CYBER MSME:

WYTYCZNE

DOTYCZĄCE WDROŻENIA REZULTATÓW PROJEKTU

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

SPIS TREŚCI

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

1. WPROWADZENIE

Cyber MSME (Cybersecurity for Micro, Small & Medium Enterprises) to międzynarodowy projekt współfinansowany przez program Unii Europejskiej Erasmus+ i realizowany przez konsorcjum stworzone przez sześciu partnerów z pięciu różnych krajów, którzy spotkali się, aby odpowiedzieć na różnorodne wyzwania, z którymi muszą sobie radzić mikro-, małe i średnie przedsiębiorstwa na swojej drodze biznesowej. Projekt jest odpowiedzią na potrzeby organizacyjne zidentyfikowane na poziomie unijnym i krajowym w odniesieniu do mikroprzedsiębiorstw i małych przedsiębiorstw w zakresie cyberbezpieczeństwa (podnoszenie kwalifikacji), a jednocześnie przyczynia się on do wzrostu konkurencyjności unijnych mikroprzedsiębiorstw i małych przedsiębiorstw poprzez zapewnienie bardziej odpowiednich i wysokiej jakości programów szkoleniowych.

W trakcie trwania projektu sześciu partnerów współpracowało nad opracowaniem pakietu narzędzi Cyber-MSME, materiałów szkoleniowych dotyczących różnych tematów przeznaczonych dla początkujących, średnio- i zaawansowanych specjalistów ds. cyberbezpieczeństwa, którzy chcą opanować umiejętności i wiedzę potrzebne do wykonywania swoich zadań i reagowania na wyzwania w tej dziedzinie. Sześciu partnerów opracowało pięć zestawów narzędzi i jedenaście kursów, mających na celu wypełnienie luk pojawiających się w literaturze i obejmujących takie tematy, jak: zwiększenie bezpieczeństwa sieci za pomocą użycia kilku podstawowych kroków, poprawa planu zarządzania cyberbezpieczeństwem, rozpoznawanie wiarygodnych adresów URL, podstawowe wskazówki dotyczące bezpieczeństwa routerów i listę zasobów, przy czym każdy z zestawów narzędzi został wzbogacony o serię kursów.

Opracowane pomoce szkoleniowe zawierają wytyczne, studia przypadków, listy kontrolne i bogaty zestaw zasobów, co zapewnia bezpłatne i gotowe do użycia narzędzia edukacyjne dla wszystkich organizacji i specjalistów zainteresowanych zrozumieniem, przewidywaniem, zarządzaniem i niwelowaniem zagrożeń dotyczących cyberbezpieczeństwa, przy jednoczesnym zwiększeniu zdolności operacyjnej do wdrażania zasad cyberbezpieczeństwa w mikro-, małych i średnich przedsiębiorstwach.

Ta grupa docelowa obejmuje środowiska wspierające przedsiębiorczość i rozwój cyfrowy oraz środowiska związane z ICT, w tym zainteresowane strony, takie jak: agencje promocji przedsiębiorczości, stowarzyszenia biznesowe, instytucje edukacyjne, konsultanci IT, uniwersytety, ośrodki badawcze itp.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Znaczne nakłady zostały zainwestowane w rozwój zestawu narzędzi Cyber-MSME, aby działał on dla wszystkich obecnych i przyszłych podmiotów gospodarczych, które nie chcą poświęcać strategicznej przewagi w dziedzinie bezpieczeństwa cyfrowego.

Ponadto, aby upewnić się, że zasoby edukacyjne rzeczywiście odpowiadają potrzebom grupy docelowej i są opracowywane zgodnie z jej wymaganiami edukacyjnymi, przeprowadzono walidację materiałów szkoleniowych, a wszyscy partnerzy wdrożyli szkolenie pilotażowe dla co najmniej 150 osób reprezentujących grupy docelowe. Dostarczyło to konsorcjum znaczących informacji zwrotnych na temat różnych aspektów szkolenia, takich jak: użyteczność, adekwatność do potrzeb i preferencji, sposoby wdrażania i treść oraz odpowiedzi, które okazały się istotne dla celów walidacji materiałów szkoleniowych. Zebrane doświadczenia stanowią treść tego dokumentu, wytyczne promujące skalowalność projektu, możliwość jego przenoszenia i powielania wyników w innych dziedzinach.

