

Cybersicherheit und Diversität: Eine Notwendigkeit in der Digitalisierung

In einer Welt, die immer stärker von digitalen Technologien geprägt ist, gewinnt das Thema Cybersicherheit zunehmend an Bedeutung. Wir alle nutzen täglich das Internet für verschiedene Zwecke, sei es zum Arbeiten, Kommunizieren oder Unterhalten. Doch während wir von den Vorteilen der digitalen Welt profitieren, dürfen wir nicht die Herausforderungen und Risiken vergessen, denen wir uns gegenübersehen. Die Digitalisierung hat das Potenzial, den Zugang zu Ressourcen und Chancen zu verbessern, aber sie birgt auch die Gefahr, bestehende Ungleichheiten zu verstärken. Daher ist es entscheidend, dass wir uns aktiv mit dem Zusammenspiel von digitaler Fairness und Diversität auseinandersetzen.

Ein wichtiger Aspekt von Cybersicherheit, der oft übersehen wird, ist die Rolle der Diversität. Die digitale Welt ist geprägt von einer Vielzahl von Menschen mit unterschiedlichen Hintergründen, Bedürfnissen und Fähigkeiten. Doch allzu oft werden Cybersicherheitslösungen und -strategien entwickelt, ohne diese Vielfalt angemessen zu berücksichtigen. Wenn wir eine digitale Zukunft aufbauen wollen, die für alle gerecht ist, müssen wir sicherstellen, dass unsere digitalen Lösungen und Technologien diese Vielfalt angemessen berücksichtigen.

Unsere Welt wird immer technisierter und digitalisierter. Der viel gerühmte „Gläserne Mensch“¹ ist heutzutage in vielen Bereichen Realität geworden. Nur den wenigsten ist es bewusst, dass sie kostenlose Dienste (wie z.B. Apps, soziale Medien, Vorteilsprogramme wie z.B. Jö, etc.) oft mit ihren Daten bezahlen. Auch wenn das einzelne Individuum kein großes Interesse darzustellen scheint, ist jedoch die Masse der Individuen eine großartige Datenquelle für die Anbieter*innen dieser Dienste. Natürlich kann es eine bewusste Entscheidung sein, seine Daten herzugeben, weil man sich damit Vorteile in einem Dienst „erkauft“. Diese Vorteile können ein besseres Einkaufserlebnis in einem Online-Shop sein oder das Merken von Einstellungen auf einer Webseite. Aber diese Entscheidung muss im vollen Bewusstsein getroffen werden können. Die Information muss so aufbereitet werden, dass transparent dargestellt wird, wo die Daten verbleiben, was mit ihnen geschieht und wer sonst noch darauf Zugriff hat und warum. Nur durch solche Informationen kann eine bewusste Entscheidung getroffen werden, ob ich einem Dienst meine Daten zur Verfügung stellen will oder eben auch nicht. Dies inkludiert auch die Information darüber, ob eine potentielle Weitergabe und bzw. ein Verkauf der Daten an dritte Parteien beinhaltet ist.

Bankkonten, soziale Dienstleistungen, Finanzämter – all diese Dienste werden in die digitale Welt wandern oder sind es teilweise schon. Teilweise gibt es diese Dienste auch noch offline, indem man z.B. noch zu einem Finanzamt gehen kann, jedoch sorgt die steigende Digitalisierung dafür, dass diese offline Zugänge mehr und mehr beschränkt werden. Viele Banken dünnen ihr Filialnetz immer mehr aus, es wird immer schwieriger Dienste, ohne ein internetfähiges Gerät zu bewältigen. Dies trifft vor allem die ältere Bevölkerung stärker, aber auch Personen, die die persönliche Betreuung in einer Filiale schätzen.

Hier setzt das Projekt INDUCE an. INDUCE² ist gefördertes Forschungsprojekt, das darauf abzielt, Cybersicherheitskompetenzen und -fähigkeiten in einer vielfältigen Gesellschaft zugänglich zu machen. Das Projekt evaluiert bestehende Cyber-Übungen anhand verschiedener Diversitätsdimensionen und Chancengerechtigkeit und entwickelt diese weiter, um der Heterogenität der Zielgruppen gerecht zu werden.

