Co-funded by the
Erasmus+ Programme
of the European Union

VERBESSERUNG DER CYBERSECURITY-BEREITSCHAFT DES EUROPÄISCHEN BERUFSBILDUNGSSEKTORS

CYBER.EU.VET

INTELLEKTUELLER OUTPUT IO 3

TOOLKIT FÜR FORTBILDUNG UND TRAINING

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

Einleitung

Die Partner des CYBER.EU.VET-Projekts haben dieses Toolkit - bestehend aus 6 Modulen und Materialien - zur Fortbildung von Lehrkräften erarbeitet. Es kann von Lehrern und Ausbildern im Berufsbildungssektor verwendet werden. Jedes Modul umfasst einen theoretischen Teil, praktische Beispiele und Aufgaben für die Arbeit in Gruppen. Das Schulungsformat kann in verschiedenen europäischen Ländern eingesetzt werden und sollte gegebenenfalls an die lokalen Bedarfe und Bedingungen angepasst werden. Anpassungen könnten sich vor allem auf die praktischen Beispiele und Fallstudien beziehen, die das Schulungsformat enthält.

DIE TRAININGSMODULE WURDEN VON DEN PARTNERN WIE FOLGT ENTWICKELT:

CYBERANGRIFFE

Modul 1

Überblick

Zielgruppe

- Lehrkräfte und Ausbilder in der Erwachsenenbildung
- Studierende
- Vertreter relevanter Organisationen oder Initiativen (NRO, nationale und regionale Behörden, Bildungseinrichtungen)

Modulbeschreibung

In Anbetracht der jährlich wachsenden Zahl und des Ausmaßes von Cyberangriffen, insbesondere vor dem Hintergrund der jüngsten wirtschaftlichen, politischen und sozialen Entwicklungen (die Folgen der Covid-19-Beschränkungen, der militärische Konflikt in der Ukraine usw.), ist es wichtig, sich häufiger mit aktuellen Cyberangriffen zu befassen.

Ziel des Moduls ist es daher, ein grundlegendes Verständnis für Cyberangriffe zu vermitteln und zu lernen, wie auf mögliche Vorfälle reagiert werden kann.

Der Inhalt dieses Moduls umfasst die folgenden Aspekte (Einheiten):

- Definition und relevante Themen
- Typologie
- Die meisten aktuellen Vorfälle (praktische Beispiele)
- Wie man sich vor Cyberangriffen schützt und auf Vorfälle reagiert

Am Ende jeder Einheit ist eine praktische Übung vorgesehen.

Lernziele

- Vermittlung eines grundlegenden Verständnisses von Fragen im Zusammenhang mit Cyberangriffen.
- Die Folgen und Auswirkungen möglicher Cyberangriffe und -bedrohungen zu verstehen.
- Die häufigsten Formen von Cyberangriffen zu erkennen und zu klassifizieren.
- Wissen, wie man auf Angriffe reagiert - wo man sich melden muss, wenn ein Vorfall eintritt.
- Informationsquellen und Literatur für weiteres und detaillierteres Lernen, für die Verfolgung tatsächlicher Cyberangriffe und für Schutzmöglichkeiten zu sichern.

Gesamtdauer

Maximal 1,5 Stunden

CYBER-ANGRIFFE

Modul 1

Dieses Modul wird vom Ausbilder in Form einer PowerPoint-Präsentation gehalten, die theoretisches Wissen vermittelt und durch visuelle Elemente, praktische Beispiele und Übungen ergänzt wird (max. 20 Minuten + eine praktische Aktivität pro Einheit).

Es wird empfohlen, die Präsentationen anhand der auf das CYBER.EU.VET-Projekt zugeschnittenen PPT-Vorlagen vorzubereiten. In Anbetracht der rasanten Entwicklungen und Fortschritte im Bereich der Cybersicherheit wird empfohlen, die Lerneinheiten laufend zu überprüfen und den Inhalt bei Bedarf an die neuesten Entwicklungen in diesem Bereich anzupassen.

Darüber hinaus wird den Ausbildern empfohlen, dieses Modul an die Bedarfe ihrer lokalen Berufsbildung anzupassen und Beispiele für aktuelle Vorfälle in der Region einzubeziehen. Dieses Modul behandelt hauptsächlich praktische Beispiele aus Lettland sowie einige internationale Beispiele. Es wird empfohlen, einen größeren Fokus auf Einheit 3 zu legen, um praktische Beispiele von Vorfällen zu analysieren und zu diskutieren, zusammen mit Bildern und Videos.

Einheit 1 - Cyberangriffe

Was bedeutet das? Einführung in das Thema

Lernaktivität 1 - Theorie

DEFINITION UND BEDEUTUNG

Cyberangriff (pl. cyber attacks) = ein Versuch, sich illegal und unbefugt Zugang zu einem Computer oder Computersystem zu verschaffen, um diesem Schaden zuzufügen. Ziel ist es, Computersysteme zu deaktivieren, zu stören, zu zerstören oder zu kontrollieren oder die in diesen Systemen gespeicherten Daten zu verändern, zu blockieren, zu löschen, zu manipulieren oder zu stehlen.

Mit dem Aufkommen der Covid-19-Beschränkungen und der Notwendigkeit, zu einer digitalen Arbeits- und Lernform überzugehen, hat die Zahl der Cyber-Bedrohungen und -Angriffe zugenommen und der digitale Schutz ist wichtiger geworden.

Der Begriff "Cyberangriff" steht in engem Zusammenhang mit Begriffen wie "Cyberbedrohung" (Möglichkeit, dass ein bestimmter Angriff stattfindet) und "Cyberrisiko".

Die häufigsten Cyber-Angriffe: Malware-Angriff, Phishing-Angriff, Man-in-the-Middle-Angriff, Passwort-Angriff, Denial-of-Service-Angriff und viele mehr.

Arten der Kommunikation der Angreifer: persönliche Kontakte, Telefon, elektronische Post, Malware.

QUELLE: https://cert.lv/lv/2022/02/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs; https://www.investopedia.com/terms/c/cybersecurity.asp

Wer kann Cyberangriffe durchführen?

Ein Cyberangriff kann von jedem Ort der Welt aus von jeder Einzelperson oder Gruppe mit einer oder mehreren verschiedenen Angriffsstrategien gestartet werden und kann sich gegen Einzelpersonen, öffentliche oder private Unternehmen (Firmen) richten.

Warum gibt es Cyberangriffe und was können sie bewirken?

Bei Angriffen in der virtuellen Umgebung geht es in der Regel um Identitätsdiebstahl, Aneignung von Computerressourcen, Informationsdiebstahl und -fälschung, Zugang zu Geschäftsgeheimnissen, Erpressung oder Verleumdung. Cyberangriffe zielen hauptsächlich auf finanziellen Gewinn (z. B. Diebstahl von Kreditkartennummern und -codes), Störung und Rache (z. B. Schädigung des Rufs einer Organisation) ab.

So werden beispielsweise Krisen wie Covid-19 oder der militärische Konflikt in der Ukraine genutzt, um die Aufmerksamkeit der Nutzer durch betrügerische E-Mails und Meldungen in den sozialen Medien zu gewinnen.

STATISTIKEN

Die durch die Pandemie erzwungene Fernarbeit hat offensichtlich die Cybersicherheitsrisiken erhöht und neue Arten von Vorfällen begünstigt. Die meisten von ihnen sind auch für Bildungseinrichtungen relevant und sollten bei Weiterbildungs- und Schulungsaktivitäten für Pädagogen und Jugendliche berücksichtigt werden.

Gemäss den von Deloitte analysierten Informationen fanden im April 2020 in der Schweiz 350 Cyberangriffe statt, verglichen mit einer Norm von 100 - 150 Cyberangriffen (Phishing, betrügerische Websites, direkte Angriffe auf Unternehmen usw.).

Die Zunahme der Telearbeit erfordert einen stärkeren Fokus auf die Cybersicherheit, da sie ein größeres Cyberrisiko darstellt. Dies zeigt sich beispielsweise daran, dass 47 % der Menschen bei der Heimarbeit auf einen Phishing-Betrug hereinfallen.

In Lettland beispielsweise wurde die höchste Anzahl bedrohter eindeutiger IP-Adressen in Lettland von Februar bis April 2020 festgestellt, als die Covid-19-Pandemie begann (über 10.000 pro Monat), so das CERT.LV (Information Technology Security Incident Response Institution of Latvia), das monatlich und jährlich Daten und einen Überblick über die wichtigsten Vorfälle unter der Bezeichnung "Kiberlaikapstākļi" (Cyber-Wetter) veröffentlicht.

QUELLE: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

INTERAKTIVES TOOL: Die Live-Cyber-Bedrohungskarte (weltweit)

Lernaktivität 1 - Praktische Übung

Diskussion mit den Teilnehmern über ihre Erfahrungen mit Cyberangriffen (10-15 Minuten): 1) Welche Arten von Cyberangriffen kennen Sie?

2) Haben Sie oder Verwandte/Freunde jemals einen Cyberangriff/Cybervorfall erlebt? Wie ist es ausgegangen?

Einheit 2 - Arten von Cyberangriffen

Lernaktivität Nr. 2 - Theorie

Die häufigsten Methoden (Arten) von Cyberangriffen

Malware ist eine bösartige Software (Würmer, Viren), die verwendet wird, um die Geräte (Computer, Telefone usw.) oder das Netzwerk des Benutzers zu schädigen. Beispiele für Malware: Spyware und Trojaner, Würmer, Viren, Adware, Spam. Je nach Art des bösartigen Codes kann Malware von Hackern verwendet werden, um sensible Daten zu stehlen oder heimlich zu kopieren, Daten zu löschen, den Zugriff auf Dateien zu blockieren, den Systembetrieb zu stören oder Systeme funktionsunfähig zu machen [DigiCERT].
Malware wird hauptsächlich zu zwei Zwecken verbreitet - um Informationen zu erhalten (Spionage-Malware, die Daten vom Gerät des Opfers weiterleitet) oder um Profit zu machen (Verschlüsselungs-Ransomware, die Daten auf dem Gerät des Benutzers verschlüsselt und später ein Lösegeld vom Benutzer verlangt) [CERT Report 2020].

Phishing oder Personal Data Scams - eine Methode, bei der ein Hacker eine scheinbar seriöse E-Mail verschickt und Benutzer auffordert, vertrauliche Informationen preiszugeben. Die Empfänger werden dazu verleitet, die in der E-Mail enthaltene Malware herunterzuladen, indem sie entweder eine angehängte Datei oder einen eingebetteten Link öffnen. In der Regel handelt es sich dabei um Websites, die wie echte Unternehmen aussehen, und die Benutzer müssen ihre persönlichen Daten (Bankkonto, Kreditkartennummern und Passwörter, einschließlich derer von Authentifizierungsdiensten) eingeben. Der Datenbetrug kann auch per Telefonanruf oder über WhatsApp-Nachrichten erfolgen [Investopedia].

Denial of Service (DoS) - Hacker bombardieren die Server einer Organisation mit großen Mengen gleichzeitiger Datenanfragen, bis das Ziel nicht mehr reagieren kann oder abstürzt, so dass die Server keine legitimen Anfragen mehr bearbeiten können. Infolgedessen ist der Zugriff auf den Dienst für die Systembenutzer nicht mehr möglich. DoS-Angriffe können von einigen Stunden bis zu vielen Monaten dauern und Unternehmen Zeit und Geld kosten, während ihre Ressourcen und Dienste nicht verfügbar sind [Investopedia].

Man-in-the-Middle - Angreifer schieben sich heimlich zwischen zwei Parteien, z. B. einen einzelnen Computernutzer und ein Finanzinstitut. Je nach den Einzelheiten des tatsächlichen Angriffs kann diese Art von Angriff genauer als Man-in-the-Browser-Angriff, Monster-in-the-Middle-Angriff oder Machine-in-the-Middle-Angriff klassifiziert werden. In diesem Fall fängt der Angreifer Daten ab, löscht oder verändert sie, während sie von einem Computer, Smartphone oder einem anderen verbundenen Gerät über ein Netzwerk übertragen werden [Investopedia, TechTarget].

Lernaktivität Nr. 2 - Praktische Aktivität

Gruppendiskussion - welche Merkmale deuten auf Angriffe/Betrugsversuche hin? (10 -15 min)

- Die Teilnehmer haben 10 Minuten Zeit, um die Merkmale aufzuschreiben
- Diskussion über die Ergebnisse

Lektion 3 - Beispiele für Bedrohungen und Angriffe

Wie lassen sich Bedrohungen erkennen?

Lernaktivität Nr. 3 - Theorie

Beispiele für Cyberangriffe (vor dem Hintergrund des Krieges in der Ukraine)

Betrügerische E-Mails in englischer Sprache, in denen zur Unterstützung einer der Parteien des militärischen Konflikts - Ukraine oder Russland - aufgerufen wird. Die Unterstützung kann durch den Kauf von Stimmen und die Stimmabgabe gezeigt werden - ein Betrug, der darauf abzielt, die Zahlungskartendaten der Nutzer zu stehlen (siehe Druckbild).

VIDEO - Wie Betrüger Spenden für den Ukraine-Krieg ergaunern - BBC News

ARTIKEL - 4 Arten von Betrügereien im Russland-Ukraine-Krieg, die auf Verbraucher abzielen

Beispiele auf der Grundlage der wichtigsten Vorfälle in Lettland (2020-2021) und anderer internationaler Fallbeispiele (gefolgt von visuellen Beispielen)

Malware

Die Covid-19-Situation wurde genutzt, um Malware zu verbreiten: z. B. E-Mails im Namen der Weltgesundheitsorganisation (WHO) mit dem Hinweis, der Anhang enthalte die neuesten Informationen über Covid-19; Links zu Diagrammen, die die Verbreitung von Covid-19 zeigen und deren Funktion darin besteht, Benutzerdaten zu stehlen; bösartige E-Mails an Gesundheitseinrichtungen zur Lieferung von Covid-19-Schutzausrüstung usw.

Die Verbreitung der weltweit gefährlichsten Malware Emotet, sowohl in globalen als auch in lettischen Netzwerken, zielt auf den Diebstahl sensibler Daten ab und geht in der Regel von einer E-Mail eines bereits infizierten Kontakts aus. Emotet dient als Türöffner für andere Computer und ermöglicht den unbefugten Zugriff auf andere Malware-Familien. Mehr als 200 lettische Unternehmen wurden infiziert.

Phishing oder Betrug mit persönlichen Daten

Die meisten Fälle betrafen den Betrug mit E-Mail- und Office-365-Daten, den Erwerb von Bank- und internationalen Zahlungssystemen (einschließlich Smart-ID - elektronisches Authentifizierungstool in Lettland), Zugangsdaten und den Betrug mit Zugangsdaten zu Konten in beliebten sozialen Medien (Facebook und Instagram). Das Covid-19-Thema wurde häufig verwendet, um die Aufmerksamkeit der Nutzer in betrügerischen E-Mails und Ankündigungen in sozialen Medien zu gewinnen.
Während der Pandemie wurden verstärkte Versuche des Datenbetrugs unter Verwendung der Marken von Paketzustelldienstleistern (Latvijas Pasts, DHL, Omniva, DPD, AliExpress usw.) beobachtet. Außerdem wurden innovative Angriffe beobachtet, z. B. ein Angriff auf die Zugriffsrechte von Office 365, der mit technischen Mitteln nur schwer zu erkennen war, da keine böswilligen Aktionen auf dem Gerät des Opfers durchgeführt wurden, sondern die Angriffe innerhalb von Office 365 erfolgten.

VIDEO Phishing (mit englischen Untertiteln)

Betrug

Intensive Betrugsversuche, einschließlich Social-Engineering-Angriffe. Die meisten Betrugsversuche zielten darauf ab, Zugangsdaten für Zahlungskarten der Bürger, finanzielle Mittel sowie E-Mail-Zugangsdaten zu erlangen. Die Angreifer verschickten betrügerische E-Mails und Textnachrichten an die Bevölkerung und führten betrügerische Telefonanrufe durch, wobei sie sich meist als Vertreter von Banken oder E-Mail-Anbietern ausgaben. Mehrere Unternehmen wurden durch BEC-Angriffe geschädigt und erlitten einen Gesamtschaden von fast 200.000 €.
Die Frage der Warenlieferung war auch Gegenstand von Betrugsversuchen gegenüber Verkäufern, die Informationen über den Verkauf von Waren auf Werbeportalen veröffentlichten. Unter dem Vorwand, interessierte Käufer zu sein und die Kommunikationsplattform WhatsApp zu nutzen, äußerten die Betrüger den Wunsch, das Produkt zu kaufen, als ob sie die Dienste eines Kurierdienstes in Anspruch nehmen würden, und forderten die Verkäufer auf, auf den gefälschten Websites von Omniva, DPD und später Latvijas Pasts Kartendaten einzugeben, um sowohl den CVV-Code als auch den Saldo zu erfahren. Die Angreifer benutzten angepasste Website-Adressen (Domänen), die den Original-Website-Adressen ähnlich waren, um die Öffentlichkeit in die Irre zu führen.

Die Angreifer versuchten auch, an Zahlungskartendaten zu gelangen, indem sie E-Mails schickten, in denen sie dazu aufforderten, ein Bitcoin-Guthaben zu beantragen, indem sie sich bei einem betrügerischen Kryptowährungsaustauschdienst anmeldeten.
Bei den aktivsten Versuchen handelte es sich um Erpressungskampagnen, bei denen die Hacker behaupteten, das Gerät eines Nutzers gehackt und kompromittierendes Material erhalten zu haben, für das ein Lösegeld gefordert wurde; betrügerische Gewinnspiele im Namen bekannter Marken, bei denen die neuesten Smartphones oder andere wertvolle Preise zu gewinnen waren.

WEITERE BEISPIELE

Irreführende Werbung in sozialen Medien - unter Verwendung der Namen berühmter lettischer Persönlichkeiten wurden Internetnutzer ohne deren Wissen aufgefordert, in Kryptowährungen zu investieren. Betrüger riefen auch an und versuchten, die Menschen zu Investitionen zu überreden. In einigen Fällen wurden wiederholte Betrugsversuche beobachtet, bei denen den Opfern von Finanzbetrug Hilfe angeboten wurde, um ihre verlorenen Mittel zurückzubekommen.

Telefonbetrug - indem sie die Telefonnummern verschiedener Kreditinstitute fälschten und sich als Bankvertreter ausgaben, nutzten die Betrüger das mangelnde Wissen der Öffentlichkeit über zusätzliche Authentifizierungsmethoden, um mehreren Tausend Nutzern finanzielle Mittel zu entziehen und den lettischen Kreditinstituten einen Gesamtschaden von Hunderttausenden von Euro zuzufügen.

Auch die Hacker passen sich an die Verbreitung der Fernarbeit an: Angesichts der Notwendigkeit für Unternehmen, schnell auf Fernarbeit umzustellen, und der Einführung des elektronischen Dokumentenverkehrs nutzen Hacker diese Situation, um ihre Angriffe anzupassen. So erhielten z. B. mehrere Buchhalter des Unternehmens E-Mails im Namen des Geschäftsführers oder eines anderen Mitarbeiters, um eine dringende Zahlung vorzunehmen oder das Lohnkonto zu ändern.

Lettland und Litauen nehmen 108 Personen wegen millionenschwerem Callcenter- Betrug fest

Eingriffe in die Geschäftskorrespondenz von Unternehmen - durch die Kompromittierung der E-Mails von Unternehmen oder deren Kooperationspartnern wählen Angreifer einen geeigneten Zeitpunkt, um einer der Parteien eine Rechnung mit einem geänderten Konto zu schicken.

Betrügerische Nachrichten - Angreifer versuchen, WhatsApp-Konten abzufangen, indem sie einen sechsstelligen Code verlangen, der versehentlich an die Telefonnummer des Empfängers gesendet wird. Da eine Nachricht von den Personen in Ihrer Kontaktliste empfangen wird, übertragen einige Personen ihre Codes und verlieren so den Zugang zu ihrem WhatsApp-Konto. Die Verwendung der Zwei-Faktor-Authentifizierung wäre ein Mittel zum Schutz vor einem solchen Angriff.

BEISPIEL Wenn der Benutzer den Zifferncode an den Hacker weitergibt (siehe Druckbildschirm und Artikel)
BEISPIEL SMS von lokaler Bank mit Betrugslink (Beispiel mit SMS von SEB Bank).

