Hamburg, Ileana; Sommer, David

Research Report

Cyber-Sicherheitstraining für kleine und mittelständische Unternehmen: Das Erasmus+ Projekt IbCyT

Forschung Aktuell, No. 12/2022

Provided in Cooperation with:
Institute for Work and Technology (IAT), Westfälische Hochschule, University of Applied Sciences

Suggested Citation: Hamburg, Ileana; Sommer, David (2022) : Cyber-Sicherheitstraining für kleine und mittelständische Unternehmen: Das Erasmus+ Projekt IbCyT, Forschung Aktuell, No. 12/2022, Institut Arbeit und Technik (IAT), Gelsenkirchen, https://doi.org/10.53190/fa/202212

This Version is available at:
https://hdl.handle.net/10419/268667

FORSCHUNG AKTUELL
12/2022

Cyber-Sicherheitstraining für kleine und mittelständische Unternehmen – Das Erasmus+ Projekt *InCyT*

Ileana Hamburg, David Sommer

Institut Arbeit und Technik

Zentrale Einrichtung der Westfälischen Hochschule Gelsenkirchen Bocholt Recklinghausen in Kooperation mit der Ruhr-Universität Bochum

Westfälische Hochschule

RUHR UNIVERSITÄT BOCHUM RUB

Auf den Punkt

- Die Anzahl von Cyberattacken auf Personen und Organisationen steigt. Insbesondere kleine und mittlere Unternehmen (KMU) haben aufgrund limitierter Ressourcen und mangelnder IT- und Cybersecurity-Kenntnisse Schwierigkeiten, gezielte Maßnahmen zu implementieren (techconsult, 2019).
- Cybersicherheitsprobleme sind komplex und interdisziplinär: Sicherheitsaktivitäten enthalten soziale, rechtliche, ethische, soziologische, psychologische, technische, aber auch wirtschaftliche und verwaltungstechnische Elemente.
- Die Nationale Initiative für Cybersicherheitsausbildung (NICE) unterstreicht, dass aufgrund der komplexen Cyberangriffe eine "integrierte Cybersicherheitsbelegschaft" notwendig ist (Petersen et al., 2020).
- Aus- und Weiterbildungseinrichtungen tragen dazu bei, die Interdisziplinarität in diesem Zusammenhang zu fördern.
- Im Rahmen des Erasmus+ Projekts *Interdisciplinary Cyber Training* (*InCyT*) wurde mit Partnern aus den Bereichen Bildung, Forschung und Wirtschaft aus sieben Ländern ein Cybersecurity-Kompetenzrahmen entwickelt, der als Ziel die Verbesserung der beruflichen Aus- und Weiterbildung (VET) sowie der Kompetenzen und Fähigkeiten von Mitarbeitenden hat, um Cyberangriffe zu verhindern.
- Ein digital unterstütztes interdisziplinäres Trainingsprogramm und eine kollaborative digitale Plattform für KMU sind in der Testphase. Zudem sind eine angepasste Version für die Berufsbildung sowie ein europäisches Übertragbarkeitsmodell geplant.

Cybersicherheit und Cyberangriffe in Deutschland

Die IT-Sicherheit beschäftigt sich mit dem Schutz der IT-Infrastruktur von Unternehmen und Organisationen mit dem Ziel, wirtschaftliche Schäden durch Cyberattacken zu verhindern. Heutzutage wird Cybersicherheit häufig als Synonym für IT-Sicherheit benutzt. Wir definieren die „Cybersicherheit als Schutz von Netzwerken, Computersystemen, cyberphysischen Systemen und Robotern vor Diebstahl oder Beschädigung ihrer Hard- und Software oder der von ihnen verarbeiteten Daten durch Cyber-Angriffe sowie vor Unterbrechung oder Missbrauch der angebotenen Dienste und Funktionen“ (Bendel, 2022).