¹ [https://de.wikipedia.org/wiki/Gl%C3%A4serner_Mensch_\(Datenschutz\)](https://de.wikipedia.org/wiki/Gl%C3%A4serner_Mensch_(Datenschutz))

² <https://induce.ait.ac.at/projekt/>

Eine der zentralen Herausforderungen im Bereich Cybersicherheit ist die Berücksichtigung der vielfältigen Bedürfnisse und Hintergründe der Nutzer. Menschen mit unterschiedlichem kulturellem Hintergrund, Geschlecht, Alter und Bildungsstand haben unterschiedliche Anforderungen und Bedürfnisse im Umgang mit digitalen Technologien und Risiken.

Durch die Entwicklung diversitätssensibler Cyber-Szenarien und Technologien trägt INDUCE dazu bei, sicherzustellen, dass Cybersicherheitslösungen für alle relevant und effektiv sind. Denn Cybersicherheit betrifft uns alle, unabhängig von unserem Hintergrund oder unserer Herkunft.

Darüber hinaus fördert INDUCE den Aufbau eines Innovationsnetzwerks, das den Wissens- und Technologietransfer zwischen verschiedenen Akteur*innen wie Wirtschaft, Behörden und Forschungseinrichtungen unterstützt. Durch diese Zusammenarbeit können langfristig Cybersicherheitskompetenzen für die Bevölkerung aufgebaut und weiterentwickelt werden.

Ein weiterer wichtiger Aspekt des Zusammenspiels von digitaler Fairness und Diversität ist die Rolle von Bildungseinrichtungen. Schüler*innen und Lehrer*innen spielen eine Schlüsselrolle bei der Förderung von digitaler Kompetenz und Bewusstsein für Cybersicherheit. INDUCE bietet hier wertvolle Erkenntnisse und Tools, die dazu beitragen können, eine Generation von digital kompetenten Bürgern heranzubilden.

Mit INDUCE können langfristig Cybersicherheitskompetenzen für die Bevölkerung aufgebaut und weiterentwickelt werden, die im Zuge der Digitalisierung zur Handlungsfähigkeit vielfältiger Zielgruppen in einer digitalen Gesellschaft beitragen.

Das Projekt beschäftigt sich mit diesen drei Bereichen:

- Awareness (Bewusstseinsbildung)
- Literacy (Lese- und Schreibfähigkeit) und
- Dexterity (Geschicklichkeit).

Diese Bereiche sind ebenso wichtig, da auch sie einen Einfluss auf das Verständnis von Cybersicherheit haben. Nachstehend werden die Begriffe erklärt.

Awareness bezieht sich auf das Bewusstsein oder die Wahrnehmung einer Person oder Gruppe von Personen über bestimmte Themen, Probleme oder Risiken. In vielen Kontexten, insbesondere im Bereich der Sicherheit und Prävention, spielt Awareness eine entscheidende Rolle, da sie dazu beiträgt, Menschen für potenzielle Gefahren zu sensibilisieren und sie dazu befähigt, angemessen darauf zu reagieren.

Im Bereich der Cybersicherheit beispielsweise bezieht sich Awareness darauf, wie gut Menschen über die Risiken und Best Practices im Umgang mit digitalen Technologien informiert sind. Eine hohe Cybersicherheits-Awareness bedeutet, dass Individuen sich der potenziellen Bedrohungen wie Phishing, Malware oder Datenlecks bewusst sind und wissen, wie sie sich davor schützen können, z. B. durch die Verwendung von sicheren Passwörtern, regelmäßige Software-Updates oder das Erkennen verdächtiger E-Mails.

Insgesamt ist Awareness ein wichtiger Faktor, um Menschen dabei zu helfen, fundierte Entscheidungen zu treffen und sich vor potenziellen Gefahren zu schützen. Sie spielt eine entscheidende Rolle bei der Schaffung einer sichereren und besser informierten Gesellschaft.

Literacy bezieht sich traditionell auf die Fähigkeit einer Person, lesen und schreiben zu können. Diese grundlegenden Fähigkeiten sind entscheidend für die Teilnahme an der Bildung, am Arbeitsleben und an der Gesellschaft insgesamt. Allerdings hat sich das Konzept der Literacy im Laufe der Zeit weiterentwickelt und umfasst mittlerweile auch andere Fähigkeiten und Kompetenzen.

Heutzutage wird Literacy oft als Sammelbegriff verwendet, der verschiedene Arten von Fähigkeiten und Kompetenzen umfasst, die für das Leben in einer zunehmend komplexen und digitalen Welt erforderlich sind. Dazu gehören beispielsweise Medienliteracy oder Digitale Literacy.

