auch **der geringe und flexible, individuell gestaltbare Zeitaufwand** trägt zur Herabsetzung einer möglichen Hemmschwelle bei. Jedes zu bearbeitende Modul ist mit einer **Zeitangabe** versehen, welche die voraussichtliche Bearbeitungsdauer (wenige Minuten) angibt. Als **Hindernis** kann sich eventuell die **notwendige Registrierung** (E-Mail-Adresse (optional), Passwort, Benutzername (Nickname möglich)) herausstellen.

Das Cybersecurity Quiz umfasst **zehn Module**, die verschiedene Themen im Bereich Cybersicherheit behandeln und sich inhaltlich am Digitalen Kompetenzmodell **DigComp 2.2 AT** orientieren[39]. Die zehn Themenbereiche umfassen dabei:

- Technische Bedrohungen

[38] https://ovosplay.com/cybersecurity-quiz; www.saferinternet.at/news-detail/neu-cyber-security-quiz/ Anbietende Organisationen: Cybersecurity Austria, Ovos, Saferinternet.at/ Österreichisches Institut für angewandte Telekommunikation, Fit4internet

[39] https://arbeiterkammer.at/ueberuns/zukunftsprogramm/zukunftsfonds/wien/DigComp_2.2_AT.pdf [18.06.2024]

- Datenschutz
- Sich vor Betrug schützen
- Einkaufen im Internet
- Cyber-Mobbing
- Fake News
- Smartphone
- Kinder sicher im Netz
- Home-Office und
- Urheberrecht

Nach der Registrierung (s.o.) können die Nutzer*innen, je **nach Nutzungskontext oder Interesse, frei wählen**, welche (Teil-)Module **in welcher Reihenfolge, Häufigkeit und Kombination** sie bearbeiten möchten. Jedes Themenmodul ist in weitere Untermodule, passend zu den jeweiligen Gefahren und Risiken in diesem Bereich, gegliedert. Dabei weist jedes Unterthema einen Entdeckungs-, Übungs- sowie Szenarioanteil auf, die in beliebiger Reihenfolge und Häufigkeit bearbeitet werden können. Im Entdeckerteil werden die Teilnehmer*innen (interaktiv) in die Gefahren und Schutzmaßnahmen des jeweiligen Sicherheitsthemas eingeführt. Die neu erworbenen Kenntnisse können im Übungs- und/ oder Szenarioteil getestet werden. Aber auch in diesen Teilen erfolgen immer wieder Erklärungen oder Hinweise in Bezug auf das richtige Verhalten in bestimmten Situationen. **Den Nutzer*innen werden auf diese Weise entsprechende Fachausdrücke vermittelt, Beispielsituationen beschrieben und praktische Handlungsanweisungen gegeben, die sich auf Sensibilisierung, Vermeidung, Erkennung und Eindämmung von Sicherheitsbedrohungen im Internet beziehen**. Nach jeder Bearbeitung eines Untermoduls erhalten die Teilnehmenden den Prozentanteil ihrer richtigen Antworten, den neuen Punktestand sowie die Anzahl gewonnener Karten, mit denen sie mit anderen Nutzer*innen Duelle austragen können. Die wachsende Punktezahl spornt zum Weiterspielen an.

Das Quiz überzeugt ebenfalls im Bereich der **visuellen und sprachlichen Gestaltung**. Die Abbildungen sind allesamt grafischer Art. Dabei werden **Männer und Frauen** nicht nur **in gleicher Häufigkeit** dargestellt, **auch in ihrer Tätigkeit** wird auf eine **stereotypenfreie, gleichwertige Darstellung** geachtet. Zusätzlich differiert die Hautfarbe der Personen, so dass hier visuell eine gewisse **kulturelle Diversität** erzeugt wird. Allerdings, entgegen der individuell auswählbaren Benutzer*innenprofile, sind hier keine Accessoires (wie kulturspezifische Kopfbedeckungen beispielsweise) sichtbar, die unterschiedliche kulturelle/religiöse Hintergründe berücksichtigen. Negativ zu bewerten ist ebenfalls, dass die Darstellungen in Körperbau, -haltung und -habitus allesamt an **junge Erwachsene** denken lassen und weder ältere Generationen noch physisch Beeinträchtigte abbilden. Wie bereits angedeutet, wird **in der Profilwahl eine breitere Diversität in Bezug auf Alter, kultureller/religiöser Hintergrund** gespannt. Hier können Teilnehmende entweder eigene Bilder einfügen oder aus einer Palette von 60 Porträtgrafiken (28 Frauen, 32 Männer, allerdings sind nicht alle Bilder eindeutig einem Geschlecht zuzuordnen) auswählen, die sich in Bezug auf Hautfarbe, Frisur, Alter (eingeschränkt, manche Personenabbildungen wirken älter, weil sie z.B. eine Glatze haben, Bart tragen o.Ä.), Kleidung oder Accessoires (Brille, Kopftuch) unterscheiden.

In der **Sprachverwendung** werden **durchgängig beide Geschlechter** genannt. Handelt es sich um Aufforderungen zur Fragenbearbeitung, wird die persönliche Anrede (Du) oder die Ich-Form gewählt. Da sich die kurzen Texte auf Informationsvermittlungen, Handlungsempfehlungen oder Szenarienbeschreibungen beschränken, kann hier **keine Aussage zu Werthaltungen** in diesen Texten gemacht werden. **Wichtige Fachausdrücke werden informierend und erklärend eingeführt**, um die Nutzer*innen damit vertraut zu machen. Zusätzlich wird das Quiz **in englischer und französischer Sprache** angeboten.

In Bezug auf die Ansprache der Zielgruppe durch Sprache und Bilder kann vermutet werden, dass sich vermehrt jüngere, aktiv im digitalen (Berufs-)Alltag stehende Generationen durch dieses Übungsformat angesprochen fühlen, weniger Personen im Senior*innenalter.

6 Handlungsempfehlungen und Maßnahmen für diversitätssensible Cyberübungen

6.1 Einleitung

Ziel 1: Entwicklung von diversitätssensiblen Cyberszenarien und Technologien in CÜ:

Gefordert wird die Untersuchung der Gestaltung und Umsetzung von Cyberübungen (CÜ). Insbesondere werden verschiedene Arten (z.B. handlungs- oder diskussionsbasiert) von CÜ auf Inhalte und deren Aufbau für verschiedene Zielgruppen (ZG) analysiert. Zudem werden nicht nur technische, sondern auch organisatorische Prozesse in Bezug auf Chancengerechtigkeit und Diversitätsdimensionen untersucht.

Ziel 2: Zugang zu praxisorientierten Cybersicherheitskompetenzen und -fähigkeiten für verschiedene ZG ermöglichen

Leitfragen:

„Welche Maßnahmen müssen nicht nur bezüglich Cyberszenarien, Technologien, Methodik und Didaktik getroffen werden, sondern auch für die Organisation von CÜ?“

„Wie können unterrepräsentierte Zielgruppen sukzessive an das Thema Cybersicherheitskompetenz und -fähigkeiten durch Cyberübungen herangeführt werden?“[40]

Ziel: ZG-spezifisches Design der Lehr- und Lerninhalte

Die **erwarteten Resultate** sind

1. die umfassende **Analyse der Literatur** und aktueller Cyberübungen unter dem Aspekt der Diversität und Chancengerechtigkeit (Kapitel 5.2). Die bereits im ersten Projektabschnitt erfolgte ausführliche Literaturrecherche wird kontinuierlich und bedarfsorientiert weitergeführt. Die Cyberübungen werden entlang demografischer, kognitiver, fachlicher, funktionaler und institutioneller Aspekte analysiert und mittels eines (de-)konstruktiven und intersektionalen Verständnis von Geschlecht und Differenz didaktisch angereichert und aufbereitet (T3.1)

und

2. Die strukturierten **Analysen von verschiedenen Arten von CÜ** und deren Auflistung nach potenziellen Zielgruppen (Kapitel 5.3). Mittels Fokusgruppeninterviews und Stakeholder*innen-Analysen werden die **Bedürfnisse der Zielgruppen** erhoben und mit dem aktuellen Format der Cyberübungen verglichen. Die Empfehlungen fließen in das **didaktische Design** ein und werden auf die Bedürfnisse und Interessenslagen der jeweiligen Gruppe abgestimmt (Kapitel 5.3.3). Um das Feld der aktuellen Nutzer*innen-Gruppe zu erweitern, wird daran gedacht, gezielt **unterrepräsentierte Gruppen zu adressieren**. Diese umfassen primär die Kategorien Gender, Alter und soziale Herkunft. Dabei werden auch die Marketing- und Disseminationsstrategie betrachtet und ggf. adaptiert (Kapitel 6.2).

- **Instrumente**: Fokusgruppen- und Expert*innen-Interviews, Teilnehmer*innen-Fragebogen, Heuristik, Beobachtungsleitfaden

Handlungsempfehlungen für chancengerechte Cyberübungen für Organisator*innen (Kapitel 6)

[40] Projektbeschreibung INDUCE, S. 24.

- Eine grundlegende **Analyse der Disseminationskanäle** und ggf. eine Anpassung an neue unterrepräsentierte Gruppen. Hier sollen Medien (z.B. soziale Medien) genutzt werden, die für diese Gruppen relevant sind. Jede Cyberübung sollte mit einem **zielgruppenspezifischen didaktischen Design** angereichert werden.
- **Instrumente**: Literatur- und ggf. Online-Recherche, Heuristik

6.2 Strukturierte Analyse von verschiedenen Arten von Cyberübungen

6.2.1 Einleitung

Wie bereits in Deliverable D3.2 dargelegt, konzentriert sich der Fokus der Analyse im Falle des Übungsangebots der CSA darauf, wie Rekrutierungs-, Unterstützungs- und Trainingsmaßnahmen zu verbessern wären, um mehr Diversität unter den Teilnehmer*innen zu erreichen. Zu diesem Zweck werden gezielt Expert*innen-Interviews durchgeführt sowie mithilfe quantitativer und qualitativer Erhebungsmethoden[41] Teilnehmer*innen und Coaches während der ECSC-Veranstaltung 2022 befragt, um den Status Quo sowie Ansatzmöglichkeiten zu ermitteln, wie in Zukunft eine breitere Diversität unter den Teilnehmer*innen erreicht werden kann. Es zeigt sich, dass unter den teilnehmenden Ländern ein großes Interesse an den Ergebnissen diesen Untersuchungen besteht. Ergänzend wird eine Literaturrecherche in Bezug auf Trainings- und Auswahlmodalitäten durchgeführt.

6.2.2 Ergänzende Literaturrecherche

Yamin et al (2021)[42] untersuchen in ihrer ersten Studie die **Selektions- und Trainingsstrategien** der nationalen Cybersecurity-Teams für den ECSC-Wettbewerb. Während des ECSC-Finales 2019 in Bukarest werden qualitative und quantitative Daten erhoben, um **Aussagen über die technischen, persönlichen und teambezogenen Eigenschaften potenzieller Kandidat*innen** für die Auswahl in das jeweilige nationale Team der befragten Länder (15 von 20) zu identifizieren. Darüber hinaus werden die verschiedenen **Trainingsstrategien und -plattformen** sowie die **Anzahl der Qualifikationsrunden** ermittelt. Es zeigt sich, dass für sechs der 15 Länder **nur technische Fähigkeiten** für die Aufnahme in das nationale Team entscheiden, erst in konkreter Vorbereitung auf das ECSC-Finale wird die Zusammenarbeit im Team fokussiert. Demgegenüber spielen **soziale und Teamfähigkeiten** für die anderen neun Länder zumindest für die endgültige Auswahl eine Rolle. Insgesamt haben die meisten Länder, mit Ausnahme von Tschechien, Spanien, Frankreich und Griechenland, **Schwierigkeiten, genügend Personen für die Wettbewerbe zu rekrutieren**. In Bezug auf die **Trainingsdauer** dominiert die Anzahl der Länder mit zwei Qualifikationsrunden und zwei Wochen Trainingszeit. Insbesondere der **Bedarf an standardisierten Trainings-Plattformen** ist hoch. Hier sind vor allem die Länder im Vorteil, deren monetäres Investment den Lizenz-Erwerb qualitativ hochwertiger Plattformen erlaubt.

Vor dem Hintergrund, dass zur Steigerung der Resilienz einer Gesellschaft gegen Cyberattacken nicht nur hoch qualifizierte Expert*innen benötigt und ausgebildet werden müssen, sondern es

[41] Vgl. Braun, V. & Clarke, V. (2006): Using thematic analysis in psychology. In: Qualitative Research in Psychology 3(2), pp.77-101. 2006. DOI: 10.1191/1478088706qp063oa.
Flick, Uwe (2009): Sozialforschung: Methoden und Anwendungen. Ein Überblick für die BA-Studiengänge. Hamburg: Rowohlt 2009.
[42] Yamin, M.M., Katt, B. & Torseth, E. (2021). Selecting and Training young Cyber Talent: A European Cybersecurity Challenge Case Study. In: Schmorrow, D.D. & Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2021. Lecture Notes in Computer Science (), vol 12776. Springer, Cham. https://doi.org/10.1007/978-3-030-78114-9_32.

auch genereller Maßnahmen des öffentlichen Bewusstseins für diese Gefahr bedarf, bewerten Yamin et al (2022)[43] den ECSC-Wettbewerb in diesem Zusammenhang als eine solche Maßnahme. Zu diesem Zweck nimmt deren, in Zusammenarbeit mit der ENISA entstandene, zweite Studie den **Auswahl- und Trainingsprozess** genauer unter die Lupe und entwickelt ein **allgemeines Modell, um den Reifegrad des CS-Systems in den jeweiligen Ländern zu bestimmen**. Dieses **TREE-Modell** bezieht das jeweilige nationale Bildungssystem mit ein und bildet eine dreistufige Organisationsstruktur nationaler Cybersecurity-Wettbewerbe zur Ausbildung und Rekrutierung einer für die jeweilige Gesellschaft notwendigen genügend großen Anzahl an Cybersecurity-Expert*innen ab. Der untere, breite „Wurzel"-Bereich adressiert dabei das **Zielpublikum in Volksschulen und Unterstufenklassen**, um generell die Teilnehmer*innen-Zahlen der nationalen Wettbewerbe zu erhöhen und ein allgemeines Bewusstsein für CS-Themen zu schaffen. Darauf aufbauend rekrutieren im „Stamm"-Level **Hochschulen und Universitäten mit MINT-Ausrichtungen** potenzielle Kandidat*innen für die Wettbewerbe, so dass auf der „Früchte"-Ebene **Expert*innen für Behörden, Wissenschaft und Industrie** abgegriffen werden können. Die Ansprache einer möglichst hohen Teilnehmer*innen-Anzahl im unteren Level soll so für einen kontinuierlichen Nachstrom im MINT-Bereich sorgen, da im Mittelbereich durch die Auswahl von Hochschulen und Universitäten mit MINT-Schwerpunkt bereits wieder ein großer Teil der potentiellen Interessent*innen außen vor bleibt.

Zudem wurden semistrukturierte Interviews mit Coaches und Team-Offiziellen während der ECSC 2021 geführt, an denen zwölf von 18 Ländern teilnehmen. Erfragt wird der **Qualifikationsprozess** des nationalen Teams, die **Anzahl der Qualifikationsrunden**, die **Anzahl der Teilnehmer*innen an den Qualifikations- und Finalrunden, die technischen, persönlichen und Team-bezogenen Fähigkeiten für eine Aufnahme in das nationale Team, der Trainingsprozess des ausgewählten Teams, die verwendeten Trainings-Plattformen sowie mögliche Verbesserungen in Bezug auf Selektion und Training**. Es zeigt sich, dass die Länder **sehr heterogene Auswahl- und Trainingsstrategien** verfolgen, was wiederum zu unterschiedlichen Resultaten im Wettbewerb führt. Daher sind die teilnehmenden Länder bestrebt, ihre nationalen Wettbewerbe insbesondere in den Bereichen der **Qualifikationsdauer**, den zu bewältigenden **Aufgaben** sowie im Hinblick auf eine **Steigerung der Diversität** zu verbessern.

Yamin et al (2022) zeigen unter Verwendung des TREE-Modells, dass insbesondere Italien und Frankreich über ein reifes Cybersecurity-System verfügen, um genügend Personen für das ECSC-Team zu gewinnen. Auch Belgien und Österreich können trotz ihrer geringen Bevölkerungsgröße eine beachtliche Teilnehmer*innen-Zahl erreichen. Die restlichen **Länder kämpfen damit, genügend viele Teilnehmer*innen zu rekrutieren, so dass, bezogen auf das TREE-Modell insbesondere die untere Stufe antizipiert werden muss**, um das Cybersecurity-Bewusstsein innerhalb der Bevölkerung sowie die Teilnehmer*innen-Anzahl zu steigern, wie dies am **Beispiel Tschechiens**, das mit 5700 Teilnehmer*innen an der Spitze liegt, ersichtlich ist[44].

Die European Union Network and Information Agency (**ENISA**)[45] greift die Studienergebnisse auf und fokussiert die **Heterogenität der Ausgangs-, Selektions- und Trainingsbedingungen**. Anhand einer eingehenden **Literaturrecherche** sowie 14 semi-strukturierten **Interviews** mit zwölf

[43] Yamin, M.M., Erdodi, L., Torseth, E. & Katt, B. (2022). Selecting and Training Young Cyber Talent: A Recurrent European Cybersecurity Challenge Case Study. In: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2022. Lecture Notes in Computer Science (). Vol 13310. Springer, Cham. https://doi.org/10.1007/978-3-031-05457-0_24.
[44] vgl. Yamin et al 2022, S. 319.
[45] European Union Agency for Cybersecurity ENISA (2021). T. De Zan & M M. Yamin: Towards a common ECSC Roadmap. Success factors for the implementation of national Cybersecurity competitions. DOI: 10.2824/657311.

Repräsentanten teilnehmender Länder und zwei EU-Vertretern und **Fragebögen** an nationale Repräsentant*innen des ECSC-Komitees werden **fünf Hauptziele von Cybersecurity-Wettbewerben und sechs Schlüsselfaktoren, um diese Ziele zu erreichen, identifiziert**[46].

Hauptziele von Cybersecurity-Wettbewerben:

- Identifikation junger CS-Talente
- Steigerung des Interesses an Cybersecurity als Thema an sich
- Steigerung des Wissens und der Fähigkeiten im Bereich der CS
- Steigerung des Interesses an CS-Karrieren und der Vernetzung von Teilnehmer*innen mit potenziellen Arbeitgeber*innen
- Schaffung eines Netzwerkes für junge CS-Expert*innen.

Hauptfaktoren, um diese Ziele zu erreichen:

- Politische Relevanz
- Regierung und Public Private Partnership
- Förderungen
- Öffentlichkeitsarbeit und Marketing-Strategien
- Organisation, Training und Cybersecurity Challenges
- Vernetzung mit potenziellen Arbeitgeber*innen und Karrierepfade.

Auf dieser Grundlage erstellt die ENISA einen Überblick des aktuellen Status der nationalen Cybersecurity-Wettbewerbe und analysiert diese Ergebnisse, um darauf aufbauend **Handlungsempfehlungen in Form einer allgemeine ECSC-Roadmap** vorzustellen, die sich an den identifizierten Schlüsselfaktoren orientieren.

6.2.2.1 ENISA Handlungsempfehlungen Öffentlichkeitsarbeit und Marketing

Im Hinblick auf das ausgewiesene Ziel der CSA, die **Steigerung der Diversität in Cybersecurity-Wettbewerben,** werden von den Handlungsempfehlungen zur Steigerung des Teilnehmer*innenfeldes vor allem die beiden Faktoren **„Öffentlichkeitsarbeit und Marketing-Strategie“** sowie **„Organisation, Training und Wettbewerb“** betrachtet und in der Folge auf INDUCE-Zwecke übertragen beziehungsweise adaptiert.

Im Bereich der **Öffentlichkeitsarbeit und des Marketings** empfiehlt die Roadmap, in Abstimmung mit der ENISA die nationale Öffentlichkeitsarbeit zu planen. Dabei sollte die zu entwerfende Strategie

- den Event medial unterstützen und so Cybersecurity-Awareness schaffen, potenzielle Teilnehmer*innen erreichen und die Anwerbungen steigern,
- Potenzielle Teilnehmer*innen adressieren und die Anwerbungen steigern,
- Sponsoren und das nationale Cybersecurity-System sichtbar machen,
- eine positive Erzählung zur Cybersecurity entwickeln und Stakeholder über Wettbewerbserfolge, als Stories aufbereitet, informieren sowie
- best practices in einem Repository sammeln und allen Ländern zur Verfügung stellen.

Um das **Cybersecurity-Bewusstsein auf nationaler Ebene** zu steigern und **mehr Teilnehmer*innen** für die Wettbewerbe zu rekrutieren, schlägt die ENISA in ihrer Roadmap drei aufeinander aufbauende Phasen vor. Zunächst sollte das **Interesse bei den 10-15-Jährigen** geweckt werden, vorzugsweise in Zusammenarbeit mit Schulen und als Teil des Lehrplans. In dieser Phase sollten der Spaß und spielerische Wettbewerbe im Vordergrund stehen. Der Fokus soll deutlich auf

[46] vgl. ENISA 2021, S. 2.

der Ausbildung eines breiten Interesses sowie der Ausbildung liegen. Die zweite Phase setzt bei den **16-22-Jährigen** an und basiert auf lokalen CTF (Capture The Flag)-Clubs, vorzugsweise in Zusammenarbeit mit nationalen e-Sport-Organisationen und Universitäten. Ziel dieser Phase ist die **kontinuierliche Wissenssteigerung**. Die dritte Phase für die **16-25-Jährigen** greift dann über den nationalen Horizont hinaus und fokussiert die **Cybersecurity-Elite** sowie Gewinner*innen der Wettbewerbe. Diese Phase sollte vor allem medienfreundlich gestaltet sein, um in den Massenmedien die **Sichtbarkeit** zu erhöhen. Dadurch bietet sich auch für die Sponsor*innen die Möglichkeit, Präsenz zu zeigen.

Unterstützt werden sollte dieses Vorgehen durch eine Strategie, welche die Cybersecurity einer breiten Öffentlichkeit zugänglich macht. Idealerweise geschieht dies durch die **Einbindung des Bildungssektors** und des nationalen Bildungsministeriums in die Informationsvermittlung über den nationalen Wettbewerb während der Qualifikationsphase sowie durch enge **Zusammenarbeit mit Hochschulen, Universitäten sowie dem öffentlichen und privaten Sektor**.

Realisieren lassen sich diese Ziele etwa durch **Forschungstage** an Universitäten, an denen der Bevölkerung die neuesten Cybersecurity-Technologien präsentiert werden, **Karrieretage** an öffentlichen und privaten Organisationen für Oberstufenschüler*innen und Studierende, um Interesse für Cybersecurity-Karrieren zu erreichen sowie **ECSC-Alumni-Treffen**, um Wissen, Erfahrungen und Möglichkeiten auszutauschen. Außerdem sollten an Schulen und Universitäten **attraktive Wettbewerbsplakate an prominenten Stellen** positioniert werden. Durch das **Bespielen von Social Media-Plattformen** mit Foto- und Video-Material sowie Live-Kommentaren und Erläuterungen technischer Details kann vor allem bei jungen Menschen Interesse geweckt und das Publikum während des Wettbewerbs mit einbezogen werden.[47]

6.2.2.2 ENISA Handlungsempfehlungen Organisation, Training und Wettbewerb

Im Hinblick auf die **Trainingsphase und den Ablauf des Wettbewerbs** rät die ENISA zu einem **niedrigeren Eingangslevel**, sodass **grundlegende Computerkenntnisse** zur Teilnahme ausreichend sind. Sollte dies möglich sein, ohne dass die Qualität und Ausrichtung des Wettbewerbs beeinträchtigt wird[48], können auf diese Art mehr Teilnehmer*innen gewonnen werden. Um diesen in der Folge auch genügend Zeit zu geben, Cybersecurity-Kenntnisse aufzubauen beziehungsweise zu erweitern, wird eine **lange oder mehrere kurze Qualifikationsrunden** vor der Auswahl der ECSC-Teams präferiert. Neben der Standardisierung der nationalen Wettbewerbe sollte gleichfalls eine **Standardisierung des nationalen Trainings** erfolgen, in der Dauer, Art, Inhalt und Zielgruppen definiert werden, um einer größtmöglichen Anzahl an Teilnehmer*innen zumindest für eine gewisse Zeit ein Training, und so die Cybersecurity-Kompetenzen einem breiteren Publikum zukommen zu lassen. Zusätzlich sollten Vorkehrungen, Richtlinien und Standards festgelegt werden, die sicherstellen, dass auch **nicht-qualifizierte Teilnehmer*innen über den Wettbewerb hinweg aktiv bleiben,** wie etwa in Österreich, Italien oder Rumänien. Zur Steigerung der Attraktivität von Cybersecurity-Karrierewegen und das Interesse an Cybersecurity als Thema an sich, schlägt die Roadmap vor, die **Karrierewege und -entwicklungen** ehemaliger Teilnehmer*innen **sichtbar** zu **machen**. Ferner sollten Maßnahmen zur **Steigerung der Gender-Diversität** getroffen werden.[49]

Zusammenfassung der ENISA-Empfehlungen:

- Eingangslevel senken (grundlegende Computerkenntnisse)
- Lange Qualifikationsrunde und Trainingsphase (Aufbau und Erweiterung von CS-Kenntnissen)

[47] vgl. ENISA 2021, Kap. 6.3, S. 44f.
[48] Anforderungen siehe: ENISA 2021: ECSC-Curricula. https://ecsc.eu/about/ecsccurricula.pdf.
[49] vgl. ENISA 2021, Kap. 6.4+6.5, S. 46-48.

- Einbindung nicht-qualifizierter Teilnehmer*innen in den ECSC
- Steigerung der Gender-Diversität
- Karrierewege und -entwicklungen sichtbar machen

6.2.3 INDUCE: Steigerung der Gender-Diversität

Zur Steigerung der Gender-Diversität in den Wettbewerben werden die identifizierten **Hauptziele** diesem Aspekt untergeordnet. Es gilt, Handlungsempfehlungen zu finden, um

- Junge weibliche CS-Talente zu identifizieren
- Interesse an CS als Thema unter Mädchen zu steigern
- CS-Wissen und -Fähigkeiten unter Mädchen zu steigern
- Interesse an CS-Karrieren unter Mädchen zu steigern
- Ein Netzwerk junger CS-Expert*innen zu schaffen

6.2.3.1 Ergebnisse Experten-Interviews

Die im Rahmen des INDUCE-Projektes durchgeführten Interviews bestätigen die oben dargestellten Ausführungen.

Am 13.12.2021 sowie am 18.02.2022 wurden von der FH OÖ **Experten-Interviews** mit einem Vertreter der CSA durchgeführt, um Aussagen über Ansatzmöglichkeiten zur Steigerung der Geschlechter-Diversität der Cybersecurity-Challenges zu ermitteln. Formuliertes Ziel der CSA ist die **Steigerung des Mädchenanteils in der Qualifikationsphase des nationalen Wettbewerbs auf 15-20%** („*Wenn wir es nachhaltig schaffen, den Anteil an Mädchen in der Challenge signifikant zu erhöhen und signifikant heißt für mich zwischen 15 und 20%*“). Der ideale Weg, um dieses Ziel zu erreichen, sei die **Einbindung der Schulen** („…*weil ich glaube, dass der Weg, dieses Ziel zu erreichen, a la longue nur über die Schulen, über die Lehrer geht*“). Die **Lehrkräfte als Multiplikator*innen** werden hier in einer entscheidenden Rolle gesehen („*Der Lehrer ist der erste Peer, der erste Mentor, der erste, der mit den Leuten arbeiten kann*“), müssen allerdings auch über entsprechende Kompetenzen verfügen und in dieser Aufgabe unterstützt werden („…*die Lehrer und Lehrerinnen müssen dabei unterstützt werden*“… „*Lehrer als Multiplikatoren sind äußerst wichtig; ist der Lehrer in Cybersecurity nicht fit, wird er dieses Thema auch nicht im Unterricht behandeln*“). Problematisch in diesem Zusammenhang ist, dass in Österreich „*Cybersecurity-Qualifikationen* […] *leider nicht im Curriculum verankert* [sind]“. Dadurch und durch den, wie sowohl die Recherche als auch die Selbstbeschreibung des Übungsformates der CSA in Kapitel 5 zeigt, bisherigen Fokus der CSA auf informationstechnisch ausgerichtete Ausbildungsstätten nehmen das Angebot der Challenge-Qualifikation im Klassenverband vor allem HTLs wahr („*hauptsächlich sprechen auf dieses Angebot HTLs an*“), so dass bereits in der Qualifikationsphase die **Teilnahmehürde für Mädchen größer** ist. Denn traditionell besuchen Mädchen seltener technisch ausgerichtete Schulen[50]. Dadurch können sie die Betreuung und Unterstützung durch Lehrer*innen nicht in Anspruch nehmen, erleben die Qualifikationsphase nicht als gemeinsames Event, sondern sind auf sich allein gestellt und auf die online-Hilfe der CSA angewiesen.

[50] Statistik Austria, Schulstatistik. Erstellt am 02.02.2023: Schulbesuch an berufsbildenden Schulen nach Fachrichtungen und Geschlecht in Prozent: Technisch gewerbliche Schulen: 27,3% Frauen,72,7% Männer. https://www.statistik.at/statistiken/bevoelkerung-und-soziales/gender-statistiken/bildung, (zuletzt aufgerufen am 02.05.2023).
Im Schuljahr 2020/21 besuchten insgesamt 18.078 Mädchen und 44.741 Jungen technisch-gewerbliche höhere Schulen. https://www.statistik.at/fileadmin/publications/BIZ_2020-21_Tabellenband.pdf.

Um diesem Problem Abhilfe zu verschaffen, wird von Seiten der FH OÖ angeregt, in der Qualifikationsphase einen **Teambewerb** anzubieten, da Frauen und Mädchen[51] in Themenbereichen, in denen sie sich unsicher fühlen beziehungsweise befürchten müssen, aufgrund stereotyper Vorstellungen beurteilt zu werden, die Arbeit im Team bevorzugen. Auch wenn die Auswertung von Teamqualifikationen bisher aufgrund fehlender Ressourcen nicht möglich ist („*Das ist in den Qualis schwierig, weil die natürlich alle online sind und sich da jeder allein zum Ziel kämpft…*"), wird der zugrunde liegende Gedanke positiv aufgenommen („[…] *eigentlich müsste man da schon an der Quali schrauben und sagen, es gibt eine Teambewerb-Quali*"; „*Grundsätzlich glaube ich schon, dass man mit einem Teambewerb in der Quali Hürden senken kann*"). Weitere Möglichkeiten bieten sich laut CSA-Experte mit **eigenen Challenge-Veranstaltungen** für junge Frauen und Mädchen sowie eigenen Frauentrainingsgruppen.

Um Mädchen und Frauen grundsätzlich für Cybersecurity-Themen zu interessieren, werden **Ansätze über Nicht-Security-Themen** diskutiert, wie zum Beispiel die Ansprache durch „*Testimonials, die jetzt nicht aus der Security-Blase stammen*", um den Aspekt des Quereinstiegs auszuschöpfen („…*vielleicht sogar der große Vorteil* [….] *weil sie da zumindest gleichwertig mit allen anderen starten* […] *es ist vielleicht im Zuge dieses ‚Ich wachs dort hinein' oder ‚Ich schau mir das einmal an' angenehmer, wenn das starke Persönlichkeiten sind*"). Hier gilt es, **Türöffner-Themen** zu finden, wie zum Beispiel Escape-Room-Spiele, die mit den Anforderungen der Wettbewerbe vergleichbar sind („…, *wenn Du in dieser Escape-Room-Thematik steckst, und Dir das gefällt und Du im Team an dem löst, bist Du vielleicht eh relativ schnell bereit, einmal diesen virtuellen Escape-Room zu probieren und da kommst Du zwangsläufig dann mit dem in Berührung, auch virtuell ums Eck zu denken*…"). Auch die Entwicklung von **online Tutorials** wird angedacht, „…*wo jeder für sich selber einmal probieren kann, im Idealfall auch sehr schnell Erfahrungen macht, die ihn bestätigen und bekräftigen, mit dem Thema weiterzumachen, aber in die andere Richtung genauso schnell vielleicht sagen, und das ist glaube ich auch wichtig: ist nicht meins, weil*…").

Es zeigt sich, dass bereits nach kurzer Projektlaufzeit ein Bewusstsein dafür geschaffen wurde, dass mit einer **zielgruppenspezifischen Kommunikation** viel erreicht werden kann („…*dann natürlich, dass die Gesamt-Kommunikation völlig falsch läuft bei uns und das Interessante ist, nicht nur bei uns in Österreich*"). Die Frage ist „… *wie kommunizieren wir die Challenge speziell für Frauen? Welche Angebote machen wir für Mädchen, um teilzunehmen, die Challenge als Leuchtturm zu nutzen, um überhaupt Frauen einmal dorthin zu bringen?*". In diesem Zusammenhang wird auch die **Zusammensetzung des Organisationsteams** angesprochen und die Erkenntnis, dass auch hier Diversität vonnöten ist, um I-Methodology zu vermeiden, denn „…*es ist so, wir leben ja in unserer Blase und glauben, sicher, die denken auch so, nein, das ist es nicht* […] *wenn nur Männer darüber nachdenken: da adaptiert man eben ein Modell, das bei uns funktioniert, einfach für Mädchen* […] *es geht allen so, warum, weil sie* [die Challenge, Anm.] *überall von Männern konzipiert und entwickelt worden ist*".

6.2.3.2 Ergebnisse Leitfaden-Interviews

Neben einer Fragebogen-gestützten Teilnehmer*innen-Befragung wurden durch INDUCE-Projektmitarbeiter*innen während des ECSC-Finales im September 2022 in Wien Leitfaden-Interviews mit den Team-Coaches der teilnehmenden Länder vor Ort durchgeführt. Die Fragen weisen geschlossene, halboffene und offene Antwortformate[52] auf und dienen der Erhebung und dem Vergleich der nationalen Anstrengungen zur Steigerung der Diversität innerhalb der Teams im Hinblick auf

[51] Und vice versa auch Männer und Jungen in Bereichen, die nach gängigen Vorstellungen eher Frauenspezifisch sind: vgl. Vancouver, J. B., & Ilgen, D. R. (1989). Effects of interpersonal orientation and the sex-type of the task on choosing to work alone or in groups. Journal of Applied Psychology, 74(6), 927-934. https://psycnet.apa.org/doi/10.1037/0021-9010.74.6.927, (zuletzt aufgerufen am 23.05.2023).
[52] Vgl. Flick 2009; Braun & Clarke 2006.

best practices und Verbesserungsmöglichkeiten. Inhaltlich beziehen sich die Fragen auf **Aspekte der Organisation, Teilnehmer*innen-Anzahl und -Verteilung, Werbung, Rekrutierung sowie Maßnahmen zur Förderung von Diversität**.

Die Aussagen der Befragten bestätigen auch hier die Ausführungen der ENISA Roadmap und die Arbeiten von Yamin et al. Auf die Frage, wie hoch der geschätzte **Anteil an weiblichen Teilnehmerinnen** am nationalen Wettbewerb ist, gaben lediglich Tschechien und die USA Werte über 30% an. Am häufigsten (sechs von 26 Antworten) wurde der Anteil weiblicher Teilnehmerinnen auf **5% oder darunter** geschätzt, Anteile von weniger als 10% respektive 15% wurden jeweils von drei Ländern genannt, während nur zwei Länder (Slowenien und Italien) Anteile zwischen 15% und 20% erreichen. Fünf Länder erheben dazu keine Daten oder verfügen über keine nationalen Wettbewerbe und vier Team-Coaches machten zu dieser Frage keine Angaben. Luxemburg und Dänemark traten jeweils mit rein männlichen Teams an, wobei Dänemark zusätzlich auf das Problem hinwies, dass sie zwar etwa 15% weibliche Interessentinnen während der Trainingsphasen hatten, diese allerdings verloren, sobald der Wettbewerb startete.

Auf die Frage, welche Aspekte verbessert werden sollten, um mehr Teilnehmerinnen für den nationalen Wettbewerb zu motivieren, wurden ebenfalls Punkte genannt, die bereits oben angesprochen wurden. 32% (neun von 28) der Befragten gaben an, dass **weibliche Vorbilder** hier einen wichtigen Beitrag liefern könnten, knapp 18% (fünf von 28) bestätigten, dass Mädchen bereits in der **Schule** für IT oder IT-Security interessiert werden müssten. Auch **eigene Veranstaltungen** für Mädchen und Frauen wie etwa eigene Trainingsgruppen wurden mit knapp 18% (fünf von 28) häufig genannt („*that they get the feeling from success*“). Mit knapp 11% (drei von 28) waren sich die Befragten jeweils darin einig, dass das **Selbstbewusstsein** der Mädchen und Frauen gestärkt werden muss, eine **positive Atmosphäre** in der Challenge entscheidend ist und eine Änderung der **Kommunikation und Bildsprache** erfolgen sollte („*less hackish selection of images*“). Weitere Aussagen legten Wert auf **Diversität bereits in der Organisation** („*the steering committee should be a mixture*”), die Verstärkung der **Sichtbarkeit des Events** (“*more exhibits and more outreach to different communities*”), das zu weckende Interesse („*get them interested in cyber, then in games*”) oder regten eigene **Frauennetzwerke** für die Cybersecurity an.

16 der 28 (> 57%) befragten Länder verfügen über **spezielle Initiativen, um die Anzahl der Teilnehmerinnen zu steigern**. Die bisherigen Erkenntnisse zeigen, dass Schulen hier eine zentrale Rolle einnehmen, um die Jugendlichen zu erreichen und es entscheidend ist, die Mädchen **bereits im Volksschulalter** für Cybersecurity zu interessieren. Denn, wenn sie älter sind, haben sie bereits andere Interessen entwickelt und sind damit für die Cybersecurity verloren („*we have to start from the first grade (seven years old) – they are already choosing their hobbies – later girls are behind*“; „*when they are 16 it´s too late*“. Eigene Programme, um **weibliche Lehrkräfte als Role Models oder Multiplikatorinnen** zu identifizieren und zu unterstützen, weisen allerdings nur neun der befragten Länder auf. Dabei weist Dänemark zusätzlich auf das Problem hin, dass, auch wenn es solche Programme gibt, es **zu wenige weibliche Professorinnen** in diesem Bereich gibt („*but the problem is that they have so few female professors in Cybersecurity*“). Diese Aussagen korrelieren mit den Angaben zur Frage, ob die antretenden Nationen weibliche Coaches in ihrem Team haben. Mehr als 46% (13 von 28) haben zumindest eine Frau im Team, diese nimmt allerdings meistens administrative Aufgaben wahr (Organisation, Unterstützung, Finanzen, Management, Kommunikation, Beobachtung oder freiwillige Teilnahme)[53]. Hier sticht allein Tschechien heraus, das einen Anteil weiblicher Coaches von 40% aufweist.

[53] Auf diesen Aspekt wurde auch bereits von INFRAPROTECT hingewiesen, siehe dazu 2. Zwischenbericht, Kap.5.

6.2.3.3 Zusammenfassung

Die Herausforderungen, die sich für die Ausrichtenden des österreichischen nationalen Wettbewerbs stellen, liegen insbesondere in der Tatsache, dass der Bildungssektor nicht in gleichem Umfang in die Wettbewerbsstruktur eingebunden ist, wie dies zum Beispiel in Tschechien der Fall ist. Tschechien verfügt nicht nur mit mehr als 5000 über die meisten Teilnehmer*innen (dicht gefolgt von Italien mit mehr als 4000) in der ersten Qualifikationsrunde, sondern mit mehr als 30% auch anteilsmäßig über die meisten weiblichen Teilnehmerinnen (trotz fehlender Diversity-Ausrichtung). Dies kann erreicht werden, weil **Tschechien** eine **breit gefächerte Disseminations-Strategie** verfolgt, die fünf unterschiedliche Kanäle adressiert. Insbesondere wird der Wettbewerb gezielt an Schulen einschließlich staatlichen und regionalen Institutionen beworben. Auch ehemalige Teilnehmer*innen, deren Freund*innen und Kontakte sind in der Weiterverbreitung von Wettbewerbs-Informationen aktiv. NGOs wiederum sprechen gezielt Lehrer*innen an, die wiederum die Informationen an ihre Schüler*innen weitergeben und soziale Netzwerke sowie die nationalen Medien wie TV und Radio sorgen für eine breit gefächerte Informationsweitergabe.[54]

Zwar ist in Österreich die Vermittlung digitaler Kompetenzen in allen Schulstufen verbindlich im Lehrplan verankert und richtet sich nach den Vorgaben des digitalen Kompetenzmodells digi.komp[55]. Die Teilnahme am nationalen ACSC wird allerdings nicht schulübergreifend beworben, sodass die Möglichkeit, die Qualifikationsphase im Klassenverband, unter Hilfestellung und Motivation der Lehrenden, durchzuführen, primär von Schulen mit IT-Schwerpunkten genutzt wird. Da diese Schulen traditionell ohnehin nur einen geringen Mädchenanteil aufweisen (siehe oben), kann auf diese Weise die Genderdiversität unter den Wettbewerbsteilnehmenden nur schwer gesteigert werden. Vielmehr ist die Hürde für interessierte Mädchen, die keine der teilnehmenden Schulen besuchen, zusätzlich höher, weil sie auf keine unmittelbare Hilfe zurückgreifen können, sondern, im Fall von Schwierigkeiten, eine eventuell angebotene „fremde“ Hilfe online hinzuziehen müssen. Hier ist zu vermuten, dass die Hemmschwelle, diese zu nutzen, sehr groß ist, beziehungsweise, dass bereits ein sehr großes Interesse an Cybersecurity und eine entsprechende Motivation vorhanden sein muss, um allein diese Qualifikationsphase zu durchlaufen und zu absolvieren.

6.3 Handlungsempfehlungen zur Steigerung der Geschlechter-Diversität

Dennoch lassen sich aus der ergänzenden Literaturrecherche sowie den Interview-Ergebnissen mögliche Ansatzpunkte und Handlungsempfehlungen zur Steigerung der Geschlechter-Diversität im nationalen Wettbewerb für INDUCE-Zwecke ableiten, von denen einige bereits in der Projektphase umgesetzt werden.

6.3.1 Handlungsempfehlungen Organisation, Training und Wettbewerb

Für die Aspekte Organisation, Training und Wettbewerb können einige INDUCE-spezifische Handlungsmaßnahmen identifiziert werden:

Niedrigere Eingangslevel in der Qualifikationsphase und längere Trainingsdauer: Auf diese Weise können auch Personen mit weniger ausgeprägten Cybersecurity-Fähigkeiten, aber vorhandenem Anfangsinteresse an der Qualifikation teilnehmen, ohne sofort an ihre Grenzen zu stoßen. Wird diese Phase mit Spiel- und Knobelfreude sowie positiven Gefühlen verbunden (erfolgreiche absolvierte Challenges), kann nicht nur das Interesse an Cybersecurity an sich gesteigert werden,

[54] Vgl.: ENISA 2021, S.26.
[55] Vgl. BM für Digitalisierung und Wirtschaftsstandort Abt. I/A/3 (Hrsg.) (2021): Digitales Kompetenzmodell für Österreich. DigComp 2.2 AT. Wien 2021.

sondern durch eine längere Trainingsphase können auch Fähigkeiten und Kenntnisse in einer breiteren Bevölkerungsschicht ausgebaut werden. Zusätzlich wird die Wahrscheinlichkeit erhöht, dass angemeldete Teilnehmer*innen, auch im Falle einer Nicht-Qualifizierung, sich für die Austragung des ECSC interessieren und weiter aktiv bleiben.

Neues, **eigenes Trainingsformat für Mädchen/ Frauen**: Da spielerische Events wie Cyberwettbewerbe vor allem solche Teilnehmer*innen anziehen, die bereits über ein breites Cybersecurity-Wissen verfügen, werden Neulinge, die nicht aus dem klassischen Cybersecurity-Feld kommen, eher abgeschreckt, was sich durch einen hohen Dropout äußert[56]. Ein eigenes Trainingsformat für Frauen kann hier helfen, einer unter Leistungsdruck sich negativ auswirkenden Selbststereotypisierung entgegenzuwirken[57]. Insbesondere im Team lassen sich Aufgaben meistern, die Frauen sich allein oder in Männer-dominierten Gruppen nicht zutrauen[58]. Auf diese Weise können Barrieren abgebaut, Wissen aufgebaut sowie Erfolgserlebnisse und damit Selbstvertrauen gefördert werden.

- Im Rahmen des INDUCE-Projektes wird dieser Ansatz konkretisiert und ein eigenes Trainingsformat für Frauen und Mädchen ab Mai 2023[59] angeboten, in dem Interessierte im Team und unter Anleitung für die anstehende Austria Cybersecurity Challenge (ACSC) trainieren können.
- Orientierung als **Best Practice** bietet hier Italien, das zwar kein eigenes Trainingsformat für Frauen aufweist, allerdings umfassende Trainingsmöglichkeiten auf der Homepage anbietet, so dass Interessierte mithilfe von Aufgaben aus früheren Challenges üben und sich selbst anhand der zur Verfügung gestellten Lösungen kontrollieren und so verbessern können.

6.3.2 Handlungsempfehlungen Öffentlichkeitsarbeit und Marketing

Ein weiterer, umfassender Ansatz, um Cybersecurity-Awareness in der breiten Bevölkerung zu erhöhen und insbesondere potenzielle Teilnehmerinnen zu erreichen, ist der Ausbau beziehungsweise die **gender-sensible Gestaltung der Öffentlichkeitsarbeit und des Marketings**. Auch hier legen die Interviews sowie die Literaturrecherche zahlreiche Möglichkeiten offen, wie der Event medial unterstützt, das nationale CS-System sowie die Sponsoren sichtbar gemacht und positive Erzählungen zur CS und deren Akteur*innen aufgebaut werden können.

Eine **Änderung der Kommunikation sowie eine gezielte Ansprache von Mädchen und Frauen auch in der Bildsprache** lässt erwarten, dass die gewünschte Zielgruppe darauf anspricht. Hier gilt es nicht nur, die Zielgruppe direkt zu adressieren, sondern auch **weibliche Vorbilder** zu identifizieren und Mädchen und Frauen in der IT-Sicherheit insgesamt sichtbarer zu machen. Es wird erwartet, dass insbesondere eine **verstärkte Präsenz und Wahrnehmung von Frauen** einen Beitrag dazu liefert, das Cybersecurity-Feld in dieser Hinsicht zu erweitern[60]. Auf diese Weise können

[56] Vgl. Tobey, D.H., Pusey, P. & Burley, D.L. (2014): Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League. Acm Inroads 2014, Vol.5 (1), 53-56, hier: S. 55f. DOI: 10.1145/2568195.2568213S.
[57] Vgl. Pusey, P., Gondree, M. & Peterson, Z. (2016): The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations. In: IEEE Security & Privacy, Vol. 14(6), 90-95. DOI: 10.1109/MSP.2016.119.
De Pater, I. E., Van Vianen, A. E. M., Fischer, A. H., & Van Ginkel, W. P. (2009). Challenging experiences: Gender differences in task choice. Journal of Managerial Psychology, 24(1), 4-28. DOI:10.1108/02683940910922519.
[58] Vgl. Vancouver & Ilgen 1989.
[59] https://verbotengut.at/news/acsc-2023-hackerinnen-team-kick-off/.
[60] Vgl. Coenraad et al (2020): Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. In: Simulation & Gamin 2020, Vol 51(5), S. 586-611, hier: S. 605. DOI: 10.1177/1046878120933312.

auch **Karrierewege und -entwicklungen** aufgezeigt werden, um das Interesse an Cybersecurity zusätzlich zu erhöhen.

Eine weitere Möglichkeit, die (Geschlechter-)Diversität unter den Teilnehmenden und den Pool der Interessent*innen an sich zu vergrößern, bietet die **Betonung der multi-disziplinären Natur**[61] und der sozioökonomischen Dimensionen von Cybersecurity anstelle der bisher stark fokussierten technischen Aspekte. Cybersecurity-Expert*innen benötigen neben grundlegenden IT-Skills ein breites Set an Fähigkeiten, das Kompetenzen wie kritisches Denken, Teamfähigkeit, Kommunikation sowie Kenntnisse in Ethik und Recht miteinschließt[62]. Insbesondere Frauen dienen fachfremde Expertisen als Türöffner in das Cybersecurity-Feld, wie Interviews von Frauen aus dem Cybersecurity-Sektor in Norwegen belegen[63].

Um mehr Frauen und Mädchen zu erreichen, sollte die **Außenwirkung des Events** reflektiert und Hacker-Stereotype sowie die militärisch angehauchte Selbstdarstellung reduziert werden. Hier bieten die **Niederlande**[64] ein **Best Practice** und adaptierbares Beispiel, wie der **Event mithilfe eines Video-Blogs als Gemeinschaftserlebnis** dargestellt und in den Rahmen einer **positiven Erzählung** eingebettet werden kann: Ein Kamerateam mit einem gut gelaunten Moderator begleitet das ECSC-Team der Niederlande mit täglichen Berichten in Form von Kurzvideos von der Abreise über die Teilnahme bis zur Ankunft zuhause. Hierbei wird der **Wettbewerb als Event** hervorgehoben, der mit **Teamgeist**, spannenden **Herausforderungen und Spaß** verbunden ist. Zahlreiche Interview-Partner*innen werden vor die Kamera geholt und geben **interessante Einblicke** in die Vorbereitungen, den Ablauf sowie **Hintergrundinformationen und Erklärungen**. Dadurch können interessierte Nicht-Teilnehmer*innen die Veranstaltung via YouTube oder Instagram verfolgen. Formate wie dieses bieten zusätzlich die Möglichkeit, **Sponsor*innen sichtbar** zu machen und **Personen, die sich nicht qualifiziert haben, dennoch mit einzubinden**, indem sie zum Beispiel bei den Dreharbeiten und Interviews mitarbeiten, Blogs erstellen, fotografieren uvm.

- Die Cybersecurity Austria unternimmt bereits zahlreiche Schritte, um den nationalen und internationalen Wettbewerb zu promoten. Neben aktiver Pressearbeit zu aktuellen Events ergehen auch Einladungen an (Hoch-)Schulen, unterstützt durch Promoter*innen als dezentrale Zellen sowie die Aktivierung ehemaliger Teilnehmer*innen. Mailing-Nachrichten via Bildungsministerium werden ebenfalls an Schulen ausgesendet. Während der IKT-Sicherheitskonferenz erfolgt die Informationskommunikation über das BMLV. Unterstützt werden diese Bemühungen durch Posts in Social-Media-Kanäle sowie über die eigene Homepage[65].
- Im Rahmen des INDUCE-Projektes konnte zudem ein weiterer Schritt unternommen werden, indem ein **eigenes Werbeposter für Mädchen** (Hacker*innen gesucht)[66] unter Berücksichtigung einer zielgruppenspezifischen Ansprache konzipiert wurde. Insbesondere Poster haben den Vorteil, dass sie sowohl online als auch an prominenten Stellen wie zum Beispiel Schulen Sichtbarkeit erzeugen und Interesse wecken können.

[61] Vgl. Shumba et al (2013): Cybersecurity, Women and Minorities: Findings and Recommendations from a Preliminary Investigation. ITiCSE-WGR´13 June 29-July 3, 2013, Canterbury, England, UK, S. 4. DOI: 10.1145/2543882.2543883.
[62] Vgl. Oliver, J.Y. & Elwell, C. (2018): Effective Competitions for Broadening Participation in Cybersecurity. 2018 ASEE Zone IV Conference: Boulder, Colorado, Mar 25. Paper ID #24157. https://peer.asee.org/29608 (zuletzt aufgerufen am 05.06.2023).
[63] Vgl. Corneliussen, H.G. (2020). What brings women to cybersecurity? A qualitative study of women´s pathways to cybersecurity in Norway. EICC 2020: Proceedings of the European Interdisciplinary Cybersecurity Conference. November 2020, 9, pp. 1-2. DOI: 10.1145/3424954.3424965.
[64] https://challengethecyber.nl/, zuletzt aufgerufen am 02.05.2023.
[65] https://verbotengut.at/.
[66] CSAU23-11821_CSC-Poster_03_RZ_ah.indd (verbotengut.at), zuletzt aufgerufen am 26.04.2023.

6.3.3 INFRAPROTECT

6.3.3.1 Einleitung

Am 17.02.2023 konnte das geplante Interaktionsspiel mit internationalen Austauschstudent*innen im Rahmen der Welcome Week am Campus Hagenberg der FH OÖ durchgeführt werden. Hintergrund dieses Programmpunktes war die sich im ersten Projektjahr entspannende Diskussion um männliche und weibliche Führungspositionen. Die These der INFRAPROTECT lautete, dass, in gemischt-geschlechtlichen Teams, in denen keine bestehenden Hierarchien existieren, die Emanation von Führungsrollen geschlechtsunabhängig ist. Diese These sollte im Spiel untersucht werden.

Dazu wurden die Teilnehmer*innen vorab über die Aufzeichnung des Spiels via Kamera informiert. Diese wurden nach Durchführung des Spiels den Teilnehmenden präsentiert und erklärt und nach der Auswertung wieder gelöscht. Alle Teilnehmer*innen erklärten sich mit ihrer Unterschrift mit einer Aufzeichnung einverstanden.

Die Studierendengruppe setzte sich aus 12 internationalen Student*innen zusammen, die sich an diesem Tag erst kennen gelernt hatten. Die Mitspielenden versammelten sich in einem großen freien Saal ohne jegliche Stolpersteine (wie Möbel etc.). Nach einer Einführung durch die Spielführer der INFRAPROTECT, in der das Ziel des Spiels und die Aufgabe der Teilnehmenden, innerhalb von 15-20 Minuten mittels Zurufen und Überlegen ein Quadrat zu bilden, erläutert wurden, wurde das etwa 40 Meter lange Seil ausgebreitet und die Studierenden erhielten eine Augenbinde. Einem willkürlich ausgewählten Spieler wurde daraufhin ein Seilende in die Hand gegeben. Mit der Aufforderung, die Augenbinden aufzusetzen, startete das Spiel.

6.3.3.2 Beobachtung

Die Interaktionen in Form von sprachlichen und nichtsprachlichen Handlungen wurden anhand des Videomaterials dokumentiert, transkribiert und anhand des aufgestellten Beobachtungsleitfadens ausgewertet. Entsprechend konnten folgende Häufigkeitsverteilungen ermittelt werden:

- Verteilung Männer: Frauen?
  - M7: F5
- Häufigkeit der Anweisungen/ Kommandos von Männern/ Frauen?
  - M: 10 Anweisungen/ Kommandos
  - F: 21 Anweisungen/ Kommandos
- Häufigkeit der Vorschläge von Männern/ Frauen?
  - M: 10
  - F: 3
- Häufigkeit opponierender (Ja, aber…) Beiträge von Männern/ Frauen?
  - M: 6 Einwände/ Bedenken
  - F: 1 Einwand/ Bedenken
- Häufigkeit kontraproduktiver Beiträge von Männern/ Frauen?
  - Keine!
- Häufigkeit unterstützender/ bestätigender Beiträge von Männern/ Frauen?
  - M: 22
  - F: 31
- Anzahl aktiver/ passiver Teilnehmer*innen? M/F-Verteilung?
  - Aktiv: 2 M, 2 F
  - Passiv: 3 M, 1 F
  - Teilweise aktiv: 2 M, 2 F

Die ermittelten Rollen, die einzelne Teilnehmer*innen während des Spiels eingenommen haben (aktiv, passiv, teilweise aktiv), wurden ebenfalls beschrieben und näher ausgeführt.

Die Beobachtung zeigt eine positive Gruppendynamik im Sinne der Kooperationsfähigkeit und des Führungsverhaltens in der Gruppe. Es überwiegt ein ruhiges, andere Teilnehmende respektierendes und abwartendes Verhalten.

Insgesamt kann ein ausgewogenes Geschlechterverhältnis in Bezug auf die Übernahme von Führungspositionen, Interaktionen sowie der Verteilung aktiver, passiver und teilweise aktiver Spieler*innen attestiert werden.

Während des Spiels kristallisiert sich eine weibliche Führungsrolle heraus, die in der Folge die Gruppe anleitet und auch von dieser akzeptiert wird. Dies wird deutlich, da auch andere aktive Teilnehmer*innen, die selbst koordinierende Funktionen ausüben, Rücksprache mit dieser Spielerin halten beziehungsweise Bestätigung des eigenen Vorgehens von ihr erwarten. Allerdings fällt auf, dass sich diese Führungsrolle erst etabliert, als bereits das strategische Vorgehen feststeht und die (männliche) Person, die zunächst die Leitung übernimmt, Unsicherheit ausstrahlt.

Bei der Festlegung des strategischen Vorgehens heben sich die Spieler*innen hervor, die auch im weiteren Verlauf eine aktive Rolle durch ihre koordinierenden Verhaltensweisen einnehmen.

Es zeigt sich ferner, dass die (ebenfalls männliche) Person, die von den Spielleitern das Seilende in die Hand gedrückt bekommt, eine gewisse Verpflichtung verspürt, sich aktiv in das Spiel einzubringen und die Gruppe anzuleiten. In der beobachteten Gruppe ist dies insbesondere in der Anfangs- und Endphase zu erkennen, in der der „Leader“ aktiv den Spielprozess in Gang bringt und ebenso beendet und dies von den Mitspieler*innen akzeptiert wird.

