Co-funded by the European Union

PRZEWODNIK DOBRYCH PRAKTYK DLA MŚP

CYBER AGENT 06.2026

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

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.

www.cyberagents.eu

WP 6: Upowszechnianie i wykorzystanie wyników

Wynik 6.4: Przewodnik po dobrych praktykach dla MŚP

Lider WP6 – Women4Cyber Foundation

TREŚĆ

WYKAZ TABEL

WPROWADZENIE

Projekt CyberAgent był realizowany przez trzy lata w ośmiu krajach europejskich: Rumunii, Belgii, Norwegii, Hiszpanii, Turcji, Polsce, Litwie i Finlandii. Projekt CyberAgent powstał w celu opracowania i przetestowania modułowego, przystępnego programu szkoleniowego z zakresu cyberbezpieczeństwa przeznaczonego dla pracowników małych i średnich przedsiębiorstw (MŚP), osób uczących się w ramach kształcenia i szkolenia zawodowego oraz studentów uczelni wyższych. Głównym rezultatem tych prac jest rola „agenta zmian w zakresie cyberbezpieczeństwa" (Cybersecurity Change Agent) – przeszkolonego, niespecjalistycznego pracownika, który pełni rolę wewnętrznego punktu odniesienia w zakresie zwiększania świadomości cyberbezpieczeństwa w swojej organizacji.

Niniejszy przewodnik przekłada doświadczenia zdobyte podczas realizacji projektu na praktyczne wskazówki dla MŚP. Wyjaśnia, na czym polega rola agenta zmian, jak zidentyfikować i wyznaczyć odpowiednią osobę, jak wspierać proces jej szkolenia oraz jak zapewnić, by kwestie równości płci były uwzględnione w procesie od samego początku. Lista kontrolna zamieszczona na końcu pomaga MŚP sprawdzić, czy na każdym etapie spełnione są odpowiednie warunki.

1. DLACZEGO CYBERBEZPIECZEŃSTWO MA ZNACZENIE DLA KAŻDEGO MAŁEGO I ŚREDNIEGO PRZEDSIĘBIORSTWA

Zgodnie z raportem ENISA „Threat Landscape 2025" cyberprzestępcy industrializują swoje ataki, co sprawia, że małe i średnie przedsiębiorstwa stają się atrakcyjnymi celami niezależnie od ich wielkości i branży. Najczęstszymi zagrożeniami, z jakimi borykają się obecnie organizacje, są oprogramowanie ransomware, phishing oraz naruszenia bezpieczeństwa danych. Oprogramowanie ransomware i naruszenia bezpieczeństwa danych stanowią większość incydentów cyberprzestępczych wymierzonych w organizacje z UE, przy czym ransomware odpowiada za ponad 80% tych przestępstw. Industrializacja tych ataków, a zwłaszcza model „Ransomware-as-a-Service", obniżyła bariery dla atakujących, sprawiając, że nawet najmniejsze organizacje stały się realnymi celami.

Szczególnie w przypadku MŚP konsekwencje cyberataku nie ograniczają się do tymczasowych zakłóceń. Według ENISA cyberataki mają poważny negatywny wpływ na działalność 90% MŚP już w ciągu tygodnia od ich wystąpienia. Jednak pomimo tego narażenia MŚP rzadko dysponują wyspecjalizowanym personelem IT lub ds. bezpieczeństwa, a ich pracownicy rzadko przechodzą usystematyzowane szkolenia z zakresu cyberbezpieczeństwa. MŚP w Europie zatrudniają około 100 milionów osób i generują ponad połowę europejskiego PKB. W związku z tym luka w cyberbezpieczeństwie w sektorze MŚP stanowi istotne zagrożenie gospodarcze i społeczne.

Większość cyberataków kończy się sukcesem z powodu czynników ludzkich, takich jak kliknięcie w link phishingowy, stosowanie słabych haseł lub otwieranie niezweryfikowanych wiadomości e-mail. Oznacza to, że pierwszą linią obrony nie jest narzędzie techniczne, lecz dobrze poinformowany i świadomy pracownik, który potrafi rozpoznać zagrożenie oraz właściwie zareagować w sytuacji incydentu. Właśnie taką rolę pełni „Cybersecurity Change Agent".".

2. AGENT ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA

Koncepcja „agenta zmian w zakresie cyberbezpieczeństwa" stanowi sedno projektu CyberAgent. W niniejszej sekcji wyjaśniono, na czym polega ta rola, dlaczego została stworzona oraz jak jest realizowana w praktyce w małych i średnich przedsiębiorstwach (MŚP).

2.1. CZYM TO JEST I DO CZEGO SŁUŻY

Małe i średnie przedsiębiorstwa stanowią filar europejskiej gospodarki, a mimo to należą do grup najbardziej narażonych na zagrożenia związane z cyberbezpieczeństwem. W przeciwieństwie do dużych firm większość MŚP nie posiada wyspecjalizowanych działów IT ani specjalistów ds. bezpieczeństwa, a ich pracownicy rzadko uczestniczą w usystematyzowanych szkoleniach z zakresu cyberbezpieczeństwa. Powoduje to utrzymującą się lukę pomiędzy zagrożeniami cybernetycznymi, z jakimi mierzą się MŚP, a ich zdolnością do skutecznego reagowania na nie.

Projekt CyberAgent oraz rola „Cybersecurity Change Agent" zostały stworzone w celu wypełnienia tej luki poprzez rozwijanie nowych kompetencji w ramach istniejących zespołów. Cybersecurity Change Agent to przeszkolony pracownik bez specjalistycznego wykształcenia technicznego, który pełni rolę wewnętrznego ambasadora świadomości cyberbezpieczeństwa, promując bezpieczne zachowania, pomagając rozpoznawać typowe zagrożenia oraz wspierając wdrażanie dobrych praktyk w zakresie cyberbezpieczeństwa w organizacji. Osoba ta służy również współpracownikom jako punkt kontaktowy i źródło podstawowego wsparcia w przypadku incydentów związanych z cyberbezpieczeństwem.

Potrzebę istnienia tej roli potwierdzają dane zebrane podczas realizacji projektu pilotażowego CyberAgent. W ośmiu krajach partnerskich w szkoleniu uczestniczyło 594 osób, w tym pracownicy MŚP, studenci uczelni wyższych oraz uczestnicy kształcenia i szkolenia zawodowego. Pracownicy MŚP są powszechnie uznawani za jedną z grup docelowych, do których najtrudniej dotrzeć w działaniach edukacyjnych, głównie ze względu na ograniczenia czasowe i obowiązki zawodowe. Mimo to wysoki wskaźnik ukończenia szkolenia wśród tej grupy potwierdza duże zainteresowanie tematyką cyberbezpieczeństwa oraz jej znaczenie w codziennej pracy przedsiębiorstw.

