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

Moduł szkoleniowy InCyT

Bezpieczeństwo informacji dla zarządzających		
Część 1, Tydzień 1 **Moduł: Wprowadzenie do webinarium**		
Działania edukacyjne	❑**Webinarium** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑**Prezentacja** ❑ **Inne**	
Odpowiedzialni za zajęcia	Gabriel Vladut Valentin Istratie	
Cele aktywności edukacyjnej	1. Wprowadzenie do projektu Erasmus+ InCyT 2. Cele 3. Wyniki i produkty 4. Jak uchronić się przed cyberatakami 5. Szkolenia i mentoring 6. Inżynieria społeczna 7. Sieć społecznościowa (media społecznościowe)	
Umiejętności do zdobycia	• TS3 Bezpieczeństwo sieci • Testy penetracji TS4 (luki w zabezpieczeniach) • SS3 Analiza poznawcza i behawioralna	
Czas trwania okresu edukacyjnego	2 tygodnie	
Wymagania wstępne	***Co jest potrzebne?***	
	• Wiedza o projekcie Erasmus+ InCyT / celach / wynikach i produktach • Jak chronić się przed cyberatakami. • Szkolenia i mentoring • Inżynieria społeczna / Sieć społecznościowa (media społecznościowe)	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Krótka informacja o module

Opis
InCyT to projekt Erasmus+, którego celem jest stworzenie ram, metodologii szkoleń, która zapewnia mechanizm dla szkolnictwa technicznego i firm do opisywania kompetencji i umiejętności niezbędnych w cyberbezpieczeństwie dla profesjonalistów i nie-profesjonalistów, w celu uniknięcia cyberataków, a także luk cyfrowych i innych zagrożeń. NIST's National Initiative for Cyber Security Education (NICE) podkreśla, że należy zrobić kluczowy krok w kierunku zaradzenia niedoborowi „osób posiadających wiedzę, umiejętności i zdolności do wykonywania zadań wymaganych do pracy z cyberbezpieczeństwem". Taka siła robocza będzie obejmować „role techniczne i nietechniczne, w których pracują kompetentni i doświadczeni ludzie". Projekt będzie chciał wdrożyć pewne rozwiązania w tym kontekście. Jego celem jest przede wszystkim opracowanie ram, które zapewniają mechanizm szkolnictwu technicznemu i firmom do opisywania luk cyfrowych i innych niezbędnych w bezpieczeństwie cybernetycznym dla profesjonalistów i nieprofesjonalistów, aby uniknąć cyberataków i pomóc im poprawić tę sytuację. Biorąc pod uwagę zalety interdyscyplinarnych programów szkoleniowych i mentoringowych, szczególnie w obszarze cyberbezpieczeństwa, projekt opracuje i przetestuje cyfrowe interdyscyplinarne programy szkoleniowe wspierane e-mentoringiem dla MŚP i dostosuje je do szkolnictwa technicznego. Konieczna jest współpraca i komunikacja między edukatorami, badaczami i osobami korzystającymi z technologii informacyjnych. Jednym z problemów jest to, że firmy, szczególnie MŚP dysponujące mniejszymi zasobami, potrzebują pomocy w ocenieniu kompetencji i luk w umiejętnościach swoich pracowników, metod oceny istniejącej sytuacji oraz wykorzystania możliwości szkoleniowych w celu przekwalifikowania pracowników. Uczniowie będą mogli być informowani o tych aspektach, czytając odpowiedni teksty, oglądając webinaria i rozwiązując ćwiczenia we własnym tempie. Wszystkie te dokumenty znajdują się na cyfrowej interaktywnej platformie projektowej. Uczniowie mogą przetestować swoje odpowiedzi na ćwiczeniach samooceny. Odpowiedzi na inne ćwiczenia należy zapisać na odpowiednim forum dyskusyjnym i przedyskutować z mentorem na wspólnym zorganizowanym spotkaniu raz w tygodniu. Uczeń może współpracować z innymi osobami i mentorem, szczególnie podczas spotkań. Otrzymają oni także wsparcie w opracowaniu e-portfolio ważnego dla ewaluacji szkolenia.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