Betrugs-E-Mails - Betrüger geben sich als nationales Postamt (Latvijas Pasts) aus und fordern die Empfänger auf, für die Zustellung einer angeblich verspäteten Sendung zu bezahlen. Der in der E-Mail angegebene Link führt zu einer gefälschten Website für betrügerische Zahlungskartendaten (siehe Druckbild).

Gefälschte Online-Shops - eine besonders hohe Aktivität wurde während der Weihnachtszeit durch Werbung in den sozialen Medien und aufgrund der Covid-19- Beschränkungen beobachtet, die Unternehmen dazu zwangen, ihre Produkte online zu verkaufen.

BEISPIELE Betrüger locken AliExpress-Nutzer in gefälschte Online-Shops (Bild und Betrugsfall); Wie man einen Betrug erkennt

Romance Scam - Betrüger nutzen Menschen aus, die auf der Suche nach einem romantischen Partner sind, oft über Dating-Websites, Apps oder soziale Medien, indem sie vorgeben, ein potenzieller Partner zu sein. Sie spielen mit emotionalen Auslösern, um Sie dazu zu bringen, Geld, Geschenke oder persönliche Daten bereitzustellen.

BEISPIEL Ermittlungsbericht über Romance Scammer [von North Lab]

Denial-of-Service-Angriffe (DoS und DDoS)

Es wurden DDoS-Angriffe auf öffentliche und kommunale Einrichtungen registriert (z. B. die Nationalbibliothek, das Zentrum für kulturelle Informationssysteme usw.) Eine Schule wurde durch lang anhaltende DDoS-Angriffe gestört. Ähnliche Berichte gingen zu Beginn des Schuljahres auch von anderen Bildungseinrichtungen ein. Auch in anderen europäischen Ländern sind Bildungseinrichtungen mit solchen Herausforderungen konfrontiert.

Sowohl in Europa als auch in Lettland wurden die folgenden Vorfälle aktuell - Erpressungsversuche, die in erster Linie auf Finanzinstitutionen oder Unternehmen des Privatsektors abzielten (die Angreifer führten eine Reihe von Probeangriffen durch und drohten damit, den Betrieb von Unternehmenswebsites oder anderen Ressourcen durch Angriffe mit bis zu 2 Tb/s auszusetzen).

WEITERE TRENDS

Gefährdete Geräte und Datenlecks

Die Kompromittierung von Geräten kann Einzelpersonen, Unternehmen sowie staatliche und kommunale Einrichtungen betreffen. Dies kann durch bereits kompromittierte E-Mails oder die Infektion eines Geräts durch das Öffnen von Anhängen oder Links von scheinbar vertrauten Kontakten wie Kollegen und Geschäftspartnern geschehen; es kann auch durch kompromittierte Websites geschehen, z. B. über ein veraltetes Plugin oder ein veraltetes Content-Management-System.

Dies war auch in den Jahren 2020-2021 der Fall, als mehrere nationale Institutionen vorübergehend den Zugang zu ihren Konten in sozialen Netzwerken verloren, da Angreifer die Kontrolle über die Profile eines der Kontoverwalter übernahmen. Es wurde über Einbrüche in Zoom- und MS-Teams-Meetings berichtet, die auf mangelndes Wissen über verfügbare Sicherheitsvorkehrungen zurückzuführen waren (z. B. Warteraum, eingeschränkter Zugang aus dem Ausland usw.).

Eindringversuche (jeder Angriff, der darauf abzielt, die Sicherheitsziele eines Unternehmens zu gefährden) - nach der Zunahme der Fernarbeit hat die Aktivität von Bots, die nach anfälligen, unzureichend konfigurierten Geräten und/oder schwachen Passwörtern für mit dem Netzwerk verbundene Geräte suchen (voreilig vom Arbeitgeber ausgegebene Geräte, private Laptops, die für die Arbeit verwendet werden, sowie schlecht geschützte RDP-Dienste mit schwachen Passwörtern), erheblich zugenommen.

VIDEO Beispiele für Eindringlinge Mehr auf der Intrusion Detection

QUELLE CERT.LV und "Kiberlaikapstākļi" (Cyber-Wetter); Investopedia
- Zusätzliche Elemente

HINWEIS Berücksichtigen Sie auch Diskussionen über andere Methoden für gefälschte und betrügerische Informationen, wie Deepfake und andere.

Lernaktivität Nr. 3 - Praktische Übung

Am Ende der Einheit wird ein Kahoot-Test organisiert, bei dem die Teilnehmer erkennen müssen, ob die bereitgestellten Informationen betrügerisch sind, und die Art (Methode) der Cyber-Bedrohung identifizieren müssen.

Einheit 4 - Was ist bei einem Zwischenfall zu tun?

Prävention und wie man sich vorbereiten kann

Lernaktivität Nr. 4 - Theorie

EINIGE TIPPS UND TRICKS ZUM SCHUTZ

Prüfen Sie Ihre E-Mails immer sorgfältig und achten Sie auf: Anhänge oder eingebettete Links von unbekannten/verdächtigen Quellen oder Absendern; Nachrichten mit einem Gefühl der Dringlichkeit, in denen Sie aufgefordert werden, etwas herunterzuladen oder eine andere Aufgabe zu erledigen; Angebote mit einem Belohnungsversprechen, das zu schön klingt, um wahr zu sein.

VIDEO Clicker (Spaidonis) mit Untertiteln auf Englisch

Achten Sie auf die Schreibweise der URL-Adresse. Phishing-Websites verwenden oft Webadressen, die einer offiziellen Website ähnlich sehen, aber einen einfachen Rechtschreibfehler enthalten, z. B. das Ersetzen einer "1" durch ein "l". Falsche oder seltsame Schreibweisen sind ein Hinweis auf einen möglichen Betrug.

Verwenden Sie sichere und unterschiedliche Passwörter für Ihre Geräte, E-Mail-Konten und Konten in sozialen Medien.
Weitere Tipps finden Sie im CYBER.EU.VET-Modul über Passwörter (Modul 4).

Wo immer möglich, sollten Sie Ihre Einstellungen so anpassen, dass Sie auf Ihren Geräten eine mehrstufige Authentifizierung verwenden. Zum Beispiel Passwort und Face ID oder Fingerabdruck auf Ihrem Telefon; Gmail hat inzwischen eine solche Einstellung, bei der ein Nutzer, wenn er sich von einem neuen Gerät aus anmeldet, nach Eingabe seines Benutzernamens und Passworts eine Aufforderung erhält, seine Identifizierung von einem anderen Gerät aus zu bestätigen, in der Regel einem Telefon.

die zweistufige Verifizierung in WhatsApp (für Android-Nutzer).

Führen Sie keine sensiblen Transaktionen über das ungesicherte öffentliche Wi-Fi in Cafés und an ähnlichen öffentlichen Orten durch.

Stellen Sie sicher, dass zumindest die wichtigsten Daten auf Ihrem Gerät eine Sicherungskopie haben (in einem Cloud-Speicher oder auf einem externen Gerät). Vergewissern Sie sich, dass Sie die erforderlichen Daten aus den Sicherungskopien wiederherstellen können, und finden Sie heraus, wie lange dies dauert.

Software-Updates - es ist wichtig, Software-Updates zu verfolgen und sie sofort zu installieren. Selbst eine Verzögerung von nur einem Tag kann kritisch sein.

Verwenden Sie ein VPN. Virtuelle private Netzwerke bieten eine weitere Schutzschicht für die Internetnutzung von zu Hause aus. Man kann sich zwar nicht allein darauf verlassen, dass sie Cyberangriffe verhindern, aber sie können eine nützliche Barriere gegen Cyberangriffe darstellen.

Verfolgen Sie regelmäßig die Nachrichten in der Welt der Angriffe und versuchen Sie zu bedenken, dass globale, nationale und lokale Ereignisse, sowohl politische als auch wirtschaftliche, aber auch solche, die mit globalem Leid verbunden sind (Pandemien, militärische Konflikte), als Thema/"Deckmantel" für potenzielle Cyberangriffe genutzt werden können.
Zusätzlich (auf Lettisch): CERT.LV Empfehlungen angesichts der sich verschlechternden geopolitischen Lage und einer Zunahme von Cyber-Bedrohungen in Europa: https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Wo kann man eine Cyber-Bedrohung oder einen Vorfall melden?
Ihr Arbeitsplatz, Ihre Bildungseinrichtung - senden Sie Screenshots, Bilder oder Videos an die zuständige Person in Ihrer Einrichtung (z. B. die IT-Abteilung). Warnen Sie Ihre Kollegen und Freunde.
Einrichtungen, die den nationalen Cyberspace unterstützen (wie im Fall von Lettland):

CERT.LV (Unterstützung bei der Lösung von Vorfällen, Überwachung des Cyberspace, Warnungen), Anleitung zur Weiterleitung betrügerischer E-Mails (auf Lettisch)
Staatliche Polizei
Latvian Safer Internet Centre (Verstöße und illegale Inhalte im Internet, Sicherheit von Kindern im Internet), und andere

INFORMATIONSQUELLEN UND TATSACHEN

Lesen Sie regelmäßig **lokale oder internationale Quellen**, um sich über die neuesten Entwicklungen im Bereich Cybersicherheit und Cyberbedrohungen zu informieren**:**

https://portswigger.net/daily-swig/cyber-attacks

https://www.euronews.com/tag/cyber-attack

OUCH! Newsletter - der weltweit führende, kostenlose Newsletter zum Thema Sicherheit für jedermann.

Links für Lettland (einige Informationen sind auch auf Englisch verfügbar):

https://www.esidross.lv/

https://cert.lv/lv/ (einschließlich "Cyber Weather" (Kiberlaikapstākļi), Anleitung zur Weiterleitung betrügerischer E-Mails (auf Lettisch)

https://drossinternets.lv/

Lernaktivität Nr. 4 - Praktische Übung

Diskussion mit den Teilnehmern: Bewertung der Nützlichkeit des Kurses (5-10 min Aktivität)

2. Lernergebnisse für das Modul

Wissen

- Die Lernenden haben ein grundlegendes Verständnis für die wichtigsten Aspekte von Cyberangriffen
- Die Lernenden haben einen Überblick über die aktuellen Vorfälle (vor dem Hintergrund der globalen Ereignisse)
- Die Lernenden wissen, welche Informationsquellen sie für Warnungen und aktuelle Bedrohungen nutzen können

Fähigkeiten

Die Lernenden sind in der Lage, gängige Arten von Cyber-Bedrohungen zu erkennen, zu klassifizieren und zu erklären.

Kompetenzen

- Die Lernenden werden in der Lage sein, eine potenzielle Cyber-Bedrohung zu erkennen und zu wissen, wo sie die Bedrohung melden müssen.
- Die Lernenden werden in der Lage sein, grundlegende Werkzeuge und Techniken auszuwählen, um sich vor Cyberangriffen zu schützen.

3. Literaturverzeichnis

CERT.LV (Information Technology Security Incident Response Institution): https://cert.lv/lv Covid-19

Phishing-Beispiele: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

Digicert, Was sind Malware, Viren, Spyware und Cookies? https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-und-cookies-und-was-unterscheidet-sie

Fichtner, E. (2022), Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common- types-of-cybersecurity-attacks

Information Technologies Security Incident Response Institutions (2021), CERT.LV Jahresbericht 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf

Informativer Bericht, Cybersecurity Strategy of Latvia 2019-2022 (nur auf Lettisch): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Latvian Safer Internet Centre (Projektplattform "Drossinternets.lv"): https://drossinternets.lvLIKTA (Lettischer Verband für Informations- und Kommunikationstechnologien): https://likta.lv/digitalas-parmainas-izglitiba/

Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: https://www.sciencedirect.com/science/article/pii/S2352484721007289

Merriam-Webster-Wörterbuch, Cyberattacke: https://www.merriam- webster.com/dictionary/cyberattack

Prat, M.K. (2021), Cyber-Angriff - Definition: https://www.techtarget.com/searchsecurity/definition/cyber-attack
Simplilearn, Cyber-Sicherheit Vollkurs 2022: https://youtu.be/yr1Psapupsc

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (auf Lettisch): https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola
Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian): https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs/

Überblick

Zielgruppe

- Lehrkräfte und Ausbilder in der Berufsbildung
- Schüler
- Vertreter von öffentlichen Einrichtungen aus dem Bildungsbereich: lokale, regionale und nationale Behörden

Beschreibung des Moduls

Heutzutage verbringen die Menschen einen großen Teil ihrer Zeit vor einem Bildschirm. Junge Menschen wachsen in einer Welt auf, in der neue Technologien gebraucht werden, und das Hauptkommunikationsmittel, das sie nutzen, ist das Internet. Die Nutzung sozialer Medien beispielsweise bietet viele Vorteile, aber auch viele Risiken. Es gibt viele Menschen, die gemobbt wurden oder gerade gemobbt werden. In den meisten Fällen waren sie sich dessen oder der Probleme, die dies in ihrem Leben verursachen kann, nicht bewusst. Aus diesem Grund möchten wir dieses Modul nutzen, um zu verstehen, was Cybermobbing ist und wie wir es verhindern können.

Lernziele

- Verständnis von Cybermobbing
- Wissen, wie man sie erkennt
- Auswirkungen von Cybermobbing
- Verstehen Sie die wichtigsten Konsequenzen
- Techniken zur Vorbeugung und zum Umgang damit liefern

Gesamtdauer

2 Stunden

Lerneinheit 1 - Wie lässt sich Cybermobbing erkennen?

Was sind die Auswirkungen?

Diese Einheit wird vom Trainer in Form einer PowerPoint-Präsentation gehalten, deren Ziel es ist, theoretisches Wissen zu vermitteln, begleitet von mehr visuellen Elementen - kurze Videos und reale Fälle von Cybermobbing, die die Informationen aus den PowerPoint-Folien zusammenfassen (max. 30 Minuten).
Es wird empfohlen, die Präsentationen anhand der für das CYBER.EU.VET-Projekt angepassten PPT-Vorlagen zu erstellen.

Lernaktivität 1

Der Trainer präsentiert den Lernenden eine Präsentation mit dem folgenden vorgeschlagenen Inhalt (max. 30 Minuten):
Cybermobbing wird zwar oft mit Cyberstalking in Verbindung gebracht, ist aber auch ein sehr ernstes Problem, das in den letzten Jahren immer häufiger auftritt.

Wie lässt sich Cybermobbing erkennen?

- Cybermobbing kann **schwer zu erkennen** sein, weil es hinter verschlossenen Türen oder an einem privaten Telefon/Computer stattfindet.

Hier sind einige der häufigsten Anzeichen dafür, dass jemand ein Opfer von Cybermobbing ist:

- Wird ungewöhnlich wütend, wenn er/sie den Computer oder das Telefon nicht benutzen kann oder nachdem er/sie den Computer benutzt hat.
- Wechselt schnell den Bildschirm oder schließt Programme, wenn jemand vorbeigeht.
- Vermeidet Diskussionen darüber, was sie am Computer tun.
- Rückzug aus der Familie oder von Freunden.
- Zurückhaltung bei der Teilnahme an Aktivitäten, die sie früher gerne gemacht haben.
- Ungeklärte Verschlechterung der schulischen Leistungen.
- Weigert sich, zur Schule zu gehen.
- Er meldet zunehmend Krankheitssymptome.
- Zeigt Anzeichen von Depression oder Traurigkeit.

Die Auswirkungen von Cybermobbing können für die Opfer verheerend sein. Betroffene können verschiedene negative Gefühle wie Traurigkeit, Wut, Frustration und Demütigung empfinden. Sie können sich auch isoliert und allein fühlen, so als ob sie niemanden hätten, an den sie sich wenden könnten.

Die Opfer können zudem in Schule und Studium leiden, da es ihnen zu peinlich sein kann, zur Schule zu gehen oder am Unterricht teilzunehmen. In einigen Fällen können die Opfer sogar an Selbstmord denken.
Cybermobbing kann auch negative Auswirkungen auf diejenigen haben, die Zeuge davon werden, wie es einer anderen Person widerfährt. Sie können sich verängstigt, hilflos und traurig fühlen. Sie können auch Probleme beim Schlafen und Essen haben und sogar Angstzustände und Depressionen entwickeln.

Auswirkungen und Folgen von Cybermobbing:
Wenn Mobbing im Internet stattfindet, kann es sich so anfühlen, als ob man überall angegriffen wird, sogar in den eigenen vier Wänden. Es kann so aussehen, als gäbe es kein Entkommen.
Die Auswirkungen können lange andauern und eine Person in vielerlei Hinsicht beeinträchtigen:

- **Seelisch:** sich verärgert, beschämt, dumm, sogar ängstlich oder wütend fühlen
- **Emotional:** sich schämen oder das Interesse an den Dingen verlieren, die man liebt
- **Körperlich:** Müdigkeit (wegen Schlafmangels) oder Symptome wie Magen- und Kopfschmerzen

Das Gefühl, von anderen ausgelacht oder belästigt zu werden, kann Menschen davon abhalten, sich zu äußern oder zu versuchen, das Problem zu lösen. In extremen Fällen kann Cybermobbing sogar dazu führen, dass sich Menschen das Leben nehmen.

VIDEO Worte tun weh | Cyberbully Kurzfilm

Auswirkungen:

- Krankheit
- Depression
- Isolierung
- Wut
- Demütigung

Lernaktivität 2

Gruppendiskussion - Fragen und Antworten; Bewertung und Feedback (max. 10 Minuten)

Sie kennen jetzt die häufigsten Anzeichen dafür, dass jemand im Internet gemobbt wird:

- Kennen Sie jemanden in dieser Situation?
- Können Sie ihnen helfen?

Einheit 2 - Wie man Cybermobbing verhindert oder stoppt

Lernaktivität 1

Trainer präsentiert den Lernenden eine Präsentation mit dem folgenden vorgeschlagenen Inhalt (max. 30 Minuten):

Cybermobbing wird durch den einfachen Zugang zu digitalen Medienplattformen und Geräten erleichtert. Oft werden diese ohne jegliche Kontrolle genutzt. Das macht Cybermobbing zu einem unglaublich schwer zu bekämpfenden Problem. Die Verhinderung dieser Praxis würde viel Zeit und Ressourcen erfordern, um jede Online-Interaktion wirksam zu überwachen. Zwar ist es oft nicht möglich, sich vollständig von digitalen Werkzeugen zu befreien, aber es gibt Methoden, die Eltern, Schüler und Pädagogen anwenden können, um das Phänomen zu bekämpfen und seine schädlichen Auswirkungen zu verringern.

Eltern können den Schaden, der durch Cybermobbing entsteht, wirksam bekämpfen, indem sie einfach mit ihren Kindern über das Thema sprechen.
Es ist auch wichtig, über Online-Sicherheit, Datenschutz und Passwortverwaltung zu sprechen. Legen Sie Richtlinien für das Online-Verhalten der Schüler fest und weisen Sie die Jugendlichen an, ihren Eltern gegenüber offen zu sein, wenn sie durch Mobbing im Internet oder in der realen Welt Schaden erlitten haben.
Jugendliche können sich davor schützen, Opfer von Cybermobbing zu werden, indem sie darauf achten, was sie veröffentlichen. Sie sollten ihre Passwörter nicht weitergeben und sicherstellen, dass ihre Online-Datenschutzeinstellungen sie schützen.
SchülerInnen spielen eine wichtige Rolle bei der Prävention von Cybermobbing. Wenn junge Menschen, die die Fakten über Cybermobbing kennen, bemerken, dass jemand anderes gemobbt wird, können sie einen vertrauenswürdigen Erwachsenen benachrichtigen. Sie sollten auch freundlich, großzügig und unterstützend zu dem Kind sein, das gemobbt wird. Lehrer, Erzieher und andere vertrauenswürdige Erwachsene müssen gemeinsam mit Eltern und Jugendlichen gegen Cybermobbing vorgehen. Oft können diese Personen Veränderungen im Verhalten eines Kindes erkennen und helfen, das Problem anzugehen, bevor die Eltern es können.

Die Technologie und das Internet sind nicht das Problem. Das eigentliche Problem sind die Menschen, die es nutzen, um anderen zu schaden. Deshalb ist es wichtig, Teenagern beizubringen, wie sie soziale Medien sicher und verantwortungsbewusst nutzen können, und ihnen bewusst zu machen, wie sie sich verhalten sollen, wenn sie von Cybermobbing betroffen sind.

Was kann man tun, wenn man Opfer von Cybermobbing wird?