2.2. GŁÓWNE OBOWIĄZKI

Agent zmian w zakresie cyberbezpieczeństwa nie jest odpowiedzialny za samodzielne rozwiązywanie problemów związanych z cyberbezpieczeństwem. Rola ta opiera się na budowaniu świadomości, komunikacji i koordynacji – jest to osoba w organizacji, która dba o to, by kwestie cyberbezpieczeństwa pozostawały w centrum uwagi oraz pomaga współpracownikom radzić sobie z nimi w codziennej pracy. Nie wymaga to żadnej wiedzy technicznej. Potrzebna jest natomiast osoba ciesząca się zaufaniem, posiadająca szerokie kontakty w organizacji oraz zmotywowana do tego, by cyberbezpieczeństwo stało się naturalną częścią sposobu działania zespołu.

· **W praktyce rola ta przekłada się na zestaw powtarzalnych,** nieskomplikowanych działań, które nie wymagają dużego nakładu czasu, ale mają istotny wpływ na kulturę bezpieczeństwa w organizacji:

· **Regularne działania uświadamiające.** Agent zmian regularnie przekazuje współpracownikom informacje uświadamiające na temat najczęstszych zagrożeń, takich jak wiadomości phishingowe, słabe hasła, niebezpieczne postępowanie z danymi czy podejrzane linki, dbając o to, by kwestia cyberbezpieczeństwa pozostawała w centrum uwagi, nie stając się przy tym uciążliwością. Może to być na przykład comiesięczna wiadomość wysyłana na czacie zespołowym, krótkie przypomnienie przed intensywnym okresem pracy lub informacja o nowym rodzaju oszustwa krążącym w branży. Forma ma mniejsze znaczenie niż regularność.

· **Uwzględnienie kwestii cyberbezpieczeństwa w porządku obrad.** Agent zmian w zakresie cyberbezpieczeństwa porusza tematy związane z cyberbezpieczeństwem podczas spotkań zespołów w formie krótkich, praktycznych dyskusji. Nie chodzi tu o długie prezentacje ani formalne szkolenia. Wystarczy pięciominutowa rozmowa na temat niedawnej próby phishingu lub przypomnienie o aktualizacji haseł, aby podtrzymać świadomość i dać do zrozumienia, że cyberbezpieczeństwo jest wspólnym obowiązkiem całej organizacji, a nie zadaniem powierzonym wyłącznie pracownikom technicznym.

· **Zachęcanie do zgłaszania zdarzeń.** Jednym z najważniejszych zadań agenta zmian w zakresie cyberbezpieczeństwa jest tworzenie kultury, w której pracownicy czują się swobodnie, zgłaszając podejrzane sytuacje, takie jak nietypowa wiadomość e-mail, nieoczekiwane zachowanie systemu czy kliknięcie przez współpracownika w coś, czego nie powinien był kliknąć. Wiele incydentów związanych z cyberbezpieczeństwem przybiera poważniejszy obrót, ponieważ pracownicy nie zgłaszają wczesnych sygnałów ostrzegawczych z obawy przed zawstydzeniem lub obwinieniem. Agent zmian pomaga uczynić zgłaszanie takich sytuacji czymś naturalnym, wykazując się otwartością i jasno wyjaśniając procedurę.

· **Wspieranie procesu wdrażania nowych pracowników.** Nowi pracownicy należą do najbardziej narażonych członków każdej organizacji z punktu widzenia cyberbezpieczeństwa, ponieważ nie znają jeszcze wewnętrznych procedur, są bardziej skłonni do ufania nieoczekiwanym prośbom i często nie zostali jeszcze przeszkoleni w zakresie podstawowych zasad bezpieczeństwa. Agent zmian w zakresie cyberbezpieczeństwa odgrywa ważną rolę we wprowadzaniu podstaw cyberbezpieczeństwa podczas wdrażania nowych pracowników, dbając o to, by dobre nawyki zostały wykształcone od pierwszego dnia, a nie wprowadzane dopiero później.

· **Pełnienie funkcji wewnętrznego punktu kontaktowego.** Osoba pełniąca rolę „agenta zmian w zakresie cyberbezpieczeństwa" to osoba, do której współpracownicy zwracają się, gdy mają pytania dotyczące cyberbezpieczeństwa lub nie są pewni, jak postąpić w danej sytuacji. Oznacza to, że wiedzą, gdzie ją znaleźć, do kogo skierować sprawę oraz jak skierować współpracownika do odpowiedniego źródła wsparcia. W małych i średnich przedsiębiorstwach, które nie dysponują wyspecjalizowanym personelem IT, rola ta wypełnia lukę, która w przeciwnym razie pozostawiłaby pracowników bez jasnego punktu odniesienia.

• **Promowanie szkoleń i ciągłego kształcenia.** Agent zmian zachęca współpracowników do korzystania z dostępnych zasobów szkoleniowych, w tym modułów CyberAgent, oraz na bieżąco śledzi zmiany w dziedzinie cyberbezpieczeństwa istotne dla sektora i działalności organizacji.

• **Gromadzenie i przekazywanie opinii.** Agent zmian gromadzi informacje zwrotne dotyczące kwestii związanych z cyberbezpieczeństwem w organizacji – tego, co pracownicy uważają za niejasne, jakie procedury nie są przestrzegane oraz jakie zagrożenia postrzegają jako najpilniejsze – a następnie przekazuje te spostrzeżenia kierownictwu. To właśnie ten cykl informacji zwrotnych pozwala organizacji z czasem stopniowo rozwijać i wzmacniać swoją kulturę bezpieczeństwa.

Tabela 1. Różnice między zadaniami pracowników technicznych a zadaniami agenta ds. zmian

SPECJALISTA DS. IT (stanowisko techniczne)	SPECJALISTA DS. CYBERBEZPIECZEŃSTWA (Rola kierownicza i kulturowa)
zarządza techniczną konfiguracją zapór sieciowych i systemów zabezpieczeń	Udostępnia współpracownikom dostosowane do potrzeb komunikaty informacyjne i ostrzeżenia dotyczące bezpieczeństwa
odpowiada za aktualizacje oprogramowania, wdrażanie poprawek oraz konfigurację techniczną systemów	zapewnia uwzględnianie kwestii cyberbezpieczeństwa w porządku obrad spotkań zespołu
Reaguje na incydenty cyberbezpieczeństwa oraz incydenty o charakterze technicznym	Zachęca współpracowników do aktywnego i przejrzystego zgłaszania podejrzanych działań
monitoruje ruch sieciowy, logi bezpieczeństwa oraz zgodność techniczną systemów	Wspiera nowych pracowników podczas procesu wdrażania do organizacji w zakresie podstawowych zasad cyberbezpieczeństwa
Wdraża techniczne środki bezpieczeństwa i zarządza dostępem do infrastruktury IT	zbiera informacje zwrotne od pracowników i przekazuje kwestie systemowe do kierownictwa lub działu IT