Die doppelt so hohe Anzahl an Anweisungen von weiblichen Teilnehmern gegenüber denen der männlichen lässt sich mit der weiblichen Führungsrolle erklären. Im Gegensatz dazu werden Handlungsvorschläge überwiegend von Männern eingebracht (Verhältnis etwa 3:1). Auch in der Häufigkeit der Einwände überwiegen eindeutig die Beiträge der Männer gegenüber der von Frauen (Verhältnis 6:1). Auffällig ist, dass kontraproduktive, störende Beiträge nicht beobachtet werden, auch wenn es Handlungsvorschläge gibt, die nicht umgesetzt werden.

6.3.3.3 Fazit

Die Tatsache, dass sich die Teilnehmer*innen untereinander nicht kennen, hat zur Folge, dass es auch keine etablierten Hierarchien gibt. Aus diesem Grund müssen sich die einzelnen Rollen und Funktionen im Spiel erst herausbilden. Auf diese Weise ist eine für die zu untersuchende These ideale Teilnehmer*innen-Basis gegeben.

Die Multikulturalität und damit auch die Multilingualität der Gruppe zwingt die Teilnehmer*innen zur Kommunikation in Englisch. Es ist zu vermuten, dass sich die Spieler*innen hierdurch noch einmal zusätzlich auf wesentliche Punkte der Kommunikation konzentrieren und längere Diskussionen eher vermeiden.

Für INDUCE-Zwecke und vor dem Hintergrund der Diskussion um traditionelle Rollenverständnisse von Männern und Frauen lässt sich beobachten, dass sich in dieser künstlichen Spielsituation ein ausgewogenes Verhältnis zwischen Männern und Frauen in Bezug auf aktives und passives sowie führendes, koordinierendes oder unterordnendes Spielverhalten und damit Rollenverständnis entwickelt. Diese Beobachtung ist insbesondere dahingehend interessant, dass, im Gegensatz zu an anderen Zeitpunkten durchgeführten Spielen mit homogenen und strukturierten Gruppen (im militärischen oder behördlichen Kontext), die Führungspositionen in der Regel von Männern eingenommen werden, die diese Funktion auch im jeweiligen Umfeld innehaben (Führung durch den

Stärkeren). Darüber hinaus fällt auf, dass der Spielerfolg (Formierung eines Quadrats gelingt) dieser multikulturellen, inhomogenen, hierarchisch nicht strukturierten Gruppe der gleiche ist wie der eines homogenen, hierarchisch geordneten, eingespielten Teams. Insofern kann die Eingangs-Hypothese bestätigt werden.

7 Design und Spezifikation diversitätssensibler Szenarien und Inhalte in Cyberübungen

7.1.1.1 Cyberübungen

Bedrohungen im Cyberraum haben in den letzten Jahren kontinuierlich zugenommen. Unternehmen, Privatpersonen und auch staatliche Einrichtungen sehen sich mit einer steigenden Anzahl an Angriffen sowie mit gezielteren und besseren Angriffsmethoden konfrontiert. Der Internet Organised Crime Threat Assessment (IOCTA) Bericht (Europol, 2021) zeigt jedes Jahr die Beurteilung der aktuellen Bedrohungslage im Cyberraum. Erfolgreiche Angriffe auf Unternehmen und Privatpersonen können existenzbedrohende Folgen verursachen, wenn z.B. sensible Daten verloren oder gestohlen werden. Noch gravierendere Konsequenzen können Angriffe auf kritische Infrastrukturen (z.B. Krankenhäuser, Stromversorger, Mobilfunkbetreiber, etc.) mit sich ziehen, da sie der Bevölkerung sehr sensible Leistungen zur Verfügung stellen, deren Ausfälle bis zum Verlust von Menschenleben führen können. Ein schockierendes Beispiel zeigt ein Cyberangriff auf drei ukrainische Stromversorger im Dezember 2015, wodurch die gesamte Stromversorgung einer Region für drei Stunden ausfiel (E-ISAC, 2016).

Um solche Situationen zu vermeiden, sollten IT-Systeme die neuesten Sicherheitstechnologien verwenden, sowie durch kontinuierliche Wartung immer am aktuellen Stand gehalten werden. Konkrete Handlungsempfehlungen für einen stabilen IT-Grundschutz werden zum Beispiel vom deutschen Bundesamt für Sicherheit in der Informationstechnik gegeben (BSI, 2020). Jedoch können Cyberangriffe auch dadurch nicht zu 100% verhindert werden. Einerseits besteht immer ein Restrisiko für bisher unentdeckte Sicherheitslücken in Software, die von Angreifenden ausgenutzt werden, bevor die Herstellerfirma darauf reagieren kann, andererseits spielt der Faktor Mensch eine sehr wichtige Rolle in der Gewährleistung von Sicherheit. Denn auch die beste und neueste Sicherheitssoftware ist nahezu machtlos gegenüber Personen, die aufgrund mangelnden Bewusstseins schadhafte Software auf ihren Geräten ausführen. Daraus lassen sich folgende zwei Schlussfolgerungen ziehen:

1. Trotz hervorragender Sicherheitsvorkehrungen und aktueller Software, müssen IT-Sicherheitsbeauftragte mit Angriffen rechnen und die Fähigkeiten und Erfahrung besitzen diese zu entdecken und abzuwehren, oder den Schaden möglichst gering zu halten.
2. Alle Personen, die Zugriff auf schützenswerte IT-Systeme haben, sollten gegenüber Cybergefahren sensibilisiert werden, um Bewusstsein zu generieren und nicht unbeabsichtigt schadhaft zu handeln.

Die Umsetzung dieser beiden Anforderungen stellt eine sehr herausfordernde Aufgabe dar. Einerseits ist es sehr schwer, Fähigkeiten und Erfahrungen im Erkennen und Abwehren von Angriffen zu erlangen, wenn man einen solchen noch nie erlebt hat, andererseits ist es ebenso schwer Bewusstsein und Sensibilität für ein Thema zu entwickeln, ohne jemals einen derartigen Vorfall und dessen Auswirkungen erlebt zu haben.

Zur Lösung dieser Herausforderungen wurden sogenannte „Cyberübungen“ entwickelt, die in den letzten Jahren sehr populär wurden und mittlerweile fester Bestandteil moderner Cybersicherheitsstrategien sind. Konkret versteht man darunter, dass zum Beispiel ein Cyberangriff in einer möglichst realistischen Trainingsumgebung simuliert wird. Dadurch werden praktische Erfahrungen in einer sicheren Umgebung ermöglicht und somit erfahrungsbasiertes Lernen sowie die Bewusstseinsbildung gefördert.

7.1.2 Definitionen und Konzepte

Cyberübungen ermöglichen es, reale Cyberszenarien zu simulieren, um den Teilnehmenden gewünschte Inhalte zu vermitteln und somit Lerneffekte zu erzielen. Dazu können unterschiedlichste Ziele verfolgt werden, die dazu führen, dass Cyberübungen in vielen Ausführungsvarianten existieren. Um die Vielfalt von Cyberübungen aufzuzeigen, werden folgend ein paar Beispiele für mögliche Ziele angeführt:

- Die technischen Fähigkeiten von IT-Sicherheitsbeauftragten im Erkennen und Abwehren von Cyberangriffen verbessern.
- Die Durchführung bestehender unternehmensinterner Notfallprozesse, um sie auf ihre Anwendungsfähigkeit im Ernstfall zu überprüfen und gegebenenfalls anzupassen.
- Das Bewusstsein für alltägliche Cybergefahren und deren möglichen Folgen stärken.
- Die im Ernstfall notwendige Kommunikation, sowohl unternehmensintern als auch mit externen Stellen, überprüfen und verbessern.

Dieser Ausschnitt an möglichen Zielen zeigt die breite Anwendungsmöglichkeit von Cyberübungen. Übungen, die fundamental unterschiedliche Ziele verfolgen, unterscheiden sich auch fundamental in ihren Anforderungen und daher in ihrer Durchführungsart. Diese vorhandene Diversität führt auch dazu, dass der Begriff „Cyberübung“ sehr umfangreich ist und nicht direkt auf die Art der Übung schließen lässt. Daher nutzen Organisationen den Begriff auch unterschiedlich und unterscheiden sich in ihren Definitionen. In folgendem Abschnitt werden daher einige Definitionen unterschiedlicher Organisationen mit den zugehörigen Referenzen erläutert.

7.1.2.1 Definitionen

Nachfolgend werden einige Definitionen für Cyberübungen und deren Mehrwert von bekannten Organisationen erläutert:

Nationales Institut für Standards und Technologie (NIST):

„*a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan*“ (Grance et al., 2006)

Finnische Agentur für Verkehr und Kommunikation (TRAFICOM):

„*an event in which the organization models and tests its preparedness for various cyber incidents*“ (TRAFICOM, 2020)

Führungsakademie der Schwedischen Gesamtverteidigung (FOI):

„*a tool for raising Cybersecurity awareness and train people to handle different situations in a controlled cyber environment“* (Wilhelmson & Svensson, 2011)

Organisation des Nordatlantikvertrags (NATO):

„*cyber exercises have been playing a very important role in testing the technical cyber capacity of nations or organizations, cyber training, and cyber awareness*“ (Seker & Ozbenli, 2018)

Bundesamt für Sicherheit in der Informationstechnik (BSI):

„Übungen trainieren die in den Plänen beschriebenen Abläufe, schaffen routinierte Handlungsabläufe und verifizieren die effiziente Funktionalität der Lösungen.“ (BSI, 2008)

Auf Basis dieser Definitionen lassen sich unterschiedliche Inhalte von Cyberübungen ableiten. Es werden Verben wie „validieren“, „testen“ und „trainieren“ verwendet und mit Kompetenzen wie „IT-Pläne“, „Vorbereitung auf Cybernotfälle“, „technische Fähigkeiten“, „routinierte Handlungsabläufe“

und „Cyberbewusstsein“ verbunden. Daraus lässt sich ableiten, dass Cyberübungen das sehr generische Ziel verfolgen, jegliche zur Abwehr von Cyberangriffen notwendige Kompetenz zu validieren und zu trainieren, um somit die Cyberverteidigung zu verbessern. Der breite Umfang einer stabilen Cyberverteidigung führt allerdings auch dazu, dass Cyberübungen ein sehr umfangreiches Themengebiet abdecken. Daher wird im nächsten Kapitel eine mögliche Klassifizierung zur Unterscheidung von Cyberübungen vorgestellt.

7.1.2.2 Klassifizierung

Die unterschiedlichen Cyberübungsziele führen auch zu gänzlich verschiedenen Ausführungsvarianten von Übungen. Um diese Typen einordnen zu können, werden folgend unterschiedliche Kategorien vorgestellt, welche die Klassifizierung von Cyberübungen erlauben. Dazu haben wir uns zu einer Einordnung entlang der Kategorien „angreifend oder verteidigend“, „diskussionsorientiert bis aktionsorientiert“ und „Übung oder Wettkampf“ entschieden, welche folgend im Detail erklärt werden.

7.1.2.2.1 Verteidigend oder angreifend

Wie bereits definiert, handelt es sich bei Cyberübungen um Events zum Testen und Trainieren der Cyberverteidigung. Nichtsdestotrotz gibt es die Möglichkeit Cyberübungen für die Teilnehmenden in unterschiedlichen Perspektiven zu gestalten. In der verteidigenden Perspektive nehmen die Teilnehmenden ihre klassische Rolle ein und versuchen simulierte Angriffe bestmöglich abzuwehren. Im Gegensatz dazu, kann es trotzdem auch hilfreich sein, einmal in die angreifende Perspektive zu schlüpfen und sich Gedanken darüber machen, wie man die eigene oder eine fremde Infrastruktur bestmöglich attackieren kann. Diese gewonnene Erfahrung erlaubt eine differenzierte Blickweise auf Angriffe und kann dabei helfen in den gewöhnlichen „Verteidigungspositionen“ ein größeres Bewusstsein für das Handeln der Angreifenden zu entwickeln.

Je nachdem in welcher Perspektive sich Teilnehmende einer Übung befinden, wird die jeweils andere Perspektive von den Übungsorganisationsteam simuliert. Jedoch ist auch eine Mischform möglich, indem Übende in der angreifenden Perspektive Infrastrukturen attackieren, die von Übenden in der verteidigenden Perspektive abgewehrt werden müssen.

7.1.2.2.2 Diskussionsorientiert bis aktionsorientiert

Cyberübungen können je nach Typ zwischen diskussionsorientiert und aktionsorientiert unterschieden werden. Diskussionsorientierte Übungen fokussieren sich auf theoretische Aufgabenstellungen, welche die Teilnehmenden durch Diskussionen zwischen unterschiedlichen Rollen oder mit Teammitgliedern zu lösen versuchen. Dabei können Abläufe, Prozesse, Entscheidungen, Kommunikationswege, Zusammenhalt und vieles mehr getestet und trainiert werden, ohne tatsächlich auf technische Details einzugehen. Aktionsorientierte Übungen erfordern im Gegensatz dazu explizit technische Aktionen der Teilnehmenden. In einer rein aktionsbasierten Übung lösen die Übenden technische Aufgabenstellungen, um somit ihre technischen Fähigkeiten zu verbessern.

Cyberübungen müssen allerdings nicht eindeutig einer der beiden Kategorien zugeordnet werden, es handelt sich dabei eher um eine Skala, anhand welcher der Grad der Verteilung zwischen Diskussionsorientierung und Aktionsorientierung definiert wird (z.B. eine Übung ist zu 80% diskussions- und zu 20% aktionsorientiert). Um einen hohen Grad an Realismus in Übungen zu erreichen, ist natürlich eine Mischung aus Diskussion und Aktion notwendig, da auch in einem tatsächlichen Notfall sowohl technische Gegenmaßnahmen als auch der korrekte Ablauf von Prozessen und Kommunikation notwendig ist.

7.1.2.2.3 Übung, Wettkampf oder Schulung

Obwohl Cyberübungen den Begriff „Übung“ schon im Namen tragen, können diese auch explizit als Wettkampf oder Schulung organisiert werden. In einer reinen Übungs- und Schulungsumgebung werden keine Bewertungsmaßnahmen getroffen, oder zumindest nicht dazu verwendet, um die Leistung unterschiedlicher Teams gegeneinander zu vergleichen. Im Wettkampf werden konkrete Leistungsparameter genutzt, um teilnehmende Teams zu bewerten und eine Rangliste zu führen.

Auch wenn eine Cyberübung reinen Übungscharakter hat und nicht das Ziel verfolgt ein siegendes Team zu küren, werden oftmals Wettkampfkomponenten wie definierte Parameter zur Leistungsmessung und auch Ranglisten in die Übung integriert, um die Motivation zwischen den Teams zu steigern und somit den Lernerfolg zu erhöhen.

7.1.2.3 Typen

Um die Vielfalt der Lernziele von Cyberübungen zu adressieren, wurden bereits eine Vielzahl an Übungstypen entwickelt, die zwar unter eigenständigen Namen bekannt, allerdings trotzdem dem Begriff „Cyberübung“ zuzuordnen sind. In diesem Kapitel sollen Beispiele für Typen erläutert und anhand der Kategorisierung des vorhergehenden Kapitels eingeordnet werden[67]. Selbstverständlich können nicht alle Cyberübungen ganz klar einem der folgenden Typen zugeordnet werden. Es gibt teilweise Überlappungen und je nach Übungsziel sind dem Design einer Übung keine Grenzen gesetzt, wodurch auch kreative Mischformen genutzt werden können.

7.1.2.3.1 Cyber Defense Exercise (CDX)

Spricht man im Allgemeinen von einer „Cyberübung“, ohne näher auf den Typ der Übung einzugehen, wird darunter am ehesten die sogenannte „Cyber Defense Exercise“ (CDX) gemeint. In der CDX nehmen die Übenden die verteidigende Rolle ein und müssen eine virtuelle Infrastruktur in einem vordefinierten Szenario gegen die Angreifenden verteidigen. In einer CDX kann man zwischen unterschiedlichen Teams unterscheiden, die bei der Durchführung der Übung unterschiedliche Aufgaben erledigen und anhand von Teamfarben identifiziert werden (Seker & Ozbenli, 2018).

1. *Blue Team.* Das Blue Team ist das verteidigende Team und besteht daher in einer CDX aus den Übenden. Sie sind dafür zuständig, die ihnen zur Verfügung gestellten virtuellen Systeme bestmöglich zu schützen und gegen Angriffe zu verteidigen. Die Anordnung eines oder mehrerer Blue Teams ist dabei frei wählbar. Man kann den Mitgliedern zum Beispiel Rollen zuteilen, um somit die tatsächlichen Strukturen und Aufgaben einer Organisation (oder einer oder mehrerer Abteilungen) darzustellen.
2. *Red Team.* Das Red Team ist das angreifende Team. Sie folgen dem Szenario, sowie dem Fortschritt des Blue Teams und greifen deren virtuellen IT-Systeme zu passenden Zeitpunkten an. Dazu haben sie die Erlaubnis, vorpräparierte Schwachstellen in den Systemen des Blue Teams zu nutzen.
3. *White Team.* Das White Team repräsentiert die Übungsleitung. Sie sind vor der Übung bereits dafür zuständig, die Lernziele zu definieren und das Szenario zu entwickeln. Während der Übung soll das White Team den Szenarioablauf mit Blick auf die Lernziele steuern und gegebenenfalls anpassen. Zusätzlich soll das White Team den Überblick bewahren und mit allen anderen Teams interagieren, um einen reibungslosen Ablauf zu gewährleisten.
4. *Yellow Team.* Das Yellow Team ist dafür zuständig, während der Übung das Bewusstsein für die aktuelle Situation darzustellen. Dafür beobachten und befragen (z.B. durch Fragebögen) sie die Blue Teams zu deren Fortschritt und berichten die Resultate an das White

[67] Die Einordnung der Typen stellt keinen allgemein gültigen Standard dar, sondern wurde von uns im Zuge dieses Deliverables entworfen.

Team. Zusätzlich können sie auftretende Fragen der Blue Teams beantworten und somit zu jedem Zeitpunkt für Klarheit sowohl beim Blue als auch beim White Team sorgen.

5. *Green Team.* Das Green Team ist für die Bereitstellung und Wartung der Übungsinfrastruktur zuständig. Das beinhaltet sowohl die Systeme des Blue Teams als auch jene des Red Teams. Zusätzlich können weitere Systeme Teil einer Übung sein, die dann ebenso in den Aufgabenbereich des Green Teams fallen (z.B. Szenario-Management, Monitoring, Bewertung, etc.).

Die Farben der Teams haben sich zu einem „Standard“ entwickelt, der auch in anderen Übungstypen genutzt werden kann. Speziell die markanten Farben Rot und Blau, die das angreifende und verteidigende Team darstellen, werden vielfach verwendet. Daher wird die CDX, aber auch andere Übungstypen, in denen es ein angreifendes und verteidigendes Team gibt, auch oft „Red Team / Blue Team Exercise“ genannt.

Eine CDX durchläuft ein vordefiniertes Szenario, dessen Inhalt maßgeblich zum Erfolg einer Übung beiträgt. Das Szenario wird nach Festlegung der Lernziele entwickelt und soll die zu testenden oder zu trainierenden Gegenmaßnahmen des Blue Teams auslösen. Das Szenario kann zwar fiktive Elemente enthalten, sollte aber nichtsdestotrotz möglichst realistisch sein, um den Teilnehmenden das Gefühl zu geben, sich in einer realen Situation zu befinden, um somit auch wahre Gegenmaßnahmen auszulösen und die Motivation zu steigern. Ein Szenario könnte zum Beispiel folgendermaßen aussehen:

> *Im IT-Netz kommt es zu einigen Ransomware-Vorfällen. Rechner von Mitarbeitenden werden infiziert was unter anderem dazu führt, dass ein Netzwerk-Share verschlüsselt wird. Die infizierten Rechner werden zudem blockiert. Die Ransomware wird von den Angreifenden auch als Sprungbrett (Remote Callback Shell[68] – ein Programm, das eine Verbindungen zu den Angreifenden hält, um Befehle entgegenzunehmen) ins Firmennetz verwendet. Über einen infizierten Administrator*innen-Rechner erhalten die Angreifenden Zugriff auf verschiedene Firmen-Server. Über den Datenverarbeitungsserver ist der Sprung ins sichere Firmen-Netz möglich. Die Angreifenden beginnen die Firma zu erpressen und drohen mit dem Veröffentlichen von geheimen Firmendaten sowie einer irreparablen Beschädigung der Server.*

Die Umsetzung des Szenarios während der Übung erfolgt in Form von Einspielungen die „Injects“ genannt werden. Ein Inject repräsentiert jegliche Information oder Aktion, die innerhalb des Szenarios an das Blue Team übergeben oder getätigt wird. Es kann sich dabei um E-Mails, Angriffe, Bilder, Videos, Diagramme, Dateien, Manipulationen und vieles mehr handeln. Injects bilden also die Grundlage zur Ausführung des Szenarios, und helfen dabei das Szenario im gewünschten Umfang zu halten. Bei Injects kann es sich zum Beispiel um folgende Aktionen handeln:

1. Das Red Team nutzt eine Schwachstelle und installiert eine infizierte Datei auf einem System eines Blue Teams.
2. Eine Person des Blue Teams bekommt eine E-Mail einer unbekannten Adresse, in welcher sie nach den Zugangsdaten zum VPN ihrer Organisation gefragt wird.
3. In einer TV-Meldung wird über die Erpressung der Organisation berichtet.

[68] Eine Remote Callback Shell ist eine Methode, mit der ein Angreifer oder Administrator remote (also aus der Ferne) Zugriff auf ein Zielsystem erhält, indem das Zielsystem selbst eine Verbindung zu einem vom Angreifer oder Administrator kontrollierten Server herstellt. (siehe auch https://de.wikipedia.org/wiki/Remote_Shell)

Einordnung:

Verteidigend. Teilnehmende bei einer CDX nehmen die verteidigende Perspektive ein und versuchen Angriffe zu verhindern oder deren Auswirkung zu verringern.

Mischung aus Diskussions- und Aktionsorientierung. Der Grat zwischen Diskussions- und Aktionsorientierung einer CDX ist vom Organisationsteam frei wählbar und hängt von den Lernzielen ab. Legt man den Fokus auf die technische Beantwortung von Angriffen, ohne Interaktionen und Prozesse zu forcieren, wird man einen eher aktionsorientierten Typ wählen. Liegt der Fokus auf der Durchführung von Prozessen und der Einhaltung von Kommunikationsrichtlinien im Notfall, wird man einen eher diskussionsorientierten Typ wählen. Ist eine CDX allerdings rein diskussionsorientiert ohne technische Grundlage, wäre die Übung eher einer Table-Top Exercise (siehe nächsten Abschnitt) zuzuordnen.

Übung. Grundsätzlich handelt es sich bei einer CDX um eine Übung. Nichtsdestotrotz versuchen einige Organisationen Bewertungsmechanismen in ihre Übungen zu inkludieren, um die Leistung der Teams festzustellen und die Motivation zu steigern.

7.1.2.3.2 Table-Top Exercise (TTX)

Der Begriff „Table-Top Exercise“ (TTX) ist nicht nur im Kontext mit Cyberübungen präsent. TTXs werden schon seit vielen Jahren in vielen verschieden Branchen (z.B. Militär, Wirtschaft, Politik, Bildung) genutzt und sind dabei zumeist unter der Bezeichnung „Planspiel“ bekannt (Kriz, 2009). Es handelt sich dabei um einfache Übungen, bei denen ein simuliertes Szenario an die Teilnehmenden herangetragen wird, welches gewünschte Interaktionen, Diskussionen und Prozesse auslösen soll. Dabei können zwar keine technischen Fähigkeiten trainiert werden, dafür liegt der Fokus stärker auf der Einhaltung von Richtlinien, Prozessen und notwendiger Kommunikation im Ernstfall.

In der TTX bildet, wie auch bei einer CDX, ein vorab entwickeltes, möglichst realistisches Szenario die Grundlage der Übung. Das Szenario wird in Form von Injects an die spielenden Teams herangetragen. Das Szenario-Beispiel der CDX kann inhaltlich auch in einer TTX angewendet werden, wobei sich die Injects allerdings voneinander unterscheiden. Da die technische Grundlage fehlt, um Injects „tatsächlich“ zu übermitteln (also z.B. einen Angriff in Form eines tatsächlichen Angriffs), bekommen die Übenden lediglich die Information, dass eine Aktion stattgefunden hat. Mögliche Injects sind:

1. Sie haben eine Phishing-E-Mail bekommen.
2. Sie haben auf einem IT-System eine schädliche Datei gefunden.
3. Ihre Anti-Virus-Software hat eine Warnung gesendet, als die E-Mail einer Partnerinnenfirma geöffnet haben.

Die Teamzusammensetzung in TTXs kann wie bei CDXs, je nach den Trainingszielen, frei gewählt werden. Übende können zum Beispiel unterschiedliche Rollen einnehmen, um die Hierarchie einer Organisation oder Abteilung abzubilden. Es können aber auch mehrere kleine Teams ohne klare Rollenzuteilung definiert werden, um lediglich Diskussionen auszulösen und mögliche Lösungsvorschläge für Probleme zu erarbeiten.

Einordnung:

Verteidigend. In TTXs im Kontext von Cyberübungen nehmen Übende die verteidigende Perspektive ein und versuchen durch Diskussion und Kommunikation vorgegebene Prozesse und Richtlinien zu trainieren und zu testen.

Diskussionsorientiert. TTXs sind rein diskussionsorientierte Übungen, ohne jeglichen Einfluss aktionsorientierter Komponenten.

Übung. TTXs sind reine Übungen zur Simulation von Szenarien, ohne Wettkampfcharakter oder den Fokus auf das Training von spezifischen Tools.

7.1.2.3.3 Capture the Flag (CTF)

Ein „Capture the Flag“ (CTF) ist ein Übungstyp, in dem die teilnehmenden Teams oder Einzelpersonen auf einer bereitgestellten, fremden IT-Infrastruktur sogenannte „Flags“ suchen müssen. Dazu müssen sie moderne Angriffstechniken verwenden, um Schwachstellen in den geschützten Systemen zu finden und dort nach den Flags suchen zu können. Bei „Flags“ handelt es sich um eine Kombination aus Buchstaben, Zahlen und Sonderzeichen, die man dem Organisationsteam übermitteln kann, um zu beweisen, dass die Flag gefunden wurde. Somit können die technischen Fähigkeiten zum Attackieren eines IT-Systems trainiert werden, um somit auch in der verteidigenden Perspektive einen besseren Überblick zu haben, wie Angriffe durchgeführt werden könnten.

Einordnung:

Angreifend. Die Teilnehmenden in einem CTF nehmen die angreifende Rolle ein, und versuchen in bereitgestellte IT-Infrastrukturen „einzudringen“, um dort nach den Flags suchen zu können.

Aktionsorientiert. CTFs sind aktionsorientierte Events, die lediglich auf die Durchführung technischer Aktionen abzielen. Diskussionsorientierte Komponenten wie Kommunikation oder Prozesse spielen dabei keine Rolle.

Wettkampf. CTFs werden in Wettkampfform ausgeführt. Teams oder Einzelpersonen haben eine gewisse Zeitspanne, in jener sie die Infrastruktur attackieren können. Wer am Ende die meisten Flags gesammelt hat, gewinnt den CTF.

7.1.2.3.4 Cybertraining

Cybertrainings bestehen aus technischen Aufgaben, welche die Übenden lösen sollen, um so ihre technischen Fähigkeiten zu verbessern. Dazu befinden sie sich meist einzeln in einer virtuellen Trainingsinfrastruktur. Anhand des Trainingsprogramms werden Aufgaben gestellt, die sowohl verteidigender als auch angreifender Natur sein können. Je nach Ausgestaltung des Trainingsprogramms, können darin auch Szenarien und Hintergrundgeschichten enthalten sein, um das Training spannender zu gestalten.

Verteidigend oder angreifend. Ein Cybertraining kann sowohl verteidigende als auch angreifende Aufgaben enthalten.

Aktionsorientiert. Cybertrainings sind aktionsorientiert und zielen auf das Trainieren der technischen Fähigkeiten ab.

Übung oder Schulung. Cyber-Trainings werden in Form von Übungen oder Schulungen abgehalten. Der Erfolg der Übenden kann zwar bewertet werden, diese Bewertung zielt allerdings auf keinen Wettkampf mit anderen Übenden ab.

7.1.2.3.5 Cyberwettkampf

Ein Cyberwettkampf findet, ähnlich wie eine CDX, auf virtuellen Systemen statt. Dabei werden allerdings sowohl das Blue, als auch das Red Team, von den Übenden gespielt. In einem typischen Cyberwettkampf haben zwei (oder mehrere) Teams identische Infrastrukturen, die sie vor Angriffen des gegnerischen Teams verteidigen und gleichzeitig das andere Team angreifen sollen. Es gibt den Cyberwettkampf allerdings auch in vielen anderen Ausführungsvarianten. Zum Beispiel kann es auch ein rein angreifendes und ein rein verteidigendes Team geben. Der Kreativität sind dabei keine Grenzen gesetzt. Die Herausforderung bei Cyberwettkämpfen ist es, eine faire Umgebung zu schaffen, in der keines der Teams benachteiligt ist.

Verteidigend und angreifend. Übende sind sowohl in der verteidigenden als auch in der angreifenden Perspektive zu finden.

Aktionsorientiert. Cyberwettkämpfe zielen lediglich auf die technische Umsetzung von einerseits verteidigenden Maßnahmen und andererseits Angriffen ab.

Wettkampf. Teams spielen gegeneinander und versuchen das jeweils andere Team zu besiegen. Die Art und Weise der Bewertung ist dabei der Übungsorganisation zu überlassen.

7.1.2.3.6 Die Kategorisierung der Übungstypen im Überblick

Übungstyp	Verteidigend oder angreifend	Diskussionsorientiert oder aktionsorientiert	Übung, Wettkampf oder Schulung
CDX	verteidigend	Mischform zwischen beidem	zumeist Übung
TTX	zumeist verteidigend	diskussionsorientiert	Übung
CTF	angreifend	aktionsorientiert	Wettkampf
Cybertraining	zumeist verteidigend	aktionsorientiert	Übung oder Schulung
Cyberwettkampf	beides	aktionsorientiert	Wettkampf

7.1.3 Lerneffekte

Cybersicherheitsbedrohungen stellen für kleine und mittlere Unternehmen (KMU) eine zunehmende Herausforderung dar. Trotz der oft beschränkten IT-Ressourcen sind KMUs zunehmend auf digitale Technologien angewiesen, wodurch das Risiko von Cyberangriffen steigt. Gleichzeitig zeigt die Forschung, dass der menschliche Faktor eine der größten Schwachstellen in der Cybersicherheit darstellt (Anderson, 2006). Cyberübungen in sicheren, simulierten Umgebungen, sogenannten Cyber Ranges, bieten eine innovative Methode zur Vermittlung von Cybersicherheitskompetenzen. Während sich diese Übungen traditionell an technisch affine Zielgruppen wie SOCs, NOCs oder CERTS richten, werden zunehmend Ansätze entwickelt, die auch weniger technikaffine Nutzer, insbesondere in KMUs, ansprechen sollen (Furnell, 2023).

Cyber Ranges bieten realitätsnahe Simulationen von IT-Infrastrukturen, in denen Angriffe und Verteidigungsstrategien unter kontrollierten Bedingungen getestet werden können. Diese Plattformen ermöglichen es den Teilnehmenden, praktische Erfahrungen zu sammeln und dabei die theoretischen Grundlagen der Cybersicherheit zu vertiefen (Chouliaras, 2021). In Bezug auf die Zielgruppe der KMU-Mitarbeitenden und nicht-technisch affinen Nutzenden ist jedoch eine Anpassung der Übungsinhalte und -methoden notwendig, um sicherzustellen, dass relevante Kenntnisse und Fähigkeiten vermittelt werden.

Forschungsergebnisse zeigen, dass praktisches Lernen, wie es in Cyber Ranges ermöglicht wird, besonders effektiv ist, um komplexe Themen wie Cybersicherheit zu vermitteln (Chouliaras, 2021), (Akpan, 2020). Durch interaktive Szenarien, die reale Bedrohungen simulieren, können Lernende die Relevanz der Theorie in der Praxis direkt erfahren. Für KMU-Mitarbeitende, die in der Regel nicht über technisches Fachwissen verfügen, sind praxisnahe Lernansätze von besonderer Bedeutung. Die Erfahrung, in einer simulierten Umgebung eine Bedrohung zu erkennen und darauf zu reagieren, fördert nicht nur das Verständnis für Cyberbedrohungen, sondern auch das Bewusstsein für die eigene Rolle in der Sicherheit der Unternehmensinfrastruktur.

Traditionell konzentrieren sich Cyberübungen auf spezifische technische Fähigkeiten, die in hochspezialisierten Rollen wie in einem Security Operations Center (SOC) benötigt werden (Jahankhani, 2021). Für nicht-technische Anwender*innen in KMUs müssen diese Übungen jedoch verein-

facht und auf relevante Szenarien angepasst werden. So sollten Cyber Ranges für diese Zielgruppe praxisnahe Herausforderungen bieten, wie das Erkennen von Phishing-E-Mails, das sichere Management von Passwörtern oder das Verständnis grundlegender Sicherheitsprotokolle (Peltier, 2014). Durch diese Herangehensweise wird eine Überforderung vermieden und gleichzeitig das Sicherheitsbewusstsein gestärkt.

Eine der zentralen Herausforderungen bei nicht-technischen Anwender*innen ist die Schaffung eines tiefgreifenden Sicherheitsbewusstseins, das über rein technische Kenntnisse hinausgeht. Cyber Ranges können hierbei helfen, indem sie eine sichere Umgebung bieten, in der die Konsequenzen von Fehlverhalten oder Nachlässigkeit sichtbar werden. Studien zeigen, dass Lernszenarien, die reale Konsequenzen simulieren, zu einem nachhaltigen Verhaltenswandel führen können (Bada, 2019). Insbesondere für KMUs, deren Mitarbeitende oft mehrere Rollen im Unternehmen ausfüllen und nicht primär auf IT-Sicherheit fokussiert sind, bieten Cyber Ranges somit eine effektive Möglichkeit, um langfristige Änderungen im Sicherheitsverhalten zu fördern.

Ein zentrales Hindernis für die Nutzung von Cyber Ranges durch KMU-Mitarbeitende ist die Motivation. Da IT-Sicherheit nicht zu den Kernaufgaben dieser Mitarbeiter*innen gehört, ist es notwendig, die Übungen nicht nur inhaltlich, sondern auch hinsichtlich der Benutzer*innenfreundlichkeit und des Spaßfaktors anzupassen (Diakoumakos, 2023). Gamification-Ansätze, wie die Einführung von Punkten, Levels oder Teamwettbewerben, können hier eine motivationale Unterstützung bieten, um das Engagement zu erhöhen. Es bleibt jedoch eine Herausforderung, diese Motivation langfristig aufrechtzuerhalten, insbesondere wenn die Notwendigkeit von Cybersicherheit im Alltag nicht immer unmittelbar wahrgenommen wird.

7.1.4 Aktuelle Zielgruppen

Cyberübungen bieten einen großen Mehrwert für eine große Zielgruppe. Dieses Kapitel soll die aktuellen Zielgruppen erläutern und eine Diskussion über mögliche weitere Zielgruppen starten.

7.1.4.1 Organisationen mit starkem IT-Security-Schwerpunkt

Große Organisationen sind heutzutage abhängig von ihrer IT-Infrastruktur. Arbeitskräfte erbringen ihre Arbeitsleistung mit Unterstützung der IT-Infrastruktur (z.B. auf Laptops oder mit Maschinen) und alle wichtigen Informationen oder Daten sind darauf gespeichert. In Bezug zur Sicherheit der Daten sehen sich die Infrastruktur-Betreibenden mit dem CIA-Dreiklang (Yampolskiy et al., 2021) konfrontiert. Es besteht aus den Komponenten Vertraulichkeit (*Confidentiality*), Integrität (*Integrity*) und Verfügbarkeit (*Availability*). *Vertraulichkeit* stellt Regeln dar, die den Zugang zu Informationen auf vertraute Personen oder Geräte einschränken. *Integrität* ist die Zusicherung, dass Informationen vertrauenswürdig und korrekt sind und *Verfügbarkeit* ist eine Garantie dafür, dass man auf die Informationen auch zuverlässig zugreifen kann. Die Einhaltung dieser drei Komponenten wird allerdings immer herausfordernder. Homeoffice, zum Beispiel, wird immer präsenter, was dazu führt, dass Informationen auch von außerhalb der Organisation verfügbar sein müssen. Darunter sollten die anderen Komponenten des Dreiklangs allerdings nicht leiden, denn ein erfolgreicher Angriff auf eine Organisation kann dramatische Folgen haben und auch dazu führen, dass die Organisation ihre Leistungen nicht mehr erbringen kann, was neben Imageschäden auch enorme wirtschaftliche Folgen haben kann. Diese Organisationen legen daher einen starken Schwerpunkt auf ihre IT-Security, um solchen Problemen bestmöglich vorzubeugen. Darunter fallen zum Beispiel auch kritische Infrastrukturen, deren Ausfall auch für die Bevölkerung spürbare Auswirkungen hätte. Sie sind daher sogar per EU-Gesetz (Europäische Union, 2016) dazu verpflichtet, gewisse Cybersecurity-Standards einzuhalten.

Solche Organisationen sind oft daran interessiert, Cyberübungen durchzuführen, in denen ein spezieller Fokus auf dem Trainieren und Testen ihrer entwickelten Notfallprozesse liegt. Dabei sollen

Arbeitsabläufe, Kommunikationswege und Richtlinien überprüft werden. Für diesen Übungsfall eignen sich sowohl eine TTX sehr gut, aber auch eine CDX, um auch die technische Komponente miteinzubeziehen.

Zusätzlich wollen einige Organisationen ihr Personal auch in der rein technischen Beantwortung von Cybervorfällen schulen, wozu sich regelmäßige Cybertrainings sehr gut eignen.

7.1.4.2 Universität / Lehre

Da Cyberübungen ein expandierendes Themengebiet darstellen und mittlerweile fest im Portfolio einer stabilen Cybersecurity vorhanden sind, sollten auch IT-Security-Studierende damit konfrontiert werden. Daher sind seit einigen Jahren auch Universitäten daran interessiert das Thema „Cyberübung“ in die Curricula von IT-Security-Studierenden zu integrieren. Einerseits werden Cyberübungen genutzt, um Wissen und Lerninhalte zu übermitteln. Dazu nehmen die Studierenden die Rolle der Übenden ein und nehmen an einer vom Lehrpersonal organisierten Übung teil. Andererseits sollen Studierende auch explizit das Konzept von Cyberübungen lernen. Dazu sollen Studierende selbst eine Übung entwerfen und durchführen. Bei den Typen der Übungen sind im universitären Kontext keine Grenzen gesetzt. Cyberübungen sind auch Teil des Forschungsbetriebes von Universitäten, was dazu führt, dass auch neuartige Typen oder Abwandlungen bestehender Typen in Form von Lehrveranstaltungen entwickelt und evaluiert werden.

7.1.4.3 Staatliche Einrichtungen, Militär

In staatlichen Einrichtungen, wie zum Beispiel Regierungseinrichtungen, oder vor allem dem Militär, gibt es eine Vielzahl geheimer und schützenswerter Informationen, die ein äußerst interessantes Angriffsziel für ausländische Geheimdienste sein könnten. Sollten solche Informationen abgegriffen oder veröffentlicht werden, könnte das eine massive Schwächung der Sicherheit des Staates bedeuten. Da die Struktur zwischen unterschiedlichen Stellen sehr vernetzt ist, sind davon auch viele unterschiedliche Institutionen betroffen, die im Ernstfall miteinander interagieren und kommunizieren müssen.

Daher sind staatliche Einrichtungen und das Militär oft an kommunikativen Übungen, die in Form von CDX oder TTX umgesetzt werden können, interessiert, um die institutionsübergreifende Kommunikation im Ernstfall zu trainieren. Zusätzlich sollen natürlich auch die technischen Fähigkeiten des Personals und dessen Wissen über aktuelle Bedrohungsszenarien, Angriffsmethoden und deren Gegenmaßnahmen aktuell gehalten werden. Dazu werden Cybertrainings genutzt.

7.1.4.4 Interessierte Einzelpersonen

Einzelpersonen nehmen meist an Cyberübungen teil, wenn sie selbst großes Interesse an der Materie haben, was dazu führt, dass Vorkenntnisse meistens schon vorhanden sind. Sie wollen ihre technischen Fähigkeiten verbessern und sich mit anderen Übenden vergleichen. Dazu werden hauptsächlich CTFs verwendet. Teilnehmende haben die Möglichkeit, legal eine zur Verfügung gestellte Infrastruktur zu attackieren und Flags zu sammeln, um sich im Wettkampf gegen andere durchzusetzen. Der Hauptaspekt, warum Einzelpersonen an CTFs teilnehmen, ist meistens die Freude am Hacken und am Wettkampf.

7.1.4.5 Fazit

Zusammenfassend besteht die aktuelle Zielgruppe aus

1. größeren Organisationen (Privatunternehmen, kritische Infrastrukturen, Regierungseinrichtungen, Militär), die ihre Prozesse im Ernstfall testen und trainieren wollen und auch müssen oder die technischen Fähigkeiten ihres Personals am aktuellen Stand halten wollen,

2. Universitäten, die in Form von Lehre und Forschung Cyberübungen durchführen, um Wissen zu vermitteln oder zu generieren, und
3. interessierten Einzelpersonen, die ihre Fähigkeiten im Wettkampf demonstrieren und verbessern wollen.

Aufgrund dieser Zielgruppendefinition lässt sich ableiten, dass die Teilnehmenden bei Cyberübungen vorwiegend IT-Expert*innen oder wichtige Entscheidungsträger*innen sind. Die NATO zum Beispiel zielt mit ihren Cyberübungen explizit auf „*technical experts, military staff and decision-makers in member nations and within NATO*“ (NATO CCDCOE, 2022a) ab. Macht man einen detaillierteren Blick auf das Profil der Teilnehmenden, so fällt auf, dass überwiegend Männer daran teilnehmen, obwohl Cyberübungen sowohl für Frauen als auch für Männer den exakt selben Mehrwert bringen. Bei einer Übung der Indiana University, zum Beispiel, betrug die Teilnamequote von Frauen 6% (Deckard & Camp, 2016).

Aus Sicht des Konsortiums im Projekt INDUCE haben Cyberübungen für mehr Gruppen (als für IT-Expert*innen, Entscheidungsträger*innen und militärischem Personal) einen hohen Mehrwert. Daher ist auch das Ziel des Projektes, Überlegungen anzustellen wie man Cyberübungen diverser gestalten kann, um einerseits eine breitere Zielgruppe anzusprechen und andererseits andere Geschlechter als Männer für Cyberübungen zu interessieren.

7.1.5 Phasen einer Übung

Die Organisation einer Cyberübung ist eine komplexe Aufgabe, die sich in mehrere Phasen unterteilen lässt. Die ENISA unterteilt sie in ihrem „Good Practice Guide on National Exercises“ (ENISA, 2009) in die Phasen *Identifizieren*, *Planen*, *Durchführen* und *Evaluieren*. Da Evaluationen einer Cyberübung wieder in die Planung einer neuen Cyberübung miteinfließen, werden die Phasen als Teil eines Lebenszyklus gesehen. In den folgenden Abschnitten wird jede Phase kurz erläutert und die Schlüssel-Aufgaben in jeder Phase werden definiert.

7.1.5.1 Identifizieren

In dieser ersten Phase wird die Notwendigkeit für eine Übung identifiziert. Dazu wird von einer Organisation festgestellt, dass gewisse Prozesse, Strukturen oder technische Fähigkeiten getestet oder trainiert werden müssen. Wurden die zu testenden Komponenten identifiziert, so kann der Typ und die Größe der Cyberübung festgelegt, ein generisches Szenario entwickelt und die Stakeholder der Übung definiert werden. Dabei handelt es sich um keine Details, sondern nur um generische Definitionen, um den ungefähren Typ, Umfang und Inhalt der Übung festzustellen.

7.1.5.2 Planen

Nachdem die Notwendigkeit für eine Cyberübung, sowie deren ungefährer Umfang identifiziert wurden, kann in die detaillierte Planungsphase übergegangen werden. In der Planungsphase sollen alle Details und Inhalte definiert und vorbereitet werden, die zum Durchführen der Übung notwendig sind. Die Planungsphase ist sehr komplex und umfasst je nach Übungstyp und Lernzielen unterschiedliche Aufgaben. Sie nimmt mehrere Monate in Anspruch. Um einen Überblick zu geben, werden folgend ein paar Beispiele für die Aufgaben in dieser Phase aufgezählt und kurz erklärt:

- *Finanzielle Ressourcen bereitstellen*: Die Planung und Durchführung einer Cyberübung ist natürlich mit großen Kosten verbunden. Die Kosten müssen identifiziert und die finanziellen Ressourcen aufgebracht werden.
- *Datum und Ort wählen*: Es muss definiert werden, wann und wo die Übung stattfinden soll. Eine Cyberübung kann natürlich auch virtuell durchgeführt werden, wo nicht alle Teilnehmenden vor Ort sind, was allerdings wieder mit größeren Infrastruktur-Herausforderungen verbunden wäre.

- *Detailliertes Szenario erstellen*: Das Szenario muss bis ins letzte Detail geplant werden. Das sollte in enger Abstimmung mit den Zielen der Übung passieren, dass das Szenario auch wirklich die Überprüfung der Ziele ermöglicht.
- *Rollen zuweisen*: Es muss definiert werden, welche Personen an der Übung teilnehmen und welche Rollen sie während der Übung einnehmen.
- *Evaluationsmethodik wählen*: Um zu evaluieren, ob die Ziele erreicht wurden, muss eine Methodik gewählt (oder erstellt) werden, welche die Überprüfung dieser Ziele ermöglicht. Mögliche Evaluierungsmethoden sind zum Beispiel: Beobachtende Fragebögen (vor und/oder nach der Übung), technische Metriken.
- *Technische Infrastruktur vorbereiten*: Alle IT-Systeme (für alle Teams) müssen vorbereitet werden. Darunter fallen zum Beispiel die Systeme der Blue Teams mit Schwachstellen oder die Systeme der Red Teams mit den vorinstallierten Angriffs-Tools. Die Infrastruktur muss in Abstimmung mit dem Szenario erstellt werden, da sie einen Teil des Szenarios darstellt.
- *Übungsmaterialien vorbereiten*: Jegliche Übungsmaterialien müssen vorbereitet werden. Übungsmaterialien könnten zum Beispiel Pläne der Infrastruktur, Szenario-Kurzbeschreibungen, Injects, Einladungen, Namenskärtchen, und vieles mehr sein.
- *Medien kontaktieren*: Handelt es sich um eine große Übung, die auch die Außenwirkung der durchführenden Organisation stärkt, könnte es von Interesse sein, Medien zu kontaktieren und zur Übung einzuladen.
- *Probelauf durchführen*: Zuletzt sollte natürlich ein Probelauf durchgeführt werden, der vorhandene Probleme aufzeigt und garantiert, dass bei der Durchführung keine unerwarteten Probleme auftreten.

Diese Aufgaben stellen nur einen Teil der möglichen Aufgaben in der Planungsphase einer Cyberübung dar. Je nach Umfang und Typ unterscheidet sich die Planungsphase in ihren Aufgaben und ist sehr individuell.

7.1.5.3 Durchführen

Nachdem die Cyberübung bis ins letzte Detail vorbereitet wurde, kann sie am geplanten Tag und Ort stattfinden. Die Übung beginnt gewöhnlicherweise mit einer Begrüßung und einer Einführung in das Szenario. Wurden alle wichtigen Informationen und auftretende Fragen geklärt, so kann die Ausführung des Szenarios beginnen. Alle Teilnehmenden sollten sich gemäß ihren Rollen oder ihrer Teamzugehörigkeit verhalten und ihre Aufgaben während der Übung erledigen (siehe zum Beispiel die Aufgaben unterschiedlicher Teams im Abschnitt 7.1.2.3.1 „Cyber Defense Exercise (CDX)“). Die Durchführung der Übung kann von einigen Stunden bis hin zu mehreren Tagen dauern. Direkt im Anschluss an die Übung, wird oft ein sogenannter „Hot Wash-Up“ durchgeführt, indem erste Eindrücke und Feedback der Übenden sowie der Übungsleitung ausgetauscht werden.

7.1.5.4 Evaluieren

Nach Abschluss der Cyberübung werden detaillierte Evaluationen durchgeführt. Einerseits für die Übenden, um deren Verhalten und Lösungsansätze zu evaluieren und andererseits für die Übungsleitung, um mögliche Verbesserungen in die nächsten Übungen miteinzuplanen. Die Evaluierungsphase beginnt grundsätzlich schon während der Übung, indem notwendige Informationen gesammelt werden, die dann nach der Übung in Ruhe ausgewertet werden können. Aufgaben in der Evaluierungsphase sind zum Beispiel:

- *Berichte und Fragebögen auswerten*: Wurden während der Übung Berichte von Übenden oder Beobachtenden erstellt oder Fragebögen von den Übenden ausgefüllt, so können diese während der Evaluierungsphase ausgewertet werden.
- *Log-Dateien analysieren*: Bei technischen Übungen können die Log-Dateien verwendet werden, um das Verhalten der Übenden zu evaluieren.

- *Feedback einholen*: Das für die Evaluation zuständige Team kann Feedback von Teilnehmenden einholen, um festzustellen wie sie die Übung empfunden haben und welche Verbesserungsvorschläge sie haben.
- *Abschlussbericht(e) erstellen*: Ein oder mehrere Abschlussberichte können erstellt werden, welche die Übung und das Feedback zusammenfassen und an die Teilnehmenden oder den durchführenden Organisationen verschickt werden können.
- *Öffentliche Dokumente erstellen*: Zur Vermarktung können öffentliche Dokumente erstellt werden, die an Medien übermittelt, oder in sozialen Medien geteilt werden.

Mit Abschluss der Evaluierungsphase kann eine durchgeführte Cyberübung als abgeschlossen gesehen werden. Nichtsdestotrotz werden die Ergebnisse dieser Phase in die Durchführung nächster Cyberübungen miteinfließen.

7.1.6 Beispiele

Cyberübungen haben sich zu einem wichtigen und viel genutzten Tool zur Gewährleistung von Cybersicherheit entwickelt. Das lässt sich unter anderem auch daran erkennen, dass große, weltweit bekannte Organisationen regelmäßig solche Übungen durchführen, um ihrem Personal oder ihren Mitgliedern die Möglichkeit zu geben ihre Fähigkeiten, sowohl technisch als auch organisatorisch, zu testen und zu trainieren. Nachfolgend werden daher einige der bekanntesten und größten Cyberübungen mit einigen interessanten Fakten vorgestellt und einem der im Kapitel 7.1.2.3 vorgestellten Übungstypen zugeordnet.

7.1.6.1 Locked Shields

Locked Shields (NATO CCDCOE, 2022b) ist eine der größten Cyberübungen weltweit und findet jedes Jahr statt. Sie wird vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) organisiert. Im Jahr 2021 nahmen 22 Blue Teams mit durchschnittlich 40 Experti*nnen an der Übung teil. Die Teams nehmen die Rolle eines Cybernotfallteams ein, das einem fiktiven Staat im Verwalten von Cybernotfällen assistieren soll. Dazu waren mehr als 5000 virtuelle Systeme involviert, die Gegenstand von mehr als 4000 Cyberattacken waren.

Das Ziel von Locked Shields ist, die Fähigkeiten von Cybersecurity-Expert*innen im Verteidigen nationaler IT-Systeme und kritischer Infrastrukturen gegen Echtzeit-Attacken zu verbessern. Dazu müssen die Teams effektiv über Notfälle berichten, strategische Entscheidungen treffen und forensische, rechtliche und mediale Herausforderungen meistern.

Locked Shields lässt sich als CDX einordnen, in der die Teilnehmenden die verteidigende Rolle einnehmen. Die Übung zielt eher auf das Lösen von technischen Herausforderungen ab, wodurch sie überwiegend eine aktionsorientierte Perspektive hat. Nichtsdestotrotz werden auch diskussionsorientierte Ansätze wie zum Beispiel Berichte, strategische Entscheidungen und rechtliche Herausforderungen implementiert. Locked Shields ist zwar eine Übung, das Organisationsteam führt aber trotzdem eine Rangliste und kürt auch ein erstplatziertes Team. Im Jahr 2024 hat das Team aus Lettland gewonnen.

7.1.6.2 Cyber Europe

Die Cyber Europe ist eine internationale Cyberübung der European Union Agency for Cybersecurity (ENISA), die großflächige Cybersicherheitsnotfälle simuliert, welche sich zu einer Cyberkrise ausweiten. Sie findet seit 2010 alle zwei Jahre statt, musste allerdings 2020 aufgrund der Covid-19 Pandemie abgesagt werden.

Die Cyber Europe 2022 (ENISA, 2022) hatte ca. 900 Teilnehmende von 27 EU-Staaten, sowie Norwegen und der Schweiz, die sowohl von öffentlichen Behörden als auch privaten Unternehmen kommen. Sie simulierte eine realistische Cyberkrise und verfolgte folgende Ziele:

1. Testen der Kooperationsprozesse auf EU-Level.
2. Bereitstellung der Möglichkeit für Mitgliedstaaten ihre nationalen Kooperationsprozesse zu testen.
3. Trainieren der Fähigkeiten auf EU- und nationaler Ebene.

Die Cyber Europe ist eine klassische CDX, in der die Teilnehmenden die verteidigende Rolle einnehmen. Der Fokus liegt etwas stärker auf der diskussionsorientierten Perspektive, insbesondere im Testen der Kooperationsprozesse innerhalb der EU. Nichtsdestotrotz enthält die Übung auch technische Herausforderungen wie zum Beispiel Malware-Analyse und -Forensik. Bei der Cyber Europe handelt es sich um eine reine Übung, die keine Bewertung der Teilnehmenden vornimmt.

7.1.6.3 Cyber Coalition

Die Cyber Coalition (NATO ACT, 2022) ist eine militärische Cyberübung, die seit 2008 jedes Jahr mit den NATO-Mitgliedstaaten sowie den Bündnispartnerinnenstaaten abgehalten wird. Sie inkludiert in etwa 1000 Personen von 30 NATO-Alliierten, weiteren Partnerinnenstaaten und der Europäischen Union. Die Übung verfolgt folgende Ziele:

1. Die existierenden Mechanismen zur Interaktion zwischen NATO, Alliierten und Partnerinnen trainieren und die Zusammenarbeit im Cyberraum verbessern.
2. Die Fähigkeiten des Bündnisses zur Durchführung von Cyberoperationen für militärische und zivile Einrichtungen durch das Trainieren von Situationsbewusstsein, Informationsaustausch und Cybernotfallmanagement verbessern.
3. Einen Beitrag zur NATO-Cyberraum Transformation leisten, indem eine Plattform bereitgestellt wird, um Fähigkeitslücken und Schulungsanforderungen zu identifizieren und in Entwicklung befindliche Verfahren zu validieren, um die Entwicklung der Cyberkriegsführung zu unterstützen und die Cyberausbildung und das Cybertraining zu verbessern.

Das Szenario der Cyber Coalition 2021 umfasste einen Cyberangriff auf Gasversorgungsleitungen, einen Cyberangriff, der den Einsatz von Truppen und die Logistik unterbricht und eine Ransomware-Attacke mit Bezug zur Covid-19 Pandemie.

Die Cyber Coalition ist eine CDX in der die Teilnehmenden in der verteidigenden Perspektive sind. Sie ist sowohl diskussions- als auchaktionsorientiert. Einerseits sind Interaktion und die Art der Zusammenarbeit sehr wichtig, andererseits sollen auch explizit technische Probleme gelöst werden. Die Cyber Coalition hat reinen Übungscharakter, in der alle Teams die auftretenden Probleme gemeinsam lösen sollen.

7.1.6.4 CSAW CTF

Der CSAW CTF (CSAW, 2022) ist einer der ältesten und bekanntesten CTFs und findet jährlich im Rahmen der CSAW Konferenz statt. Er ist sowohl für Studierende, die in das Feld der Cybersicherheit eintauchen wollen, als auch für fortgeschrittene Studierende und Professionelle, die ihre Skills trainieren wollen, geeignet. Spielende können online teilnehmen und versuchen in die bereitgestellte Infrastruktur einzubrechen und *Flags* zu finden, wofür sie wiederum Punkte bekommen. 2021 erreichen in Summe 1216 Teams zumindest einen Punkt im CTF. Der CSAW CTF wird in zwei Runden ausgetragen: einer Qualifikationsrunde, die jedes Jahr im September stattfindet, und einer Finalrunde im November.

Der CSAW CTF ist (wie der Name schon vermuten lässt) als CTF einzuordnen. Die Teilnehmenden sind in der angreifenden Perspektive und arbeiten rein aktionsorientiert. Zudem wird der CSAW CTF als Wettkampf abgehalten, in welchem Punkte gesammelt und siegende Teams gekürt werden.

7.2 Phasen einer Übung in Bezug zu Diversität

Bei der Planung und Durchführung von Cyberübungen ist es entscheidend, Diversitätsaspekte in jeder Phase zu berücksichtigen. Dies ermöglicht die Teilnahme und den Lernerfolg für eine breite Zielgruppe mit unterschiedlichen Hintergründen, Fähigkeiten und Erfahrungen. Das Einbeziehen von Diversität erhöht nicht nur die Inklusivität, sondern erweitert auch die Perspektiven und erhöht die Effektivität der Übung.