Ende Oktober 2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen jährlichen Bericht zum Stand der IT-Sicherheit in Deutschland vorgelegt (BSI, 2022). Er gibt einen umfassenden und fundierten Überblick über die IT-Bedrohungen, denen sich Staat, Wirtschaft und Gesellschaft in Deutschland gegenübersehen. So haben beispielsweise Ransomware-Vorfälle deutlich zugenommen und in allen Branchen zu erheblichen Störungen geführt. In Deutschland waren neben Produktionsbetrieben auch Krankenhäuser und Kommunen betroffen. Zu den technischen Kernergebnissen des Berichts gehören die Entdeckung von rund 114 Millionen neuen Malware-Typen weltweit (BSI, 2022). In Deutschland werden täglich bis zu 110.000 Typen in deutschen IT-Systemen (mit Schwerpunkt auf mobilen Geräten) verzeichnet und gezielte Angriffe zur Nichtverfügbarkeit eines Dienstes oder Servers durchgeführt. Darunter DDoS-Angriffe mit einer Bandbreite von bis zu 300 Gbit/Sekunde (ebd.). Das BSI (2022) hat mehr als 11.5 Millionen Malware-Infektionswarnungen an deutsche Netzbetreiber verschickt. In den Netzen der Bundesbehörden konnten 770.000 bösartige E-Mails abgefangen werden, die meisten davon mit Hilfe der BSI-eigenen Anti-Malware-Datenbank. Laut BSI (2022) ist Emotet eine der derzeit gefährlichsten und am weitesten verbreiteten Malware. Durch die zunehmende Nutzung von Online-Kollaborationsplattformen, E-Commerce, E-Banking und E-Government-Diensten, die Verlagerung von Bildungsaktivitäten auf E-Learning sowie durch Technologien wie QR-Codes, kontaktlose Zahlungen und Direct-to-Consumer-Modelle wie Hauslieferungen, Click-and-Collect-Dienste und Fernhilfe per Chat oder Telefon finden Kriminelle neue Angriffsfelder, wodurch zu erwarten ist, dass solche Cyber-Angriffe in Zukunft zunehmen werden (Streim & Mann, 2021).

Auf Basis einer Hochrechnung mit dem Fokus auf digitale Wirtschaftsspionage, Sabotage und Datendiebstahl schätzt die Bitkom-Studie den Gesamtschaden für Industrieunternehmen in den vergangenen zwei Jahren auf rund 205 Milliarden Euro (ebd.).

Cybersicherheit und Dimensionen von Cyber-Angriffen in KMU

Kleine und mittlere Unternehmen (KMU) spielen eine wichtige Rolle für die Beschäftigung und sind eine tragende Säule der Volkswirtschaft (Braun, 2020). Daher besteht ein großes

Interesse an den Daten dieser Unternehmen. Als KMU gelten nach der EU-Definition Unternehmen mit 250 oder weniger Beschäftigten, deren Jahresumsatz 50 Millionen Euro nicht überschreitet (Europäische Kommission, 2003).

Mehrere Studien und Berichte deuten darauf hin, dass KMU im Allgemeinen die IT-Risiken aufgrund ihrer geringen Größe unterschätzen (Dreißigacker, Engemann et al., 2017; Knirsch, 2019). Sie betrachten die IT- und Cybersicherheit-Problematik als ein Thema für große Unternehmen. Ein Großteil der KMU ist der Überzeugung, dass sie kein wirkliches Ziel für gefährliche Cyberangriffe wären (Engemann et al., 2017). Computerviren, Trojaner, Push-Mails etc. betreffen jedoch zunehmend auch KMU.

Die Umfrage des Certified Security Operations Center (2021) zeigt, dass im Jahr 2018 26% der mittelständischen Unternehmen Opfer eines erfolgreichen Cyberangriffs wurden, 90% der Malware als Anhang oder Link in einer E-Mail verbreitet wurde und es durchschnittlich 99 Tage dauert, bis ein Unternehmen einen Cyberangriff bemerkt.

Dabei haben 26 % aller kleinen und mittleren Unternehmen mindestens eine der folgenden Konsequenzen erlebt:

- Sie erlitten einen kompletten oder teilweisen Ausfall der IT-Systeme
- Einstellung der Produktion
- Sie konnten ihren Lieferungen/Aufträgen nicht nachkommen
- Rückkauf ihrer durch Ransomware verschlüsselten oder gestohlenen Daten
- Raub sensibler Daten
- Sie mussten sich gegenüber ihren Kunden in Bezug auf den Datenschutz rechtfertigen
- Sie erlitten einen Imageschaden

Dabei erweist sich das Bewusstsein und das Engagement der Führungsebene, die wiederum das Budget, die Zuweisung von Ressourcen und die wirksame Umsetzung der Cybersicherheitspraktiken beeinflusst, als potenzielles Grundproblem der Cybersicherheit (Proofpoint, 2022)..

Einige wichtige Probleme auch für deutsche KMU sind:

- Geringes Bewusstsein des Personals für Cybersicherheit
- Unzureichender Schutz von kritischen und sensiblen Informationen
- Fehlendes Budget
- Mangel an Cybersicherheitsexperten
- Fehlen geeigneter Cybersicherheitsrichtlinien speziell für KMU
- Schatten-IT, d.h. Verlagerung der Arbeit in ein IKT-Umfeld, das nicht der Kontrolle der KMU unterliegt
- Geringe Unterstützung durch das Management.