3. WYBÓR I MIANOWANIE AGENTA ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA

Wybór odpowiedniej osoby na stanowisko „agenta zmian w zakresie cyberbezpieczeństwa" oraz zapewnienie jej warunków sprzyjających osiągnięciu sukcesu to kluczowe decyzje, które należy podjąć przy wdrażaniu tej funkcji w organizacji. Projekt pilotażowy „CyberAgent" wykazał, że rola ta sprawdza się najlepiej, gdy pełni ją osoba postrzegana jako godna zaufania, znająca procedury organizacji oraz ciesząca się poparciem kierownictwa. W niniejszej sekcji przedstawiono praktyczne wskazówki dotyczące jasnego zdefiniowania tej roli w celu zapewnienia długoterminowego sukcesu oraz precyzyjnego zdefiniowania tej roli oraz wyboru odpowiedniego kandydata w celu zapewnienia jej długoterminowej skuteczności..

3.1. JAK WYBRAĆ ODPOWIEDNIEGO KANDYDATA

Zgodnie z wynikami programu pilotażowego CyberAgent najskuteczniejsi „agenci zmian w zakresie cyberbezpieczeństwa" to niekoniecznie osoby z wcześniejszym doświadczeniem technicznym. W ośmiu krajach objętych programem pilotażowym uczestnicy z sektora MŚP, którzy najaktywniej angażowali się w szkolenia i wykazywali największy potencjał, to osoby łączące świadomość organizacyjną z umiejętnościami komunikacyjnymi oraz autentyczną motywacją do wprowadzania zmian w swoim miejscu pracy. Na podstawie doświadczeń zebranych w ramach programu pilotażowego można stwierdzić, że następujące cechy zazwyczaj sprzyjają odniesieniu sukcesu w tej roli:

- Znajomość wewnętrznych procesów organizacji oraz praktyk związanych z przetwarzaniem danych.
- Dobre umiejętności komunikacyjne i interpersonalne.
- Wsparcie ze strony kierownictwa.

Co ważne, stanowisko to nie wymaga wykształcenia technicznego ani doświadczenia w branży IT. Dlatego pracownicy zajmujący stanowiska administracyjne, w działach kadr, operacyjnym i kierowniczym mogą skutecznie pełnić funkcję agenta zmian, pod warunkiem że otrzymają odpowiednie szkolenie i wsparcie. Rezygnacja z wymogu posiadania wiedzy technicznej jest świadomym wyborem projektowym, który znacznie poszerza pulę potencjalnych kandydatów i otwiera drzwi do różnorodności płciowej, co wykazał program pilotażowy.

Po wyłonieniu kandydata należy nadać tej roli widoczność i legitymizację w ramach organizacji. Zakres obowiązków powinien zostać ogłoszony w całej organizacji i jasno zdefiniowany: za co odpowiada agent zmian w zakresie cyberbezpieczeństwa, komu podlega oraz czego się od niego nie oczekuje.

3.2. PEŁNIENIE TEJ ROLI

K Kolejnym krokiem jest wdrożenie tej roli w organizacji. Poniższe kroki opierają się bezpośrednio na wnioskach wyciągniętych z projektu pilotażowego CyberAgent realizowanego w krajach partnerskich i zostały zaprojektowane tak, aby dostosowane do potrzeb małych i średnich przedsiębiorstw (MŚP) niezależnie od ich wielkości.

3.2.1. SZKOLENIE OSOBY ODPOWIEDZIALNEJ ZA WPROWADZANIE ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA

Wybierz najbardziej odpowiednią osobę w swojej organizacji i zapewnij jej dostęp do programu szkoleniowego CyberAgent. Program składa się z dziewięciu modułów obejmujących zarządzanie programem bezpieczeństwa (M1), administrację systemową (M2), narzędzia analityczne (M3), operacje bezpieczeństwa (M4), zarządzanie bezpieczeństwem i politykę bezpieczeństwa (M5), planowanie cyberbezpieczeństwa (M6), zarządzanie ryzykiem (M7), ciągłość działania (M8) oraz rozwój kariery w dziedzinie cyberbezpieczeństwa (M9).

Te dziewięć modułów zostało formalnie ujętych w dwóch oficjalnych wynikach projektu: D3.1, obejmującym program nauczania dla uczelni wyższych, oraz D3.2, obejmującym program nauczania dla kształcenia i szkolenia zawodowego. Moduły, o których mowa w niniejszym przewodniku, odpowiadają zatem bezpośrednio treściom opisanym w dokumentach D3.1 i D3.2 i są dostępne za pośrednictwem platformy CyberAgent niezależnie od przynależności instytucjonalnej uczestnika szkolenia. Ponadto program nauczania jest dostosowany do poziomów 4–6 Europejskiej Ramy Kwalifikacji (EQF) dla pracowników MŚP, zapewniając podstawowe umiejętności i wiedzę z zakresu cyberbezpieczeństwa wraz z praktycznym zastosowaniem w obszarach kompetencji technicznych, analitycznych, zarządzania ryzykiem oraz kompetencji organizacyjnych.

Szkolenie odbywa się we własnym tempie i jest dostępne online, co oznacza, że wybrany pracownik może je ukończyć w sposób elastyczny, dostosowując się do swoich bieżących obowiązków służbowych. Po ukończeniu modułu i zdaniu testu sprawdzającego wiedzę z wynikiem co najmniej 75% „agent zmian w zakresie cyberbezpieczeństwa" otrzymuje certyfikat ukończenia kursu dla danego modułu, który stanowi formalny dowód nabytych kompetencji i może służyć do dokumentowania ukończenia szkolenia w ramach organizacji.

3.2.2. OKREŚLENIE OBOWIĄZKÓW I WŁĄCZENIE DO ISTNIEJĄCYCH STRUKTUR

Po rozpoczęciu lub zakończeniu szkolenia organizacja powinna formalnie określić zakres obowiązków agenta zmian w zakresie cyberbezpieczeństwa oraz włączyć tę rolę do istniejących struktur organizacyjnych. Oznacza to uzgodnienie, czym będzie się zajmował agent zmian, ile czasu poświęci na pełnienie tej roli oraz z kim będzie współpracował, a także poinformowanie o tym całego zespołu.