W niniejszym dokumencie zostaną uwzględnione wszystkie kluczowe zalecenia, wnioski wyciągnięte z realizacji projektu, dotyczące tego, jak w pełni wykorzystać materiały szkoleniowe i skutecznie zastosować tę wiedzę w przyszłości. Ma to na celu dostarczenie potencjalnym użytkownikom praktycznych, opartych na doświadczeniu spostrzeżeń zebranych podczas kursów pilotażowych i wdrażania opracowanych zestawów narzędzi. Obejmuje różnorodne zalecenia dotyczące sposobu komunikowania się z użytkownikami, utrzymania aktywnego uczestnictwa podczas realizacji programów szkoleniowych korzystania z zasobów platformy cyber OZE, a także niektóre spostrzeżenia od trenerów w zakresie najbardziej efektywnych sposobów prowadzenia szkolenia i współpracy z uczniami.

Wytyczne te oraz nasze spostrzeżenia i opinie na temat używania zestawu narzędzi Cyber-MSME, nie stanowią jednoznacznych zasad wdrażania szkoleń Cyber-MSME. Wręcz przeciwnie, potencjalni użytkownicy są bardzo zachęcani do eksperymentowania. Ich wkład w realizację szkoleń, rozpowszechnianie cennej wiedzy i doskonalenie umiejętności w dziedzinie cyberbezpieczeństwa, wzbogacają naszą pracę i wysiłki w tej dziedzinie.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Niniejszy dokument i jego treść odzwierciedlają wyłącznie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w nim zawartych.

2. REZULTATY EDUKACYJNE

Zestawy narzędzi i szkolenia w dziedzinie cyberbezpieczeństwa są wynikiem osiągniętych efektów szkoleń i dostosowane do EQF 3-5, w następujący sposób:

-Znajomość faktów, zasad, procesów i ogólnych pojęć z zakresu cyberbezpieczeństwa, zdobycie szeregu umiejętności poznawczych i praktycznych wymaganych do realizacji zadań i rozwiązywania problemów poprzez wybór i zastosowanie podstawowych metod, narzędzi, materiałów i informacji;

-Wiedza merytoryczna i teoretyczna w dziedzinie cyberbezpieczeństwa, z szeregiem umiejętności poznawczych i praktycznych wymaganych do generowania rozwiązań konkretnych problemów w dziedzinie cyberbezpieczeństwa;

-Kompleksowa, specjalistyczna, praktyczna i teoretyczna wiedza z zakresu cyberbezpieczeństwa oraz świadomość granic tej wiedzy, z kompleksowym zakresem umiejętności poznawczych i praktycznych wymaganych do opracowania kreatywnych rozwiązań abstrakcyjnych problemów.

Zestawy narzędzi i szkolenia Cyber-MSME koncentrują się wokół serii konkretnych efektów edukacyjnych dla każdego z modułów, a my wymienimy tylko kilka z nich w niniejszych wytycznych, aby mieć wgląd w ich zakres.

Pod koniec modułów uczniowie będą potrafili:

-Zidentyfikować kryzys cybernetyczny i potencjalne zagrożenia w organizacji;

-Unikać typowych błędów cybernetycznych, jednocześnie ulepszając swój plan zarządzania kryzysami cybernetycznymi;

-Zdefiniować i rozpoznać projekt skoncentrowany na człowieku;

-Zdefiniować i stworzyć program bug bounty;

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.
Niniejszy dokument i jego treść odzwierciedlają wyłącznie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w nim zawartych.

-Rozpoznać i rozróżnić najczęściej stosowane techniki inżynierii społecznej;

-Zrozumieć na czym polega skanowanie luk w zabezpieczeniach, hakowanie systemu i działanie złośliwych programów;

-Poznać EntreComp Framework i nabyć wiedzę o tym, jakie może to mieć znaczenie dla bezpieczeństwa cybernetycznego i efektywności IT;

-Zapoznać się z DigComp Framework – oficjalnymi wytycznymi UE w zakresie kształcenia i szkolenia umiejętności cyfrowych;

-Wiedzieć, co robić przed, w trakcie i po cyberataku;

-Używać najbardziej odpowiednich narzędzi do identyfikacji i reagowania na cyberataki.