Argumente für Cybersicherheitsmaßnahmen (Bartels, 2020) in KMU sind:

- Die Existenzsicherung des Unternehmens
- Die Vermeidung von Strafen (es existieren eine Reihe von Gesetzen, Vorschriften und Normen, die Unternehmen einhalten müssen)
- Die Chance, Kunden zu gewinnen und im eigenen Unternehmen zu halten. Kunden erwarten, dass ihre Daten bei einem Unternehmen, dem sie diese Daten anvertrauen, sicher sind.

Cybersicherheit sollte Teil der Unternehmensstrategie werden, damit der Aspekt Sicherheit bei allen Planungsaktivitäten stets berücksichtigt, mit einem eigenen Budget versehen und kontinuierlich weiterentwickelt wird. Für den Aufbau und die Entwicklung einer effizienten und effektiven Cybersicherheitsstrategie sollten sich die Aktivitäten u. a. auf die Handlungsfelder Technologie, Prozessorganisation und Fachpersonal konzentrieren. (Hamburg, 2020).

Beispiele für das Handlungsfeld Technologie sind der Einsatz von Virenschutzprogrammen und Firewalls, das regelmäßige Ausrollen von Software-Updates und Patches. Zudem sollten regelmäßig Back-ups erstellt sowie die Spiegelung dieser Back-ups auf ein anderes Medium vorgenommen werden. Die Verwendung von Passwörtern und idealerweise sogar eine Multi-Faktor-Authentifizierung verhindert den Zugang von ungewollten Nutzern. Darüber hinaus ist die Anwendung eines rollenbasierten Berechtigungsmanagements sowie die Nutzung von Verschlüsselungsmechanismen, z. B. die Verschlüsselung von E-Mails oder aber die Nutzung einer VPN-Verbindung, essentiell (Hamburg, 2020).

Im zweiten Handlungsfeld Prozesse und Organisation wird der Fokus auf einen ganzheitlichen Ansatz der Cybersicherheit gelegt. Der Schutz vor Hackern und Cyber-Angriffen ist nicht nur die Aufgabe der IT-Verantwortlichen. Für eine funktionierende Cybersicherheit müssen Unternehmen verstärkt alle Mitarbeitenden einbeziehen. Der Faktor Mensch ist mittlerweile die größte Schwachstelle im Unternehmen, wenn es um den Schutz von Daten und IT-Systemen geht. Deswegen sollte im Handlungsfeld Fachpersonal das mittelfristige Ziel sein, in geschultes Fachpersonal mit Kenntnissen und Erfahrungen in den Bereichen IT-und Cybersicherheit sowie Datenschutz zu investieren (Hamburg, 2020).

Interdisziplinäres Training im Bereich der Cybersicherheit

Der Umgang mit Cybersecurity erfordert neben technischen Kompetenzen auch nicht-technisches Wissen über Gesetze, Vorschriften, Richtlinien und Ethik im Zusammenhang mit Cybersicherheit und Datenschutz (Hamburg, 2020).

Da nicht alle Sicherheitsfachleute sowie Führungskräfte und Mitarbeitenden einen vollumfänglichen Blick dafür haben, geeignete Maßnahmen zu entwickeln und anzuwenden, kann Fort- und Weiterbildung dazu beitragen, die Interdisziplinarität in diesem Zusammenhang

zu unterstützen. So können beispielsweise Grundlagen der technischen Cybersicherheit mit anderen Bereichen in interdisziplinären Ansätzen kombiniert werden.

Viele CybersicherheitsexpertInnen versuchen, Sicherheitsvorfälle im Rahmen ihrer Arbeit zu lösen. Sinnvoll ist es, auch darüber hinaus nach Schnittstellen zwischen den Problemen zu suchen. In diesem Zusammenhang könnte ein interdisziplinärer Ansatz Erkenntnisse aus allen Bereichen liefern, um eine integriertere und realistischere Grundlage für das Verständnis von Cybersicherheit zu erreichen (Stockmann, 2013).

Die grundlegende Frage ist, wie man in kurzer Zeit Studierende und Arbeitskräfte mit diesen interdisziplinären Fähigkeiten ausbilden kann. Die Vermittlung von Cybersicherheit in der Ausbildung erfolgt traditionell in Form von Vorlesungen und Laborübungen, in denen die Lernenden praktische Erfahrungen sammeln können. Dieser Ansatz bietet den Studierenden jedoch nicht die Möglichkeit, die komplexen und oft nicht klar definierten Probleme der Cybersicherheit in der Praxis zu erkunden. Kurse mit interdisziplinären Themen sollten so entwickelt werden, dass Studierende mit unterschiedlichem Hintergrund diese erfolgreich absolvieren können, indem sie Bildungsressourcen nutzen, die in einem offenen Format verfügbar sind. Diese Kurse sollten die Fähigkeit der Studierenden fördern, Entscheidungen, beispielsweise über die Auswirkungen der technologischen Entwicklung auf Individuen und Gesellschaften, zu treffen (Hamburg, 2020).