Projekt pilotażowy wykazał, że rola agenta zmian w zakresie cyberbezpieczeństwa jest najbardziej trwała, gdy jest włączona z istniejącymi strukturami organizacyjnymi, a nie funkcjonuje w izolacji. Może to oznaczać włączenie jej do porządku obrad regularnych spotkań zespołu lub powiązanie z istniejącą strukturą ds. bezpieczeństwa i higieny pracy lub zgodności z przepisami. Celem jest uczynienie świadomości w zakresie cyberbezpieczeństwa naturalną częścią codziennej pracy oraz wspólną odpowiedzialnością organizacyjną, a nie odrębnym działaniem...

3.2.3. ZWIĘKSZANIE ŚWIADOMOŚCI WEWNĘTRZNEJ NA TEMAT TEJ ROLI

Agent zmian w zakresie cyberbezpieczeństwa nie może skutecznie działać, jeśli współpracownicy nie wiedzą, kim jest ani czym się zajmuje. Aby zapewnić wybranemu pracownikowi legitymację organizacyjną niezbędną do pełnienia jego funkcji, konieczne jest wdrożenie jasnej komunikacji wewnętrznej opisującej jego rolę oraz zakres obowiązków oraz organizowanie regularnych spotkań, podczas których pracownicy będą mogli zadawać pytania.

Poza wstępnym ogłoszeniem należy zachęcać agenta zmian do utrzymywania widoczności kwestii cyberbezpieczeństwa w organizacji poprzez regularne działania komunikacyjne. Nie oznacza to długich szkoleń ani formalnych prezentacji. W kontekście małych i średnich przedsiębiorstw można to realizować w formie krótkich działań bezpośrednio związanych z sytuacjami, które pracownicy rozpoznają w swojej codziennej pracy. Regularne przeglądy i monitorowanie roli agenta zmian w zakresie cyberbezpieczeństwa

3.2.4. UTRZYMYWANIE W DŁUŻSZEJ PERSPEKTYWIE CZASOWEJ

Aby rola agenta zmian w zakresie cyberbezpieczeństwa mogła przynieść trwałe efekty, organizacja musi stworzyć warunki umożliwiające jej kontynuację i rozwój. Oznacza to wdrożenie procesu przeglądu przeprowadzanego co najmniej raz w roku, mającego na celu ocenę tego, co się sprawdza, jakie luki nadal istnieją oraz czy agent zmian w zakresie cyberbezpieczeństwa potrzebuje dodatkowego szkolenia lub wsparcia.

Wyniki projektu pilotażowego wskazują, że utrzymanie zaangażowania wymaga czegoś więcej niż tylko wstępnego szkolenia. Uczestnicy z sektora MŚP konsekwentnie potrzebują elastycznych terminów, przypomnień oraz wsparcia okresowego w celu utrzymania tempa działań. Wprowadzenie prostego corocznego przeglądu oraz zapewnienie agentowi zmian w zakresie cyberbezpieczeństwa stałego dostępu do zasobów stanowią minimalny warunek utrzymania skuteczności tej roli w dłuższej perspektywie.

4. RÓWNOŚĆ PŁCI I WŁĄCZAJĄCY CHARAKTER PROGRAMU

Cyberbezpieczeństwo pozostaje jedną z dziedzin europejskiej gospodarki, w których dominują mężczyźni. Kobiety stanowią około 20% pracowników sektora cyberbezpieczeństwa w całej UE, a ich udział w szkoleniach z tej dziedziny odzwierciedla tę samą nierównowagę. Ze względu na istniejącą lukę w umiejętnościach i talentach branża, która czerpie z zaledwie ułamka dostępnej puli kadr, będzie miała trudności z zaspokojeniem popytu na skalę wymaganą przez obecny krajobraz zagrożeń.

Projekt CyberAgent został zaprojektowany z wyraźnym celem uwzględnienia kwestii płci oraz promowania równości płci i włączenia społecznego, a nie jako dodatek. W dziedzinie, w której kobiety zazwyczaj stanowią niewielką mniejszość wśród uczestników szkoleń, duży udział kobiet w programie pilotażowym jest znaczącym wynikiem i był efektem ukierunkowanych strategii promocyjnych oraz podejścia sprzyjającego włączeniu społecznemu

4.1. DLACZEGO MA TO ZNACZENIE DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

W przypadku małych i średnich przedsiębiorstw (MŚP) kwestia płci w kontekście cyberbezpieczeństwa dotyczy zarówno kadry pracowniczej, jak i kultury organizacyjnej. Większość MŚP nie zatrudnia specjalistów ds. cyberbezpieczeństwa. Ich cyberodporność zależy od świadomości i zachowań wszystkich pracowników, zwłaszcza osób zajmujących stanowiska administracyjne, kadrowe, finansowe i operacyjne. Dlatego wykluczenie kobiet ze szkoleń uświadamiających w zakresie cyberbezpieczeństwa stanowi istotne ryzyko dla bezpieczeństwa organizacyjnego.

Jednocześnie rola „agenta zmian w zakresie cyberbezpieczeństwa" stanowi konkretną okazję do rozwiązania problemu nierównowagi płci w cyberbezpieczeństwie wewnątrz małych i średnich przedsiębiorstw. Ponieważ rola ta opiera się raczej na umiejętnościach komunikacyjnych, świadomości organizacyjnej i podejściu zarządczym niż na wiedzy technicznej, doskonale nadaje się dla szerokiego spektrum profili zawodowych i oferuje kobietom zajmującym stanowiska nietechniczne uznaną ścieżkę rozwoju w dziedzinie cyberbezpieczeństwa, która nie wymaga zmiany zawodu ani kwalifikacji technicznych.

4.2. KONKRETNE DZIAŁANIA MAJĄCE NA CELU ZWIĘKSZENIE UDZIAŁU KOBIET ORAZ GRUP NIEDOSTATECZNIE REPREZENTOWANYCH

Poniższe praktyczne działania wynikają z doświadczeń zdobytych w ramach projektu pilotażowego CyberAgent i zostały opracowane tak, aby mogły być wdrażane przez małe i średnie przedsiębiorstwa (MŚP) każdej wielkości.

Belgijski projekt pilotażowy wykazał, że kierowanie działań informacyjnych za pośrednictwem sieci, którym kobiety już ufają, takich jak stowarzyszenia zawodowe i sieci kobiet biznesu, zwiększa udział kobiet. W praktyce oznacza to, że gdy małe lub średnie przedsiębiorstwo poszukuje kandydatek na stanowisko „agenta zmian w zakresie cyberbezpieczeństwa", powinno aktywnie angażować wszelkie sieci zawodowe kobiet istotne dla danej branży lub regionu, zamiast polegać wyłącznie na ogłoszeniach publicznych.