Wszystkie te dziedziny edukacji są omawiane w materiałach szkoleniowych, z których każdy obejmuje określony temat, taki jak: stan cyberbezpieczeństwa na terenie Europy, zastosowanie EntreComp w cyberbezpieczeństwie, inżynieria społeczna, narzędzia ICT do zapobiegania i rozpoznawania ryzyka cybernetycznego w cyfrowym świecie, zarządzanie kryzysowe itp. Jak wspomniano powyżej, wszystkie te moduły wraz z ich konkretnymi efektami uczenia się są dostępne w dowolnym momencie i bezpłatnie na platformie OER.

3. PROFIL ZAWODOWY EKSPERTA DS. CYBERBEZPIECZŃSTWA MSME

Przed przedstawieniem podsumowania z realizacji programu pilotażowego określimy profil zawodowy eksperta MSME Cyber Security oraz ścieżkę kariery, która jest niezbędna, aby wiedzieć, jak wdrażać szkolenia w organizacji i aby uzyskać status eksperta.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Niniejszy dokument i jego treść odzwierciedlają wyłącznie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w nim zawartych.

Ekspert ds. cyberbezpieczeństwa powinien opanować szereg następujących obszarów wiedzy:

- Jak spełnić wymagania norm bezpieczeństwa w Unii Europejskiej;
- Zagrożenia cybernetyczne i najsłabsze punkty planu zarządzania bezpieczeństwem;
- Przydatne narzędzia w organizacji bezpiecznego środowiska pracy;
- Specjalistyczna terminologia potrzebna do zrozumienia środowiska cyberbezpieczeństwa;
- Jak reagować i przywracać systemy po atakach;
- Jak osiągnąć kolejny poziom wiedzy na temat cyberbezpieczeństwa.

Ponadto, oprócz opanowania pewnej wiedzy, osoba na stanowisku eksperta ds. cyberbezpieczeństwa powinna być w stanie wykonać następujące czynności:

- Tworzenie i wdrażanie procedur bezpieczeństwa;
- Działanie w bezpiecznym środowisku internetowym;
- Korzystanie z narzędzi i systemów, aby uniknąć zagrożeń cybernetycznych;
- Tworzenie bezpiecznych warunków pracy przy niskich kosztach;
- Wdrożenie planu zarządzania kryzysowego i odzyskiwania systemów po awarii;
- Rozwijanie firmy i doskonalenie umiejętności jej pracowników poprzez dzielenie się swoją wiedzą.

Niewątpliwie wszystkie te umiejętności i wiedza nie są osiągane natychmiastowo, ale wymagają kształcenia, a projekt Cyber-MSME zapewnia odpowiednie materiały edukacyjne. Pierwszy, podstawowy poziom bycia ekspertem ds. cyberbezpieczeństwa stanowią analitycy ds. cyberprzestępczości, audytorzy IT i osoby reagujące na incydenty, którzy powinni wziąć udział w kursach takich, jak: "Europejskie ramy kompetencji

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+"

Przy wsparciu programu Unii Europejskiej Erasmus+.

Niniejszy dokument i jego treść odzwierciedlają wyłącznie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w nim zawartych.

cyfrowych: DigComp 2.1." oraz " „Cyberbezpieczeństwo na poziome UE Polityki, strategie i zasoby wsparcia”

Oba te kursy zapewniają przegląd instytucjonalnych ustaleń dotyczących znaczenia i wspierania sieci, a także ustanawiają wspólny model odniesienia dla tego, co Komisja Europejska przewiduje jako kluczowe kompetencje i umiejętności w dziedzinie informatyki i biegłości cyfrowej, niezbędną wiedzę dla każdego specjalisty ds. Bezpieczeństwa cybernetycznego na poziomie podstawowym.

Ekspert ds. Cyberbezpieczeństwa średniego szczebla jest reprezentowany przez analityków bezpieczeństwa cybernetycznego, konsultantów ds. Cyberbezpieczeństwa i pentesterów, którzy już opanowali podstawy bezpieczeństwa cybernetycznego i chcą lepiej zrozumieć bezpieczeństwo, aby trzymać zagrożenia cybernetyczne z dala od organizacji, dla której pracują, a także być w stanie korzystać z narzędzi ICT w celu zapobiegania zagrożeniom cybernetycznym w cyfrowym świecie. W tym celu w ramach projektu Cyber-MSME opracowano dwa zestawy narzędzi i trzy zalecane kursy, które można wykorzystać w każdej organizacji.