Insgesamt bezieht sich Literacy also auf die Fähigkeit, Informationen zu verstehen, zu interpretieren und darauf basierend fundierte Entscheidungen zu treffen. In einer zunehmend komplexen und digitalen Welt sind diese Fähigkeiten wichtiger denn je, um aktiv am gesellschaftlichen Leben teilzuhaben und sich persönlich weiterzuentwickeln.

Cyber Literacy bezieht sich auf das Verständnis und die Fähigkeiten einer Person im Umgang mit Aspekten der digitalen Welt, insbesondere im Bereich der Cybersicherheit und Informationstechnologie. Es geht darum, Grundkenntnisse und Bewusstsein für die verschiedenen Facetten der Cyberwelt zu entwickeln, um sich sicher und kompetent in einer zunehmend vernetzten und digitalen Umgebung zu bewegen. Cyber Literacy ist entscheidend, da sie dazu beiträgt, Benutzer*innen vor Cyberbedrohungen zu schützen, das Vertrauen in digitale Technologien zu stärken und die Fähigkeiten der Gesellschaft im Umgang mit der sich ständig weiterentwickelnden digitalen Welt zu verbessern. Es ist ein lebenslanges Lernen, da sich Technologien und Bedrohungen weiterentwickeln.

Dexterity bezieht sich auf die Geschicklichkeit, Feinmotorik und Fingerfertigkeit einer Person bei der Ausführung von präzisen und koordinierten Bewegungen. Es ist die Fähigkeit, komplexe Aufgaben mit den Händen auszuführen, insbesondere solche, die präzise Koordination, Bewegungskontrolle und Fingerfertigkeit erfordern. Dexterity ist entscheidend in verschiedenen Kontexten, wie beispielsweise beim Spielen von Musikinstrumenten, der Bedienung von feinen Werkzeugen oder der Durchführung von präzisen Handgriffen in der Chirurgie. Es kann auch auf die allgemeine Geschicklichkeit und Fingerfertigkeit im Alltag hinweisen.

Cyber Dexterity ist ein Begriff, der auf die Fähigkeiten und Kompetenzen einer Person im Bereich der Cybersecurity anspielt. Es bezieht sich auf die Geschicklichkeit, das Verständnis und die Handlungsfähigkeit im Umgang mit den Herausforderungen und Bedrohungen im Cyberspace. Cyber Dexterity ist entscheidend, da die Bedrohungen im Cyberspace immer ausgefeilter werden. Sowohl individuelle Fachkräfte als auch Organisationen als Ganzes müssen ihre Cyber dexterity ständig verbessern, um mit den Herausforderungen der Cybersicherheit Schritt zu halten. Dies kann durch Schulungen, praktische Erfahrungen und kontinuierliche Weiterbildung erreicht werden.

Ein Hauptziel des Projektes ist es, die Awareness (Bewusstseinsbildung), die Literacy und die Dexterity zu erhöhen. Jedoch wurde das Projekt mit Herausforderungen konfrontiert, die nicht überwunden werden konnten, was aber nicht bedeutet, dass sie nicht gelöst werden können. Das Projekt hat gezeigt, dass es wichtig ist, über Cybersicherheit über alle Bevölkerungsschichten hinweg zu reden und über das Thema zu sensibilisieren. Aber es hat auch gezeigt, dass man nicht alle über „einen Kamm scheren kann“ und man zielgruppenorientierte Angebote anbieten muss, um hier einen Effekt zu erzielen. Des Weiteren müssen die Angebote auch an die Zielgruppe herangebracht werden, was sich teilweise als schwierig ergeben hat. Hier muss ein ganzheitlicher Ansatz gefunden werden, um mehr Personen und Gruppen ansprechen zu können.

Die Sprache und wie die Inhalte vermittelt werden ist hier essenziell. Es müssen die soziokulturellen Aspekte aber auch technologische Entwicklungen und individuelle Lernbedürfnisse einbezogen werden. Es ist wichtig, dass es für diese unterschiedlichen Gruppen Angebote gibt, die nicht für alle gleich sind,

sondern nach Bildungsniveau, kognitiven Einschränkungen, Alter, kultureller Hintergrund, und dgl. unterscheiden. Die oben erwähnten Cyber Übungen oder Maßnahmen zur Bewusstseinsbildung müssen so gestaltet sein, dass diese von einer breiten Masse verstanden, aber auch akzeptiert werden. Keiner darf sich davon über- oder unterfordert oder sich in irgendeiner Form beleidigt fühlen.