Należy przedstawiać tę rolę w kategoriach wpływu na organizację, a nie wiedzy technicznej. Kobiety zajmujące stanowiska nietechniczne chętniej angażują się w szkolenia z zakresu cyberbezpieczeństwa i podejmują się funkcji agenta zmian, gdy rola ta jest przedstawiana w kategoriach wartości, jaką wnosi dla organizacji, a nie w kategoriach umiejętności technicznych. Rolę tę można przedstawić jako taką, która chroni bezpieczeństwo organizacji, wspiera współpracowników i przyczynia się do lepszego zarządzania. Istotne znaczenie ma język używany w komunikacji wewnętrznej, opisach stanowisk oraz materiałach rekrutacyjnych.

5. NAJLEPSZE PRAKTYKI

Powołanie osoby odpowiedzialnej za wprowadzanie zmian w zakresie cyberbezpieczeństwa stanowi ważny pierwszy krok, jednak rola ta może przynieść trwałe efekty jedynie wtedy, gdy będzie funkcjonować w ramach kultury organizacyjnej, która aktywnie ją wspiera. Poniższe najlepsze praktyki mają na celu pomóc małym i średnim przedsiębiorstwom w stworzeniu odpowiednich warunków, które pozwolą tej osobie odnieść sukces, a także sprawią, że świadomość w zakresie cyberbezpieczeństwa stanie się naturalną częścią funkcjonowania organizacji oraz jej codziennych procesów operacyjnych..

- **Zachęcaj do otwartej komunikacji**. Pracownicy powinni czuć się swobodnie, zgłaszając błędy, podejrzane sytuacje lub obawy dotyczące bezpieczeństwa, bez obawy przed obwinieniem lub zawstydzeniem. W wielu organizacjach incydenty związane z cyberbezpieczeństwem eskalują właśnie dlatego, że pracownicy wahają się przed zgłoszeniem czegoś, co budzi ich wątpliwości lub za co czują się odpowiedzialni.

- **Niech to będzie proste i wpisane w codzienne nawyki**. Podnoszenie świadomości w zakresie cyberbezpieczeństwa nie musi przybierać formy formalnych szkoleń czy długotrwałych warsztatów. Krótkie, praktyczne przypomnienia wplecione w istniejące rutyny są często skuteczniejsze niż sporadyczne, intensywne szkolenia. Celem jest uczynienie cyberbezpieczeństwa nawykiem działającym w tle, a nie sporadycznym wydarzeniem.

- **Dokumentuj każdy etap procesu**. Jednym z najbardziej praktycznych działań, jakie może podjąć małe lub średnie przedsiębiorstwo, jest spisanie podstawowych zasad dotyczących cyberbezpieczeństwa: w jaki sposób zarządza się hasłami, jak przechowuje się i udostępnia dane wrażliwe, co należy zrobić w przypadku otrzymania podejrzanego e-maila oraz z kim należy się skontaktować w razie incydentu. Nie muszą to być formalne dokumenty regulaminowe. Wystarczy jednostronicowy przewodnik dostępny dla wszystkich pracowników.

- **Zacznij od góry**. Zachowania, jakich oczekuje się od pracowników, muszą być wyraźnie demonstrowane przez kierowników i kadrę kierowniczą. Jeśli kierownictwo nie przestrzega podstawowych zasad bezpieczeństwa, wysyła to sygnał, że przestrzeganie tych zasad jest opcjonalne. Wiarygodność agenta zmian w organizacji zależy po części od tego, czy otaczająca go kultura wspiera to, co stara się on promować.

- **Dbaj o ciągłą świadomość**. Zagrożenia dla cyberbezpieczeństwa nieustannie ewoluują, a pojedyncze szkolenie szybko traci na aktualności. Podnoszenie świadomości należy traktować jako proces ciągły, a nie jednorazowe działanie. Oznacza to regularne kontakty, okresowe szkolenia odświeżające oraz obecność osoby pełniącej rolę „agenta zmian w zakresie cyberbezpieczeństwa", która na bieżąco śledzi aktualności i przekazuje odpowiednie informacje w organizacji.

5.1. INFORMACJE JAKOŚCIOWE Z KRAJOWYCH PROJEKTÓW PILOTAŻOWYCH

Z opinii jakościowych wynika, że uczestnicy ogólnie pozytywnie ocenili szkolenie, a wielu z nich stwierdziło, że nie wskazano potrzeby wprowadzenia istotnych zmian ani usprawnień. Najczęściej powtarzającymi się tematami w odpowiedziach otwartych (D5.3 – Ocena programu szkoleniowego CyberAgent w zakresie podnoszenia kwalifikacji) były: użyteczność platformy, nawigacja lub przebieg procesu oceny; kwestie związane z dostępnością techniczną lub niezawodnością; pozytywna ocena dostępności, elastyczności i wysokiej jakości treści merytorycznych; prośby o więcej praktycznych przypadków, ćwiczeń praktycznych lub rzeczywistych przykładów z sektora MŚP intensywność i gęstość treści, struktura lub zróżnicowanie ścieżek nauczania.

Warto zauważyć, że trzeci najczęściej poruszany temat (pozytywna ocena dostępności, elastyczności i szerokiej wiedzy) odzwierciedla uznanie ze strony uczestników, którzy stwierdzili, że nie są potrzebne żadne ulepszenia, i z własnej inicjatywy dobrowolnie podkreślili mocne strony programu. Jest to istotny sygnał jakościowy: w polu tekstowym przeznaczonym na krytykę prawie jedna czwarta odpowiedzi jakościowych wyrażała zadowolenie z dostępności i zakresu szkolenia.

5.2. KROKI DO PODJĘCIA W CELU WDROŻENIA I ZARZĄDZANIA SZKOLENIAMI W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH

Przeprowadzone na szeroką skalę wdrożenie pilotażowe platformy CyberAgent w ośmiu krajach europejskich dostarczyło kluczowych informacji na temat tego, w jaki sposób małe i średnie przedsiębiorstwa wdrażają i utrwalają umiejętności w zakresie cyberbezpieczeństwa. W oparciu o dane zebrane przy użyciu metod mieszanych oraz zidentyfikowane bariery wdrożeniowe i edukacyjne uczestników szkolenia, udokumentowane w końcowym raporcie z oceny szkolenia (D5.3), zaleca się kierownictwu przedsiębiorstw wdrożenie poniższych wewnętrznych działań zarządczych, technicznych i strategicznych w celu zwiększenia jego wpływu na poziomie organizacyjnym oraz operacyjnym..

Porady dotyczące zarządzania jakością

Materiały szkoleniowe CyberAgent zawierają obszerną wiedzę operacyjną i strategiczną. Menedżerowie powinni unikać przydzielania całego programu szkoleniowego za jednym razem; zamiast tego opracowanie modułowego harmonogramu szkoleniowego pozwala zapobiec zmęczeniu poznawczemu i zapewnia stopniową integrację nowych kompetencji z codziennymi procesami operacyjnymi organizacji.