Zaawansowany ekspert ds. cyberbezpieczeństwa jest reprezentowany przez menedżerów ds. Bezpieczeństwa cybernetycznego i architektów bezpieczeństwa cybernetycznego, z ogromnym doświadczeniem i wiedzą w zakresie bezpieczeństwa informacji i systemów, sieci i kryptografii, którzy mogą poszerzyć swoją wiedzę dzięki zestawom narzędzi i kursom oferowanym przez projekt Cyber-MSME, takim jak "Projektowanie skoncentrowane na człowieku a priorytety firmy - wytyczne" i "Zarządzanie kryzysowe - włamali się do mnie, co dalej?".

Wszystkie te zasoby edukacyjne mogą być wykorzystywane zarówno przez organizacje, jak i osoby chcące nabyć nowe umiejętności w dziedzinie, która jest coraz bardziej obecna w dzisiejszym społeczeństwie, czyli cyberbezpieczeństwie.

Również każda osoba aktywnie poszukująca pracy powinna zainteresować się takimi zasobami edukacyjnymi, ponieważ dostarczają one informacji i praktycznych umiejętności, które mogą okazać się atutem na rynku pracy. Wszystkie wspomniane szkolenia powinny być dostosowane do grupy docelowej, ze szczególnym uwzględnieniem potrzeb stażystów, a my przedstawimy Państwu nasz program pilotażowy i sposób, w jaki wdrożyliśmy te szkolenia z grupą docelową.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

4. PRZYGOTOWANIE PROGRAMU PILOTAŻOWEGO

Przygotowanie programu pilotażowego zaplanowano dwutorowo - przygotowanie na poziomie projektu oraz na poziomie organizacji. Na poziomie projektu CTS Customized Training Solutions, jeden z sześciu partnerów, przygotował dokument określający harmonogram, zadania i sposoby realizacji pilotażowej wersji szkolenia, który zawierał również wskazówki, jak zorganizować działania edukacyjne i jakie narzędzia wykorzystać do zbierania informacji zwrotnych od użytkowników.

Okazało się to cennym wkładem w przygotowanie programu pilotażowego, ponieważ wszyscy partnerzy mieli dostęp do struktury i wytycznych operacyjnych w dalszym przygotowaniu programu pilotażowego na poziomie organizacji. Na tym etapie reszta partnerów określiła własne harmonogramy, formaty i czas trwania sesji, w których będą organizować szkolenie, a następnie sesję zbierania informacji zwrotnych od uczestników w celu przeanalizowania jak największej ilości danych na temat wrażeń, komentarzy i sugestii dotyczących poprawy szkolenia. Pod koniec fazy walidacji wszyscy partnerzy dostarczyli do CTS Customized Training Solutions formularze informacji zwrotnych, aby umożliwić opracowanie wytycznych dotyczących całości szkolenia.

Na poziomie organizacji przygotowanie programu pilotażowego obejmowało kilka kroków, takich jak: rekrutacja uczestników, nawiązanie z nimi komunikacji, wybór odpowiednich narzędzi i strategii, przeprowadzenie szkolenia i zebranie informacji zwrotnej. W krótkim podsumowaniu tego, w jaki sposób partnerzy wybrali uczestników i zaprosili ich na wydarzenie, widzimy, że zostali oni pozyskani spośród klientów biznesowych każdego z partnerów, zwłaszcza z mikro, małych i średnich przedsiębiorstw, a także za pośrednictwem mediów społecznościowych. Partnerzy zapewnili akcje promocyjne w mediach społecznościowych, skierowane do małych przedsiębiorców, pracowników i bezrobotnych, nauczycieli i innych organizatorów kształcenia i szkolenia zawodowego, którzy dołączyli do wydarzeń. Kanałami poprzez które docierano do grup odbiorców były e-maile i reklamy w mediach społecznościowych.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Szkolenia odbywały się stacjonarnie i przebiegały w kilku krokach: trenerzy / nauczyciele przedstawili się i krótko wyjaśnili cele projektu, a następnie uczestnicy przedstawili się i wyrazili swoje oczekiwania wobec kursu.

Następnie nauczyciele zaprezentowali treść materiałów edukacyjnych opracowanych przez partnerów, a także platformę OER, a stażystów zachęcano do częstego zadawania pytań w celu wyjaśnienia ewentualnych wątpliwości lub do wniesienia do dyskusji swoich osobistych doświadczeń w dziedzinie cyberbezpieczeństwa.