- Beantworten oder kommentieren Sie die Cyberbully-Nachricht NICHT.
- BLOCKIEREN Sie die beteiligten Personen.
- LOGGEN Sie sich von der Website, auf der das Mobbing stattfindet, AUS.
- Sichern Sie Ihre PASSWORDS und überprüfen Sie Ihre PRIVACY CONTROLS.
- Speichern Sie alles. Machen Sie einen Screenshot oder drucken Sie den Vorfall als Beweismittel aus.
- Cybermobbing melden: Fast jede technische Website bietet die Möglichkeit, jemanden wegen Cybermobbing zu melden.
- Erzählen Sie einer vertrauenswürdigen erwachsenen Person, was vor sich geht, oder wenden Sie sich an die Strafverfolgungsbehörden.

Was sollten Sie tun, wenn Sie Cybermobbing beobachten?

- Informiere deine Eltern oder einen Erwachsenen deines Vertrauens und bitte sie um Rat.
- Melden Sie die Situation dem Anbieter der Technologie, der App oder der sozialen Medien.
- Wenn die Situation Mitschüler betrifft, informieren Sie Ihre Lehrer.
- Zeigen Sie der Person, die gemobbt wird, Ihre Unterstützung, indem Sie ihr zum Beispiel eine freundliche Nachricht schicken.

Rechtliche Schritte einleiten: Sowohl Verleumdung als auch üble Nachrede sind Straftaten, die zu einem Prozess führen können.

Bitten Sie um Hilfe:

- Es ist sehr schwierig, allein mit Cybermobbing umzugehen.

VIDEO Emmas Geschichte: Cybermobbing durch einen besten Freund

Wie kann ich mich selbst aufklären?

- **Organisationen**, die helfen können: Es gibt viele Organisationen, die Informationen über Cybermobbing weitergeben. Die unten aufgeführten Websites erstellen und teilen nützliche Inhalte, die für alle, die Angst vor Cybermobbing haben oder davon betroffen sind, wirklich hilfreich sind.
- **Blogs und Podcasts**: Blogs und Podcasts, die sich mit dem Thema befassen, sind eine gute Möglichkeit, um auf dem Laufenden zu bleiben und die neuesten Ratschläge oder Perspektiven zu erhalten.
- **Bücher**
- **Apps und Software**: Es gibt zahlreiche Produkte, mit denen Eltern die Online-Aktivitäten ihrer Kinder einschränken und/oder überwachen können. Es ist Sache der Eltern zu entscheiden, ob diese Art der Überwachung je nach Alter und Internetgewohnheiten des Kindes angemessen ist. Einige Programme suchen sogar nach Sprache, die als Mobbing eingestuft werden könnte. Es gibt auch Unternehmen, die mit Schulen zusammenarbeiten, um eine anonyme Meldung von Mobbing-Vorfällen zu ermöglichen.

Lernaktivität 2

Gruppendiskussion - Fragen und Antworten; Bewertung und Feedback (max. 15 Minuten)

Schreibübung:
Beschreiben Sie eine Situation, in der Sie wissen, dass es zu Cybermobbing kommt. Diese kann real oder fiktiv sein.
Können Sie helfen? Wie? Warum oder warum nicht? Erklären Sie, wie Sie sich dabei fühlen.

2. Lernergebnisse für das Modul

Wissen

Die Lernenden wissen, wie sie Cybermobbing erkennen können und wie sich das Opfer fühlt und erlebt.

- Wenn Jugendliche, Erwachsene und Pädagogen die Fakten über Cybermobbing kennen und wissen, wie sie dagegen vorgehen können, können sie dazu beitragen, eine bessere, einfühlsamere digitale Welt zu schaffen.

Fertigkeiten

- Die Lernenden wissen, wie sie erkennen können, wenn jemand im Internet gemobbt wird
- Der Lernende wird in der Lage sein, zu verstehen, welches Maß an Reaktion und Unterstützung je nach dem vorliegenden Szenario erforderlich ist.

Zuständigkeiten

- Der Lernende ist in der Lage, eine Episode von Cybermobbing zu erkennen und sofort mit den richtigen Mitteln dagegen vorzugehen.
- Der Lernende ist in der Lage, die beste Methode der Unterstützung zu erkennen, die für den jeweiligen Fall am besten geeignet ist.

3. Literaturverzeichnis

https://socialmediavictims.org/cyberbullying/effects/
https://americanspcc.org/impact-of-cyberbullying/ https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.security.org/resources/cyberbullying-resources-books-podcasts/

PRÄVENTION VON CYBERBULLYING

Modul 3

Überblick

Zielgruppe

- Lehrkräfte und Ausbilder in der Berufsbildung
- Schüler
- Vertreter von öffentlichen Einrichtungen aus dem Bildungsbereich: lokale, regionale und nationale Behörden

Beschreibung des Moduls

Dies ist ein Folgemodul zu "Cybermobbing. Was ist das? Wie können wir es erkennen?" und vermittelt den Zielgruppen die Kompetenzen zur Verbreitung des Bewusstseins für Cybermobbing und zur Bereitstellung von Präventionstechniken, um nicht Opfer von Cybermobbing zu werden.

Lernziele

Verständnis für die Bedeutung der Prävention
Bewusstsein für Cybermobbing schaffen
Sensibilisierung für Techniken zur Verhinderung von Cybermobbing

Gesamtdauer

1,5 Stunden

Einheit 1 - Warum Cybermobbing verhindern?

Diese Einheit wird von der Lehrkraft als PowerPoint-Präsentation zur Verfügung gestellt, die sowohl theoretisches Material als auch visuelle Elemente wie kurze Filme und reale Cybermobbing-Szenarien enthält, die die Informationen aus den PowerPoint-Folien zusammenfassen (jeweils 20 bis 30 Minuten pro Einheit).
Wir empfehlen, die Präsentationen anhand der auf das CYBER.EU.VET-Projekt zugeschnittenen PPT-Vorlagen vorzubereiten. Im Anschluss an die Präsentation findet eine Gruppendiskussion statt, in der jeder über das Gelernte nachdenken kann.

Lernaktivität 1

Der Trainer präsentiert den Schülern eine Präsentation mit dem folgenden vorgeschlagenen Inhalt (max. 20 Minuten):

Vorbeugen oder intervenieren?
Forschungsergebnissen zufolge haben Personen, die Cybermobbing ausgesetzt sind, eine Vielzahl negativer Folgen, darunter emotionale, körperliche, geistige und akademische Schwierigkeiten. Darüber hinaus ist Cybermobbing eine erhebliche Stressquelle für junge Menschen. Die Opfer sind durch Cybermobbing psychisch verletzt, schämen sich und haben manchmal Angst. Sie geben sich nicht nur selbst die Schuld für die Belästigung und den Missbrauch, sondern fühlen sich auch sehr verunsichert. Einer Studie zufolge zeigen über 35 % der Personen, die von Cybermobbing betroffen sind, Stresssymptome. Diese Art von Mobbing kann besonders schädlich sein, da sie oft sehr öffentlich ist. Normalerweise können viele Menschen sehen, was geschrieben oder gepostet wird. Es ist schwierig, wenn nicht gar unmöglich, alle Spuren von etwas zu löschen, wenn es einmal online veröffentlicht worden ist. Das bedeutet, dass das Mobbing fortgesetzt werden kann.

Wenn Menschen in den sozialen Medien, über Textnachrichten, Sofortchats und Blogposts häufig von anderen belästigt werden, können sie anfangen, sich hoffnungslos zu fühlen. Sie haben vielleicht das Gefühl, dass Selbstmord die einzige Möglichkeit ist, ihr Leiden zu beenden. Da die Gefahren von Cybermobbing so gravierend sind, müssen Ausbilder in der Erwachsenenbildung ihre Schüler[AB1] unbedingt über dieses Problem aufklären, bevor es echten Schaden anrichtet. Präventive Maßnahmen verringern das Risiko, Opfer von Cybermobbing zu werden.

Lernaktivität 2

Gruppendiskussion (max. 10 Minuten)

Fragen Sie Ihre Schüler:
Warum ist Prävention bei Cybermobbing so wichtig?
Wurden sie jemals über Cybermobbing informiert?
Wie erfahren sie normalerweise von Cybermobbing?

Einheit 2 - Bewusst machen

Lernaktivität 1

Der Trainer hält vor den Schülern eine Präsentation mit folgendem Inhalt (max. 30 Minuten): Es ist wichtig, mit den Schülern zu besprechen, wie sie soziale Medien sicher und verantwortungsbewusst nutzen können, indem sie Cybermobbing-Täter erkennen und lernen, was zu tun ist, wenn sie online gemobbt werden.

VIDEO Cybermobbing - Wie man Cyber-Missbrauch vermeidet

ERST DENKEN, DANN BUCHEN

Die Schülerinnen und Schüler sollten es sich zur Gewohnheit machen, ihre Arbeit durchzulesen, bevor sie sie veröffentlichen. Sie können den Beitrag in den Notizbereich ihres Computers oder Smartphones tippen und ihn dann einige Stunden später noch einmal lesen, um zu entscheiden, ob er veröffentlicht werden soll oder nicht. Da Cybermobber das, was sie posten, gegen sie verwenden könnten, werden sie weniger geneigt sein, etwas zu sagen, das sie später bereuen oder das gegen sie verwendet werden könnte.

Sicher, wenn jemand etwas gegen einen verwenden will, wird er sich bemühen, selbst die unbedeutendsten Informationen zu bekommen, aber eine Überprüfung vor der Veröffentlichung kann die Schwere des Cyberangriffs verringern. Nachzudenken, bevor man etwas veröffentlicht, kann helfen, eine gesunde Beziehung zu den sozialen Medien zu unterhalten.

VORSICHT MIT ÖFFENTLICHEN GERÄTEN

Studierende sollten auch vorsichtig sein, wenn sie öffentliche Geräte wie Universitäts-oder Bibliothekscomputer benutzen, da es viele Möglichkeiten gibt, wie jemand dies ausnutzen könnte.

Es gibt viele Möglichkeiten, wie öffentliche Geräte mit bösartigen Programmen infiziert werden können, z. B. mit Keyloggern.

Ein Keylogger ist den meisten Quellen zufolge eine Softwareanwendung, die diskret alle Tastenanschläge überwacht und protokolliert. Sie können verwendet werden, um Passwörter und andere persönliche Informationen abzufangen, die über die Tastatur eingegeben werden, und stellen eine große Gefahr für die Nutzer dar, z. B. indem sie Cyber-Kriminellen Zugang zu Ihren Social-Media-Konten gewähren. Das Wichtigste bei Keyloggern ist, dass sie oft nicht von Antivirenprogrammen erkannt werden, da es viele legitime Keylogger auf dem Markt gibt, die der Kindersicherung, der Unternehmenssicherheit usw. dienen.

VIDEO Könnte ein Keylogger Sie ausspionieren?

Abgesehen von speziellen Überwachungsprogrammen sollten die Schüler auch daran erinnert werden, sich von ihren Konten abzumelden, da sie diese möglicherweise unbeabsichtigt offen lassen und denjenigen zugänglich machen, die die Computer neben ihnen benutzen.

ONLINE-SCHUTZ

Es ist wichtig, überall sichere Passwörter zu verwenden, um Cybermobbing und andere betrügerische Aktivitäten zu bekämpfen. Ein sicheres Passwort ist ein Passwort, das nicht leicht erraten oder kompromittiert werden kann. Ein sicheres Passwort sollte lang sein, eine Kombination aus Zahlen, Sonderzeichen und Klein-/Großbuchstaben enthalten und auf keinen Fall offensichtliche Informationen wie Name, Geburtsdatum usw. enthalten. Indem Sie Ihre Konten schützen, stellen Sie sicher, dass niemand Zugang zu ihnen hat.

CYBERMOBBING SOLLTE GEMELDET WERDEN.

Machen Sie Ihren Schülern klar, wie wichtig es ist, Cybermobbing zu melden. Dazu gehört nicht nur das Aufspüren von Cybermobbing, sondern auch das Informieren der Social-Media-Plattform, des Internetanbieters und anderer relevanter Parteien. Um der Belästigung ein Ende zu setzen, müssen sie möglicherweise sogar die örtlichen Behörden informieren.

Nachdem sie alle erforderlichen Unterlagen eingereicht haben, müssen die Schüler die erforderlichen Maßnahmen ergreifen, um die für das Cybermobbing verantwortliche Person oder das Konto zu sperren. Sie sollten sich auch darüber im Klaren sein, dass der Täter auch nach der Sperrung alternative Konten erstellen könnte, um sich dem Opfer zu nähern.

Die gute Nachricht in Bezug auf Online-Mobbing, das online stattfindet, ist, dass es in der Regel aufgezeichnet und aufbewahrt werden kann und jemandem vorgelegt werden kann, der helfen kann. Die Opfer sollten diese Beweise für den Fall aufbewahren, dass die Dinge aus dem Ruder laufen.

VIDEO: CYBER-MOBBING IGNORIEREN ODER MELDEN

Lernaktivität 2

Stellen Sie den Schülern die folgende Fallstudie vor

YouProMe Erasmus+ Projekt - www.youpromeproject.eu

Jessica ist 18 Jahre alt. Sie lebt mit ihren beiden Eltern, die beide berufstätig sind und immer viel zu tun haben. Jessica ist das älteste von drei Kindern. In der Familie gibt es niemanden mit bekannten gesundheitlichen Problemen. Sie geht in die Schule und ist eine fleißige Schülerin. Sie hat eine Leidenschaft für Tiere und geht gerne mit ihren Freunden aus. Sie hat einen Freund. Jessica hat ein Mobiltelefon und nutzt regelmäßig soziale Netzwerke.

Jessica berichtet: "Ich habe meinem Freund vor ein paar Wochen ein paar Bilder geschickt. Ich dachte sowieso, er sei mein Freund, aber dann hat er sie seinem Freund gezeigt und der hat sie an alle geschickt. Die Schule hat es herausgefunden, und jetzt hat die Polizei mit ihm und seinem Freund gesprochen. Seitdem bin ich nicht mehr in die Schule gegangen, aber alle nennen mich jetzt in den sozialen Medien eine Schlampe. Ich kann es nicht ertragen, wenn sie mich anstarren, und ich weiß schon, was sie denken. Sogar die Mädchen haben eine ähnliche Meinung über mich. Das Blöde ist, dass das jeder macht, jeder schickt Bilder, aber ich hatte einfach das Pech, einen Freund zu haben, der mich betrogen hat. Ich werde nie wieder jemandem vertrauen. Ich habe das Gefühl, dass alles vorbei ist und es jetzt kein Zurück mehr gibt."

Infolgedessen hat Jessica einen Monat lang der Schule ferngeblieben und weigert sich, wiederzukommen. Sie hat alle ihre Schulsportaktivitäten abgebrochen. Ihre Mutter sprach mit dem Sportjugendbetreuer und sagte, sie sei besorgt über einige der "dunklen" Dinge, die Jessica gesagt habe. Jessica ist bestrebt, ihre Online-Präsenz zu ändern und ihr anfängliches Selbstvertrauen wiederzuerlangen. Jessica und ihre Familie wissen nicht, welche Unterstützung es gibt und wie sie ihre psychische Gesundheit am besten fördern können, und sie wissen auch nicht, wie ein Jugendbetreuer in dieser Situation vermitteln kann. Jessica hat das Risiko des Internetmissbrauchs erkannt und ist sich bewusst, dass sie Unterstützung benötigt, um ihre psychische Gesundheit in den Griff zu bekommen, da dies ihre Entscheidungsfindung beeinflusst hat.

Nun können Sie auf der Grundlage dieser Fragen ein Gespräch beginnen (max. 30 Minuten):

- Welche Risiken gibt es hier?
- Welche Dienste sollten Sie einbeziehen?
- Welches Vorgehen schlagen Sie Jessica und ihrer Mutter vor?

2. Lernergebnisse für das Modul

Wissen

- Die Lernenden verstehen, wie wichtig es ist, Cybermobbing zu verhindern.
- Die Lernenden wissen, welche Techniken es gibt, um zu verhindern, dass sie Opfer von Cybermobbing werden.

Fähigkeiten

- Die Lernenden sind in der Lage, ein Bewusstsein für die Prävention von Cybermobbing zu schaffen.
- Die Lernenden sind in der Lage, ihren Schülern wichtige Präventionstechniken zu vermitteln.

Kompetenzen

- Je nach Situation kann der Lernende bestimmen, welche Art von Unterstützung erforderlich ist
- Die Lernenden sind in der Lage, effiziente Veranstaltungen zur Sensibilisierung gegen Cybermobbing durchzuführen

3. Literaturverzeichnis

https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808 https://anti-bullyingalliance.org.uk/sites/default/files/uploads/attachments/cyberbullying- and-send-module-final%281%29_1.pdf https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/ https://www.connectsafely.org/tips-to-help-stop-cyberbullying/

AUTHENTIFIZIERUNG UND PASSWORT

Modul 4

1. Modul-Übersicht

Zielgruppe

- Lehrkräfte und Ausbilder in der Berufsbildung
- Schüler
- Vertreter von öffentlichen Einrichtungen aus dem Bildungsbereich: lokale, regionale und nationale Behörden

Beschreibung des Moduls

Berufsbildungsfachleute und ihre Schüler sind täglich mit verschiedenen Bedrohungen der Cybersicherheit konfrontiert. Es gibt zwar verschiedene online verfügbare Lehrmaterialien zum Thema Cybersicherheit, aber sie sind nicht alle auf dem neuesten Stand oder werden von den Lernenden entweder als zu grundlegend oder zu komplex empfunden.
Die Lerninhalte dieses Moduls vermitteln den Lernenden Fähigkeiten und Kenntnisse, um ihr Verständnis von Authentifizierung und Passwörtern zu verbessern, um ihre Ausbildungskapazitäten zu stärken, aber auch um ihre Fähigkeiten zu verbessern, damit sie Angriffe auf die Cybersicherheit vermeiden können. Besser ausgerüstete Ausbilder in der beruflichen Bildung werden in der Lage sein, ihre Schüler dabei zu unterstützen, die täglichen Bedrohungen zu erkennen, denen sie ausgesetzt sind.

Lernziele

Verbessertes Verständnis der Authentifizierung im Bereich der Cybersicherheit

- Verbessern Sie das Verständnis für verschiedene Authentifizierungsmethoden
- Verbesserung des Verständnisses der wichtigsten Merkmale der gängigsten Authentifizierungsmethoden
- Verstehen Sie Risiken, die mit der Nichtverwendung komplexer Passwörter verbunden sind
- Bereitstellung von Techniken zur einfachen Verwaltung komplexer Passwörter

Gesamtdauer

2 Stunden

AUTHENTIFIZIERUNG UND PASSWORT

Modul 4

Einheit 1 - Authentifizierung

Diese Einheit wird vom Trainer in Form einer PowerPoint-Präsentation gehalten, die theoretisches Wissen vermittelt und durch visuelle Elemente ergänzt wird - kurze Videos, die die Informationen aus den PowerPoint-Folien zusammenfassen (max. 20 Minuten).
Es wird empfohlen, die Präsentationen anhand der auf das CYBER.EU.VET-Projekt zugeschnittenen PPT-Vorlagen vorzubereiten. In Anbetracht der rasanten Entwicklungen und Fortschritte im Bereich der Cybersicherheit wird empfohlen, die Einheiten kontinuierlich zu überprüfen und den Inhalt gegebenenfalls an die neuesten Entwicklungen in diesem Bereich anzupassen.
An die Präsentation schließt sich eine 10-minütige Gruppendiskussion an, um den Lernprozess zu reflektieren und das Verständnis der Lernenden für das Thema zu bewerten, während gleichzeitig Raum für weitere Fragen und Feedback geschaffen wird.

Lernaktivität 1

Der Trainer hält eine Präsentation mit dem folgenden vorgeschlagenen Inhalt (max. 20 Minuten):

Was ist Authentifizierung?
Der Vorgang der Authentifizierung im Zusammenhang mit Computersystemen bedeutet die Sicherstellung und Bestätigung der Identität eines Benutzers. Bevor ein Benutzer versucht, auf in einem Netz gespeicherte Informationen zuzugreifen, muss er seine Identität und die Berechtigung zum Zugriff auf die Daten nachweisen. Bei der Anmeldung in einem Netz muss ein Benutzer eindeutige Anmeldeinformationen wie einen Benutzernamen und ein Kennwort angeben, um das Netz vor dem Eindringen von Hackern zu schützen. In den letzten Jahren wurde die Authentifizierung weiter ausgebaut, so dass nun noch mehr persönliche Informationen des Benutzers erforderlich sind, z. B. biometrische Daten, um die Sicherheit des Kontos und des Netzes vor Personen zu gewährleisten, die über die technischen Fähigkeiten verfügen, Schwachstellen auszunutzen.