Porady dotyczące integracji technicznej

Wstępne dane z programu pilotażowego wykazały, że techniczne utrudnienia związane z wdrożeniem, takie jak opóźnienia lub blokowanie lub filtrowanie wiadomości e-mail zawierających potwierdzenia rejestracji na platformie, mogą utrudniać wczesne przyjęcie rozwiązania. Przed uruchomieniem rejestracji użytkowników kierownictwo powinno skoordynować działania z administratorami filtrów sieciowych, aby zapewnić niezakłócony dostęp do zewnętrznych platform i domen e-learningowych, a także poinformować pracowników o konieczności monitorowania folderów ze spamem..

Wskazówki dotyczące wdrożenia strategicznego

Dane z krajowego programu pilotażowego wykazały, że moduły strategiczne wyższego poziomu – w szczególności M6 (Planowanie cyberbezpieczeństwa) i M8 (Ciągłość działania) – wymagają solidnego doświadczenia, aby można było w pełni wykorzystać ich potencjał. Aby zmaksymalizować natychmiastową wartość biznesową, moduły te powinny być skierowane konkretnie do personelu pełniącego obowiązki kierownicze, operacyjne oraz do pracowników odpowiedzialnych za podejmowanie decyzji strategicznych i operacyjnych w organizacji..

5.2.1. GŁOS OSOBY WPROWADZAJĄCEJ ZMIANY

W fazie pilotażowej, w ramach której zebrano łącznie 272 wyczerpujące odpowiedzi ankietowe z ośmiu krajów europejskich, zidentyfikowano trzy przekrojowe skutki dla grup docelowych.

Wysoka elastyczność realizacji szkolenia i równowaga między pracą a nauką

Aż 86,0% respondentów zgodziło się lub zdecydowanie zgodziło się, że asynchroniczny format szkolenia, umożliwiający naukę we własnym tempie, był na tyle elastyczny, że można go było płynnie wkomponować w ich harmonogramy zawodowe i akademickie, pozwalając pracownikom MŚP na pogodzenie rozwijania kompetencji zawodowych z codziennymi obowiązkami operacyjnymi.

Znaczenie metodologiczne dla personelu nietechnicznego

Wyniki programu pilotażowego potwierdzają zasadniczą koncepcję edukacyjną programu nauczania CyberAgent, dowodząc, że skuteczna cyberodporność organizacji nie wymaga zaawansowanych umiejętności technicznych ani programistycznych. Zgodnie z danymi z oceny wpływu zawartymi w dokumencie D5.3 77,2% uczestników stwierdziło, że szkolenie pozwoliło im jasno zrozumieć, w jaki sposób ich konkretne role zawodowe wpływają na codzienne praktyki bezpieczeństwa w przedsiębiorstwie i jak je chronią.

Mierzalny postęp wiedzy w stosunku do poziomu wyjściowego osób niebędących ekspertami

Analizy platformy pokazują, że 89,3% wszystkich uczestników osiągnęło potwierdzony wzrost wiedzy z zakresu cyberbezpieczeństwa. Co istotne, postęp ten był najbardziej widoczny wśród osób zupełnie początkujących: 90,9% uczestników, którzy przed rozpoczęciem programu ocenili swój początkowy poziom zrozumienia jako „bardzo niski", zgłosiło zdecydowany wzrost wiedzy i pewności siebie w rozpoznawaniu korporacyjnych zagrożeń cybernetycznych.

5.2.2. „CO NALEŻY, A CZEGO NIE NALEŻY ROBIĆ"

Na podstawie opinii przekazanych przez kraje uczestniczące w programie pilotażowym na temat „zróżnicowania ścieżek kształcenia" przedstawiamy zalecenia dla przedsiębiorstw:

Tabela 2 „Co robić, a czego nie robić"

NIE NALEŻY (pułapki dla MŚP)	ZALECANE (najlepsze praktyki)
Oczekiwanie, że pracownik zapozna się ze wszystkimi 8 modułami w nierealistycznie skróconym terminie (np. w ciągu tygodnia lub miesiąca). Badania pilotażowe (D5.3) wykazały, że brak czasu wynikający z codziennych obowiązków służbowych stanowił główną przeszkodę dla pracowników MŚP, co skutkowało niższym odsetkiem osób, które zaliczyły wszystkie moduły szkoleniowe z pozytywnym wynikiem test.	Opracowanie elastycznego, indywidualnego harmonogramu nauki dostosowanego do potrzeb i dostępności pracownika, z wykorzystaniem zasad mikrouczenia. Umożliwienie uczestnikom skupienia się na modułach, które bezpośrednio przyczyniają się do poprawy wyników w konkretnym obszarze ich pracy.
Oczekiwanie, że przeszkolony agent ds. zmian w zakresie cyberbezpieczeństwa zastąpi wyspecjalizowanych inżynierów IT lub samodzielnie rozwiąże złożone incydenty cyberbezpieczeństwa. Przenoszenie kluczowych oczekiwań dotyczących infrastruktury technicznej na pracowników o profilu nietechnicznym powoduje poważną niejasność oraz ryzyko błędnego przypisania odpowiedzialności (role misalignment).	Zachęcanie osoby wprowadzającej zmiany do pełnienia roli wewnętrznego koordynatora ds. bezpieczeństwa oraz osoby promującej świadomość w tym zakresie. Osoby te są najbardziej skuteczne, gdy promują kulturę bezpieczeństwa, przypominają o wewnętrznych szkoleniach oraz przekazują krótkie aktualności podczas spotkań zespołów.
Pozostawienie procesu e-learningu całkowicie bez nadzoru, tak aby przebiegał on w trybie automatycznym, bez wglądu ze strony firmy. Sam link rejestracyjny nie gwarantuje długoterminowej wartości dla organizacji.	Wykorzystanie ustrukturyzowanego systemu monitorowania (np. tabela 3) do śledzenia kamieni milowych oraz przydzielanie wewnętrznych mentorów. Wnioski z oceny projektu pilotażowego (D5.3) potwierdzają, że wyznaczenie konkretnego kierownika lub mentora wyraźnie koreluje z potwierdzonym zakończeniem testów.
Pozwalając na samodzielną naukę w całkowitej izolacji, narażamy się na ryzyko, że poszczególne trudności w nauce lub ukryte problemy techniczne pozostaną niezauważone. Bez interakcji osoby zupełnie początkujące często utkną w martwym punkcie i po cichu rezygnują z programu, gdy napotkają przeszkodę.	Połączenie nauki we własnym tempie z proaktywnymi elementami operacyjnymi, takimi jak krótkie sprawdziany wiedzy czy cyfrowe przypomnienia. Aktywne dostosowanie zarządzania bezpośrednio eliminuje bariery w nauce, zwiększając motywację pracowników i wskaźniki ukończenia kursów.