Ponadto uczestnicy byli zachęcani do korzystania z bezpłatnego dostępu do treści edukacyjnych jako cennego zasobu w radzeniu sobie z wyzwaniami związanymi z bezpieczeństwem cybernetycznym. Na koniec uczestnicy zostali poproszeni o przekazanie osobistej opinii na temat wydarzenia i materiałów edukacyjnych.

5. OTWARTA PLATFORMA EDUKACYJNA JAKO CYFROWE WSPARCIE

Jednym z głównych celów tego projektu było zbudowanie platformy internetowej - nośnika otwartych zasobów edukacyjnych (OER), stanowiącego środowisko szkoleniowe, przy użyciu którego można dzielić się wiedzą na temat głównych aspektów, które należy wziąć pod uwagę w dziedzinie cyberbezpieczeństwa. Ponieważ projekt jest skierowany do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, którym brakuje niezbędnych narzędzi i zasobów do zarządzania ryzykiem związanym z bezpieczeństwem cyfrowym, platforma OER ma na celu dostarczenie potencjalnym odbiorcomcałej niezbędnej wiedzy, dostępnej w jednym miejscu, a wszystkie treści będą całkowicie otwarte i dostępne za darmo.

Z technicznego punktu widzenia platforma posiada publiczny ‘front-end’ Cyber-MSME (interfejs użytkownika) oraz prywatną/ukrytą sekcję back-office. Za jej pośrednictwem zawartość stron internetowych jest zarządzana przez PHP i zaawansowane technologie inżynieryjne (Ajax, DHTML, Javascript) w celu stworzenia środowiska charakteryzującego się użytecznością - strona jednocześnie wyświetla treści i posiada narzędzia w pięciu różnych językach: angielskim, rumuńskim, włoskim, polskim i hiszpańskim. Aby platforma w pełni spełniała swoje cele i potrzeby potencjalnych odbiorców, partnerzy zapewnili jej pełną funkcjonalność i dostępność, co oznacza, że nie jest wymagane logowanie ani rejestracja, a cała zawartość jest bezpłatna i osiągalna w dowolnym momencie.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Sposób skonstruowania platformy spełnia wymagania Otwartej Platformy ICT (ICT), czyli ma na celu ekspansję grupy docelowej projektu poprzez pomaganie studentom w kształceniu i szkoleniu zawodowym (VET) oraz poszerzaniu i pogłębianiu umiejętności cyfrowych (ICT). Platforma OER służy jako platforma e-learningowa, w której treści szkoleniowe, wraz ze wszystkimi zestawami narzędzi i kursami, są wyświetlane według wyszukiwanych kategorii np. obszaru / tematu, dzięki inteligentnym funkcjom przeglądania. Wytyczne te zawarte są również w platformie, służącej zwiększeniu możliwości wykorzystania wyników projektów realizowanych w ramach grup docelowych.

Jedną z funkcjonalności zaimplementowanych w ramach platformy jest ‘back-office’, w skład którego wchodzą:

- Sekcja użytkowników back office, która pozwala nam dodawać użytkowników do platformy;
- Sekcja wiadomości, która pozwala nam dodawać wiadomości i wydarzenia w części publicznej, w każdym języku;
- Sekcja FAQ;
- Sekcja partnerzy;
- Sekcja dokumentów, w której możemy przesłać zasoby edukacyjne z możliwością wysłania alertu do wszystkich, aby poinformować, że nowy dokument został przesłany;
- Sekcja terminów;
- Sekcja Słownik zawierająca terminy, które mogą być przydatne;
- Sekcja współpracownicy;
- Sekcja kategorii pogrupowanych w obszary tematyczne, takie jak: symulacje kryzysu cybernetycznego i lista kontrolna gotowości cyberprzestrzeni;
- Sekcja szkoleniowa z materiałami edukacyjnymi wymienionymi w sekcji szkoleniowej, które można wyszukać według odniesienia, tytułu szkolenia, daty

i języka;

- Sekcja treści szkoleniowych z zasobami edukacyjnymi, które są łatwe w użyciu i dostosowane do grup szkoleniowych, w oparciu o ich specyficzne potrzeby.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.

Niniejszy dokument i jego treść odzwierciedlają wyłącznie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w nim zawartych.

Jak wspomnieliśmy wcześniej, platforma OER to cyfrowe wsparcie dla wszystkich osób uczących się, pracujących w obszarze kształcenia zawodowego, a także dla uczących się samodzielnie, które to osoby są zachęcane do korzystania z niej zarówno w środowisku cyfrowym, jak i bezpośrednim.