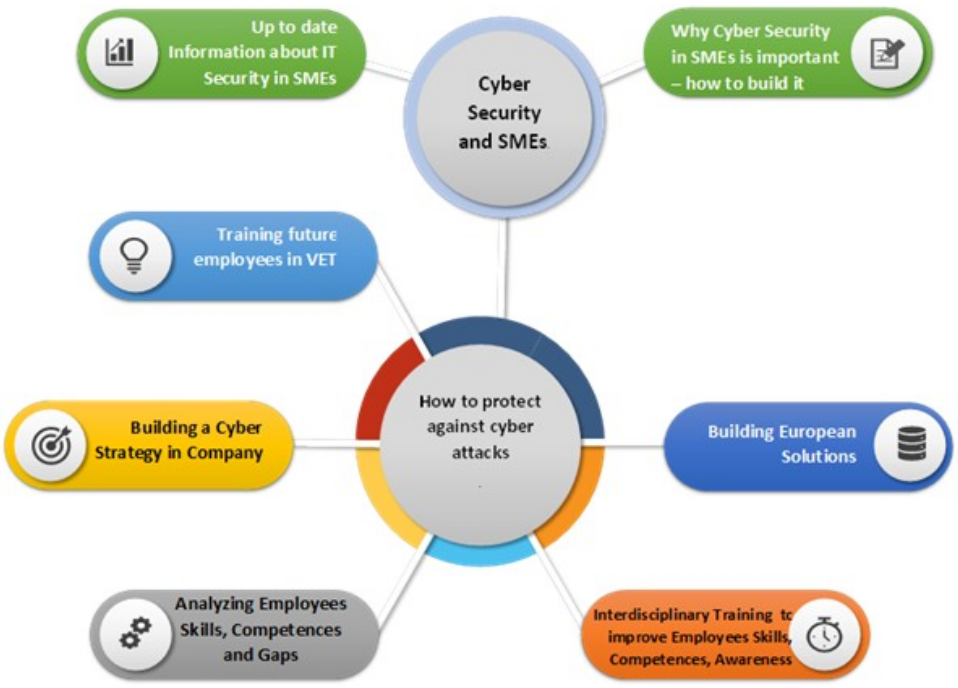
Co-funded by the Erasmus+ Programme of the European Union

Treść materiału edukacyjnego

Ramy kompetencji

W naszym projekcie odbędą się 3 spotkania międzynarodowe. Zostało to zaplanowane w 3, 13 i 20 miesiącu trwania projektu. Odbędą się dodatkowe spotkania projektowe, ponieważ uważamy, że 3 spotkania nie wystarczą do prowadzenia 24-miesięcznego projektu. Spotkania te odbywają się online i odbywają się regularnie co miesiąc. Spotkania te zorganizuje zespół zarządzający projektem.

Projekty będą prowadzone przez koordynatora projektu, lidera WP. W naszym projekcie odbędzie się 7 wydarzeń upowszechniających. Każda instytucja partnerska zorganizuje te działania, aby popularyzować ideę projektu w swoim kraju i dzielić się wypracowanymi produktami. Każda instytucja partnerska przeprowadzi Interdyscyplinarne Szkolenie dla pracowników i nauczycieli MŚP w zakresie cyberbezpieczeństwa we własnym kraju.



Cele

Projekt InCyT będzie chciał wdrożyć kilka rozwiązań:

• Opracowanie Ramy, która zapewni mechanizmy dla szkolnictwa technicznego i firmom opisujące

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

kompetencje i umiejętności niezbędne w bezpieczeństwie cybernetycznym profesjonalistom i nie-profesjonalistom, w celu uniknięcia cyberataków, a także luk cyfrowych i innych.

• Biorąc pod uwagę zalety interdyscyplinarnych programów szkoleniowych i mentoringowych, szczególnie w dziedzinie cyberbezpieczeństwa, projekt opracuje i przetestuje wspierane cyfrowe interdyscyplinarne programy szkoleniowe oraz platformę współpracy e-learningowej dla MŚP.

• Dostosowanie propozycja do wymogów szkolnictwa technicznego.

• Opracowanie europejskiego modelu możliwości przenoszenia.

• Biorąc pod uwagę zalety interdyscyplinarnych programów szkoleniowych i mentoringowych, szczególnie w obszarze cyberbezpieczeństwa, projekt opracuje i przetestuje cyfrowe interdyscyplinarne programy szkoleniowe wspierane e-mentoringiem dla MŚP i dostosuje je do szkolnictwa technicznego.