6. PLAN DZIAŁAŃ DOTYCZĄCY WDROŻENIA PROGRAMU „AGENT ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA

Pomyślne wdrożenie roli agenta zmian w zakresie cyberbezpieczeństwa zaczyna się na długo przed samym mianowaniem. Poświęcenie czasu na ocenę aktualnej sytuacji organizacji, zdobycie wewnętrznego poparcia oraz jasne zdefiniowanie tej roli od samego początku znacznie zwiększa szanse na długoterminowy sukces. Poniższe kroki mają na celu praktyczne przeprowadzenie małych i średnich przedsiębiorstw przez tę fazę przygotowawczą.

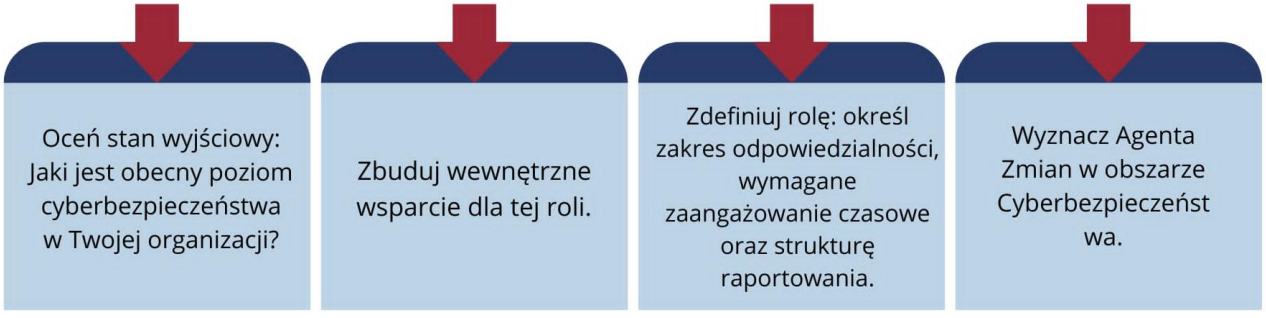
1. Pierwszym krokiem jest ocena aktualnej sytuacji organizacji. Oznacza to rzetelne przeanalizowanie stosowanych obecnie praktyk w zakresie cyberbezpieczeństwa oraz tych, których brakuje. Czy pracownicy są świadomi podstawowych zagrożeń, takich jak phishing? Czy istnieje procedura zgłaszania podejrzanych zdarzeń? Czy w całym zespole dane wrażliwe są przetwarzane w spójny sposób?

2. Drugim krokiem jest zapewnienie wewnętrznego poparcia dla tej funkcji. Agent zmian nie może skutecznie działać bez wsparcia kierownictwa. Przed wyborem kandydata decyzja o wprowadzeniu tej funkcji powinna zostać omówiona i uzgodniona na szczeblu kierowniczym, przy wyraźnym zobowiązaniu do przeznaczenia na nią odpowiedniej ilości czasu, formalnego uznania tej funkcji oraz aktywnego wspierania osoby, która ją obejmie.

3. Trzecim krokiem jest zdefiniowanie stanowiska przed jego obsadzeniem. Oznacza to uzgodnienie zakresu obowiązków, oczekiwanego nakładu czasu oraz tego, jak stanowisko to będzie wpisane w istniejącą strukturę organizacyjną. Jasny zakres obowiązków, nawet w postaci prostego, jednoparagrafowego opisu, pozwala uniknąć niejasności i zapewnia przyszłemu agentowi zmian w dziedzinie cyberbezpieczeństwa legitymację niezbędną do działania.

Dopiero po wdrożeniu tych trzech kroków organizacja jest gotowa do wyłonienia i zatrudnienia odpowiedniego kandydata. W poniższej sekcji przedstawiono listę kontrolną, która pomoże w pomyślnym obsadzeniu tego stanowiska.

Rysunek 1 – Wizualny plan działania dotyczący wdrożenia agenta ds. zmian w zakresie cyberbezpieczeństwa



7. LISTA KONTROLNA

Poniższa lista kontrolna ma na celu sprawdzenie, czy spełnione są kluczowe warunki niezbędne do pomyślnego wdrożenia programu „Cybersecurity Change Agent". Opiera się ona na wnioskach wyciągniętych z projektu pilotażowego „CyberAgent".

7.1. ZARZĄDZANIE

[ ] Rola „agenta zmian" została formalnie zatwierdzona i uwzględniona w budżecie

[ ] Określono jasny zakres zadań: zakres obowiązków, wymagany nakład czasu oraz struktura podległości służbowej

[ ] Informacja o powołaniu na tę funkcję została przekazana całej organizacji

[ ] Na najbliższe 12 miesięcy zaplanowano przegląd tej funkcji

[ ] Osoba pełniąca rolę agenta zmian zarezerwowała w swoim harmonogramie czas na realizację tej funkcji

7.2. ZASOBY LUDZKIE

[ ] W procesie selekcji mogły wziąć udział wszystkie osoby, niezależnie od płci czy pochodzenia

[ ] Rola ta została przedstawiona w kategoriach wpływu na organizację, a nie wiedzy technicznej

[ ] Obowiązki agenta ds. zmian zostały uwzględnione w opisie stanowiska lub celach

[ ] W trakcie wdrażania nowi pracownicy zapoznają się z programem „Cybersecurity Change Agent

[ ] Prowadzone jest rejestr szkoleń i certyfikatów agenta ds. zmian

7.3. AGENT DS. ZMIAN W ZAKRESIE CYBERBEZPIECZEŃSTWA

[ ] Zarejestrowano się na platformie CyberAgent oraz uzgodniono plan nauki

[ ] Ukończono co najmniej jeden moduł i uzyskano certyfikat

[ ] Współpracownicy wiedzą, jak skontaktować się z agentem ds. zmian

[ ]Podstawowe zasady dotyczące cyberbezpieczeństwa są udokumentowane i dostępne dla wszystkich pracowników

[ ] Wprowadzono regularne działania informacyjne (spotkania, komunikaty lub przypomnienia)

[ ] Istnieje jasna procedura, zgodnie z którą pracownicy mogą zgłaszać podejrzane sytuacje

[]Informacje zwrotne dotyczące kwestii związanych z cyberbezpieczeństwem są regularnie gromadzone i przekazywane kierownictwu

8. JAK OCENIĆ, CZY WDROŻENIE BYŁO UDANE

Pełnienie roli agenta zmian w zakresie cyberbezpieczeństwa to nieustanne zobowiązanie. Poniższe wskaźniki mogą pomóc małym i średnim przedsiębiorstwom w ocenie, czy rola ta przynosi rzeczywiste efekty w dłuższej perspektywie czasowej.