Dies stellt die Gesellschaft und auch die Behörden vor eine große Herausforderung, wenn der Weg in Richtung Digitalisierung weiter beschritten werden soll – wovon aus heutiger Sicht wohl auszugehen ist, siehe Digital Austria³. Das ist ein Appell an alle, die sich damit beschäftigen und auch nicht damit beschäftigen, sich dem Thema Cyber Security anzunehmen. Wir laufen sonst Gefahr, Teile der Bevölkerung zurückzulassen, die unter Umständen nicht zurückgelassen werden wollen. Auf der anderen Seite müssen sich auch Vereine und andere Organisationen einbringen, um in die verschiedenen sozialen und kulturellen Gruppen vorzudringen und hier Bewusstsein für das Thema Cybersicherheit schaffen. In den Schulen muss das Thema spielerisch schon in der Volksschule angegangen werden, da auch schon Kleinkinder die Smartphones ihrer Eltern oder Spielkonsolen, die mit dem Internet verbunden sind, verwenden. Diese Geräte sind oft Einfallstoren für unerwünschte Dinge, die im besten Fall nur Kleinigkeiten sind, aber im schlimmsten Fall ganze Existenzen bedrohen können, wenn z.B. ein Datenverlust des Cloud-Speichers eintritt, wenn durch eine Unachtsamkeit die Rechnung nicht bezahlt wurde.

Insgesamt zeigt das Projekt INDUCE, dass digitale Fairness und Diversität eng miteinander verbunden sind. Indem wir die Vielfalt unserer Gesellschaft in den Mittelpunkt unserer digitalen Lösungen stellen, können wir eine gerechtere und sicherere digitale Zukunft für alle schaffen. In einer zunehmend vernetzten Welt ist Cybersicherheit mehr als nur ein technisches Problem. Sie ist eine gesamtgesellschaftliche Herausforderung, die ein breites Spektrum von Akteur*innen und Ansätzen erfordert. Das Projekt INDUCE zeigt, dass Cybersicherheit und Diversität eng miteinander verbunden sind und nur gemeinsam angegangen werden können.

³ <https://www.digitalaustria.gv.at/>

Weiterführende Tipps und Links für Interessierte:

Es gibt verschiedene Möglichkeiten, wie Sie Ihre Cyber Literacy verbessern können. Hier sind einige Tipps, die Ihnen helfen können:

- Nutzen Sie verschiedene Quellen, um sich über digitale Themen zu informieren.
- Üben Sie den kritischen Umgang mit digitalen Informationen. Prüfen Sie die Glaubwürdigkeit, Relevanz und Aktualität der Informationen, die Sie online finden oder erhalten.
- Schützen Sie Ihre Privatsphäre und Sicherheit online. Verwenden Sie starke Passwörter, Antivirensoftware und sichere Verbindungen, um Ihre Daten und Geräte vor Cyberangriffen zu schützen.
- Weitere Tipps: <https://induce.ait.ac.at/induce-cybersecurity-tips/>

Wenn Sie weitere Tipps, Unterlagen und Materialensuchen, um Ihre Cyber Literacy zu verbessern, können Sie sich diese Webseiten ansehen:

- <https://insights.gostudent.org/digitale-kompetenz-definition-und-beispiele>
- <https://www.wien.gv.at/menschen/frauen/stichwort/gewalt/cyber-gewalt/kompetenzstelle.html>
- <https://www.hardreset.info/de/articles/top8-computer-literacy-tips/>
- <https://www.bpb.de/lernen/digitale-bildung/politische-bildung-in-einer-digitalen-welt/324982/medienkompetenz-und-digital-literacy/>

Kontakt:

PETRA KÖLNDORFER

Security & Communication Technologies

Center for Digital Safety & Security

AIT Austrian Institute of Technology GmbH

Giefinggasse 4 | 1210 Vienna | Austria

T +43 50550-2822 | M +43 664 8157920

petra.koelndorfer@ait.ac.at | www.ait.ac.at

Das Projekt "INDUCE" wird aus Mitteln der Nationalstiftung für Forschung, Technologie und Entwicklung sowie dem Österreich-Fonds finanziert. Die Abwicklung des Förderungsprogramms Laura Bassi 4.0 erfolgt durch die Österreichische Forschungsförderungsgesellschaft (FFG) und mit freundlicher Unterstützung des Bundesministeriums für Arbeit und Wirtschaft (BMAW).