VIDEO: WAS IST AUTHENTIFIZIERUNG?

Warum ist Authentifizierung wichtig?
Die Authentifizierung ist ein entscheidender Schritt, um die Daten der Nutzer zu schützen
und den unbefugten Zugriff auf Online-Daten zu verhindern und zu blockieren. Wenn die Authentifizierung nicht sicher ist, kann das System leicht angegriffen und gehackt werden, und Cyberkriminelle können sich Zugang zu Daten und Informationen verschaffen, die im System gespeichert sind.

AUTHENTIFIZIERUNG UND PASSWORT

Es ist sehr wichtig, dies zu verhindern und dafür zu sorgen, dass die Nutzer die verschiedenen kostenlosen oder kostenpflichtigen Authentifizierungsmethoden kennen, um einen unbefugten Zugriff auf ihre persönlichen oder beruflichen Daten zu verhindern. Für Organisationen und Unternehmen empfehlen wir, in hochwertige Authentifizierungswerkzeuge zu investieren, um ihre Online-Daten vor möglichen Verstößen zu schützen.

VIDEO: WÖCHENTLICHER TIP ZUR CYBERSICHERHEIT - AUTHENTIFIZIERUNG

Gängige Methoden zur Passwortauthentifizierung

In Anbetracht der sich ständig ändernden Arten von Cyber-Bedrohungen und -Angriffen wurde in den letzten Jahren eine breite Palette verschiedener Authentifizierungsmethoden entwickelt.

Einige der gängigsten Authentifizierungsmethoden sind:

1. Standard-Passwort-Authentifizierung
2. Zwei-Faktoren-Authentifizierung
3. Token-Authentifizierung
4. Biometrische Authentifizierung
5. Computererkennungs-Authentifizierung
6. CAPTCHAS

1. STANDARD-PASSWORT-AUTHENTIFIZIERUNG

- Die einfachste und am häufigsten verwendete Form der Authentifizierung:
- Verlangt die Eingabe eines Benutzernamens zusammen mit einem Geheimcode oder einem Passwort, das den Zugang zu einem Netzwerk, Konto oder einer Anwendung ermöglicht.

Um das Risiko der Kompromittierung eines Passworts zu verringern, sollten die Nutzer ein sicheres Passwort wählen. Ein sicherer Passwort-Manager oder eine Software kann helfen, den unbefugten Zugriff auf die online gespeicherten Daten zu verhindern.

2. ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

Bei der Zwei-Faktor-Authentifizierung müssen sich die Benutzer mit etwas, das sie "wissen", und etwas, das sie "haben", authentifizieren. Ein Passwort dient als "etwas, das sie wissen", und ein bestimmter physischer Gegenstand wie ein Smartphone dient als "etwas, das sie haben".

Bei der Zwei-Faktor-Authentifizierung muss der Benutzer in der Regel seinen Benutzernamen, ein Kennwort und einen einmaligen Code eingeben, der an ein physisches Gerät (Mobiltelefon, Kartenlesegerät usw.) gesendet wurde.

3.TOKEN-AUTHENTIFIZIERUNG

Token-Systeme verwenden ein speziell angefertigtes physisches Gerät für die Zwei-Faktor-Authentifizierung und werden empfohlen, wenn Sie sich nicht auf Mobiltelefone verlassen möchten.
Dabei kann es sich um einen Dongle handeln, der in den USB-Anschluss Ihres Geräts eingesteckt wird, oder um eine Smartcard mit Radiofrequenz-Identifikations- oder Nahfeldkommunikations-Chip.
Um die Sicherheit eines Token-Systems zu gewährleisten, muss sichergestellt werden, dass das physische Authentifizierungsgerät (d. h. der Dongle oder die Chipkarte) nicht in die falschen Hände gerät.

4. BIOMETRISCHE AUTHENTIFIZIERUNG

Die biometrische Authentifizierung stützt sich auf die physischen Merkmale eines Benutzers, um ihn zu identifizieren. Bei der biometrischen Authentifizierung können Fingerabdrücke, Netzhaut- oder Iris-Scans oder Gesichts- und Stimmerkennung verwendet werden. Dies ist eine äußerst sichere Form der Authentifizierung, da keine zwei Personen die gleichen physischen Merkmale aufweisen. Die biometrische Authentifizierung ist ein wirksames Mittel, um genau zu wissen, wer sich im System anmeldet.

5. AUTHENTIFIZIERUNG DURCH COMPUTERERKENNUNG

Die Computererkennung ist eine Methode zur Authentifizierung von Passwörtern, bei der die Legitimität eines Benutzers überprüft wird, indem sichergestellt wird, dass er sich auf einem bestimmten Gerät befindet. Diese Systeme installieren ein kleines Software-Plug-in auf dem Gerät des Benutzers, wenn dieser sich zum ersten Mal erfolgreich anmeldet.
Dieses Plug-in enthält eine kryptografische Gerätemarkierung. Wenn sich der Benutzer das nächste Mal anmeldet, wird die Markierung überprüft, um sicherzustellen, dass er sich auf demselben, vertrauenswürdigen Gerät befindet.
Dieses System ist für den Nutzer unsichtbar und erfordert von ihm keine zusätzlichen Authentifizierungsmaßnahmen. Sie geben einfach wie gewohnt ihren Benutzernamen und ihr Passwort ein, und die Überprüfung erfolgt automatisch.
Um ein hohes Sicherheitsniveau aufrechtzuerhalten, müssen Authentifizierungssysteme mit Computererkennung die Anmeldung von neuen Geräten mit anderen Formen der Verifizierung ermöglichen (z. B. Zwei-Faktor-Authentifizierung mit einem per SMS übermittelten Code).

6. CAPTCHAS

CAPTCHAs konzentrieren sich nicht auf die Überprüfung eines bestimmten Benutzers, im Gegensatz zu den anderen in diesem Artikel aufgeführten Methoden. Stattdessen zielen CAPTCHAs darauf ab, festzustellen, ob ein Benutzer ein Mensch ist, und verhindern
computergesteuerte Versuche, in Konten einzubrechen (z. B. Brute-Force-Angriffe).
Das CAPTCHA-System zeigt ein verzerrtes Bild aus Buchstaben und Zahlen oder Bildern an und fordert den Benutzer auf, das Gesehene einzugeben. Da Computer und Bots Schwierigkeiten haben, diese Verzerrungen richtig zu erkennen, erhöhen CAPTCHAs die Sicherheit, indem sie eine zusätzliche Barriere für automatisierte Hacking-Systeme schaffen.

Lernaktivität 2

Gruppendiskussion - Fragen und Antworten, Bewertung und Feedback (max. 10 Minuten)
Empfohlene Fragen zur Bewertung:

- Was ist Authentifizierung?
- Warum ist Authentifizierung wichtig?
- Was sind die gängigsten Authentifizierungsmethoden, die derzeit verwendet werden, und was sind ihre Hauptmerkmale?

Einheit 2 - Passwort

Lernaktivität 1

1.DINGE, DIE MAN NICHT TUN SOLLTE

Folien mit Bildern, die Dinge veranschaulichen, die Menschen nicht tun sollten, um ins Publikum zu gelangen

FALLSTUDIEN

"Die belgische Polizei hat es mit dem WiFi-Passwort veröffentlicht. Dies wurde im nationalen Fernsehen gezeigt" - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/

"Ein Passwort für die hawaiianische Notfallbehörde war in einem öffentlichen Foto versteckt, geschrieben auf einem Post-it-Zettel" - https://www.businessinsider.com/hawaii-emergency-agency-password- discovered-in-photo-sparkss-security-criticism-2018-1

"Vier peinliche Passwort-Lecks im Live-TV" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. STATISTIK

Präsentation einiger Statistiken:

- 81 % der Datenschutzverletzungen sind auf mangelhafte Passwortsicherheit zurückzuführen
- Schlechte Passwortgewohnheiten von Mitarbeitern
- Top 200 der häufigsten Passwörter

3.DIE BEDEUTUNG EINES SICHEREN PASSWORTS

Die Anatomie eines unhackbaren Passworts

4. GRUNDREGELN

Beschreiben Sie eine Reihe von Grundregeln wie:

- Vermeiden Sie es, die Passwort-Manager des Browsers zu verwenden, da dies eine einfache Möglichkeit für "Malware" ist, sich Zugang zu ihnen zu verschaffen.
- Geben Sie Ihr Passwort nicht weiter.
- Passwörter auswendig lernen, nicht auf Papier oder in digitaler Form aufzeichnenPasswörter regelmäßig ändern (mindestens alle zwei Monate)
- Wenn möglich, aktivieren Sie die Zwei-Faktor-Authentifizierung
- Jedes Passwort darf nur auf einer Plattform verwendet werden.
- Ändern Sie das ursprüngliche Passwort beim Kauf eines Geräts
- Verwenden Sie keine gängigen Wörter. Eine der häufigsten Angriffsarten ist die Verwendung von "Wörterbüchern".

Regeln für ein sicheres Passwort:

- Erstellen Sie komplexe Passwörter: mindestens 12 Zeichen, mit Groß- und Kleinbuchstaben, mit Ziffern und Sonderzeichen
- Verwenden Sie keine leicht auffindbaren Begriffe wie Name, Geburtsort oder bekannte Begriffe, Name des Haustiers, Autokennzeichen, Handynummer, Geburtstage von Familienmitgliedern usw.

Auswendiglernen statt Aufnehmen:

- Erstellen Sie einen persönlichen "Schlüssel", der Teil aller Passwörter ist
- Verwenden Sie ein Sprichwort, allgemeine Ausdrücke oder etwas, das Sie sich leicht merken können.
- Verwenden Sie zum Beispiel die ersten beiden Buchstaben eines jeden Wortes
- Umschalten zwischen Großbuchstaben, Kleinbuchstaben und Symbolen
- Etwas hinzufügen, das mit der Website/dem Werkzeug assoziiert wird

Lernaktivität 2

Gruppenübungen

Testen Sie die Länge Ihres Passworts! - https://www.passwordmonster.com Wurde ich bereits geknackt? - https://haveibeenpwned.com/Passwords

Empfohlene Fragen zur Bewertung:

- Wie viele Jahre hält Ihr Passwort einer normalen Crack-Algorithmus-Maschine stand?
- Sollte ich mein Passwort ändern?

Lernaktivität 3

Der Trainer präsentiert den Lernenden eine Präsentation mit dem folgenden vorgeschlagenen Inhalt (max. 20 Minuten):

Was sind Passwort-Manager?

- Digitale Tresore
- Ermöglicht die Speicherung von Anmeldeinformationen und Notizen zu verschiedenen Diensten
- Auch die Bankdaten können geschützt werden
- Ein einziger Hauptschlüssel

Biometrische Authentifizierung kann verwendet werden

Lokale Passwort-Manager

- Speichern der Daten auf dem aktuellen Gerät
- Die Passwortdatei ist verschlüsselt
- Jedes Passwort muss in einer separaten verschlüsselten Datei gespeichert werden
- Darf nur auf einem einzigen Gerät verwendet werden wie z.B. Keypass XC

Online-Passwort-Manager

- Daten werden in der Cloud gespeichert
- Ermöglichen Sie den Zugriff auf Anmeldeinformationen und Notizen verschiedener Dienste von jedem Gerät aus
- Keine Installation erforderlich
- Ein einziger Hauptschlüssel
- Die Daten werden vom Gerät zum Server verschlüsselt

Beispiele für Online-Passwortmanager sind Bitwarden, Latspass, Keeper, 1Password

Lernaktivität 4

Gruppenarbeit
Erstellen Sie ein komplexes Passwort
Installieren Sie einen Passwort-Manager auf Ihrem Laptop oder Smartphone
Aktivieren Sie MFA

Diskussion und Feedback (max. 10 Minuten)
Empfohlene Fragen zur Bewertung:
Wie schwierig war es? Werden Sie diese bewährten Verfahren anwenden?

2. Lernergebnisse für das Modul

Wissen

- Definition von Authentifizierung, ihre Bedeutung und einige der gängigsten Authentifizierungsmethoden zu verstehen
- Verständnis der Risiken, die mit der Nichtverwendung komplexer Passwörter verbunden sind
- Bewährte Verfahren für die Verwaltung persönlicher Passwörter anwenden

Fähigkeiten

- Identifizierung und Anwendung der geeignetsten und angemessensten Authentifizierungsmethode
- Identifizieren und Anwenden der angemessensten und geeignetsten Passwortkomplexität

Kompetenzen

- die Bedeutung von Authentifizierung kennen
- über die geeignetste Autorisierungsmethode für verschiedene Online-Aktivitäten zu entscheiden und sie anzuwenden, zur Verbesserung der Online-Sicherheit
- die Bedeutung der Verwendung komplexer Passwörter erkennen
- Strukturierung von Best-Practice-Techniken zur Verwaltung persönlicher Passwörter

3. Literaturverzeichnis

https://www.sangfor.com/blog/cybersecurity/the-basics-of-authentication-in-cyber-Sicherheit https://www.passportalmsp.com/blog/which-password-authentication-method-works-

WI-FI SICHERHEIT

Modul 5

Überblick

Zielgruppe

- Lehrkräfte und Ausbilder in der Berufsbildung
- Schüler
- Vertreter von öffentlichen Einrichtungen aus dem Bildungsbereich: lokale, regionale und nationale Behörden

Gliederung des Moduls

Das vorliegende Modul wird sich darauf konzentrieren, die tatsächlichen Bedrohungen zu beleuchten, die sich mit öffentlichen Wifi-Systemen verbinden, wie sie funktionieren und wie man sie schließlich verhindern kann.

Lernziele

- Sensibilisierung für Missverständnisse bei der Nutzung öffentlicher WLAN-Netze
- Vermittlung von Kenntnissen über die Gefahren bei der Nutzung öffentlicher Wifi-Netze

Gesamtdauer

1 Stunde

Einheit 1

Das Modul umfasst sowohl Video-Lernteile als auch offene Diskussionen. Konkret wird zunächst ein erstes Einführungsvideo gezeigt. Dieses Video demonstriert mit Hilfe eines Experten, dass öffentliche Netzwerke ein riskanter Ort sind, um sich mit dem Internet zu verbinden. Allerdings ist dieses erste Video sehr kurz und erlaubt es nicht, viel von dem darunter liegenden Prozess zu erfassen. Dieser erste Teil schließt mit einer Diskussion unter den Lernenden ab.

Einheit 2

Zweitens wird ein spezifischeres Video in Betracht gezogen. Trotz seiner informellen Art, das Thema anzusprechen, vermittelt es definitiv ein besseres Verständnis der Materie. Nach der Vorführung des Videos wird der Moderator gebeten, eine Diskussion unter den Teilnehmern über die Risiken öffentlicher Netzwerke anzuregen und, wenn möglich, ihre persönlichen Erfahrungen mitzuteilen.

Lernaktivität 1

Einer der Aspekte, auf den dieses Modul aufmerksam machen möchte, ist die Leichtigkeit, mit der die Bedrohungen durch das öffentliche WLAN vorgetragen werden. Eine kontinuierliche Lernaktivität ist der Versuch, die durch die Videoinhalte dieses Moduls gelernten Vorschläge anzuwenden, vom Restaurant/der Bar, in dem/der die TeilnehmerInnen ihre Mittagspause verbringen, bis zum Bahnhof und Flughafen, wo die TeilnehmerInnen nach der Mobilität nicht mehr nach Hause kommen werden

2. Literaturverzeichnis

https://www. youtube. com/watch? v=4YbXXW3DLQM& ab_channel=Techquickie
https://www. youtube. com/watch? v=1OVTmrXGHyU& ab_channel=CBSBoston
https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
https://goodspeed.io/blog/7-dangers-of-public-wifi.html https://www. youtube.
com/watch? v=NkNgW3TwMy8& ab_channel=TheModernRogue

DIE NUTZUNG VON SOZIALEN NETZWERKEN

Modul 6

Überblick

Zielgruppe

- Lehrkräfte und Ausbilder in der Berufsbildung
- Schüler
- Vertreter von öffentlichen Einrichtungen aus dem Bildungsbereich: lokale, regionale und nationale Behörden

Modul-Übersicht

Soziale Netzwerke haben einen nie dagewesenen Platz im beruflichen, pädagogischen und privaten Bereich des täglichen Lebens der Menschen eingenommen, einschließlich derjenigen von Berufsbildungslehrern und ihren Schülern. Während die Vorteile einer solchen Integration leichter zu erkennen und als integraler Bestandteil der formellen und informellen Bildung anzunehmen sind, wurde den vielfältigen Risiken, die damit verbunden sind, nicht die gebührende Aufmerksamkeit zuteil, und sie werden oft von den Ausbildern selbst ignoriert.

Ein vereinfachter Ansatz, der häufig in Bezug auf das vielschichtige Thema der Sicherheit sozialer Netzwerke verwendet wird, sowie die Komplexität einiger der verfügbaren Schulungsmaterialien reichen nicht aus, um die erforderlichen Kapazitäten zur Vorbeugung und Reaktion auf die durch die Nutzung dieser Plattformen entstehenden Bedrohungen aufzubauen.

Mit diesem Modul wird versucht, den Lernenden ein Grundwissen zu vermitteln und ihre Ausbildungskapazität zu stärken, aber auch ihren persönlichen Umgang hinsichtlich der Sicherheit sozialer Netzwerke zu verbessern.

Lernziele

- Verständnis der Cyber-Risiken und -Bedrohungen im Zusammenhang mit der Nutzung sozialer Mediennetzwerke
- Verstärkung der Auswirkungen von Fehlinformationsprozessen auf die Sicherheit von UGC-Plattformen
- Identifizierung der verschiedenen Arten von Bedrohungen der Cybersicherheit
- Stärkung der Kapazitäten zur Vorbeugung und Reaktion auf Cyber-
- Bedrohungen in den sozialen Medien Bereitstellung von Techniken zur Verwaltung leicht verständlicher Passwörter

Gesamtdauer

2 Stunden

Einheit 1 - Bedrohungen durch soziale Medien

Diese Einheit wird durch den Einsatz einer Power Point-Präsentation erleichtert und durch die Lektüre von Schlagzeilen eingeleitet, die weit verbreitete Geschichten über Opfer von Cyberbedrohungen in den sozialen Medien enthalten (gestohlene Fotos von Prominenten, Menschen, die aufgrund von Fake News über Impfungen ihr Leben verloren haben, usw.). Die Geschichten und der Inhalt werden kontextbezogen angepasst und auf den neuesten Stand gebracht.
An die Präsentation schließt sich eine 10-minütige Gruppendiskussion an, um das Gelernte zu reflektieren und die Fähigkeit der Lernenden zu bewerten, das Thema zu verstehen, aber auch um Raum für weitere Fragen und Feedback zu schaffen.

Lernaktivität 1

Der Trainer präsentiert den Lernenden eine Präsentation mit den folgenden vorgeschlagenen Inhalten (max. 20 Minuten):

Was ist ein soziales Netzwerk?
Ein soziales Netzwerk ist online eine soziale Struktur, die aus Einzelpersonen oder Organisationen besteht, die als Knotenpunkte bezeichnet werden und durch eine oder mehrere spezifische Arten von gegenseitiger Abhängigkeit miteinander verbunden sind, z. B. Freundschaft, gemeinsames Interesse und Austausch von Finanzen, Glaubensbeziehungen, Wissen oder Prestige. Social-Networking-Sites wie Facebook, Tweeter, Instagram usw. werden nicht nur zur Kommunikation oder Interaktion mit anderen Menschen weltweit genutzt, sondern sind auch ein wirksames Mittel zur Unternehmensförderung. Im Gegensatz zu den traditionellen Web- und Medienplattformen dienen die sozialen Medien ausschließlich der Aufnahme und Verbreitung von nutzergenerierten Inhalten (UGC) nach Kriterien (Algorithmen), die auf den von den Nutzern selbst geäußerten und in den Daten registrierten Aktionen und Präferenzen basieren. In diesem Sinne sind alle Nutzer aktive Teilnehmer an der Nachhaltigkeit der Prozesse in sozialen Netzwerken.