Zusätzlich zu solchen Lehrveranstaltungen sollten in Unternehmen interdisziplinäre Schulungen zur Cybersicherheit organisiert werden, um Cyberangriffe besser abzuwehren. Zudem sollte das menschliche Verhalten im Fokus stehen und kreative Denkfähigkeiten entwickelt werden, um Aktivitäten der Hacker-Community zu vermeiden und jegliche Formen von Angriffen zu erkennen und zu bekämpfen. Es ist bekannt, dass ein Großteil der Vorfälle im Bereich der Cybersicherheit auf Entscheidungen oder Verhaltensweisen von Menschen zurückzuführen ist (Lebek et al., 2014). Zwar konzentriert sich ein technischer Ansatz der Cybersicherheit darauf, wie die Technologie zur Vermeidung von Cyberangriffen eingesetzt werden kann. Jedoch ist auch ein humanzentrierter Ansatz erforderlich, der sich auf die Fragen und komplexen Probleme konzentriert, die mit der weit verbreiteten Integration von Technologie in das tägliche Arbeitsleben (Hamburg, 2020).

Das Erasmus+ Projekt InCyT (Interdisciplinary Cyber Training)

Das zweijährige Erasmus+ Projekt *InCyT* wird vom IAT der Westfälischen Hochschule Gelsenkirchen koordiniert. Die Partner sind Paydas Egitim Kultur VE Sanat Dernegi, Zonguldak in der Türkei, SC IPA SA CIFATT Craiova in Rumänien, European Training Center Copenhagen in Dänemark, MAG - UNINETTUNO S.R.L. in Italien, Politechnika Rzeszowska (PRz) in Polen und die Fachhochschule St. Pölten in Österreich. Die Zusammenarbeit und Kommu-

nikation zwischen TrainerInnen, ForscherInnen und AnwenderInnen von Informationstechnologien sind von Bedeutung. Ein Problem besteht darin, dass Unternehmen, insbesondere KMU, mit geringen Ressourcen Unterstützung bei der Bewertung der Fähigkeiten und Qualifikationslücken ihrer Angestellten, bei der Nutzung digitaler Methoden zur Verbesserung der bestehenden Situation und bei der Organisation von Ausbildungsmöglichkeiten zur Umschulung ihrer Angestellten benötigen. Die folgende Abbildung zeigt einige Aktivitäten, die durch das Projekt unterstützt werden.

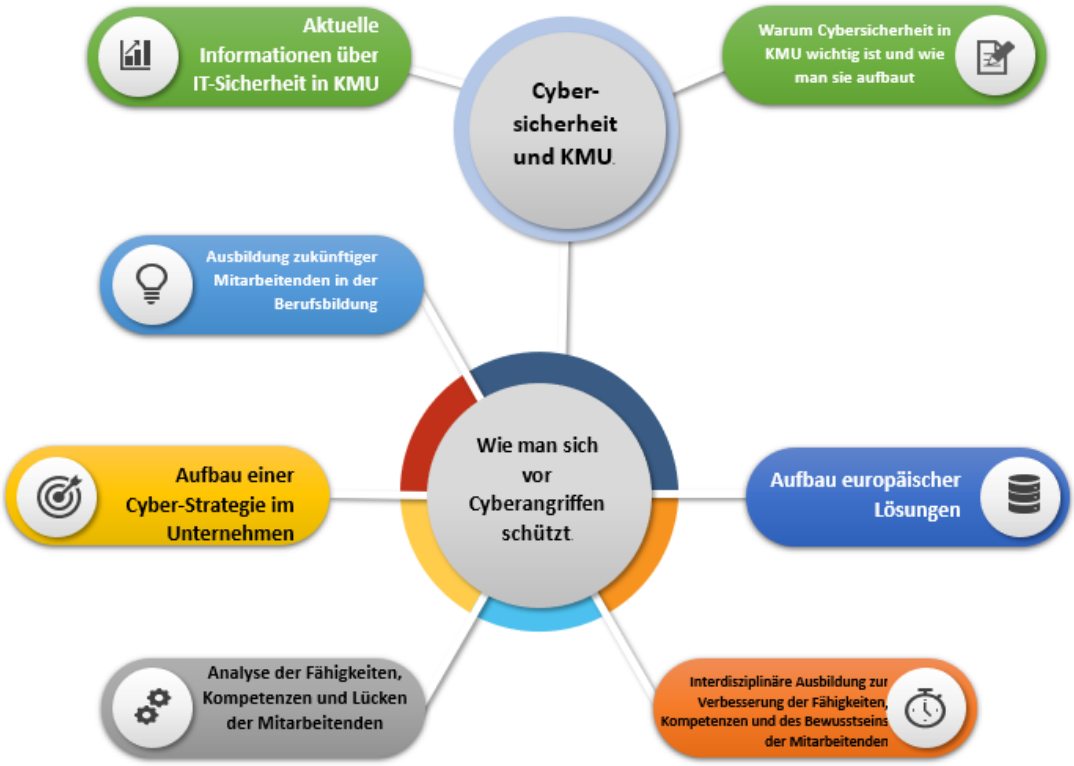

Abb.1: Projektaktivitäten, eigene Darstellung

Das Projekt *InCyT* fokussiert sich entsprechend auf Cybersicherheit für kleine und mittlere Unternehmen (KMU) sowie Berufs- und Ausbildungseinrichtungen und auf das Ziel wie man Cyberangriffe insbesondere durch geeignete Schulungen abwehren oder verhindern kann.

Die Ziele des *InCyT*-Projekts, von denen einige bereits verwirklicht wurden, sind die folgenden:

- Es wurde ein Cybersecurity-Kompetenzrahmen entwickelt, der in der beruflichen Bildung und in Unternehmen eingesetzt werden kann. Der von den EU-Projektpartnern entwickelte Kompetenzrahmen wird unter Berücksichtigung der Besonderheiten der KMU in den Partnerländern und der europäischen Gesetzgebung kontinuierlich aktualisiert. Dieser soll als Plattform für Angebot und Nachfrage von Cybersicherheitsfähigkeiten und -kompetenzen dienen.

- Ein digitales interdisziplinäres Training und ein Mentoring für KMU-Manager und Mitarbeitende, unterstützt durch eine interaktive digitale Plattform (www.incytproject.eu/elearning/), befinden sich in der Testphase.
- Der Schwerpunkt wird auf der Praktikabilität liegen. Besonderes Augenmerk wird daraufgelegt, eine breite Akzeptanz bei Mitarbeitenden, Führungspersonal und CyberberaterInnen von KMU zu schaffen und das Projekt in den Partnerländern erfolgreich umzusetzen.
- Darüber hinaus werden Unternehmen und Berufsbildungseinrichtungen dabei unterstützt, den Ist-Zustand und die notwendigen Qualifikationen zu analysieren, um entsprechende Maßnahmen in den Organisationen und Ausbildungsgängen zu ergreifen.
- Eine angepasste Version für die berufliche Bildung (VET) und ein europäisches Übertragbarkeitsmodell werden entwickelt und getestet.

Von Beginn des Projekts an wurden Informationen an KMUs in ganz Europa verbreitet und insbesondere Unternehmen aus den Partnerländern des Projekts dazu ermutigt, Netzwerke aufzubauen, die es ihnen ermöglichen, zusammenzuarbeiten, um Cyberangriffe zu vermeiden.

Neben der Literaturrecherche bilden Interviews mit IT-BeratungsexpertInnen für Cybersicherheit die zweite Quelle, um einen Überblick über Cybersicherheitsprobleme in KMU zu erhalten. Bei den ExpertInnen handelt es sich um Fachleute, die die Unternehmen bei der Vermeidung von Cyberangriffen unterstützen. In jedem Partnerland wurden IT-BeratungsexpertInnen befragt, um detaillierte Einblicke in die Cybersicherheit von KMU, ihre Probleme und ihre Bedürfnisse zu erhalten.

In jedem Partnerland wurde ein fünfseitiger Bericht erstellt, der die Dimensionen der Cybersicherheitsprobleme in KMU aufzeigt. Darüber hinaus wurde eine Übersicht über Unterstützungsprogramme mit Links und einer kurzen Beschreibung des Inhalts dieser Links erstellt, wo die BesucherInnen des Projektportals über die Trainingsmodule im Rahmen des Projekts hinaus vertiefende Informationen erhalten. Ein länderübergreifender Bericht war ein wichtiger Output, der auf Sekundärforschung in den Partnerländern und den thematischen Ergebnissen von ExpertInneninterviews basierte. Die Zusammenfassung des Berichts wurde auf dem Projekt-Webportal in allen Partnersprachen für ein breites Publikum veröffentlicht.

Das Trainingsprogramm

Nach den Interviews und Kurzstudien, die zu Beginn des Projekts durchgeführt wurden, ist das Programm in zwei Module gegliedert, eines für Führungskräfte und eines für Mitarbeitende, wobei jedes Modul eine Reihe von Einheiten und Themen umfasst.

Die entwickelten Trainingsmodule sind die folgenden:

1. Einführung in die Informationssicherheit, interne Kontrollsysteme
2. Grundlagen der Kryptographie
3. Schadsoftware
4. Sicherheit auf Geschäftsreisen
5. Privatsphäre und Datenschutz
6. Social Engineering / SPAM / Phishing
7. Sicherheit und Datenschutz in sozialen Netzwerken
8. Management der Informationssicherheit
9. Sicherheit von Dritten/Anbietern
10. Cyber-Risiko und Resilienz

Das Training wird über eine interaktive digitale Plattform, Streaming-Webinare, sowie über Selbsteinschätzungsübungen und Diskussionsforen durchgeführt, in denen die Antworten veröffentlicht werden. Jede Woche hält ein(e) MentorIn eine Sitzung mit den Lernenden ab, um ihnen zu helfen und Feedback zu geben, aber auch selber zu erhalten. Dies wird, neben speziellen Übungen, zur Entwicklung des kritischen Denkens der Lernenden beitragen. Die von den Lernenden in den Diskussionsforen gespeicherten Problemlösungen werden anschließend in Gruppen diskutiert.

Zwei Module, die im Rahmen von *InCyT* entwickelt wurden, befassen sich mit Social Engineering und Social Networking und werden aufgrund ihrer Relevanz hier näher vorgestellt. Social Engineering bezieht sich auf ein breites Spektrum an Malware-Aktivitäten, die durch menschliche Interaktionen durchgeführt werden. Es nutzt psychologische Manipulationstrategien, um BenutzerInnen dazu zu bringen, Sicherheitsfehler zu begehen oder sensible Informationen preiszugeben. Social Engineering ist eine effektive Form von Cyber-Angriffen. Ein erfolgreicher sozialer Angriff kann erhebliche Folgen haben. Social-Engineering-Training, das häufig Teil von Programmen zur Förderung des Sicherheitsbewusstseins ist, vermittelt den Mitarbeitenden das Wissen und die Werkzeuge, die sie benötigen, um diese Arten von Angriffen zu erkennen und sich selbst und ihr Unternehmen zu schützen (Weßelmann, 2008). Es ist notwendig, einen interdisziplinären Ansatz zu verwenden, um Social Engineering und seine Komplexität zu verstehen. In der Literatur werden Perspektiven aus verschiedenen Disziplinen beleuchtet, wie beispielsweise aus der Informationstechnologie, Psychologie, Wirtschaft und Ethik. Abbildung 2 veranschaulicht diese Sichtweise (Washo, 2021).

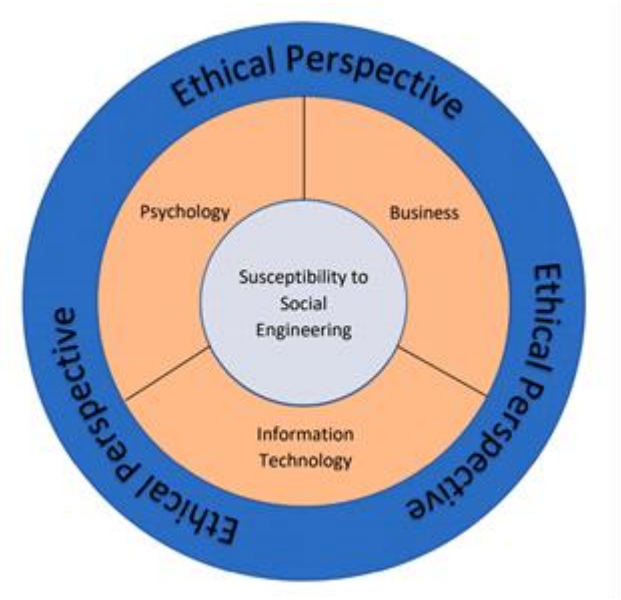

Abb. 2: Social Engineering aus interdisziplinärer Sicht (Washo, 2021)

Phishing ist eine der beliebtesten Arten von Social-Engineering-Angriffen; Phishing-Betrügereien sind E-Mail- und SMS-Kampagnen, die darauf abzielen, bei den Opfern den Eindruck von Dringlichkeit zu erwecken sowie Neugier oder Angst zu erzeugen. Eine PBL-Übung in diesem Modul befasste sich mit dem Erstellen und Starten von Phishing-Angriffen und der Untersuchung von Maßnahmen, wenn Phishing-E-Mails eintreffen. Die Lernenden können die kollaborative Projektplattform und auch andere webbasierte Software nutzen, die es mehreren BenutzerInnen ermöglicht, gleichzeitig zu arbeiten und zu kommentieren.

Ein weiteres Trainingsmodul befasst sich mit sozialen Netzwerken. Mit der schnell wachsenden Technologie haben soziale (online) Netzwerke in den letzten Jahren an Popularität gewonnen. Ein Grund dafür ist ihre Fähigkeit, den NutzerInnen eine Plattform für die Kommunikation zu bieten. Soziales Networking bezieht sich auf die Nutzung von internetbasierten Social-Media-Sites, um mit FreundInnen, Familie, KollegInnen, KundInnen oder KlientInnen in Verbindung zu bleiben.

Der interdisziplinäre Bereich, der sich mit der Untersuchung sozialer Netzwerke befasst, ist die soziale Netzwerkanalyse (SNA) und umfasst Erkenntnisse aus anderen Disziplinen wie beispielsweise der Soziologie, Anthropologie, Psychologie und Kommunikation. SNA ist Teil einer interdisziplinären Studie, die sich auf alle Arten von Netzwerken bezieht. Netzwerkwissenschaft umfasst dabei die Arbeiten aus der Physik, der Informatik, den Datenwissenschaften, der Biologie, dem Ingenieurwesen, der Mathematik und anderen Bereichen. Die Beziehung zwischen diesen Bereichen ist in Abbildung 3 dargestellt.

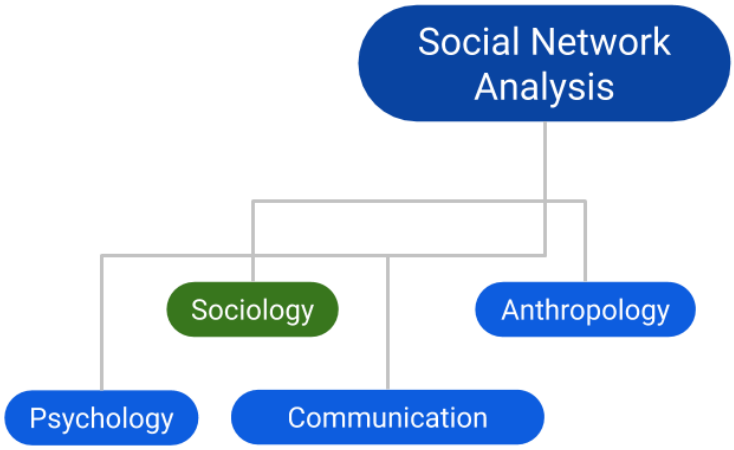

Abb. 3: Soziale Netzwerkanalyse (SNA), (Lizardo, o.J.)

Am Ende des *InCyT*-Trainings sollen die Lernenden ein elektronisches Portfolio erstellen, um ihre Arbeit zu organisieren und ihre Lernerfahrungen zu präsentieren. Diese dienen als Bewertungsinstrumente für die Ausbildung, bieten den Lernenden die Möglichkeit, über das Gelernte zu reflektieren, und geben den ArbeitgeberInnen die Möglichkeit, einzusehen, was die TeilnehmerInnen gelernt haben.

Den Lernenden wurden u.a. die nachfolgenden Fragen gestellt: Was hat Ihnen an der Schulung am besten gefallen? Was hilft Ihnen am meisten, die Inhalte zu lernen? Waren die Materialien und die digitale Plattform einfach zu verwenden? Können Sie die erlernten Fähigkeiten und Kenntnisse in Ihrem Beruf anwenden?

Fazit

Cybersicherheit ist aufgrund der vielen Cyberangriffe, der intensiven Nutzung von Technologien und der entsprechenden Qualifikationslücken der ArbeitnehmerInnen ein wichtiges Thema in Unternehmen. Dabei sind besonders KMU aufgrund von mangelnden Ressourcen und fehlenden Cyber-Sicherheitsstrategien Ziel von Cyberangriffen. Als Reaktion darauf wird in der Überprüfung der Cybersicherheitspolitik eine nationale Strategie gefordert, um das Bewusstsein für das Thema zu schärfen und cybersichere Arbeitskräfte auszubilden, die über Fachwissen und Fähigkeiten verfügen, um potenzielle Bedrohungen abzuwehren. Die Cybersicherheit wird vielfach erforscht, jedoch im Vergleich zu anderen Bereichen in der Praxis nicht ausreichend berücksichtigt. Sie ist in der traditionellen Informatik verwurzelt, hat aber Verbindungen zu anderen Disziplinen. Die Dringlichkeit, sich schnell gegen Cyber-Kriminalität zu schützen, macht es notwendig, interdisziplinäre Wege und die Zusammenarbeit zwischen Disziplinen und Menschen auch in der Bildung und Ausbildung

zu berücksichtigen. Das Erasmus+ Projekt *Interdisciplinary Cyber Training (InCyT)* mit Partnern aus sieben europäischen Ländern leistet einen Beitrag dazu, die Relevanz von Cybersicherheit und interdisziplinären Lösungsansätzen für KMU zu verdeutlichen.

Literatur

Bartels, S. (2020). Cyber Security für KMUs: IT-Sicherheit leicht gemacht. Online verfügbar unter: https://fortschritt.co/index.php/blog-de/180-cyber-security-fuer-kmus-it-sicherheit-leicht-gemacht.

Bendel, O. (2022). Cybersecurity Definition: Was ist "Cybersecurity"? Gabler Wirtschaftslexikon. Online verfügbar unter: https://wirtschaftslexikon.gabler.de/definition/cybersecurity-99856.

Braun, S. (2020). Mittelstand im Überblick - Volkswirtschaftliche Bedeutung der KMU. Online verfügbar unter: https://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/volkswirtschaftliche-bedeutung-der-kmu/deutschland.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022). Die Lage der IT-Sicherheit in Deutschland 2022. Online verfügbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

CSOC – Certified Security Operations Center (2021). Cyber-Sicherheitsreport 2021. Online verfügbar unter: https://www.csoc.de/cybersicherheitsreport-2021/

Dreißigacker, A., von Skarczinski, B. & Wolliner, G. R. (2020). Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Bundesministerium für Wirtschaft und Energie.

Engemann, P., Fischer, D., Gosdzik, B., Koller, T. & Moore, N. (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. Online verfügbar unter: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf.

Europäische Kommission (2003). EMPFEHLUNG DER KOMMISSION vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Online verfügbar unter: https://www.ifm-bonn.org/definitionen/kmu-definition-der-eu-kommission.

Hamburg I. (2020). Creating innovative structures in workplace and vocational digital learning to ensure social distancing, ICDS 2020: The fourteenth international conference on digital society 3. 124-127.

Hamburg, I. (2021). Approaches to support learning in today's workplace. In: VI International Scientific Conference Winter Session: Industry 4.0. 8-11 December 2021, Borovets, Bulgaria, 284-288.

Knirsch, R. (2019). Telekom legt aktuelle Zahlen zur Cybersicherheit vor. Online verfügbar unter https://www.telekom.com/de/medien/medieninformationen/detail/telekom-legt-aktuelle-zahlen-zur-cybersicherheit-vor-573046.

Lebek B., Uffen, J., Neumann, M., Hohler B. & Breitner, M.H. (2014). Information Security Awarness and Behavior: A Theory-Based Literature Review. Management Research Review, 37, 1049-1092.

Lizardo, O. (o.J.). What is A Social Network? Online verfügbar unter: https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html.

Petersen, R., Santos, Danielle, Smith, M.C., Wetzel, K.A. & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181.

Proofpoint (2022). Cybersecurity: The 2022 Board Perspective. Board director views on the global threat landscape, cybersecurity priorities and CISO relations. Online verfügbar unter: https://cams.mit.edu/wp-content/uploads/Board-of-Directors-Cyber-Attitudes.pdf

Stockman, M. (2013). Infusing Social Science into Cybersecurity Education. Proceedings of the 14th Annual ACM SIGITE Conference on Information Technology Education. 121-124.

Streim, A. & Mann, S. (2021). Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr. Online verfügbar unter:https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr.

techconsult (2019). IT-Sicherheit im Mittelstand. Online verfügbar unter: https://www.techconsult.de/studie-it-sicherheit-mittelstand.

Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. Online verfügbar unter:https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research .

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. Datenschutz und Datensicherheit. DuD. 601–604.

Autoren:

Dr. Ileana Hamburg ist Research Fellow im Forschungsschwerpunkt Arbeit und Wandel des Instituts Arbeit und Technik.

David Sommer ist Wissenschaftliche Hilfskraft im Forschungsschwerpunkt Arbeit und Wandel des Instituts Arbeit und Technik.

Kontakt: hamburg@iat.eu, sommer@iat.eu

Forschung Aktuell

ISSN 1866 – 0835

DOI: https://doi.org/10.53190/fa/202212

Institut Arbeit und Technik der Westfälischen Hochschule

Gelsenkirchen – Bocholt – Recklinghausen

Redaktionsschluss: 01.12.2022

https://www.iat.eu/publikationen/forschung-aktuell.html

Redaktion

Claudia Braczko

Tel.: 0209 - 1707 176 Institut Arbeit und Technik

Fax: 0209 - 1707 110 Munscheidstr. 14

E-Mail: **braczko@iat.eu** 45886 Gelsenkirchen

IAT im Internet: **http://www.iat.eu**