7.2.1 Punkte, die man miteinbeziehen müsste

Bei der Gestaltung von Cyberübungen unter Berücksichtigung von Diversität sind mehrere Faktoren entscheidend:

- **Geschlecht**: Alle Geschlechter sollten in gleichberechtigten Rollen und Aufgaben eingebunden werden, um Stereotypen zu vermeiden und eine gleichwertige Teilnahme zu ermöglichen.
- **Altersgruppen**: Übungsinhalte sollten so gestaltet sein, dass sowohl jüngere als auch ältere Teilnehmer*innen aktiv teilnehmen können.
- **Hintergründe und Fähigkeiten**: Teilnehmende aus verschiedenen Bildungshintergründen (z.B. IT-Expert*innen, Nicht-Techniker*innen) und unterschiedliche kulturelle und soziale Kontexte sollten berücksichtigt werden.
- **Zugänglichkeit**: Niedrigschwellige Einstiege für Menschen mit wenig technischer Erfahrung oder Sprachbarrieren müssen gewährleistet sein.
- **Spezifische Zielgruppen**: Menschen aus besonderen Lebenslagen, wie Migrant*innen (aufgrund Sprachbarrieren oder verminderter Zugang zu IT) oder Personen in sozioökonomisch benachteiligten Gebieten, benötigen möglicherweise besondere Berücksichtigung in der Übungsgestaltung.

7.2.2 Wie kann man das machen?

Um Diversität in Cyberübungen zu integrieren, sollten folgende Maßnahmen umgesetzt werden:

- **Aufteilung der Rollen**: Rollen sollten bewusst so zugeteilt werden, dass sie Geschlechterstereotypen vermeiden. Alle Geschlechter sollten sowohl in Führungsrollen als auch in technischen Positionen vertreten sein.
- **Mehrsprachige Materialien**: Übungsinhalte sollten, wenn möglich, in verschiedenen Sprachen bereitgestellt werden, um eine sprachliche Barriere zu minimieren. Auch die Verwendung von Leichter Sprache ist angebracht.
- **Anpassung der Inhalte**: Übungen sollten in mehreren Schwierigkeitsgraden angeboten werden, um den Fähigkeiten der Teilnehmenden gerecht zu werden. Dabei kann das Mentimeter-Tool zur schnellen Meinungsabfrage und Anpassung der Inhalte in Echtzeit verwendet werden, wenn es allen Teilnehmenden möglich ist, dies zu verwenden.
- **Niedrigschwellige Zugänge**: Einfache digitale Plattformen, wie z.B. das Mentimeter-Planspiel, bieten eine gute Möglichkeit, Teilnehmende ohne umfangreiche Vorkenntnisse in die Übung zu integrieren.

7.2.3 KSÖ-Planspiel: Rollen von Frauen und Männern

Im KSÖ-Planspiel wurde darauf geachtet, sowohl Frauen als auch Männer in verschiedenen Rollen zu integrieren. Frauen wurden häufig in organisatorischen oder strategischen Rollen gesehen, während Männer oft in operativen oder technischen Aufgabenbereichen zu finden waren. Diese Aufteilung spiegelt oft bestehende Geschlechterstereotype wider, weshalb zukünftige Übungen be-

wusst darauf achten sollten, diese Muster zu durchbrechen, indem Frauen in technischen und Führungsrollen eingebunden werden und Männer ebenfalls administrative oder organisatorische Aufgaben übernehmen.

7.2.4 Übungen in anderen Bereichen etablieren

Um Cyberübungen in anderen Bereichen, wie bei Senior*innen, Migrant*innen oder in sozialen Brennpunkten, erfolgreich zu etablieren, sind gezielte Anpassungen notwendig:

- **Senior*innen** (ohne nennenswerte Erfahrung mit IT): Übungen für ältere Menschen sollten langsamere Erklärungen und intuitive Bedienbarkeit bieten. Zusätzlich könnte die Vermittlung grundlegender Techniken und Begriffe eingebunden werden, um Ängste vor der Technologie abzubauen.
- **Migrant*innen**: Mehrsprachige Anleitungen und kulturell angepasste Szenarien helfen, diese Zielgruppe zu erreichen. Ein kulturell angepasstes Szenario könnte man so umsetzen, dass gewisse Namen oder Dinge, die in dem betreffenden Kulturkreis vorkommen, verwendet werden. Auch die Integration von realistischen Situationen, wie digitale Betrugsfälle, Sicherheitsfragen bei der Nutzung von Online-Diensten udgl., könnte für Migrant*innen relevant sein.
- **„Brennpunkt"-Orte**: Übungen sollten auf lokale Herausforderungen eingehen, z.B. Cyberkriminalität im Alltag. Niedrigschwellige Einstiege und praktische Beispiele sind hier besonders wichtig.
- **Menschen mit Behinderung**: Anpassung der Materialen an die verschiedenen Bedürfnisse der Personen, z.B. Möglichkeit der Nutzung eines Screenreader, Blasmaus, Braille-Ausgabe, etc.

7.2.5 Thematische Inhalte in einer Übung

Die inhaltliche Gestaltung der Übungen sollte sich thematisch an den spezifischen Bedürfnissen der Teilnehmenden orientieren. Mögliche Inhalte sind:

- **Grundlagen der Cybersicherheit**: Einfache Erklärungen zu Bedrohungen wie Phishing, Malware und Datenschutz.
- **Technische Aufgaben**: Für fortgeschrittene Teilnehmende können technische Aufgaben wie das Erkennen und Abwehren von Angriffen eingebaut werden.
- **Realistische Szenarien**: Szenarien, die den Alltag der Zielgruppen widerspiegeln, etwa der Schutz vor Identitätsdiebstahl oder der sichere Umgang mit sozialen Medien.

7.2.6 Umsetzungsmöglichkeiten in den einzelnen Phasen

Die Umsetzung einer (diversitätssensiblen) Übung erfolgt in verschiedenen Phasen:

- **Planungsphase**: In dieser Phase wird die Zielgruppe definiert und die Übung entsprechend angepasst. Diversitätsfaktoren wie Geschlecht, Alter und Bildungshintergrund sollten bereits hier berücksichtigt werden.
- **Durchführungsphase**: Während der Übung sollten flexible Anpassungen möglich sein. Mentimeter und ähnliche Tools können genutzt werden, um in Echtzeit auf das Feedback der Teilnehmenden zu reagieren und die Inhalte anzupassen.
- **Evaluationsphase**: Nach der Übung ist es wichtig, Feedback zur Inklusion und Diversität einzuholen. Dabei sollte darauf geachtet werden, ob alle Teilnehmenden sich eingebunden gefühlt haben und ob bestimmte Gruppen benachteiligt waren, sowie welche Gruppen noch gefehlt haben.

7.2.7 Mentimeter-Planspiel: Niederschwelliger Zugang

Das Mentimeter-Planspiel bietet eine hervorragende Möglichkeit, den Zugang zu Cyberübungen niederschwellig zu gestalten. Die Erfahrung hat gezeigt, dass durch den Einsatz von einfachen Abstimmungstools können Teilnehmer ohne technisches Vorwissen schnell und einfach eingebunden werden. Die intuitive Bedienung und die Möglichkeit, live auf die Eingaben der Teilnehmenden zu reagieren, machen Mentimeter zu einem effektiven Werkzeug, um auch technisch unerfahrene oder zögerliche Zielgruppen zu erreichen.

Dieser Ansatz bietet eine praxisnahe, diversitätssensible Gestaltung von Cyberübungen und hilft, eine breitere Beteiligung zu fördern.

7.3 Umfrage zu Planspielen

Das Konsortium hat die Umfrage sorgfältig entwickelt, um eine präzise und zielgerichtete Erhebung sicherzustellen. Die Fragen wurden zunächst innerhalb des Konsortiums eingehend diskutiert und abgestimmt, um alle relevanten Aspekte zu berücksichtigen. Im Anschluss daran wurden die Inhalte der Umfrage mit Vertreter*innen der Zielgruppe validiert. Dieser Validierungsprozess stellte sicher, dass die Fragen klar formuliert und auf die Bedürfnisse sowie die Erfahrungen der Zielgruppe abgestimmt waren, um eine hohe Zielgenauigkeit und valide Ergebnisse zu gewährleisten.

Durch diese methodische Herangehensweise wurde sichergestellt, dass die Umfrage nicht nur theoretisch fundiert, sondern auch praktisch relevant ist. Die Einbeziehung der Zielgruppenvertreter*innen in die Validierung trug wesentlich dazu bei, eventuelle Missverständnisse oder Unklarheiten in den Fragen frühzeitig zu erkennen und zu korrigieren. So konnte eine fundierte Basis geschaffen werden, auf der die Ergebnisse der Umfrage verlässlich interpretiert werden können.

7.3.1 Methodischer Hintergrund

Der Bereich der Online-Befragungen hat sich in den letzten Jahren deutlich weiterentwickelt und zeichnet sich heute durch eine deutlich geringere Fehleranfälligkeit, eine geringere Belastung der Teilnehmenden (im Sinne von Zeitaufwand) und größere Robustheit als andere Formen der schriftlichen Befragung aus[69]. Online-Umfragen haben eine deutlich höhere Akzeptanz und eine höhere Rücklaufquote als postalische Befragungen. Die Hauptgründe dafür sind die bessere Erreichbarkeit der Teilnehmenden über die E-Mail-Adresse, die Möglichkeit, die Beantwortung komplexerer Fragen aktiv zu begleiten, die Belastung der Befragten durch Filterfragen zu reduzieren und schließlich die Möglichkeit des zeitnahen, direkten und wiederholten Nachfassens. Gleichzeitig sind die Ansprüche der Befragten an die Qualität von Umfragen gestiegen und die Aufmerksamkeitsspanne der Befragten hat sich allgemein verringert[70].

Eine wichtige Voraussetzung für den Erfolg ist die konzeptionelle Grundlage, die es den Teilnehmenden ermöglicht nur relevante Fragen/Informationen mit Hilfe von spezifischen Filterfragen zu stellen, gezielte Antwortkategorien und Hilfestellungen anzubieten und die Belastung der Befragten so gering wie möglich zu halten. In diesem Sinne unterscheiden sich standardisierte Online-Befragungen deutlich von Einzelinterviews oder Fokusgruppen, die ebenfalls Teil des vorliegenden Analysekonzepts sind und wesentlich offener gestaltet und damit besser geeignet sind, systemische

[69] Giuseppe Iarossi. The power of survey design: a user's guide for managing surveys, interpreting results, and influencing respondents. World Bank. OCLC: ocm61520417.
[70] Gideon, L. (Ed.). (2012). *Handbook of survey methodology for the social sciences* (Vol. 513). New York: Springer.

Zusammenhänge und Muster zu diskutieren oder Spannungslinien in direkter Interaktion mit den Teilnehmenden darzulegen[71].

Die hohe Sensibilität dieses Fragebogens erlaubt es den verschiedenen Teilnehmenden, individuell durch den Fragebogen zu navigieren (mit Hilfe verschiedener Filterfragen), sodass sie nur die Fragen beantworten müssen, die für sie relevant sind. Darüber hinaus wird bei der Entwicklung der Online-Umfrage darauf geachtet, dass nur solche Daten erhoben werden, die nicht aus anderen Datenquellen gewonnen werden können. Außerdem ermöglicht die Online-Umfrage aktuelle und zeitnahe Daten wie z.B. Bewertungen zu erhalten. Dies führt zu einer Effizienzsteigerung sowohl auf der Seite der Befragten als auch auf der Seite der Erstellenden der Umfrage.

7.3.2 Zielgruppe und Sampling

In der Online-Befragung wurde die Zielgruppe differenziert, um aussagekräftige und repräsentative Ergebnisse zu generieren. Dabei wurden zwei wesentliche Gruppen der Befragten berücksichtigt: die der Beschäftigten und die der Studierenden. Diese Unterscheidung ermöglicht es, spezifische Aussagen und Rückschlüsse in Bezug auf unterschiedliche soziodemografische und berufliche Hintergründe zu treffen.

1. Beschäftigte

Die Gruppe der Beschäftigten stellt eine zentrale Zielgruppe der Umfrage dar, da sie einen wesentlichen Teil der Gesellschaft repräsentiert. Personen in dieser Gruppe befinden sich in verschiedenen Beschäftigungsverhältnissen, darunter Vollzeit-, Teilzeit- oder auch selbstständige Tätigkeiten. Für diese Gruppe sind insbesondere Fragen von Interesse, die sich auf die Vereinbarkeit von Beruf und Freizeit, berufliche Anforderungen, Arbeitszeitmodelle und möglicherweise auf den Umgang mit neuen Technologien oder Homeoffice-Modellen beziehen. Zudem wird erwartet, dass sich ihre Perspektiven aufgrund ihrer Berufserfahrung und spezifischer fachlicher Hintergründe von denen der Studierenden signifikant unterscheiden. Die Erhebung von Daten in dieser Gruppe erfolgte hauptsächlich durch digitale Verbreitung der Umfrage über berufliche Netzwerke und gegebenenfalls durch Kooperationen mit Unternehmen oder Organisationen, die Zugang zu dieser Population haben.

2. Studierende

Die zweite zentrale Zielgruppe umfasst Studierende. Diese Gruppe zeichnet sich durch eine hohe Heterogenität hinsichtlich der Fachrichtungen und Semesterzugehörigkeiten aus. Ziel der Befragung ist es, eine repräsentative Stichprobe der Studierendenpopulation zu erreichen, indem die Umfrage breit gestreut wird. Dazu wurde die Umfrage an verschiedene Universitäten verteilt und gezielt in verschiedenen Kursen unterschiedlicher Fachrichtungen und Semesterstufen eingebettet. Dieses Vorgehen stellt sicher, dass sowohl Studienanfänger*innen als auch fortgeschrittene Studierende, möglicherweise sogar Examenskandidat*innen, erfasst werden, um ein umfassendes Bild der Studierendenschaft und ihrer jeweiligen Ansichten und Bedürfnisse zu erhalten.

Durch die Einbeziehung dieser zwei Gruppen können mögliche Unterschiede in den Perspektiven und Erfahrungen der Beschäftigten und der Studierenden herausgearbeitet werden. Während die Beschäftigten möglicherweise stärker von realen Berufserfahrungen berichten können, sind Studierende tendenziell mit anderen Herausforderungen, wie beispielsweise akademischen Anforderungen und der Vorbereitung auf den Berufseinstieg, konfrontiert. Die Untersuchung dieser beiden Gruppen trägt somit dazu bei, differenzierte Einblicke in ihre jeweiligen Lebenssituationen und Einstellungen zu gewinnen.

[71] Survey methodology. OCLC: ocn302189175.

7.3.3 Aufbau der Umfrage

Im Rahmen der Befragung ist es essenziell, die Struktur nach den verschiedenen Zielgruppen klar zu differenzieren, um gezielte und aussagekräftige Ergebnisse zu generieren. Jede Zielgruppe erhält dabei spezifisch auf sie zugeschnittene Fragen, die jedoch alle auf das gleiche übergeordnete Ziel abzielen: die Erhebung relevanter Daten zur Wahrnehmung und Verknüpfung von Planspielen im Kontext der Cybersicherheit. Die Fragebögen sind so konzipiert, dass sie verschiedene Informationspools bedienen, wobei jede Fragekategorie unterschiedliche Aspekte des Befragungsthemas abdeckt. Diese Vorgehensweise ermöglicht es, die individuellen Perspektiven und Erfahrungswerte der Teilnehmenden besser zu erfassen und in einen größeren Zusammenhang zu setzen.

7.3.3.1 Kategorien der Befragung

Die Fragen lassen sich in drei zentrale Kategorien unterteilen, die jeweils auf unterschiedliche Informationsziele abzielen und komplementäre Daten liefern:

7.3.3.1.1 Allgemeine Fragen

Die allgemeinen Fragen dienen der Erfassung der aktuellen Situation der Befragten und liefern kontextuelle Informationen, die für die Einordnung der weiteren Daten essenziell sind. Diese Fragen sind bewusst so gestaltet, dass sie keinen direkten persönlichen Bezug herstellen, sondern vielmehr ein allgemeines Stimmungsbild sowie potenzielle Herausforderungen oder Themenfelder erfassen, die für die Zielgruppen relevant sind. Beispielsweise könnte nach der allgemeinen Vertrautheit mit Planspielen oder der bisherigen Teilnahme an solchen Formaten gefragt werden. Dies ermöglicht einen ersten Überblick über das Umfeld, in dem die Teilnehmenden agieren.

7.3.3.1.2 Ausbildungsspezifische Fragen

In diesem Abschnitt liegt der Fokus auf dem Ausbildungsstand der Teilnehmenden, insbesondere im Hinblick auf ihre Qualifikationen im Bereich der Cybersicherheit. Die Befragten sollen sowohl ihren allgemeinen Bildungsweg als auch ihre spezifischen Kenntnisse und Erfahrungen im Bereich der Cybersicherheit beschreiben. Dieser Fragenblock zielt darauf ab, Unterschiede und Gemeinsamkeiten in der Wahrnehmung und Anwendung von Planspielen bei den verschiedenen Zielgruppen aufzuzeigen. Er ermöglicht es zu analysieren, ob und inwiefern das Ausbildungsniveau die Art und Weise beeinflusst, wie Planspiele verstanden und bewertet werden.

Darüber hinaus sollen die Teilnehmenden darlegen, in welchem Maße ihre Ausbildung sie auf die Herausforderungen in der Cybersicherheit vorbereitet hat und ob sie Planspiele als nützliches Werkzeug zur Vertiefung ihrer Kenntnisse und Fähigkeiten betrachten. Diese differenzierte Erfassung erlaubt es, Zusammenhänge zwischen dem Ausbildungsstand und der Effektivität von Planspielen im Lernprozess zu identifizieren.

7.3.3.2 Ziel der Befragung

Das übergeordnete Ziel der Befragung ist es, Einblicke in die Wahrnehmung von Planspielen in verschiedenen Zielgruppen zu gewinnen und zu untersuchen, inwiefern diese als Instrument zur Verbesserung der Cybersicherheitskompetenzen angesehen werden. Durch die Strukturierung der Befragung in verschiedene Fragekategorien und die Fokussierung auf unterschiedliche Informationspools wird es möglich, umfassende und differenzierte Daten zu erheben, die eine fundierte Analyse der Zielgruppen und ihrer spezifischen Bedürfnisse ermöglichen. Dies bildet die Grundlage für weitere Maßnahmen zur Optimierung von Planspielen im Kontext der Cybersicherheit, indem gezielt auf die jeweilige Ausbildung und Erfahrungswelt der Teilnehmenden eingegangen werden kann.

Die Erkenntnisse aus dieser Befragung werden dazu beitragen, zukünftige Bildungsformate in der Cybersicherheit effizienter zu gestalten und besser an die Bedürfnisse der unterschiedlichen Zielgruppen anzupassen.

7.3.4 Ergebnisse und Interpretation

7.3.4.1 Allgemeiner Teil

Die deutliche Mehrheit der Teilnehmenden an der Umfrage besteht aus Personen (siehe

Abbildung 7), die sich als „männlich“ oder „weiblich“ identifizieren, was darauf hindeutet, dass die Umfrage eine überwiegend binäre Geschlechterverteilung widerspiegelt. Die Kategorien „Divers“ und „Anderes“ weisen einen sehr geringen Anteil auf, was entweder auf die geringe Anzahl nichtbinärer oder anderer Geschlechtsidentitäten in der Stichprobe oder möglicherweise auf mangelnde Repräsentation oder Teilnahmebereitschaft dieser Gruppen hinweisen könnte.

Ein weiterer interessanter Aspekt ist der sehr kleine Anteil an Personen, die „keine Angabe“ zu ihrem Geschlecht machen. Dies könnte auf eine geringe Zurückhaltung der Befragten bei der Offenlegung ihrer Geschlechtsidentität hinweisen, was eventuell für die Transparenz und Anonymität der Umfrage spricht.

Die Geschlechterverteilung in einer Umfrage ist oft ein entscheidender Faktor, da sie Rückschlüsse darauf zulässt, wie ausgewogen die Umfrage hinsichtlich der Repräsentation verschiedener Gruppen ist. In diesem Fall dominiert die binäre Geschlechterverteilung (männlich/weiblich). Sollten die Themen der Umfrage geschlechtsspezifische Auswirkungen haben, könnte dies die Interpretation der Ergebnisse beeinflussen.

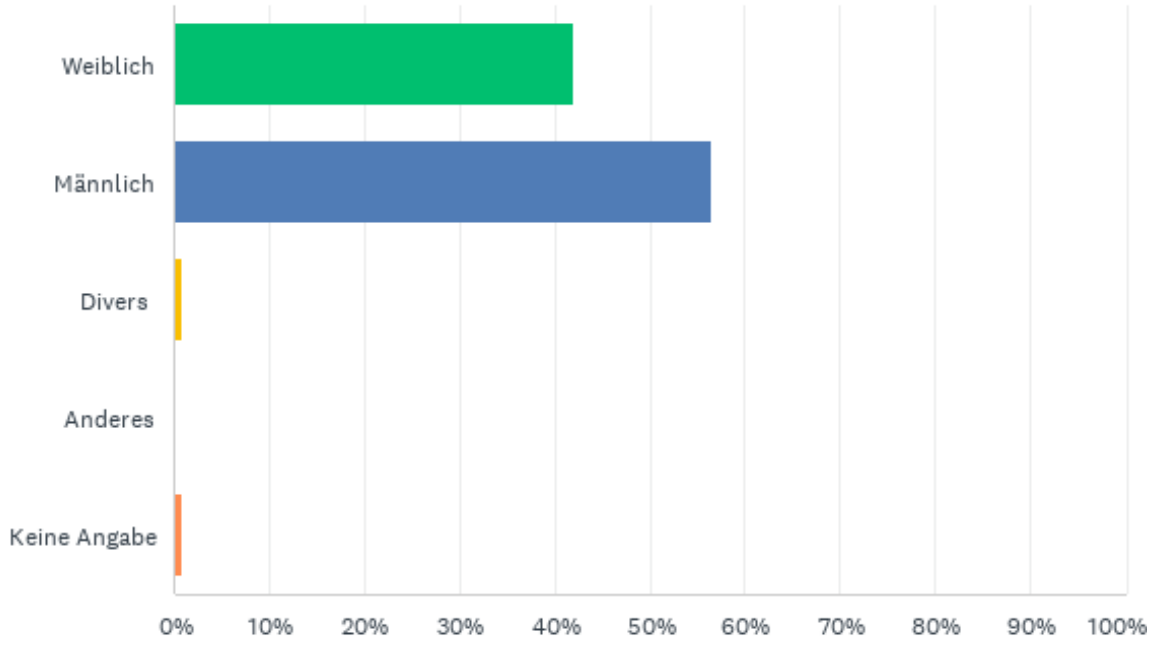


ABBILDUNG 7 GESCHLECHTERVERTEILUNG IN DER UMFRAGE

Die Ergebnisse (siehe Abbildung 8) zeigen, dass der überwiegende Teil der Befragten erwerbstätig ist, während ein geringerer Teil ein duales Modell verfolgt (also sowohl studiert als auch arbeitet). Die Gruppe, die ausschließlich studiert, ist die kleinste, was darauf hindeutet, dass die Umfrage eine überwiegend berufstätige Population ansprach.

Der Arbeits- oder Studienstatus zeigt verschiedene Perspektiven oder Präferenzen in Bezug auf Zeitmanagement, Stress oder finanzielle Prioritäten beeinflussen. Besonders der Anteil derjenigen, die sowohl studieren als auch arbeiten, könnte auf einen Anstieg des Trends hinweisen, Studium und Beruf parallel zu führen, was Herausforderungen im Bereich der Work-Life-Balance nach sich zieht. Die Verteilung zeigt eine klare Prävalenz von Berufstätigen in der Stichprobe.

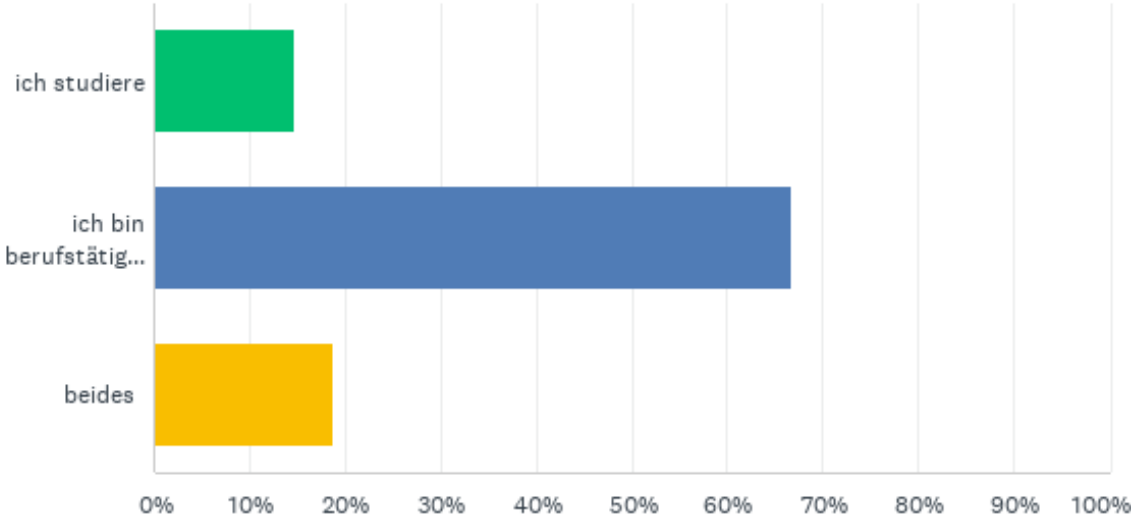


ABBILDUNG 8 AUSBILDUNG DER TEILNEHMER

Die dominierenden Branchen (siehe Abbildung 9) in der Umfrage sind Information und Kommunikation sowie sonstige freiberufliche, wissenschaftliche und technische Tätigkeiten. Dies könnte darauf hinweisen, dass die Teilnehmenden der Umfrage überwiegend aus technisch orientierten, wissensbasierten oder kreativen Berufen stammen. Die geringe Beteiligung aus Bereichen wie Beherbergung und Gastronomie, Verkehr und Logistik oder Gesundheits- und Sozialwesen ist auf die Rücklaufquote zurückzuführen.

Die deutliche Dominanz bestimmter Sektoren sollte bei der Interpretation der Umfrageergebnisse berücksichtigt werden. Da Teilnehmende aus den Bereichen Information und Kommunikation sowie freiberufliche Tätigkeiten überproportional vertreten sind, könnten deren berufliche Perspektiven und Herausforderungen die Ergebnisse der Umfrage stark beeinflussen.

Zudem sollten die gering vertretenen Branchen wie Gesundheitswesen und Landwirtschaft gesondert betrachtet werden, um zu analysieren, ob die geringe Teilnahme auf strukturelle Gegebenheiten (z. B. Schichtarbeit oder andere Arbeitsbedingungen) zurückzuführen ist, welche die Teilnahme an Umfragen erschweren.

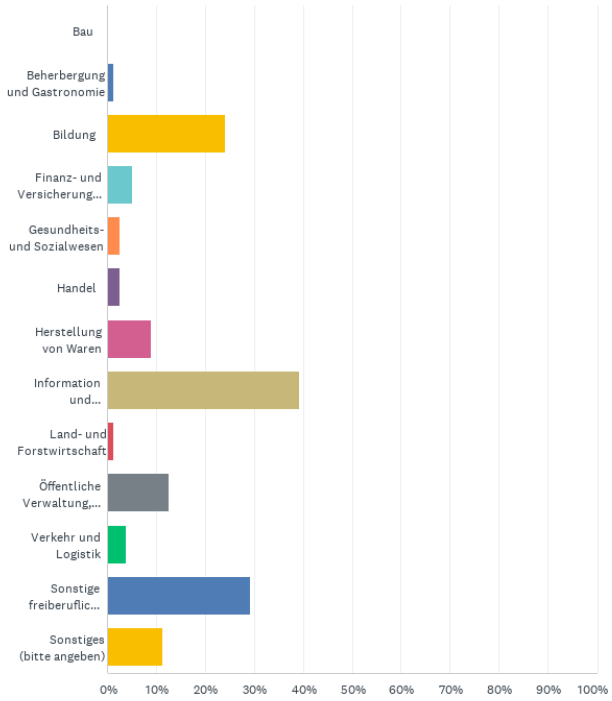


ABBILDUNG 9 BRANCHENEINORDNUNG

7.3.4.2 Spezifischer Teil

Die Abbildung 10 zeigt, dass Planspiele im Bereich Cybersicherheit zwar vielen Menschen bekannt sind, die tatsächliche Teilnahme jedoch geringer ausfällt. Es gibt eine Lücke zwischen der theoretischen Kenntnis solcher Planspiele und der praktischen Anwendung. Dies könnte darauf hinweisen, dass es zwar Schulungen oder Informationsquellen zu solchen Übungen gibt, sie jedoch nicht immer aktiv oder häufig genutzt werden.

Die Tatsache, dass ein erheblicher Teil der Befragten (25+ %) noch nie von Cybersicherheits-Planspielen gehört hat, deutet darauf hin, dass in einigen Bereichen noch Aufklärungsbedarf besteht. Besonders in Branchen oder Berufsgruppen, die mit Cybersicherheit weniger in Berührung kommen, könnte das Bewusstsein für diese Art von Übungen gering sein.

Diese Ergebnisse liefern weiter wichtige Information darüber, wie verbreitet und zugänglich Planspiele zur Cybersicherheit sind. In einem wissenschaftlichen Kontext dient das als Hinweis darauf, dass praktische Cybersicherheitsübungen in bestimmten Sektoren oder Berufsfeldern nicht weit verbreitet sind oder nicht ausreichend in die Weiterbildung integriert wird.

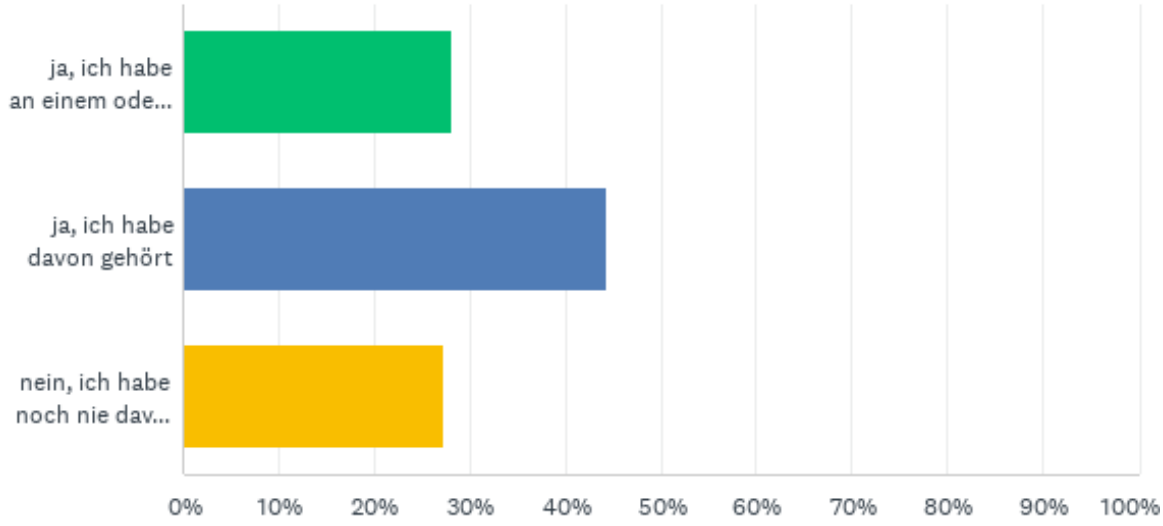


ABBILDUNG 10 KENNTNIS ÜBER PLANSPIELE

Die Ergebnisse zeigen, dass Planspiele (siehe Abbildung 11) als besonders nützlich in den Bereichen **Sicherheit, Technik** und **Wirtschaft** angesehen werden. Dies deutet darauf hin, dass in diesen **Feldern ein starkes Bedürfnis nach simulationsbasiertem Lernen** und Krisenmanagement besteht (siehe Abbildung 12). Insbesondere in sicherheitskritischen Szenarien, wie z. B. im Katastrophenschutz oder in der Cyberabwehr, sowie in technischen und wirtschaftlichen Krisensituationen, können Planspiele komplexe Prozesse realistisch abbilden. Dies führt zu einer hohen Akzeptanz und Relevanz in diesen Bereichen, da sie es ermöglichen, strategische Entscheidungsprozesse und Notfallszenarien effektiv zu simulieren und zu trainieren.

Auch in den **Feldern Bildung und Politik** werden Planspiele als sinnvolle Methode angesehen. Sie bieten eine Möglichkeit, politische Prozesse oder bildungsbezogene Themen durch die Simulation komplexer Szenarien zu veranschaulichen. So können Planspiele in der Politik verwendet werden, um Entscheidungsfindungen in internationalen Beziehungen oder demokratischen Prozessen zu üben. In der Bildung tragen sie dazu bei, das Verständnis für komplexe Zusammenhänge zu vertiefen und das Problemlösungsverhalten zu fördern.

Interessanterweise erhält der Bereich Recht die geringste Zustimmung, was darauf hindeutet, dass Planspiele in diesem Feld als weniger anwendbar oder relevant angesehen werden. Dies könnte daran liegen, dass juristische Fragestellungen häufig als zu komplex oder formalisiert betrachtet werden, um sie durch simulationsbasierte Ansätze angemessen abzubilden. Hier könnten andere didaktische Methoden, wie Fallstudien oder theoretische Diskussionen, bevorzugt werden, da sie die strukturierten und regelbasierten Anforderungen des Rechtswesens besser erfüllen.

Die Ergebnisse bieten wertvolle Erkenntnisse darüber, in welchen Bereichen Planspiele als effektives Werkzeug für Bildung, Training und Krisenmanagement angesehen werden. Die hohe Akzeptanz in den Bereichen Sicherheit und Wirtschaft könnte darauf hindeuten, dass diese Branchen das potenzielle Risiko, beispielsweise durch Cyberangriffe oder wirtschaftliche Krisen, besonders gut erkennen und daher einen höheren Bedarf an Simulationen haben, um auf solche Herausforderungen vorbereitet zu sein. Auch in technischen Bereichen stößt der simulationsbasierte Ansatz auf breite Zustimmung, was die Bedeutung von Planspielen bei der Vorbereitung auf technologische Entwicklungen und Herausforderungen unterstreicht.

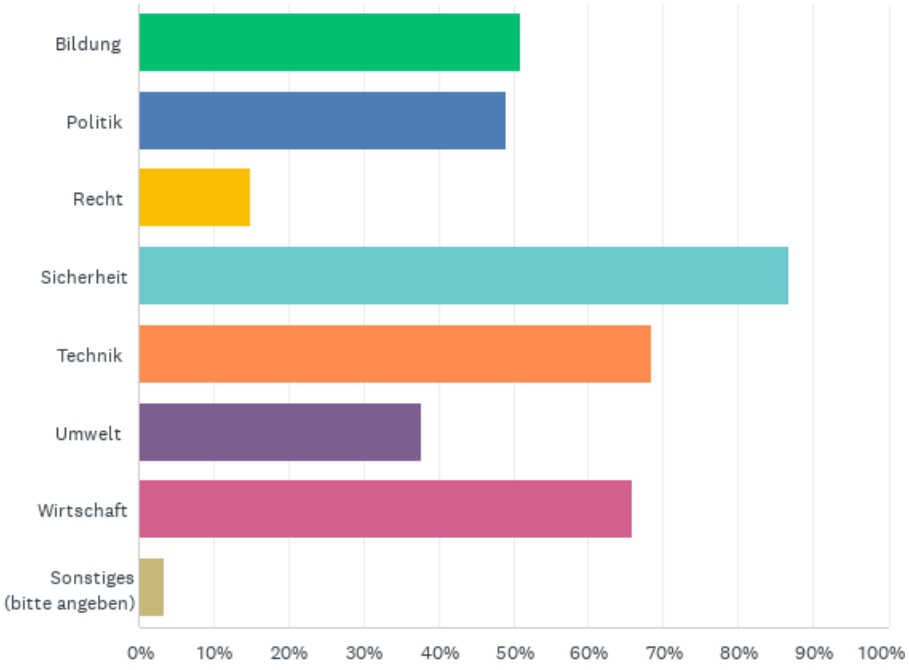


ABBILDUNG 11 EINSATZMÖGLICHKEITEN VON PLANSPIELEN

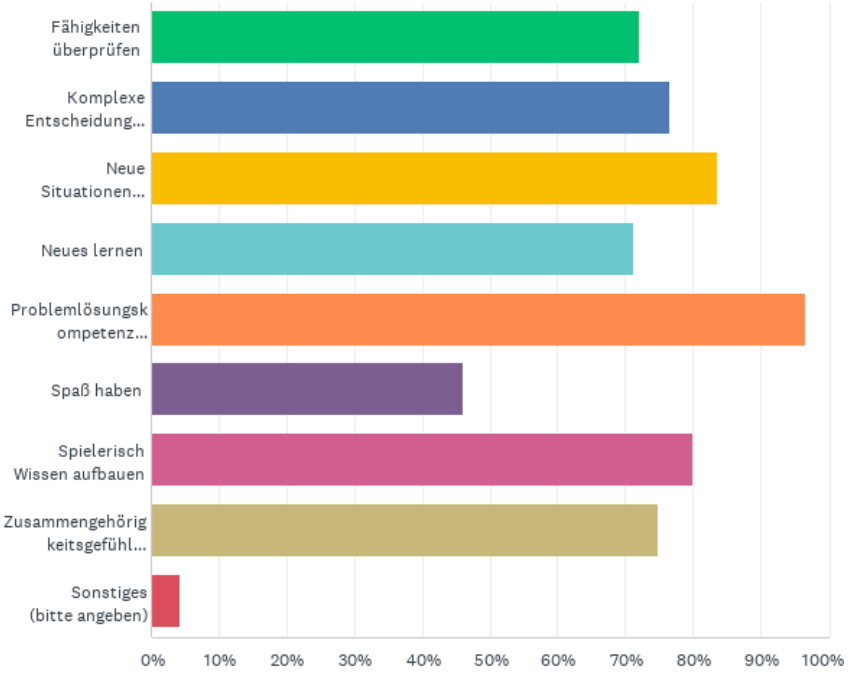


ABBILDUNG 12 MÖGLICHER MEHRWERT VON PLANSPIELEN

Die Antworten (siehe Abbildung 13) zeigen deutlich, dass der Verlust des Datenzugriffs und der Reputationsschaden die größten Sorgen im Zusammenhang mit Cyberangriffen darstellen. Dies deutet darauf hin, dass die Teilnehmer*innen den immateriellen Schaden (Verlust des Zugriffs, Verlust von Daten oder Ruf) ernster nehmen als rein finanzielle Verluste. Dies könnte insbesondere für Menschen relevant sein, die stark von der digitalen Welt abhängig sind, sei es beruflich oder privat.

Auch der Verlust von Geräten und die Folgen eines Datenverlusts werden als erhebliches Risiko wahrgenommen, was zeigt, dass es wichtig ist, nicht nur Daten zu schützen, sondern auch die physischen Geräte, auf denen sie gespeichert sind.

Diese Ergebnisse liefern wertvolle Erkenntnisse darüber, welche Auswirkungen von Cyberangriffen von verschiedenen Personengruppen als am bedrohlichsten wahrgenommen werden. Insbesondere in Berufen, in denen Daten eine zentrale Rolle spielen (z. B. im Informationssektor), könnten der Verlust des Datenzugriffs und der Reputationsschaden zu langfristigen Problemen führen. Dies weist auf die Bedeutung robuster Cybersicherheitsmaßnahmen hin, um diese potenziellen Risiken zu minimieren.

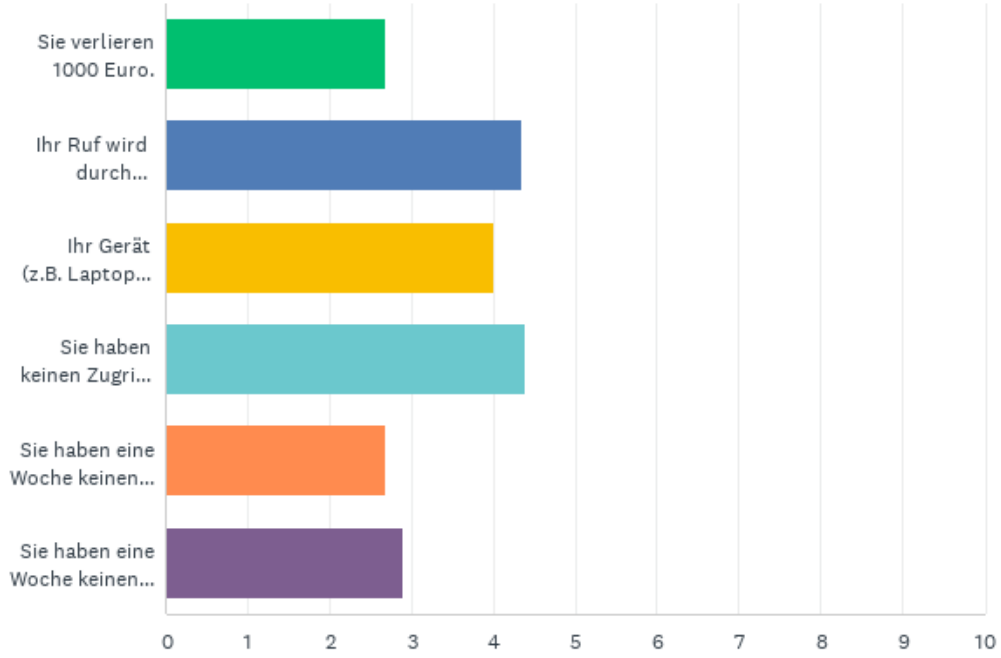


ABBILDUNG 13 AUSWIRKUNGEN

Die Umfrageergebnisse verdeutlichen mehrere zentrale Tendenzen im Hinblick auf die Zusammensetzung der Stichprobe und die Relevanz von Planspielen als Lern- und Krisenmanagement-Werkzeug in verschiedenen Berufssektoren. Die überwiegend binäre Geschlechterverteilung und die vorherrschende Berufstätigkeit der Teilnehmenden weisen auf eine spezifische Bevölkerungsgruppe hin, die in erster Linie aus den technisch-wissenschaftlichen Sektoren stammt.

Planspiele werden besonders in den Bereichen Sicherheit, Technik und Wirtschaft als nützlich angesehen, was darauf hinweist, dass diese Sektoren ein starkes Bedürfnis nach praxisorientiertem, simulationsbasiertem Lernen haben. Besonders in sicherheitskritischen Szenarien und technologischen Kontexten scheint die Fähigkeit, komplexe Krisen realistisch zu simulieren und strategisch zu reagieren, von hohem Wert zu sein. Gleichzeitig zeigt die Umfrage, dass in weniger technisch orientierten Bereichen, wie dem Recht, Planspiele als weniger relevant wahrgenommen werden, was auf spezifische strukturelle und didaktische Anforderungen dieser Berufe zurückzuführen sein könnte, zusätzlich sind in diesen Bereichen das Werkzeug „Planspiele“ noch nicht so gängig.

Insgesamt betont die Umfrage die Bedeutung von Planspielen in der modernen Ausbildung und im Krisenmanagement, insbesondere in stark digitalisierten und technologisch orientierten Bereichen. Gleichzeitig zeigt sie auf, dass in einigen Berufssektoren ein Informations- und Aufklärungsbedarf

besteht, um das Bewusstsein für die Notwendigkeit und den Nutzen solcher simulationsbasierten Ansätze zu schärfen. Dies eröffnet Potenziale für zukünftige Forschung und Weiterentwicklungen im Bereich der Cybersicherheit und der beruflichen Weiterbildung.

7.4 Designideen für diversitätssensible Cyberübungen

In diesem Kapitel sollen die wichtigsten Design-Ideen der im Kapitel Demonstrator(en) für diversitätssensiblen vorgestellten Cybersicherheitsübungen vorgestellt und diskutiert werden. Das Design der entwickelten Übungen ziel darauf ab, diversitätsfreundlichen, niederschwelligen, aber dennoch praxisnahen Inhalt zu vermitteln, um eine möglichst breite Zielgruppe in das Thema Cybersicherheit einzuführen und ein Bewusstsein für grundlegende Sicherheitsmaßnahmen zu schaffen.

Es wurden vier Haupttypen von Cyberübungen beschrieben, die speziell darauf ausgerichtet sind, unterschiedliche Zielgruppen anzusprechen:

- **Mentimeter-Planspiel**: Ein interaktives Planspiel, das typische Herausforderungen eines Arbeitstages im Home-Office simuliert. Die Teilnehmenden wählen in verschiedenen Situationen mögliche Reaktionen aus, wodurch sowohl die richtigen Handlungsweisen vermittelt als auch Diskussionen angeregt werden. Das Szenario ist flexibel anpassbar, um unterschiedliche Zielgruppen wie Lehrer*innen oder Mitarbeitende aus unterschiedlichen Bereichen einzubeziehen.
- **Mini-Szenarien**: Kurze Übungen zu Themen wie Smart Home, unsichere WLAN-Netze, Passwortsicherheit, Backups, Deep Fakes und Phishing. Diese Übungen dauern jeweils etwa 20-30 Minuten und ermöglichen es auch unerfahrenen Nutzer*innen, grundlegende Sicherheitskonzepte kennenzulernen und zu üben. Der Fokus liegt auf einfachen Erklärungen und praxisnahen Erfahrungen.
- **Level-Up Trainingskurs**: Ein spielerischer Ansatz, um Besucher*innen von Messen grundlegende Cybersicherheitskonzepte näherzubringen. Dabei werden Fragen zu Passwortsicherheit, Angriffstechniken und Prävention gestellt sowie praktische Übungen, wie z.B. eine SQL-Injection, durchgeführt.
- **ARES Workshop CTF (Capture the Flag)**: Ein interaktiver Workshop, der auf die vertiefende Auseinandersetzung mit Cybersicherheitsthemen abzielt. Die Teilnehmenden mussten „Flags“ in verschiedenen, komplexeren Aufgaben finden, die Aspekte wie Netzwerkverkehrsanalyse, Verschlüsselung und Passwortsicherheit abdecken.

Die Designideen hinter diesen Cyberübungen basieren auf der Inklusion und der Zugänglichkeit für alle gesellschaftlichen Gruppen, unabhängig von Geschlecht, Alter, technischer Vorerfahrung oder sozialer Herkunft. Diese Ansätze unterscheiden sich von traditionellen technischen Planspielen, die häufig für IT-Expert*innen und Fachleute mit tieferem Wissen konzipiert sind. Die Überlegungen hinter den Designideen lassen sich in folgenden Aspekten zusammenfassen:

- **Niedrigschwellige Teilnahme**: Durch kurze, einfache Übungen sollen auch Menschen ohne technische Vorkenntnisse mitgenommen werden. Dies ermöglicht eine breitere Zielgruppenansprache, da die Übungen einfach gestaltet sind und komplexe Begriffe vermieden oder erklärt werden.
- **Diversitätsdimensionen berücksichtigen**: Das Projekt INDUCE berücksichtigt verschiedene Diversitätsdimensionen (wie Gender, Alter und soziale Herkunft). Dadurch werden die Übungen flexibel gestaltet und jeweils auf die Bedürfnisse der Zielgruppe angepasst. Ein Beispiel ist die Anpassung des Mentimeter-Planspiels an den spezifischen Kontext von Lehrer*innen, um deren Lebens- und Arbeitsrealität besser abzubilden.
- **Interaktivität und Praxisnähe**: Die Übungen sind nicht rein theoretisch, sondern stark interaktiv und praxisorientiert. Dadurch können Teilnehmende konkrete Handlungsschritte im

Bereich der Cybersicherheit selbst erleben und ausprobieren. Dies fördert nicht nur das Verständnis, sondern auch die Fähigkeit, Gelerntes im Alltag anzuwenden.

- **Gamification**: Ansätze wie der „Capture the Flag“-Workshop oder das Fragespiel im Level-Up Kurs nutzen spielerische Elemente, um das Lernen unterhaltsam zu gestalten und die Motivation zu steigern. Durch das Erlebnislernen werden Teilnehmer*innen dazu angeregt, sich tiefergehend mit den Themen zu befassen.

Die Designideen für diversitätssensible Szenarien und Cyberübungen zielen darauf ab, Barrieren für den Zugang zu Cybersicherheit zu senken und möglichst viele Menschen für das Thema zu sensibilisieren. Durch die Kombination aus einfacher Sprache, interaktiven Elementen und einem bewussten Fokus auf die Diversität der Zielgruppen konnten Inhalte entwickelt werden, die sowohl für Anfänger*innen als auch für Fortgeschrittene geeignet sind. Dadurch wird ein breiterer Zugang ermöglicht, der weit über rein technische Zielgruppen hinausgeht, und eine Basis für mehr Sicherheit in einer zunehmend digitalisierten Gesellschaft geschaffen.

8 Demonstrator(en) für diversitätssensiblen Cyberübungen

8.1 Einleitung

Das Projekt INDUCE zielt darauf ab, existierende Cyberübungen auf Chancengerechtigkeit für verschiedene Zielgruppen unter Einbezug verschiedener Diversitätsdimensionen (z.B. Gender, Alter und soziale Herkunft) zu evaluieren und aufbauend darauf Cyberszenarien, Algorithmen und Technologien neu zu entwickeln, zu erweitern und zu adaptieren. Um dieses Ziel zu erreichen, müssen Cyberübungen umgestaltet werden, um nicht nur gezielte Trainings für gezielte Personengruppen zu ermöglichen, sondern einen Ansatz zu verfolgen, um die breite Masse anzusprechen und einerseits Cybersicherheitslerninhalte zu vermitteln und andererseits Personen mit unterschiedlichstem Hintergrund an das Thema Cybersicherheit heranzuführen.

Im Projekt INDUCE sollen niederschwellige Schulungen für verschiedene Zielgruppen erstellt werden. Um dieses Ziel zu erreichen, wurde die Idee von kurzen und kurzweiligen Übungseinheiten geboren. Aufbauend auf der Erfahrung mit der AIT Cyber Range[72] und der Durchführung von großen Planspielen[73] wurden daher kleinere Übungen gestaltet, die das Ziel erreichbar machen sollen. Der Grundgedanke ist der, dass Menschen unterschiedlicher Herkunft, unterschiedlicher Ausbildungsstände, Alter, etc. diese ohne Probleme meistern sollen können. Die Übungen sollen für Klein- und Kleinstunternehmen genauso hilfreich sein, wie für Schüler*innen, Studierende oder auch Pensionist*innen. Deshalb wird auch auf eine einfache Sprache geachtet, die z.B. wenige Fachwörter enthält oder diese im Zug der Übung auch erklärt werden.

Als Ergebnis dieser Überlegungen sind folgende Cyberübungen (oder Cybertrainings) entstanden.

- Mentimeter Planspiel
- Mini-Szenarien
- Level-Up Trainingsumgebung
- ARES Workshop CTF

In diesem Deliverable werden die entwickelten Cyberübungen vorgestellt und näher beschrieben.

8.2 AIT Cyber Range

Die AIT Cyber Range des AIT Austrian Institute of Technology ist eine virtuelle Umgebung für die flexible Simulation von kritischen IT- und industriellen OT-Systemen mit komplexen Netzwerken, verschiedenen Systemkomponenten und Benutzer*innen. Sie bietet eine sichere und realistische Umgebung für das Trainieren und Testen von Cybersicherheitsvorfällen in skalierbaren Szenarien, ohne reale Produktionssysteme zu verwenden. So können verschiedene Sicherheitsprozesse für den Live-Betrieb geprobt und spezielle Incident-Response-Prozesse für Cybervorfälle getestet werden, um höchste Sicherheitsanforderungen an Systemarchitekturen und Betriebsprozesse zu erfüllen. Die AIT Cyber Range Trainings und Übungen richten sich aktuell vorwiegend an IT-Fachleute, CERTs/CSIRTs, Management und Beiräte in Industrie, Forschung und Verwaltung.

Die AIT Cyber Range unterstützt

- **Ausbildung**
  Cybersicherheitsschulung zur Verbesserung der Cybersicherheitsfähigkeiten von Mitarbeitenden (vom allgemeinen Personal bis hin zu Management) in Organisationen.

[72] https://www.ait.ac.at/themen/cyber-security/ait-cyber-range-training
[73] z.B.: KSÖ Planspiel 2021 und 2017

- **Übung**
  Praktische Erfahrungen mit dem Management und der Reaktion auf Vorfälle für Mitarbeitende, CERTs/CSIRTs in einer simulierten virtuellen Umgebung.
- **Forschung**
  Forschung zur Cybersicherheit von Infrastrukturen und Szenarien, die erforderlich sind, um die Widerstandsfähigkeit von Organisationen zu erhalten.
- **Entwicklung**
  Sichere Entwicklung von Software für das Störungsmanagement und die Cybersicherheit.

Die AIT Cyber Range wurde vom AIT in einer strategischen Kooperation mit der IAEA International Atomic Energy Association[74] entwickelt. Neben der Nutzung der AIT Cyber Range im akademischen Bereich für die Ausbildung wird sie für globale Cybersicherheitstrainings für den Nuklearsektor sowie für staatliche Übungen zur Cybersicherheit verwendet.

Nutzung der AIT Cyber Range

- Zusätzlich zu den klassischen IT-, dedizierten Kompetenz- und Cybersecurity-Funktionen für den industriellen OT-Sektor (Operational Technology)
- Hochflexible Serviceplattform (Architektur, Szenarien usw.), die Schulungen und Übungen entsprechend den Kund*innenanforderungen ermöglicht
- Hohe Kompetenz am AIT bei Technologien, Methoden und Werkzeugen der Cybersicherheit aufgrund der engen Vernetzung zu Forschung und Forschungsprogrammen.

8.3 Mentimeter Planspiel

Der erste Lösungsansatz zur Vermittlung von Cybersicherheitsbasics wurde im Anschluss an die Auswertung der Umfrage in Deliverable 4.1 entwickelt. Aufgrund dessen wurde via Mentimeter ein passendes Szenario erstellt und interaktiv übermittelt. Das Basis-Szenario spielt in der „was wäre wenn“ Perspektive und führt die teilnehmenden Personen durch einen alltäglichen Arbeitstag im Home Office. Im Laufe des Szenarios treten einige Cybersicherheitsprobleme auf. Die teilnehmenden Personen können dazu jeweils über Mentimeter aus vorgegebenen Antwortmöglichkeiten anonym wählen, wie sie auf die auftretenden Probleme reagieren würden. Die aggregierten Ergebnisse werden im Anschluss direkt diskutiert, um somit Bewusstsein für die Situation und Gefühl für die richtigen Reaktionen zu entwickeln. Die Themen, die dabei (unterbewusst) behandelt wurden, sind die allgemeinen Schutzziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Darauf wurden die Teilnehmer*innen im Anschluss an die Übung auch hingewiesen. In Summe dauerte die Cyberübung jeweils in etwa 30 Minuten mit anschließender Diskussion. Somit kann die Cyberübung ideal in regulären Workshop-Slots durchgeführt werden. Das Basis-Szenario „Home-Office“ kann dabei ohne viel Aufwand leicht adaptiert werden, um für eine bestimmte Personengruppe ansprechender zu werden. Bei einer Durchführung wurde zum Beispiel statt dem „Home-Office“ das „Lehrer*innenzimmer“ genutzt, um die Übung an eine Durchführung mit Lehrer*innen anzupassen. In Summe wurde das Szenario mittlerweile zwei Mal erfolgreich durchgeführt:

- 23.06.2022 Laura Bassi Netzwerkforum – 7 Teilnehmer*innen
- 02.11.2022 eEducation Fachtagung Linz – ca. 40 Teilnehmer*innen

Anschließend werden wir das Basis „Home-Office“ Szenario anhand der Präsentationsinhalte und der gestellten Fragen näher erklären:

1. **Erklärungen zum Planspiel:** Die Teilnehmer*innen stellen im Szenario sich selbst dar und simulieren einen stressigen Home-Office-Tag, an dem viele berufliche Tasks anstehen,

[74] www.iaea.org

aber auch die eine oder andere private Aufgabe erledigt werden muss. Gearbeitet wird auf einem beruflichen Arbeitslaptop.