Was ist eine Bedrohung durch soziale Medien?
Eine Bedrohung durch soziale Medien kann alles sein, was die Sicherheit eines Kontos gefährdet. Eine Cyber-Bedrohung kann sowohl absichtlich als auch unabsichtlich, gezielt oder nicht gezielt sein, und sie kann von einer Vielzahl von Quellen ausgehen, einschließlich ausländischer Nationen, die Spionage und Informationskrieg betreiben, Kriminellen, Hackern, Virenschreibern, verärgerten Mitarbeitern und Auftragnehmern, die innerhalb einer Organisation arbeiten.

Wie eine Bedrohung durch soziale Medien aussieht

Da soziale Netzwerke eine enorme Anzahl von Nutzern haben und enorme Datenmengen speichern, sind sie ein natürliches Ziel für Spammer, Phishing und bösartige Angriffe. Zu den sozialen Online-Angriffen gehören außerdem Identitätsdiebstahl, Verleumdung, Stalking, Verletzung der persönlichen Würde und Cybermobbing. Hacker erstellen falsche Profile und imitieren Persönlichkeiten oder Marken oder verleumden eine bekannte Person in einem Netzwerk von Freunden.

Aus Datenschutzgründen dürfen Nutzerprofile niemals Informationen im Internet veröffentlichen und verbreiten. Informationen auf persönlichen Homepages können sehr sensible Daten wie Geburtsdaten, Privatadressen, persönliche Handynummern usw. enthalten. Diese Informationen können von Hackern genutzt werden, die Social- Engineering-Techniken anwenden, um in den Genuss solcher sensiblen Informationen zu kommen und Geld zu stehlen.

Wie sich die Bedrohungen durch soziale Medien plattformübergreifend verändern

Die Art und Weise, wie ein Angreifer eine Social-Media-Bedrohung ausführt, hängt von seinen Zielen ab. Facebook erlaubt es den Nutzern, ihre Bilder und Kommentare privat zu halten, so dass ein Angreifer sich oft mit den Freunden eines Zielnutzers anfreundet oder direkt eine Freundschaftsanfrage an einen Zielnutzer sendet, um auf dessen Beiträge zuzugreifen. LinkedIn ist ein weiteres gängiges Ziel in den sozialen Medien, das für Geschäftsnetzwerke bekannt ist. Wenn ein Angreifer es auf ein Unternehmen abgesehen hat, ist LinkedIn eine hervorragende Social-Media-Website, um geschäftliche E-Mails für einen Phishing-Angriff zu sammeln. Da auf vielen Social-Media-Plattformen die Beiträge der Nutzer öffentlich angezeigt werden, können Angreifer unbemerkt Daten sammeln, ohne dass die Nutzer davon wissen. Einige Angreifer gehen noch einen Schritt weiter und verschaffen sich Zugang zu Benutzerdaten, indem sie gezielt Benutzer oder deren Freunde kontaktieren.

Warum ist es wichtig, über OSN-Bedrohungen zu sprechen?

Am 30. Dezember 2020 gibt es fast 4 Milliarden Nutzer in der Internetlandschaft. Von der Gesamtbevölkerung im Internet gibt es 2,7 Milliarden dynamische monatliche Kunden auf Facebook, 330 Millionen aktive Nutzer auf Twitter und 320 Millionen aktive Nutzer auf Pinterest. Die Nutzung von Social-Networking-Sites nimmt exponentiell zu. Betrachtet man nur Facebook, so werden jede Sekunde sieben neue Profile erstellt, 510.000 Kommentare in den 60er Jahren gepostet, 298.000 Statusmeldungen aktualisiert und 136.000 Fotos inderselben Zeit hochgeladen. Da eine riesige Menge an Daten hochgeladen wird, besteht ein hohes Risiko einer Sicherheitsverletzung. Jeder kann bösartige Inhalte hochladen, die in Multimediadaten oder mit verkürzten URLs (Uniform Resource Locators) versteckt sind. Es gibt rund 83 Millionen gefälschte Profile, die illegalen Nutzern oder Fachleuten zu Test- und Forschungszwecken gehören. Täglich werden rund 100.000 Websites gehackt.

Obwohl einige Social-Networking-Sites wie Twitter die Weitergabe privater Informationen an Nutzer nicht zulassen, können erfahrene Angreifer auf diese Informationen schließen. vertrauliche Informationen durch die Analyse der Beiträge von Nutzern und der Informationen, die sie online teilen. Die persönlichen Informationen, die wir online weitergeben, könnten Cyberkriminellen genügen, um an unsere E-Mails und Passwörter zu gelangen.

Der Wert von personenbezogenen Daten

Soziale Mediennetzwerke bieten ihre Dienste oft kostenlos an. Persönliche Informationen sind nicht nur die Währung der sozialen Netzwerke, sondern auch das Hauptziel von Cyberbedrohungen in den sozialen Medien.

Da viele Menschen ihre persönlichen Daten auf Social-Media-Plattformen preisgeben, ist es leicht, einen Angriff zu starten. Angreifer können diese Daten leicht sammeln und zu ihrem Vorteil nutzen. Das Sammeln von Informationen, um sie zu stehlen, ist nur eine Art der Nutzung sozialer Medien für Aufklärungszwecke. Die in sozialen Medien geposteten Informationen könnten dazu verwendet werden, Passwörter zu erlangen oder sich als Geschäftsbenutzer auszugeben.

Mit einer Liste von Zielpersonen könnte ein Angreifer dann Social-Media-Konten nach persönlichen Informationen durchsuchen. Persönliche Informationen können dem Angreifer helfen, das Vertrauen der Zielperson in einem Social Engineering-Angriff zu gewinnen. Sie können auch verwendet werden, um Antworten auf Sicherheitsfragen für eine Kontoübernahme zu erraten oder um sich einem Benutzer mit höheren Privilegien zu nähern. Die Namen von Haustieren, Lieblingssportmannschaften und der Bildungsweg sind allesamt potenzielle Hinweise auf Passwörter oder Antworten auf Fragen, mit denen die Identität des Benutzers überprüft werden kann, um ein Passwort zurückzusetzen.

Warum sollte man sich über OSN-Bedrohungen informieren?

Die benutzerfreundlichen Schnittstellen und Prozesse, die diese Plattformen anbieten, könnten auf Menschen ohne die erforderlichen Kenntnisse und Fähigkeiten für einen sicheren Zugang zu ihren Diensten und Inhalten abgezielt haben.

Aufklärung ist der Schlüssel zum Schutz vor Bedrohungen durch soziale Netzwerke im Internet. Der erste Schritt besteht darin, die Nutzer über die Gefahren aufzuklären, die entstehen, wenn man zu viele Informationen online preisgibt. Selbst auf privat eingestellte Social- Media-Konten könnten für einen Angriff genutzt werden, wenn der Angreifer Zugang zu privaten Feeds erhält. Nutzer sollten niemals private Unternehmensinformationen auf ihren Social-Media-Konten veröffentlichen oder Informationen, die für eine Kontoübernahme verwendet werden könnten.

Der zweite Schritt besteht darin, die Nutzer darüber aufzuklären, wie digitale Inhalte produziert und verbreitet werden und wie sie die Nutzer dazu bringen können, bestimmte Ziele zu verfolgen, für die die Inhalte erstellt wurden. Alle Inhalte der sozialen Medien werden von den Nutzern entsprechend ihrer persönlichen und/oder kollektiven Ziele erstellt und verbreitet. Aus diesen Gründen sind einige dieser Inhalte möglicherweise nicht immer zweckmäßig, wahr oder ethisch vertretbar.
Schließlich müssen die Nutzer über die sichere Nutzung und Wartung der Geräte aufgeklärt werden, über die sie auf die Online-Dienste sozialer Netzwerke zugreifen, da sie normalerweise als Risiko- und Einbruchsvektoren dienen. Einige diesbezügliche Schulungspunkte wurden bereits in anderen Schulungsmodulen erläutert und umfassen:

- Vermeiden Sie es, auf Werbung zu klicken, insbesondere auf Popups, die den Nutzer auffordern, Software herunterzuladen, um Inhalte anzuzeigen.
- Geben Sie keine Passwörter weiter.
- Vermeiden Sie Nachrichten oder Beiträge in sozialen Medien, die zu schnellem Handeln auffordern, als Social Engineering-Technik
- Akzeptieren Sie keine Freundschaftsanfragen von unbekannten Personen, auch wenn der Benutzer mehrere gemeinsame Freunde hat
- Vermeiden Sie die Nutzung von Social-Media-Websites an öffentlichen WLAN-Hotspots (ein gängiger Ort für Angreifer, um Daten mit Hilfe von Man-in-the-Middle-Angriffen [mitm] auszuspähen)
- Ändern Sie regelmäßig die Zugangscodes und Passwörter

Lernaktivität 2

Bitten Sie die Lernenden, ihren eigenen Namen in einer von sozialen Medien betriebenen Suchmaschine oder bei Google zu suchen und alle privaten Informationen aufzulisten, die durch die zahlreichen gefundenen Inhalte aufgedeckt werden können (Geburtsort und - datum, Details und Informationen über Familienmitglieder, Adressen, Telefonnummern, Haustiere, Liebespartner, Hobbys und Vorlieben). Fordern Sie sie auf, sich zu überlegen, wie diese Informationen gegen sie verwendet werden könnten.

Einheit 2 - Arten von Bedrohungen in sozialen Netzwerken

Lernaktivität 1

Bitten Sie die Lernenden, eine Sicherheitsbedrohung aufzulisten, der sie ihrer Meinung nach in den sozialen Medien begegnen könnten, und bitten Sie sie zu erklären, ob sie glauben, dass es diese Bedrohung gab, bevor online soziale Netzwerke existierten.

VERSCHIEDENE BEDROHUNGEN IN SOZIALEN NETZWERKEN UND MEDIEN

Risiken und Bedrohungen lassen sich in drei Kategorien einteilen:

1. Zu den konventionellen Bedrohungen gehören solche, mit denen die Nutzer seit den Anfängen der sozialen Netzwerke konfrontiert sind.
2. Bei den modernen Bedrohungen handelt es sich um Angriffe, die fortgeschrittene Techniken zur Kompromittierung von Benutzerkonten einsetzen.
3. Gezielte Angriffe sind Angriffe, die auf einen bestimmten Benutzer gerichtet sind.

KONVENTIONELLE BEDROHUNGEN

Spam

Spam ist der Begriff für unerwünschte elektronische Massennachrichten. Obwohl E-Mails der herkömmliche Weg sind, um Spam zu verbreiten, sind Social-Networking-Plattformen bei der Verbreitung von Spam erfolgreicher. Die Kommunikationsdaten legitimer Benutzer können leicht von Unternehmenswebsites, Blogs und Newsgroups abgerufen werden. Es ist nicht schwer, die Zielkunden davon zu überzeugen, Spam-Nachrichten zu lesen und darauf zu vertrauen, dass sie geschützt sind. Bei den meisten Spam-Nachrichten handelt es sich um kommerzielle Werbung, sie können auch dazu verwendet werden, sensible Daten von Benutzern zu sammeln, oder sie können Viren, Malware oder Betrug enthalten.

Malware-Angriff

Malware ist eine programmierte Anwendung, die ausdrücklich entwickelt wurde, um ein Computersystem zu kontaminieren oder darauf zuzugreifen, in der Regel ohne das Wissen des Benutzers. Malware kann die Struktur sozialer Netzwerke nutzen, um sich über freigegebene URLs oder OSN-Unteranwendungen wie E-Games oder Plugins zu verbreiten.

Phishing

Ein Phishing-Angriff ist eine Art von Social-Engineering-Angriff, bei dem der Angreifer über gefälschte Websites und E-Mails, die echt zu sein scheinen, an sensible und vertrauliche Informationen wie Benutzername, Passwort und Kreditkartendaten eines Benutzers gelangt.

Im Falle von OSN muss ein Angreifer den Kunden auf eine gefälschte Seite locken, auf der er einen Phishing-Angriff durchführen kann. Um dies zu erreichen, verwendet der Angreifer verschiedene Social-Engineering-Methoden. So kann er beispielsweise eine Nachricht an einen Benutzer senden, in der es heißt: "Ihre persönlichen Bilder sind auf dieser Website freigegeben, bitte überprüfen Sie das". Wenn der Benutzer auf diese URL klickt, wird er auf eine gefälschte Website umgeleitet, die wie eine legitime Social-Networking-Website aussieht.

MODERNE BEDROHUNGEN

Cross-Site-Scripting-Angriff

Cross-Site-Scripting ist ein sehr weit verbreiteter Angriffsvektor unter Angreifern. Bei diesem Angriff wird grundsätzlich ein bösartiges JavaScript im Browser des Opfers mit verschiedenen Techniken ausgeführt. Der Browser kann mit einem einzigen Klick auf eine Schaltfläche gekapert werden, die ein bösartiges Skript an den Server sendet. Dieses Skript wird als Bumerang zum Opfer zurückgeschickt und im Browser ausgeführt. Attraktive Links und Schaltflächen auf beliebten Social-Media-Websites wie Twitter und Facebook können den Benutzer dazu verleiten, URLs zu folgen, sowie Viren-Popup-Warnungen und vielversprechende Anzeigen oder Multimedia-Inhalte, die den Besuch eines Links oder das Klicken auf eine Schaltfläche erfordern, um freigeschaltet zu werden. Manche Nutzer werden aufgefordert, JavaScript-Links in die Adressleiste ihres Browsers zu kopieren und einzufügen. Diese Angriffe können entweder Informationen stehlen oder als Spyware fungieren. Solche Angriffe können auch Computer kapern, um Angriffe auf ahnungslose Benutzer zu starten, während der eigentliche Urheber des Angriffs hinter dem kompromittierten Rechner verborgen ist.

Angriff durch das Klonen von Profilen

Bei diesem Angriff klont der Angreifer das Profil des Nutzers aufgrund von Vorkenntnissen oder online gesammelten Informationen. Der Angreifer kann dieses geklonte Profil entweder in derselben oder in einer anderen Social-Networking-Plattform verwenden, um eine vertrauensvolle Beziehung zu den Freunden des echten Nutzers aufzubauen. Sobald die Verbindung hergestellt ist, gaukelt der Angreifer den Freunden des Opfers vor, dass sie an die Gültigkeit des gefälschten Profils glauben und erfolgreich auf vertrauliche Informationen zugreifen können, die in ihren öffentlichen Profilen nicht freigegeben sind. Dieser Angriff kann auch für andere Arten von Cyberkriminalität wie Cybermobbing, Cyberstalking und Erpressung genutzt werden.

Hijacking

Beim Hijacking kompromittiert der Angreifer das Konto eines Benutzers oder übernimmt die Kontrolle darüber, um Online-Betrug zu begehen. Websites ohne Multi-Faktor- Authentifizierung und Konten mit schwachen Passwörtern sind anfälliger für Hijacking, da Passwörter durch Phishing erlangt werden können. Sobald ein Konto gekapert wurde, kann der Hijacker Nachrichten versenden, den bösartigen Link weitergeben und die Kontoinformationen ändern, wodurch die Kontrolle des Benutzers über sein eigenes Konto und sein Ansehen gefährdet wird.

Inferenz-Angriff

Bei einem Inferenzangriff werden aus anderen Statistiken, die der Nutzer in einem OSN veröffentlicht, vertrauliche Informationen des Nutzers abgeleitet, die dieser möglicherweise nicht preisgeben möchte. Dabei werden Data-Mining-Verfahren für sichtbar verfügbare Daten wie die Freundesliste des Benutzers und die Netzwerktopologie verwendet. Mit dieser Technik kann ein Angreifer die geheimen Informationen eines Unternehmens oder die geografischen und bildungsbezogenen Informationen eines Nutzers finden.

Sybil-Angriff / Botnet

Bei einem Sybil-Angriff behauptet ein Knoten mehrere Identitäten in einem Netzwerk. Dies kann für Social-Networking-Plattformen schädlich sein, da sie eine große Anzahl von Nutzern enthalten, die über ein Peer-to-Peer-Netzwerk verbunden sind. Peers sind die Computerrahmen, die über das Internet miteinander verbunden sind und die ohne einen zentralen Server unkompliziert Daten austauschen können. Dieses Netzwerk von Maschinen kann auch als BotNet bezeichnet werden. Eine Online-Einheit kann mehrere gefälschte Identitäten erstellen und diese Identitäten verwenden, um Junk-Informationen und Malware zu verbreiten oder sogar den Ruf und die Popularität einer Organisation zu beeinträchtigen. So kann zum Beispiel eine Web-Umfrage manipuliert werden, indem verschiedene Internet-Protokoll (IP)-Lieferungen genutzt werden, um eine enorme Anzahl von Stimmen abzugeben, und der Angreifer kann einen echten Kunden überstimmen. Eine ähnliche Armee kann zum Beispiel eine einzige Nachricht mehrfach teilen und ihren Inhalt viral machen.

Clickjacking

Clickjacking ist ein Verfahren, bei dem der Angreifer einen Benutzer dazu verleitet, auf eine andere Seite zu klicken als die, auf die er eigentlich klicken wollte. Der Angreifer nutzt die Schwachstelle des Browsers aus, um diesen Angriff durchzuführen. Er lädt eine andere Seite als transparente Schicht über die Seite, auf die der Benutzer zugreifen möchte. Die beiden bekannten Varianten des Clickjacking sind Likejacking und Cursorjacking. Die vordere Ebene zeigt den Inhalt, mit dem der Kunde geködert werden kann. Wenn der Kunde auf diesen Inhalt tippt, tippt er tatsächlich auf die Gefällt-mir-Schaltfläche. Je mehr Personen den Beitrag mögen, desto mehr verbreitet er sich. Beim Cursor-Jacking ersetzt ein Angreifer den eigentlichen Cursor durch ein benutzerdefiniertes Cursor-Bild. Der eigentliche Cursor wird von seiner eigentlichen Mausposition verschoben. Auf diese Weise kann der Angreifer einen Verbraucher durch geschickte Positionierung von Seitenelementen dazu verleiten, auf die bösartige Website zu klicken.

Angriffe auf die Anonymisierung

In vielen sozialen Netzwerken wie Twitter und Facebook können die Nutzer ihre wahre Identität verbergen oder schützen, bevor sie Daten freigeben, indem sie einen Alias oder einen erfundenen Namen verwenden. Wenn jedoch ein Dritter die wahre Identität des Nutzers herausfinden möchte, kann dies durch die Verfolgung von Cookies, Netzwerktopologien und Benutzergruppeneintragungen geschehen, um die wahre Identität des Kunden aufzudecken. Es handelt sich dabei um eine Art von Information-Mining- Methode, bei der mysteriöse Informationen mit anderen Informationsquellen abgeglichen werden, um die unbekannten Informationen wiederzuerkennen. Ein Angreifer kann Informationen über die Gruppenzugehörigkeit eines Benutzers sammeln, indem er den Verlauf seines Browsers stiehlt und diesen mit den gesammelten Daten kombiniert. Auf diese Weise kann der Angreifer den Benutzer, der die Website des Angreifers besucht, deanonymisieren.

GEZIELTE BEDROHUNGEN

Cybermobbing

Cybermobbing ist die Nutzung elektronischer Medien wie E-Mails, Chats, Telefongespräche und soziale Online-Netzwerke, um eine Person zu schikanieren oder zu belästigen. Im Gegensatz zu traditionellem Mobbing ist Cybermobbing ein kontinuierlicher Prozess, da es ständig über soziale Medien aufrechterhalten wird. Der Angreifer sendet wiederholt einschüchternde Nachrichten, sexuelle Bemerkungen, postet Gerüchte und veröffentlicht manchmal peinliche Bilder oder Videos, um eine Person zu belästigen. Er kann auch persönliche oder private Informationen über das Opfer veröffentlichen, um es in Verlegenheit zu bringen oder zu demütigen. Cybermobbing kann auch zufällig geschehen, obwohl wiederholte Muster solcher E-Mails, Texte und Online-Posts selten zufällig sind.

Cyber-Grooming

Cyber-Grooming ist der Aufbau einer intimen und emotionalen Beziehung zum Opfer (in der Regel Kinder und Jugendliche) mit der Absicht, sexuellen oder psychischen Missbrauch zu erzwingen. Die Daten sind oft wollüstiger Natur durch sexuelle Unterhaltungen, Bilder und Videos, die dem Angreifer einen Vorteil verschaffen, um das Kind zu bedrohen und zu erpressen. Die Angreifer nähern sich Teenagern oder Kindern häufig über gefälschte Identitäten auf kinderfreundlichen Websites, so dass sie schutzlos sind und nicht wissen, dass sie mit dem Ziel des Cyber-Groomings angelockt worden sind. Das Opfer kann aber auch unwissentlich den Grooming-Prozess in Gang setzen, wenn es lohnende Angebote erhält, z. B. Bargeld als Gegenleistung für Kontaktdaten oder persönliche Fotos von sich. Die Anonymität und die Zugänglichkeit der modernen Medien ermöglichen es den Groomern, sich mehreren Jugendlichen gleichzeitig zu nähern, was die Zahl der Fälle von Cyber-Grooming exponentiell erhöht.