Z naszego punktu widzenia platforma OER okazała się niezastąpioną pomocą w prowadzeniu szkoleń, ponieważ trenerzy traktowali ją jako źródło wiedzy dostępne po szkoleniu w dowolnym momencie, a także pokazali uczącym się, jak wykorzystać ją do samodzielnej nauki, by poszerzyć wiedzę na temat obszaru cyberbezpieczeństwa, a także jak uzyskać dostęp do sekcji testów i informacji zwrotnej o kursach i, które osoby korzystające z OER uznały za intuicyjne i wciągające.

6. UWAGI NAUCZYCIELI / MENTORÓW

Wytyczne zawierają wnioski płynące po zrealizowanych szkoleniach, a także spostrzeżenia na temat możliwego odbioru treści lekcji przez uczniów, ich ogólnej wiedzy o omawianych tematach, najbardziej odpowiednich metod realizacji w oparciu o daną treść wykładu i innych doświadczeń związanych z uczeniem się w ogóle. Z perspektywy trenerów wiedza osób uczestniczących w szkoleniu była elementarna, ale wszyscy wykazywali duże zainteresowanie tematami poruszanymi podczas lekcji i powiedzieli, że są zadowoleni z eksploracji zasobów edukacyjnych za pośrednictwem platformy OER. Zapytani o najbardziej odpowiednie podejście do prowadzenia szkolenia, mentorzy stwierdzili, że łączenie tematów z wielu różnych kursów dało najlepsze wyniki i doradzili korzystanie zarówno z programu online, jak i stacjonarnego przy wsparciu platformy OER. Ponadto, po zakończeniu procedur testowych i sprawdzeniu w praktyce, co zadziałało, a co nie, trenerzy byli w stanie przedstawić kilka pomysłów na poprawę, sugerując, że dobrym podejściem byłoby włączenie testu oceny wiedzy przed rozpoczęciem modułów z jednej strony i wykorzystanie bardziej rzeczywistych scenariuszy do zaangażowania uczniów z drugiej strony.

7. WSKAZÓWKI

Przesłaniem, które nasi trenerzy kierują do organizacji, które planują wykorzystać treści i narzędzia Cyber-MSME u siebie, jest poświęcenie czasu na poznanie materiałów edukacyjnych i znalezienie sposobów na dostosowanie ich do różnych grup docelowych, w oparciu o ich potrzeby, ogólną wiedzę na temat oraz obszary działania zawodowego.

Ponadto, oprócz uwag i zaleceń trenerów, raport mapujący pokazuje statystyki i potrzeby każdego z krajów partnerskich, co stanowi dobry punkt wyjścia do organizowania szkoleń. Wytyczne wraz z opiniami trenerów są podstawą prowadzenia szkoleń, jednak gorąco zachęcamy wszystkich potencjalnych użytkowników do dostosowania materiałów edukacyjnych do kontekstu, w którym działają i do potrzeb grupy odbiorców szkoleń. Trenerom zaleca się angażowanie uczestników w realizację kursu oraz aktywne budowanie środowiska szkoleniowego opartego na rozwoju i współtworzeniu treści.

8. UWAGI KOŃCOWE

Na zakończenie projektu opracowaliśmy dwa podsumowania w celu promowania skalowalności projektu, jego przenoszenia i powielania jego wyników w praktyce w innych dziedzinach, a także przegląd spostrzeżeń partnerów w dziedzinie cyberbezpieczeństwa wraz zaleceniami, którymi chcą się podzielić z decydentami i wszystkimi, którzy chcą korzystać z zestawów narzędzi i kursów.

„WYTYCZNE” są jedną z dwóch części tych rezultatów. Drugi dokument to „POLICY PAPER”, który stanowi wkład w zakres działań polityków i lokalnych decydentów w dziedzinie bezpieczeństwa cybernetycznego, gotowości cybernetycznej i odporności cybernetycznej sektora prywatnego – ze szczególnym odniesieniem do mikro- i małych średnich przedsiębiorstw – i bardziej ogólnie, podejście do aspektów takich jak konkurencyjność MŚP, kształcenie i szkolenie zawodowe na poziomie menedżerskim, rozwój biznesu, cyfryzacja ogółu obywateli UE.

Projekt współfinansowany w ramach programu Unii Europejskiej „Erasmus+”

Przy wsparciu programu Unii Europejskiej Erasmus+.