2. **Einstiegsfragen:** Zur Auflockerung und zum Kennenlernen der Mentimeter-Plattform wurde eine Einstiegsfrage gestellt. Sie lauten: *„Mit welchem Getränk starten Sie in Ihren Homeoffice-Tag?“* und *„Welche unerwünschten Besucher*innen werden Ihre heutige Videokonferenz stören?“*
3. **Verfügbarkeit:** Durch den Stress und die Unaufmerksamkeit wird unabsichtlich auf eine Phishing-Email geklickt. Es wird eine Verschlüsselungsattacke ausgeführt und alle Daten am PC sind verschlüsselt. Es wird ein Lösegeld in Höhe von 0,00025 Bitcoin gefordert. Am Laptop waren sowohl private Dateien (wichtige Passwörter, private Fotos, Adressbücher) als auch berufliche Dateien (personenbezogene Kund*innendaten, Arbeitsdokumente des letzten Quartals, geheime Arbeitsdokumente). Im Anschluss an diese Erklärungen wurde folgende Frage gestellt: *„Wie schlimm wäre für Sie der Verlust welcher Daten?“.* Für die meisten Personen wurde der Verlust der privaten Daten schlimmer gewertet als der Verlust der beruflichen Daten. Zudem wurde gefragt: *„Welche der folgenden Schritte würden Sie in dieser Situation setzen?“.* Die meisten Personen würden daraufhin eine Person oder Organisation um Hilfe fragen. Die nächste Frage lautete: *„Sie haben sich entschieden eine Person um Hilfe zu fragen. Die Person rät Ihnen, nicht zu bezahlen. Was tun Sie im Anschluss?“* Die meisten haben diese Frage mit „Ich bezahle nicht“ beantwortet.
4. **Vertraulichkeit:** Hier wurde direkt mit einer Fragestellung begonnen. *„Plötzlich sendet Ihnen ein wertvoller Kunde einen Link zu. Dieser zeigt, dass Daten von diesem im Internet aufgetaucht sind. Was tun Sie?*“ Die meisten Personen antworteten darauf, dass sie sich den Link vorerst genauer ansehen oder eine Person oder Organisation um Hilfe fragen. Danach wurde gefragt wen die Teilnehmer*innen in dieser Situation kontaktieren würden. Die meisten würden erneut eine Person in ihrer Organisation kontaktieren oder ihre IT-Dienstleister*innen.
5. **Integrität:** Dann wird eine E-Mail im Namen der teilnehmenden Person ausgeschickt. Die Person wird darüber von Freunden informiert. Danach wird folgende Frage gestellt: *„Wie reagieren Sie auf diese Information?“* Die meisten Personen würden daraufhin eine Person oder Organisation um Hilfe fragen oder ihr E-Mail-Passwort neu setzen.
6. **Diskussion:** Im Anschluss wird mit den Teilnehmenden über die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität diskutiert und es werden Erfahrungen ausgetauscht.

Dieses Planspiel ermöglicht den Teilnehmenden ohne Notwendigkeit von Vorkenntnissen oder technischer Unterstützung ein Cyber-Vorfallsszenario zu durchlaufen und mögliche Reaktionen darauf zu diskutieren. Somit kann Bewusstsein für solche Szenarien geschafft werden.

8.4 Mini-Szenarios

Die von uns sogenannten „Mini-Szenarios“ sollen einen niederschwelligen Einstieg zu Cyberübungen liefern. Sie haben das Ziel, Cybersicherheitsgrundlagen in kleinen, kurzen Szenarios auch für unerfahrene Nutzerinnen und Nutzer zugänglich zu machen. So kann das Wissen über Cybersicherheit in Form von kleinen und verständlichen Übungen in eine breitere Öffentlichkeit getragen werden. Basierend auf der komplexen Infrastruktur der AIT Cyber Range werden Schulungen so gestaltet, dass Benutzer*innen jeglicher Herkunft, diese auch anwenden und verstehen können. Daher wurde versucht, Thematiken zu finden, die von der Zielgruppe angenommen werden und die für nützlich erachtet werden. Zusätzlich wird auf eine inklusive und einfache Sprache geachtet, damit die Einführung in die Materie nicht zu schwer wird. Die Idee ist, dass der Einstieg in die Cybersecurity geschaffen wird und eine Bewusstseinsbildung hinsichtlich der Maßnahmen für die Absicherung von Systemen da ist.

Die Mini-Szenarien sind daher zur Bewusstseinsbildung und Einführung in einige Cybersicherheits-basics gedacht. Nichtsdestotrotz sollen sie vorwiegend Hands-on auf der AIT Cyber Range ausgeführt werden. Es handelt sich dabei um kurze Szenarien (20-30 Minuten pro Szenario), welche aus drei wesentlichen Teilen bestehen:

1. Einführung: Eine kurze Einführung in das Szenario und die verwendeten Tools.
2. Hands-on: Praktische Übung zum Ausprobieren vorwiegend auf der AIT Cyber Range.
3. Auflösung: Auflösung der Übungen mit anschließenden Diskussionen und Erklärungen.

Zur Teilnahme an den Mini-Szenarien sind keine Vorkenntnisse notwendig. Sie können modular verwendet werden und je nach Kontext, Zielgruppe und Zeiterfordernis unterschiedliche eingesetzt werden. Sie wurden so ausgewählt, dass sie realitätsnah sind und eine wichtige Cybersicherheitsinformation beinhaltet, die nahezu jede Person betrifft. In den nachfolgenden Kapiteln werden sechs Mini-Szenarien sowie deren Inhalte, Ziele und technische Anforderungen detailliert dargestellt.

8.4.1 Smart Home

Das Smart Home Szenario soll auf die Relevanz von Sicherheit im Internet der Dinge (Internet of Things, IoT) hinweisen und vermitteln, wie herausfordernd es sein kann, dies sicherzustellen.

Ziele

Das konkrete Lernziel der Teilnehmenden ist, zu erkennen, was ein IoT-Endgerät sein kann, und dass die Datensammlung dieser Geräte oftmals sehr umfassend und ohne Beschränkungen vor sich geht. Die Teilnehmenden sollen erkennen können, wie sie Sicherheitseinstellungen vornehmen können und warum sie dies tun sollten.

Szenariobeschreibung

1. **Einführung*:***
   Sie haben sich für Ihr Zuhause einige Geräte besorgt, um ihr Heim „smart“ zu machen. Darunter ist auch eine intelligente Beleuchtung. Die intelligente Beleuchtung wird während der Installation mittels WLAN mit dem kabellosen Internet verbunden. Nun können Sie via App oder Web-Zugang Ihre Beleuchtung steuern.
2. ***Hands-on:***
   Die Umsetzung erfolgt auf einem Desktop-System (normaler PC-Zugang). Über diesen PC ist es möglich, die Beleuchtung zu analysieren (IP-Adresse, Sicherheitseinstellungen). Danach ist der Aufruf anderer Beleuchtungen möglich. Nun ist ersichtlich, dass in der näheren Umgebung auch andere (ungesicherte) Beleuchtungen existieren. Diese Übung kann auch mit anderen IoT-Geräten wie Sensoren, Webcams, etc. durchgeführt werden.
3. ***Auflösung:***
   Die Key-Messages, die vermittelt werden sollen, sind, dass man IoT Geräte prüfen sollte und notwendige Sicherheitseinstellungen vornehmen kann und soll. Dies wird anhand der genannten Beleuchtung vorgezeigt. Des Weiteren wird auf Seiten im Internet aufmerksam gemacht, die Informationen von unsicheren IoT-Geräten sammeln (wie z.B. shodan.io[75]).

Infrastruktur / Ressourcen

Zur Durchführung der Übung wird ein Web-Server benötigt, wo eine Website läuft, über die man die Beleuchtung ein- und ausschalten kann. Des Weiteren muss natürlich eine Schnittstelle gebaut werden, die es erlaubt eine physische, smarte Beleuchtung mit der AIT Cyber Range zu verbinden. Zudem benötigt jede teilnehmende Person eine Client-Maschine, die den Zugang zur Infrastruktur ermöglicht.

[75] https://www.shodan.io/

8.4.2 Unsicheres WLAN / Verschlüsselung

Dieses Mini-Szenario richtet sich an Teilnehmer*innen, die verstehen sollen, wie unsichere Internetverbindungen ihre persönliche Sicherheit beeinträchtigen können. Das Szenario beginnt mit einer Erklärung der grundlegenden Konzepte von Internetverbindungen und Netzwerksicherheit, einschließlich Verschlüsselung und Authentifizierung. Weiters wird den Teilnehmenden gezeigt, wie unsichere Internetverbindungen identifiziert werden können und welche Risiken bei der Verwendung entstehen können. Im praktischen Teil des Kurses werden Werkzeuge und Techniken gezeigt und zur Verfügung gestellt, um die Fähigkeit zu erhalten, selbstständig eine sichere Internetverbindung herzustellen, um so sicher im Internet verkehren zu können.

Ziele

Das Mini-Szenario soll den Teilnehmenden ermöglichen, die Funktionsweise von Internetverbindungen besser zu verstehen. Zudem wird vermittelt, welche Maßnahmen ergriffen werden können, um die Sicherheit im Internet zu verbessern. Das Szenario soll mit einer Diskussion über bewährte Methoden, die zur Verbesserung der Netzwerksicherheit führen, beendet werden.

Szenariobeschreibung

1. ***Einführung:***
   Die Teilnehmer*innen befinden sich in einer Alltagssituation und suchen nach Informationen zu Weiterbildungen und führen Unterhaltungen mit Freund*innen und Bekannten mittels Messenger Diensten durch. Die aufgerufenen Webseiten verfügen in der Standardkonfiguration über keine sichere Verbindung. Dies kann leicht von den Teilnehmer*innen über die Adresszeile beobachtet werden und durch das explizite Aufrufen über „https://“ behoben werden. Potenzielle Angreifer*innen könnten in der unverschlüsselten Konfiguration jede Nachricht mitlesen und jede Suchanfrage abfangen und umleiten.
2. ***Hands-on:***
   Die Teilnehmer*innen werden angewiesen, eine Website bewusst über eine unsichere Website aufzurufen. Auf der Website befindet sich ein Anmeldefeld, wo sich die Teilnehmenden mit User*innenname und Passwort anmelden können. Wird dies über eine unverschlüsselte Verbindung (http) gemacht, so werden diese Daten unverschlüsselt übermittelt. Die Übungsleitung platziert sich in der Mitte zwischen Server und den Teilnehmenden und kann so die Eingaben sichtbar machen. Danach wird das Ganze über eine verschlüsselte Verbindung (https) wiederholt. Nun kann man die Eingaben nicht mehr nachvollziehen.
3. ***Auflösung:***
   Nach der Übung wird den Teilnehmenden gezeigt, welche Probleme es am System oder in der Verbindung gegeben hat und wie diese einfach behoben werden können. Dazu wird nochmals explizit darauf eingegangen, was es bedeutet, wenn unverschlüsselte Verbindungen genutzt werden und welche Auswirkungen dies haben kann.

Infrastruktur / Ressourcen

Zur Durchführung der Übung wird ein Web-Server benötigt, wo Webseiten laufen, die sowohl verschlüsselte als auch unverschlüsselte Verbindungen zulassen. Zudem benötigt jede teilnehmende Person eine Client-Maschine, die den Zugang zur Infrastruktur ermöglicht.

8.4.3 Passwörter / Authentifizierung

In dieser Übung sollen die Teilnehmenden die Passwörter für vielgenutzte Services abändern. Dabei werden wichtige Basics im Bezug zur Passwortsicherheit übermittelt.

Ziele

Es soll vermittelt werden, wie wichtig es ist, dass unterschiedliche Passwörter bei unterschiedlichen Seiten genutzt werden. Zudem sollen die Teilnehmenden die Anforderungen an ein sicheres Passwort, sowie den Umgang mit Passwortmanagern, lernen.

Szenariobeschreibung

1. ***Einführung:***
   Auf dem Desktop der Teilnehmenden befindet sich eine Datei „einheitspasswort.txt“, in welcher das Passwort für alle genutzten Services hinterlegt ist. Die Aufgabe der Teilnehmenden ist es nun, sich bei allen Services anzumelden, das Passwort zu ändern und sicher aufzubewahren.
2. ***Hands-on:***
   Alle Services haben ein einfaches Einheitspasswort, welches in einer Datei namens „einheitspasswort.txt“ auf dem Desktop abgespeichert ist. Die Teilnehmenden können sich damit bei allen Services einloggen und die Passwörter abändern. Dazu können sie auch den bereits installierten Passwortmanager als Unterstützung nutzen.
3. ***Auflösung:***
   Es wird die Wichtigkeit betont, unterschiedliche Passwörter für die unterschiedlichen Seiten zu nutzen. Als Benutzende einer Seite hat man keinen Einblick wie Passwörter gespeichert sind und ob die Betreiber*innen eventuell Zugriff auf das Passwort haben. Falls ja, und das Passwort bei mehreren Seiten verwendet wird, hat eine Person, die das Passwort kennt, auch Zugriff auf alle anderen Services. Zudem werden Anforderungen an ein sicheres Passwort erläutert. Ein sicheres Passwort sollte keine persönlichen Daten beinhalten (z.B. Name, Geburtsdatum), aus Buchstaben, Zahlen und Sonderzeichen bestehen und eine je nach Anforderung passende Länge haben (8-12 Zeichen gelten als ausreichend sicher). Es wird nochmals eine Erklärung zu Passwortmanagern gemacht. Passwortmanager unterstützen dabei, Passwörter zu speichern. Somit kann man komplexe, unterschiedliche Passwörter wählen, ohne diese zu vergessen oder unsicher in txt-Dateien oder auf Zetteln aufzubewahren.

Infrastruktur / Ressourcen

Zur Durchführung der Übung wird ein Web-Server benötigt, wo einige Services laufen, die das Ändern von Passwörtern ermöglichen (OwnCloud, Wordpress, etc.). Zudem benötigt jede teilnehmende Person eine Client-Maschine, die den Zugang zur Infrastruktur ermöglicht.

8.4.4 Backups

In dieser Übung wird die Auswirkung eines kompletten Datenverlustes aufgezeigt und Grundlagen über Backup-Erstellung und Datensicherheit übermittelt.

Ziele

Es sollen die Auswirkungen eines Datenverlustes und somit die Wichtigkeit von Backups vermittelt werden. Zudem wollen wir das Bewusstsein für einen Ransomware-Angriff vermitteln und die Möglichkeiten zur Erstellung von Backups diskutieren.

Szenariobeschreibung

1. ***Einführung:***
   Die Teilnehmenden besitzen auf ihrer Client-Maschine einige Ordner, in denen sowohl private Daten (Fotos, Ausweisdokumente, Kontaktdaten, etc.) als auch wichtige berufliche Dokumente gespeichert sind. Da diese Daten bis jetzt noch nicht gesichert sind, soll im Zuge des Mini-Szenarios eine Datensicherung vorgenommen werden. Die Teilnehmenden können die Daten auf der OwnCloud speichern, die Zugangsdaten dazu sind im Passwortmanager abgelegt.

2. ***:***
   Die Teilnehmenden bekommen einige Minuten die Möglichkeit, die Datensicherung vorzunehmen. Nach der Datensicherung wird ein Ransomware-Skript ausgeführt und die Daten sind alle verschlüsselt. Das System wird komplett zurückgesetzt und die Daten sind verloren. Nun soll das Backup aus der OwnCloud geladen werden. Wurde zuvor getestet, ob das überhaupt funktioniert oder die Dateien beim Kopieren vielleicht fehlerhaft übertragen wurden?
3. ***Auflösung:***
   Es werden Möglichkeiten diskutiert, um Daten zu sichern, sowie einige Beispiele gezeigt. Zudem wird nochmals die Wichtigkeit von Backups erläutert und darauf hingewiesen, was es bedeutet, alle Daten zu verlieren.

Infrastruktur / Ressourcen

Zur Durchführung der Übung wird eine OwnCloud-Instanz zur Datensicherung benötigt. Zudem wird ein Skript benötigt, welches die Daten auf der Client-Maschine löscht oder verschlüsselt, um danach das Laden des Backups üben zu können. Zudem benötigt jede teilnehmende Person eine Client-Maschine, die den Zugang zur Infrastruktur ermöglicht.

8.4.5 Deep Fakes

Dieses Mini-Szenario soll den Teilnehmer*innen aufzeigen wie Deep Fakes funktionieren und welche potenzielle Gefahr davon ausgeht.

Ziele

Ziel der Übung ist es, dass die Teilnehmer*innen Bewusstsein und Medienkompetenzen aufbauen und Informationen, Videos und Daten aus dem Internet kritisch hinterfragen. Zudem sollen die Teilnehmenden lernen, wie man die Richtigkeit von Informationen sicherstellen kann.

Szenariobeschreibung

1. **Einführung:**
   Den Teilnehmenden werden Suchmethoden und Tools gezeigt, mit denen es möglich ist, Informationen zu verifizieren oder widersprüchliche Aussagen zu erkennen. Dazu werden im ersten Schritt einige Deep Fakes und Falschinformationen gezeigt und erklärt.
2. **Hands-on:**
   Den Teilnehmenden werden einige Videos gezeigt. Sie können danach Informationen darüber suchen und sollen beantworten, ob es sich dabei um einen Fake oder ein reales Video handelt.
3. **Auflösung:**
   Es wird aufgedeckt, welche Videos Desinformationen verbreitet haben und wie diese erkannt hätten werden können.

Infrastruktur / Ressourcen

Zur Durchführung der Übung werden lediglich Deep-Fake Videos und dementsprechend passende echte Videos benötigt.

8.4.6 Phishing

Dieses Mini-Szenario beschäftigt sich mit dem Themenkomplex der Phishing-Mails. Dazu erhalten die Teilnehmer*innen einen Überblick über die Varianten von Phishing-Mails und die Ziele, die durch die Angreifenden verfolgt werden.

Ziele

Das Ziel dieses Mini-Szenarios ist es, Bewusstsein für Phishing E-Mails zu schaffen und Möglichkeiten zu deren Identifikation zu vermitteln.

Szenariobeschreibung

1. **Einführung:**
   Den Teilnehmenden werden einige Phishing E-Mails gezeigt und gemeinsam untersucht, woran man diese erkennen kann.
2. **Hands-on:**
   Die Teilnehmenden sollen selbstständig eine Vielzahl von E-Mails analysieren und feststellen, bei welchen es sich um Phishing E-Mails handelt, oder welche legitimierte E-Mails sind.
3. **Auflösung:**
   Zur Auflösung wird aufgedeckt, welche E-Mails die Phishing E-Mails waren. Es wird gemeinsam analysiert, woran man dies erkennen könnte. Zudem wird nochmals diskutiert, welche Gefahr von Phishing E-Mails ausgeht und worauf man besonders achten muss.

Infrastruktur / Ressourcen

Zur Durchführung der Übung wird ein Mail-Server benötigt, über welchen die Teilnehmenden E-Mails abfragen können. Zudem benötigt jede teilnehmende Person eine Client-Maschine, die den Zugang zur Infrastruktur ermöglicht.

Die Mini-Szenarien wurden 28. September 2024 auf der Pädagogischen Hochschule Wien durchgeführt.

ABBILDUNG 14 IMPRESSIONEN MINI SZENARIEN 28.09.2024

8.5 Level-Up Trainingskurs

Der Level-Up Trainingskurs wurde dazu entwickelt, um den Besucher*innen einer Messe eine Möglichkeit zu bieten, um kurz und spielerisch grundlegende Themen der Cybersicherheit auseinanderzusetzen. Dazu gab es ein Fragespiel mit einigen Fragen zu Angriffstechniken, Passwortsicherheit und Maßnahmen zur Prävention von Cyberangriffen. Zudem erstellten wir auf der AIT Cyber Range eine vulnerable Web-Applikation, die es den Besucher*innen ermöglichte, unter einer umfassenden Anleitung eine SQL-Injection durchzuführen. Des Weiteren konnten die Besucher*innen eine Übung zu Kryptografie durchführen. Das Angebot richtete sich an das auf der Messe „Level-Up“ anwesende Publikum, also vorwiegend junge Menschen mit mehr oder weniger Vorkenntnissen in Cybersecurity. Diese Herangehensweise ermöglichte wertvolle Einblicke in die Welt der IT-Sicherheit.

Nachfolgend sind die Fragen zu den jeweiligen Themen sowie die Antwortmöglichkeiten aufgelistet. Die richtige Antwort ist jeweils in grün hinterlegt.

Angriffe:

- Welches der folgenden ist ein Beispiel für Social Engineering?
  - Das Scannen von Netzwerken nach Sicherheitslücken
  - Das Verschlüsseln von Daten zur Sicherheit

  - Das Manipulieren von Menschen, um vertrauliche Informationen preiszugeben
  - Das Installieren von Antivirensoftware
- Was ist ein Brute-Force-Angriff?
  - Ein physischer Angriff auf Server-Hardware
  - Der Versuch, Passwörter durch Ausprobieren vieler Kombinationen zu erraten
  - Eine Netzwerkdiagnosetechnik
  - Eine Methode zur Datenverschlüsselung
- Was bedeutet DDoS-Angriff?
  - Ein Angriff, bei dem ein Netzwerk mit einer Flut von Anfragen überlastet wird
  - Ein Versuch, Passwörter durch Raten zu erraten
  - Ein physischer Angriff auf Netzwerk-Hardware
  - Eine Methode zur Datenkomprimierung
- Was ist das Ziel eines Man-in-the-Middle-Angriffs?
  - Die Manipulation von Hardware
  - Das Abfangen und mögliche Verändern von Daten während der Übertragung
  - Die Installation von Antivirensoftware
  - Die Verbesserung der Netzwerkgeschwindigkeit
- Was versteht man unter Zero-Day-Exploit?
  - Ein Sicherheitsupdate, das am selben Tag veröffentlicht wird
  - Ein neuer Computervirus, der noch nicht bekannt ist
  - Eine Sicherheitslücke, die ausgenutzt wird, bevor der Hersteller sie beheben kann
  - Ein Schutzmechanismus gegen Malware

Passwortsicherheit:

- Welches ist eine Methode, um ein sicheres Passwort zu erstellen?
  - Geburtstagsdaten verwenden
  - Namen von Haustieren verwenden
  - Eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
  - Einfache Wörter aus dem Wörterbuch verwenden
- Welches der folgenden Passwörter ist am sichersten?
  - SuperSecretPassword
  - SecurePassword1986
  - 4m%8Phi!m
  - 3x@mpl3P@$$w0rd!
- Welche der folgenden Aussagen über Passwörter ist korrekt?
  - Je länger das Passwort, desto schwieriger ist es zu knacken
  - Kurze Passwörter können, wenn sie besonders komplex sind, auch sicher sein
  - Wenn ich ein wirklich sicheres Passwort habe, kann ich es auch für mehrere Dienste verwenden
  - Geburtsdaten sind bei der Nutzung in Passwörtern unbedenklich
- Was ist Zwei-Faktor-Authentifizierung (2FA)?
  - Eine Methode zur Datenwiederherstellung
  - Ein Verfahren, das zwei verschiedene Methoden zur Verifizierung der Identität einer benutzenden Person erfordert
  - Ein Verschlüsselungsalgorithmus für zusätzliche Sicherheit des Passworts
  - Ein Passwortmanager

Prävention:

- Was ist eine Firewall?

    - Ein Gerät zur Verbesserung der WLAN-Reichweite
    - Eine Software oder Hardware, die den Datenverkehr zwischen zwei Netzwerken überwacht und kontrolliert
    - Ein Programm zur Erstellung von Backups
    - Ein Protokoll zur Datenkomprimierung
- Warum ist es wichtig, Software-Updates zu installieren?
    - Sie verbessern immer die Benutzeroberfläche
    - Sie fügen neue Funktionen hinzu
    - Sie beheben Sicherheitslücken und schützen vor Bedrohungen
    - Sie erhöhen immer die Internetgeschwindigkeit
- Was ist das Hauptziel von Antivirus-Software?
    - Die Geschwindigkeit des Computers zu erhöhen
    - Die Überwachung der Internetnutzung
    - Das Erkennen und Entfernen von Schadsoftware
    - Das Erstellen von Sicherheitskopien
- Was ist der Hauptzweck einer Datenverschlüsselung?
    - Die Beschleunigung der Datenübertragung
    - Die Reduzierung des Speicherplatzes
    - Der Schutz von Daten vor unbefugtem Zugriff
    - Die Verbesserung der Bildqualität
- Warum sollte man niemals unbekannte USB-Sticks verwenden?
    - Sie sind immer langsam
    - Sie könnten beschädigt sein
    - Sie könnten Malware enthalten, die den Computer infiziert
    - Sie sind immer zu klein, um wichtige Daten zu speichern
- Welche der folgenden Maßnahmen kann helfen, die Sicherheit eines drahtlosen Netzwerks zu erhöhen?
    - Das Verwenden von Standardpasswörtern
    - Das Deaktivieren von Verschlüsselung
    - Das Ändern des Standard-SSIDs und Verwenden starker Passwörter
    - Das Teilen des WLAN-Passworts mit allen

Der Level-Up Trainingskurs wurde am 29. und 30. Juni 2024 auf der Messe „Level-Up“ im Messegelände Salzburg durchgeführt.

8.6 ARES Workshop CTF

Der ARES Workshop Capture the Flag (CTF) wurde entwickelt, um den Teilnehmer*innen die Möglichkeit zu bieten, auf spielerische Weise tiefergehende Kenntnisse der Cybersicherheit zu erwerben. In einem interaktiven Format verfolgten die Teilnehmer*innen verschiedene Aufgaben, die darauf abzielten, versteckte „Flags“ auf der AIT Cyber Range zu finden. Jede Aufgabe wurde von umfassenden Erklärungen begleitet, sodass auch Personen ohne spezifische Vorkenntnisse eine Chance hatten, die Herausforderungen zu meistern. Das Konzept basierte auf den Mechanismen eines typischen Computerspiels, bei dem verschiedene Rätsel gelöst werden müssen, um Fortschritte zu erzielen. Der CTF wurde am 30. Juli 2024 im Rahmen der ARES Konferenz 2024 (The International Conference on Availability, Reliability and Security 2024) als Workshop durchgeführt und stieß auf großes Interesse.

Das Ziel des Workshops war es, den Teilnehmer*innen grundlegende wie auch fortgeschrittenere Fähigkeiten im Bereich der IT-Sicherheit zu vermitteln. Dabei standen folgende Aspekte im Fokus:

- **Vertiefung der Kenntnisse über Cybersicherheitstools:** Durch die praktische Anwendung von Tools wie Wireshark sollten die Teilnehmenden deren Funktionsweise und Nutzen in der IT-Sicherheit besser verstehen.
- **Sensibilisierung für typische Schwachstellen und Sicherheitslücken:** Die Herausforderungen zielten darauf ab, typische Sicherheitsrisiken sichtbar zu machen, die im Alltag und in IT-Systemen auftreten können.
- **Erlebnisorientiertes Lernen:** Der CTF wurde als „Gamified Learning“ aufgebaut, bei dem Lernen durch Spaß und Herausforderungen besonders gefördert wird.

Der CTF bestand aus verschiedenen Aufgaben, die unterschiedliche Facetten der Cybersicherheit abdeckten. Jede Aufgabe beinhaltete eine neue Herausforderung, die spezifische Fähigkeiten erforderte, aber stets so gestaltet war, dass auch Anfänger*innen davon profitieren konnten. Dabei waren Aufgaben vorwiegende so aufgebaut, dass man gewisse Sachen lösen musste, um Hinweise auf folgende Aufgaben zu erlangen. Im Folgenden sind die wesentlichen Aufgaben sowie die Ziele und Herausforderungen beschrieben:

- **Analyse von Wireshark-Paketen**: Das Ziel ist es, den Teilnehmer*innen die Möglichkeit zu geben, den Netzwerkverkehr mithilfe des Tools Wireshark zu analysieren. Sie sollten vor allem lernen, wie Netzwerk-Pakete aufgebaut sind, und wie Traffic im Internet eigentlich vonstattengeht.
- **Durchforsten von Ordnern:** Das Ziel war es, Grundlagen des Dateimanagements zu erlernen und zu verstehen, wie sensible Daten innerhalb eines Dateisystems verborgen oder versteckt sein könnten. Dabei wurden Techniken zur effizienten Dateisuche und zur Nutzung von Kommandozeilen-Tools vermittelt.
- **Analyse von HTTP und HTTPS:** Es sollten die Unterschiede zwischen verschlüsselten und unverschlüsselten Verbindungen verstanden und die Risiken von unverschlüsselten Verbindungen erkannt werden. Dazu waren Webseiten implementiert, die sowohl über HTTP als auch über HTTPS erreichbar waren. Es ging darum zu erkennen, welche Informationen bei der unverschlüsselten Verbindung für Angreifer*innen sichtbar wären, und wie eine sichere Verbindung zum Schutz von Daten beitragen kann. Dazu wurde auch die Analyse von Wireshark-Paketen verwendet.
- **Kryptografische Zeichenfolgen entschlüsseln:** Damit sollten grundlegende kryptografische Methoden und deren Anwendung verstanden werden. Die Aufgabe beinhaltete die Anwendung von Techniken wie Caesar-Verschlüsselung oder Base64-Decodierung, um die versteckten Flags zu extrahieren.
- **Passwortmanager:** Ein zentraler Trainingspunkt war auch die Anwendung eines Passwortmanagers. Die Teilnehmer*innen sollten die Wichtigkeit sicherer und einzigartiger Passwörter verstehen und lernen wie Passwortmanager dabei unterstützen können, komplexe und unterschiedliche Passwörter sicher zu speichern.

Zur Durchführung des Workshops wurde die AIT Cyber Range genutzt. Jede teilnehmende Person hatte Zugriff auf eine virtuelle Maschine, auf der die Tools installiert waren, die für die jeweiligen Aufgaben benötigt wurden.

Beim von uns getauften „CyberHunt - Hands-On Workshop CyberHunt“[76] gab es zwei nacheinander verlaufende Sessions die jeweils 90 Minuten dauerten. Es gab keine Voranmeldung, die Personen kamen zum Workshoptermin lt. Agenda. Bei CyberHunt 1 kamen 18 Personen. Davon waren 15 männliche und 3 weibliche Teilnehmende. Bei CyberHunt 2 waren etwas weniger, und zwar 11 Personen, wovon 7 männlich und 3 weiblich waren. Das heißt, es gab einen Frauenanteil von 21%. Das Organisationskomitee der ARES Konferenz war so freundlich uns eine Geschlechterverteilung der Konferenz 2024 zukommen zu lassen, diese betrug 282 männliche und 80 weibliche

[76] https://www.ares-conference.eu/cyberhunt (letzter Besuch am 01.10.2024)

Teilnehmer. Das ergibt einen Frauenanteil von 22%. Hier sieht man, dass unser Workshop genau im Schnitt der Konferenz lag.

ABBILDUNG 15 IMPRESSIONEN CYBERHUNT ARES KONFERENZ 2024

8.7 Conclusio

Die unterschiedlichen Cyberübungstypen, die im Projekt INDUCE entwickelt wurden, haben gezeigt, dass niederschwellige, diversitätsfreundliche Ansätze im Bereich des Cybersicherheitstrainings äußerst effektiv sein können. Die Entwicklung und Durchführung von unterschiedlichen Formaten, wie dem Mentimeter-Planspiel, den Mini-Szenarien, dem Level-Up Trainingskurs und dem ARES Workshop CTF, haben eine breite Zielgruppe angesprochen und dabei Cybersicherheitsinhalte verständlich und spielerisch vermittelt. Besonders hervorzuheben ist die Vielfalt der Übungen, die von kurzen interaktiven Szenarien bis hin zu praxisnahen CTF-Herausforderungen reichte, und damit sowohl Anfänger*innen als auch Fortgeschrittene gleichermaßen einbezog.

Durch die bewusste Gestaltung der Übungen auf der AIT Cyber Range und die Fokussierung auf verständliche Sprache sowie den spielerischen Umgang mit den Themen, konnten wichtige Cybersicherheitsaspekte erfolgreich vermittelt werden. Die diversen Cyberübungen konnten so einen wertvollen Beitrag zur Sensibilisierung und Weiterbildung im Bereich der Cybersicherheit leisten, und haben gezeigt, dass ein diversitätsorientierter und inklusiver Ansatz nicht nur nötig, sondern auch praktikabel ist, um die breite Bevölkerung in der IT-Sicherheit zu stärken.

9 Konzept und Gestaltung der Future Labs (INFRA)

9.1 Einleitung INFRAPROTECT® Future Labs (IFLs)

Das Ziel der INFRAPROTECT® Future Labs ist es, eine „Laborumgebung“ zu schaffen in der die Anforderungen an die verschiedenen Diversitätsdimensionen bei Cybersecurity Themen erfasst und strukturiert werden können. Auf Basis dieser Zielsetzung wurde ein „Wissensspeicher“ auf einer Web-Plattform zusammengestellt, der in weiterer Folge für die weiteren Entwicklungsschritte herangezogen werden kann oder genutzt wurde. Dazu wurden die bestehenden Inhalte von Cybersecurity Übungen und die in AP4 entwickelten Szenarien und Übungen an die Zielgruppenbedürfnisse angepasst und strukturiert. Hierzu wurden die Ergebnisse aus AP2-AP4 genutzt. Der Wissensspeicher dient in weiterer Folge als Grundlage um verschiedene „Work-Flows“ abzubilden. Im Wesentlichen wurden folgende Punkte verfolgt:

- Erfassung und Zusammenstellung der Diversitätsdimensionen zur Definition und Festlegung der Aus- und Fortbildungsschwerpunkte der Dialoggruppen
- Vorbereitung und Design von Übungssettings und Übungsschwerpunkte sowie auch interaktive gestaltete Quizlets
- Freie Gestaltungsmöglichkeit von Diversitätsdimensions-, spezifischen Unterstützungs-, Nachlese- und Nachhör-Unterlagen (es wurden erste Schritte unternommen diese auch umzusetzen)
- Entwicklung von Aufbereitungs- aber auch Verteilmechanismen, um die Unterlagen in geschlossenen, aber auch offenen Gruppen zielgruppenspezifisch auf mobilen Devices zur Verfügung stellen zu können.

Der Schwerpunkt der Arbeiten im AP5 lag darin, die Aufbereitungs- und Verteilmechanismen zielgerichtet möglichst barrierefrei einer oder mehreren Gruppen während einer Übung sowie im Nachgang zu Aus- und Fortbildungen oder für weiterführende Übungen zur Verfügung zu stellen. Auf Basis der Ergebnisse der Arbeiten in AP2 und AP3 wurde hier ein interaktives Medium geschaffen, das auf allen gängigen Smartphones und Tablets funktioniert.

Die Aufbereitung der Inhalte können im Wesentlich nach zwei Gesichtspunkten strukturiert werden:

- Spezielle interaktive Hilfestellungen und Begleitung bei Übungen sowie bei Aus- und Fortbildungen
- Interaktive Hilfestellungen bei Realfällen (INFRAPROTECT®-Joker)

Im Ergebnis sind daher drei wesentliche Bausteine entwickelt worden:

- Tool zur Erfassung und Strukturierung von Cybersecurity Themen, die inhaltlich nach Verfügbarkeit, Integrität und Vertraulichkeit Zielgruppen-spezifisch aber auch bedarfsorientiert aufbereitet werden können (Freie Zusammenstellung von Themen und Arbeitsschwerpunkten, je nach Zielgruppenbedarf)
- Tool zur Distribution der Aufbereitungen via WEB-Download (es können Einzelpersonen aber auch Personengruppen erfasst und angesprochen werden)
- Inhaltlich frei gestaltbare Smartphone/Tablet/PC-App (Android, iOS, Windows), die entweder übungsspezifisch, allgemein präventiv oder reaktiv genutzt werden kann.

9.2 Zielsetzung der INFRAPROTECT® Future Labs (IFLs)

Die Grundidee des Arbeitspakets 5 war eine verbindende Funktion zwischen den definierten übergeordneten Zielen des Projekts darzustellen.

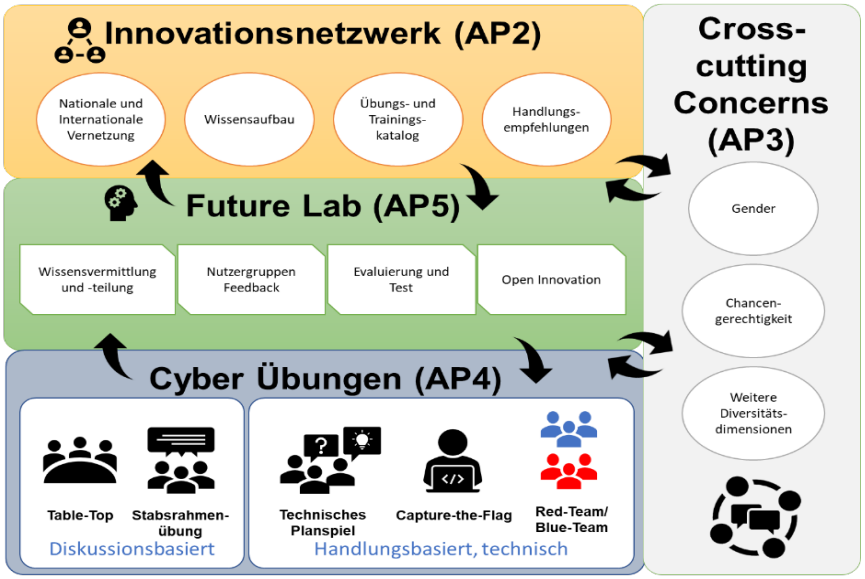


ABBILDUNG 16 ARBEITSPAKET STRUKTUR INDUCE

Das Design der INFRAPROTECT® Future Labs hat sich daher zum Ziel gesetzt:

- **Aus- und Fortbildung interaktiv und Dialoggruppen-spezifisch** zu unterstützen. Die Inhalte und Anforderungen wurden in AP2 bis AP3 gesammelt, zusammengestellt und ausgewertet. Ziel war die Anpassung der Themen und die Komplexität der aufbereiteten Themen an die Zielgruppen.
- **Übungen mit interaktiven Hilfestellungen zu begleiten und Hilfestellungen auf einem aktuellen Medium zur Verfügung zu stellen.** Der INFRAPROTECT® Joker geht dabei über eine deskriptive Hilfestellung hinaus, in dem er den Nutzenden zu Lösungen oder zu Lerninhalten durch „Tipp@Tricks“ hinführt.
- Das **gewonnene Wissen** strukturiert nach einer Übung in einer auf die Zielgruppe maßgeschneiderten **mobilen App** auch für Realfälle **immer verfügbar zu halten;** die App kann auf allen gängigen mobilen Devices zur Verfügung gestellt werden**.**
- Einen **Wissensspeicher** so **aufzubereiten** und zusammenzustellen, dass **Cybersecurity-Themen** je nach Zielgruppenbedarf **rasch und zielgerichtet** aufbereitet und verteilt werden können.
- **Erlerntes Wissen unmittelbar nach Übungen und/oder Aus- und Fortbildungen** basierend auf den Übungs- und Fortbildungserkenntnissen wird **angepasst, verteilt** und damit **verfügbar** gemacht werden.
- **Varianten und Möglichkeiten der Inhaltsaufbereitung von Cybersecurity Themen angepasst und iterierend an die Zielgruppenbedürfnisse möglichst einfach zu ermöglichen**
- **Die Weiterentwicklung von Incident- und Notfallmaßnahmen bei KMU, Kleinstunternehmen und Einzelunternehmer*innen** bei Cybersecurity Vorfällen zu unterstützen

Das Design der INFRAPROTECT® Future Labs orientiert sich dabei an dem PDCA-Zyklus.

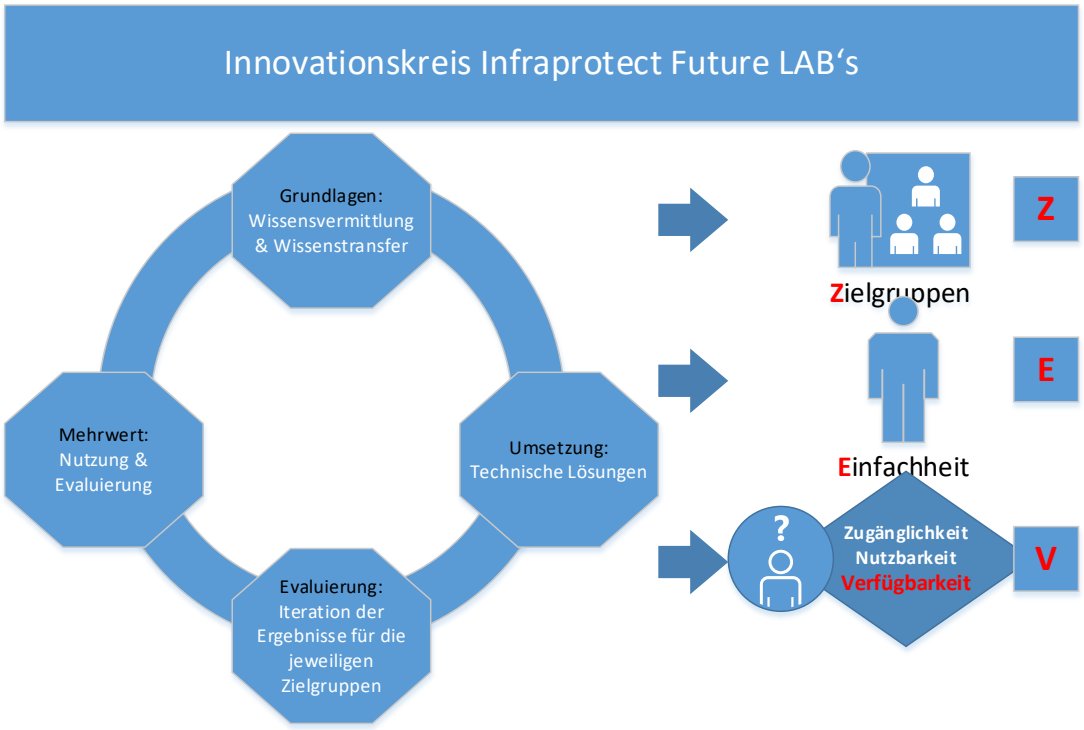


ABBILDUNG 17 PDCA-ZYKLUS

Im Fokus steht die Berücksichtigung der Bedürfnisse der identifizierten Zielgruppen, um mit Cybersecurity-Ereignissen oder -Situationen umgehen zu können. Die Ereignisbewältigungsstrategien sollen daher einfach verständlich und in weiterer Folge nachhaltig verfügbar gemacht werden. Um diesen Ansprüchen und Zielen gerecht zu werden, wurden in den IFLs mehrere technische Bausteine entwickelt, die sich in Summe als unterstützende Werkzeuge für die übergeordneten Projektziele von INDUCE nutzen lassen.

9.3 Technisches Design und Umsetzung der IFLs

9.3.1 Übersicht der INFRAPROTECT® Future Labs

Die IFLs bestehen im Wesentlichen aus drei Bausteinen:

- Baustein Wissensspeicher
- Baustein Distribution
- Baustein Vorhalten / Nachhaltigkeit / Hilfestellung

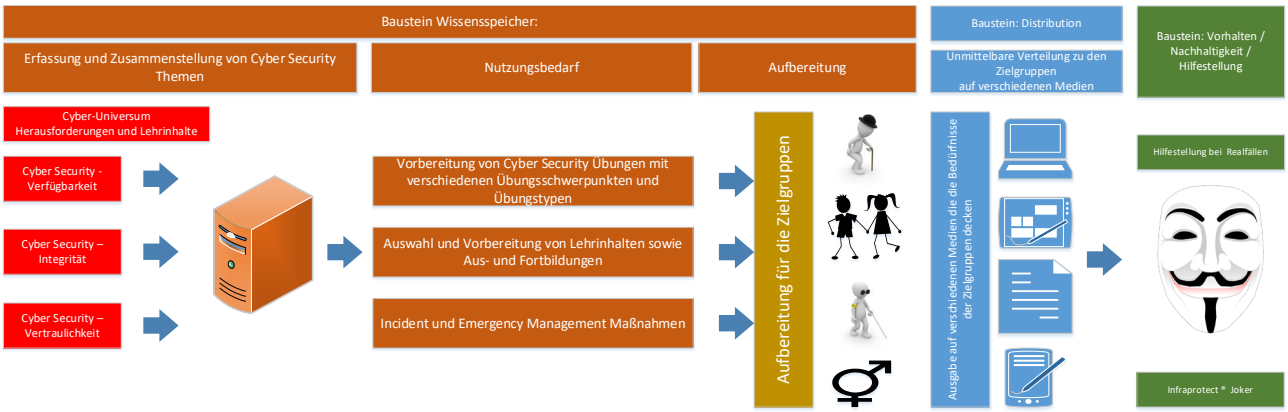


ABBILDUNG 18 ÜBERSICHT DESIGN DER INFRAPROTECT® FUTURE LABS (IFL)

9.3.2 Baustein Wissensspeicher der IFLs

Der Wissensspeicher besteht im Wesentlichen aus drei Aspekten:

- Dem Themenspeicher per se, der auf Basis rein technisch-organisatorischer Aspekte vorstrukturiert wurde.
- Welche Aufgabenstellungen zur Themenvorbereitung, für Übungen oder für Aus- und Fortbildungen, aber auch für die Entwicklung von Maßnahmenplänen in einem Ernstfall?
- Für welche Zielgruppe, welchem Nutzungsbedarf müssen die Inhalte aufbereitet werden?

Die Zusammenstellung von Cyberthemen erfolgte grundsätzlich nach Verfügbarkeits-, Integritäts- und Vertraulichkeitsthemen. Die Inhalte wurden in den AP3 und AP4 erfasst und in einem ersten Schritt in mehreren Excel-Arbeitsblättern strukturiert und in weiterer Folge geclustert. Die Inhalte wurden dabei nach rein technisch-organisatorischen Gesichtspunkten zusammengestellt. Eine gedankliche Struktur ist in folgender Abbildung zusammengestellt:

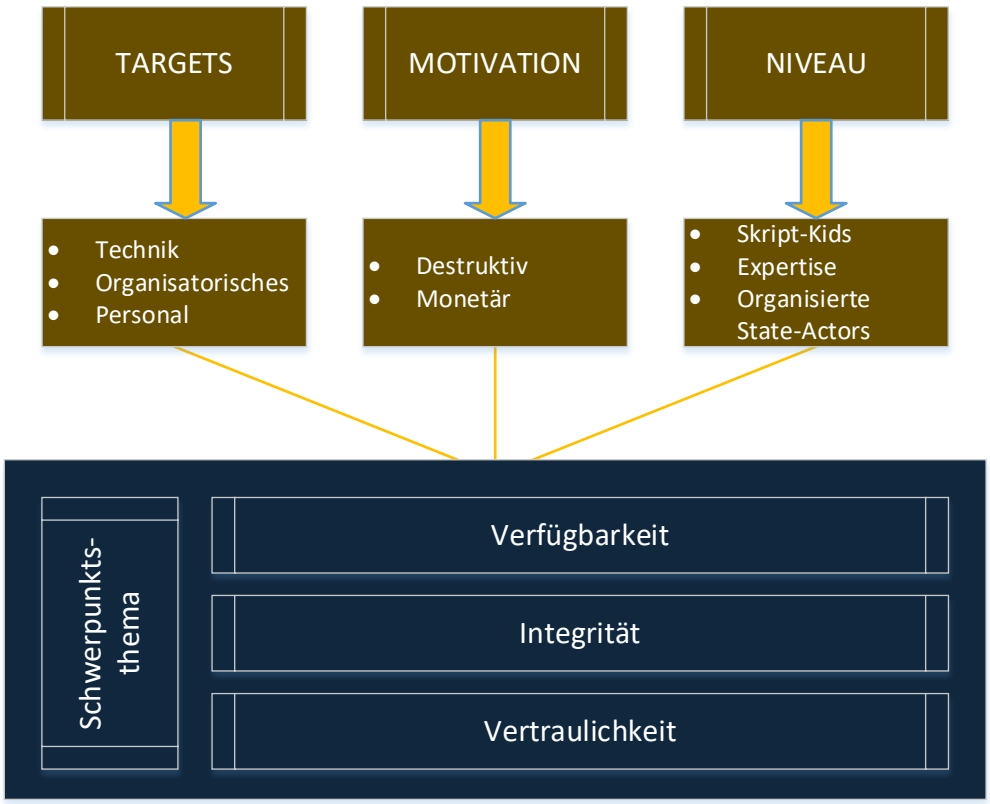


ABBILDUNG 19 ZUSAMMENSTELLUNG DER CYBERSECURITY THEMEN

9.3.2.1 Wissensspeicher: Erfassen und Zusammenstellung von Cybersecurity Themen

In folgender Abbildung sind die Themen beispielhaft technisch-organisatorisch strukturiert erfasst:

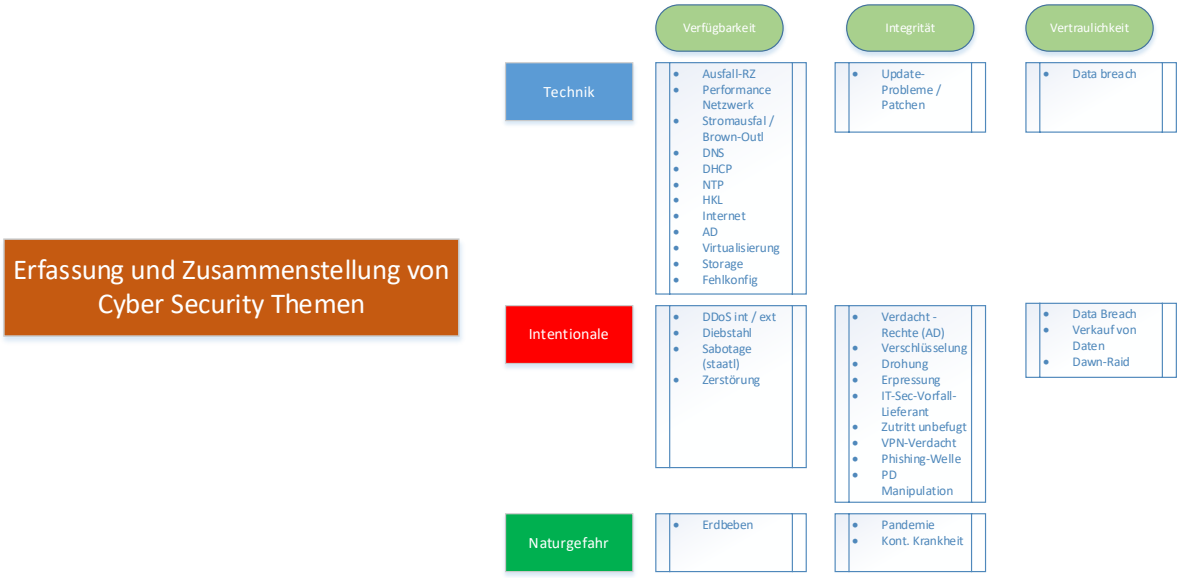


ABBILDUNG 20 ERFASSUNG UND ZUSAMMENSTELLUNG VON CYBERSECURITY THEMEN

9.3.2.2 Wissensspeicher: Nutzungsbedarf

Der Nutzungsbedarf wurde auf drei wesentliche Aspekte ausgerichtet:

Vorbereitung von Cyber Security Übungen mit verschiedenen Übungsschwerpunkten und Übungstypen

Auswahl und Vorbereitung von Lehrinhalten sowie Aus- und Fortbildungen

Incident und Emergency Management Maßnahmen

Im AP 4 sind die weiterentwickelten Szenarien dargestellt. Mit Blick auf die IFLs wurden die in ACCSA entwickelten Übungskomplexitäten für den Nutzungsbedarf herangezogen.

Lehrinhalte werden aus dem Wissensspeicher in mehrere „Abschnitte“ zerlegt.

Entwicklung und Implementierung von Notfallplänen.

9.3.2.2.1 Vorbereitung und Nutzung des Wissensspeichers für Übungen

Grundsätzlich werden die Szenarien nachfolgender Übungstypen strukturiert[77]:

Übungskomplexität	INFRAPROTECT® Grundlagen für die Einordnung von Übungskomplexitäten	BSI Standard 100-4
Einfach	Alarmübung/Einberufungsübung	Funktionstest
Normal	Team-Stress-Tests	Stabsübung
Anspruchsvoll	Ereignismanagement Übung (angekündigt)	Stabsrahmenübung
Komplex	Ereignismanagement Übung (unangekündigt)	Stabsrahmenübung + Kommunikations- und Alarmierungsübung
Sehr komplex	Vollübung ggfs. auch mit dislozierten Anteilen	Vollübung

Die Inhaltliche Ausgestaltung wurde im AP4 dargestellt. Die IFLs unterstützen in allen Phasen der Entwicklung von Cyberübungen.

[77] Vgl. dazu auch ACCSA Abschnitt 14.1

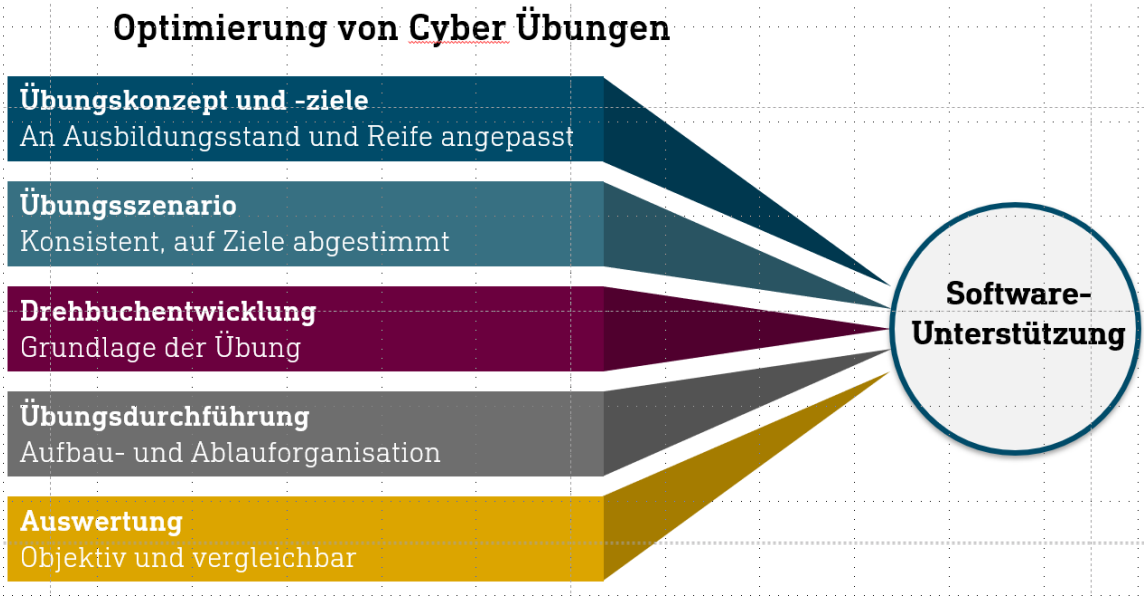


ABBILDUNG 21 OPTIMIERUNG VON CYBERÜBUNGEN

9.3.2.2.2 Nutzung des Wissensspeichers für die Verteilung von Lehrinhalten

Die Themen werden im Wissensspeicher in kleinteilig zusammengestellten Inhaltsabschnitten vorgehalten. Die Ordnungsstruktur richtet sich nach Verfügbarkeits-, Integritäts- und Vertraulichkeitsthemen.

Am Beispiel der Vorbereitung für eine Lehrstunde im Rahmen der Lego League, durchgeführt am 17.01.23 am Georg von Peuerbach Gymnasium, soll die technische Umsetzung verdeutlicht werden. Rechts die Darstellung der Abschnitte aus dem umfassenden Wissensspeicher, der in weiterer Folge zu einer App zusammengestellt wurde. Diese wurde den Schüler*innen zum „interaktiven Lernen“ zur Verfügung gestellt und ad hoc zum Download auf ihr Handy, Tablet oder Laptop angeboten. Links der Vortrag zu Cybersecurity für Kleinautomatisationen.

ABBILDUNG 22 ERGEBNIS: FOTO VON HANDY/TABLET-APP

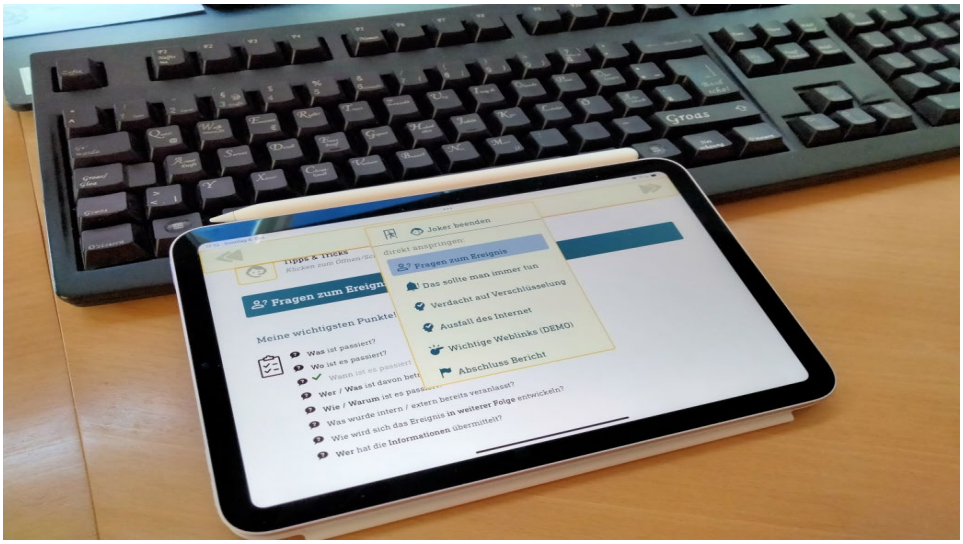


ABBILDUNG 23 UNTERSTÜTZENDE FORTBILDUNGS-APP, HIER FÜR SCHÜLER*INNEN IN DER 4.KLASSE GYMNASIUM

9.3.2.2.3 Nutzung des Wissensspeichers für die Entwicklung von Notfallplänen

Die Abschnitte können auch zur Abbildung von einfachen und/oder komplexen Notfallplänen herangezogen und assembliert werden. Im Ergebnis entstehen einerseits eine interaktiv nutzbare Mobile-App sowie ein ausdruckbares Dokument. Die inhaltliche Ausgestaltung und die Detaillierungstiefe werden im Arbeitsschritt Aufbereitung durchgeführt und festgelegt.

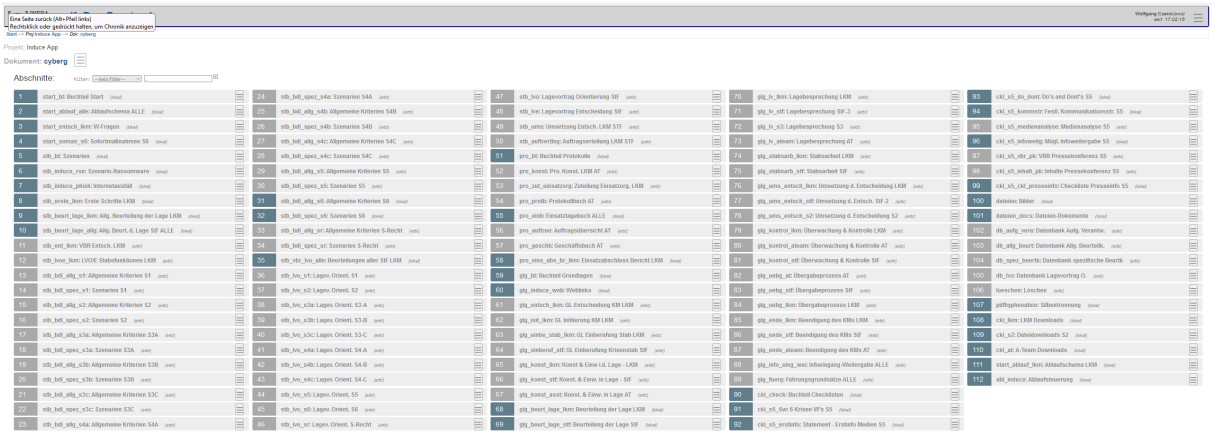


ABBILDUNG 24 ÜBERSICHT ÜBER EINEN KOMPLEX ABGELEITETEN NOTFALLPLAN BASIEREND AUF 112 ABSCHNITTEN AUS DEM WISSENSSPEICHER

In Abbildung 25 wird ein exemplarischer IT-Security Notfallplan für ein KMU in der App dargestellt.

ABBILDUNG 25 IT-SECURITY NOTFALLPLAN FÜR KMU

9.3.2.3 Wissensspeicher Aufbereitung

Basierend auf den Ergebnissen aus AP2 und AP3 wurden Zielgruppen definiert. Die Auswahl fand nach den folgenden Gesichtspunkten statt und kann anhand dieser vorgenommen werden.

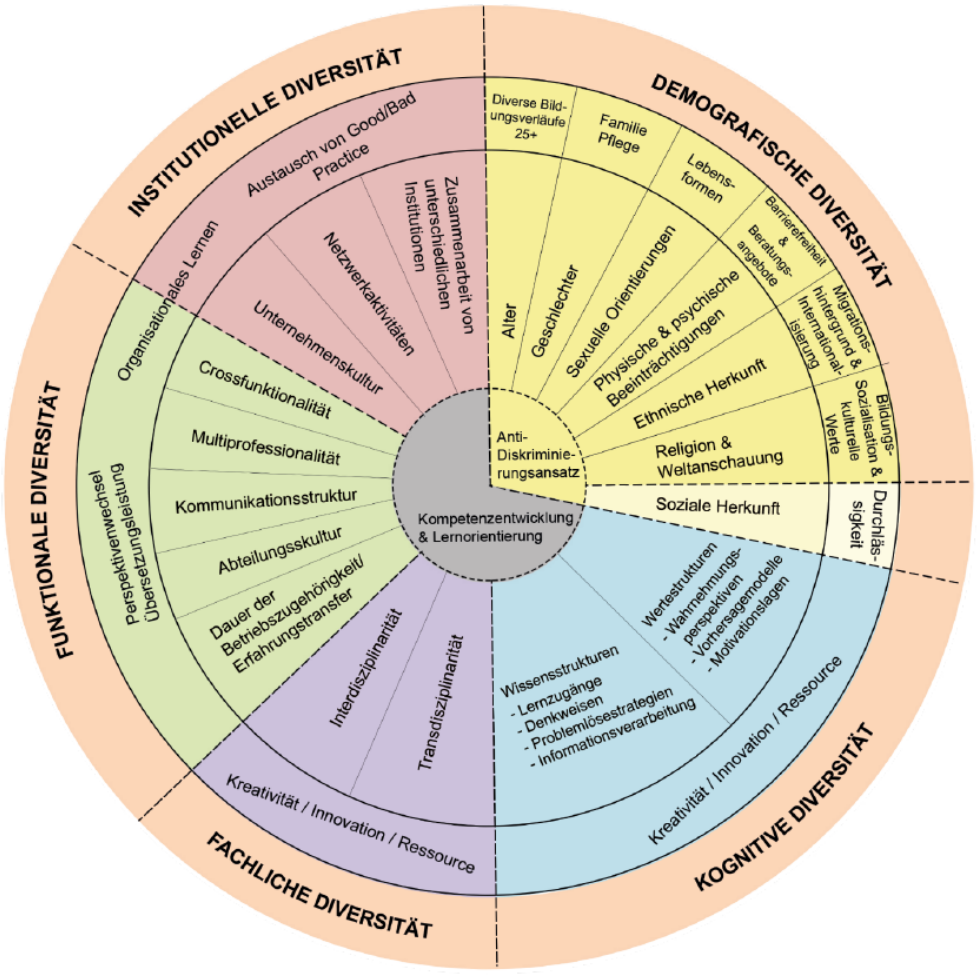


ABBILDUNG 26 DIVERSITÄTSDIMENSIONEN FH OBERÖSTERREICH

Im AP3 wurden mögliche Zielgruppen definiert. Im Rahmen der IFLs wurden neben den Kernzielgruppen der INFRAPROTECT® drei Zielgruppen näher ausdifferenziert betrachtet:

- KMU mit einer Mitarbeiter*innenzahl <100 Mitarbeiter*innen (Apotheken, Steuerberatungsunternehmen, Planungs-, Design- und Architekturbüros, kleine IT-Unternehmen)
- Einzelunternehmer*innen (Friseur*innen, Kosmetikstudios, etc.)
- Schüler*innen zumeist an Gymnasien oder Höheren Technischen Lehranstalten
-

Rein Gender-differenzierte Zielgruppen wurden in einem eigenen Workstream bei SBA (Stefanie Jakoubi) betrachtet.

Um die Aufbereitung der Zielgruppen entsprechend weiter zu detaillieren, fanden im Zeitraum November 2022 bis Ende Juni 2023 27 Workshops zu jeweils 2-3 Stunden für Apotheker*innen, statt. Erste Ergebnisse wurden zum Beispiel in Schladming am 06.03.2023 beim APOkongress (Wissenschaftliche Fortbildungen für Apotheker*innen) einem größeren Publikum vorgestellt und dabei evaluiert.

Im Zeitraum Mai 2023 bis Ende Juli 2024 fanden in Summe 15 Workshops mit Steuerberatungsunternehmer*innen statt. Hier wurden in Einzelinterviews die Anforderungen an die IT-Security erörtert.

Im Rahmen der Genese des Projekts und Feedbacks zu den mobilen Apps haben sich einige zuerst wenig beachtete Rahmenbedingungen als wichtig herausgestellt.

Je nach Bildungsniveau aber auch determiniert durch das Alter der Nutzer*innen mussten in mehreren Iterationen sowohl Graphiken als auch die Texte bei den Hilfestellungen (INFRAPROTECT®-Joker-Funktion) überarbeitet werden. Hinführende Tipps und eine Farbgebung, welche die Wichtigkeit von Arbeitsschritten und Empfehlungen herausstreichen sollen, wurden mehrfach bedürfniskonform angepasst.

Die jüngere Generation benötigt zum Erfassen deutlich mehr Piktogramme und Bilder als die Generation 40+.

Ein Potential für künftige Entwicklungen wird die deutliche Verbesserung und Berücksichtigung von barrierefreien Funktionen in den Apps adressieren müssen.

Dazu wurde u.a. bei Dokumentationen von Ereignisbewältigungsstrategien eine Spracheingabefunktion eingeführt.

Die Möglichkeit, individuell handschriftlich erfasste Inhalte nach erfolgter Übung oder Fortbildung den Lehrinhalten in der individualisierten App bei den entsprechenden Arbeitsschritten und den Maßnahmenplänen unmittelbar anzuhängen oder beizulegen, war eine zentrale Forderung. Die Integration der App in bestehende Arbeitsumgebungen wurde durch die Einbindung von Microsoft-Office365-Applikationen Rechnung getragen.

Zusammenfassend kann man festhalten, dass im Rahmen des Projekts die zielgruppenspezifische Inhaltsaufbereitung im Vordergrund stand. Mit Verfügbarkeit der ersten Prototypen konnten dann auch technische Anforderungen, die sich aus den verschiedenen Diversitätsanforderungen ableiten, formuliert und zum Teil berücksichtigt werden.

9.3.3 Baustein Distribution der IFLs

Bis dato wurden fachliche Inhalte über die üblichen Verteilmechanismen wie z.B. E-Mail, Download von Dokumenten auf zentralen File-Services oder Verweis auf Literatur bei Fortbildungsveranstaltungen, Newsletter mit Fachthemen etc. an die Zielgruppen verteilt. Mit dem Baustein Distribution der IFLs können nun neben den gewohnten Distributionswegen auch individualisierte Apps mit entsprechend zielgruppenspezifischen Inhalten über einen kanalisierten Distributionsweg (ohne Nutzung der App-Stores für Android-, iOS oder Windows Systeme) verteilt werden.

9.3.3.1 Technische Ausgestaltung der Distribution der „IFP-Loader“

Es besteht der Anspruch an das IFL, alle gängigen Betriebssysteme in die Laborumgebung zu integrieren. Die Informationen und die Tools sollen sich an spezielle Zielgruppen richten und in

einigen Fällen nur durch diese genutzt werden. Mit Blick auf IT-Security Themen kam eine Verteilung von Inhalten über die gewohnten Zugriffsmechanismen auf Apps nicht in Frage. Windows App Store, Google Play Store und iOS App Store kommen daher nicht in Betracht, da Apps im Wesentlichen von allen Internet Nutzer*innen heruntergeladen werden können. Der Distributionsmechanismus musste daher in zwei Stufen ausgestaltet werden:

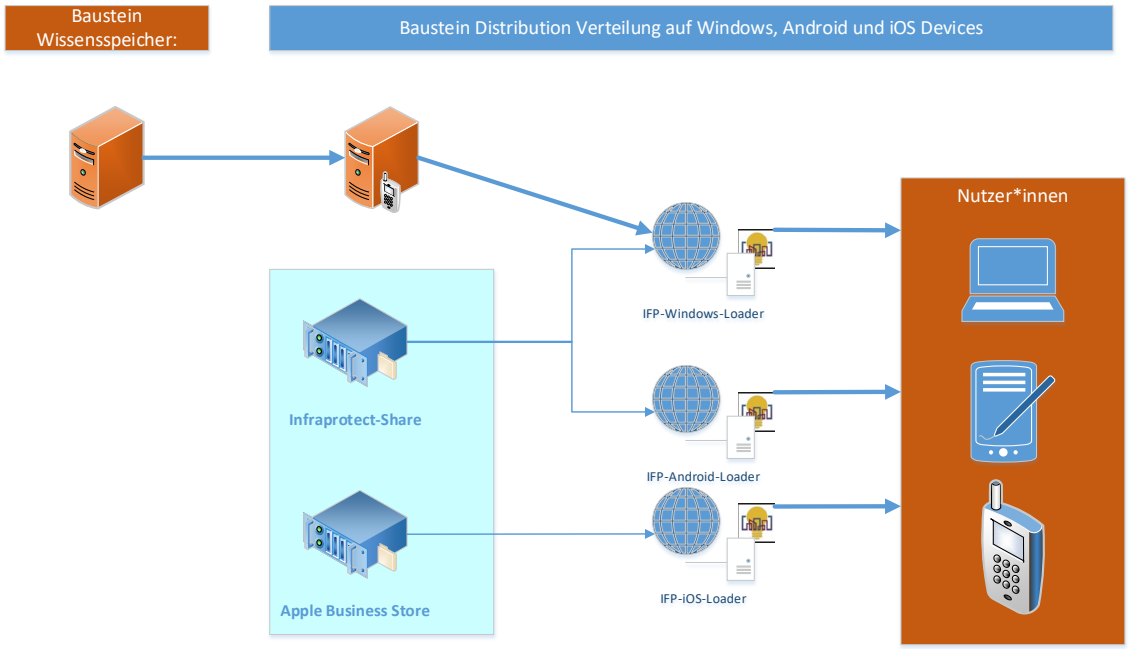


ABBILDUNG 27 DARSTELLUNG DISTRIBUTIONSMECHANISMUS

Das IFL stellt in einem ersten Schritt Loader-Software zur Verfügung. Die IFL-Loader Software der IFP-Loader für Windows und Android kann vom INFRAPROTECT® Share direkt bezogen werden.

Bei iOS muss dieser Schritt aus Gründen der Applevorgaben zwingend über den Apple Business Store erfolgen. Dazu bekommt jede*r Teilnehmer*in einen Weblink zugeschickt, um den IFP-Loader downloaden zu können. In diesem Arbeitsschritt werden KEINE Inhalte heruntergeladen.

Für Schulungen kann/muss/sollte dieser Schritt im Vorfeld kommuniziert werden. Bei der Entwicklung von Übungen und für Incident/Emergency Response Pläne wird dies im Zuge der Vorbereitungs- und Entwicklungsarbeiten durchgeführt.

Sobald der IFP-Loader installiert ist, kann man die im Wissensspeicher aufbereiteten Inhalte an Einzelpersonen oder an eine Gruppe verteilen. Dabei wird jede*r Teilnehmer*in einzeln erfasst, um in weiterer Folge individualisierte Inhalte oder gruppengültige Inhalte verteilen zu können. Dazu wird ein Token versandt. Der IFP-Loader erkennt anhand dieses Tokens welche individualisierten Inhalte zu laden sind und. installiert werden können. Danach stehen den Nutzenden eine individuell gestaltete App mit den entsprechenden Inhalten auf dem eigenen Device zur Verfügung.

9.3.3.1.1 Verteilungsserver

ABBILDUNG 28 VERWALTUNGSOBERFLÄCHE ZUM VERTEILUNGSSERVER

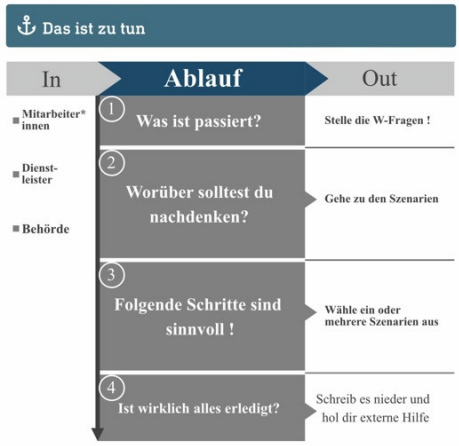
Aus diesem Tool heraus werden die einzelnen „Produkte“ verteilt.

Hier ein Screen-Shot aus einem iPAD-mini für das DEMO-Produkt CyerGuide. Nach Installation kann der Nutzende sofort loslegen. Je nach aufbereitetem Inhalt kann die App genutzt werden.

ABBILDUNG 29 SCREENSHOT DER APP

9.3.4 Baustein Vorhalten / Nachhaltigkeit / Hilfestellung in IFLs

Neben der Aus- und Fortbildung sowie Nutzung der begleitenden Hilfestellung bei Cybersecurity Übungen stellen die Entwicklung und Implementierung von Notfallplänen einen wesentlichen Teil der Supportleistungen der IFLs dar. Das IFL erlaubt mehr oder weniger frei gestaltbare App-Lösungen.



Die nachfolgende Übersicht zeigt einen Ausschnitt eines idealtypischen Plans, der für die jeweiligen Zielgruppen individuell angepasst werden kann.

Die Vorgehensweise orientiert sich dabei an den Zielgruppen für die eine Incident/ Emergency Plan-Unterstützung designt werden soll. Die Zielgruppen definieren die Aufbereitung, die Unterstützungsmöglichkeiten und den Detaillierungsgrad.

Ja nach Zielgruppe kann die Dokumentation auch barrierefrei über Spracheingaben erfolgen

Alle Eingaben und Tätigkeiten werden mit einem Zeitstempel versehen, um die Handlungen nachvollziehen zu können. (Diese Funktion kann auch deaktiviert werden).

Nach erfolgtem Training oder einer Übung können sich die Teilnehmenden auch ihre individuellen Notizen in die App-integrieren, um in einem Realfall wieder erinnert zu werden. Der INFRAPROTECT®-Joker wird sie daran erinnern und gibt „Tipps@Tricks“ in den jeweiligen Arbeitsschritten

9.4 Übungsevaluation nach Diversitätsdimensionen

Die Evaluierungen von Cyberübungen wurden im Rahmen der IFLs als moderierte Workshops umgesetzt. Dabei wurden grundsätzlich mehrere Reflexionsschritte durchlaufen. In allen Workshops wurde ein interaktiver Austausch mit den Zielgruppen anhand möglichst greifbarer Szenarien ermöglicht.

Die IFLs verfolgen dabei folgenden übergeordneten Ziele:

- Identifikation und Auswahl diversifizierter Auswertemethoden, basierend auf verschiedenen Zielgruppen
- Weiterentwicklung der Aufbereitung von Cybersecurity Themen für verschiedene Zielgruppen

- Weiterentwicklung des INFRAPROTECT® Reifegrad-Modells zur Vorbereitung, Durchführung und Auswertung von Übungen, basierend auf verschiedenen Diversitätsdimensionen.

Die Ziele wurden grundsätzlich in drei Schritten verfolgt:

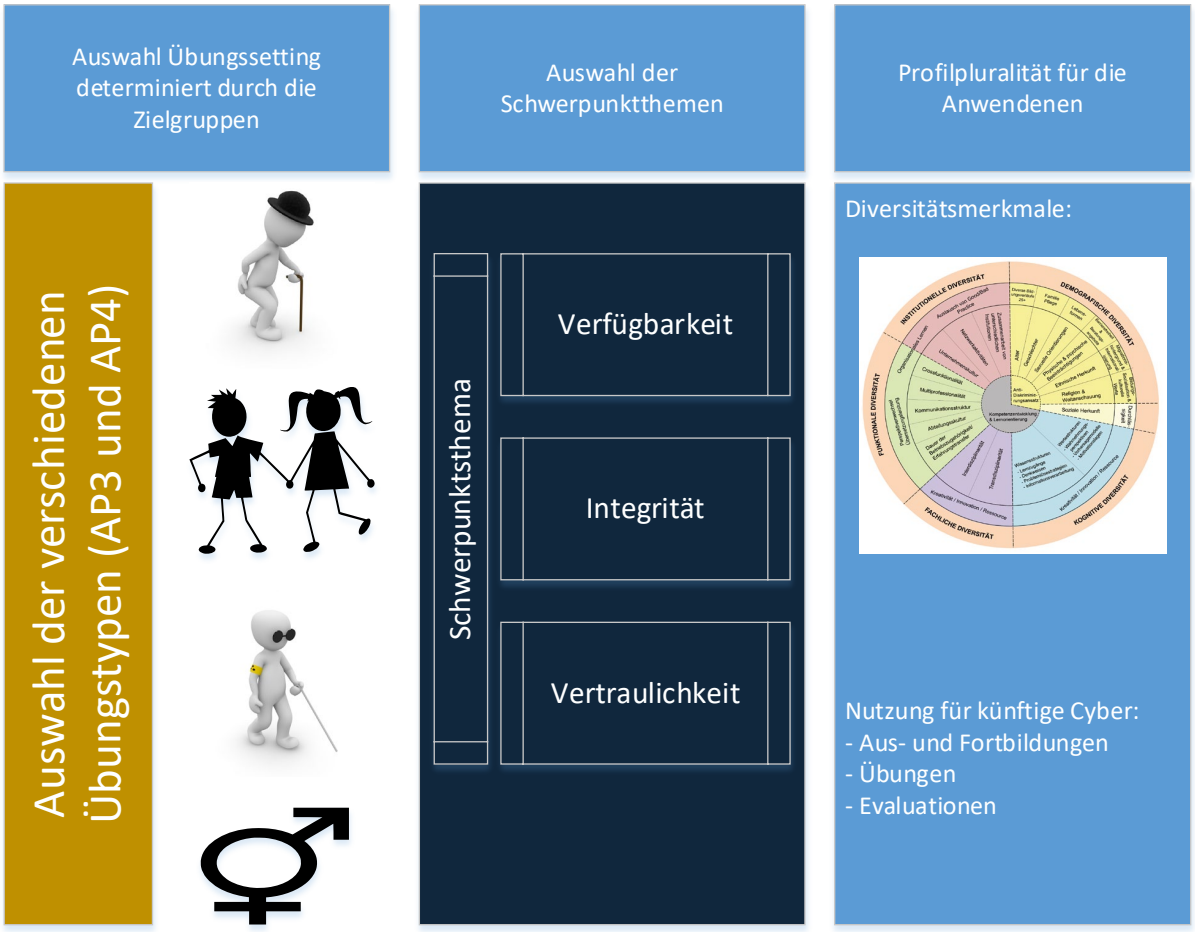


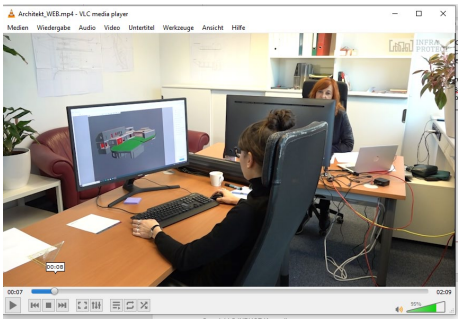
ABBILDUNG 30 ZIELVERFOLGUNG

Die beiden ersten Schritte basieren auf den Ergebnissen von AP2-AP4.

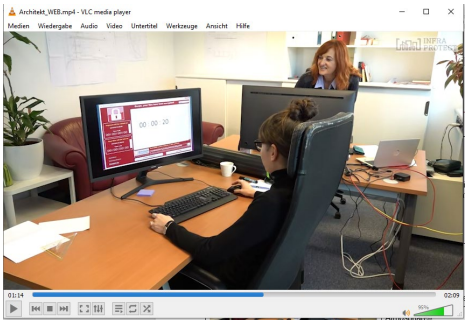
9.4.1 Schritt 1 und 2 – Übungssetting und Auswahl der Szenarien

Dazu wurden drei initiierende Videos zusammengestellt, die im Wesentlichen auf Verfügbarkeits-, Integritäts- und Vertraulichkeitsthemen hinführen sollten. Kurzdarstellung der Sequenzen:

Intro Vorstellung der Ziele des Workshops zur Evaluation



Darstellung der anzunehmenden Situation – möglichst in einer bekannten Atmosphäre



Darstellung der Schadwirkung mit einem wesentlichen Stressfaktor hier ein Count-down

Initiierende Fragen, die eine offene Diskussion erlaubt

In dieser Art und Weise wurden drei impulsgebende Videos mit realitätsnahen Beispielen von Cyberbedrohungen gedreht und in weiterer Folge für die Übungen genutzt.

Abhängig von der Zielgruppengröße wurde entweder eine moderierte Diskussion gestartet oder es wurde darauf aufbauend eine längere Übung mit verschiedenen zusätzlichen Injects durchgeführt. Für die weiteren Schritte ist es wichtig aufzuzeigen, dass die Größe der Teilnehmendengruppen immer ≥ 8 Personen waren, um der verfolgten Systematik gerecht zu werden. Nicht berücksichtigt sind daher Hybridveranstaltungen in den Schulen (Lego League), da es sich hier um spielerische Fragestellungen gehandelt hat. Die Systematik ist in AP4 beschrieben. Die Schulklassen hatten Gruppengrößen von 2, 4, 6 und 24 Schüler*innen.

Für die Fortentwicklung der Übungsevaluierungen wurden im Zeitraum 2023 und 2024 (bis Ende August) 24 Cyber Exercises mit Übungsteilnehmenden ≥ 8 Personen durchgeführt und in weiterer Folge anonymisiert ausgewertet. In Summe haben an diesen Übungen in unterschiedlichen Dimensionen 390 Teilnehmende mitgewirkt. Allerdings in stark unterschiedlichen Rollen. Von den 390 erfassten Teilnehmenden waren 65 in einer hybriden Rolle tätig. Einmal als aktive Teilnehmende und einmal als Teil der Übungsvorbereitungen.

Die Verteilung der Teilnehmenden kann man wie folgt darstellen:

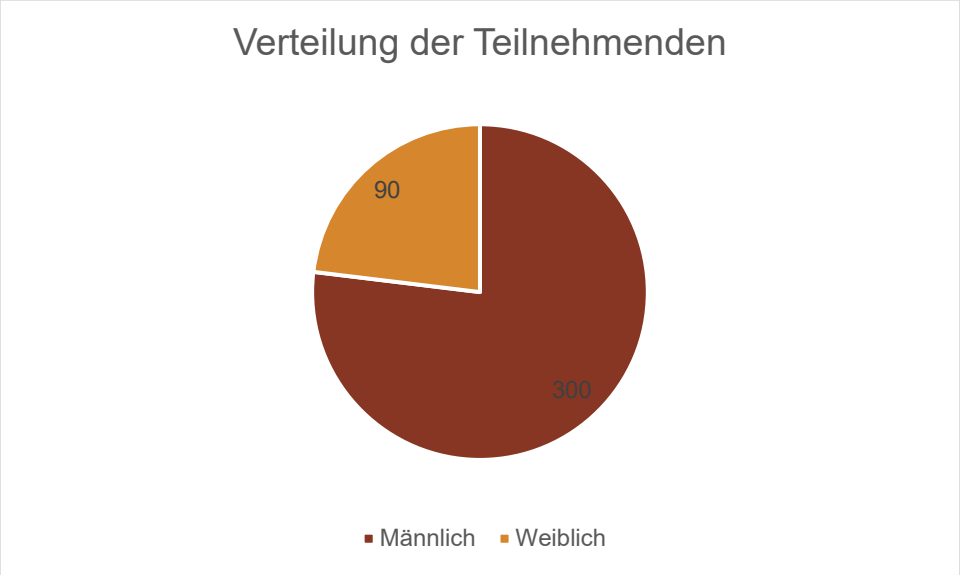


ABBILDUNG 31 VERTEILUNG DER TEILNEHMENDEN

Die Altersverteilung in Summe stellt sich wie folgt dar:

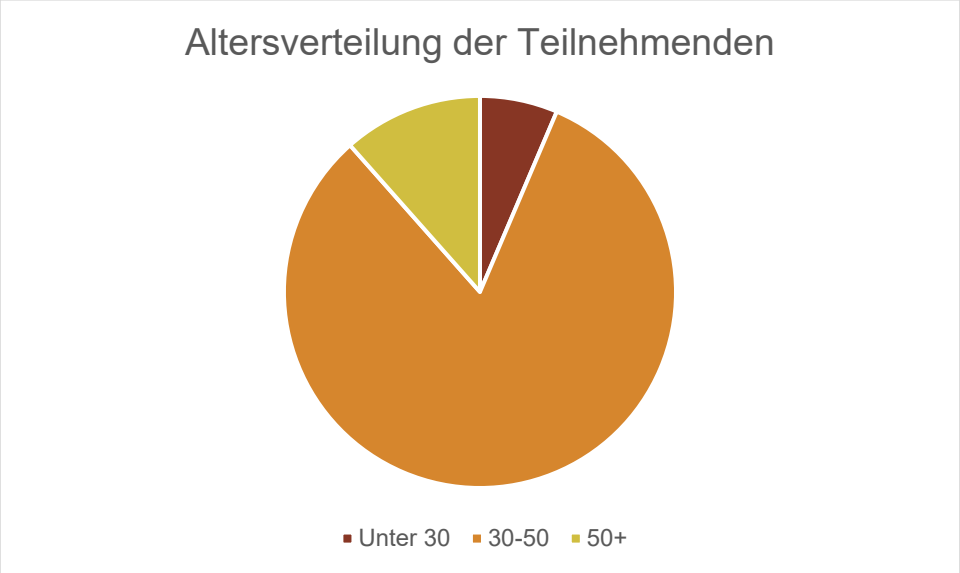


ABBILDUNG 32 ALTERSVERTEILUNG DER TEILNEHMENDEN

Weitere Aufteilungen

ABBILDUNG 33 ALTERSVERTEILUNG WEIBLICHER UND MÄNNLICHER TEILNEHMENDEN

9.4.2 Weiterführende Grundlagen

9.4.2.1 Allgemeines

Die weiteren Arbeitsschritte basieren im Wesentlichen auf der von INFRAPROTECT® entwickelten Grundvorgehensweise zur Übungsauswertung, die in den IFLs zur Anwendung gebracht wurden. Diese Vorgehensweise wurde in ACCSA[78] bereits detailliert beschrieben.

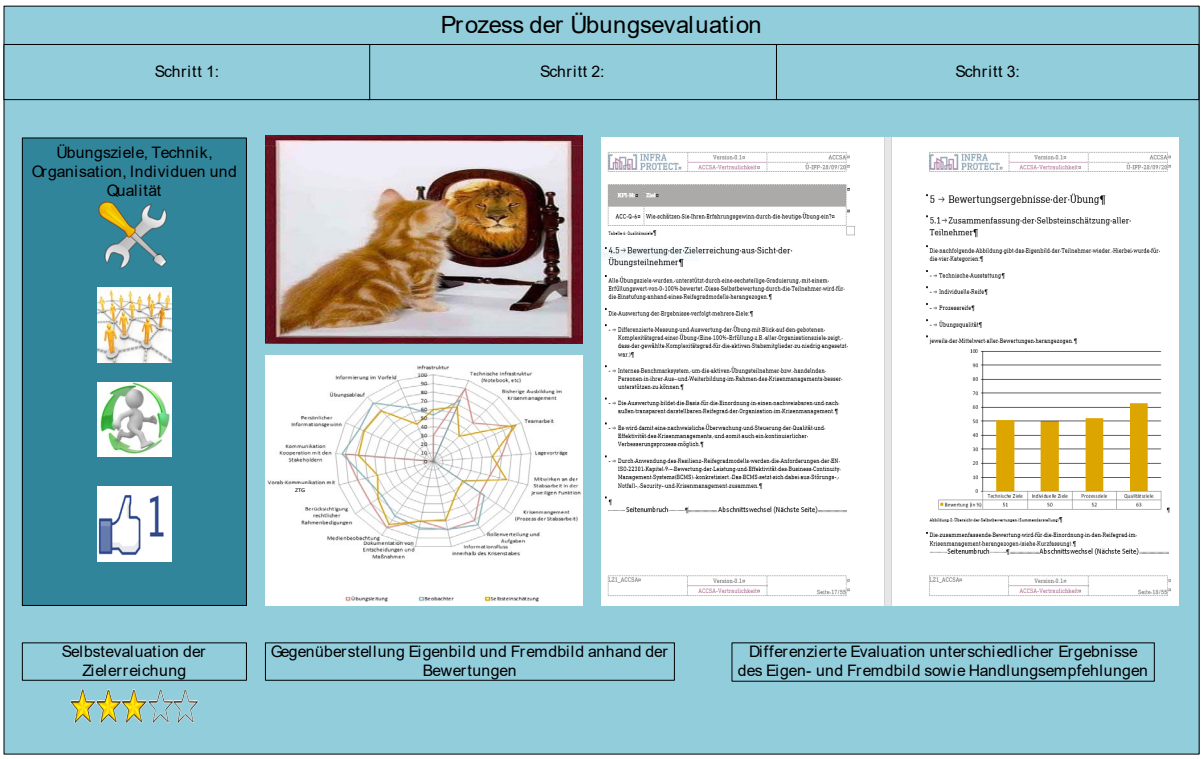


ABBILDUNG 34 ACCSA-GRUNDVORGEHENSWEISE DER ÜBUNGSBEWERTUNG

In diesem Modell fokussieren die individuellen Anforderungen im Wesentlichen auf die Fragen der Aus- und Fortbildung auf „Expert*innenniveau“.

Um eine diversitätsgerechte Aufbereitung von Cybersecurity Übungen zu adressieren, wurden nun in weiterer Folge persönlich-soziale Kerneigenschaften aus 236 Faktoren oder Eigenschaften zusammengestellt und in weiterer Folge analysiert. Ziel dieser Vorgehensweise ist es, wesentliche

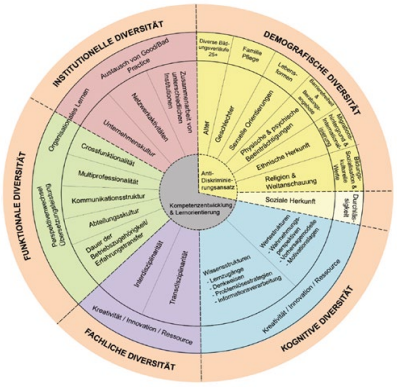
[78] https://projekte.ffg.at/projekt/2742376 (Besuch am 18.11.2024)

Eigenschaften von Individuen für die Bewertung von Übungsergebnissen aber auch für eine diversifizierte Grundlagenvermittlung besser zu verstehen.

Im Wesentlichen sind daher neben den Fachkompetenzen = Wissen / Handlungswissen, die persönlich-sozialen Kerneigenschaften von Individuen zu analysieren.

Hier wurde ein Schritt gewagt, der ergebnisoffen unter den genannten Bedingungen relevante Persönlichkeitsbereiche adressieren helfen soll.

9.4.2.2 Analyse der Persönlichkeitsbereiche



Ausgehend von den 5 Dimensionen wurden 236 „Persönlichkeitsfaktoren“ in einer ersten Iteration zusammengestellt und ausgewertet. Vgl. dazu auch Anhang 12.4.

Daraus wurden 20 Persönlichkeitsbereiche identifiziert und gewichtet. Basis dieser Zusammenstellung sind die im Literaturverzeichnis assemblierten Fragebögen, Modelle und wissenschaftlichen Grundlagen, die zuerst aufgelistet, dann Bereichen zugeordnet wurden.

Der eigentliche Fokus liegt dabei auf signifikanten Persönlichkeitsmerkmalen, die einerseits die bessere Vorbereitung auf nicht alltäglichen Ereignisbewältigungssituationen erlaubt und die andererseits Faktoren aufzeigen soll, die ein optimiertes Zusammenwirken in einer Gruppe unterstützen können.

Die Auswertung der Literatur ergibt im Wesentlichen folgendes bereits gewichtetes Bild von „Persönlichkeitseigenschaften“, die in weiterer Folge als relevant oder als nicht relevant für die Ereignisbewältigung von „Stresssituationen=Cyberattacken“ beachtet werden können oder sollten. Diese gilt es in weiterer Folge entsprechend zu adressieren.

Es sind dies:

- Selbstorientierung
- Sozialorientierung
- Kognitive Fähigkeiten
- Selbstkontrolle
- Dominanz
- Kooperationsfähigkeit
- Flexibilität
- Kommunikationsfähigkeit
- Motiviertheit
- Empathie
- Selbstwirksamkeit
- Gewissenhaftigkeit
- Selbsteinschätzung
- Belastbarkeit
- Offenheit

- Aktivität
- Ethik
- Extraversion
- Kreativität
- Sexualität

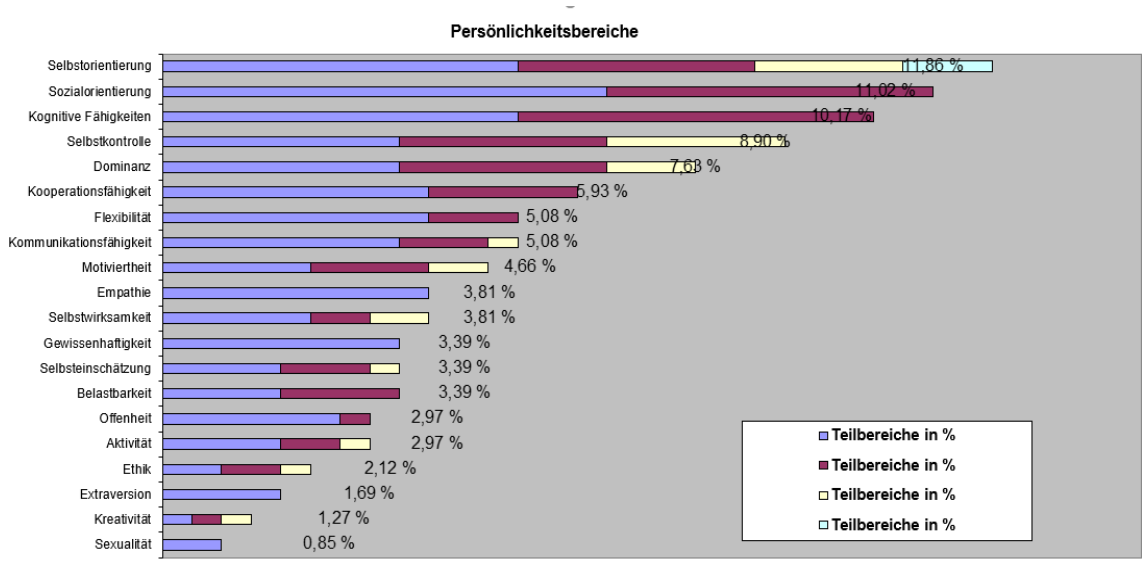


ABBILDUNG 35 HÄUFIGKEITEN AUS DEN 236 FAKTOREN

9.4.2.2.1 Übersicht der Gewichtung der 236 Faktoren

Um die Signifikanz der Faktoren mit Blick auf die individuellen Anforderungen bei der Ereignisbewältigung herauszuarbeiten, wurde die Häufigkeit der genannten Faktoren ausgewertet und gewichtet.

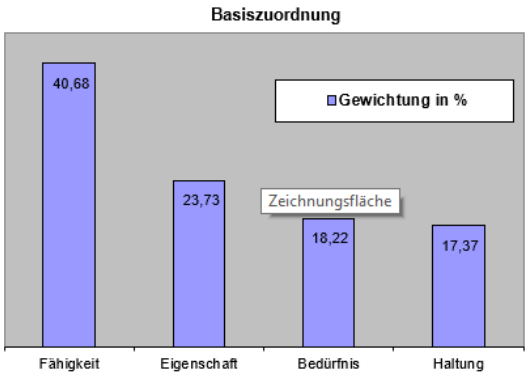
Bereich	Absolut					Gewichtung in %	Teilbereiche in %	Teilbereiche in %	Teilbereiche in %	Teilbereiche in %
Selbstorientierung	28	12	8	5	3	11,86	5,08	3,39	2,12	1,27
Sozialorientierung	26	15	11			11,02	6,36	4,66	0,00	0,00
Kognitive Fähigkeiten	24	12	12			10,17	5,08	5,08	0,00	0,00
Selbstkontrolle	21	8	7	6		8,90	3,39	2,97	2,54	0,00
Dominanz	18	8	7	3		7,63	3,39	2,97	1,27	0,00
Kooperationsfähigkeit	14	9	5			5,93	3,81	2,12	0,00	0,00
Flexibilität	12	9	3			5,08	3,81	1,27	0,00	0,00
Kommunikationsfähigkeit	12	8	3	1		5,08	3,39	1,27	0,42	0,00
Motiviertheit	11	5	4	2		4,66	2,12	1,69	0,85	0,00
Empathie	9	9				3,81	3,81	0,00	0,00	0,00
Selbstwirksamkeit	9	5	2	2		3,81	2,12	0,85	0,85	0,00
Gewissenhaftigkeit	8	8				3,39	3,39	0,00	0,00	0,00
Selbsteinschätzung	8	4	3	1		3,39	1,69	1,27	0,42	0,00
Belastbarkeit	8	4	4			3,39	1,69	1,69	0,00	0,00
Offenheit	7	6	1			2,97	2,54	0,42	0,00	0,00
Aktivität	7	4	2	1		2,97	1,69	0,85	0,42	0,00
Ethik	5	2	2	1		2,12	0,85	0,85	0,42	0,00
Extraversion	4	4				1,69	1,69	0,00	0,00	0,00
Kreativität	3	1	1	1		1,27	0,42	0,42	0,42	0,00
Sexualität	2	2				0,85	0,85	0,00	0,00	0,00

TABELLE 1 GEWICHGUTN DER 236 FAKTOREN

Aus den betrachteten 236 Persönlichkeitsfaktoren wurden in weiterer Folge noch für den Untersuchungszweck vier wesentliche Basiszuordnungen abgeleitet.

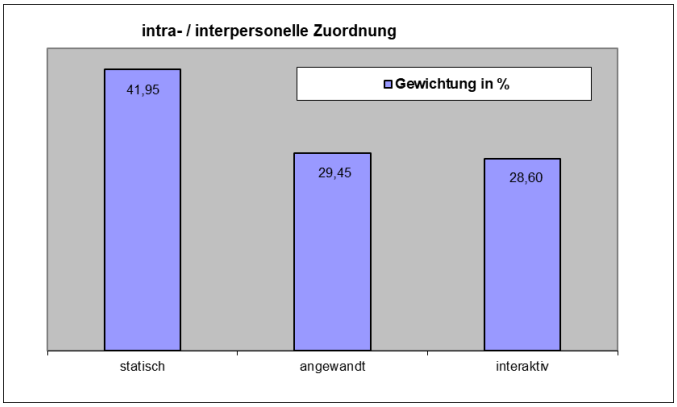
9.4.2.2.2 Primäre Basiszuordnung von Persönlichkeitsfaktoren

Hier wurden mit Blick auf die Aufgabenstellung - vier Basiszuordnungen der Faktoren - aggregiert und in weiterer Folge für die Bewertung von individuellen Faktoren bei Cyberübungen formuliert:



- Fähigkeiten beschreibt u.a. die Fähigkeiten zur Interaktion, Teamfähigkeit, Integrationsfähigkeit, etc.
- Eigenschaften beschreibt u.a. Flexibilität, gewissenhaft, etc.
- Bedürfnis beschreibt u.a. Erfolg zu haben, ein Ereignis zu bewältigen, unabhängig und autonom zu bleiben
- Haltung beschreibt u.a. Besorgtheit, Wertschätzung

Um die Auswertung und in weiterer Folge entsprechende Bewertungskriterien formulieren zu können, wurden für die Kollaboration – ein spezielles Augenmerk der Ereignisbewältigung – drei Sichten auf die Persönlichkeitsbereiche herausgearbeitet:



- Statisch interpretierbare Faktoren z.B. Besorgtheit
- Faktoren die „angewandt“ werden wie z.B. Wachsamkeit aber auch Neugierde
- interaktiv wie z.B. Konfliktbereitschaft, aber auch Offenheit und Kommunikationsbereitschaft

Die hier dargestellten Gewichtungen beziehen sich ausschließlich auf die Häufigkeiten in den erhobenen 236 Persönlichkeitsbereichen und erlauben grundsätzlich keine absolute Wertung der „Wichtigkeit“ bei der Beurteilung der Persönlichkeitsbereiche. Sie dienen aber in weiterer Folge zur Differenzierung der zu erfassenden Kernziele bei der weiteren und differenzierten Auswertung von Übungen.

9.4.2.2.3 Ergebnisdarstellung der genutzten Faktoren

Abbildung 36 zeigt die Häufigkeit der Zuordnung zu den als relevant unterstellten Basisbereichen (blaue Balken) und die weinroten Balken stellen die Häufigkeit dar, wenn man synonym die Faktoren nach „Verhalten“ auswertet.

Aus diesen Ergebnissen wurde ein Fragebogen entwickelt, der in weiterer Folge im Nachgang an Cybersecurity Übungen genutzt werden soll.

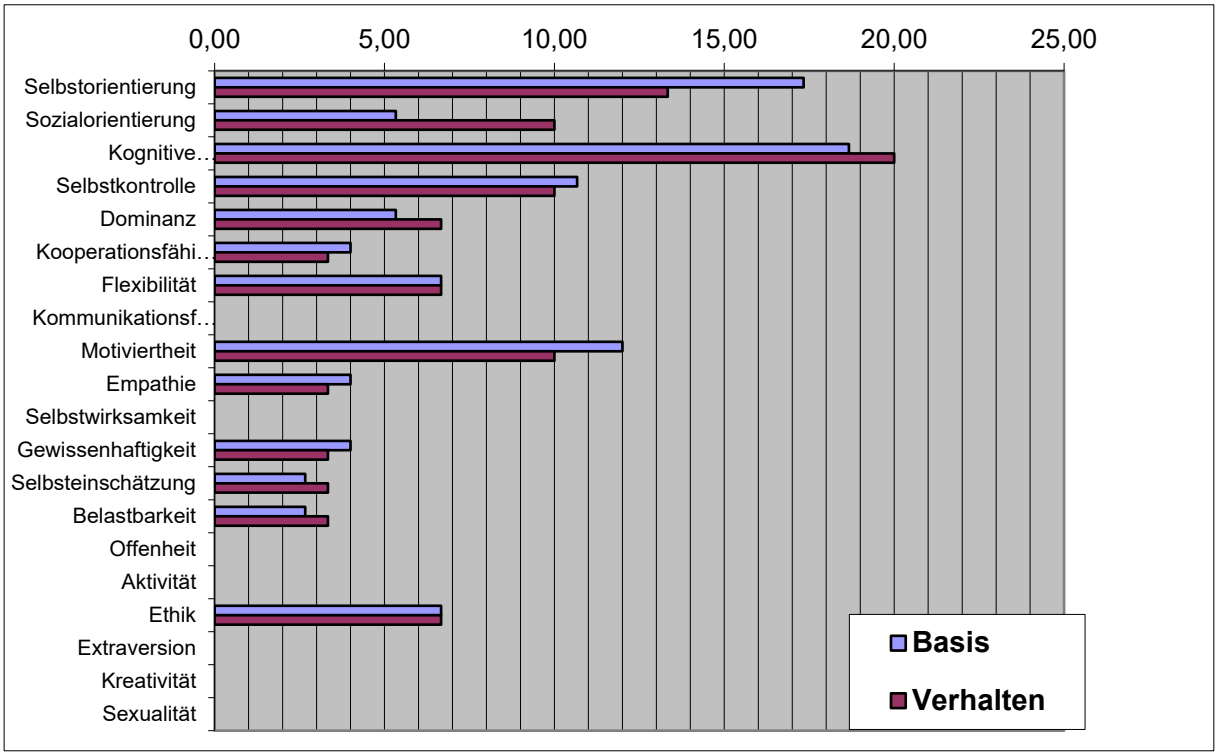


ABBILDUNG 36 ERGEBNISSE DER HÄUFIGKEITEN NACH KERNBEREICHEN

9.4.2.3 Abgeleiteter Fragenkatalog

Basierend auf den beschriebenen Grundlagen und Auswertungen wurden ein Fragenkatalog zusammengestellt. Der Fragenkatalog umfasst im Wesentlichen folgende Punkte:

1. Fragen und Einschätzung der Wichtigkeit von Persönlichkeitsbereichen (statisch / angewandt / interaktiv)
2. Selbsteinschätzung
3. Selbstwirksamkeit
4. Sozialorientierung / Soziale Kompetenz
5. Ethik / Moral und Gewissen
6. Selbstkontrolle & -Orientierung
7. Dominanz / Kontrolle über das Umfeld
8. Kommunikationsorientierung

9.4.2.3.1 Frage 1 zur Wichtigkeit der Persönlichkeitsbereiche

Wählen Sie aus untenstehender Tabelle die 15 wichtigsten Persönlichkeitsaspekte aus und reihen Sie diese nach ihrer Priorität von 1 (am Wichtigsten) bis 15:

Wachsamkeit		Kontrolle		sich im Griff haben	
bei einem Scherz mitlachen		ein Höchstmaß an Arbeit leisten		sich in andere einfühlen können	
eigenes Verhalten reflektieren		nicht ablenken lassen		ethische Werte leben	
anpacken / Initiative zeigen		Akzeptanz		im Team auf Problemlösung konzentrieren	
Problemlösungsfähigkeit		Abläufe koordinieren		Empathie	
flexibel agieren		Gerechtigkeitssinn		gerecht handeln	
Höchstleistung erbringen und einfordern		Perfektion vorleben und einfordern		Wertschätzung	
verschiedene Sichtweisen einnehmen		ruhig bleiben		im sozialen Umfeld moralisch handeln	
Selbsteinschätzung		Einfühlungsvermögen zeigen		Leistungsdrang	
gewissenhaft arbeiten		die Stetigkeit im Team bewahren		sich nicht aus der Fassung bringen lassen	
im Team mehrere Sichtweisen fördern		Führungsanspruch geltend machen		Belastbarkeit	
wachsam sein		Koordinationsfähigkeit		in einer Gruppe auf Fairness achten	
Verzicht		im Team auf das Ziel hinweisen		gesundheitsbewußt agieren	
innerhalb des Teams koordinieren		Gewissenhaftigkeit		Konzentration	
wertschätzend agieren		kontrolliert handeln		flexibel auf andere reagieren	
Flexibilität		Zielorientierung		Kritikfähigkeit	
auch unter Druck anderen noch Last abnehmen		im Team die Hoffnung aufrecht halten		auch mal einen Scherz machen	
Perfektionismus		eigene Aggressionen im Griff haben		Selbstkontrolle	
andere akzeptieren		Entscheidungsfähigkeit		stetig handeln / arbeiten	
Optimismus bewahren		zurückstecken können		deeskalierendes Verhalten	
andere zur Gewissenhaftigkeit anhalten		Humor		Dominanz ausüben	
Entscheidungen treffen können		zugunsten anderer verzichten		die Gesundheit aller berücksichtigen	
Gesundheitsbewusstsein		Engagement		verzichten können	
im Team aktiv mitwirken		Kritik konstruktiv üben und annehmen können		Vielfalt an Perspektiven	
Gelassenheit		nach Perfektion streben		bei der Sache bleiben	

9.4.2.3.2 Frage 2 Selbsteinschätzung

Zu welchem Grad verfüge ich über die in Frage 1 gestellten Persönlichkeitsaspekte für meine Funktion im Notfallmanagement?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Ich verfüge fast ausschließlich über eine Persönlichkeitsausprägung die im Notfallmanagement unbedeutend ist.	Einige wichtige Aspekte der Persönlichkeit sind bei mir teilweise ausgeprägt	Ich verfüge über mehrere wichtige Persönlichkeitsaspekte und einige dieser sind gut ausgeprägt.	Die Mehrzahl der wichtigen Merkmale sind bei mir zumindest mäßig ausgeprägt	Ich verfüge über alle bedeutenden Ausprägungen im Notfallmanagement in mäßiger Ausprägung.	Sämtliche wichtigen Persönlichkeitsaspekte sind bei mir überdurchschnittlich gut ausgeprägt

oder Variante

Markieren Sie Persönlichkeitsmerkmale die bei Ihnen besonders stark ausgeprägt sind mit +, jene Merkmale bei denen Sie persönlichen Entwicklungsbedarf erkennen mit –.

9.4.2.3.3 Frage 3 Selbstwirksamkeit

In welchem Ausmaß kann ich meine persönlichen Ressourcen im Rahmen meiner Tätigkeit im Notfallmanagement nutzen?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Meine Fähigkeiten liegen in Bereichen die in meiner Funktion nicht ausschlaggebend sind.	Die strikte Organisation und Vorgehensweise erlaubt es kaum, meine Stärken einzusetzen.	Ich habe zwar ein gewisses Maß an Handlungsspielraum, bin aber dennoch eingeschränkt	Ich kann mich in meiner Funktion gut einbringen und meine Fähigkeiten großteils nutzen.	Meine Ressourcen decken die Anforderungen ab und ich habe den Freiraum diese zu nutzen.	Ich bin die richtige Person an der richtigen Stelle und kann meine Fähigkeiten voll im Sinne der Aufgabenstellung entfalten.

oder

Wie schätze ich meine persönliche Motivation und Arbeitsmoral innerhalb des Teams nach einer dramatischen Lageänderung ein?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Spontan fühle ich mich überfordert, versuche aber weiterhin mein Bestes zu geben.	Der erste Eindruck entmutigt zwar, aber es muss weiter gearbeitet werden.	Jetzt wird es heftig, aber mit Engagement und Durchhaltevermögen wird die Lage gemeistert	Geht nicht, gibt´s nicht! Es wird nicht leicht aber wir kommen ans Ziel.	Klar ist das jetzt hart, aber am Ende werde ich mich gut fühlen, es geschafft zu haben.	Solche Herausforderungen spornen mich erst richtig an über meine Grenzen hinaus zu wachsen.

9.4.2.3.4 Frage 4 Sozialorientierung / Soziale Kompetenz

Zu welchem Grad ist das Notfallmanagement-Team im Anlassfall bereits eingespielt?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Ich habe die meisten anderen Personen des Teams schon einmal gesehen oder kenne zumindest ihre Namen.	Alle sind einander bekannt, die Arbeit im Team ist aber noch wenig erprobt.	Auf funktionaler Ebene sind die Abläufe eingespielt, Persönliches ist nicht näher bekannt.	Wir haben als Team schon einige Erfahrungen in der Zusammenarbeit gemacht.	Wir kennen gegenseitig die persönlichen Stärken und Schwächen der Einzelnen und kommen damit gut zurecht.	Wir sind ein eingespieltes Team und kennen Stärken und Schwächen. Kleine „Ticks" beeinträchtigen die Arbeit überhaupt nicht.

9.4.2.3.5 Frage 5 Ethik / Moral und Gewissen

Wie bedeutsam sind Lageinformationen für Personen außerhalb des Notfallmanagement-Teams?

a.) an der Bewältigung des Notfalls Beteiligte z.B. in Hilfsfunktionen

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Nötig sind nur konkrete Aufträge. Einblick ins Lagebild schafft nur Verunsicherung.	Es berührt sie nicht großartig etwas zu erfahren, sie machen einfach ihren Job.	Wenn es leicht geht sollten aktuelle Infos an alle gegeben werden, die Mithelfen.	Alle Mitwirkenden sind ausreichend mit Informationen zu versorgen.	Die Leistungsfähigkeit gut informierter Menschen wird, durch die Orientierung die man ihnen gibt, gesteigert.	Es ist absolut wichtig sämtliche Personen die mitwirken immer am laufenden zu halten.

b.) durch den Notfall Betroffene, die aber selbst nichts tun können

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Je weniger Betroffene mitbekommen, umso besser ist es. Sie können ohnehin nichts zur Situation beitragen.	Grobe Infos zeigen dass etwas getan wird. Genaue Angaben sind für Außenstehende nicht verständlich.	Wenige, aber detaillierte Infos sind nötig, Betroffenen eine Lagekenntnis zu geben.	Über die Vorgänge im Rahmen des Notfallmanagements sollten regelmäßig informiert werden.	So viel wie möglich sollte mit Bedacht auf Inhalt und Wirkung der Information weiter gegeben werden.	Es ist nötig betroffenen jede Veränderung transparent darzustellen. Maximale Offenheit beruhigt und schafft Vertrauen.

9.4.2.3.6 Frage 6 Selbstkontrolle &-Orientierung (umgekehrte Wertigkeit)

Wie weitreichend beurteile ich mein Engagement bei der Umsetzung nötiger Maßnahmen?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Ich erfülle exakt die Aufgaben für die ich zuständig bin und keinesfalls mehr.	Ich mache mir Gedanken was ich über meinen Aufgabenbereich hinaus tun könnte.	Es kommt gelegentlich vor, dass ich auch außerhalb meiner Funktion Hand anlege.	Wenn ich gerade nicht voll eingebunden bin, übernehme ich Tätigkeiten außerhalb meiner Zuständigkeit.	Ich erledige notwendige Dinge auch wenn sie nicht in meiner Verantwortung liegen.	Ich agiere mit maximalem Engagement an allen Ecken und Enden wo es nötig ist anzupacken.

9.4.2.3.7 Frage 7 Überwachung & Kontrolle

Wie hoch schätze ich den Leistungsgrad von „Beteiligten“ (nicht Team), wenn keine Überwachung / Kontrolle stattfindet?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Wenn es keine Überwachung gibt wird auch fast nichts getan.	Nur Kontrolle bringt Menschen dazu unter Belastung mehr als ein Minimum zu tun.	Ohne Kontrolle wird schon gearbeitet, aber echte Leistung wird nicht erbracht.	Für engagierte Menschen ist es eine Motivation wenn der Leistungsgrad überprüft wird.	Überwachung und Kontrolle dient nicht primär der Leistungsmotivation ist aber ein Ansporn.	Im Notfallmanagement gibt jeder volle Leistung. Kontrolle ist unnötig.

Oder

Wie hoch schätze ich den Leistungsgrad von „Beteiligten“ (nicht Team), wenn Überwachung / Kontrolle stattfindet, aber nicht dokumentiert wird?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Jeder weiß, das überwacht wird, aber es wird nicht festgehalten.	Kontrolle erhöht die Leistung ein wenig, ohne Dokumentation aber nur geringfügig.	Überwachung ist immer wirksam. Die Wirkung darf aber nicht überbewertet werden.	Das Wissen kontrolliert zu werden, erhöht auf jeden Fall die Leistungen.	Allein durch Kontrolle erhöht sich das Engagement ganz wesentlich.	Durch Überwachung gibt jeder sein Maximum. Egal ob auch Aufzeichnungen gemacht werden.

Oder

Wie hoch schätze ich den Leistungsgrad von „Beteiligten“ (nicht Team), wenn Überwachung / Kontrolle stattfindet und genau dokumentiert wird?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Überwachung und Dokumentation gehören im Notfallmanagement dazu, haben aber kaum Auswirkung auf die Leistung.	Wenn Beobachtungen fest gehalten werden, steigt im geringen Maß auch das Engagement.	Dokumentierte Kontrollergebnisse heben die Leistungskurve merkbar an.	Die Kenntnis über nachvollziehbare Kontrollvorgänge bewirkt hohen Arbeitseinsatz.	Die Dokumentation von Überwachung und Kontrolle führt zu einem sehr hohen Leistungsgrad	Eine strikte Überwachung der Vorgänge mit exakter Dokumentation garantiert maximale Leistung.

9.4.2.3.8 Frage 8 Kommunikationsorientierung

Zu welchem Grad muss Zusammenarbeit und Kommunikation im Notfallmanagement-Team geregelt sein (Häufigkeit und Dauer von Besprechungen, einheitlicher Wortschatz, etc.), um ein optimales Arbeitsergebnis sicher zu stellen?

0%-10%	10%-30%	30%-50%	50%-70%	70%-90%	90%-100%
Auch ohne Regelungen wird bedarfsgerecht kommuniziert.	Gewisse Festlegungen in der Kommunikation führen auch zu besseren Ergebnissen	Kommunikationsvorgaben tragen einen Teil zu einem guten Arbeitsablauf bei.	Klare Regelung führt zu deutlicher Verbesserung der Zielerreichung.	Ein genauer Abgleich der Kommunikation trägt wesentlich zum Erfolg bei.	Exakte Kommunikationsvorgaben sichern bestmögliche Ergebnisse.

9.5 Lessons identified & Lessons learned

Die grundsätzliche Konzeption der IFLs kann in der angedachten Form weiterentwickelt werden, da sich in den Übungen der Bedarf nach hinführenden Unterstützungstools immer wieder bestätigt hat. Das technische Design erlaubt eine einfache Anpassung und Distribution von Inhalten auf mobilen Devices. Dieses Angebot wird hier mehr als dankend angenommen.

Mit Blick auf die verschiedenen Zielgruppen kann man darstellen, dass die Bereitschaft Cyberrisikomanagement bis in die „letzte“ Stufe vorzubereiten grundsätzlich mit zunehmender Unternehmensgröße steigt.

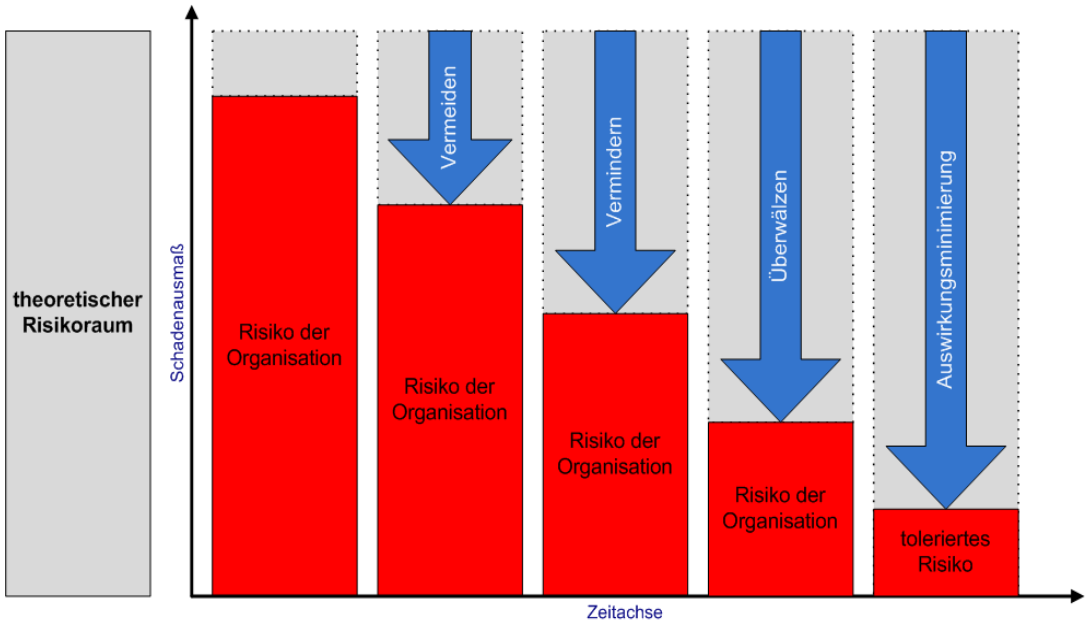


ABBILDUNG 37 ANLEHNUNG AN DIE ONR 49000

Einzelunternehmer*innen haben mehrheitlich erklärt, das Risiko zu überwälzen. Dies gilt auch für kleine Steuerberatungskanzleien (vier bis acht Mitarbeitende) bis hin zu größeren Apotheken. Das Überwälzen besteht im Wesentlich darin, vermeintlich wissende Dienstleister*innen bei Ereignissen hinzuzuziehen. Keine der in AP3 identifizierten Zielgruppen hat den Anspruch erhoben, Cybersicherheitsvorfälle autark, also allein, zu lösen. Man stützt sich hier primär auf das Wissen und Methoden der Softwareherstellenden und Dienstleistenden ab.

Dieser Rückgriff auf externe Expertise erfolgt dabei zumeist ungeprüft und unreflektiert.

Die spezifische Aufbereitung von Inhalten, die auf Cybersicherheitsvorfälle vorbereiten, ist primär ein Thema des Alters der angesprochenen Gruppen. Der Genderaspekt spielt dabei eine untergeordnete Rolle. Zumindest lässt sich aus den Arbeiten in AP4 und AP5 kein signifikanter Unterschied zwischen männlich und weiblich im Umgang mit Ereignisbewältigungsstrategien bei Cybersecurity Themen erkennen. Grundsätzlich sind bei Cybersecurity Übungen weibliche Teilnehmende immer noch um mehr als 50% unterrepräsentiert (vgl. dazu Abbildung 31 Verteilung der Teilnehme). Im AP3 wurden daher ganz gezielt weibliche Nachwuchskräfte angesprochen.

Bei der Entwicklung der IFLs wurden die fünf wesentlichen Ausbildungsgrundsätze der Erwachsenen Aus- und Fortbildung angewandt und implementiert. Die IFLs richten sich daher im Schwerpunkt an Zielgruppen, die mindestens die Schulpflicht bereits absolviert haben. In AP3 und AP4 wurden jüngere Schüler*innen in die Entwicklung integriert. Im Kern werden die IFLs jedoch für die Weiterentwicklung von Cybersecurity-Übungen bei Erwachsenen eingesetzt werden. Um möglichst

alle Sinne der Ausbildungsteilnehmenden zu adressieren, ist eine entsprechende Gestaltung der Aus- und Fortbildung erforderlich. Dies soll und wird durch die technische Flexibilität bei den Unterstützungswerkzeugen erreicht, welche die Nutzung von unterschiedlichen Medien erlaubt und unterstützt.

Der **Grundsatz der Anschaulichkeit** wird durch die Videos und durch die Nutzung der mobilen App bei Übungen unterstützt. Das bloße Reden über Dinge oder Vorgänge führt noch nicht zu klaren und unmissverständlichen Vorstellungen und Eindrücken. Seit jeher gilt folglich der Grundsatz, dass „Sache, Wort, Wirklichkeit und Begrifflichkeiten“ (Nuissl, 2017), (Türk et al., 2022) zusammenwirken müssen.

Dieser **Grundsatz der Mitarbeit** ist eines der wichtigsten Prinzipien und wird in den IFLs und durch die Cyber Range Zielgruppen spezifisch umgesetzt.

Der **Grundsatz der Zeitgemäßheit** wird durch die Nutzung aktueller und zeitgemäßer Medien aber auch inhaltlich durch die Aktualität der Themenstellungen (vgl. dazu AP4 - Inhalte der Cyberübungen) sichergestellt.

Der **Grundsatz der Wirklichkeitsnähe** wird mit allen zur Verfügung stehenden Mitteln hergestellt. Aktuelle Attacken in der Cyber Range können so nachgestellt werden. Die IFL-Tools sollen bei realen Vorfällen eine Guidance erlauben. In den Übungssettings wurde immer darauf geachtet, dass die realen Gegebenheiten bei den Organisationen abgebildet werden. Mit Blick auf den Diversitätsanspruch wurden die Inhalte und Aufgabenkomplexitäten immer an die realen Aufgaben der Personen in ihren wirklichen Rollen angepasst und interaktiv erklärt und implementiert.

Der **Grundsatz der Vergessenssicherung** wird in den IFLs insbesondere durch die iterative und individualisierbare Zusammenstellung von „Unterstützungsunterlagen und Werkzeugen“ entsprechend umgesetzt. Dies wird zielgruppenspezifisch „neu“ und basierend auf dem Wissensspeicher weiterentwickelt.

Mit den IFLs wurden didaktisch methodische Aufbereitungen von diversitätsspezifischen Themenbereichen in Grobziele und Detailziele heruntergebrochen und mit verschiedenen Medien an die Zielgruppen herangetragen.

Dabei wurden entsprechend den Zielgruppen berücksichtigt:

- die Förderung der Eigenaktivität: Die Teilnehmenden mussten zum Teil selbständig, zum Teil unter Anleitung Probleme selbst entdecken und lösen.
- die Erfahrungsbezogenheit: Jede*r Teilnehmende hat aus dem eigenen Erfahrungshorizont die Möglichkeit sich die Unterstützungswerkzeuge selbst anzupassen und kann damit an die eigenen Erkenntnisse anknüpfen
- die didaktischen Methoden der Übungen sind den Teilnehmenden angepasst, um bedarfsorientierte Diversitätsdimensionen vorzubereiten, durchzuführen und auszuwerten

10 Fazit und Ausblick

Im INDUCE-Projekt konnte herausgearbeitet werden, dass Cybersicherheit in einer digitalisierten Gesellschaft nicht nur eine technologische Herausforderung ist, sondern auch stark von Diversitätsaspekten beeinflusst wird. Durch die Entwicklung und Implementierung diversitätssensibler Cyberübungen wurde ein wichtiger Schritt zur Förderung von Cybersicherheitskompetenzen in verschiedenen Zielgruppen unternommen. Insbesondere die Einbeziehung von unterrepräsentierten Gruppen wie Frauen, älteren Menschen und technikfernen Personen stellt sicher, dass Cybersicherheit für alle Bevölkerungsgruppen zugänglich und relevant ist.

Ein wesentlicher Erfolg des Projekts war der Aufbau eines Innovationsnetzwerks, das den Wissenstransfer zwischen Wirtschaft, Behörden und Forschung förderte. Dieses Netzwerk bildete die Grundlage für die nachhaltige Verbreitung und Weiterentwicklung der im Projekt erarbeiteten Konzepte und Methoden.

Die durchgeführten Future Labs und die praxisorientierte Erprobung der Cyberübungen haben gezeigt, dass es möglich ist, die Sicherheitskompetenzen diverser Zielgruppen zu stärken und so einen Beitrag zur Erhöhung der Cybersicherheit in Österreich zu leisten. Die Ergebnisse des Projekts legen den Grundstein für zukünftige Initiativen, die darauf abzielen, die digitale Resilienz der Gesellschaft weiter zu verbessern.

Mit der erfolgreichen Umsetzung der Projektziele hat INDUCE einen bedeutenden Beitrag zur Cybersicherheit und Chancengerechtigkeit im digitalen Raum geleistet. Die gewonnenen Erkenntnisse und entwickelten Tools bieten eine wertvolle Ressource für die Fortführung und Erweiterung von Cybersicherheitsinitiativen in der Zukunft.

Jedoch muss man auch zugeben, dass es in so einem Projekt nie möglich ist, alle Aspekte des Themas umfassend zu betrachten. Es ist evident, dass es viele unterschiedlichen Initiativen gibt, die auf unterschiedliche Gruppen abzielen und unterschiedliche Lerninhalte enthalten. Das Projekt gab einen kurzen Abriss darüber, jedoch ist die Arbeit damit noch nicht beendet. Es braucht mehr koordinierte und für spezielle Gruppen abgestimmte Initiativen, die dieses Thema tiefergreifend beleuchten und bearbeiten.

11 Literaturverzeichnis

AIT Austrian Insititute of Technology. (2020). Cybersecurity Literacy And Dexterity through Cyber Exercises. Projektbeschreibung für Förderungsansuchen des Programms Laura Bassi 4.0. 2. Ausschreibung. Wien: 2020. Abgerufen am 11.01.2022, von https://www.ffg.at/laura-bassi-4.0-2-ausschreibung.

Akpan, B. und Kennedy, T. J. Hrsg., Science education in theory and practice: an introductory guide to learning theory. in Springer texts in education. Cham, Switzerland: Springer, 2020.

Anderson, R. und Moore, T. „The Economics of Information Security“, Science, Bd. 314, Nr. 5799, S. 610–613, Okt. 2006, doi: 10.1126/science.1130992.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Bamberg, E & Keller, M., Wohlert, C. & Zeh, A. Das arbeitspsychologische Stressmodell, FÜR EIN GESUNDES BERUFSLEBEN. "BGW-Stresskonzept."

Bath, C. (2009). De-Gendering informatischer Artefakte: Grundlagen einer kritisch-feministischen Technikgestaltung. Dissertation zur Erlangung des Grades einer Doktorin der Ingenieurwissenschaften. Bremen.

Berg, A. (2020). Senioren in der digitalen Welt. BitKom. Abgerufen am 28.02.2022, von https://www.bitkom.org/sites/default/files/2020-08/bitkom-prasentation-senioren-in-der-digitalen-welt-18-08-2020.pdf.

Birk, M.V., Atkins, Ch., Bowey, J.T. & Mandryk, R.L. (2016). Fostering intrinsic motivation through Avatar identification in digital games. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems 2016, pp. 2982-2995. DOI: 10.1145/2858036.2858062.

Birkenbihl, M. (2014). Train the trainer: Arbeitshandbuch für Ausbilder und Dozenten. mi Wirtschaftsbuch.

Braun, V. & Clarke, V. (2013). Successful Qualitative Research. A practical guide for beginners. London.

Braun, V. & Clarke, V. (2006): Using thematic analysis in psychology. In: Qualitative Research in Psychology 3(2), pp.77-101. 2006. DOI: 10.1191/1478088706qp063oa.

Bundeskriminalamt. (2020). Cybercrime Bundeslagebild 2019. Wiesbaden. Abgerufen am 28.02.2022, von https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html.

Bundeskriminalamt. (2021). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland. Jahrbuch 2019. Band 2: Opfer. 67. Ausgabe V2.0. Wiesbaden. Abgerufen am 07.03.2022, von https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2019/PKSJahrbuch/pksJahrbuch_node.html.

Bundesministerium für Inneres. (2019). Kriminalitätsbericht. Statistik und Analyse 2019. Abgerufen am 07.03.2022, von https://www.bmi.gv.at/508/files/SIB_2019/3_SIB_2019_Kriminalitaetsbericht_2019_Statistik_und_Analyse.pdf.

Bundesministerium für Inneres. (2020). Cybercrime Report 2019. Wien. Abgerufen am 07.03.2022, von https://bundeskriminalamt.at/306/files/Cybercrime_2019.pdf.

Bundesministerium für Digitalisierung und Wirtschaftsstandort: Digitales Kompetenzmodell für Österreich. DigComp 2.2 AT. Wien, Juli 2021. Online abrufbar unter https://arbeiterkammer.at/ueberuns/zukunftsprogramm/zukunftsfonds/wien/DigComp_2.2_AT.pdf [zuletzt aufgerufen am 18.06.2024].

Burmeister, M., & Burmeister, M. (2019). Phasen der Teamentwicklung. Navigationssystem Werteorientierung in der Mitarbeiterführung: Subjektivierung der Werte, 43-44.

Bruce, A. (2007). Kritikkompetenz im Management. Der Einfluss der Kritikkompetenz auf den beruflichen Erfolg von Führungskräften. Wiesbaden: Edition KWV Springer Gabler.

BSI. (2008). BSI-Standard 100-4: Notfallmanagement Version 1.0. Abgerufen am 23.03.2022 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1

Chouliaras, N. & Kittes, G. & Kantzavelou, I. & Maglaras, L. & Pantziou, G. und Ferrag, M. A. „Cyber Ranges and TestBeds for Education, Training, and Research“, Appl. Sci., Bd. 11, Nr. 4, S. 1809, Feb. 2021, doi: 10.3390/app11041809.

Chouliaras, N. & Kittes, G. & Kantzavelou, I. & Maglaras, L. & Pantziou, G. und Ferrag, M. A. „Cyber Ranges and TestBeds for Education, Training, and Research“, Appl. Sci., Bd. 11, Nr. 4, S. 1809, Feb. 2021, doi: 10.3390/app11041809.

Clark, D, Tanner-Smith, E. & Killingsworth, S. (2016). Digital Games, design, and learning: A systematic review and meta-analysis. Review of Educational Research 86 (1), pp. 79-122. DOI: 10.3102/0034654315582065.

Coenraad, M., Pellicone, A., Ketelhut, D.J., Cukier, M., Plane, J. & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation & Gaming, 51 (5). pp.586-611. DOI: 10.1177/1046878120933312.

Cohn, R. C., & Stumm, G. (2000). Themenzentrierte Interaktion (TZI). Wörterbuch der Psychotherapie, 700-701.

Corneliussen, H.G. (2020). What brings women to cybersecurity? A qualitative study of women´s pathways to cybersecurity in Norway. Proceedings of the European Interdisciplinary Cybersecurity Conference 9, pp. 1-2. DOI: 10.1145/3424954.3424965.

Csikszentmihalyi, M. (Ed.). (1995). Die außergewöhnliche Erfahrung im Alltag: Die Psychologie des flow-Erlebnisses. Klett-Cotta.

CSAW. (2022). Abgerufen am 31.03.2022 von https://www.csaw.io/ctf

Diakoumakos, I. „Enhancing Cybersecurity Education and Training through Gamification“, in Proceedings of the 2nd International Conference of the ACM Greek SIGCHI Chapter, Athens Greece: ACM, Sep. 2023, S. 1–5. doi: 10.1145/3609987.3610016.

De Pater, I. E., Van Vianen, A. E. M., Fischer, A. H., & Van Ginkel, W. P. (2009). Challenging experiences: Gender differences in task choice. Journal of Managerial Psychology, 24(1), 4-28. doi:10.1108/02683940910922519.

Deckard, G. M., & Camp, L. J. (2016). Measuring efficacy of a classroom training week for a cybersecurity training exercise. 2016 IEEE Symposium on Technologies for Homeland Security (HST), 1–6. https://doi.org/10.1109/THS.2016.7568940

Duggan, M. (2015). Gaming and Gamers. Pew Research Center. Abgerufen am 10.01.2022, von https://pewresearch.org/internet/2015/12/15/gaming-and-gamers/.

E-ISAC. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Abgerufen am 23.03.2022 von https://africautc.org/wp-content/uploads/2018/05/E-ISAC_SANS_Ukraine_DUC_5.pdf

European Commission. (2013). Women active in the ICT Sector. Luxembourg: Publications Office of the European Union. DOI: 10.2759/27822.

Europol. (2021). IOCTA Internet Organised Crime Threat Assessment 2021. Abgerufen am 23.03.2022 von https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Europäische Union. (2016). Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Abgerufen am 23.03.2022 von https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148

European Union Agency for Cybersecurity ENISA. (2018). Cyber Europe 2018: After action report : findings from a cyber crisis exercise in Europe. Publications Office. https://data.europa.eu/doi/10.2824/369640

European Union Agency for Cybersecurity ENISA. (2022). Cyber Europe 2018: After action report : Findings fm a PAN_EUROPEN cyber crisis Exercise. Publications Office. https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report/@@download/fullReport

European Union Agency for Cybersecurity ENISA (2021). T. De Zan & M M. Yamin: Towards a common ECSC Roadmap. Success factors for the implementation of national Cybersecurity competitions. DOI: 10.2824/657311.

European Union Agency for Cybersecurity ENISA. (2009). Good Practice Guide on National Exercises – Enhancing the Resilience of Public Communications Networks. Abgerufen am 23.03.2022 von https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

Erharter, D. (2013). G-U-T. Gender & Diversity, Usability und Testing als Qualitätssicherung von Apps und Websites. Teil A Guideline.

Erharter, D. (2013). G-U-T. Gender & Diversity, Usability und Testing als Qualitätssicherung von Apps und Websites. Teil B Reflexion.

Erharter, D. (2013). G-U-T. Gender & Diversity, Usability und Testing als Qualitätssicherung von Apps und Websites. Teil C1 Heuristik Apps & Tablets.

Erharter, D. (2013). G-U-T. Gender & Diversity, Usability und Testing als Qualitätssicherung von Apps und Websites. Teil C2 Heuristik Websites.

Erharter, D. (2014). Gender- und Diversity-Faktoren in interaktiven Medien. In: Seidl, Markus; Schmiedl, Grischa (Hrsg.): Forum Medientechnik-Next Generation, New Ideas. Glückstadt: Hülsbusch 2014, S. 43-55.

Erharter, D. (2015). Gendergerechtes Forschungsdesign an der Schnittstelle Mensch-Technik. In: Diefenbach, S, Henze, N. & Pielot, M. (Hrsg.), Mensch und Computer 2015 Tagungsband, Stuttgart: Oldenbourg Wissenschaftsverlag, S. 63-72.

Flick, U. (2009). Sozialforschung: Methoden und Anwendungen. Ein Überblick für die BA-Studiengänge. Reinbek bei Hamburg: Rowohlt-Taschenbuch-Verlag.

Furnell, S. und Clarke, N. L. Hrsg., Human aspects of information security and assurance: 17th IFIP WG 11.12 international symposium, HAISA 2023, Kent, UK, July 4-6, 2023: proceedings. in IFIP advances in information and communication technology, no. 674. Cham: Springer, 2023.

Gaisch, M. & Aichinger, R. (2016). Das Diversity Wheel der FH OÖ: Wie die Umsetzung einer ganzheitlichen Diversitätskultur an der Fachhochschule gelingen kann. FFH 2016.

Gaisch, M., Preymann, S. & Aichinger, R. (2019). Diversity management at the tertiary level: an attempt to extend existing paradigms. Journal of Applied Research in Higher Education 12 (12). DOI: 10.1108/JARHE-03-2018-0048.

Gaisch, M., & Kerschbaumer, B. (2019). Frauen in der digitalen Zukunft: Stereotype durchbrechen: Ergebnisse einer Umfrage unter österreichischen Schülerinnen zum Thema Frauen und Informatik 2019

Gaisch, M. & Rammer, V. (2018). Mehr Frauen in die Informatik. Einschätzung von österreichischen Schülerinnen zu Barrieren und Aktivierungsmaßnahmen von Informatik-Studiengängen. Abgerufen am 02.03.2022, von https://www.fh-ooe.at/fileadmin/user_upload/fhooe/landing-pages/durchstarterinnen/fhooe-Poster_Frauen_in_die_IT_Studienergebnisse.pdf.

Goleman, D., & Griese, F. (1996). Emotionale Intelligenz (p. 204ff). München: Hanser.

Gottschall, Karel (2010): Kompetenzen – Überblick und Auseinandersetzung mit einem Kompetenzatlas.

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities (NIST SP 800-84; 0 Aufl., S. NIST SP 800-84). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-84

Gruber, M. (2011). Teams in der Sozialen Arbeit mit Fokus auf Teamkonflikte.

Hamari, J. & Koivisto, J. und H. Sarsa, „Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification“, in 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI: IEEE, Jan. 2014, S. 3025–3034. doi: 10.1109/HICSS.2014.377.

Hissnauer, W. Arbeiten im Team.

Jahankhani, H. & Meda, L. N. K. und Samadi, M. „Cybersecurity Challenges in Small and Medium Enterprise (SMEs)“, in Blockchain and Other Emerging Technologies for Digital Business Strategies, H. Jahankhani, D. V. Kilpin, und S. Kendzierskyj, Hrsg., in Advanced Sciences and Technologies for Security Applications. , Cham: Springer International Publishing, 2022, S. 1–19. doi: 10.1007/978-3-030-98225-6_1.

Kang, S. M., Day, J. D., & Meara, N. M. (2006). Soziale und emotionale Intelligenz: Gemeinsamkeiten und Unterschiede. na.

Ketelhut, D.J. (2007). The Impact of Student Self-efficacy on Scientific Inquiry Skills: An Exploratory Investigation in River City, a Multi-user Virtual Environment. Journal of Science Education and Technologies, Vol. 16 (1). Pp 99-111. DOI: 10.1007/s10956-006-9038-y.

Kluge, A. (2004). Resilienzforschung. Aktueller Forschungsstand. Kommentierte Auswahlbibliographie, EU-Projekt: Arbeitsfähigkeit erhalten (AEIOU). Marburg, 1-35.

Kriz, W. (2009). Planspiel. In S. Kühl, P. Strodtholz, & A. Taffertshofer (Hrsg.), Handbuch Methoden der Organisationsforschung: Quantitative und Qualitative Methoden (S. 558–578). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91570-8_27

Laura Bassi 4.0. (2020). Programmdokument gemäß Punkt 4.1 der Richtlinien für die Österreichische Förderungsgesesllschaft mbH zur Förderung der angewandten Forschung, Entwicklung und Innovation, FFG-RL Offensiv. Version 2.0. Nationalstiftung für Forschung, Technologie und Entwicklung Österreich Fonds. Wien: Bundesministerium Digitalisierung und Wirtschaftsstandort.

Leicht-Scholten, C. & Schroeder, U. (2014). Informatikkultur neu denken – Konzepte für Studium und Lehre. Integration von Gender und Diversity in MINT-Studiengängen. Aachen: Springer Vieweg.

Martin, A., & Purwin, J. (2001). Soziale Fähigkeiten in Arbeitsgruppen: eine empirische Studie zur Ermittlung der Kooperationsfähigkeit.

Maslow, A. & Freud, S & Schirm, R. und Birkenbihl, M. Der Mensch und sein Selbstwertgefühl

Mayerhofer, W. (2009). Das Fokusgruppeninterview. In Buber, R. & Holzmüller, H.H. (Hrsg.) Qualitative Marktforschung. Gabler. Pp. 477-490. DOI: 10.1007/978-3-8349-9441-7_30.

Mayring, P. (1991). Qualitative Inhaltsanalyse. In U. Flick, E v. Kardoff, H. Keupp, L.v. Rosenstiel & S. Wolff (Hrsg.), Handbuch qualitative Forschung: Grundlagen, Konzepte, Methoden und Anwendungen. (2019) München: Beltz. S. 209-213. Abgerufen am 28.02.2022, von https://nbn-resolving.org/urn:nbn:de:0168-ssoar-37278.

Meredith, L. S., Sherbourne, C. D., Gaillot, S. J., Hansell, L., Ritschard, H. V., Parker, A. M., & Wrenn, G. (2011). Promoting psychological resilience in the US military. Rand health quarterly, 1(2).

Müller, M. and Schmid, A. (2009). motionale Kompetenz als Prädiktor für effektive Stressverarbeitung.

NATO CCDCOE. (2022a). Abgerufen am 23.03.2022 von https://ccdcoe.org/exercises/

NATO CCDCOE. (2022b). Abgerufen am 23.03.2022 von https://ccdcoe.org/exercises/locked-shields/

NATO ACT. (2022). Abgerufen am 23.03.2022 von https://www.act.nato.int/cyber-coalition

Nuissl, E. (2017). Ordnungsgrundsätze der Erwachsenenbildung in Deutschland. In: Tippelt, R., von Hippel, A. (eds) Handbuch Erwachsenenbildung/Weiterbildung. Springer Reference Sozialwissenschaften. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-531-20001-9_25-1

Oliver, J.Y. & Elwell, C. (2018). Effective Competitions for Broadening Participation in Cybersecurity. ASEE Zone IV Conference: Boulder, Colorado. https://peer.asee.org/29608 (zuletzt aufgerufen am 05.06.2023).

Peltier, T. R. Information security fundamentals, 2. ed. in An Auerbach book. Boca Raton,Fla: CRC Press, 2014.

Pusey, P., Gondree, M. & Peterson, Z. (2016): The outcomes of Cybersecurity Competitions and Implications for underrepresented populations. IEEE Security & Privacy November/December 2016, 90-95.

Rehm, M. (1964). Das Planspiel als Bildungsmittel: In Verwaltung und Wirtschaft, in Politik und Wehrwesen, in Erziehung und Unterricht. Heidelberg: Quelle & Meyer

Reidl, S., Streicher, J, Hock, M., Hausner, B., Waibel, G. & Gürtl, F. (2020). Digitale Ungleichheit. Wie sie entsteht, was sie bewirkt … und was dagegen hilft. Wien: FFG.

Rheinberg, F., Vollmeyer, R., & Engeser, S. (2003). Die erfassung des flow-erlebens.

Schlüsselkompetenzen im Kompetenzmodell Kantonale Verwaltung Bern (KOM-BE), https://www.pa.fin.be.ch/de/start/themen/werte-und-strategie/kompetenzmodell-kanton-bern.html (letzter Besuch am 27.11.2024)

Scharnhorst, Julia (2010): Resilienzforschung in Theorie und Praxis. Individuelle Widerstandskraft – eine notwendige Kernkompetenz? In: Personalführung1/2010, S.3451. DGFP.

Schmorrow, D.D.& Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2021. Lecture Notes in Computer Science (), vol 12776. Springer, Cham. https://doi.org/10.1007/978-3-030-78114-9_32.

Schmorrow, D.D. & Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2022. Lecture Notes in Computer Science (). Vol 13310. Springer, Cham. https://doi.org/10.1007/978-3-031-05457-0_24.

Schulze, R. (2006). Theorie, Messung und Anwendungsfelder emotionaler Intelligenz: Rahmenkonzepte. na.

Schwind, S. (2010). Teamfähigkeit.

Shumba, R., Taylor, C., Acholonu, G., Ferguson-Boucher, K., Franklin, G., Bace, R., Sweedyk, E., Turner, C., Sande, C., Hall, L. (2013). Cybersecurity, Women and Minorities: Findings and Recommendations from a Preliminary Investigation. Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education – working group reports, pp. 1-14. DOI: /10.1145/2543882.2543883.

Seelheim, T., & Witte, E. H. (2007). Teamfähigkeit und Performance. Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO), 38, 73-95.

Seifert, A., & Schelling, H. R. (2015). Digitale Senioren. Nutzung von Informations-und Kommunikationstechnologien (IKT) durch Menschen ab 65 Jahren in der Schweiz im Jahr 2015. University of Zurich. Abgerufen am 28.02.2022, von https://www.zora.uzh.ch/id/eprint/116078/1/Studie-Digitale-Senioren-2015.pdf.

Seker, E., & Ozbenli, H. H. (2018). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity), 1–9. https://doi.org/10.1109/CyberSecPODS.2018.8560673

Seyda, S., & Flake, R. (2019). Chancengleichheit und Digitalisierung: Frauen und Männer in der digitalen Arbeitswelt. KOFA-Studie No.4/2019. Abgerufen am 28.02.2022, von https://www.econstor.eu/handle/10419/207756.

Tietje, F. Einführung in die Themenzentrierte Interaktion (TZI).

Trimmel, J. M. (2009) Einführung in die gruppen- und sozialraumbezogenen Methoden der Sozialen Arbeit.

Tobey, D.H., Pusey, P. & Burley, D.L. (2014). Engaging Learners in Cybersecurity careers: lessons from the launch of the National Cyber League. Acm Inroads, Vol 5 (1), pp. 53-56. DOI: 10.1145/2568195.2568213.

TRAFICOM. (2020). Instructions for organising cyber exercises – A manual for cyber exercise organisers. Abgerufen am 23.03.2022 von https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf

Türk, E., Erharter, D., Berger, D., & Strigl, A. (2022). Das VREDE-Phasenmodell für Gruppenentscheidungen. Die Komplexität von Gruppenentscheidungen anerken-nen und meistern. Konfliktdynamik, 11(2), 126-135.

Vancouver, J. B., & Ilgen, D. R. (1989). Effects of interpersonal orientation and the sex-type of the task on choosing to work alone or in groups. Journal of Applied Psychology, 74(6), 927-934. https://psycnet.apa.org/doi/10.1037/0021-9010.74.6.927, zuletzt aufgerufen am 23.05.2023.

Wilhelmson, N., & Svensson, T. (2011). Handbook for planning, running and evaluating information technology and Cybersecurity exercises. Försvarshögskolan (FHS). http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-8132

Wolter, B. (2005). „Resilienzforschung "–das Geheimnis der inneren Stärke... Systhema, 3(2005), 19.

Yamin, M.M., Katt, B. & Torseth, E. (2021). Selecting and Training young Cyber Talent: A European Cybersecurity Challenge Case Study. In: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2021. Lecture Notes in Computer Science (), vol 12776. Springer, Cham. https://doi.org/10.1007/978-3-030-78114-9_32.

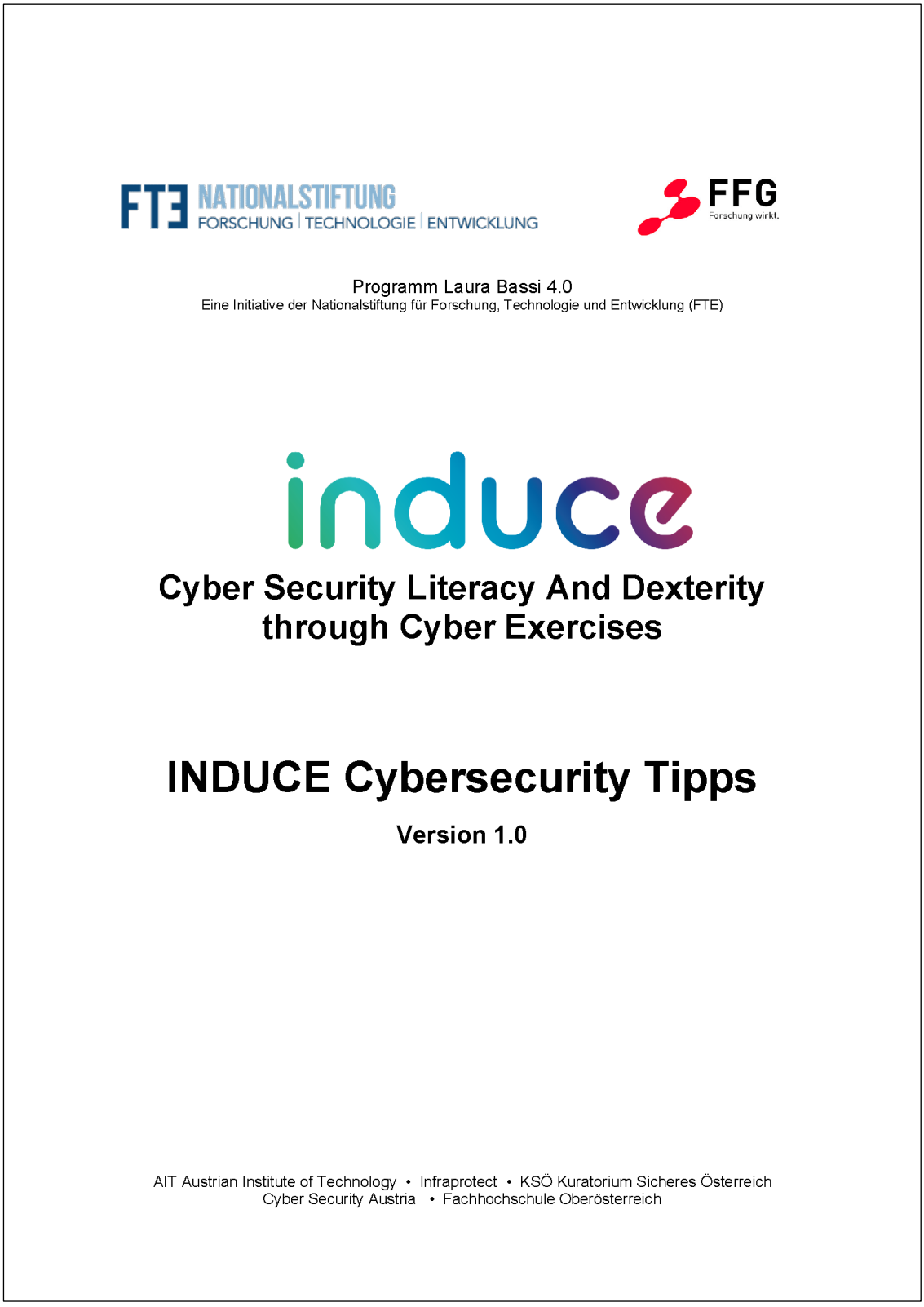
Yamin, M.M., Erdodi, L., Torseth, E. & Katt, B. (2022): Selecting and Training Young Cyber Talent: A Recurrent European Cybersecurity Challenge Case Study: in: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2022. Lecture Notes in Computer Science (). Vol 13310. Springer, Cham. https://doi.org/10.1007/978-3-031-05457-0_24.

Yampolskiy, M., Gatlin, J., & Yung, M. (2021). Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, 3–9. https://doi.org/10.1145/3462223.3485618

Zehrer, A., & Mössenlechner, C. (2010). Leadership-Kompetenzen in Krisensituationen. Change Leadership: Den Wandel antizipieren und aktiv gestalten, 181-209.

12 Anhang

12.1 Cybersecurity Tipps Sammlung



FTE NATIONALSTIFTUNG
FORSCHUNG | TECHNOLOGIE | ENTWICKLUNG

FFG
Forschung wirkt.

Programm Laura Bassi 4.0
Eine Initiative der Nationalstiftung für Forschung, Technologie und Entwicklung (FTE)

induce

Cyber Security Literacy And Dexterity through Cyber Exercises

INDUCE Cybersecurity Tipps

Version 1.0

AIT Austrian Institute of Technology • Infraprotect • KSÖ Kuratorium Sicheres Österreich
Cyber Security Austria • Fachhochschule Oberösterreich

1 Cybersecurity-Tipp 1

Gefälschte E-Mails – Phishing

Wenn Sie eine E-Mail erhalten, in der Sie vor einer Kontosperrung gewarnt werden oder in der behauptet wird, dass Sie einen Preis gewonnen haben, oder aufgefordert werden, dringend Ihre Identität zu bestätigen

klicken Sie auf KEINEN Link aus dieser E-Mail und laden Sie KEINE Datei herunter!

Das ist ein **PHISHING**-Betrug.

Die Betrüger wollen Sie dazu bringen, **persönliche Daten** preiszugeben oder unwissentlich **bösartige Programme** (**MALWARE**) herunterzuladen.

Löschen Sie diese E-Mail.

Haben Sie Zeit und Lust für passende Cyber-Übungen?

Sich vor Betrug schützen (ovosplay.com)1 - Wenn Sie die Übungen am Computer machen, wählen Sie „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im grünen Teil „Sich vor Betrug schützen“

Weitere **hilfreiche Infos** wie auch **aktuelle Phishing-Fallen** finden Sie hier:

- Aktuelle Betrugswarnungen - WKO.at[2]
- Phishing, Smishing & Vishing: So schützen Sie sich vor Datendiebstahl! - Watchlist Internet (watchlist-internet.at)[3]
- Was ist „Phishing“ und was kann ich dagegen tun? - saferinternet.at[4]
- Phishing (oesterreich.gv.at)[5]

2 Cybersecurity-Tipp 2

Vorsicht bei drahtlosem Internet

Meistens steigen wir ins Internet **ohne Kabel** ein, also **drahtlos**. Dafür gibt es folgende Funktionen:

- **WLAN** - lokales Netzwerk für Laptops, Mobiltelefone usw.,
- **Bluetooth** - Datenübertragung zwischen Geräten über **kurze Distanz** (einige Meter),
- **NFC** = Nahfeldkommunikation - Datenübertragung zwischen Geräten über eine **sehr kurze Distanz** (10-20 Zentimeter), z. B. beim kontaktlosen Bezahlen.

Mit WLAN-Netzwerken haben wir zuhause oder in Unternehmen zu tun. Bei richtigen Einstellungen bieten sie eine gewisse Sicherheit. Vorsicht aber bei öffentlichen gratis **HOTSPOTS**, d. h. **den offenen Internet-Zugriffspunkten** im Zug, am Flughafen oder im Hotel! Diese sind nicht geschützt. Zudem gibt es auch **Fake-WLANs**, d. h., ein Netzwerk heißt z. B. ÖBB oder wie Ihr

[1] https://phishingquiz.withgoogle.com/
[2] https://www.wko.at/warnungen/aktuelle-betrugsversuche
[3] https://www.watchlist-internet.at/news/phishing-smishing-vishing-so-schuetzen-sie-sich-vor-datendiebstahl/
[4] https://www.saferinternet.at/news-detail/phishing-wie-betrueger-innen-unsere-daten-angeln
[5] https://www.oesterreich.gv.at/themen/onlinesicherheit_internet_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/2/2.html

Lieblingsrestaurant, aber dahinter lauern Cyberkriminelle. Falls möglich, fragen Sie nach dem richtigen Namen des Netzwerks.

Wenn Sie also im öffentlichen **WLAN (Drahtlos-Netzwerk)** unterwegs sind,

- nehmen Sie **keine Zahlungen** vor und verwenden Sie **keine Anmeldedaten,**
- **laden Sie nichts herunter**, d. h., verschieben Sie alle **Downloads auf später**, wenn Sie wieder in einem gesicherten WLAN-Netz sind,
- verzichten Sie auch auf Online-Shopping,
- lassen Sie sich nicht auf Bildschirm und Tastatur schauen.

Schalten Sie WLAN nur dann ein, wenn Sie es brauchen. **Keine automatische WLAN-Suche.**

Auch lesenswert:

- Sicherheits-Falle WLAN - WKO.at: https://www.wko.at/it-sicherheit/sicherheits-falle-wlan
- Das Risiko bei öffentlichen WLANs minimieren - WKO.at: https://www.wko.at/tirol/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/risiko-oeffentliches-wlan-minimieren

Übung:

Wenn Sie die Übungen am Computer machen, wählen Sie „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im roten Teil „Smartphone“[6].

3 Cybersecurity-Tipp 3

Link angeklickt, Anhang geöffnet

Wenn Sie voreilig einen **Link angeklickt oder einen Anhang geöffnet haben**, dann

- entweder landen Sie auf einer **gefälschten Webseite**
- oder laden Sie direkt auf Ihren Computer ein **Schadprogramm** herunter.

So kann man sich in solch einem Fall **retten**:

- Ziehen Sie den Stecker raus und rufen Sie eine/n IT-Experten/-in Ihres Vertrauens an. Haben Sie keine/n? Dann: Cyber-Security-Hotline - WKO.at - **24h-Call Center, Notfallhilfe und Erstinformation**[7]
- Geben Sie auf der Website, die sich nach dem Anklicken geöffnet hat, keinen Benutzernamen und keine Passwörter an
- Lassen Sie Ihren PC mit einem aktualisiertem Virenschutzprogramm durchsuchen
- Sicherheitshalber können Sie Ihre Zugangsdaten und Passwörter auf einem anderen Gerät ändern

Weitere hilfreiche Infos:

[6] https://www.wko.at/tirol/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/risiko-oeffentliches-wlan-minimieren
[7] https://www.wko.at/it-sicherheit/cyber-security-hotline#:~:text=Die%20Cyber%2DSecurity%2DHotline%20ist,kostenlos)%20telefonische%20Erstinformation%20und%20Notfallhilfe

Was tun, wenn Kriminelle Ihre Daten gestohlen haben?[8]

4 Cybersecurity-Tipp 4

Sich nicht manipulieren lassen – Social Engineering

Es ist nur menschlich, nervös zu werden, wenn ein Anruf von (vermeintlichen) Polizeibeamten oder eine alarmierende E-Mail von Ihrer Bank kommt. Besonders, wenn Sie gerade in Eile oder im Stress und überfordert sind. Dann passiert es schnell, dass Sie einen verhängnisvollen Klick ausführen oder Ihre Zugangsdaten angeben. Der Schaden kann verheerende Folgen für Sie persönlich und für Ihr Unternehmen haben. Auch, wenn Sie an einem bestgesicherten Computer arbeiten, ist es wahrscheinlich, dass Sie den psychologischen Tricks der Betrüger erliegen.

Versuchen Sie sich also diese **Automatismen** einzuprägen, die Sie dann auch im Stress abrufen können:

- bei jedem E-Mail-Anhang und jedem Link (**auch in SMS!**) **misstrauisch** sein – **nicht klicken** - und im Zweifel - beim Absender telefonisch oder persönlich **nachfragen**,
- Absender/innen der **E-Mail-Adresse genau überprüfen**,
- eine **unpersönliche Anrede** als Hinweis auf Betrug deuten,
- die **Dringlichkeit** der vermeintlich notwendigen Updates, Verifizierungen usw. ignorieren,
- **keine vertraulichen Daten oder Zugangsdaten** per E-Mail oder am Telefon angeben,
- **persönliche Informationen in sozialen Medien** meiden (separate E-Mail-Konten für soziale Netzwerke verwenden),
- bei einer E-Mail, in der steht, dass Sie etwas gewonnen hätten, einfach die Finger davonlassen (**Fake-Gewinnspiele**).

Hier können Sie Ihre Reaktionen in echt überprüfen: Onlinebetrug-Simulator (aknoe.at)[9]

Weitere Infos:

Social Engineering - der Mitarbeiter als Angriffsziel - WKO.at[10]

5 Cybersecurity-Tipp 5

Digitale Geräte schützen

Wenn Sie Ihr Haus verlassen, sperren Sie die Tür zu. So sollten Sie auch Ihr digitales Gerät sperren, wenn Sie es verlassen (z. B. durch gleichzeitiges Drücken von Windows-Taste und L-Taste). Damit schützen Sie Ihren Computer vor Unbefugten.

Voraussetzung für eine **Bildschirmsperre** ist ein **passwortgeschütztes Benutzerkonto**. Es empfiehlt sich auch ein separates Benutzerkonto für Geschäftszwecke.

Wenn Sie einen **Blickschutzfilter** verwenden, sind Ihre Geräte vor fremden Blicken im öffentlichen Raum geschützt. Solche Blickschutzfilter sind einfach zu befestigen und zu entfernen.
Ein **No-Go** ist das **Anstecken von USB**-Laufwerken/Sticks, die Ihnen nicht gehören. Es ist, als ob Sie eine Person in Ihr Haus einladen, die sich dann aber unerlaubterweise auch in absolut privaten

[8] https://www.watchlist-internet.at/news/was-tun-wenn-kriminelle-ihre-daten-gestohlen-haben/

[9] https://phishing.onlinebetrug.aknoe.at/Identity/Account/RegisterEmail
[10] https://www.wko.at/it-sicherheit/social-engineering-der-mitarbeiter-als-angriffsziel

Bereichen umschaut. Und sie öffnet sogar Fenster, um später ohne Ihr Wissen mit bösen Absichten wiederzukommen.

Weiterführende Infos:

- Onlinesicherheit – Kontomanagement[11]
- Sicherheitsrisiko Smartphone - WKO.at[12]
- BSI - Benutzerkonten (bund.de) mit Kurzvideo[13]

6 Cybersecurity-Tipp 6

Warum möchte mich jemand angreifen?

Cyberangriffe betreffen längst nicht nur große Konzerne oder die öffentliche Verwaltung. Auch Klein- und Kleinst-Unternehmen werden von Cyberkriminellen ins Visier genommen. Die Motivation der Angreifer/innen kann vielfältig sein, z.B.:

- **Geld:**
  - Durch Erpressung oder Täuschung werden Sie dazu gebracht, einen Geldbetrag an Betrüger/innen zu überweisen oder
  - Ihre Daten werden ausgespäht und es kommt zu unberechtigten Abbuchungen von Ihrem Konto.
- **Neugierde, Spaß:**
  - Möchtegern-Hacker/innen, sogenannte Script-Kiddies (Script – eine Datei mit Befehlsfolge) brechen in Ihr System ein, weil sie darin eine befriedigende Herausforderung sehen. Dies kann Ihnen auch einen hohen, nicht umkehrbaren Schaden verursachen.
- **Zerstörungswut:**
  - Vandalen können z. B. Ihre ehemaligen Mitarbeiter/innen oder Konkurrenten/innen sein, die Ihnen schaden wollen.
- **Spionage:**
  - Angreifer/innen verschaffen sich Zugriff auf Ihre Kundendaten, Pläne, Buchhaltungssysteme usw., um sich Vorteile zu sichern.[14]

Übung:

Sich vor Betrug schützen (ovosplay.com). Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im grünen Teil **„Sich vor Betrug schützen“ -„Diverse Betrugsfälle“**[15]

7 Cybersecurity-Tipp 7

Persönliche Daten preisgegeben: Identitätsdiebstahl-Alarm!

[11] https://www.onlinesicherheit.gv.at/Themen/Praevention/Konten-und-Passwoerter/Kontomanagement.html
[12] https://www.wko.at/it-sicherheit/sicherheitsrisiko-smartphone
[13] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Basisschutz-fuer-Computer/Benutzerkonten/benutzerkonten_node.html
[14] Pohlmann, Norbert (2022): Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.
[15] https://cybersecurityquiz.app.ovosplay.com/#/login

Wenn Sie im Stress nicht genug wachsam waren und **Ihre persönlichen Daten oder Zugangsberechtigungen preisgegeben** haben, dann können die Betrüger/innen in Ihrem Namen vieles unternehmen, z.B.:

- Bestellungen aufgeben,
- Geld von Ihrem Bankkonto abbuchen,
- ein neues Konto für Geldwäsche eröffnen,
- Ihre E-Mail-Adresse für betrügerische E-Mails nutzen,
- Ihre Social-Media-Profile übernehmen,
- diverse Verträge abschließen.

Was können Sie tun?

- Ihre Zugangsdaten umgehend auf einem anderen Gerät ändern,
- die Notlage sofort Ihrem/Ihrer IT-Administrator/in melden
- oder die Cyber-Security-Hotline - WKO.at anrufen[16] (24h-Call Center, Notfallhilfe und Erstinformation).

Weitere Infos:

- Identitätsdiebstahl: Das sind die gängigsten Betrugsmaschen - Watchlist Internet (watchlist-internet.at) (u. A.: betrügerische Marktforschungsinstitute, Stellenanzeigen, Kleinanzeigen)[17]
- Onlinesicherheit - Identitätsdiebstahl (Frühwarnsignale, Gegenmaßnahmen)[18]

8 Cybersecurity-Tipp 8

Betrügerische E-Mails schnell erkennen

Cyberattacken erfolgen oft automatisiert. Es werden **Massen-E-Mails** mit **verseuchten** Anhängen oder Links verschickt. Immer fällt jemand darauf herein, sei es aus Unachtsamkeit, aus Unwissenheit oder aus anderen Gründen.

- Es gibt einige Tricks, wie Sie betrügerische E-Mails **erkennen** können:
  - Fahren Sie mit der Maus über die **Absender/in-Adresse** oder den zugeschickten **Link**, ohne diesen anzuklicken. So entdecken Sie möglicherweise Folgendes:
  - Sonderzeichen oder Rechtschreibfehler (z. B. ein „f“ statt „ff“, fehlende Buchstaben wie „AMZON“),
  - der/die Absender/in stimmt mit der vorgetäuschten Institution/Person nicht überein (privater Name, institutionsfremde Domäne wie „gmail.com“)
- Überprüfen Sie das **Dateiformat** des Anhangs:
  - eine Datei mit Endung „.exe“ enthält möglicherweise ein ausführbares Schadprogramm,
  - auch andere Dateiformate sind fragwürdig: z. B. „.img“ oder „.jar“,
  - es gibt keine Garantie, dass pdf- oder docx-Dateien sicher sind,
  - manchmal ist der Dateiname länger als es auf den ersten Blick erscheint, z. B. „pdf.exe“

[16] https://www.wko.at/it-sicherheit/cyber-security-hotline#:~:text=Die%20Cyber%2DSecurity%2DHotline%20ist,kostenlos)%20telefonische%20Erstinformation%20und%20Notfallhilfe
[17] https://www.watchlist-internet.at/news/identitaetsdiebstahl-das-sind-die-gaengigsten-betrugsmaschen/?sword_list%5B0%5D=Identit%C3%A4tsdiebstahl&no_cache=1
[18] https://www.onlinesicherheit.gv.at/Themen/Gefahren-im-Netz/Privatsphaere/Identitaetsdiebstahl.html

- Im Text der E-Mail finden Sie Rechtschreib- oder Grammatikfehler, z. B. „fur“ statt „für“, manchmal erkennen Sie eine schlechte Übersetzung
- Sie werden oft unpersönlich angesprochen mit z. B. *Kunde, Herr/Frau, Hallo, Guten Tag*

E-Mails mit verdächtigen Links oder Anhängen sind als **gefährlich** einzustufen!

Übungen:

- Technische Bedrohungen (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im blauen Teil **„Technische Bedrohungen“ - „Schadsoftware“**[19]
- BAKgame – IT-Sicherheit in der Wirtschaft - Phishing-Quiz[20]

9 Cybersecurity-Tipp 9

Passwörter – Schlüssel zur digitalen Sicherheit

Wenn Sie Ihren Computer mit dem Passwort „1234“, „abcdf“, „Administrator“ oder „Ichliebedich“ schützen, dann schützen Sie ihn damit nicht wirklich. Solche Passwörter können **innerhalb weniger Sekunden geknackt** werden.

Wollen Sie keine leichte Beute für Betrüger/innen mehr sein, dann brauchen Sie ein langes und starkes Passwort, z. B. **Anfangsbuchstaben einer Passphrase** wie z.B.:

„In 6 Wochen werde ich mich um 50% besser in der Cybersicherheit auskennen und keinen € wegen Cyberangriffen verlieren 😊“ – „**I6Wwimu50%bidCauk€wCv:)**“

Übung:

Einführung: Passwörter (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im gelben Teil **„Datenschutz“ – „Passwörter“**[21]

10 Cybersecurity-Tipp 10

Datenverlust – passiert auch ohne Cyberkriminelle

Vor Missgeschick oder Pech sind wir auch im digitalen Leben nicht gefeit. Wenn Ihre **Daten plötzlich weg** sind, ist das ärgerlich und kann in Ihrem Unternehmen massive Probleme zur Folge haben. Wie kann es zu einem Datenverlust kommen? Hier die häufigsten Ursachen:

1. physische Beschädigung
    a. Wasserschaden – Kaffee oder Wasser über Laptop-Tastatur verschüttet oder undichte Laptoptasche bei Regen
    b. Gerät heruntergefallen
    c. Gewitter und Blitzeinschlag ins Stromnetz
    d. Hitze- oder Kälteeinwirkungen
    e. Stromausfall im falschen Moment
2. Bedien- und Fahrlässigkeitsfehler

[19] https://cybersecurityquiz.app.ovosplay.com/#/login
[20] https://play.bakgame.de/PhishingQuiz/
[21] https://cybersecurityquiz.app.ovosplay.com/#/login

a. Daten versehentlich gelöscht
b. Dateninhalte versehentlich überschrieben
c. USB-Stick verloren
d. fehlerhafte Neuinstallation oder Festplatten-Formatierung

3. **Programm-(=Software)Fehler** wie z. B. bei fehlgeschlagenen Aktualisierungen

Sichern Sie deshalb Ihre Daten regelmäßig **auf einem externen Speichermedium** (z. B. USB-Festplatte).

Weiterführende Infos:

- Datensicherung mit Konzept – darauf müssen Sie bei der Planung achten - WKO.at[22]
- Datensicherung: Das ist zu beachten (fit4internet.at)[23]

11 Cybersecurity-Tipp 11

Der PC streikt? Keine Panik, mit Backups ist Ihr Business auf der sicheren Seite

Auch wenn Sie alle Schutzmaßnahmen richtig befolgen, kann immer etwas Schlimmes passieren (Kaffee verschüttet, Brand, Cyberangriff, Defekte).

Ohne ein **Backup (=Sicherheitskopie)** Ihrer Daten **riskieren** Sie jederzeit, dass Sie alles verlieren.

Erstellen Sie also noch heute ein Backup und tragen Sie die nächsten **Backup-Termine** in Ihren Kalender ein. Wie geht das?

- Kopieren Sie alles zumindest auf eine **externe Festplatte** (im Handel erhältlich) oder
- speichern Sie Ihre Daten in der **Cloud** (darauf werden wir noch eingehen).

Fertig, Ihre Datensammlung ist gesichert. Überprüfen Sie noch, ob die Daten sicher wiederherstellbar sind. Bitte daran denken: Lagern Sie Ihre Sicherheitskopie **an einem räumlich getrennten Ort**!

Es ist auch möglich, mehr als „nur" Ihre Dateien (Kund/innendaten, Buchhaltungsunterlagen, E-Mails etc.) zu sichern. Möchten Sie im Notfall Ihr **ganzes System** wiederherstellen können, gibt es dafür die **Image-Sicherung**. Solch ein Speicher-Abbild der Festplatte beinhaltet alles: auch Ihr Betriebssystem, alle Einstellungen, Anwendungen und Daten. Ein/e IT-Dienstleister/in hilft Ihnen dabei.

Weitere Infos und Übungen:

- Anleitung zur Datensicherung - WKO.at Video[24]
- Backups | Digitalführerschein (DiFü) (xn--dif-joa.de) Infos und Quiz[25]
- Online-Quiz Lerneinheit 3 "Datensicherung & Notfallplanung" | Bottom-Up (dsin-berufsschulen.de)[26]
- DsiN-Computercheck - Sicherheitstipps (computercheck24.com) – wählen Sie Ihr System (zB Windows) und gehen Sie zum Teil „Sichern Sie regelmäßig Ihre Daten"

[22] https://www.wko.at/it-sicherheit/datensicherung-mit-konzept-darauf-muessen-sie-achten
[23] https://www.fit4internet.at/page/dranbleiben/461
[24] https://www.wko.at/it-sicherheit/anleitung-zur-datensicherung
[25] https://xn--dif-joa.de/journey-section/backups-lv1-privat/
[26] https://www.dsin-berufsschulen.de/online-quiz-lerneinheit-3-datensicherung-notfallplanung

12 Cybersecurity-Tipp 12

Wenn Ransomware Ihre Geschäftsdaten entführt

„Deine Daten werden unwiederbringlich verschlüsselt, wenn du nicht zahlst" – eine solche Erpressung heißt **RANSOMWARE.** Das ist ein **Erpressungs- und Verschlüsselungs-Schadprogramm** - heutzutage die größte Gefahr im Internet.

Cyberkriminelle haben auf Ihrem Computer unbemerkt ein Schadprogramm installiert. Sie konnten dadurch auf Ihre wichtigen Daten zugreifen und sie verschlüsseln, d. h., für Sie sind die **Daten nicht mehr lesbar**. Von Ihnen wird nun ein **Lösegeld** verlangt – oft mehrere Tausend Euro, die meistens in Bitcoin zu zahlen wären. So können die Betrüger/innen anonym bleiben.

Allerdings gibt es keine Garantie, dass Sie den Zugriff auf Ihre Daten tatsächlich zurückerhalten. Möglich ist auch, dass Ihre Daten inzwischen beschädigt wurden.

Im Falle eines Ransomware-Angriffs empfiehlt sich daher: **nicht zahlen** und **nicht verhandeln**! Wenden Sie sich an den/die IT-Dienstleister/in Ihres Vertrauens, um die Attacke fachkundig abzuwehren und den Schaden zu begrenzen.

Bei Unsicherheit hier anrufen: Cyber-Security-Hotline - WKO.at[27] (24h-Call Center, Notfallhilfe und Erstinformation).

Weitere Infos und Übungen:

- No more ransom[28]
- Technische Bedrohungen (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion" - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im blauen Teil **„Technische Bedrohungen" – „Ransomware"**[29]

13 Cybersecurity-Tipp 13

Firewall – Ihre digitale Brandmauer

Ein unverzichtbares Element Ihrer digitalen Sicherheit ist die **Firewall**.

Das ist ein Programm, das überprüft, welche Daten auf den Computer hereingelassen werden und welche nicht. Daten aus nicht vertrauenswürdigen Quellen kommen bestenfalls nicht durch.

Auch wenn der Computer ohne Ihr Wissen verdächtige Daten versendet, werden Sie von der Firewall alarmiert. Das kann infolge eines noch nicht entdeckten Cyber-Angriffs vonstattengehen.

Diese Schutzwand ist oft schon im Betriebssystem eingebaut. Auch WLAN-Router (=Netzwerkgeräte) sind meistens mit Firewall-Funktionen ausgestattet.

Überprüfen Sie also, ob Ihre Firewall **aktiviert** und dementsprechend **eingestellt** ist (z. B.: *Einstellungen – Suchen – Firewallstatus überprüfen*). Falls nicht, steht die Tür offen und kein/e Türsteher/in regelt den Einlass.

[27] https://www.wko.at/it-sicherheit/cyber-security-hotline#:~:text=Die%20Cyber%2DSecurity%2DHotline%20ist,kostenlos)%20telefonische%20Erstinformation%20und%20Notfallhilfe
[28] www.nomoreransom.org/de/index.html
[29] https://cybersecurityquiz.app.ovosplay.com/#/login

Weitere Infos:

- DsiN-Computercheck - Sicherheitstipps (computercheck24.com)[30] – wählen Sie Ihr System (z.B. Windows), gehen Sie zum Teil „Schützen Sie Ihren Computer mit einer Firewall“
- Schritt-für-Schritt-Anleitung[31]

14 Cybersecurity-Tipp 14

Ein Notfallplan minimiert Schäden

Im Fall eines Cyber-Angriffs müssen Sie schnell und gezielt handeln. So reduzieren Sie die Folgekosten für Datenrettung, Betriebsunterbrechung und Schadensersatzansprüche, Rechtsberatung oder PR-Beratung bei Imageschäden.

Sehr hilfreich ist daher ein klarer Plan, was im Ernstfall zu tun ist. Auf Ihrer **Notfall-Karte** kann z.B. stehen:

1. weitere Arbeit am Computer einstellen,
2. das Gerät vom Netzwerk trennen,
3. Beobachtungen dokumentieren,
4. Beweise sichern (Datum/Uhrzeit notieren, Bildschirm fotografieren, kurze Notizen: wer, was, wann, wo und warum hat gerade etwas am Computer getan),
5. Cyber Security Hotline anrufen (Cyber-Security-Hotline - WKO.at)[32]

Um sich für einen IT-Notfall optimal zu wappnen, können Sie eine/n IT-Dienstleister/in zu Rate ziehen. Sinnvoll ist vielleicht auch ein **Penetrationstest**, bei dem alle Schwachstellen Ihrer Geräte aufgespürt werden. Als Ergebnis des Tests bekommen Sie Ihr individuelles **Notfallkonzept**.

Weitere Infos:

- Muster Cyber Notfallplan (wko.at)[33]
- Was tun, wenn Ihr Unternehmen Opfer von Cybercrime wurde? - Watchlist Internet (watchlist-internet.at)[34]

15 Cybersecurity-Tipp 15

Wann ist ein Passwort nicht stark genug?

Besonders **leicht zu knacken** sind Passwörter, die Folgendes enthalten:

- Wörter aus dem Wörterbuch,
- Informationen aus dem Privat- oder Berufsleben (Haustier, Automarke, Heimatstadt, erste Liebe, Geburtsdaten usw.),
- Buchstaben, die durch ähnliche Zahlen ersetzt wurden, z.B. 5 für S.

Vermeiden Sie auch:

[30] https://www.computercheck24.com/visor_server_1/dsin30/de/securitytips.page
[31] https://www.computercheck24.com/visor/app/cmscontent/_visor30/dsin30/pdf/firewall_win10_use_de.pdf
[32] https://www.wko.at/it-sicherheit/cyber-security-hotline#:~:text=Die%20Cyber%2DSecurity%2DHotline%20ist,kostenlos)%20telefonische%20Erstinformation%20und%20Notfallhilfe
[33] https://www.wko.at/stmk/gewerbe-handwerk/bau/muster-cyber-notfallplan.pdf
[34] https://www.watchlist-internet.at/news/was-tun-wenn-ihr-unternehmen-opfer-von-cybercrime-wurde/

- **Passwort-Recycling**, d.h. das gleiche Passwort bei verschiedenen Online-Diensten,
- **Niederschreiben** Ihrer Passwörter (digital oder auf Papier),
- **Teilen** Ihrer Passwörter (z. B. für Streaming-Dienste),
- **Versenden** der Passwörter per SMS oder E-Mail,
- **allzu einfache Fragestellungen** zur Passwortwiederherstellung, z. B. "Wie lautet der Name deines Haustiers?“ – die Antwort findet ein/e Hacker/in schnell heraus und besorgt sich problemlos ein neues Passwort für Ihr Konto oder Profil.

Ein starkes Passwort darf **nicht zu kurz** (mindestens 8 Zeichen) und **nicht direkt beobachtbar** (0000, 1234, qwertz, w2e3r4t5– die Tasten liegen eng nebeneinander) sein.

Wenn Sie einen Passwortmanager oder die 2-Faktor-Authentifizierung verwenden, erhöht sich Ihre IT-Sicherheit deutlich. Auf diese Werkzeuge kommen wir noch in einem der nächsten Cybersecurity-Tipps zurück.

Eine Aufstellung der 200 häufigsten Passwörter 2022 ist auf der NordPass Seite zu finden (scrollen Sie bitte nach unten, um absolute Favoriten zu sehen)[35].

Übungen:

- Log-ins und Passwörter | Digitalführerschein (DiFü) (xn--dif-joa.de)[36]

16 Cybersecurity-Tipp 16

Aktualisierungen – immer auf dem neuesten Stand

Wenn die automatischen **Updates** – also die **Aktualisierungen von Programmen** – nicht aktiviert sind, erkennt Ihr Computer nur alte Bedrohungen und bleibt offen für neue Viren oder andere Arten von Malware (=Schadprogramme).

Aktualisiert werden sollten sowohl **Programme** als auch **Plugins**, d.h. kleine Zusatzprogramme im Browser z.B. zum Abspielen von Musik, die oft Sicherheitslücken haben.

Machen Sie einen Computercheck, um veraltete Programme zu finden: DsiN-Computercheck - Starten (computercheck24.com)[37].

Auch das Betriebssystem wie Windows soll sich automatisch aktualisieren. Überprüfen Sie Ihre Einstellungen für Updates.

Übungen:

- Technische Bedrohungen (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im blauen Teil „Technische Bedrohungen“ -„Updates“[38]
- DsiN-Computercheck - Aktuelle Downloads (computercheck24.com)[39]

[35] https://nordpass.com/de/most-common-passwords-list/
[36] https://xn--dif-joa.de/journey-section/logins-und-passwoerter-lv3-privat/
[37] https://www.computercheck24.com/visor_server_1/dsin30/de/showAudit.action;jsessionid=3D8AD57499F597A65EACF305C52FC085
[38] https://cybersecurityquiz.app.ovosplay.com/#/login
[39] https://www.computercheck24.com/visor_server_1/dsin30/de/downloadlinks.page

- Automatische Updates für iOS, Windows und Android einrichten | Digitalführerschein (DiFü) (xn--dif-joa.de)[40]

17 Cybersecurity-Tipp 17

CEO-Betrug. Ist das wirklich der*die Vorgesetzte?

Wie funktioniert dieser Cyber-Angriff? Betrüger*innen überprüfen, z. B. mit einer E-Mail, ob der*die Chef*in im Büro anwesend ist. Kommt eine Abwesenheitsnotiz zurück, stehen die Chancen auf das Gelingen eines **Cheftricks** nicht schlecht.

Als Mitarbeiter*in werden Sie nun mit einer gefälschten E-Mail um **Geldüberweisung** gebeten. Die Absenderadresse ist nur scheinbar echt. Das Anliegen sei **absolut vertraulich und dringend zu erledigen.** Wenn der*die falsche Chef*in Sie anruft, kann es sogar sein, dass die **Stimme simuliert** ist! Dabei wird Ihnen das Gefühl vermittelt, Sie wegen besonderer fachlicher Kompetenzen und Ihrer absoluten Zuverlässigkeit für diese delikate Aktion auserwählt zu haben. Fühlen Sie sich geehrt und übernehmen den Auftrag?

Auf der sicheren Seite sind Sie nur, wenn Sie sich den Auftrag in einer **persönlichen Rücksprache** und zusätzlich noch schriftlich bestätigen lassen. Sonst könnte eine Geldüberweisung einen enormen Schaden verursachen.

Infos, Beispiele:

- CEO-Fraud: Wenn sich Kriminelle als Geschäftsführung ausgeben… - Watchlist Internet (watchlist-internet.at)[41]
- Europol: at.pdf (europa.eu)[42]

Übung:

Sich vor Betrug schützen (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion“ - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im blauen Teil „Technische Bedrohungen“ - **„Unternehmensbetrug“**[43]

18 Cybersecurity-Tipp 18

DoS- oder DDoS-Attacke – unter Beschuss der Massen

Wenn die Website Ihres Unternehmens plötzlich gar nicht mehr oder auffallend langsam geht, haben Sie möglicherweise mit einer **DoS-Attacke** zu tun.

DoS steht für **„Denial of Service“ – „Verweigerung des Dienstes“.**

Hacker:innen wollen Ihnen schaden, indem sie sehr viele Anfragen über Ihre Website schicken. Das überlastet das System und Ihre Website stürzt ab. Sie sind für Ihre Kund:innen nicht mehr erreichbar.

[40] https://xn--dif-joa.de/nachrichten/nachrichten-gefahrenschutz/windows-android-ios-macos-so-geht-die-update-automatik/
[41] https://www.watchlist-internet.at/news/ceo-betrug-wenn-sich-kriminelle-als-geschaeftsfuehrung-ausgeben/
[42] https://www.europol.europa.eu/sites/default/files/documents/at.pdf
[43] https://cybersecurityquiz.app.ovosplay.com/#/login

Wenn Sie nicht nur von einem, sondern von hunderten oder gar tausenden Endgeräten angegriffen werden, ist das ein **DDoS-Angriff, „Distributed Denial of Service" – „verteilter Dienstverweigerung-Angriff"**, noch verheerender!

Falls Sie also feststellen, dass die Nicht-Verfügbarkeit der Webseite Ihres Unternehmens tatsächlich folgenschwer wäre, lassen Sie sich von einem/r IT-Experten/in beraten.

Die Erstinformation bekommen Sie bei der Cyber-Security-Hotline - WKO.at[44].

Weitere Infos:

- DDoS-Angriffe – Allgemeine Informationen (onlinesicherheit.gv.at)[45]
- Umfangreiche Information des BMI: Distributed Denial of Service (DDoS) (dsn.gv.at)[46]
- DDoS-Attacken: Tipps zum Erkennen und Abwehren - datensicherheit.de[47]

Übung:

Technische Bedrohungen (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion" - bei erster Anwendung ist eine unkomplizierte Registrierung notwendig – Übungen für heute finden Sie im blauen Teil „Technische Bedrohungen" -„Backups"[48]

19 Cybersecurity-Tipp 19

Vertrauliche Botschaften verschlüsseln – Schritt für Schritt

Dateien, die via E-Mail, SMS oder über WhatsApp etc. verschickt werden, können auch von anderen als den direkten Empfänger/innen gelesen werden. Möchten Sie streng vertrauliche Dokumente versenden, so können Sie diese zusätzlich verschlüsseln. Dafür würden sich zum Beispiel diese Möglichkeiten bieten:

1. In einem Microsoft-Windows-Dokument (zum Beispiel „Word") wählen Sie: *Datei – Informationen – Dokument schützen – mit **Kennwort** verschlüsseln* (mind. 8 Zeichen, Groß-/Kleinbuchstaben, Sonderzeichen). Das Kennwort geben Sie dem/der Empfänger/in persönlich, und, falls nicht möglich, per SMS.
2. 7-Zip
    a. ein kostenloses Kompressionsprogramm (z.B. hier erhältlich: 7-Zip | heise Download[49]),
    b. praktisch bei großen Dokumenten,
    c. Dokument kann so dicht in eine Datei verpackt (**=komprimiert**) werden, dass es weniger Speicherplatz erfordert,
    d. Dokument kann mit einem **Kennwort** verschlüsselt werden: Dateispeicherort öffnen (im Explorer, z.B. unter „Downloads") – rechte Maustaste – 7-Zip wählen – *zu einem Archiv hinzufügen* – unter *Verschlüsselung* Passwort eingeben - das

[44] https://www.wko.at/it-sicherheit/cyber-security-hotline#:~:text=Die%20Cyber%2DSecurity%2DHotline%20ist,kostenlos)%20telefonische%20Erstinformation%20und%20Notfallhilfe
[45] https://www.onlinesicherheit.gv.at/Services/Technologie-Schwerpunkte/DDoS/DDoS-Angriffe-Allgemeine-Informationen.html
[46] https://www.dsn.gv.at/501/files/Cyber_Ratgeber/Schriftenreihe_Cybersicherheit_Distributed_Denial_of_Service_DDoS_Februar_2022_BF_20220216.pdf
[47] https://www.datensicherheit.de/ddos-attacken-tipps-erkennen-abwehren
[48] https://cybersecurityquiz.app.ovosplay.com/#/login
[49] https://www.heise.de/download/product/7-zip-13139

komprimierte und verschlüsselte Dokument verschicken – Passwort persönlich oder per SMS

Übung:

Home-Office (ovosplay.com) - Wenn Sie die Übungen am Computer machen, wählen Sie bitte „Zur Webversion" – bei erster Anwendung ist eine unkomplizierte Registrierung notwendig. Die Übungen passend für das heutige Thema finden Sie im grünen Teil **„Home-Office" - Verschlüsselung**[50]

20 Cybersecurity-Tipp 20

Wie erkennen Sie, dass ein/e Hacker/in an Ihrem Computer im Hintergrund aktiv ist?

Plötzlich wollen die Computer-Programme (**=Applikationen**) nicht starten oder sind sehr langsam. Das ist nicht nur eine Nervenprobe für Sie, sondern kann auch ein möglicher Cyber-Angriff sein. So machen Sie im Verdachtsfall selbst den ersten **Sicherheits-Check**:

- den **Windows Defender** öffnen (z. B. in das Suchfeld unten auf der Taskleiste – oft als Lupe angezeigt - „Windows Defender" eintippen),
- **Viren- und Bedrohungsschutz** wählen,
- **Scanoption** wählen,
- **Vollständige Überprüfung** wählen – **Jetzt überprüfen**,
- infizierte Objekte werden in die Quarantäne verschoben,
- diese Dateien UNBEDINGT löschen,
- den/die IT-Dienstleister/in Ihres Vertrauens das Gerät sicherheitshalber überprüfen lassen.

Auf alle Fälle können Sie ihn/sie auch bitten, einen **Rettungs-Bootstick** erstellen zu lassen. Auf so einem USB-Stick wird Ihr Windows-Betriebssystem ohne Daten gespeichert. Bei einer Beschädigung können Sie Windows mit dem Stick wiederherstellen und starten.

21 Cybersecurity-Tipp 21

Digitale Rückendeckung stärken. Warum braucht man Logging und Monitoring?

Bei einem Cybervorfall bleibt uns meist nichts anderes übrig, als uns an einen/e IT-Experten/in zu wenden. Wir hoffen dann sehr, dass sie/er den Computer – also die Daten, das System, die Programme – erfolgreich „rettet".

Damit dies tatsächlich gelingt, müssen die IT-Experten/innen wissen, was genau – Schritt für Schritt – passiert ist. Das heißt, sie brauchen eine **Aufzeichnung (=Logging-Protokoll)** aller vorhergehenden Ereignisse, z.B.,

- wer, wann und wo sich ein- und ausgeloggt hat,
- welches Programm gestartet wurde (E-Mail-Programm wie Outlook, Buchhaltungsprogramm, Übersetzungssoftware wie Trados Studio, Grafikprogramm usw.),
- wer und wann auf Daten im Firmennetzwerk zurückgegriffen hat,
- wer etwas hochgeladen oder heruntergeladen hat.

[50] https://cybersecurityquiz.app.ovosplay.com/#/login

Für solch eine **Protokollierung** aller Ereignisse im Computer gibt es verschiedene Standards und Normen, z.B. ISO27000-Reihe oder CIS Top18[51]. Das *AIT Austria Institut of Technology* hat all diese Normen im Zuge des Forschungsprojektes *CyberMonoLog* in einem einzigen Dokument zusammengeführt. Wenn die dort genannten Anweisungen umgesetzt werden, kann ein Cyberangriff dank eines optimal sichergestellten **Monitorings (=Überwachung)** möglichst früh entdeckt und schnell abgewehrt werden.

Daher sind Unternehmer/innen und Computernutzer/innen gut beraten, sich dieses detaillierte Regelwerk anzusehen, ihre/n IT-Experten/in darauf aufmerksam zu machen und die Umsetzung in die Wege zu leiten.

Anwendungs-Tipp für Ihre IT-Dienstleister/innen: CyberMonoLog[52]

22 Cybersecurity-Tipp 22

Wurden meine Passwörter enttarnt oder meine Identitätsdaten ausspioniert?

Datenlecks sind keine abstrakte Gefahr. Ihre Daten oder die Ihrer Kunden kursieren möglicherweise bereits auf verschiedenen Hackerforen oder frei im Netz, ohne dass es Ihnen bewusst ist. Sie können aber die Sicherheit Ihrer E-Mail-Adresse oder Ihrer Passwörter sehr einfach überprüfen:

- Gehen Sie auf die Seite: Have I Been Pwned: Check if your email has been compromised in a data breach[53],
- überprüfen Sie dort **Ihre E-Mail-Adressen**,
- mögliche Resultate sind: **Good News – no pwnage found!** oder **Oh no – pwnade!** Dort sehen Sie, wann und wie der Datenabfluss stattgefunden hat.

Sie können auch checken, ob Ihr **Passwort** geleakt wurde: Have I Been Pwned: Pwned Passwords[54]. Das ist eine Datenbank mit Millionen von Passwörtern aus der realen Welt, die zuvor bei Datenschutzverletzungen offengelegt wurden.

Empfehlenswert ist ebenfalls der Checker des Hasso-Plattner-Instituts: Identity Leak Checker (hpi.de)[55]. Dieser Dienst überprüft Ihre E-Mail-Adresse und schickt Ihnen umgehend eine Antwort, ob Sie von einem Datendiebstahl betroffen sind.

23 Cybersecurity-Tipp 23

Gefälschte Links in SMS – Smishing

Smartphones nutzen wir oft unterwegs, wo unsere Konzentration oft niedriger ist als am Computer. Wenn dann eine SMS mit einem **Link** kommt, kann es schnell passieren, dass wir ihn automatisch anklicken.

Dieser Link führt möglicherweise zu einer **gefälschten** Webseite z. B. einer **Bank**, einer **Behörde** oder eines **Lieferdienstes**. Wenn Sie sich dort mit Ihren Daten anmelden, fallen Ihr **Benutzername und Ihr Passwort** in die Hände der Betrüger/innen. Diese Daten lassen sich für verschiedene illegale Aktivitäten nutzen, z. B. für unautorisierte Überweisungen.

[51] https://www.cisecurity.org/controls/cis-controls-list
[52] https://induce.ait.ac.at/cybermonolog-guidelines/
[53] https://haveibeenpwned.com/
[54] https://haveibeenpwned.com/Passwords
[55] https://sec.hpi.de/ilc/search?lang=de

Mit solch einem Link können Sie auch auf einer Webseite mit einem schädlichen Programm landen. Wenn diese **Malware** sich auf Ihrem Handy einnistet, passiert zum Beispiel Folgendes: Die Betrüger/innen stehlen Ihre Daten, kontrollieren Ihr Gerät oder können es verschlüsseln und Lösegeld fordern.

Im Falle von Smishing, gehen Sie am besten zur offiziellen Internetseite (von DHL, Amazon, Finanzamt, Bank usw.), melden Sie sich dort an und überprüfen Sie, ob tatsächlich eine Mitteilung an Sie vorhanden ist.

Die aktuellen Smishing-Warnungen:

- Smishing: Vorsicht vor betrügerischer Reisepass-SMS! - Watchlist Internet (watchlist-internet.at)[56]
- Smishing: Vorsicht vor Fake Magenta-SMS - Watchlist Internet (watchlist-internet.at)[57]
- **Smishing melden**: Meldeformular Rufnummernmissbrauch | RTR[58]

24 Cybersecurity-Tipp 24

GEWINNQUIZ

Wählen Sie bitte die richtige Antwort:

1. **Ein anderes Wort für ein bösartiges Schadprogramm ist:**
   a. Software
   b. Malware
   c. Adware

Leider falsch: Software sind Programme, die auf einem digitalen Gerät installiert sind und verwendet werden können. Es gibt u. a. Systemsoftware (z. B. Windows, Android, Linux) und Anwendungssoftware (z. B. MS Word, Adobe Photoshop, Mozilla Firefox). Das sind keine Schadprogramme.

Richtig! Malware = **mal**icious (bösartig) + Soft**ware**

Leider falsch: Adware = **Ad**vertising + Soft**ware**. Adware zeigt Benutzer/innen eines digitalen Geräts unerwünschte Werbung an.

2. **Wie heißt die Technologie, die beim kontaktlosen Bezahlen verwendet wird?**
   a. NFC
   b. RFID
   c. 7-Zip

Richtig! NFC = Near Field Communication, Nahfeldkommunikation – eine drahtlose Datenübertragung zwischen Geräten über eine sehr kurze Distanz (10-20 Zentimeter)

Leider falsch: RFID = Radio Frequency Identification, Radiofrequenz-Identifikation – eine automatische berührungslose Identifizierung von Objekten mithilfe von Funkwellen. Eingesetzt z. B. bei Zugangskontrolle zu Gebäuden oder Fahrzeugidentifikation für Mauterhebung

[56] https://www.watchlist-internet.at/news/smishing-vorsicht-vor-betruegerischen-sms/
[57] https://www.watchlist-internet.at/news/smishing-vorsicht-vor-diesem-fake-magenta-sms/?sword_list%5B0%5D=smishing&no_cache=1
[58] https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/meldeformular.de.html

Leider falsch: 7-Zip ist ein kostenloses Kompressionsprogramm, mit dem man Dateien oder Ordner komprimieren (=dicht verpacken) und wieder entpacken kann.

3. **Wozu verwendet man Image-Sicherung?**
    a. um Fotos in der Cloud zu speichern
    b. um ein gesamtes Computersystem zu sichern
    c. um Präsentationen als PDF zu speichern

Leider falsch: Um Fotos in der Cloud (=Wolke) zu speichern, braucht man einen Cloud-Speicherdienst, z. B. Google Drive, Dropbox, Microsoft OneDrive, iCloud, Amazon Drive.

Richtig! Image-Sicherung ist ein System-Backup (=Sicherheitskopie), eine exakte Kopie des gesamten Systems, einschließlich Einstellungen und Konfigurationen.

Leider falsch: Das macht man direkt im Präsentationsprogramm. Man klickt auf „Datei“, dann auf „Speichern unter“ (oder „Exportieren“) und man wählt in der Liste der Dateiformate die Option „PDF“ aus.

4. **Was versteht man unter „Passwort-Recycling“?**
    a. regelmäßige Passwortänderung
    b. Entsorgen der Notizen mit allen Passwörtern
    c. Verwendung des gleichen Passworts für mehrere verschiedene Konten oder Online-Dienste

Leider falsch: Das gehört zur Passworthygiene, also zu bewährten Praktiken im Umgang mit Passwörtern. Durch eine regelmäßige Passwortänderung verringert man das Risiko einer unbefugten Nutzung. Andere Empfehlungen sind u. a.: ausreichende Passwortstärke und -länge, Nutzung eines Passwortmanagers und der Zwei-Faktor-Authentifizierung (2FA). Passwort-Recycling ist etwas anderes.

Leider falsch: Man soll Passwörter gar nicht auf Papier notieren, denn das ist aus Sicherheitsgründen sehr problematisch. Eine fremde Person könnte auf die Passwörter zugreifen (mitnehmen oder fotografieren) oder man wirft den Zettel selbst versehentlich weg.

Richtig! Es geht um Passwort-Wiederverwendung (auch Reusing Passwords), d. h., man verwendet ein und dasselbe Passwort für E-Mail, soziale Medien, Online-Banking usw. Bei einem Cyberangriff sind alle Dienste und Konten gleichzeitig und gleichermaßen gefährdet!

5. **Wir würden uns sehr freuen, wenn Sie uns ein kurzes Feedback zu unseren „Cybersecurity-Tipps“ geben:**
    a. **Wie oft lesen Sie die „Cybersecurity-Tipps“?**
        i. Ich habe bisher alle Tipps gelesen
        ii. Ich lese die Tipps, aber nicht regelmäßig
        iii. Ich habe weniger als die Hälfte gelesen
        iv. Ich habe bisher keine Tipps gelesen, erst bin ich auf das Gewinnquiz aufmerksam geworden
    b. **Gefallen Ihnen die „Cybersecurity-Tipps“? Welche Antwort trifft auf Sie am meisten zu?**
        i. Ja, weil sie kurz sind.
        ii. Ja, weil sie in einer verständlichen Sprache geschrieben sind.
        iii. Ja, weil sie erklären, was man machen soll.
        iv. Nein, weil sie für mich zu einfach sind.
        v. Nein, weil ich keine Zeit dafür habe.
        vi. Nein, Cybersicherheit interessiert mich nicht.

vii. Ich habe keine Meinung dazu.

c. **Haben Sie noch weitere Kommentare oder Überlegungen zu den „Cybersecurity-Tipps“?**
   i. Ja, ich möchte Folgendes hinzufügen:
   .....
   ii. Nein

25 Cybersecurity-Tipp 25

Passwort-Manager: Entlastung durch ein Master-Passwort

Um Passwörter **sicher und bequem** zu speichern und zu verwalten, gibt es spezielle Programme. Sie heißen Passwort-Manager und können auf Ihrem Computer, Smartphone oder Tablet installiert werden.

In einen Passwort-Manager steigen Sie **mit einem sogenannten „Master-Passwort“** ein. Alle weiteren Passwörter werden dort **in einer verschlüsselten Datenbank** aufbewahrt. Sind Sie im Passwort-Manager angemeldet, brauchen Sie sich nicht mehr an die anderen Passwörter zu erinnern.

Daher ist es sehr wichtig, das **Master-Passwort nicht zu vergessen!** In solch einem Fall werden Sie keinen Zugriff mehr auf alle Online-Dienste haben, deren Passwörter im Passwort-Manager hinterlegt wurden. Es empfiehlt sich daher, das Master-Passwort ausnahmsweise auch auf Papier zu notieren und es an einem sicheren Ort abzulegen. Natürlich sollte man diese Notiz nicht als „Mein Master-Passwort“ beschriften.

Ein Passwort-Manager bietet auch weitere Vorteile. Falls man z. B. für eine Registrierung ein neues Passwort braucht, entfällt die Suche nach einer einzigartigen Kombination aus Buchstaben, Zahlen und Sonderzeichen. Ihr Passwort-Manager **generiert selbst** starke Passwörter.

Sehr bequem ist die **Funktion des automatischen Ausfüllens von Anmeldedaten**. Dadurch loggen Sie sich bei Ihren Online-Diensten ohne händische Anmeldung ein. Dies geschieht einfach im Hintergrund.

Auf dem Markt gibt es sowohl kostenpflichtige als auch kostenlose Passwort-Manager. Bekannt sind z.B. KeePass oder Bitwarden.

Übung:

Log-ins und Passwörter - Digitalführerschein (DiFü) (difue.de) – Punkt 3[59]

26 Cybersecurity-Tipp 26

Doppelt geschützt mit Zwei-Faktor-Authentifizierung

Es gibt immer mehr Online-Dienste, die zur Erhöhung der Sicherheit die Zwei-Faktor-Authentifizierung (**2FA**) anbieten. Diese Methode kennen Sie möglicherweise bereits vom Online-Banking. Da ist es erforderlich, nicht nur die Anmeldedaten einzutippen, sondern die Anmeldung zusätzlich am Handy zu bestätigen. Falls Ihr Passwort von Betrüger/innen abgefangen wurde, ist Ihr Online-Konto weiterhin vor einem unbefugten Zugriff geschützt.

[59] https://difue.de/lernzentrale/beruflich/level3/datenwelt/log-ins-und-passwoerter/

Als zweiter Faktor kann ein temporärer SMS-Code, eine spezielle Authentifizierungs-App oder ein physischer Sicherheitsschlüssel dienen.

Überprüfen Sie also, ob Ihr E-Mail-Anbieter, Ihre sozialen Medien oder andere Dienste wie z.B. YouTube diese Funktion haben. Das sehen Sie unter den Sicherheitseinstellungen des Dienstes und dort können Sie die 2FA auch aktivieren, meistens mithilfe einer einfachen Anleitung. Solch eine zusätzliche Sicherheitsebene ist ein wichtiger Schritt zum Schutz Ihrer digitalen Identität.

Weitere Informationen

- Die 2-Faktor-Authentifizierung: Online-Banking und Amtswege doppelt sicher (fit4internet.at)[60]
- Log-ins und Passwörter - Digitalführerschein (DiFü) (difue.de) – Punkt 4[61]

27 Cybersecurity-Tipp 27

Was sind Plugins und warum sind sie oft nicht cyber-sicher?

Plugins sind kleine **Zusatzprogramme**, mit denen man Musik oder Videos abspielen (zB *VLC media player*), die Werbung blockieren (zB *AdBlock Plus*), Rechtschreibung und Grammatik prüfen (zB *Grammarly*) oder Anmeldedaten aufbewahren (zB *LastPass*) kann. Sie bieten also zusätzliche **Funktionen oder Erweiterungen** zum bestehenden Programm.

Aus Sicherheitssicht sind sie jedoch oft problematisch. Viele Plugins werden nämlich nicht regelmäßig aktualisiert oder von Entwickler/innen gar nicht mehr unterstützt. **Veraltete Versionen** haben also oft **Sicherheitslücken**, die von Cyberkriminellen ausgenutzt werden können.

Plugins interagieren mit einem Browser (=Computer-Programm zum Aufrufen von Internetseiten) oder mit einem anderen Programm. Wenn ein Plugin unsicher ist, kann das die gesamte Plattform beeinträchtigen. Ein/e Betrüger/in schleust sich über das Plugin auf andere Bereiche des Systems ein.

Daher empfiehlt es sich, nur vertrauenswürdige Plugins aus verifizierten Quellen zu verwenden und sie durch Aktualisierungen immer auf dem neuesten Stand zu halten. Die nicht mehr benötigten Plugins soll man systematisch deinstallieren.

Beispiel eines nützlichen und vertrauenswürdigen Plugins:

- Ihr Schutz vor Fake-Shops - Fake-Shop Detector (fakeshop.at)[62]

28 Cybersecurity-Tipp 28

Unternehmensdaten in der digitalen Wolke

Einige **Cloud-Dienste** sind in einem EPU oder KMU nicht mehr wegzudenken. Im **Cloud-Speicher** werden die Geschäftsdaten online aufbewahrt und synchronisiert, sodass man darauf auch von anderen Geräten zugreifen kann. Für **Videokonferenzen** kommt ebenfalls eine Cloud-Lösung zum Einsatz. Cloud-basierte **E-Mail-Dienste** ermöglichen eine schnelle schriftliche Kommunikation und eine Terminverwaltung von unterwegs. Bei der Planung und Organisation von Aufgaben sind cloud-basierte **Projektmanagement**-Tools nützlich. Auch **Buchhaltung** und **Kundenbeziehungs-**

[60] https://www.fit4internet.at/page/dranbleiben/183
[61] https://difue.de/lernzentrale/beruflich/level3/datenwelt/log-ins-und-passwoerter/
[62] https://www.fakeshop.at/ueber-fake-shop-detector/

Management (CRM – Customer Relationship Management) können in der digitalen Wolke abgewickelt werden.

Daher ist es ratsam, das **Angebot verschiedener Cloud-Anbieter/innen zu vergleichen** und die richtige Cloud für eigene Geschäftsdaten zu wählen. Dabei sind folgende Punkte zu beachten:

- **Datenschutz**: Zertifizierungen, Einhaltung der DSGVO
- **Standort der Cloud-Server**: Wo befindet sind das Rechenzentrum? In Österreich, in einem anderen europäischen Land, in Amerika oder in Asien?
- **Datenverschlüsselung**: Verfügt die Cloud über eigenes Verschlüsselungssystem, sodass die Daten nur verschlüsselt in die Cloud hochgeladen werden?
- **Vertragsbedingungen**, z. B. wie die Verfügbarkeit der Cloud oder der Kundensupport gewährleistet werden? Was passiert mit Daten im Falle einer Naturkatastrophe?
- **Backup-** (=Sicherheitskopie) **und Wiederherstellungsmöglichkeiten** bei einem Datenverlust oder einem Ransomware-Angriff (Verschlüsselung und Erpressung)
- **Benutzerfreundlichkeit** und Funktionalität der Plattform

Infos:

- Cloud Anwendungen für kleine Unternehmen - WKO.at[63]

Übungen:

- Datenschutz (ovosplay.com)[64]

29 Cybersecurity-Tipp 29

Apps sicherheitsbewusst installieren

Zahlreiche nützliche Apps können den Alltag erleichtern. Bevor Sie aber eine herunterladen, überprüfen Sie kurz, ob es sich nicht um eine **Download-Falle** handelt.

Prüfen Sie das Unternehmen, das die App entwickelt hat. Woher kommt es? Wie reagiert der Kundensupport der **Entwickler/innen** auf Bewertungen und Kommentare anderer Nutzer/innen?

Finden Sie die gewünschte App **in einem offiziellen App Store** (Verkaufsplattform mit einem Katalog), wie z. B. Apple App Store oder Google Play Store? Ihre **Authentizität** können Sie auch überprüfen, indem Sie sich auf der offiziellen Website des Unternehmens informieren.

Lesen Sie vor der Installation einer App, welche **Berechtigungen** erforderlich sind. Wenn sie ungewöhnlich viele verlangt, die mit der Funktion der App in keinem Zusammenhang stehen, ist ein Misstrauen angebracht.

Installieren Sie die **Aktualisierungen der Apps**. Die Entwickler/innen beheben auf diese Weise die aufgetretenen Sicherheitslücken oder Probleme.

Aktuelle Warnmeldung: Warnung von Experten: Über 60.000 schädliche Android-Apps entdeckt - CHIP[65]

[63] https://www.wko.at/digitalisierung/cloud-computing
[64] https://cybersecurityquiz.app.ovosplay.com/#/login
[65] https://www.chip.de/news/Ueber-60.000-schaedliche-Android-Apps-entdeckt-Experten-warnen_184822598.html

Die wichtigsten Einstellungen für ein sicheres Smartphone - Watchlist Internet (watchlist-internet.at)[66]

30 Cybersecurity-Tipp 30

Aktuelle Sicherheitswarnungen

Cyberkriminelle greifen nicht nur mit bereits bekannten Methoden an, sie denken sich dauernd neue, **immer raffiniertere Tricks** aus. Daher ist es ratsam, sich über die neuesten Entwicklungen und Warnungen zu informieren. So bleibt der Überraschungseffekt bei einer neuen Betrugsmasche aus.

Es gibt aber auch bösartige Sicherheitswarnungen, deren Ziel ist, Sie in Panik zu versetzen und zu schädlichen Aktionen zu bewegen. **Scareware** („**scare**“=erschrecken + „Soft**ware**“=Programm) erscheint oft als Pop-up-Fenster und enthält eine aufdringlich bunte Meldung über eine vermeintliche Funktionsstörung Ihres Systems. Um den Schaden abzuwenden, werden Sie aufgefordert, sofort – oft sehen Sie auch einen Countdown-Zähler – etwas herunterzuladen. Es kann sich sowohl um ein kostenloses oder ein kostenpflichtiges „Sicherheitsprogramm“ handeln.

Es ist also wichtig, Scareware zu erkennen und sie zu ignorieren. Nutzen Sie nur vertrauenswürdige Quellen, die aktuelle Sicherheitswarnungen bieten. Z. B. bekommen Sie mit einem kostenlosen Newsletter von **Watchlist Internet** jeden Freitag eine E-Mail mit den neuesten Betrugsfällen. Es gibt zusätzlich eine entsprechende Smartphone-App, mit der Sie über neue Warnmeldungen sofort benachrichtigt werden.

Auch die Wirtschaftskammer Österreich bietet eine Übersicht aktueller Betrugswarnungen.

- Watchlist Internet – Online-Betrug, -Fallen & -Fakes im Blick (watchlist-internet.at)[67]
- Aktuelle Betrugswarnungen - WKO.at[68]
- So bleiben Sie mit der Watchlist Internet am Laufenden! - Watchlist Internet (watchlist-internet.at)[69]

[66] https://www.watchlist-internet.at/news/die-wichtigsten-einstellungen-fuer-ein-sicheres-smartphone/
[67] https://www.watchlist-internet.at/
[68] https://www.wko.at/warnungen/aktuelle-betrugsversuche
[69] https://www.watchlist-internet.at/news/so-bleiben-sie-mit-der-watchlist-internet-am-laufenden/?sword_list%5B0%5D=Android&no_cache=1

12.2 INDUCE Umfrage 2022

induce

Umfrage zu Planspielen

Diese Online-Umfrage ist Teil des Projektes „INDUCE“ (https://induce.ait.ac.at). Das Projekt INDUCE untersucht den Einsatz von Planspielen für verschiedene Personengruppen.

Die Umfrage richtet sich an alle Personen ohne oder mit Vorerfahrung zu Planspielen.

Die Ziele der Umfrage sind das Wissen über Planspiele und den Einsatz und den Mehrwert von Planspielen für Personen zu untersuchen und interessante Situationen in Planspielen auszuwerten.

Die Beantwortung des gesamten Fragebogens dauert etwa 6 Minuten. Die Beantwortung der Fragen ist freiwillig und die Umfrage kann jederzeit unterbrochen werden. Die erhobenen Daten werden lediglich für die Zeit der Umfrage und dessen Auswertung gespeichert und danach gelöscht (spätestens mit Projektende im April 2024). Die Umfrage ist von 01.02.2022 – 28.02.2022 geöffnet.

Für weitere Fragen zur Umfrage und dem Projekt können Sie sich an Dr. Maria Leitner (maria.leitner@ait.ac.at) wenden.

1

induce

Umfrage zu Planspielen

1. Welches Geschlecht haben Sie?

- ◯ Weiblich
- ◯ Männlich
- ◯ Divers
- ◯ Anderes
- ◯ Keine Angabe

2. Wie alt sind Sie?

- ◯ Unter 18
- ◯ 18 bis 24
- ◯ 25 bis 34
- ◯ 35 bis 44
- ◯ 45 bis 60
- ◯ über 60

3. Sind Sie berufstätig und / oder studieren Sie?

- ◯ ich studiere
- ◯ ich bin berufstätig bzw. arbeitssuchend
- ◯ beides

2

induce

Umfrage zu Planspielen

4. Welchem Bereich (bzw. welchen Bereichen) würden Sie Ihr Studium primär zuordnen?

- ○ Geisteswissenschaften
- ○ Lebenswissenschaften
- ○ MINT (Mathematik, Informatik, Naturwissenschaft und Technik)
- ○ Sozial- und Verhaltenswissenschaften
- ○ Wirtschaftswissenschaften
- ○ Sonstiges (bitte angeben)

3

induce

Umfrage zu Planspielen

5. In welcher Branche (bzw. welchen Branchen) ist Ihre aktuelle oder vormalige Organisation tätig? (Mehrfachantworten sind möglich.)

- ☐ Bau
- ☐ Beherbergung und Gastronomie
- ☐ Bildung
- ☐ Finanz- und Versicherungsleistungen
- ☐ Gesundheits- und Sozialwesen
- ☐ Handel
- ☐ Herstellung von Waren
- ☐ Information und Kommunikation
- ☐ Land- und Forstwirtschaft
- ☐ Öffentliche Verwaltung, Verteidigung, Sozialversicherung
- ☐ Verkehr und Logistik
- ☐ Sonstige freiberufliche, technische, wirtschaftliche, wissenschaftliche Dienstleistungen
- ☐ Sonstiges (bitte angeben)

6. Welchem Aufgabenbereich würden Sie Ihre aktuelle oder vormalige Arbeit primär zuschreiben? (Mehrfachantworten sind möglich.)

- ☐ Beschaffung
- ☐ Bildung
- ☐ Finanzierung
- ☐ Forschung und Entwicklung
- ☐ Information und Informationsverarbeitung
- ☐ Logistik
- ☐ Personalwesen
- ☐ Pflege und Betreuung
- ☐ Produktion
- ☐ Unternehmensleitung
- ☐ Vertrieb
- ☐ Verwaltung
- ☐ Sonstiges (bitte angeben)

4

induce

Umfrage zu Planspielen

7. Welchem Bereich (bzw. welchen Bereichen) würden Sie Ihr Studium primär zuordnen?

- ○ Geisteswissenschaften
- ○ Lebenswissenschaften
- ○ MINT (Mathematik, Informatik, Naturwissenschaft und Technik)
- ○ Sozial- und Verhaltenswissenschaften
- ○ Wirtschaftswissenschaften
- ○ Sonstiges (bitte angeben)

8. In welcher Branche (bzw. welchen Branchen) ist Ihre aktuelle oder vormalige Organisation tätig? (Mehrfachantworten sind möglich.)

- ☐ Bau
- ☐ Beherbergung und Gastronomie
- ☐ Bildung
- ☐ Finanz- und Versicherungsleistungen
- ☐ Gesundheits- und Sozialwesen
- ☐ Handel
- ☐ Herstellung von Waren
- ☐ Information und Kommunikation
- ☐ Land- und Forstwirtschaft
- ☐ Öffentliche Verwaltung, Verteidigung, Sozialversicherung
- ☐ Verkehr und Logistik
- ☐ Sonstige freiberufliche, technische, wirtschaftliche, wissenschaftliche Dienstleistungen
- ☐ Sonstiges (bitte angeben)

9. Welchem Aufgabenbereich würden Sie Ihre aktuelle oder vormalige Arbeit primär zuschreiben? (Mehrfachantworten sind möglich.)

- ☐ Beschaffung
- ☐ Bildung
- ☐ Finanzierung
- ☐ Forschung und Entwicklung
- ☐ Information und Informationsverarbeitung
- ☐ Logistik
- ☐ Personalwesen
- ☐ Pflege und Betreuung
- ☐ Produktion
- ☐ Unternehmensleitung
- ☐ Vertrieb
- ☐ Verwaltung
- ☐ Sonstiges (bitte angeben)

5

induce

Umfrage zu Planspielen

10. Haben Sie schon einmal von Planspielen oder Cyber Übungen gehört?

- ○ ja, ich habe an einem oder mehreren teilgenommen
- ○ ja, ich habe davon gehört
- ○ nein, ich habe noch nie davon gehört oder daran teilgenommen

Was ist ein Planspiel?

In einem Planspiel nehmen Teilnehmende verschiedene Rollen ein und lösen gemeinsam eine Aufgabe. Beispiele sind:

- Ein Blackout tritt ein und Krisenmanager*innen müssen darauf reagieren.
- Ein Computer wird von einem Virus befallen und das Problem muss von den Teilnehmenden gelöst werden.

7

induce

Umfrage zu Planspielen

11. In welchem Bereich werden Planspiele ihrer Meinung nach typischerweise eingesetzt? (Mehrfachantworten sind möglich.)

- [ ] Bildung
- [ ] Politik
- [ ] Recht
- [ ] Sicherheit
- [ ] Technik
- [ ] Umwelt
- [ ] Wirtschaft
- [ ] Sonstiges (bitte angeben)

12. Welchen Mehrwert könnten Planspiele Ihrer Meinung nach haben? (Mehrfachantworten sind möglich.)

- [ ] Fähigkeiten überprüfen
- [ ] Komplexe Entscheidungen treffen
- [ ] Neue Situationen erleben
- [ ] Neues lernen
- [ ] Problemlösungskompetenz stärken
- [ ] Spaß haben
- [ ] Spielerisch Wissen aufbauen
- [ ] Zusammengehörigkeitsgefühl stärken
- [ ] Sonstiges (bitte angeben)

8

induce

Umfrage zu Planspielen

13. Planspiele werden vermehrt zur Vermittlung der Themen Sicherheit und Datenschutz genutzt. Welche der folgenden Situationen wären für Sie in einem Planspiel interessant?

	gar nicht interessant	weniger interessant	neutral	interessant	sehr interessant
Ich habe den Anhang einer E-Mail von einer mir unbekannten Person geöffnet.	○	○	○	○	○
Mein digitales Gerät (z.B. Laptop oder Handy) wird verschlüsselt und ich habe keinen Zugriff auf meine Daten.	○	○	○	○	○
Beim Online Shopping werden meine Bankdaten gestohlen und unerlaubterweise genutzt.	○	○	○	○	○
Mein Profil in den sozialen Medien wird unerlaubt von einer anderen Person genutzt.	○	○	○	○	○
Mein digitales Gerät wird durch ein unbekanntes Programm gestört.	○	○	○	○	○
Meine Fotos (oder andere Daten) sind unerlaubt im Internet aufgetaucht.	○	○	○	○	○
Mit meinen Teammitgliedern treffen wir komplexe Entscheidungen.	○	○	○	○	○
Meine Geräte gegen Hacker*innen verteidigen.	○	○	○	○	○
Eine Krisensituation üben/durchspielen in meiner Organisation.	○	○	○	○	○

Sonstiges (bitte angeben)

9

induce

Umfrage zu Planspielen

14. Welches dieser Ereignisse würde Sie persönlich am stärksten betreffen? Bitte reihen Sie die Ereignisse von 1 (größter Schaden) bis 6 (geringster Schaden).

Sie verlieren 1000 Euro.

Ihr Ruf wird durch Unwahrheiten im Internet geschädigt.

Ihr Gerät (z.B. Laptop, Handy) wird gestohlen.

Sie haben keinen Zugriff auf Ihre persönlichen Daten (z.B. private Fotos, Passwörter).

Sie haben eine Woche keinen Internetzugriff.

Sie haben eine Woche keinen Zugriff auf Ihre persönlichen Konten (z.B. Bank, Social-Media).

10

induce

Umfrage zu Planspielen

15. Haben Sie Interesse an weiteren Informationen?

- ☐ Ja, ich würde gern an einem Interview für das Projekt INDUCE teilnehmen.
- ☐ Ja, ich würde gern an einem Planspiel im Projekt INDUCE teilnehmen.
- ☐ Ja, senden Sie mir die Ergebnisse der Umfrage zu.
- ☐ Nein danke.

E-Mail-Adresse (optional)

16. Was möchten Sie uns sonst noch mitteilen?

11

induce

Umfrage zu Planspielen

Vielen Dank, dass Sie sich die Zeit genommen haben, um an dieser Umfrage teilzunehmen.

Mehr Informationen zum Projekt finden Sie auf https://induce.ait.ac.at
Für weitere Fragen zur Umfrage oder zum Projekt können Sie sich an Dr. Maria Leitner (maria.leitner@ait.ac.at) wenden.

12

12.3 Ergebnisse Umfrage Cybersecurity Tipps

Cybersecurity-Tipps: Selbsttest

LimeSurvey

WKW Umfragen
Cybersecurity-Tipps: Selbsttest

Ergebnisse

Umfrage 963925

Anzahl der Datensätze in dieser Abfrage:	55
Gesamtzahl der Datensätze dieser Umfrage:	55
Anteil in Prozent:	100.00%

LimeSurvey

WKW Umfragen
Cybersecurity-Tipps: Selbsttest

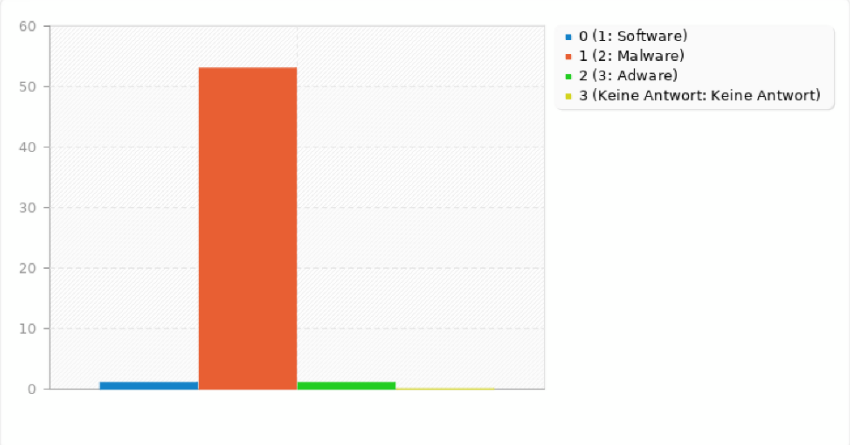
Zusammenfassung für a1

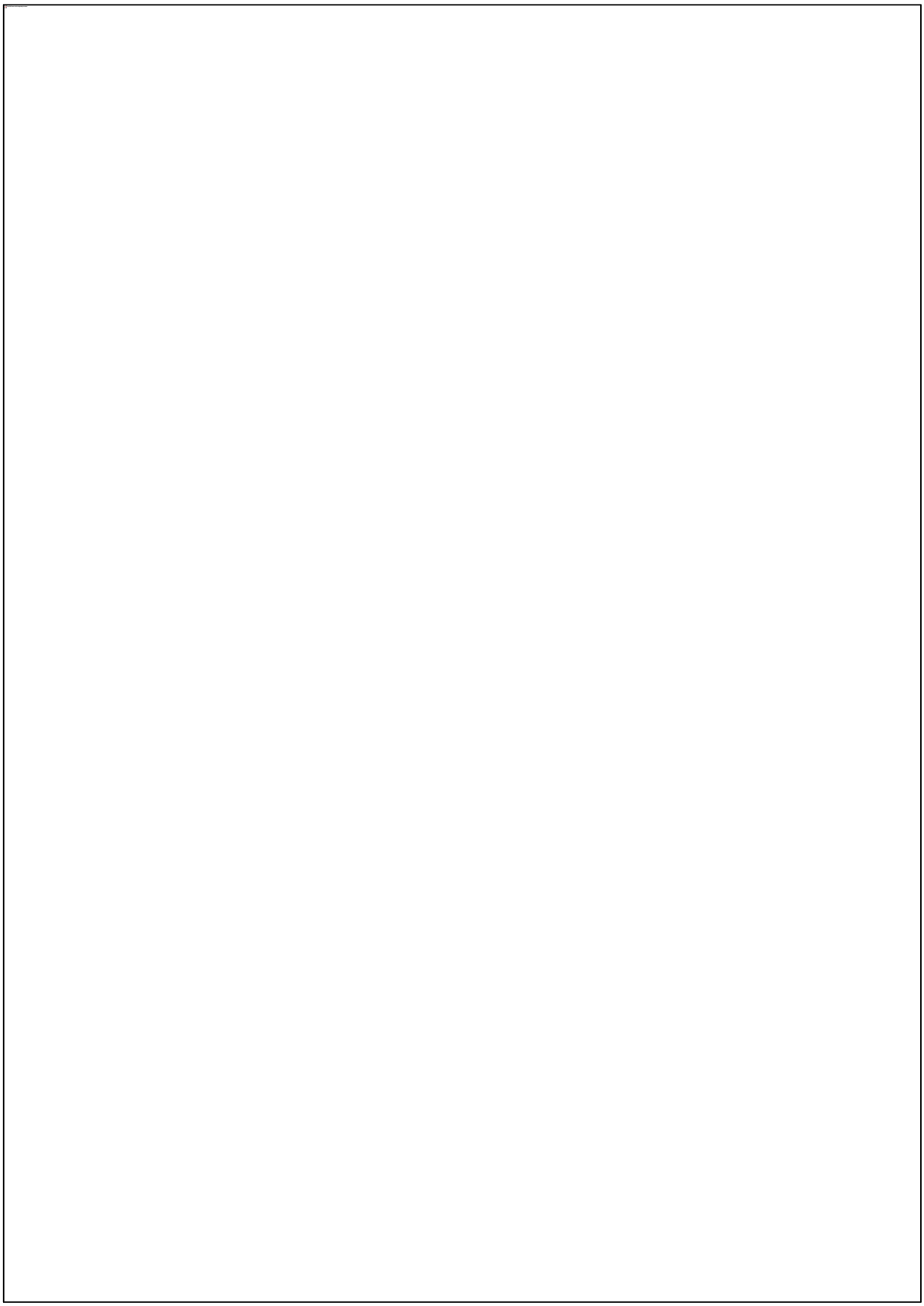
Ein anderes Wort für ein bösartiges Schadprogramm ist:

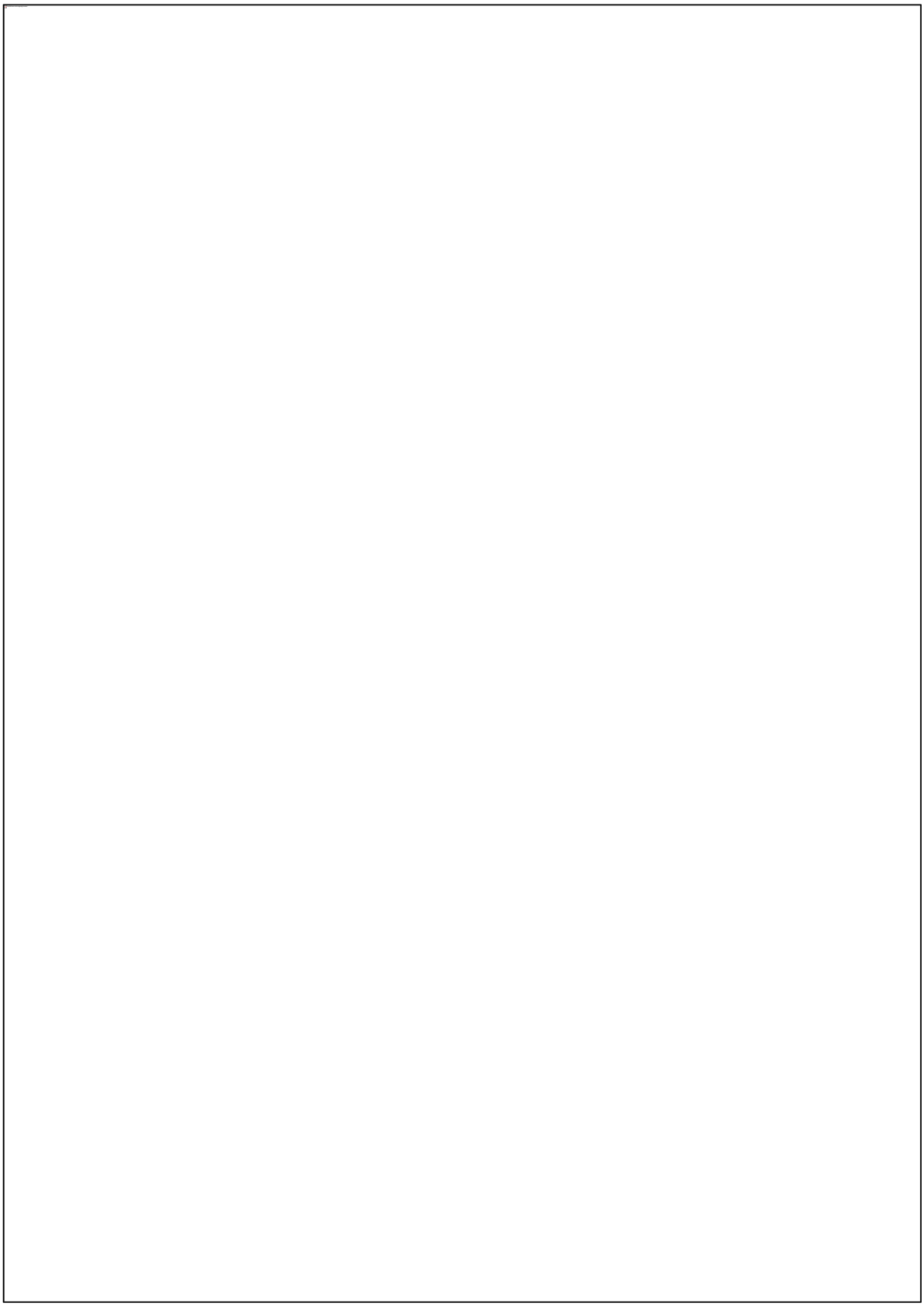
Antwort	Anzahl	Prozent
Software (1)	1	1.82%
Malware (2)	53	96.36%
Adware (3)	1	1.82%
Keine Antwort	0	0.00%

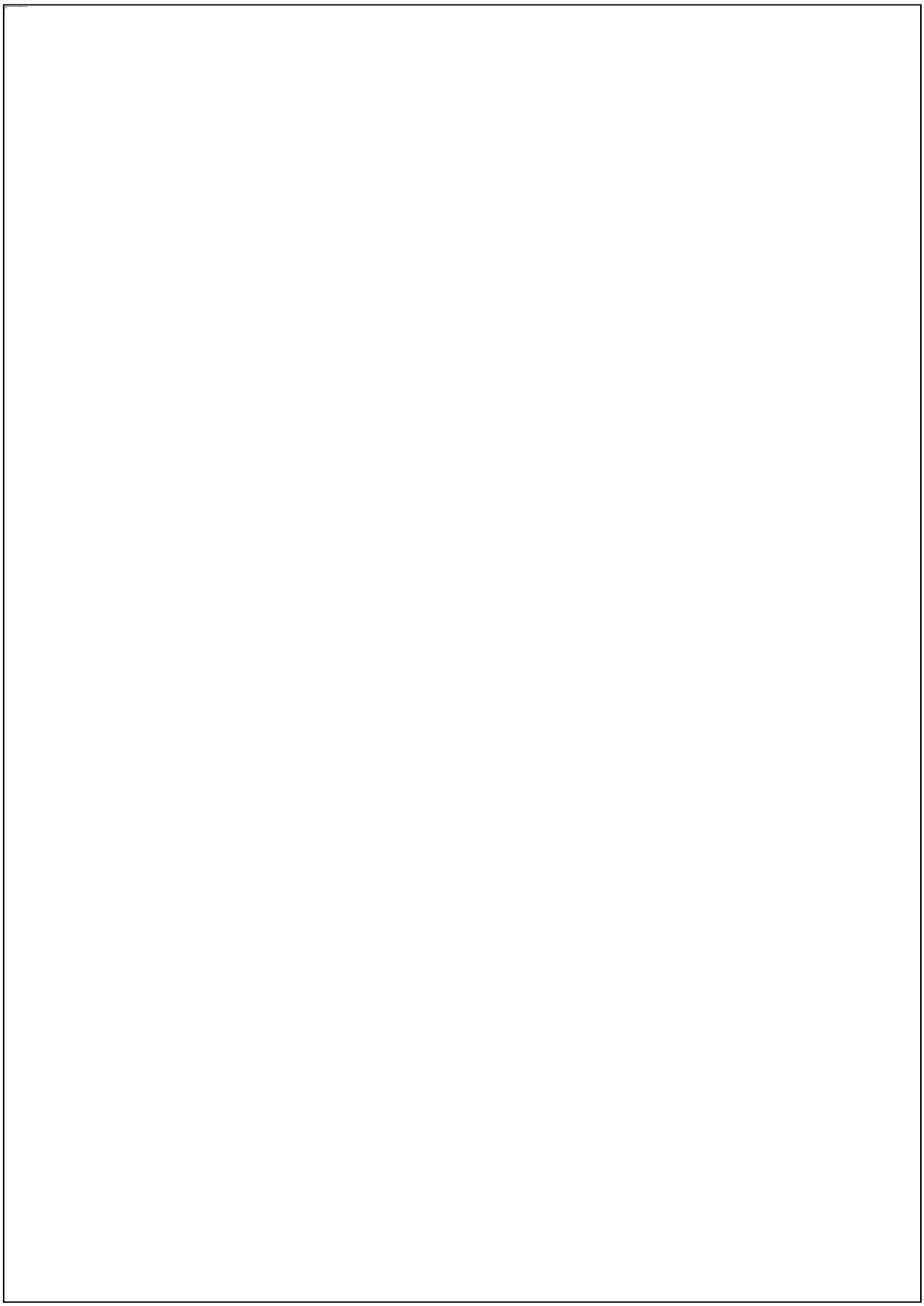
Zusammenfassung für a1

Ein anderes Wort für ein bösartiges Schadprogramm ist:









LimeSurvey

WKW Umfragen
Cybersecurity-Tipps: Selbsttest

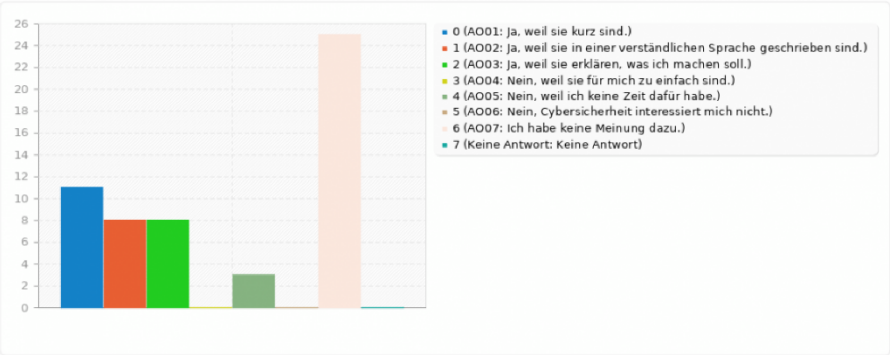
Zusammenfassung für b2

Gefallen Ihnen die „Cybersecurity-Tipps“? Welche Antwort trifft auf Sie am meisten zu?

Antwort	Anzahl	Prozent
Ja, weil sie kurz sind. (AO01)	11	20.00%
Ja, weil sie in einer verständlichen Sprache geschrieben sind. (AO02)	8	14.55%
Ja, weil sie erklären, was ich machen soll. (AO03)	8	14.55%
Nein, weil sie für mich zu einfach sind. (AO04)	0	0.00%
Nein, weil ich keine Zeit dafür habe. (AO05)	3	5.45%
Nein, Cybersicherheit interessiert mich nicht. (AO06)	0	0.00%
Ich habe keine Meinung dazu. (AO07)	25	45.45%
Keine Antwort	0	0.00%

Zusammenfassung für b2

Gefallen Ihnen die „Cybersecurity-Tipps“? Welche Antwort trifft auf Sie am meisten zu?



LimeSurvey

WKW Umfragen
Cybersecurity-Tipps: Selbsttest

Zusammenfassung für b3

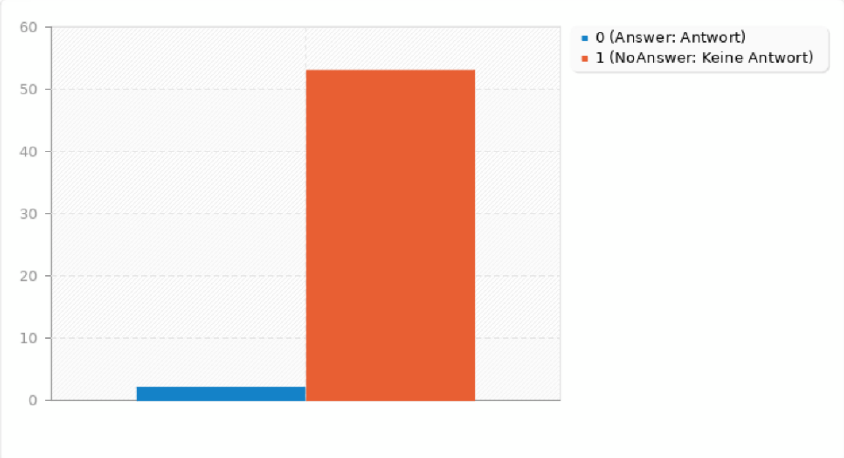
Haben Sie noch weitere Kommentare oder Überlegungen zu den „Cybersecurity-Tipps“?

Antwort	Anzahl	Prozent
Antwort	2	3.64%
Keine Antwort	53	96.36%

ID	Antwort
53	danke
105	Nein, alles gut für mich

Zusammenfassung für b3

Haben Sie noch weitere Kommentare oder Überlegungen zu den „Cybersecurity-Tipps“?



Seite 9 / 9

12.4 Persönlichkeitsbereiche & Dimension

	Modelle	wer	Dimension
001	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Zuversicht
002	Freiburger Persönlichkeits Inventar (FPI)		Lebenszufriedenheit
003	Freiburger Persönlichkeits Inventar (FPI)		Lebenszufriedenheit
004	Selbstwertgefühl	Birkenbihl	Erfolg aus Arbeit
005	Selbstwertgefühl	Birkenbihl	Wertschätzung
006	SCARF Modell	Rock David	Status, Wichtigkeit und Selbstverständnis
007	Resilienz im höhren Lebensalter	Wagnild und Young	Unabhängigkeit
008	SCARF Modell	Rock David	Autonomie
009	Resilienz im höhren Lebensalter	Wagnild und Young	Gleichmut (Gelassenheit)
010	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Privatheit
011	SCARF Modell	Rock David	Sicherheit, Vorhersagen, Widerholungen, Authentizität
012	Insights MDI Leadership-Check		Ästhetisches Motiv: Streben nach Selbsterfüllung und Harmonie
013	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Zielbezug der Kommunikation
014	Resilienz im höhren Lebensalter	Wagnild und Young	Neugierde
015	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Besorgtheit
016	Big Five Persönlichkeitstest		Neurotizismus
017	NEOFFI - Neo Fünf Faktoren Inventar		Neurotizismus: Neigung zu Ängstlichkeit, Grübel und Zweifel. Innere Unruhe und Gefühl der Leere.
018	Freiburger Persönlichkeits Inventar (FPI)		Neurotizismus
019	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Anspannung (Angespanntheit)
020	Freiburger Persönlichkeits Inventar (FPI)		Beanspruchung
021	Resilienz im höhren Lebensalter	Wagnild und Young	Zugang zu medizinischer Versorgung
022	Freiburger Persönlichkeits Inventar (FPI)		Körperliche Beschwerden
023	Freiburger Persönlichkeits Inventar (FPI)		Körperliche Beschwerden
024	Freiburger Persönlichkeits Inventar (FPI)		Gesundheitssorgen
025	Freiburger Persönlichkeits Inventar (FPI)		Gesundheitssorgen
026	Kritikkompetenz	Bruce	Humor
027	Kritikkompetenz	Bruce	Humor
028	Kritikkompetenz	Bruce	Humor
029	Emotionale Intelligenz	Goleman	Bindungsfähigkeit
030	Resilienz im höhren Lebensalter	Wagnild und Young	soziale Kompetenz
031	Resilienz im höhren Lebensalter	Wagnild und Young	soziale Aktivität

	Modelle	wer	Dimension
032	Teamfähigkeit	Anja Seelheim, Erich Witte	Interaktionsfähigkeit
033	Teamfähigkeit	Anja Seelheim, Erich Witte	Kontaktfähigkeit
034	Soziale Kernkompetenzen	Crisand	Kontaktfähigkeit
035	Soziale Kernkompetenzen	Crisand	Teamfähigkeit
036	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Netzwerkfähigkeit
037	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	soziale Kompetenz (z. B. Kontaktfreude)
038	NEOFFI - Neo Fünf Faktoren Inventar		Soziale Verträglichkeit: Mitfühlend, Helfer, beliebt, nicht aggressiv.
039	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Kontaktfähigkeit
040	Teamfähigkeit	Anja Seelheim, Erich Witte	Integrationsfähigkeit
041	Soziale Kernkompetenzen	Crisand	Kritikfähigkeit
042	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Sozialibilität (Fähigkeit sich sozial einzufügen oder Sozialität auszunutzen)
043	Emotionale Intelligenz	Goleman	Teamfähigkeit
044	SCARF Modell	Rock David	Beziehung, Kontakt, Vertrauen, Zugehörigkeit
045	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Interesse an anderen Personen
046	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Interesse an anderen Personen
047	Fünf-Faktoren-Modell der Persönlichkeit	Big Five	Verträglichkeit
048	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Wärme (z. B. Wohlfühlen in Gesellschaft)
049	Freiburger Persönlichkeits Inventar (FPI)		Soziale Orientierung
050	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Teamorientierung
051	Resilienz im höheren Lebensalter	Wagnild und Young	Bedeutsamkeit und existentielle Einzigartigkeit jedes Lebens
052	Kritikkompetenz	Bruce	Akzeptanz
053	Big Five Persönlichkeitstest		Verträglichkeit
054	Insights MDI Leadership-Check		Soziales Motiv: Streben nach Altruismus und Hilfsbereitschaft
055	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Entscheidungsfähigkeit
056	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Konzeptionelle Fähigkeit
057	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	logisches Schlussfolgern (können)
058	Hermann-Dominanz-Inventar (H.D.I.)		Der Analytiker: analytisch, ruhig, ernsthaft, konzentriert
059	Soziale Kernkompetenzen	Crisand	Koordinationsfähigkeit
060	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Organisationstalent

	Modelle	wer	Dimension
061	Flow-Konzept	Csikszentmihalyi	Konzentration
062	Konzentrationstest d2		Schnelligkeit
063	Management-Potential-Kurztest (MPT-K)		unternehmerisches Denken
064	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Wachsamkeit (z. B. Misstrauen)
065	Flow-Konzept	Csikszentmihalyi	Zielorientierung
066	Konzentrationstest d2		Stetigkeit
067	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Konzeptionelle Fähigkeit anwenden (konzeptionelles Denken)
068	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	logisches Schlussfolgern (handeln)
069	Hermann-Dominanz-Inventar (H.D.I.)		Der Analytiker: analytisch, ruhig, ernsthaft, konzentriert
070	Management-Potential-Kurztest (MPT-K)		unternehmerisches Denken
071	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Wachsamkeit (z. B. Misstrauen)
072	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Wachsamkeit (z. B. Misstrauen)
073	Flow-Konzept	Csikszentmihalyi	Zielorientierung
074	Flow-Konzept	Csikszentmihalyi	Zielorientierung
075	Flow-Konzept	Csikszentmihalyi	Zielorientierung
076	DISG Profil		stetig
077	Insights MDI Leadership-Check		stetig
078	Insights MDI Leadership-Check		Theoretisches Motiv: Inneres Streben nach Bildung und Wissen
079	Emotionale Intelligenz	Goleman	Selbstregulierung
080	Emotionale Intelligenz	Goleman	Selbstkontrolle
081	Emotionale Kompetenz	Stamoulis	Regulation von Emotionen
082	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Selbstführung
083	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Selbstmanagement
084	Kritikkompetenz	Bruce	Selbstüberwachung
085	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Gratifikationsaufschub
086	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Selbstgenügsamkeit
087	Selbstwertgefühl	Birkenbihl	angepasste Aggressivität
088	Selbstwertgefühl	Birkenbihl	angepasste Aggressivität
089	Freiburger Persönlichkeits Inventar (FPI)		Erregbarkeit
090	Freiburger Persönlichkeits Inventar (FPI)		Aggressivität
091	Freiburger Persönlichkeits Inventar (FPI)		Aggressivität
092	Kritikkompetenz	Bruce	Reaktanz (Widerstand)
093	Resilienz im höhren Lebensalter	Wagnild und Young	Beharrlichkeit
094	Emotionale Intelligenz	Goleman	Bindungsfähigkeit

	Modelle	wer	Dimension
095	Hermann-Dominanz-Inventar (H.D.I.)		Der sicherheitsbedürftige Organisator: kontrolliert, dominant, organisiert
096	Freiburger Persönlichkeits Inventar (FPI)		Gehemmtheit
097	Resilienz im höhren Lebensalter	Wagnild und Young	Neugierde
098	Resilienz im höhren Lebensalter	Wagnild und Young	Neugierde
099	Insights MDI Leadership-Check		Traditionelles Motiv: Streben nach festen Werten und Zugehörigkeit
100	Resilienz im höheren Lebensalter	Wagnild und Young	Kontrolle über das Umfeld
101	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Überzeugungskraft
102	Soziale Kernkompetenzen	Crisand	Durchsetzungsfähigkeit
103	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Durchsetzungsvermögen
104	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Entscheidungsfähigkeit
105	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Durchsetzungsstärke
106	Management-Potential-Kurztest (MPT-K)		Durchsetzungsvermögen
107	Management-Potential-Kurztest (MPT-K)		Team-Führung
108	Resilienz im höheren Lebensalter	Wagnild und Young	Kontrolle über das Umfeld
109	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Dominanz
110	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Führungsmotivation
111	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Durchsetzungsstärke
112	DISG Profil		dominant
113	Insights MDI Leadership-Check		dominant
114	Management-Potential-Kurztest (MPT-K)		Team-Führung
115	Resilienz im höheren Lebensalter	Wagnild und Young	Kontrolle über das Umfeld
116	Hermann-Dominanz-Inventar (H.D.I.)		Der sicherheitsbedürftige Organisator: kontrolliert, dominant, organisiert
117	Insights MDI Leadership-Check		Individualistisches Motiv: Streben nach Anerkennung und persönlichem Vorteil
118	Kritikkompetenz	Bruce	Kooperationsbereitschaft
119	Teamfähigkeit	Anja Seelheim, Erich Witte	Kooperationsfähigkeit
120	Teamfähigkeit	Anja Seelheim, Erich Witte	Konsensfähigkeit
121	Soziale Kernkompetenzen	Crisand	Kooperationsfähigkeit
122	Soziale Kernkompetenzen	Crisand	Kompromissfähigkeit
123	Kritikkompetenz	Bruce	Perspektivenübernahme

	Modelle	wer	Dimension
124	Kritikkompetenz	Bruce	Perspektivenübernahme
125	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Ambiguitätstoleranz (andere Benennung/Perspektive zulassen)
126	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Ambiguitätstoleranz (andere Benennung/Perspektive zulassen)
127	Kritikkompetenz	Bruce	Konfliktbereitschaft
128	Emotionale Intelligenz	Goleman	Konfliktfähigkeit
129	Teamfähigkeit	Anja Seelheim, Erich Witte	Konfliktfähigkeit
130	Soziale Kernkompetenzen	Crisand	Konfliktfähigkeit
131	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Konfliktlösungsfähigkeit
132	Kritikkompetenz	Bruce	Veränderungsbereitschaft
133	Emotionale Intelligenz	Goleman	Anpassungsfähigkeit
134	Resilienz im höhren Lebensalter	Wagnild und Young	Flexibilität
135	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Flexibilität
136	Soziale Kernkompetenzen	Crisand	Rollenflexibilität
137	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Flexibilität
138	Resilienz im höhren Lebensalter	Wagnild und Young	Ressourcenvielfalt
139	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Offenheit für Veränderungen
140	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Problemlösungsfähigkeit
141	Resilienz im höhren Lebensalter	Wagnild und Young	Anpassungsfähigkeit
142	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Perspektivenwechsel
143	Soziale Kernkompetenzen	Crisand	Interpersonelle Flexibilität
144	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Interpretation von Signalen
145	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Interpretation von Signalen
146	Teamfähigkeit	Anja Seelheim, Erich Witte	Kommunikationsfähigkeit
147	Soziale Kernkompetenzen	Crisand	Kommunikationsfähigkeit
148	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Überzeugungsfähigkeit
149	Flow-Konzept	Csikszentmihalyi	kontinuierliches und unmittelbares Feedback
150	Emotionale Intelligenz	Goleman	Kommunikationsfähigkeit
151	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Vermittlung von Authentizität
152	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Zielbezug der Kommunikation

	Modelle	wer	Dimension
153	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Beherrschung von Kommunikationsregeln
154	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Sachliche Argumentationsfähigkeit
155	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Befriedigung aus der Kommunikation
156	Emotionale Intelligenz	Goleman	Motivation
157	Emotionale Intelligenz	Goleman	Engagement
158	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Einsatzbereitschaft
159	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Gestaltungsmotivation
160	Insights MDI Leadership-Check		Ökonomisches Motiv: Streben nach Gewinn und Nutzenorientierung
161	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Antriebsstärke
162	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Leistungsmotivation
163	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Leistungsmotivation
164	Freiburger Persönlichkeits Inventar (FPI)		Leistungsorientierung
165	Emotionale Intelligenz	Goleman	Leistungsdrang
166	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Perfektionismus
167	Emotionale Intelligenz	Goleman	Empathie
168	Emotionale Kompetenz	Stamoulis	Sensitivität für die Emotionen anderer
169	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Einfühlung
170	Soziale Kernkompetenzen	Crisand	Empathie
171	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Empfindsamkeit
172	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Sensitivität
173	Hermann-Dominanz-Inventar (H.D.I.)		Der Emotionale: zwischenmenschlich, einfühlsam, gesprächig
174	Hermann-Dominanz-Inventar (H.D.I.)		Der Emotionale: zwischenmenschlich, einfühlsam, gesprächig
175	Hermann-Dominanz-Inventar (H.D.I.)		Der Emotionale: zwischenmenschlich, einfühlsam, gesprächig
176	Kritikkompetenz	Bruce	Selbstwert
177	Emotionale Intelligenz	Goleman	Selbstvertrauen
178	Resilienz im höhren Lebensalter	Wagnild und Young	Selbstvertrauen
179	Flow-Konzept	Csikszentmihalyi	Selbstwirksamkeit
180	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Selbstwirksamkeit

	Modelle	wer	Dimension
181	Emotionale Intelligenz	Goleman	Optimismus
182	Resilienz im höhren Lebensalter	Wagnild und Young	Einstellung, dass das Leben einen Sinn hat
183	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Abgehobenheit (z. B. mangelnde Realitätsnähe)
184	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Abgehobenheit (z. B. mangelnde Realitätsnähe)
185	Emotionale Intelligenz	Goleman	Gewissenhaftigkeit
186	Fünf-Faktoren-Modell der Persönlichkeit	Big Five	Gewissenhaftigkeit
187	Big Five Persönlichkeitstest		Gewissenhaftigkeit
188	NEOFFI - Neo Fünf Faktoren Inventar		Gewissenhaftigkeit: Pflichtbewusst, genau, ordentlich.
189	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Gewissenhaftigkeit
190	DISG Profil		gewissenhaft
191	Insights MDI Leadership-Check		gewissenhaft
192	Konzentrationstest d2		Genauigkeit
193	Emotionale Intelligenz	Goleman	Selbstwahrnehmung (Selbstreflexion)
194	Emotionale Intelligenz	Goleman	Selbsteinschätzung
195	Soziale Kernkompetenzen	Crisand	Selbstreflexion
196	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Selbstbewusstsein
197	Selbstwertgefühl	Birkenbihl	optimales Verhältnis zwischen REAL-ICH und IDEAL-ICH
198	Selbstwertgefühl	Birkenbihl	optimales Verhältnis zwischen REAL-ICH und IDEAL-ICH
199	Flow-Konzept	Csikszentmihalyi	Herausforderung muss mit Fähigkeiten bewältigt werden können
200	Emotionale Kompetenz	Stamoulis	Sensitivität für die eigenen Emotionen
201	Emotionale Intelligenz	Goleman	emotionales Bewusstsein
202	Fünf-Faktoren-Modell der Persönlichkeit	Big Five	Emotionale Stabilität
203	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	emotionale Stabilität
204	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Emotionale Stabilität
205	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Belastbarkeit
206	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Belastbarkeit
207	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Belastbarkeit
208	Resilienz im höhren Lebensalter	Wagnild und Young	psychische Robustheit
209	Emotionale Intelligenz	Goleman	Offenheit für Innovationen
210	Fünf-Faktoren-Modell der Persönlichkeit	Big Five	Offenheit für neue Erfahrungen
211	Big Five Persönlichkeitstest		Offenheit für Erfahrungen
212	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Offenheit für Veränderungen

	Modelle	wer	Dimension
213	NEOFFI - Neo Fünf Faktoren Inventar		Offenheit für Erfahrungen: Offen für Neues, neugierig, Forscher.
214	Freiburger Persönlichkeits Inventar (FPI)		Offenheit
215	Emotionale Intelligenz	Goleman	Vertrauenswürdigkeit
216	Emotionale Intelligenz	Goleman	Initiative
217	Leadership-Kompetenz in Krisensituationen	Anita Zehrer, Claudia Mössenlechner	Initiative
218	DISG Profil		initiativ/überzeugend
219	Insights MDI Leadership-Check		initiativ/überzeugend
220	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Handlungsorientierung (Orientierung zur Ganzheitlichkeit)
221	Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)		Handlungsorientierung (Orientierung zur Ganzheitlichkeit)
222	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Lebhaftigkeit
223	SCARF Modell	Rock David	Gerechtigkeit geben und empfangen
224	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Gerechtigkeitssinn
225	Selbstwertgefühl	Birkenbihl	Übereinstimmung mit dem Gewissen
226	Selbstwertgefühl	Birkenbihl	Übereinstimmung mit dem Gewissen
227	16-Persönlichkeitsfaktoren-Test	Raymond B. Cattell	Regelbewusstsein (z. B. Moral)
228	Fünf-Faktoren-Modell der Persönlichkeit	Big Five	Extraversion
229	Big Five Persönlichkeitstest		Extraversion
230	NEOFFI - Neo Fünf Faktoren Inventar		Extraversion: Streben nach Geselligkeit und Abenteuern, kontaktfreudig, aus sich heraus gehend.
231	Freiburger Persönlichkeits Inventar (FPI)		Extraversion
232	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Vorstellungskraft
233	Kooperationsfähigkeit	Albert Martin und Jeannette Purwin	Kreativität
234	Hermann-Dominanz-Inventar (H.D.I.)		Der Visionär: strategisch, experimentierfreudig, keativ
235	Selbstwertgefühl	Birkenbihl	erotisch-sexuelle Befriedigung
236	Selbstwertgefühl	Birkenbihl	erotisch-sexuelle Befriedigung

12.5 Persönlichkeitsbereiche & Zuordnung

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
001	Haltung	Selbstorientierung	Kompetenz	innerer Vorgang
002	Haltung	Selbstorientierung	Kompetenz	Interaktion
003	Fähigkeit	Selbstorientierung	Kompetenz	innerer Vorgang
004	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
005	Haltung	Selbstorientierung	Kompetenz	Interaktion
006	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
007	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
008	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
009	Eigenschaft	Selbstorientierung	Kompetenz	innerer Vorgang
010	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
011	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
012	Bedürfnis	Selbstorientierung	innerer Vorgang	Kompetenz
013	Bedürfnis	Kommunikationsfähigkeit	Interaktion	innerer Vorgang
014	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
015	Haltung	Selbstorientierung	Kompetenz	Interaktion
016	Eigenschaft	Selbstorientierung	Kompetenz	innerer Vorgang
017	Haltung	Selbstorientierung	Kompetenz	Interaktion
018	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
019	Eigenschaft	Selbstorientierung	innerer Vorgang	innerer Vorgang
020	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
021	Bedürfnis	Selbstorientierung	innerer Vorgang	innerer Vorgang
022	Bedürfnis	Selbstorientierung	innerer Vorgang	innerer Vorgang
023	Haltung	Selbstorientierung	Kompetenz	Interaktion
024	Bedürfnis	Selbstorientierung	innerer Vorgang	innerer Vorgang
025	Haltung	Selbstorientierung	Kompetenz	Interaktion
026	Eigenschaft	Selbstorientierung	innerer Vorgang	Interaktion
027	Fähigkeit	Selbstorientierung	Kompetenz	Interaktion
028	Bedürfnis	Selbstorientierung	innerer Vorgang	Interaktion
029	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
030	Fähigkeit	Sozialorientierung	Interaktion	Kompetenz
031	Eigenschaft	Sozialorientierung	Interaktion	innerer Vorgang
032	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
033	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
034	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
035	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
036	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
037	Fähigkeit	Sozialorientierung	Interaktion	Kompetenz
038	Eigenschaft	Sozialorientierung	innerer Vorgang	Interaktion
039	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
040	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
041	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
042	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
043	Fähigkeit	Sozialorientierung	Kompetenz	Interaktion
044	Bedürfnis	Sozialorientierung	Interaktion	innerer Vorgang
045	Eigenschaft	Sozialorientierung	innerer Vorgang	Interaktion
046	Bedürfnis	Sozialorientierung	innerer Vorgang	Interaktion
047	Eigenschaft	Sozialorientierung	Kompetenz	Interaktion
048	Bedürfnis	Sozialorientierung	innerer Vorgang	Interaktion
049	Bedürfnis	Sozialorientierung	innerer Vorgang	Interaktion
050	Bedürfnis	Sozialorientierung	innerer Vorgang	Interaktion
051	Haltung	Sozialorientierung	Kompetenz	Interaktion
052	Haltung	Sozialorientierung	Interaktion	innerer Vorgang
053	Eigenschaft	Sozialorientierung	Kompetenz	Interaktion
054	Bedürfnis	Sozialorientierung	Interaktion	innerer Vorgang
055	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
056	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
057	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
058	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
059	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
060	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
061	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
062	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
063	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
064	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
065	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
066	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	Kompetenz
067	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
068	Fähigkeit	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
069	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
070	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
071	Bedürfnis	Kognitive Fähigkeiten	Interaktion	Interaktion
072	Bedürfnis	Kognitive Fähigkeiten	innerer Vorgang	innerer Vorgang
073	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
074	Haltung	Kognitive Fähigkeiten	Kompetenz	Interaktion
075	Bedürfnis	Kognitive Fähigkeiten	innerer Vorgang	Interaktion
076	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	innerer Vorgang
077	Eigenschaft	Kognitive Fähigkeiten	Kompetenz	Interaktion
078	Bedürfnis	Kognitive Fähigkeiten	innerer Vorgang	innerer Vorgang
079	Fähigkeit	Selbstkontrolle	Kompetenz	innerer Vorgang
080	Fähigkeit	Selbstkontrolle	Kompetenz	innerer Vorgang
081	Fähigkeit	Selbstkontrolle	Kompetenz	innerer Vorgang
082	Fähigkeit	Selbstkontrolle	Kompetenz	innerer Vorgang
083	Fähigkeit	Selbstkontrolle	Kompetenz	innerer Vorgang
084	Fähigkeit	Selbstkontrolle	innerer Vorgang	Kompetenz

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
085	Fähigkeit	Selbstkontrolle	innerer Vorgang	Kompetenz
086	Eigenschaft	Selbstkontrolle	Kompetenz	innerer Vorgang
087	Haltung	Selbstkontrolle	Kompetenz	Interaktion
088	Fähigkeit	Selbstkontrolle	innerer Vorgang	Interaktion
089	Eigenschaft	Selbstkontrolle	innerer Vorgang	innerer Vorgang
090	Eigenschaft	Selbstkontrolle	innerer Vorgang	Interaktion
091	Haltung	Selbstkontrolle	Kompetenz	Interaktion
092	Haltung	Selbstkontrolle	Kompetenz	innerer Vorgang
093	Eigenschaft	Selbstkontrolle	Kompetenz	Interaktion
094	Fähigkeit	Selbstkontrolle	innerer Vorgang	Interaktion
095	Bedürfnis	Selbstkontrolle	innerer Vorgang	innerer Vorgang
096	Eigenschaft	Selbstkontrolle	innerer Vorgang	innerer Vorgang
097	Eigenschaft	Selbstkontrolle	innerer Vorgang	Interaktion
098	Haltung	Selbstkontrolle	innerer Vorgang	innerer Vorgang
099	Bedürfnis	Selbstkontrolle	innerer Vorgang	Interaktion
100	Fähigkeit	Dominanz	Kompetenz	Interaktion
101	Fähigkeit	Dominanz	Kompetenz	Interaktion
102	Fähigkeit	Dominanz	Kompetenz	Interaktion
103	Fähigkeit	Dominanz	Kompetenz	Interaktion
104	Fähigkeit	Dominanz	Kompetenz	Interaktion
105	Fähigkeit	Dominanz	Kompetenz	Interaktion
106	Fähigkeit	Dominanz	Kompetenz	Interaktion
107	Fähigkeit	Dominanz	Kompetenz	Interaktion
108	Eigenschaft	Dominanz	Kompetenz	Interaktion
109	Haltung	Dominanz	Kompetenz	Interaktion
110	Eigenschaft	Dominanz	Kompetenz	Interaktion
111	Eigenschaft	Dominanz	Kompetenz	Interaktion
112	Eigenschaft	Dominanz	Kompetenz	Interaktion
113	Eigenschaft	Dominanz	Kompetenz	Interaktion
114	Eigenschaft	Dominanz	Kompetenz	Interaktion
115	Bedürfnis	Dominanz	innerer Vorgang	Interaktion
116	Bedürfnis	Dominanz	innerer Vorgang	Interaktion
117	Bedürfnis	Dominanz	Interaktion	innerer Vorgang
118	Haltung	Kooperationsfähigkeit	Kompetenz	Interaktion
119	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
120	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
121	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
122	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
123	Fähigkeit	Kooperationsfähigkeit	innerer Vorgang	Interaktion
124	Haltung	Kooperationsfähigkeit	Kompetenz	Interaktion
125	Eigenschaft	Kooperationsfähigkeit	innerer Vorgang	Interaktion
126	Haltung	Kooperationsfähigkeit	Kompetenz	Interaktion
127	Haltung	Kooperationsfähigkeit	Interaktion	Kompetenz

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
128	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
129	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
130	Eigenschaft	Kooperationsfähigkeit	Kompetenz	Interaktion
131	Fähigkeit	Kooperationsfähigkeit	Kompetenz	Interaktion
132	Haltung	Flexibilität	Kompetenz	Interaktion
133	Fähigkeit	Flexibilität	Kompetenz	Interaktion
134	Eigenschaft	Flexibilität	Kompetenz	innerer Vorgang
135	Eigenschaft	Flexibilität	Kompetenz	innerer Vorgang
136	Fähigkeit	Flexibilität	Kompetenz	innerer Vorgang
137	Eigenschaft	Flexibilität	Kompetenz	innerer Vorgang
138	Fähigkeit	Flexibilität	Kompetenz	Kompetenz
139	Haltung	Flexibilität	Kompetenz	innerer Vorgang
140	Fähigkeit	Flexibilität	Kompetenz	innerer Vorgang
141	Eigenschaft	Flexibilität	Kompetenz	Interaktion
142	Fähigkeit	Flexibilität	Kompetenz	Interaktion
143	Fähigkeit	Flexibilität	Kompetenz	Interaktion
144	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
145	Eigenschaft	Kommunikationsfähigkeit	innerer Vorgang	Interaktion
146	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
147	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
148	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
149	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
150	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
151	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
152	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
153	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	Interaktion
154	Fähigkeit	Kommunikationsfähigkeit	Kompetenz	innerer Vorgang
155	Bedürfnis	Kommunikationsfähigkeit	Interaktion	innerer Vorgang
156	Haltung	Motiviertheit	innerer Vorgang	Interaktion
157	Eigenschaft	Motiviertheit	innerer Vorgang	Kompetenz
158	Haltung	Motiviertheit	Kompetenz	innerer Vorgang
159	Eigenschaft	Motiviertheit	innerer Vorgang	Kompetenz
160	Bedürfnis	Motiviertheit	innerer Vorgang	Interaktion
161	Fähigkeit	Motiviertheit	Kompetenz	innerer Vorgang
162	Haltung	Motiviertheit	Kompetenz	innerer Vorgang
163	Fähigkeit	Motiviertheit	Kompetenz	innerer Vorgang
164	Eigenschaft	Motiviertheit	Kompetenz	innerer Vorgang
165	Bedürfnis	Motiviertheit	innerer Vorgang	innerer Vorgang
166	Haltung	Motiviertheit	Kompetenz	innerer Vorgang
167	Fähigkeit	Empathie	Kompetenz	Interaktion
168	Fähigkeit	Empathie	Kompetenz	Interaktion
169	Fähigkeit	Empathie	Kompetenz	Interaktion
170	Fähigkeit	Empathie	Kompetenz	Interaktion

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
171	Eigenschaft	Empathie	innerer Vorgang	Interaktion
172	Fähigkeit	Empathie	Kompetenz	Interaktion
173	Fähigkeit	Empathie	Kompetenz	Interaktion
174	Bedürfnis	Empathie	Interaktion	Kompetenz
175	Eigenschaft	Empathie	Kompetenz	Interaktion
176	Bedürfnis	Selbstwirksamkeit	innerer Vorgang	Interaktion
177	Haltung	Selbstwirksamkeit	Kompetenz	Kompetenz
178	Eigenschaft	Selbstwirksamkeit	Kompetenz	Kompetenz
179	Haltung	Selbstwirksamkeit	Kompetenz	innerer Vorgang
180	Haltung	Selbstwirksamkeit	Kompetenz	innerer Vorgang
181	Haltung	Selbstwirksamkeit	Kompetenz	innerer Vorgang
182	Haltung	Selbstwirksamkeit	Kompetenz	Kompetenz
183	Eigenschaft	Selbstwirksamkeit	innerer Vorgang	Interaktion
184	Haltung	Selbstwirksamkeit	Kompetenz	innerer Vorgang
185	Eigenschaft	Gewissenhaftigkeit	Kompetenz	Kompetenz
186	Haltung	Gewissenhaftigkeit	Kompetenz	innerer Vorgang
187	Bedürfnis	Gewissenhaftigkeit	innerer Vorgang	Kompetenz
188	Eigenschaft	Gewissenhaftigkeit	Kompetenz	Kompetenz
189	Haltung	Gewissenhaftigkeit	Kompetenz	innerer Vorgang
190	Eigenschaft	Gewissenhaftigkeit	Kompetenz	Kompetenz
191	Eigenschaft	Gewissenhaftigkeit	Kompetenz	Kompetenz
192	Eigenschaft	Gewissenhaftigkeit	Kompetenz	Kompetenz
193	Fähigkeit	Selbsteinschätzung	Kompetenz	innerer Vorgang
194	Fähigkeit	Selbsteinschätzung	Kompetenz	innerer Vorgang
195	Fähigkeit	Selbsteinschätzung	Kompetenz	innerer Vorgang
196	Fähigkeit	Selbsteinschätzung	Kompetenz	innerer Vorgang
197	Haltung	Selbsteinschätzung	Kompetenz	innerer Vorgang
198	Bedürfnis	Selbsteinschätzung	innerer Vorgang	innerer Vorgang
199	Bedürfnis	Selbsteinschätzung	innerer Vorgang	innerer Vorgang
200	Fähigkeit	Selbsteinschätzung	Kompetenz	innerer Vorgang
201	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
202	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
203	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
204	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
205	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
206	Fähigkeit	Belastbarkeit	Kompetenz	Interaktion
207	Haltung	Belastbarkeit	Kompetenz	Kompetenz
208	Fähigkeit	Belastbarkeit	Kompetenz	innerer Vorgang
209	Haltung	Offenheit	Kompetenz	Interaktion
210	Haltung	Offenheit	Kompetenz	innerer Vorgang
211	Haltung	Offenheit	innerer Vorgang	Interaktion
212	Haltung	Offenheit	Kompetenz	innerer Vorgang
213	Fähigkeit	Offenheit	Kompetenz	innerer Vorgang

Nr.	Basis	Bereich	primäre Zuordnung	sekundäre Zuordnung
214	Eigenschaft	Offenheit	Kompetenz	innerer Vorgang
215	Eigenschaft	Offenheit	Interaktion	Kompetenz
216	Eigenschaft	Aktivität	Kompetenz	Interaktion
217	Eigenschaft	Aktivität	Kompetenz	Interaktion
218	Eigenschaft	Aktivität	Kompetenz	Interaktion
219	Bedürfnis	Aktivität	innerer Vorgang	Interaktion
220	Eigenschaft	Aktivität	Kompetenz	Interaktion
221	Fähigkeit	Aktivität	Kompetenz	Interaktion
222	Eigenschaft	Aktivität	Kompetenz	innerer Vorgang
223	Bedürfnis	Ethik	Interaktion	innerer Vorgang
224	Fähigkeit	Ethik	Kompetenz	innerer Vorgang
225	Bedürfnis	Ethik	innerer Vorgang	innerer Vorgang
226	Haltung	Ethik	Kompetenz	Kompetenz
227	Fähigkeit	Ethik	Kompetenz	innerer Vorgang
228	Eigenschaft	Extraversion	innerer Vorgang	Interaktion
229	Eigenschaft	Extraversion	innerer Vorgang	Interaktion
230	Bedürfnis	Extraversion	innerer Vorgang	Interaktion
231	Haltung	Extraversion	Kompetenz	Interaktion
232	Fähigkeit	Kreativität	Kompetenz	Kompetenz
233	Fähigkeit	Kreativität	Kompetenz	innerer Vorgang
234	Eigenschaft	Kreativität	Kompetenz	innerer Vorgang
235	Bedürfnis	Sexualität	innerer Vorgang	Interaktion
236	Fähigkeit	Sexualität	Kompetenz	innerer Vorgang

12.6 Übersicht aktuelle und adaptierte CÜ

	INFRAPROTECT	KSÖ	AIT	CSA
Name/ Bezeichnung der aktuellen Cyber-Übung	Funktionstest, Kommunikationsübung, Plan Reviews, Stabsübungen, Stasbrahmenübungen, Krisenkommunikationsübung, Vollübung	KSÖ-Cybersicherheits-Planspiel	strategisches Planspiel (1) und technisches Planspiel (2)	ACSC 2022 (inkl. Quali), ECSC 2022 und open ECSC 2022, NTL
aktuell angesprochene Zielgruppe(n)	Unternehmen, Organisationen, Behörden	Unternehmen, Organisationen, Behörden	1: Management-Ebene und Entscheidungsträger; zu 2: IT-bezogene Fachbereiche; Organisationen, die mit Sicherheit befasst sind	primär: Cybersicherheitsnachwuchst-Talente 14-10/ 20-25; sekundär: Lehrkörper (die eigentlichen Multiplikatoren), Medien, Sponsoren und Behörden
zu erweiternde/ neu zu erschließende Zielgruppe(n)	KMU's (Steuerberatungen, Buchhaltung, Tischlereien, Tourismus, Baufirmen	Klein- und Kleinstunternehmer/innen, EPU insbesondere: Gewerbe und Handwerk, Information und Consulting, Tourismus	Berufstätige, Studierende, Arbeitnehmer*innen, die im IT-Umfeld aktiv sind und noch nicht über genügend IT-Sicherheit haben; Fokus auf ZG Frauen, weil diese anders angesprochen werden müssen; Herausforderung: Wie gewinne ich die Frauen?	offene Klasse: Menschen, die schon im Berufsleben stehen oder älter sind; Universitäten/ Schulen (insb. Lehrer neben HTLs, vor allem neuer Fokus auf AHS mit Schwerpunkt Informatik/ Firmen/ Behörden; Frauen und Mädchen)
Maßnahmen zur Erschließung neuer Zielgruppen (Fokusgruppeninterviews, Umfragen unter bisher nicht repräsentierten Gruppen, Bedarfsanalysen)	Vernetzung via WKO, Interviews und Awarenessschulungen	1) Überblicksrecherche zum vorhandenen Angebot im Bereich der Cybersicherheit 2) Vorbereitung eines niederschwelligen Awareness-Programms für Klein- und Kleinstunternehmer/innen als Fundament für Praxis-Workshops	1. Schritt: Umfrage (Hoffnung: Kontakte zu potentiellen Interviewpartner*innen?); 2. Schritt: Interviews mit Frauen, die bereits an Übungen teilgenommen haben oder mit einer gemischten Gruppe; 3: Intensivierung der Forschungsprojekte und stärkere Verfügbarmachung der Planspiele für eine breitere Zielgruppe;	Verstärkung im Lehrer-Ausbildungs-Modell; Multiplikatorgetrieben/ ledrigschwellige Zugänge via Quizz-Duell-App; Entwicklung einer Internediat-Lösung zum Sprung Hacking Lab/ sihe Leistungspyramide; Def. Des NTL nationalen Trainingslagers mit Schwerpunkt Entwicklung von Zielgruppen-prientierten Trainingsinhalten/ Customerjourney- Wie sehen Frauen Security?
aktuelle Zielgruppenansprache (Werbung, Netzwerke, Arbeitgeber)	HP-Angebote, Webinare, ständig Vernetzung via anderer Branchen	Das aktuelle Angebot für die neu zu erschließende Zielgruppe umfasst: - die themenspezifischen Webseiten mit bereitgestellten Erklärtexten und Erklärvideos, - Webinare in Form frontal gehaltenener Vorträge. (Detaillierte Auflistung der laufenden Initiativen - siehe Anhang) Mit diesen Mitteln werden Personen erreicht, die ohnehin motiviert sind, sich mit dem Thema Cybersicherheit zu befassen. Für Personen mit Berührungsängsten in Bezug auf IT-Themen oder ohne Bewusstsein über die Bedeutsamkeit der digitalen Sicherheit für eigenes Unternehmen sind die Webinare und Lernmaterialien nicht genung niederschwellig. Zudem ist das vorhandene Angebot wenig handlungsorientiert. Es fehlt an Workshops mit praktischen Übungen.	primär über die Arbeitgeber; Ausnahme: KSÖ-Planspiel (KSÖ lädt ein)	Die Challenge selbst richtet sich als Exzellenz-Bewerb an talentierte Lehrlinge, Schüler und Studenten mit Interessensschwerpunkt Cyber Security; Ausbildungsstätten wie HTLs; AHS mit Informatik-Schwerpunkt, FHs; Unis; hier insb. Lehrkräfte/ Lehrgangsleiter mit Sicherheitsschwerpunkten sowie Behörden und alle Unternehmen sowie grundsätzlich alle Security-interessierten Vertreter Europas; spezielle Zielgruppe: Medeien und andere Kommunikations-Multiplikatoren als eigentliche "Vergbreiter" der Idee; je überzeugter sie vom Konzept und der Idee der Challenge und ihrer Notwendigkeit sind, umso engagierter und zielgerichteter erfolgt ihre Unterstützung. Offene Klasse Ansprache: insb. Emerging Talents (Studierende der Studienrichtungen IT, Techn. Mäthematik, Softwareentwicklung...) und andererseits Sicherheitsforscher*innen/ FAchleute/Professionals in den Bereichen IT- und Cybersecurity
adaptierte/ erweiterte Zielgruppenansprache (Sensibilisierung über Werbung, Netzwerke, Anzeigen; gezielte Ansprache, Role Models)	Einstieg via Fragenkatalog und Newsletters mit einfachen Tipps & Tricks	Sensibilisierung und Aktivierung über folgende Kanäle: - Newsletter der Wirtschaftskammer, insbesondere: - Frau in der Wirtschaft, Ausschuss für Ein-Personen-Unternehmen, - EPU-Plattform "Wir sind 1 und trotzdem ganz schön viele". KSÖ-Präsenz bei folgenden Veranstaltungen zwecks Erweiterung der Zielgruppenansprache: - 18.10.2021: *Zugang für Unbefugte geöffnet? Cybersecuity im Homeoffice* - Präsenz- und Online-Event in Zusammenarbeit mit der Wirtschaftskammer Wien, - 25.11.2021: IT- und Beratertag der WKÖ, - 07.12.2021: eDAY21 der WKÖ.	evtl. Einladung zu offenen Planspielen?	to do: Mundpropaganda-Modell bzw. affiliate-programm für Teilnehmer und Interessierte. Die ACSC erreicht durchschnittlich rund 600 Sicherheitsinteressierte - und liegt mit etwa 100 Pressecllppings/ Jahr erfolgreich auf Kurs (orf.on, standard, futurzone..), auch 2-3 Fernsehclips (ZIB) und Radiobeiträge (Morgenjournal, Nachrichten Ö3) ermöglichen relativ hohe Reichweiten. Der online Auftritt "verbirgt" erreicht rund 30k unique visitors, die ECSC.eu rund 90k
Kontext/Setting aktuelle Cyber-Übung	primär KRITIS, DAX-Unternehmen, sowie Unternehmen der Daseinsvorsorge sowie Handel und Logistik	gesamtgesellschaftliche Cyber-Bedrohungsszenarien wie z. B. Ausfall des Internets in ganz Österreich, Datendiebstahl, Cyber-Erpressung in Unternehmen der kritischen Infrastruktur, Terrorbedrohung, Erprobung der EU-Richtlinie zur Netzwerk- und Informationssicherheit, Angriff auf ein Pharmaunternehmen mit Schlüsselfunktion in der Bekämpfung der Pandemie Teilnehmende: Behörden, Vertreter der kritischen Infrastruktur, CERTs, Wissenschaftsvertreter, Interessenvertretungen, Medienvertreter	Awareness-Schulung (Bsp.:Anklicken von Links); Festigung von Lehrinhalten (Prozessfestigung, je nach Fachbereich); Simulation: fiktive Geschichte mit Bezug zum Unternehmen; Angriffssimulationen (wie verhält sich der Angreifer?); User-Simulationen; zu 1: (interaktive) Schulung mit unterschiedlichen Themen für verschiedene ZG; Inhalte werden durchgespielt; zu 2: technische Infrastruktur, auf der direkt	Fachkräftemangel ist für Europas Wirtschaft und Gesellschaften zum spürbaren Problem geworden – dies gilt ins besonders auch für IKT-Sicherheitsfachkräfte. Eine Reihe nationaler Bewerbe versuchte dieser Entwicklung mit der Durchführung lokaler Challenges konkrete Maßnahmen entgegen zu setzen.
adaptierter, diversitäts-sensibler Kontext	Altersgruppe > 50.	Fokus auf Cyber-Sicherheit und Cyber-Risiken in einem Klein-/Kleinstunternehmen, Berücksichtigung von (unterjdurchschnittlich ausgeprägten technischen Skills der Unternehmer/innen, Sensibilisierung für die Problematik im Vorfeld der praktischen Cyber-Übungen	Simulationen sollen variabler gestaltet und an die jeweiligen ZG angepasst werden (Umfrage: welche Szenarien "passen" zu welchen ZG?)	Zielsetzung: Challenges diversitätssensibler erstellen und andere Zielgruppen erreichen sowie die Information über die Challenges an sich zur Thematisierung/Sensibilisierung des Bereiches nutzen; Möglichkeit, auch Umfragen auf Landing Pages einzubauen, um nähere Informationen über Nutzer*innenverhalten sowie Selbsteinschätzung abzufragen
Methodik/ Didaktik aktuelle Cyber-Übungen	gemäß NATO Training Exercise Directive, Erwachsenen Aus- Fortbildungsgrundsätze Erfahrungswissensvermittlung	Training in einer IT-Simulationsumgebung, der „AIT Cyber Range" mit mehreren Spielergruppen	(interaktive) Schulungen; strategische (angeleitet von Moderator mit anschließender Gruppendiskussion)und technische (Team erarbeitet sich selbständig die Lösungen; Spielleiter) Planspiele; Awareness-Schulung	Die A/ECSC wurde aus mehreren Gründen konzipiert. Nicht nur soll jenen ersten Veranstaltung/ändern die Möglichkeit des Europäischen Vergleichskampfes geboten werden und somit ein entsprechendes Benchmarking/Fingerprinting der eigenen nationalen Ressourcen im Vergleich mit anderen Ländern ermöglicht werden , sondern vor allem steht die massive Aufwertung der jeweiligen nationalen Veranstaltungen im Vordergrund. Zusätzliche Anreize werden für alle Stakeholder, die durch diese Challenges angesprochen werden, geschaffen.
adaptierte/ erweiterte Methodik/ Didaktik	Gaming, geleitete Trainings, unterstützt durch entsprechende KPIs	Die Zielgruppenansprache wird mit folgenden diverstitätssensiblen Methoden angepasst: - Microlearning, - Storytelling, - Emotionalisierung der Lerninhalte, - Versuch eines humoristischen Ansatzes, - handlungsorientierte Aktivierung.	strategische Übungen (1) haben sich bewährt (Ziel: Awareness); technische Übungen (2): evtl. kürzen, um "Neue" nicht abzuschrecken; Unterstützung und Support sind dabei besonders wichtig	Autodidakten, Schulen/Hochschulen (Lehrbetrieb), CTF-Communities, Rolemodels (derzeit nur männlich), Lehrlingsausbildungsbereiche - primär via HackingLab-Plattform zu den jeweiligen Security-Schwerpunkten

Aktuelle Initiativen und Angebote		
1.	**„IT-Sicherheit für KMU“ vom „Haus der Digitalisierung“ mit der WKNÖ**	
	Services	**Veranstaltungen**
	Cyber-Security-Hotline der WKO	Awareness-Vortrag und Tipps „Cyber-Gefahren“
	WKO OnlineRatgeber ratgeber.wko.at/itsafe	Webinar „Sicherheit im Internet: Phishing & Co“ - Veranstaltung mit EVN Chief Information Security Officer Wolfgang Löw
	„IT-Sicherheit-Tipps für KMU“ Video auf www.virtuelleshaus.at mit Oberst Walter Unger	Webinar „Cybersicheres Zuhause und Homeoffice“
		Kleingruppen-Workshops zu den Bedrohungsszenarien www.virtuelleshaus.at
2.	**www.it-safe.at (enthält Verweis auf KMU.DIGITAL) it-safe.at ist eine Aktion der Bundessparte Information und Consulting (BSIC) in der Wirtschaftskammer Österreich (WKÖ).**	
	Services	**Veranstaltungen**
	KMU.DIGITAL Förderung Gefördert werden folgende Maßnahmen: - Statusanalyse im Bereich IT- und Cybersecurity - Förderung 80 % max. 400 Euro, - Strategieberatung im Bereich IT-und Cybersecurity-Förderung 50 % max. 1.000 Euro, - Umsetzung von Digitalisierungsprojekten im Bereich IT- und Cybersecurity – 30 % Zuschuss (max. 6.000 Euro)	Webinarreihe zum Datenschutz https://www.wko.at/service/wirtschaftsrecht-gewerberecht/webinare-dsgvo.html
	Online-Ratgeber IT-Sicherheit im Unternehmen Stand: 30.11.2020 (https://www.wko.at/site/it-safe/online-ratgeber.html), Themen: Ransomware, Sicherheit am Smartphone, Datensicherung (Erklärvideo)	
	Erklärtexte oder -videos Ich habe einen Vorfall - Checkliste, 7 Tipps für mehr Cybersicherheit im Unternehmen, DDoS Angriffe gegen Unternehmen, Microsoft Exchange Sicherheitslücke - Unternehmen massiv betroffen Cybersecurity am E-Day 2021, Oktober ist European Cyber Security Month, Vorsicht vor Online-Betrügern Datensicherungsarten im Überblick Cyber-Versicherungen: Das Risiko einfach auslagern? Social Engineering - der Mitarbeiter als Angriffsziel, IT-Sicherheitsstrategie: Was ist alles zu beachten?, Cybersicherheit für Unternehmen, Cloud Anwendungen für kleine Unternehmen, Online-Fakeshops erkennen, Cybersicher im Homeoffice, Cybersicherheit in Zeiten des Coronavirus, Datenschutz in Coronazeiten, Ransomware - Daten gegen Lösegeld, Aktuelle Betrugswarnungen, Gütesiegel Austrian Cloud – meine Daten bleiben rot-weiß-rot	
	IT-Sicherheitshandbuch für KMU, Stand: 12.11.2019 (9. Auflage)	
3.	**diverse Webinare in der WKO**	
		18.10.2021 - Zugang für Unbefugte geöffnet? Cybersecurity im Homeoffice
		20.10.2021 - Sind Sie sicher, dass ihre Daten sicher sind? - Datenschutz und Datensicherheit 2021
		29.11.2021 - Smartphones, Suchmaschinen, Apps & Google. Wie Sie Ihre Spuren verwischen und sensible Daten wirklich schützen
		ab 06.10.2021 - Online-Vortragsreihe Cyber-Security für Sprachdienstleister

	WKO - Themen - Innovation, Technologie und Digitalisierung - IT-Sicherheit, Datensicherheit	
	Strategien und Ratgeber zur IT-Sicherheit, IT-Sicherheit für KMU und EPU, Gesetzliche Richtlinien zur IT- und Datensicherheit, Umgang mit Daten, Datensicherung, Gefahrenquellen, Sicherheit in Netzwerken, IT- und Datensicherheit auf mobilen Endgeräten, Informationssicherheit im Unternehmensalltag	
4.	**DIH-OST - Webinar-Reihe "Sicheres Homeoffice" (Veranstalter: FH St. Pölten / April-Mai 2020)**	
	12 Aufzeichnungen zum Nachschauen	
5.	**Weitere Angebote - Beispiele**	
	Watchlist Internet: Watchlist Internet – Online-Betrug, -Fallen & -Fakes im Blick (watchlist-internet.at)	
	saferinternet.at	
	onlinesicherheit.gv.at (Partner bei it-safe.at Das IKT-Sicherheitsportal ist eine ressortübergreifende Initiative in Kooperation mit der heimischen Wirtschaft und stellt ein auf elektronischem Wege abrufbares Internetportal für Themen rund um die Sicherheit der Informations- und Kommunikationstechnologie (IKT) dar. Initiatoren sind: Bundesministerium für Finanzen, Bundeskanzleramt und A-SIT Zentrum für sichere Informationstechnologie - Austria.	