Cyberstalking

Cyberstalking ist die Beobachtung einer Person über das Internet, E-Mail oder eine andere Art der elektronischen Korrespondenz, die zu Angst vor Gewalt führt und den psychischen Frieden dieser Person stört. Es handelt sich dabei um eine Verletzung des Rechts auf Privatsphäre einer Person. Der Angreifer spürt die persönlichen oder vertraulichen Informationen des Opfers auf und nutzt sie, um es den ganzen Tag über mit kontinuierlichen und anhaltenden Nachrichten zu bedrohen. Dieses Verhalten macht das Opfer außerordentlich besorgt um seine eigene Sicherheit und löst bei ihm eine Art von Ärger, Angst oder Unruhe aus. Die meisten Menschen geben heutzutage in ihren Profilen in sozialen Netzwerken ihre persönlichen Daten wie Telefonnummer, Wohnort, Region und Termine sowie ihren Aufenthaltsort an. Ein Angreifer kann diese Daten sammeln und sie für Cyberstalking nutzen.

Lernaktivität 2

Bitten Sie die Lernenden, in Zweiergruppen zu arbeiten, und bitten Sie sie, ihren jeweiligen Partner zu verkörpern, während sie ihn 10 Minuten lang interviewen. Fordern Sie sie auf, ihre Antworten zu versuchen, indem sie versuchen, die erforderlichen Informationen aus der Art und Weise, wie sie sich kleiden, aus den Geräten, die sie bei sich tragen, und aus anderen kontextbezogenen Details, die sie für nützlich halten, um sie zu verkörpern, zu erhalten.

Lernaktivität 3

Bitten Sie die Lernenden, eine Minute lang durch ihre Social-Media-Feeds zu scrollen und alle Aufrufe zu Aktionen, Links und Schaltflächen zu zählen, auf die sie klicken sollen. Bitten Sie sie, in der Gruppe darüber nachzudenken, inwiefern jeder dieser Links eine potenzielle Bedrohung darstellt und wie sie entscheiden sollten, wann sie mit dem Inhalt interagieren und wann nicht.

Lektion 3 - Tipps zum Schutz in sozialen Medien

Lernaktivität 1

Verteilen Sie an jeden Lernenden eine oder mehrere Karten mit Screenshots von (erfundenen) Social-Media-Veröffentlichungen von verschiedenen Plattformen und fordern Sie die Lernenden auf, herauszufinden, welche sensiblen Informationen sie aus dem einzelnen Beitrag erhalten können und welche möglichen Bedrohungen von diesem Beitrag ausgehen können.

WAS IST DER SCHUTZ SOZIALER MEDIEN?

Richtlinien zum Schutz sozialer Medien sollen den unbefugten Zugriff auf Ihre Konten in sozialen Medien verhindern, Ihre Online-Identität vor falscher Identität oder Datendiebstahl schützen und Ihr Netzwerk vor bösartigen Identitäten oder Inhalten in sozialen Medien bewahren.

Da die Modalitäten und Ziele von OSN-Bedrohungen häufig von der Art der Plattform abhängen, sollten auch einige spezifische Praktiken zur Verhinderung von Bedrohungen entsprechend berücksichtigt werden.

ALLGEMEINE PRAKTIKEN

Verwenden Sie ein sicheres Passwort: Um die Sicherheit der Konten zu gewährleisten, sollten die Benutzer ein sicheres Passwort wählen. Es sollte nicht zu kurz sein, da kurze Passwörter leicht erraten werden können. Es sollte lang genug sein und muss alphanumerische Werte mit einigen Sonderzeichen enthalten. Benutzer sollten nicht dasselbe Passwort verwenden, das sie auch für andere Konten benutzen, denn wenn ein Angreifer dieses Passwort in Erfahrung bringt, kann er alle Konten dieses Benutzers kompromittieren.

Begrenzung der Standortfreigabe: Heutzutage ist die Weitergabe des Standorts ein Trend geworden. Viele Social-Networking-Sites haben auch eine Geotagging-Funktion eingeführt, die automatisch den geografischen Standort eines Nutzers markiert, wenn dieser Multimedia-Inhalte in soziale Medien hochlädt. Der Nutzer muss die Funktion auf manuell umstellen, damit der Standort nicht automatisch markiert wird. Die Nutzer müssen ihre Multimediainhalte sehr sorgfältig online hochladen, da sie sensible Metadaten enthalten können, und es wird empfohlen, das Geotagging auf allen mobilen Geräten und Konten auf den manuellen Modus umzustellen.

Seien Sie bei Freundschaftsanfragen wählerisch: Es wurde beobachtet, dass viele Nutzer Freundschaftsanfragen annehmen, ohne das vollständige Profil des Anfragenden zu analysieren. Im Allgemeinen werden Freundschaftsanfragen auf der Grundlage gemeinsamer Freunde angenommen. Wenn der Anfragende einige gemeinsame Freunde hat, akzeptieren sie die Anfrage. Manchmal machen Angreifer ihr Profil absichtlich attraktiv oder sie geben sich als ein Konto aus. Wenn also die Person, die eine Freundschaftsanfrage sendet, unbekannt ist, sollte man diese Freundschaftsanfrage ignorieren. Es könnte sich um ein gefälschtes Konto handeln, das versucht, sensible Informationen zu stehlen.

Seien Sie vorsichtig mit dem, was Sie teilen: Nutzer sollten mit ihren Beiträgen vorsichtig sein, da sie ihre persönlichen Daten und manchmal auch die anderer Personen preisgeben können. Viele Organisationen haben strenge Regeln und Vorschriften für den Austausch von Informationen und Multimedia-Inhalten. Es gibt viele Berichte über Menschen, die wegen der illegalen Weitergabe von Informationen entlassen wurden.

Diese Situation kann vermieden werden, wenn die Mitarbeiter gut über die Protokolle der Organisation, in der sie arbeiten, bezüglich der Bilder, Videos und Nachrichten, die sie online veröffentlichen, informiert sind. Die unrechtmäßige Weitergabe von Informationen kann dem Ruf eines Unternehmens auf dem Markt schaden, ebenso wie seinen Daten und seinem geistigen Eigentum.

Achten Sie auf Links und Anwendungen von Drittanbietern: Illegitime Nutzer können sich Zugang zum Konto einer anderen Person verschaffen und sensible Informationen erhalten, indem sie einen bösartigen Link teilen. Heutzutage werden verkürzte URLs auf verschiedenen Social-Media-Plattformen sehr beliebt. Diese verkürzten URLs können mit bösartigem Code oder Skripten verschleiert sein. Diese Skripte versuchen, die persönlichen und vertraulichen Informationen eines Benutzers zu sammeln, was dazu dienen kann, die Privatsphäre des Benutzers zu verletzen. Außerdem können Hacker Schwachstellen in Anwendungen von Drittanbietern ausnutzen, die in viele beliebte soziale Netzwerke integriert sind. Ein Beispiel für eine solche Anwendung eines Drittanbieters sind Spiele, die in sozialen Online-Netzwerken gespielt werden können und bei denen die öffentlichen Daten eines Nutzers abgefragt werden, um ihre Dienste in Anspruch zu nehmen. Diese Informationen können an Außenstehende oder Dritte weitergegeben werden. Um dieses Risiko zu vermeiden, sollten die Benutzer bei der Installation von Anwendungen Dritter in ihrem Profil vorsichtig sein.

Installieren Sie Internet-Sicherheitssoftware: Einige Bedrohungen, deren Muster bekannt ist, können durch Antivirenprogramme leicht erkannt werden. Bedrohungen wie Cyber-Grooming und Cyber-Mobbing können bis zu einem gewissen Grad mit Hilfe von Antiviren-Software erkannt werden.

TIPPS FÜR DIE NUTZUNG SOZIALER NETZWERKE UND DAS TEILEN VON MULTIMEDIA-INHALTEN

- Man sollte keine sensiblen Informationen in seinen Fotos oder Bildunterschriften veröffentlichen. Es kann gefährlich sein, zu viele private Informationen in einem Profil preiszugeben.
- Die Weitergabe des aktuellen Standorts in sozialen Medien sollte vermieden werden. Die von verschiedenen Multimedia-Plattformen angebotenen Geotagging-Dienste sollten manuell ausgeschaltet werden.
- Wenn eine Anwendung über einen längeren Zeitraum nicht genutzt wird, ist es besser, den Zugang zu dieser Anwendung zu sperren. Es gibt so viele Anwendungen von Drittanbietern, die Social-Media-Konten zur Anmeldung verwenden. Aus Sicherheits- und Datenschutzgründen sollte man nur vertrauenswürdigen Anwendungen Zugang gewähren.

Aktivieren Sie nach Möglichkeit die zweistufige Authentifizierung für alle Ihre Konten in sozialen Medien. Dies bietet eine zusätzliche Sicherheitsebene für das Konto. Für den Fall, dass ein Angreifer das Passwort eines Nutzers herausfindet, benötigt dieser noch einen zweiten Faktor, um sich zu authentifizieren. Der zweite Faktor besteht aus einem einmaligen, zeitabhängigen Code, den die Nutzer per SMS auf ihr Mobiltelefon erhalten.

DIE NUTZUNG VON SOZIALEN NETZWERKEN

Modul 6

SO BEWEGEN SIE SICH SICHER IN DISKUSSIONSFOREN

Man sollte aufpassen, wenn man auf Links klickt, die von verschiedenen Quellen bereitgestellt werden. Es könnte sich um eine verdächtige Website handeln, die versucht, die Anmeldedaten des Benutzers zu erhalten.

Die Nutzer sollten immer ein Auge auf die URL der Website haben. Schädliche Websites können zwingend ununterscheidbar von echten Websites aussehen. Die URL kann jedoch geringfügige Unstimmigkeiten enthalten, wie z. B. eine leicht abweichende Schreibweise (z. B. eine "0" statt eines "o", die bei schnellem Lesen nicht zu erkennen ist) oder einen alternativen Domänennamen.

Seien Sie vorsichtig mit Mitteilungen, in denen der Kunde aufgefordert wird, umgehend zu handeln, in denen etwas angeboten wird, das unrealistisch klingt, oder in denen persönliche Informationen verlangt werden.

TIPPS ZUR SICHERHEIT IN SOZIALEN NETZWERKEN

- Jede Plattform bietet Einstellungs-, Konfigurations- und Datenschutzbereiche, mit denen eingeschränkt werden kann, wer und welche Gruppen verschiedene Aspekte des Nutzerprofils sehen können. Die Datenschutzeinstellungen, die von den Websites als Standardeinstellungen bereitgestellt werden, sollten nicht unverändert gelassen werden.
- Je mehr Details weitergegeben werden, desto einfacher ist es für einen Angreifer, diese Informationen zu nutzen, um Identitäten zu stehlen oder andere Cyberstraftaten zu begehen. Daher sollte der Informationsaustausch begrenzt werden.
- Bevor man eine Freundschaftsanfrage annimmt, sollte man das Profil des Anfragenden vollständig überprüfen. Man kann verschiedene Gruppen für den Austausch unterschiedlicher Informationen erstellen, z. B. eine Gruppe für Kollegen und Familie

VERHALTEN IN BERUFLICHEN NETZWERKEN

- Um ein professionelles Netzwerk sicher nutzen zu können, sollte man also die Angaben anderer Nutzer prüfen, bevor man sie in seine Kontaktliste aufnimmt. Im Allgemeinen gibt ein Gegner nicht viele Details über seine Karriere an.
- Ein Nutzer sollte prüfen, ob das Profil einer Person Rechtschreib- oder Grammatikfehler enthält, denn wenn sich jemand um eine Stelle bewirbt, sollte es sehr gut geschrieben sein und keine Rechtschreib- oder Grammatikfehler enthalten. Es sollte genaue und gut präsentierte Informationen über die Person enthalten.
- Wenn ein Nutzer in einem beruflichen Netzwerk sicher bleiben will, ist es sinnvoll, auf die Beständigkeit der Karriere einer Person zu achten. Ein Profil, das sich in kurzer Zeit ständig und definitiv ändert, wird von Angreifern am häufigsten als Lockmittel verwendet. Wenn der Betrüger eine bestimmte Art von Organisation oder eine vertikale Ebene ins Visier nehmen will, kann er einfach eine neue Position hinzufügen, die für seine Ziele relevant sein könnte.

Man sollte auch Informationen gegenprüfen. Wenn eine Person behauptet, aus dem Unternehmen des Arbeitgebers zu stammen, kann der Nutzer das Verzeichnis des Unternehmens überprüfen und sollte nicht zögern, sich bei der Personalabteilung des
Unternehmens zu vergewissern.

Lernaktivität 2

Bitten Sie die Lernenden zu erklären, wer ihrer Meinung nach Zugriff auf den letzten Beitrag hat, den sie in ihrem Lieblings-Netzwerk veröffentlicht haben. Helfen Sie ihnen schließlich, ihre Privatsphäre-Einstellungen zu überprüfen und zu sehen, wie viel von dem, was sie gesagt haben, der Wahrheit entspricht. Eröffnen Sie eine Gruppendiskussion über ihre Ergebnisse.

Lernaktivität 3

Bitten Sie die Lernenden, sich die Karten, die sie während der **Lernaktivität 1 dieser Einheit** erhalten haben, noch einmal anzuschauen, und fragen Sie sie, ob sie zusätzliche Risiken in den zuvor vorgestellten Veröffentlichungen in den sozialen Medien erkennen können. Fragen Sie sie, was sie tun würden, um diese Risiken zu mindern.

2. Lernergebnisse für das Modul

Wissen

- Cyber-Risiken und -Bedrohungen im Zusammenhang mit der Nutzung von sozialen Mediennetzwerken
- Sicherheit von UGC-Plattformen (UGC = User Generated Content)

Fähigkeiten

Identifizierung verschiedener Arten von Bedrohungen der Cybersicherheit

Kompetenzen

- Vorbeugung und Reaktion auf Cyber-Bedrohungen in sozialen Medien
- Verwaltung komplexer Passwörter

3. Literaturverzeichnis

https://www.proofpoint.com/us/threat-reference/social-media-threats
https://www.digitalshadows.com/blog-and-research/how-cybercriminals-weaponize- social- media/
https://www.researchgate.net/publication/221663523_Cyber_Threats_In_Social_Networking_Websites
https://www.researchgate.net/publication/324860729_Social_Media_Security_Risks_Cyber_Bedrohungen_und_Risiken_Vermeidungs-_und_Minderungs_Techniken

Co-funded by the
Erasmus+ Programme
of the European Union

YBER.VET.EU

VERBESSERUNG DER CYBERSECURITY-BEREITSCHAFT DES EUROPÄISCHEN BERUFSBILDUNGSSEKTORS

LEHR- UND ANSCHAUUNGS MATERIALIEN

SCHULUNGS- UND LEHRMATERIAL FÜR DEN BERUFSBILDUNGSSEKTOR ZUM THEMA CYBERSICHERHEIT

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

EINFÜHRUNG IN DIE MATERIALIEN

GAME JAMS

INTRO

Vom Herbst 2021, im Zusammenhang mit dem Europäischen Monat der Cybersicherheit, bis zum Frühjahr 2022 organisierten die Partner des CYBER.VET.EU Projekts mehrere GameJams in den Ländern der Partner. Junge Menschen waren daran beteiligt, um ihnen die Möglichkeit zu geben, sich mit Themen der Cybersicherheit auseinanderzusetzen und neue Werkzeuge zu erlernen.

Das Hauptziel bestand darin, das Bewusstsein für die Cybersicherheit zu schärfen. Wir wendeten uns dem Prozess der "Gamification" zu, um eine Lösung zu erhalten, die einfach zu übernehmen, schnell zu implementieren, mit der Zeit skalierbar und integrativ ist. Der Prozess der "Gamification", definiert als "die Anwendung von Spielmechanismen in nicht spielerischen Kontexten mit dem Ziel, das Engagement zu fördern und die Motivation zu steigern", ist eine bewährte Methode, um die BenutzerInnen bei Lernaktivitäten zu halten, mit großartigen Ergebnissen auch über kurze Zeiträume hinweg, dank der Nutzung von Unterhaltung, die die TeilnehmerInnen motiviert, sich mehr mit dem Material zu beschäftigen und zu üben. Diese Ausgabe ist eine Kombination aus Leitfaden, Schulung und Übung und lässt sich leicht aktualisieren, wenn neues Material hinzugefügt werden soll.

ERGEBNISSE VON AKTIVITÄTEN / GAME JAMS

- Erhöhtes Bewusstsein für digitale Sicherheit
- Stärkung des Bewusstseins für digitale Sicherheit im Umfeld der Teilnehmer (Familie, Freunde, Kollegen)
- Verringerung der Malware-Erfolgsrate innerhalb der Institutionen
- Verringerung der Datenlecks
- Erhöhtes Interesse für den Cybersicherheitssektor als Beschäftigungsmöglichkeit

AEII / INERCIA DIGITAL [ES]

AKTIVITÄTEN

Die wichtigsten Aktivitäten, die von den spanischen Partnern AEII und Inercia Digital durchgeführt wurden, waren: Hackathon
GameJams
Info-Tage
Internationale Konferenz
Verbreitungsveranstaltung

ERGEBNISSE

Die GameJam-Sitzungen in Spanien lieferten einige nützliche Ergebnisse, die hier eingesehen werden können:
https://scratch.mit.edu/projects/611211889/
https://scratch.mit.edu/projects/611201682/
https://www. youtube. com/watch? v=3QFI9iB0iJU& t=124s

ON SCRATCH

https://scratch.mit.edu/projects/611211889/
Cybersecurity - Under Attack

https://scratch.mit.edu/projects/610354561/
Spanisch

https://scratch.mit.edu/projects/611201682/
https://scratch.mit.edu/projects/714361293/
Spanisch
https://scratch.mit.edu/projects/714362963/
Spanisch
https://scratch.mit.edu/projects/714362911/
on phishing - a remix
https://scratch.mit.edu/projects/606933322
on phishing - Englisch

AEII / INERCIA DIGITAL [ES]

GAME JAM

AEII / INERCIA DIGITAL [ES]

Hackathon

Die spanischen Partner AEII und Inercia Digital nahmen vom 20. bis 22. Oktober 2021 an einem Online-Hackathon mit 47 Teilnehmern teil, darunter viele IT-Experten. https://www.comprometidosporelfuturo.com/proyectos# unterstützt von Boehringer Ingelheim in Spanien.

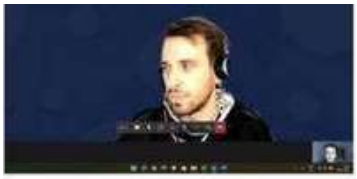
ZU LÖSENDES PROBLEM

Cybermobbing ist eine der größten Internetgefahren für junge Menschen. Häufig finden sich Beiträge mit beleidigendem Inhalt, die dazu benutzt werden, die Opfer zu belästigen und zu verhöhnen.
Cybermobbing verursacht bei den Opfern häufig schwere Störungen wie posttraumatische Belastungsstörungen, Depressionen, Selbstmordgedanken und -verhalten oder Angstzustände.

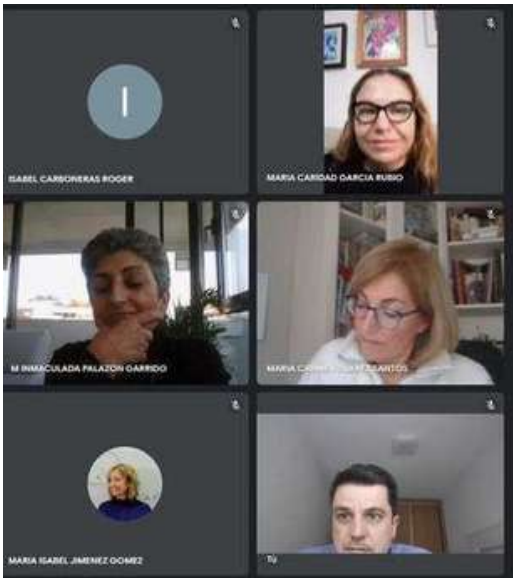
Die Aufgabe hier war, zu untersuchen und zu analysieren, was junge Menschen über Sicherheit wissen, und sie anschließend für die Risiken zu sensibilisieren, denen sie in ihren Bildungseinrichtungen und im täglichen Leben ausgesetzt sind.
Ziel war es, mittels 'Gamification' das Bewusstsein von Schülern und Lehrern für Fragen der Sicherheit bei der Nutzung der neuen Technologien im Alltag zu schärfen.

ERGEBNISSE

- Spiel und Animation im Zusammenhang mit Cybersicherheit in der Bildung
- Einbeziehung von öffentlichen Verwaltungen, berufsbildenden Schulen, IT-Experten, Lehrern, Schülern und Projektpartnern
- Erstellung von kurzen interaktiven Videos



AEII / INERCIA DIGITAL [ES]



Zahlreiche Umfragen haben gezeigt, dass das Wissen über Cybersicherheit bei Lehrern und Schülern in den Berufsbildungszentren in Spanien im Allgemeinen immer noch gering ist. Aus diesem Grund sind dieses Projekt und andere ähnliche Projekte in Spanien sehr wichtig.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

GAME JAM

NGO Nest Berlin, Extrafondente Open Source - EOS und IASIS haben im Februar 2022 gemeinsam eine GameJam Session durchgeführt. Der GameJam begann am Samstag, den 12. Februar, und dauerte insgesamt 6 Tage. Die nationalen Teams entwickelten und arbeiteten gemeinsam an einem Spielentwurf (für ein Online- oder Brettspiel).

Eine unabhängige Jury wurde einberufen und gebeten, den Spielentwurf nach gemeinsamen Leitlinien und einer Bewertungsvorlage zu bewerten.

Das Siegerteam erhielt ein sechsmonatiges Mentoring sowie technische Ressourcen, um die Spielidee weiterzuentwickeln.

ÜBER DAS SPIEL

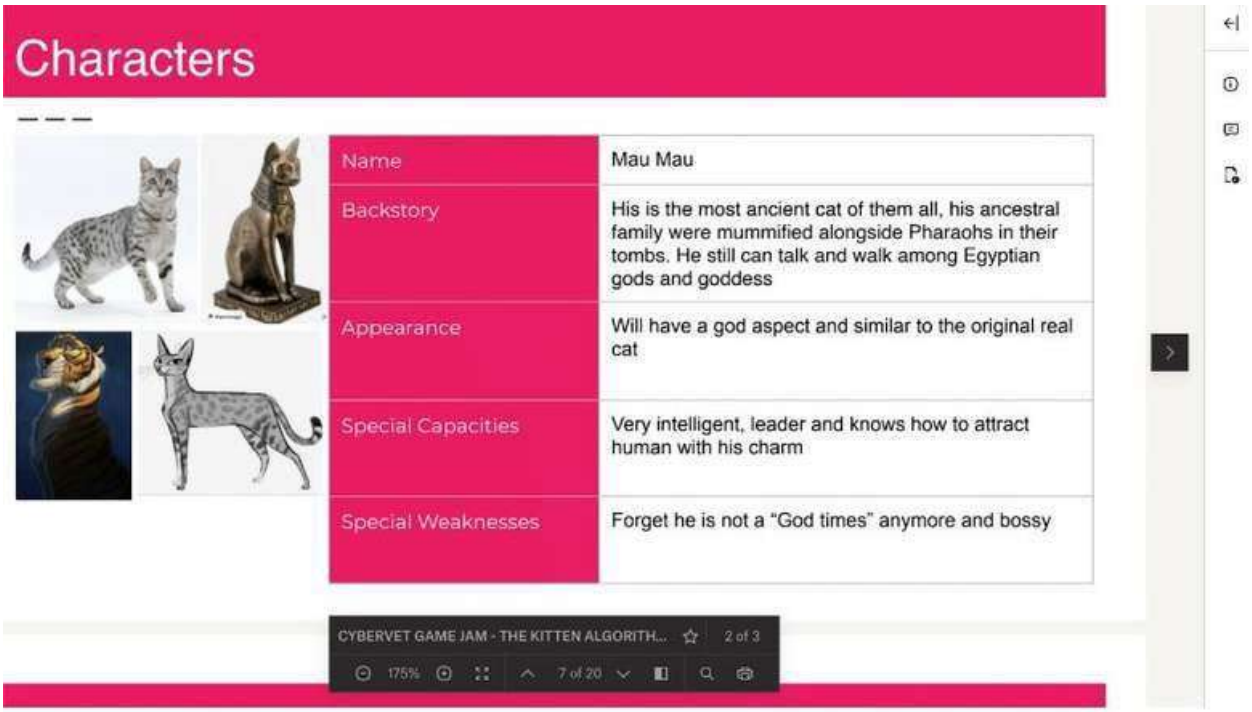
Es handelt sich um ein strategisches Brettspiel für 2 bis 6 Spieler, das etwa 30 bis 60 Minuten Spielzeit benötigt. In diesem Spiel trickst du die Menschen aus, um sie davon zu überzeugen, dass du die beste Katze bist und mehr Prestige bekommst, indem du so viele menschliche Katzendiener wie möglich bekommst. Halte die Augen offen, denn die anderen Boss-Katzen werden aktiv versuchen, deinen Weg zu den Menschen zu sabotieren und den Ruhm für sich selbst zu erobern. Traue ihren niedlichen Gesichtern nicht!

Du verlierst das Spiel, wenn du nicht eine hohe Anzahl von Menschen als Diener hast oder die 10. Runde vorbei ist und keiner der Spieler mindestens 4 Menschen unter seinem Kommando hat.

Die Schwierigkeit besteht darin, dass es 6 Bosse gibt, die versuchen, die Menschen auszutricksen, damit sie ihre Diener werden und die Bosse sie kontrollieren können, aber alle haben das gleiche Ziel und einige könnten den Menschen sogar helfen, sich von der Kontrolle der Katzen zu befreien.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

Mau Mau



LECSA (LV)

GAME JAM

Der lettische Partner LECSA organisierte vom 27. September bis 1. Oktober 2021 eine GameJam-Session. Aufgrund der pandemischen Einschränkungen und der unterschiedlichen Standorte der Teilnehmer wurde die Veranstaltung als Hybridveranstaltung organisiert (vor Ort in der Technischen Schule Saldus und über die Plattform Zoom). Während der Veranstaltung wurden 6 Teams (4-5 Personen pro Team) gebildet, die an der Entwicklung von Spielprototypen arbeiteten. Um greifbare Ergebnisse zu erzielen, sah das Game Jam-Konzept die Entwicklung von zwei Arten von Spielen vor - Computer- und Brettspiele.

AKTIVITÄTEN

August - September 2021 war der Planung und Organisation der Veranstaltung gewidmet (Suche nach Experten für Cybersicherheit und Spielentwicklung, Informationsverteilung an potenzielle Teilnehmer, Planung der Tagesordnung und Festlegung von Kriterien für das Spiel, usw.)

Multiplikator-Veranstaltung - Aktuelles zu Cyberangriffen (27.09.2021): Vorstellung des CYBER.EU.VET-Projekts und Vortrag über die Trends bei Cyberangriffen mit Herrn Armins Palms, Cybersecurity-Experte von CERT.LV (IT Security Incident Response Institution of the Republic of Latvia)
Anzahl der Teilnehmer: 26 Personen
Ort: Technische Schule Saldus (Stadt Saldus) und ZOOM-Plattform

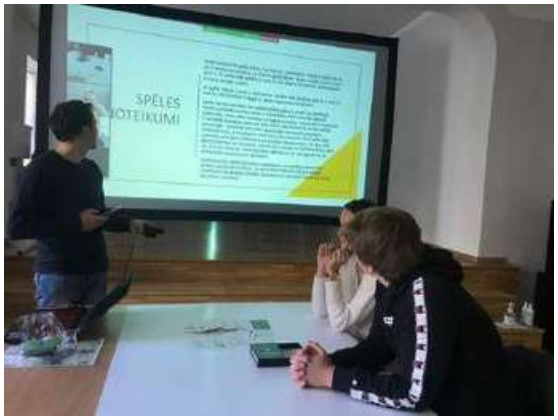
Ankündigung des Game Jame (27.09.2021): Definition und Diskussion über die aktuellen Herausforderungen im Bereich der Cybersicherheit (Bedarfsanalyse); Bildung von Teams, Treffen mit Mentoren und Diskussion über die weitere Arbeit (Workshop zur Spiele-Engine Unity), Brainstorming zur Spielidee und zum Konzept. Game Jam-Aktivitäten im Gange (28.09-30.09.2021): Teams arbeiteten an der Entwicklung von Prototypen, bei Bedarf wurde Rücksprache mit Mentoren gehalten.
Pitching über den Fortschritt (30.09.2021): Pitching über die Konzepte des Spiels und den Arbeitsfortschritt, um Anregungen der Mentoren zu erhalten.

Großes Finale (01.10.2021): Vier Teams haben ihre Ergebnisse präsentiert und die Mentoren haben eine Bewertung abgegeben. Ein Team, das ein Computerspiel entwickelt hat, ist ausgeschieden. Abschluss der Veranstaltung und informelle Diskussion.
Anzahl der Teilnehmer: 30
Ort: Technische Schule Saldus und ZOOM-Plattform

LECSA (LV)

ERGEBNISSE

1. Prototyp des Online-Spiels - The Virus
2. Brettspiel - Karten über Sicherheit
3. Brettspiel - Cyberwar
4. Kartenspiel - Cyber Mind



BEISPIEL Cyber Mind - ein Kartenspiel für 2 oder 4 Spieler

Cyber Mind ist ein pädagogisches Kartenspiel mit Quiz-Elementen. Die Hauptaufgabe des Spiels besteht darin, die Grundlagen der alltäglichen Sicherheit im Internet zu vermitteln und aufzuzeigen, was man sich durch unbedachte Handlungen im Internet antut. Es behandelt Themen wie Internetsicherheit und Datenschutz im Zusammenhang mit der Nutzung sozialer Netzwerke. Im Ergebnis des Spiels sollen die Menschen (Spieler) in der Lage sein, Betrugsversuche im realen Leben zu erkennen.

Entwickelt vom Team Veiksminieki (aus dem Lettischen: Erfolgreiche Menschen), Studenten der Technischen Schule Saldus während des Game Jam in Lettland (Oktober 2021): Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere & andere.

Niveau: grundlegend (für Anfänger). Zielgruppe: Schüler, Studenten, Lehrer und Eltern

Das Spiel enthält: 50 Karten, 2 Gesundheitspads (zum Zählen der Gesundheit der Spieler), 2 Würfel und Regelkarte.

LECSA (LV)

GAME JAM

ÜBER

Die Versuche von Cyberangriffen in der Welt nehmen täglich zu. Deshalb hat die Weltregierung die Idee, ein Turnier zu veranstalten, um Personen zu identifizieren, die Cyberrisiken mit sich bringen, und ihnen entgegenzuwirken.

Lernspiel, das dabei hilft, die wichtigsten Arten von Cyberangriffen, Vorbeugungs- und Beseitigungsmethoden kennenzulernen, indem man sich selbst oder sein Team schützt und einen Gegenangriff auf den Gegner startet. Ziel des Spiels ist es, dem/den Gegner/n das Leben zu nehmen.

WIE MAN SPIELT - SPIELE + REGELN

Anzahl der Spieler: 2 oder 4 Personen (1 gegen 1 oder 2 gegen 2).

Jeder Spieler oder jedes Team (bei 2 gegen 2) hat zu Beginn des Spiels "100 Leben" (Health=HP). Das Zählen der Lebenspunkte erfolgt mit Hilfe von schwarzen Notizblöcken oder anderen verfügbaren Notizen.

Beauftragen Sie, wenn möglich, eine separate Person, die den Verbrauch von Energie und Gesundheit der Spieler verfolgt und berechnet. Andernfalls müssen die Spieler dies selbst tun.

Jeder Spieler erhält 5 Karten. Wenn das Spiel 2 gegen 2 gespielt wird, haben beide Spieler "eine gemeinsame Hand" im Team oder 10 Karten zusammen.

Es gibt drei Arten von Karten: Angriffskarten (rot), Schildkarten (gelb) und Lebens- oder Heilungskarten (grün).

Das Spiel wird in Runden gespielt. Der Spieler/das Team, der/das die höchste Zahl würfelt, beginnt das Spiel.

Jede Karte kostet Energie. Zu Beginn jeder Runde würfelt der Spieler mit 2 Würfeln, um eine Energie zu bestimmen, die oben auf der Karte (in blau) angegeben ist. Die Karten müssen gespielt werden, damit die gewürfelte Energiemenge nicht überschritten wird. Der Spieler/das Team, der/das die Runde anführt, kann angreifen (mit Angriffskarten), sich schützen (Schildkarten) oder Leben hinzufügen (Heilungskarten), während Zweitplatzierte nur Angriffs- und Schildkarten verwenden können, um ihre Lebensschwäche zu minimieren.

Beachten Sie, dass die maximale Anzahl von Leben pro Spieler/Team während des Spiels 100 HP betragen kann (z.B. wenn die Summe von Leben und Energie nach der Runde insgesamt 110 HP ergibt, bleibt Ihre Anzahl von Leben trotzdem - 100 HP). Das Spiel endet, sobald ein Spieler/Team keine Leben mehr hat (0 Leben). Wenn das Spiel keine Karten mehr hat, müssen Sie die Karten vom Stapel neu mischen.

LECSA (LV)

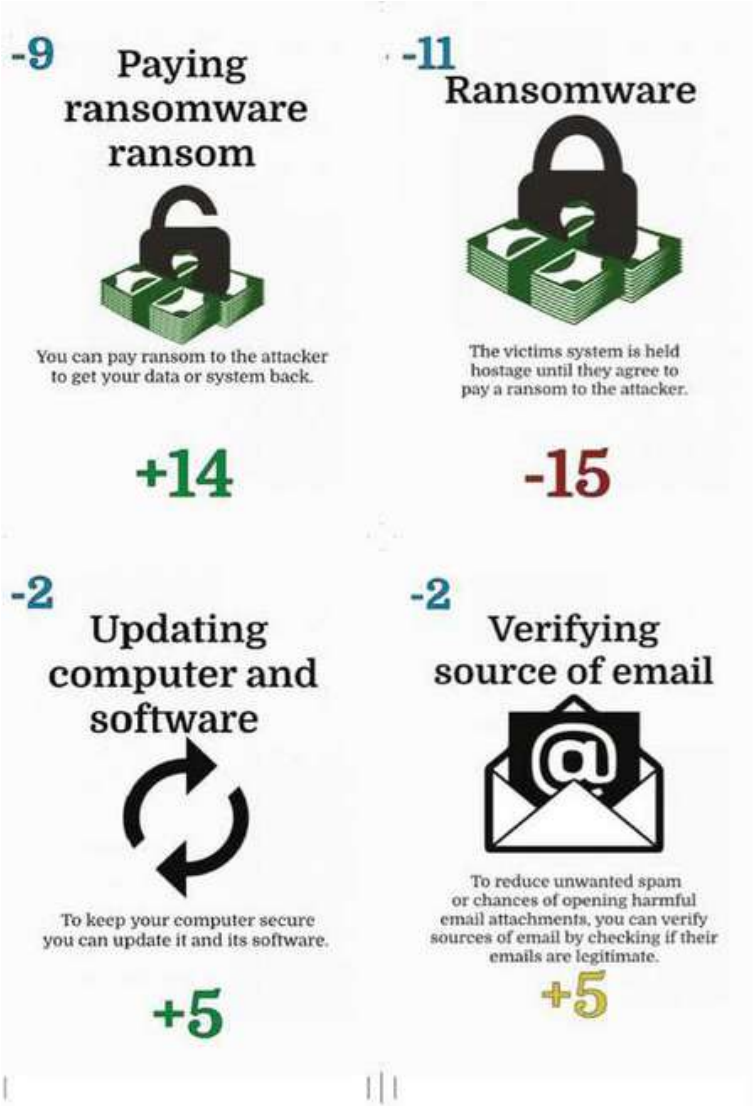
Beispiele für Karten

In **Blau** - Energie

In **Rot** - Angriffskarten

In **gelb** - Schildkarten

In **grün** - Heilkarten



Beispiel für die Berechnung der HP (Health Points)

BEISPIEL Cyberwar - ein Brettspiel

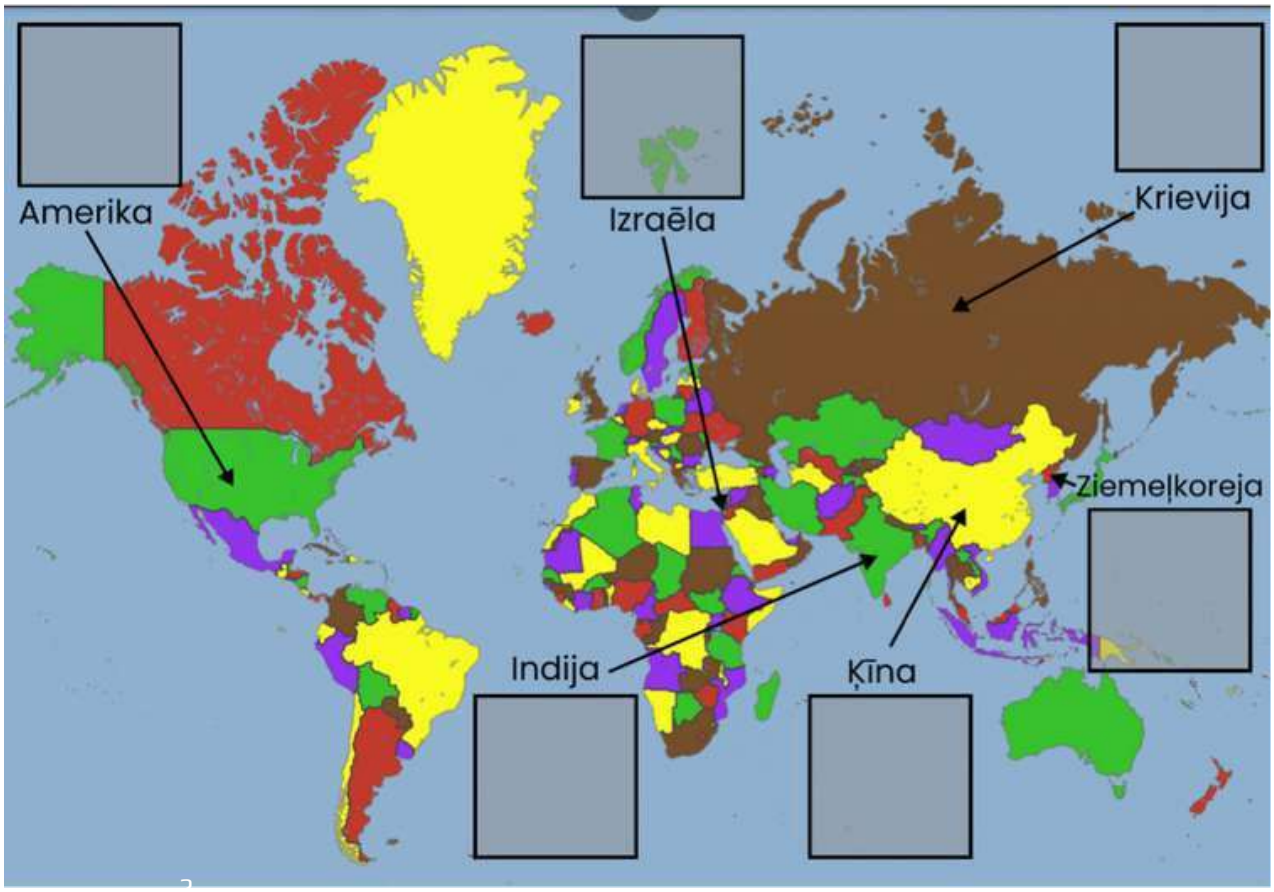
Entwickelt vom Team Exodus (Studenten der Technischen Schule Saldus)
Leiter des Teams: Valdemārs Šperbergs.

2-6 Spieler < - > Geeignet für Personen ab 15 Jahren
Ein Brettspiel mit starker Betonung auf Taktik und Zufall (Chance).

Niveau: Lernspiel für jene, die schon etwas über Cybersicherheit wissen.
Das **Spiel enthält:** Weltkarte, 2 Würfel, Server, Karten mit den Funktionen "Angriff", "Verteidigung" oder "Reaktion", Legende der Schwachstellen.

ÜBER DAS SPIEL

Das Ziel des Spiels ist es, das vom Spieler vertretene Land zu schützen und andere Länder anzugreifen, um den Cyberwar zu gewinnen. In Cyberwar muss jeder Spieler ein Land wählen, das er vertritt. Jeder Spieler hat einen Server mit 3 Sicherheitslücken. Das Ziel des Spielers ist es, die Server anderer Länder zu hacken, indem er zwei von drei Schwachstellen ausnutzt, oder zwei von drei Schwachstellen auf seinem eigenen Server zu beheben.



LECSA (LV)

WIE GESPIELT WIRD

Die Spieler wählen das Land aus, das sie vertreten wollen, und platzieren ein Serverobjekt an einem bestimmten Ort auf der Karte. Jedes Land hat seine eigenen Boni.

Jeder Spieler zieht (nimmt) zufällig 3 Schwachstellen - eine aus jeder Schwierigkeitsstufe - und legt sie verdeckt an die entsprechenden Stellen auf seinen Serverfeldern. Die Schwachstellen sind den Spielern nicht bekannt.

Schwachstellen haben 3 Schwierigkeitsgrade. Der Schwierigkeitsgrad bestimmt auch, wie viele Angriffe erforderlich sind, um eine Schwachstelle auszunutzen (siehe "Angriffe"), und wie viele Züge es braucht, um die Schwachstelle zu beheben (siehe "Verteidigung").

Das Spiel findet in Runden statt, in denen folgende Aktionen (Züge) ausgeführt werden können - **Scannen**, **Angriff** und **Verteidigung**. Die Spieler bestimmen die Reihenfolge der Spieler, indem sie zwei Würfel werfen.

START

Jeder Spieler erhält zu Beginn jeder Runde 4 Karten. Am Ende der Runde ist es möglich, 2 Karten zu behalten oder sie gegen vorhandene auszutauschen.

Die 1. Runde ist eine Scanning-Runde, in der keine Angriffs- oder Verteidigungskarten erlaubt sind. In den folgenden Runden können die Spieler wählen, ob sie scannen oder angreifen oder versuchen, ihre Schwachstellen zu reparieren (siehe Verteidigung). Das Spiel wird Runde für Runde fortgesetzt, bis eine Siegbedingung erreicht ist.

Scannen

Der Angreifer wählt ein Land aus, das er auf seine Verwundbarkeit hin überprüft (z. B. "Ich überprüfe eine russische Verwundbarkeit der Stufe 2"). Der Spieler führt ein Scanning durch - würfelt mit zwei Würfeln und wendet die Boni seines Landes an, vergleicht mit dem Schwierigkeitsgrad der Verwundbarkeit + Boni des Landes des Opfers.

Wenn der Angreifer eine Zahl gewürfelt hat, die dem Schwierigkeitsgrad der Schwachstelle des Opfers entspricht oder darüber liegt, kann der Angreifer die gescannte Schwachstelle betrachten. Länderboni werden nicht hinzugefügt, wenn Sie selbst scannen.

Schwierigkeitsgrade

1. - Spieler muss mindestens die Zahl 4 würfeln (ohne Länderbonus)
2. - Spieler muss mindestens die Zahl 8 würfeln (ohne Länderbonus)
3. - Der Spieler muss mindestens 11 würfeln (ohne Länderbonus).

ANGRIFF

Der Spieler nennt das Ziel des Angriffs (z.B. "Ich greife eine russische Schwachstelle der Stufe 2 an") und deckt die Angriffskarte für alle Spieler auf und legt sie neben die Schwachstelle.

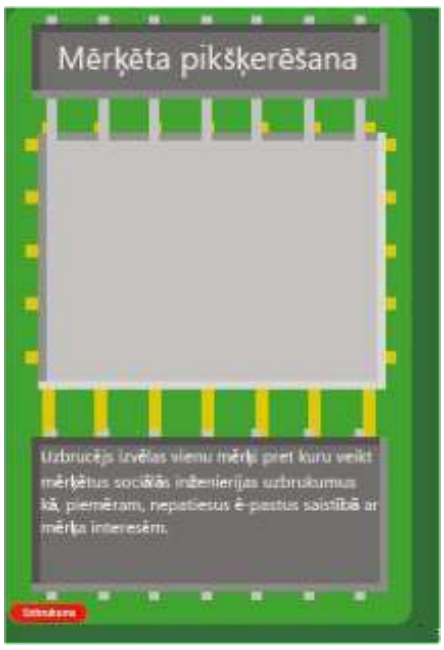
Der Spieler würfelt, um zu sehen, ob der Angriff funktioniert, indem er den Wurf mit der Verwundbarkeitsschwierigkeit + Boni vergleicht (wenn die gewürfelte Zahl + Boni mit der Schwierigkeit übereinstimmt oder diese übersteigt, ist der Angriff erfolgreich).

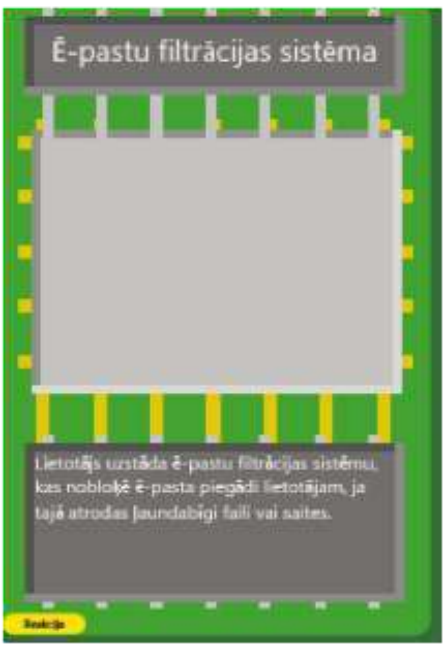
Angriffe können mit der Reaktionskarte, die für den jeweiligen Angriff vorgesehen ist, zurückgedrängt werden. Jeder Angriff hat seine eigene Art von Reaktion, die gespielt werden kann, und seine eigene Art von Verwundbarkeit, für die sie funktioniert.

Wenn der Angriff fehlschlägt oder durch eine Reaktionskarte blockiert wird, bleiben die ausgespielten Angriffs- und Reaktionskarten bis zum Ende der nächsten Runde auf dem Tisch liegen und verhindern, dass andere Spieler mit demselben Angriff für dieselbe Schwachstelle angreifen können. Nach dem Zug kommen beide Karten zurück auf den Stapel.

Schwierigkeitsgrade

1. - Spieler muss mindestens die Zahl 4 würfeln (ohne Länderbonus)
2. - Spieler muss mindestens die Zahl 8 würfeln (ohne Länderbonus)
3. - Spieler muss mindestens 11 würfeln (ohne Länderbonus)





LECSA (LV)

VERTEIDIGUNG

Verteidigung - die Wahl der richtigen Methode gegen eine bestimmte Schwachstelle. Reaktionskarten stoppen (annullieren) den eingehenden Angriff (und alle anderen Angriffe, die auf dieselbe Schwachstelle abzielen) für 1 Runde.

Um einen eingehenden Angriff abzubrechen, legt der Spieler eine Reaktionskarte, die dem Angriffstyp entspricht (siehe Tabelle mit den Verwundbarkeiten), auf die Angriffskarte, sobald der Angriff gespielt wird.

Um eine Verletzung zu reparieren, legt der Spieler eine Verteidigungskarte neben die zu reparierende Verletzung.

Andere Spieler können diese Verletzung angreifen, solange sie sich in Verteidigung befindet (bevor der Verteidigungszug zu Ende ist). Wenn der Spieler versucht, eine Verletzung auf seinem Server mit einer Défense-Karte zu reparieren, kann sie nicht angreifen, aber er kann versuchen, Angriffe mit Reaktionskarten zu verhindern. Für eine vollständige Reparatur wird |Schwierigkeitsgrad + 1| Runde benötigt. Während der Reparaturphase ist die Aktion Scannen erlaubt.

Wenn die Verteidigungsmethode nicht korrekt ist, überspringt der Spieler 3 Runden und kann in dieser Zeit keine Verteidigungskarten einsetzen (Reaktionen und Abtastaktionen sind erlaubt).

Bonus-Punkte der Länder

USA: +2 beim Scannen

Russland: +2 für Angriffe

China: +2 zur Abwehr von Angriffen

Nordkorea: +2 für Verteidigung gegen Scanning

Indien: +1 bei allen Angriffen, -1 gegen Angriffe

Israel: +3 bei allen Angriffen, -3 gegen Angriffe

Schwachstellen nach Ebenen

Vulnerability	Attacks	Défense	Reaction
1st vulnerability level			
SSH server with username	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel with User Name	Password guessing	Blocking external requests	Settings of Blocked Period
Untrained employee	Phishing campaigns	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list
Vulnerable SMB protocol	Exploitation of EternalBlue	Fixing vulnerability CVE-2017-0144	n/a
XSS vulnerability	Code injection;	Introductory	Introduction of the

SQL injection	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Router panel with default username and password	Using default data	Complete replacement of authentication data	One session limit
2nd vulnerability level			
SSH server	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel	Username guessing	Blocking external requests	Settings of Blocked Period
XSS vulnerability with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
SQL injection with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Incompletely configured firewall	Packet fragmentation	Repair configuration	IDS implementation
WiFi network with WEP security	Packet Phishing	Using the WPA2 standard	RADIUS implementation
Busy CEO/boss	Phishing – catching the big fish	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list
3rd vulnerability level			
Service failure	DDoS	IP address blocking and load limiting	Load balancers
Vulnerable OpenSSL program	Heartbleed exploitation	Repair of CVE-2014-0160	n/a
Vulnerable Print Spooler program	PrintNightmare exploitation	Repair of CVE-2021-36958	n/a
Buffer overflow vulnerability	Buffer overflow	Introduction of buffer limits	Increasing the buffer
Weak hashing algorithm	Decryption of the hash value	Improving the hash algorithm	Usage of a strong and long password
Lazy IT expert	Targeted phishing	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list

LECSA (LV)

SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

Ievainojams SMB protokols

XSS ievainojums

SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

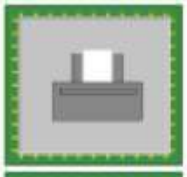
SQL injekcija ar filtru

Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma

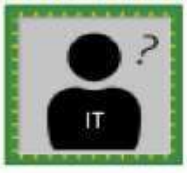


Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)

TIPPS & ERFAHRUNGEN VOM GAMEJAM IN LETTLAND

Während der 2-tägigen Veranstaltung kann kein echtes Computerspiel entwickelt werden, sondern nur ein erster Prototyp, der je nach Motivation der Teilnehmer weiterentwickelt werden kann oder nicht.
Preise oder andere Arten von Vorteilen können dazu beitragen, mehr Teilnehmer einzubeziehen und am Ende bessere (greifbarere) Ergebnisse zu erzielen (in unserem Fall wurden Pizza und Getränke am Ende der Veranstaltung bereitgestellt, weitere Unterstützung durch Mentoren (z. B. Platzierung von Spielen auf der Plattform).
Mentoren, die sich mit der Entwicklung von Spielen und mit Fragen der Cybersicherheit befassen, spielen eine wichtige Rolle beim Game Jam, indem sie die Teilnehmer beraten und unterstützen.
Planung im Voraus - da es sich um eine recht komplexe Veranstaltung handelt, die eine sorgfältige Planung erfordert. Die Organisatoren müssen bedenken, dass einige Teams aus dem Wettbewerb ausscheiden könnten (aufgrund der begrenzten Zeit).

Schau Dir auch die Facebook-Beiträge mit den Ergebnissen der Veranstaltung an:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

Die Veranstaltung wurde von LECSA in Zusammenarbeit mit der Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums durchgeführt.

MEATH PARTNERSHIP (IE)

AKTIVITÄTEN

- Informationstreffen zur Bedarfsermittlung mit Studenten (Codierungstraining in einer lokalen Einrichtung der Erwachsenenbildung)
- 2-tägiger GameJam (Online-Informationssession am 1. Tag; Tag 2 ist dem Game Jam gewidmet)
- Multiplikator-Veranstaltung - Cybersecurity Awareness Morning

BESCHREIBUNG & ERGEBNISSE

1) Informationstreffen zur Bedarfsermittlung mit Studenten (Codierungstraining in einer lokalen Einrichtung der Erwachsenenbildung)

BESCHREIBUNG

Um das Projekt bekannt zu machen und die Hauptthemen für den Game Jam zu bestimmen, veranstaltete das Team von Meath Partnership eine Informationsveranstaltung mit den Schülern eines lokalen Programmierkurses. Nach dem Austausch von Informationen über Cybersicherheit und der Diskussion über die jüngsten Bedrohungen folgte ein Gruppen-Brainstorming, bei dem die SchülerInnen in zwei Gruppen aufgeteilt wurden, um Fragen zu diskutieren, die zur Ermittlung der interessantesten Themen führten, die während des Gamejams weiter erforscht werden sollten.
Weitere Informationen über den Gamejam und das CYBER.EU.VET-Projekt wurden den Teilnehmern an diesem Tag ebenfalls mitgeteilt.

BEISPIEL FÜR EINSCHÄTZUNG UND BEDARFSANALYSE


YBER.VET.EU

Co-funded by the
Erasmus+ Programme
of the European Union

Needs assessment meeting guidelines

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

MEATH PARTNERSHIP (IE)

ERGEBNISSE

Als Ergebnis dieser Aktivität gewann das Team von Meath Partnership ein besseres Verständnis für das allgemeine Wissen der SchülerInnen in Bezug auf Cybersicherheit und Cyberbedrohungen und sammelte Informationen, die in den Planungs- und Umsetzungsprozess des GameJams einflossen.

Schüler bei der Selbsteinschätzung und Beantwortung der Fragen

MEATH PARTNERSHIP (IE)

GAME JAM

2) 2-tägiger Gamejam
(Online-Informationssession am 1. Tag; Tag 2 ist dem Game Jam gewidmet)

BESCHREIBUNG

TAG 1 war der Begrüßung der Teilnehmer, der Vorstellung des CYBER.EU.VET-Projekts und der Eröffnung des Game Jams gewidmet sowie dem Informationsaustausch über die beiden Themen, die während der Bedarfsermittlung ermittelt wurden. Den Teilnehmern wurde die Möglichkeit geboten, einzeln oder in einem Team zu arbeiten. Sie hatten auch die Möglichkeit, Fragen zu stellen oder weitere Erläuterungen zu den Verfahren zu erhalten. im Zusammenhang mit der Entwicklung der Spiele an Tag 2.

TAG 2 war der Entwicklung der Spiele gewidmet. Mitglieder unseres Teams und ein IT-Support-Experte standen den Teilnehmern während der gesamten Dauer des Game Jams über Zoom zur Verfügung, von 9 Uhr bis 21 Uhr.
Die TeilnehmerInnen wurden eingeladen, ihre Spiele auf die Itchio-Plattform unter einem eigens für diese Veranstaltung erstellten Profil hochzuladen: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

ERGEBNISSE

Nachdem die Teilnehmer ihre Spielentwürfe dem Team vorgestellt hatten, beschloss ein Teilnehmer, das Spiel zur weiteren Bewertung hochzuladen. Die übrigen Teilnehmer beschlossen, ihre Entwürfe nicht einzureichen, da sie sich noch in einem sehr frühen Stadium befanden.

Click or not click

Online interactive cybersecurity game

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Interaktives Online-Spiel zur Cybersicherheit:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Multiplikator-Veranstaltung - Cybersecurity Awareness Morning

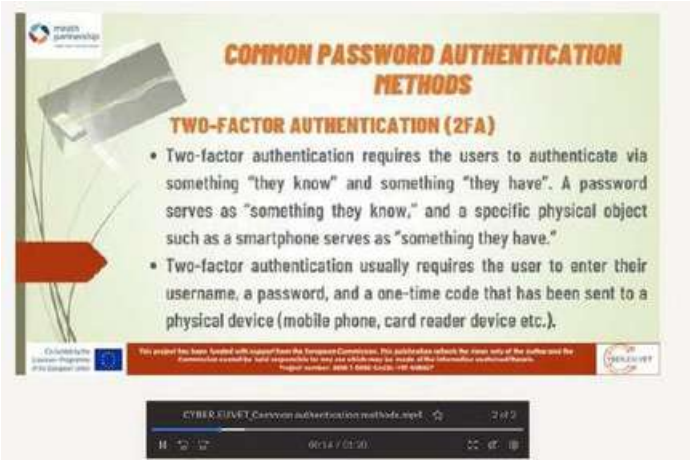
Datum: November 2021

BESCHREIBUNG

Die Multiplikatorenveranstaltung wurde online über Zoom abgehalten, um das Projekt und seine Aktivitäten bekannt zu machen. Die Veranstaltung wurde unter einer Vielzahl von Akteuren, die an Cybersicherheit interessiert oder beteiligt sind, weit verbreitet. Die Veranstaltung begann mit einer Präsentation und einem Überblick über das Projekt und den Game Jam, gefolgt von einer Präsentation und Diskussion über Cybersicherheit und dem Austausch praktischer Informationen darüber, wie man online bleiben kann (die aktuellen Cyber-Bedrohungen und wie man mögliche Angriffe verhindern kann).

ERGEBNISSE

Die Multiplikatorenveranstaltung trug dazu bei, den Bekanntheitsgrad des Projekts zu erhöhen, und bot außerdem die Möglichkeit, die seit Projektbeginn erreichten Meilensteine einem breiteren Publikum vorzustellen. Es war auch eine gute Gelegenheit, praktische Informationen und Ratschläge zur Cybersicherheit mit den Teilnehmern der Veranstaltung zu teilen.



COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

AKTIVITÄTEN

1) Cyber & Ethical Hacking Post-Graduierung für zukünftige Fachleute und Marktlehrer (Okt. 2021 - Feb. 2022 (in Partnerschaft mit einer lokalen Beratungsfirma namens Cybersec)

2) 2 GameJam-Sessions, die im Januar 2022 an berufsbildenden Schulen durchgeführt wurden: Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

3) Ein dreieinhalbtägiges Cybertraining für Gymnasiasten im März 2022 an der Universität Lusofona als Teil der Tecweb-Veranstaltung - https://tecweb.ulusofona.pt

ERGEBNISSE

Verbreitungsbericht, in dem Sie die verschiedenen Tests sehen können, die während eines Kalenderjahres (April 2021 bis April 2022) durchgeführt wurden. In diesem Bericht sind Screenshots von Veröffentlichungen in sozialen Netzwerken, Plakate von verschiedenen Veranstaltungen und Fragebögen zum Bewusstsein für Cybersicherheit zu sehen (in portugiesischer Sprache verfügbar unter
https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).
Während des Cyberjams wurde auf der Grundlage der Umfragen zum Bewusstsein für Cybersicherheit auch eine Reihe von benutzerfreundlichen/interaktiven Minispielen zu einfachen Situationen durchgeführt.

TANDEM PLUS NETZWERK [FR] - MIT IASIS [GR]

GAME JAM

Spielentwicklung Cyberopolis (IASIS)

Dieses Spiel ist ein Brettspiel, das sich an Personen richtet, die sich für Cybersicherheit interessieren, mit maximal 2-4 Spielern, und dessen Hauptaspekte Datenvertraulichkeit und Datenintegrität sind... während die Themen, mit denen es sich beschäftigt, Malware, Phishing, webbasierte Angriffe, Angriffe auf Webanwendungen, Spam, Identitätsdiebstahl, DDoS und Man in the middle sind...

Sehen Sie sich das Bild von ''Cyberopolis'' an, um besser zu verstehen, welche Schritte während des Spiels zu befolgen sind und welche Aufgaben zu lösen sind...

Screenshots des Spiels während der GameJam-Sitzung, auf denen wir den Erfolg des Spiels und das große Interesse der TeilnehmerInnen sehen können.

TANDEM PLUS NETZWERK [FR] - MIT IASIS [GR]

VIDEO - Vorbeugung von Cybermobbing

Dieses vom griechischen Partner entwickelte Video bringt den Besuchern verschiedene Möglichkeiten zur Prävention und Bekämpfung von Cybermobbing näher.

YBER.EU.VET

Funded by the European Union

DISCLAIMER

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Gestaltung
NGO Nest Berlin e.V.
Berlin, 2022

Co-funded by the
Erasmus+ Programme
of the European Union