Rezultatami projektu będą:

• Ramy metodologiczne wdrażania rozwiązania.

• Istniejące i odbyte szkolenia (kursy).

• Możliwości ich udoskonalenia poprzez zastosowanie interdyscyplinarności i mentoringu.

• Metodologia uczenia się i mentoringu.

Produkty:

1. Ramy.

2. Cyfrowy interdyscyplinarny materiał szkoleniowy dotyczący cyberbezpieczeństwa dla MŚP, wspierany mentoringiem i dostosowaną metodologią specjalnego kursu dla szkolnictwa technicznego.

3. Platforma cyfrowa wspierająca szkolenie.

4. Raport, w jaki sposób umiejętności interdyscyplinarne zapewniają korzyści dla MŚP i szkolnictwa technicznego.

5. Europejski model transferu dla przetestowanych interdyscyplinarnych szkoleń i mentoringu

Partnerzy z: Niemiec (koordynator), Turcji, Polski, Włoch, Austrii, Danii, Rumunii.

Aktywności

• Ramy metodologiczne bezpieczeństwa cybernetycznego – organizacje wiodące: IAT, Niemcy, Włochy.

• Cyfrowy interdyscyplinarny materiał szkoleniowy dotyczący bezpieczeństwa cybernetycznego –

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

organizacja wiodąca: Uniwersytet Nauk Stosowanych St. Pölten, Austria.

• Platforma teleinformatyczna dla bezpieczeństwa cybernetycznego – organizacja wiodąca: IPA, Rumunia.

• Model Metodologiczny Cyberbezpieczeństwa - Organizacja wiodąca: Politechnika Rzeszowska, Polska.

• Model możliwości przenoszenia – organizacja wiodąca: Europejskie Centrum Szkoleniowe Kopenhaga, Dania.

• Wydarzenia upowszechniające – organizacja wiodąca: Turcja.

Jak uchronić się przed cyberatakami

Gospodarka cyfrowa opiera się przede wszystkim na danych. W dobie Przemysłu 4.0, systemów cyber-fizycznych i Internetu Rzeczy, coraz więcej produktów i procesów ulega cyfryzacji. Cyberbezpieczeństwo, czyli ochrona tych danych i związanych z nimi systemów przetwarzania informacji, ma dziś większe znaczenie niż kiedykolwiek w historii gospodarczej.

Procesy biznesowe mogą zostać znacząco zakłócone, spowolnione lub nawet całkowicie zablokowane, na przykład jeśli rekordy danych są nieprawidłowe, niekompletne lub w ogóle niedostępne, synchronizacja danych między systemami jest zakłócona, systemy IT działają nieprawidłowo lub całkowicie zawodzą.

W szczególności MŚP są celem działalności przestępczej związanej z tymi kwestiami. W przeciwieństwie do wielkich korporacji, ich zasoby są ograniczone – i hakerzy o tym wiedzą! MŚP są podstawą gospodarki w Europie, co oznacza, że ponad 99% firm w Niemczech to MŚP.

Ponad połowa siły roboczej jest zatrudniona przez MŚP. Dlatego konieczne jest pomaganie MŚP w unikaniu cyberataków.

Cyber Security Education Initiative wskazuje, że należy podjąć krytyczny krok w celu rozwiązania problemu braku „osób posiadających wiedzę, umiejętności i zdolności do wykonywania zadań wymaganych do pracy w zakresie cyberbezpieczeństwa".

Do takiej grupy należą „funkcje techniczne i nietechniczne, które pełnią pracownicy z wiedzą i doświadczeniem".

Trudno jest jednak stworzyć siłę roboczą z niezbędnymi umiejętnościami interdyscyplinarnymi i rozwiązać problem komunikacji między edukatorami, badaczami i osobami korzystającymi z technologii informatycznych.

Konieczna jest współpraca i komunikacja między tymi grupami.

Jednym z problemów jest to, że firmy, zwłaszcza MŚP o mniejszych zasobach, potrzebują pomocy w ocenie umiejętności i braków swoich pracowników, wykorzystując metody cyfrowe do poprawy

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

istniejącej sytuacji i organizując możliwości szkoleń w celu przekwalifikowania pracowników.

Szkolenia i mentoring

Przedsiębiorcy, w tym przyszli, potrzebują złożonych sposobów myślenia oraz umiejętności rozumienia i integrowania wiedzy z różnych sektorów, co wymaga interdyscyplinarnego uczenia się.

Złożone problemy inżynierskie wymagają stworzenia sytuacji interdyscyplinarnej w niemal naturalny sposób.

W podejściu interdyscyplinarnym uczący się powinni integrować informacje z różnych dyscyplin i dziedzin.

Rozwijają interdyscyplinarne zrozumienie, uczą się integrować obszary wiedzy i specyficzne dla dyscypliny sposoby myślenia.

Zwiększa to umiejętności poznawcze i krytyczne myślenie bardziej niż za pomocą pojedynczych środków dyscyplinarnych.

Inżynieria społeczna

• oznacza manipulowanie ludźmi (często przy użyciu metod psychologicznych) w celu uzyskania dostępu do danych, dokumentów i informacji interesujących napastnika.

• jest obecnie jednym z głównych zagrożeń dla bezpieczeństwa informacji i stanowi skuteczną formę cyberprzestępczości.

• może mieć niebezpieczne reperkusje, na przykład naruszenie danych, bardziej niż jakikolwiek inny rodzaj ataku.

• ataki mają cel finansowy i w związku z tym organizacje straciły znaczne kwoty pieniędzy.

• jest szczególnie niebezpieczny, ponieważ opiera się bardziej na błędach ludzkich niż na lukach w oprogramowaniu i systemach operacyjnych.

Firmy:

• mogą cierpieć z powodu utraty produktywności, spadku morale pracowników i trudności w powrocie do zdrowia.

• mają nadszarpniętą reputację, ponieważ klienci nie są przekonani, że organizacja może się chronić.

• często trzeba wyzwolić starą reakcję na incydent.

• powinien zapewnić oprogramowanie zabezpieczające, które pomoże zapobiegać przyszłym atakom.

• często musieliby przekwalifikować pracowników, aby byli gotowi na ataki.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Szkolenie z inżynierii społecznej (świadomość cybernetyczna)

• pracowników i menedżerów, dla których ważne jest rozpoznanie ataków socjotechnicznych, ponieważ ryzyko stania się ofiarą jest wysokie.

• mogą zostać włączone do programów uświadamiających społeczności, jednostki i obywateli oraz chronić jednostki i ich organizacje.

• szczególnie brakuje MŚP, które dysponują mniejszymi zasobami, dlatego należy im pomóc w poważnym podejściu do szkolenia w zakresie świadomości cybernetycznej i zapewnić pracownikom możliwości ich odbycia.

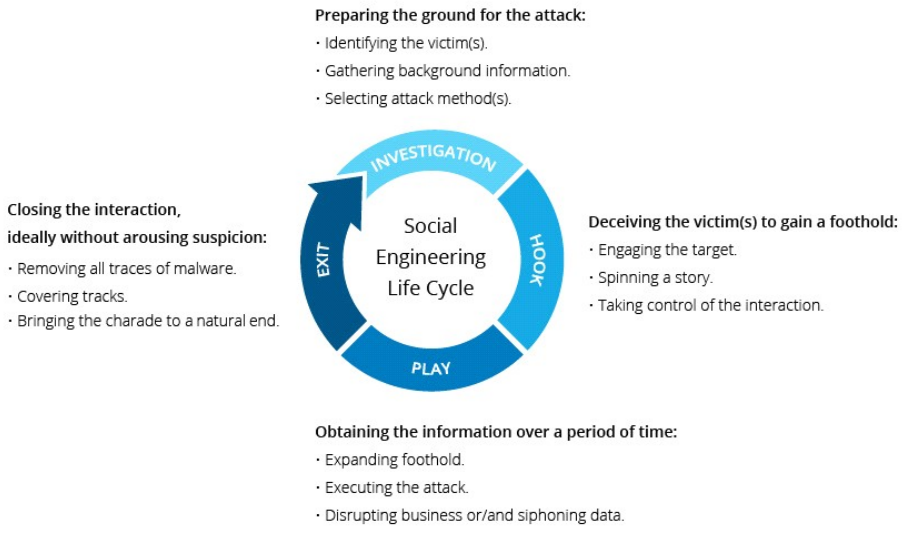
Cykl życia ataku socjotechnicznego

Napastnik:

• najpierw zbadaj wybraną ofiarę, aby zebrać niezbędne podstawowe informacje, takie jak punkty wejścia i słabe protokoły bezpieczeństwa, które są wymagane do ataku.

• następnie spróbuj zdobyć zaufanie ofiary i zapewnić zachęty do działań, które zwykle nie są praktykami bezpieczeństwa, takimi jak pozyskiwanie poufnych informacji lub udzielanie dostępu do krytycznych zasobów.

Rysunek wyjaśnia cykl życia ataku.



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Sieć społeczna

• stał się bardzo popularny w ostatnich latach, zapewniając użytkownikom platformę do komunikowania się z rodziną, przyjaciółmi i współpracownikami.

• Sieci społecznościowe odnoszą się do korzystania z internetowych serwisów społecznościowych do łączenia się i komunikowania z przyjaciółmi, rodziną, współpracownikami, klientami lub klientami.

• mają swoje serwery w centrach danych, które są współlokowane z głównymi punktami dostępu do sieci w Internecie.

Role mediów społecznościowych (rysunek) pokazują niektóre obszary, w których media społecznościowe odgrywają rolę:

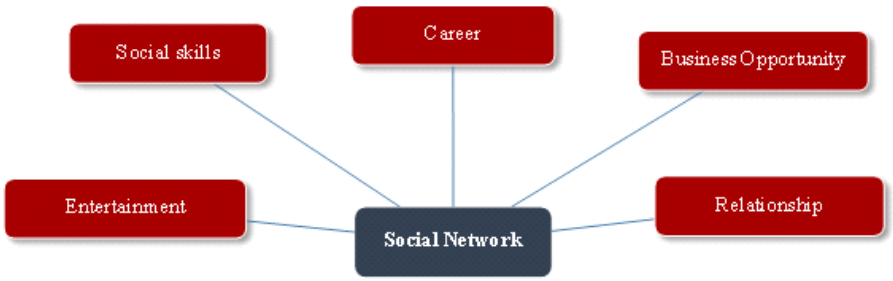
• rozrywka

• budowanie możliwości biznesowych

• kariera zawodowa

• poprawa umiejętności społecznych

• rozwijanie relacji z innymi osobami



Sieć społeczna:

• jest podstawą dla marketerów poszukujących klientów, aby zwiększyć rozpoznawalność marki, wspierać lojalność wobec marki, poprawić współczynniki konwersji, zapewnić dostęp i zaangażowanie nowych, niedawnych i starych klientów.

• umożliwienie, poprzez udostępnianie wpisów na blogach, zdjęć, filmów wideo lub komentarzy w sieciach społecznościowych, większej liczbie osób odwiedzenie strony internetowej firmy i zostanie jej klientami.

• utrudnia nadążanie za zmianami, a także wpływa na wskaźnik sukcesu marketingowego firmy.

Najpopularniejsze serwisy społecznościowe (media społecznościowe) w Stanach Zjednoczonych i Europie to:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

• Facebook

• Instagram

• Twitter

• Youtube

• WhatsApp

• LinkedIn, który pomaga łączyć specjalistów ze współpracownikami, kontaktami biznesowymi i pracodawcami.

Serwisy społecznościowe opierają się na rozwijaniu i utrzymywaniu relacji osobistych i biznesowych przy użyciu technologii i serwisów społecznościowych (Media społecznościowe), które umożliwiają ludziom i firmom łączenie się ze sobą, rozwijanie relacji, dzielenie się informacjami, pomysłami i wiadomościami.

Członkowie rodziny mogą pozostawać w kontakcie za pośrednictwem osobistych sieci społecznościowych, takich jak Facebook, udostępniać zdjęcia i wysyłać inne wiadomości o swoim życiu.

Ludzie mogą również łączyć się z innymi (obcymi), którzy mają te same zainteresowania.

Media społecznościowe mają również wady, w tym rozpowszechnianie dezinformacji oraz wysokie koszty korzystania i utrzymywania profili w mediach społecznościowych.

Funkcjonalność platform społecznościowych można podzielić na:

Funkcje sieciowe służą do wzmacniania relacji społecznych między użytkownikami na platformach wirtualnych i zapewniają funkcjonalność budowania i utrzymywania wykresu sieci społecznościowej.

Funkcje danych są odpowiedzialne za zarządzanie treściami dostarczanymi przez użytkowników i komunikacją między użytkownikami, pomagając poprawić (rozszerzyć) interakcję użytkowników i uatrakcyjnić platformę

Funkcje kontroli dostępu mają na celu wdrożenie zdefiniowanych przez użytkownika środków ochrony prywatności i ograniczenie nieautoryzowanego dostępu do danych i informacji dostarczonych przez użytkownika.

Zalety i wady sieci społecznościowych

Korzyści

Media społecznościowe umożliwiają firmom:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

• połączenie się z nowymi i istniejącymi klientami.

• możliwość tworzenia, promowania i zwiększania świadomość marki.

• polegać na recenzjach i komentarzach swoich klientów, które są ważne dla zwiększenia sprzedaży marki i wyższych pozycji w wyszukiwarkach.

• możliwość stworzenia nowej marki. aby wykazać swoim klientom wysoki poziom usług.

• możliwość ulepszania produktów i relacji z konsumentami.

Wady
• mogą przyczynić się do rozpowszechniania dezinformacji.

• może mieć negatywny wpływ na firmy, ponieważ krytyka marki bardzo szybko rozprzestrzeniła się w mediach społecznościowych.

• wymaga godzin pracy i kosztów każdego tygodnia w celu zbudowania i utrzymania profilu firmy.

Bezpieczeństwo i prywatność w sieciach społecznościowych

• Informacje udostępniane w sieciach społecznościowych i mediach rozprzestrzeniają się bardzo szybko, co czyni je atrakcyjnymi dla atakujących.

• Kwestie bezpieczeństwa i prywatności związane z informacjami udostępnianymi przez użytkownika, gdy użytkownik przesyła zawartość osobistą, taką jak zdjęcia, filmy i dźwięk, powinny być przestrzegane, ponieważ atakujący może złośliwie wykorzystać udostępnione informacje do nielegalnych celów.

• Brak świadomości użytkowników na temat bezpieczeństwa i prywatności może prowadzić do różnych cyberataków za pośrednictwem mediów społecznościowych.

Zagrożenia można podzielić na trzy kategorie:

• Konwencjonalne zagrożenia obejmują zagrożenia, które użytkownicy napotkali od początku istnienia sieci społecznościowej.

• Współczesne zagrożenia to ataki wykorzystujące zaawansowane techniki w celu złamania zabezpieczeń kont użytkowników.

• Ataki ukierunkowane to ataki wymierzone w konkretnego użytkownika, które mogą zostać popełnione przez dowolnego użytkownika w ramach różnych osobistych wendet.

Rozwiązania dla operatorów sieci społecznościowych

• Zaproponowano procedury uwierzytelniania, takie jak CAPTCHA, uwierzytelnianie wieloskładnikowe i identyfikacja zdjęć znajomych.

• Ustawienia bezpieczeństwa i prywatności, aby umożliwić klientowi wprowadzanie danych

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

osobowych przed niepożądanym dostępem osób postronnych lub aplikacji.

• Zgłoszenia użytkowników o wszelkich formach nadużyć lub naruszeń zasad przez dowolnego użytkownika w ich sieci. oznacza to, że gdy Facebook otrzyma zgłoszenie użytkownika, jest ono sprawdzane i usuwane zgodnie ze standardami społeczności Facebooka.

Pytania:

Forum dyskusyjne, na które należy odpowiedzieć krótkim wyjaśnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji szkoleniowych.

1. Jakie są Twoje oczekiwania wobec projektu InCyT
2. Jak uchronić się przed cyberatakami?
3. Co to jest socjotechnika?
4. Sieć społecznościowa (media społecznościowe).

Pytania samooceny. Po udzieleniu odpowiedzi uczeń może zobaczyć wyniki i porównać je z tymi zapisanymi na platformie

- Jak chronić się przed cyberatakami.
- Co to jest inżynieria społeczna.
- Sieć społecznościowa (media społecznościowe).

Załączniki

Prezentacja PowerPoint

Filmy Video

References:

- InCyT – Interdisciplinary Cyber Training
- Cyber Incident Recovery
- Minimize Cyber Attacks - Cyber Resiliency Strategy
- How to Prevent Cyberattacks: Top Ways to Protect Yourself
- Social Media Security: How Safe is Your Information?
- Internal Controls Over Information Systems
- Social Media Adoption Brings New Risks
- Social Media Security – 5 Security Tips
- 19 Social Media Security Best Practices

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.