[ ] Od czasu powołania agenta zmian w zakresie cyberbezpieczeństwa wzrosła liczba pracowników biorących udział w działaniach podnoszących świadomość w zakresie cyberbezpieczeństwa

[ ] Kwestia cyberbezpieczeństwa jest regularnie poruszana podczas spotkań zespołu i nie jest już traktowana jako temat wyjątkowy

[ ] Pracownicy wiedzą, kim jest osoba pełniąca rolę agenta zmian w zakresie cyberbezpieczeństwa, i nie mają oporów przed zwracaniem się do niej z pytaniami lub wątpliwościami

[ ] Wzrosła liczba zgłoszonych podejrzanych wiadomości e-mail, incydentów lub innych obaw dotyczących bezpieczeństwa

[ ] Od momentu powołania agenta zmian w zakresie cyberbezpieczeństwa ukończono dodatkowe moduły szkoleniowe

[ ] Okresowo gromadzone są opinie pracowników dotyczące cyberbezpieczeństwa w organizacji, a następnie podejmowane są odpowiednie działania

8.1. WYTYCZNE DLA KIEROWNICTWA DOTYCZĄCE DOSTOSOWYWANIA I NARZĄDZANIA SZABLONÓW

Aby zapewnić, że podnoszenie kwalifikacji Państwa „agenta zmian w zakresie cyberbezpieczeństwa" przełoży się na długoterminową odporność przedsiębiorstwa, niezbędne jest ciągłe monitorowanie strukturalne. Tabela 3 zawiera praktyczny szablon monitorowania przeznaczony dla menedżerów z sektora MŚP, służący do oceny wyjściowego poziomu organizacji przed szkoleniem oraz pomiaru konkretnych postępów w zakresie kultury bezpieczeństwa po 6 i 12 miesiącach od powołania.

Kierownicy powinni traktować ten szablon jako dynamiczne ramy. W zależności od wielkości przedsiębiorstwa, sektora działalności i istniejącej infrastruktury, zachęca się do dostosowywania i rozszerzania tej matrycy:

- **Dostosowywanie skal**
  Mikroprzedsiębiorstwa (zatrudniające mniej niż 10 pracowników) mogą uprościć wskaźniki oparte na wartościach procentowych, zastępując je bezpośrednią liczbą pracowników, aby ułatwić monitorowanie sytuacji.

- **Rozwijanie wskaźników**
  Przedsiębiorstwom działającym w środowiskach o wysokim stopniu cyfryzacji lub wysokim ryzyku zaleca się dodanie wierszy dotyczących konkretnych celów, takich jak „odsetek pracowników korzystających z uwierzytelniania wieloskładnikowego (MFA)" lub „średni czas reakcji na symulowane zagrożenie".

- **Lokalizacja**
  Kolumnę „Zalecane źródło danych" należy dostosować do konkretnych wewnętrznych kanałów komunikacji (np. śledzenie za pośrednictwem Slacka, ankiet w MS Teams lub fizycznych dzienników prowadzonych podczas odpraw zespołowych).

Tabela 3. Szablon monitorowania po powołaniu dla menedżerów MŚP

Wskaźnik sukcesu	**Jednostka / skala pomiaru**	**Wartość bazowa (przed wdrożeniem)**	**Postęp (6 miesięcy))**	**Cel (12 miesięcy))**	**Zalecane źródło danych**
Gotowość pracowników na ataki phishingowe	% pracowników pewnych w rozpoznawaniu i obsłudze podejrzanych wiadomości e-mail	%	%	%	Wewnętrzna ankieta lub dane z platformy CyberAgent
Częstotliwość uwzględniania w spotkaniach	Liczba spotkań zespołu, na których poruszono temat cyberbezpieczeństwa	Liczba / ilość	Liczba / ilość	Liczba / ilość	Protokoły lub agendy spotkań zespołu
Częstotliwość aktywnego zgłaszania incydentów	Liczba udokumentowanych zgłoszonych podejrzanych incydentów	Liczba / miesiąc	Liczba / miesiąc	Liczba / miesiąc	Wewnętrzny rejestr incydentów bezpieczeństwa lub pętla informacji zwrotnej IT
Widoczność agenta zmian	% pracowników, którzy poprawnie identyfikują osobę pełniącą rolę agenta zmian w zakresie cyberbezpieczeństwa	%	%	%	Short internal questionnaire

Wskaźnik sukcesu	Jednostka / skala pomiaru	Wartość bazowa (przed wdrożeniem)	Postęp (6 miesięcy))	Cel (12 miesięcy))	Zalecane źródło danych
Zaangażowanie w postęp na platformie	Liczba pracowników aktywnie uczestniczących w mikrolearningu	Liczba / ilość	Liczba / ilość	Liczba / ilość	Panel analityczny platformy CyberAgent dla menedżerów / dashboard analityczny platformy CyberAgent

PODSUMOWANIE

Cyberbezpieczeństwo nie jest już kwestią dotyczącą wyłącznie dużych organizacji posiadających wyspecjalizowane działy IT. W miarę jak sytuacja w zakresie zagrożeń nieustannie się zmienia, a wymagania regulacyjne wobec małych i średnich przedsiębiorstw rosną, pojawia się pytanie, w jaki sposób mogą one się bronić, korzystając z zasobów, którymi faktycznie dysponują.

Rola „agenta zmian w zakresie cyberbezpieczeństwa" stanowi praktyczną i proporcjonalną odpowiedź na to pytanie. Nie wymaga ona zatrudniania specjalisty, inwestowania w drogie narzędzia ani gruntownej przebudowy istniejących procesów. Wymaga ona zidentyfikowania odpowiedniej osoby w organizacji, zapewnienia jej szkolenia i upoważnienia do działania oraz stworzenia warunków, dzięki którym świadomość w zakresie cyberbezpieczeństwa stanie się częścią codziennej pracy.

Projekt „CyberAgent" pokazał, że jest to możliwe. W ośmiu krajach europejskich pracownicy MŚP bez przygotowania technicznego ukończyli szkolenie, objęli tę rolę i zaczęli zmieniać podejście swoich organizacji do cyberbezpieczeństwa. Dowody są jednoznaczne: gdy bariera wejścia zostaje obniżona, gdy rola ta jest osadzona w kulturze organizacyjnej, a nie w wiedzy technicznej, oraz gdy inkluzywność traktowana jest jako zasada projektowa, a nie dodatek, wyniki przychodzą same.

Niniejszy przewodnik stanowi zaproszenie do zrobienia tego pierwszego kroku. Plan działania jest gotowy. Narzędzia są dostępne. Ta rola jest w zasięgu ręki każdego MŚP, które jest gotowe zainwestować w swoich pracowników.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau