CyberAgent

Co-funded by the European Union

Raport mapowania potrzeb szkoleniowych agentów zmian w zakresie cyberbezpieczeństwa w MŚP.

CYBER AGENT 10.2023

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

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Pakiet roboczy 2: Podejście i projekt struktury CyberAgent

Element dostarczany 2.2: Raport mapowania potrzeb szkoleniowych agentów zmian w zakresie cyberbezpieczeństwa w MŚP.

Lider WP2 – Olemisen Balanssia ry
Lider produktu 2.2 – Olemisen Balanssia ry

CONTENT

WSTĘP

Celem niniejszego raportu z projektu jest analiza i mapowanie potrzeb szkoleniowych w celu zidentyfikowania odpowiednich kompetencji wymaganych od agenta zmian w cyberbezpieczeństwie MŚP. Poprzez kompleksowy przegląd aktualnej oferty edukacyjnej i zrozumienie preferencji MŚP w zakresie kwestii cyberbezpieczeństwa, niniejszy raport ma na celu wypełnienie luki pomiędzy obecnymi kompetencjami i zdefiniowanie idealnego wymaganego zestawu umiejętności.

W miarę jak zagrożenia cybernetyczne stają się coraz bardziej wyrafinowane, MŚP muszą koniecznie zapewnić sobie odpowiednio przeszkolony personel do zwalczania tych zagrożeń. W tym kontekście kluczową rolę odgrywają agenci zmiany w obszarze cyberbezpieczeństwa. W tym raporcie z projektu analizowano krajobraz cyberbezpieczeństwa z różnych perspektyw: edukacji i szkoleń, inkluzywność płci oraz obecnego stanu MŚP i instytucji szkolnych.

1. METODOLOGIA

W tym procesie mapowania zastosowaliśmy podejście mieszane, łącząc badania źródłowe i badania terenowe.

W ramach badania źródłowego przeprowadzono kompleksowy przegląd literatury:

- Przegląd istniejących i powstających przepisów edukacyjnych na poziomie kształcenia i szkolenia zawodowego w zakresie cyberbezpieczeństwa w każdym kraju partnerskim. Pozyskiwanie i kompilowanie artykułów, oficjalnych dokumentów, badań i raportów związanych z treściami i potrzebami szkoleń w zakresie cyberbezpieczeństwa.
- Analiza kursów VET i szkolnictwa wyższego, ich programy nauczania i ich znaczenie dla rzeczywistych wyzwań związanych z cyberbezpieczeństwem.

Celem było:

- Identyfikacja aktualnych elementów programu kursów z zakresu cyberbezpieczeństwa oferowanych na poziomach kształcenia i szkolenia zawodowego w każdym kraju.
- Ocena, w jaki sposób te programy nauczania odpowiadają wyzwaniom związanym z cyberbezpieczeństwem.
- Identyfikacja, czy istnieją konkretne strategie lub programy mające na celu zaangażowanie większej liczby kobiet w badania nad cyberbezpieczeństwem.

Na etapie badań terenowych przeprowadziliśmy 2 ankiety. Jedna przeznaczona dla nauczycieli i trenerów z obu kategorii VET i HE z każdego kraju, aby zrozumieć niuanse aktualnych przepisów szkoleniowych. Druga dostosowana do MŚP, aby uzyskać pogląd i zrozumieć sytuację w firmach w zakresie cyberbezpieczeństwa: w jaki sposób pracownicy są zaangażowani i zaangażowani w te tematy, wyzwania i potrzeby. W badaniach terenowych skupiono się również na określeniu cech charakterystycznych, potrzeb szkoleniowych i preferencji edukacyjnych, ze szczególnym uwzględnieniem potrzeb kobiet w zakresie cyberbezpieczeństwa.

W obu ankietach uzyskaliśmy znaczną liczbę odpowiedzi. 190 nauczycieli i trenerów z VET i uczelni oraz 176 z pracowników MŚP.

Ankieta 1: Mapowanie potrzeb szkoleniowych dla agentów zmian w cyberbezpieczeństwie MŚP – **badanie VET i HEI.**

Typ instytucji	**Odpowiedzi**	**Kobieta**	**Mężczyzna**	**Wolę nie mówić**
HEI (Instytucje szkolnictwa wyższego)	104	28	73	3
VET (kształcenie i szkolenie zawodowe)	86	36	48	2
Całkowity	**190**	**64**	**121**	**5**

Ankieta 2: Mapowanie potrzeb szkoleniowych MŚP agentów zmian w cyberbezpieczeństwie – **badanie MŚP.**

Liczba odpowiedzi	**Liczba**
MŚP	176
Całkowita	**176**

Kwestionariusze i pełne dane można znaleźć w Załączniku C i D.

2. BADANIA (WSZYSCY PARTNERZY)

2.1. AKTUALNE PRZEPISY DOTYCZĄCE EDUKACJI I SZKOLEŃ

W tej części przedstawiono badania i wnioski wynikające z badań źródeł informacji i ankiet, podkreślając mocne strony i luki w obecnej infrastrukturze edukacyjnej i szkoleniowej w krajach partnerskich.

2.1.1. PRZEGLĄD EDUKACJI W ZAKRESIE CYBERBEZPIECZEŃSTWA W RAMACH KSZTAŁCENIA I SZKOLENIA ZAWODOWEGO I SZKOLNICTWA WYŻSZEGO

Przeprowadziliśmy szeroką analizę krajobrazu edukacji w zakresie cyberbezpieczeństwa we wszystkich krajach partnerskich, aby opisać jego obecny stan i uruchomić odpowiednie aspekty edukacji i szkoleń w zakresie cyberbezpieczeństwa.

Na Litwie przeszukanie [1]bazy danych AIKOS ujawniło łącznie sześć formalnych programów edukacji w zakresie cyberbezpieczeństwa oferowanych przez litewskie instytucje, obejmujących zarówno studia licencjackie, jak i magisterskie:

Kierunek studiów	Program	Instytucja	ECTS	Stopień
Inżynieria informatyczna	Bezpieczeństwo informacji i technologii informatycznych[2]	Politechnika w Kownie	120	Magister informatyki
Zarządzanie	Zarządzanie cyberbezpieczeństwem[3]	Uniwersytet Mykolasa Romerisa	90	Magister zarządzania przedsiębiorstwem
Inżynieria informatyczna	Bezpieczeństwo informacji i technologii informatycznych[4]	Wileński Uniwersytet Techniczny Giedymina	120	Magister informatyki
Inżynieria informatyczna	Systemy informacyjne i cyberbezpieczeństwo[5]	Uniwersytet Wileński	210	Licencjat z informatyki
Inżynieria informatyczna	Technologie Systemów Informatycznych i Cyberbezpieczeństwo[6]	Kolegium Mariampola	180	Profesjonalny licencjat z informatyki
Inżynieria informatyczna	Cybersystemy i bezpieczeństwo[7]	Kolegium w Kownie	180	Profesjonalny licencjat z informatyki

[1]**Słowa kluczowe używane w wyszukiwaniu programów to *cyber, bezpieczeństwo* i ich odmiany. Źródło:** https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

Programy cyberbezpieczeństwa na poziomie magisterskim charakteryzują się odrębnymi, ale uzupełniającymi się podejściami. Uniwersytet w Kownie kładzie nacisk na metodologię badań, metody bezpieczeństwa informacji i prawne aspekty przestrzeni elektronicznej, koncentrując się na rozwoju umiejętności projektowania i wdrażania bezpiecznych systemów informatycznych. Wileński Uniwersytet Techniczny Giedymina stawia na kształcenie specjalistów o systematycznym podejściu do zagadnień bezpieczeństwa informacji, łącząc wiedzę naukową z metodami i technologiami zapewniającymi bezpieczeństwo informacji, a także wspierając krytyczne myślenie i przywództwo. Uniwersytet Mykolasa Romerisa jednak wyraźnie skłania się w stronę zarządzania cyberbezpieczeństwem, którego celem jest kształcenie specjalistów biegłych w nadzorowaniu nowoczesnych środowisk IT i złożonych zadań związanych z cyberbezpieczeństwem, ze szczególnym naciskiem na zarządzanie strategiczne w dynamicznych kontekstach technologicznych.

Programy studiów licencjackich w zakresie cyberbezpieczeństwa kładą główny nacisk na rozwój wykwalifikowanych specjalistów w dziedzinie informatyki i cyberbezpieczeństwa, ale każdy z nich kładzie inny nacisk. Program Uniwersytetu Wileńskiego jest zorientowany na zapewnienie kompleksowych podstaw inżynierii informatycznej, koncentrując się na analizie, projektowaniu, rozwoju i utrzymaniu bezpiecznych systemów informatycznych. Mariampole College, mając także na celu kształcenie kompetentnych specjalistów w dziedzinie informatyki, kładzie większy nacisk na aspekty praktyczne, takie jak tworzenie, utrzymywanie i administrowanie sieciami i systemami komputerowymi. Kaunas College wyróżnia się dążeniem do przygotowania specjalistów posiadających umiejętności nie tylko w zakresie projektowania i wdrażania systemów cybernetycznych, ale także kierowania zespołami, rozumienia implikacji etycznych, prawnych i społecznych oraz skutecznej pracy w środowiskach wielokulturowych. Chociaż celem wszystkich trzech instytucji jest wyposażenie studentów w umiejętności techniczne w zakresie cyberbezpieczeństwa, ich cele różnią się od biegłości technicznej (Uniwersytet Wileński), praktycznego zastosowania i rozwoju umiejętności miękkich (Kolegium Mariampolskie) po połączenie względów technicznych, przywództwa i etycznych (Kolegium w Kownie).

Badanie ujawniło również cztery zarejestrowane programy pozaformalnej edukacji dorosłych w zakresie cyberbezpieczeństwa, każdy skupiający się na umiejętnościach niezbędnych do rozpoznawania, badania i zapobiegania cyberatakom, w szczególności z wykorzystaniem kryptografii. Chociaż wszystkie programy mają ten sam główny cel, różnią się one podejściami i zakresami. Niektóre koncentrują się na cyberbezpieczeństwie i strategiach zapobiegawczych, podczas gdy inne oferują szerszy program nauczania, obejmujący programowanie, obejmujący takie obszary, jak inżynieria społeczna, zarządzanie tożsamością i zarządzanie ryzykiem. Warto zauważyć, że kilka programów rozpoczyna się od podstawowego programowania i przechodzi do zaawansowanych tematów cyberbezpieczeństwa, odpowiednich dla początkujących. Jeden z wyróżniających się programów, realizowany we współpracy z Cybint, przeznaczony jest dla osób z ograniczoną wiedzą informatyczną, oferując praktyczne umiejętności praktyczne zarówno w pełnym, jak i niepełnym wymiarze godzin. Programy te mają na celu łącznie rozwój

różnorodnych kompetencji w zakresie cyberbezpieczeństwa, począwszy od programowania podstawowego po dogłębną naukę skoncentrowaną na aplikacjach.

Na programy edukacyjne związane z cyberbezpieczeństwem miało wpływ kilka polityk mających na celu wzmocnienie bezpieczeństwa narodowego i obronności Finlandii. Rośnie liczba inicjatyw badawczo-rozwojowych, programów edukacyjnych i szkoleniowych oraz certyfikowanych specjalistów w dziedzinie cyberbezpieczeństwa. Fińska strategia bezpieczeństwa cybernetycznego (2019) (**https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/**) i Program rozwoju cyberbezpieczeństwa (2021) podkreślają znaczenie budowania krajowych kompetencji w zakresie bezpieczeństwa cybernetycznego poprzez edukację i badania. Dla systemu edukacji szkolnej celem jest wyposażenie uczniów w umiejętności i wiedzę umożliwiające bezpieczne poruszanie się w cyfrowym świecie oraz świadomość zagrożeń cybernetycznych i środków ochrony **Lehto-IWS-018.pdf (jyu.fi)**

W fińskim kształceniu i szkoleniu zawodowym (VET) w większości materiałów cyberbezpieczeństwo nie jest wyraźnie podkreślone jako odrębny lub wyspecjalizowany obszar. Nie musi to jednak oznaczać, że cyberbezpieczeństwo jest całkowicie nieobecne w programach kształcenia i szkolenia zawodowego. Biorąc pod uwagę rosnące znaczenie umiejętności cyfrowych i cyberbezpieczeństwa we wszystkich sektorach, tematy te zostały włączone do szerszych programów edukacji informatycznej i technicznej. Należy zauważyć, że organizatorzy kształcenia i szkolenia zawodowego w Finlandii mają swobodę organizowania swojej oferty edukacyjnej zgodnie z wymogami regionalnymi i branżowymi. Fińskie kształcenie i szkolenie zawodowe przeszło niedawno najszerszą reformę od prawie 20 lat. Celem reformy z 2018 r. było stworzenie bardziej wydajnego i elastycznego, opartego na kompetencjach i zorientowanego na klienta systemu kształcenia i szkolenia zawodowego, poprawa jego efektywności oraz lepsze dopasowanie kwalifikacji do potrzeb rynku pracy. Odbywa się to głównie poprzez ograniczenie przepisów i wprowadzenie większej autonomii i odpowiedzialności organizatorów kształcenia i szkolenia zawodowego. (Źródło: **https://www.cedefop.europa.eu/files/8133_en.pdf)** Oznacza to, że niektóre instytucje mogą oferować bardziej wyspecjalizowane moduły w obszarach takich jak cyberbezpieczeństwo, w zależności od wymagań lokalnego przemysłu i partnerstw . Jak wynika z badań Lehto, cyberbezpieczeństwo nie jest oddzielnym tematem, ale zintegrowanym z różnymi tematami, szczególnie w kontekście technologii informacyjno-komunikacyjnych (ICT). Obowiązek nauczania spoczywa na nauczycielach, którzy powinni włączyć edukację w zakresie cyberbezpieczeństwa do swoich przedmiotów. Podejście to prowadzi do różnic w sposobie jego wdrażania w różnych szkołach i klasach oraz podkreśla potrzebę bardziej uporządkowanego i spójnego podejścia do nauczania o cyberbezpieczeństwie, w tym potencjalnego uczynienia go odrębnym przedmiotem lub bardziej widoczną częścią edukacji w zakresie ICT.

Na poziomie szkolnictwa wyższego fińskie uniwersytety oferują kompleksowe programy studiów w zakresie bezpieczeństwa cybernetycznego. Programy te mają na celu wyposażenie studentów w zaawansowaną wiedzę i umiejętności z różnych obszarów cyberbezpieczeństwa. Wiele z nich oferuje tytuł magistra w zakresie bezpieczeństwa informacji i technologii

informatycznych, koncentrując się na implikacjach i zastosowaniach tych koncepcji w świecie rzeczywistym. Są one dostępne na miejscu i zdalnie.

Sektor cyberbezpieczeństwa w Belgii odnotowuje zwiększone zapotrzebowanie na wykwalifikowanych specjalistów – około 4000 wolnych stanowisk w dziedzinie cyberbezpieczeństwa (stan na listopad 2022 r.). Uznając pilność i potrzebę wypełnienia tej luki, wprowadzono różne inicjatywy i programy edukacyjne mające na celu rozwój krajowej wiedzy specjalistycznej w zakresie cyberbezpieczeństwa. Liczne instytucje w Belgii, takie jak KU Leuven, Solvay Business School, Howest University of Applied Sciences i wiele innych opracowały specjalistyczne programy w języku angielskim, francuskim i holenderskim, które są w stanie dotrzeć do szerokiego grona odbiorców. Jednak badania przeprowadzone przez belgijską organizację Agoria podkreśliły potrzebę ustawicznego szkolenia także wśród specjalistów, którzy nie studiują już na uniwersytecie, aby być na bieżąco z dziedziną cyberbezpieczeństwa i związanymi z nią zagrożeniami. Belgijska strategia cyberbezpieczeństwa na lata 2021–2025 uznaje wysoki poziom integracji cyberbezpieczeństwa w środowisku akademickim kraju i podkreśla kluczową rolę, jaką odgrywają uniwersytety i inne instytucje edukacyjne we wzmacnianiu wysiłków badawczo-rozwojowych w tej dziedzinie. Według bazy danych CBB (Centrum Cyberbezpieczeństwa Belgii), w Belgii istnieją 33 kierunki (licencjackie, magisterskie i certyfikujące) oferowane przez instytucje szkolnictwa wyższego, co stanowi całą gamę programów VET oferowanych zarówno w sektorze publicznym, jak i prywatnym . CBB to organ nadzorujący, koordynujący i monitorujący wdrażanie belgijskiej strategii bezpieczeństwa cybernetycznego, a obecnie opracowujący bezpłatne szkolenie pracowników w zakresie świadomości cyberbezpieczeństwa dla belgijskich pracowników, aby jeszcze bardziej rozpowszechnić wiedzę na temat cyberbezpieczeństwa wśród społeczeństwa. Ogólnie rzecz biorąc, belgijska strategia cyberbezpieczeństwa podkreśla znaczenie szerzenia wiedzy i umiejętności w zakresie cyberbezpieczeństwa poprzez edukację i zobowiązuje się do poszerzania kursów akademickich, promowania badań w tej dziedzinie, zachęcania do edukacji w zakresie przedmiotów STEM i zapewniania możliwości szkolenia praktycznego, aby sprostać rosnącemu zapotrzebowaniu na specjalistów w belgijskiej branży cyberbezpieczeństwa.

W Norwegii cyberbezpieczeństwo nie jest głównym przedmiotem, którego można uczyć się na poziomie kształcenia i szkolenia zawodowego. Elementy programu zawarte są w programie kształcenia i szkolenia zawodowego o nazwie „Komputer i Elektronika". Nie ma ram Ministerstwa Edukacji dotyczących cyberbezpieczeństwa, w ogólnych podstawowych umiejętnościach alfabetyzacji cyfrowej dla wszystkich placówek edukacyjnych wspomniano jedynie, że uczniowie powinni umieć korzystać z zasobów cyfrowych i poruszać się po nich w sieciach i poza nimi oraz zapewniać bezpieczeństwo informacji i danych.

W Narodowej Strategii Kompetencji w zakresie Cyberbezpieczeństwa wskazano 14 listopada 2023 r., jak ważne jest, aby uczniowie szkół kształcenia i szkolenia zawodowego zdobywali wiedzę na temat cyberbezpieczeństwa. Dla wielu przedmiotów zawodowych jest to bardzo istotne i ważne. Na kursach zawodowych brakuje materiałów edukacyjnych dotyczących cyberbezpieczeństwa, a nauczycielom brakuje umiejętności nauczania, szczególnie w

obszarach takich jak prywatność, technologia inteligentnego domu i IoT. Istniejące programy edukacji w zakresie cyberbezpieczeństwa, takie jak GenCyber i CyberFirst, nie odpowiadają konkretnie potrzebom tego programu zawodowego. (**źródło 1 – 2**)

Planuje się, że dzięki współpracy między UiO, NTNU i nauczycielami w wybranych szkołach kształcenia i szkolenia zawodowego zostaną opracowane materiały dydaktyczne dotyczące cyberbezpieczeństwa, które później zostaną udostępnione na krajowej platformie edukacyjnej **NDLA (National Digital Learning Arena)** .

W ramach szkolnictwa wyższego można znaleźć zarówno roczny program w zakresie kultury bezpieczeństwa cyfrowego, jak i programy licencjackie w zakresie bezpieczeństwa cybernetycznego. Przedmiot jest również uwzględniony w wielu programach magisterskich z zakresu nauk o danych i informatyki. Istnieje wiele szczegółowych studiów nad bezpieczeństwem cybernetycznym, takich jak informatyka stosowana i technologie informacyjne, licencjat z bezpieczeństwa cybernetycznego, licencjat z kryminalistyki cyfrowej, infrastruktura cyfrowa i cyberbezpieczeństwo, kultura bezpieczeństwa cyfrowego i magisterium oparte na doświadczeniu w zakresie bezpieczeństwa informacji. Istnieją również badania, w których bezpieczeństwo cybernetyczne jest uwzględnione jako kultura HSE i wiodące miejskie spółdzielnie zajmujące się gotowością na wypadek sytuacji kryzysowych oraz praca zarządów w praktyce, a także roczne badanie dotyczące zarządzania kryzysowego.

W Polsce w ostatnich latach wzrosła liczba studiów cyberbezpieczeństwa. Na uniwersytetach otwiera się coraz więcej kursów cybernetycznych, a jednocześnie rośnie liczba kursów kształcenia i szkolenia zawodowego.
W ostatnich latach w Polsce wzrosło zapotrzebowanie na zawody cybernetyczne, wzrosła także świadomość cyberbezpieczeństwa w polskiej delegacji , która promuje firmy, aby zatrudniały ekspertów ds. cyberbezpieczeństwa i chroniły informacje.
W Polsce, podobnie jak w większości krajów europejskich, stopień naukowy jest uważany za obowiązkowy, dlatego kursy cyber są często dodatkowym kierunkiem studiów po uzyskaniu stopnia naukowego. Ponieważ większość studiów Akshmi jest dłuższa, ale teoretyczna. Istnieją kursy cybernetyczne, które są krótkie, ale większość z nich koncentruje się na praktycznej nauce, która przygotowuje do prawdziwej pracy.
Dużym wyzwaniem dla studenta kierunku cybernetycznego jest to, że większość instytucji kształcenia i szkolenia zawodowego nie posiada własnego finansowania, dlatego wymagane jest rozwiązanie finansowe dla uczestników i dlatego ta opcja nie zawsze jest odpowiednia dla zainteresowanych.

Nawet jeśli cyberbezpieczeństwo powinno być priorytetem we wszystkich obszarach działalności, system kształcenia i szkolenia zawodowego w Rumunii nie jest jeszcze gotowy, aby zapewnić uczniom kompetencje w tej dziedzinie. Analizując Program nauczania dla niższego cyklu liceum – kierunek technologiczny – w żadnym obszarze kształcenia zawodowego, w programie nauczania kultury technicznej nie przewidziano jednostek efektów kształcenia w zakresie cyberbezpieczeństwa. Niektóre szczegółowe kompetencje w tym zakresie można

znaleźć w programie nauczania wiedzy ogólnej, w dyscyplinie Technologie informacyjne i komunikacyjne, w programie nauczania w klasie IX. To są:

1. Opis i zastosowanie środków bezpieczeństwa w korzystaniu z Internetu:

- Inteligentne korzystanie z Internetu
- Znaczenie szyfrowania transmisji danych
- Stosowanie podpisu cyfrowego
- Sposoby obrony przed wirusami

2. Korzystanie z usługi czatu:

- Prezentacja aplikacji współpracujących do wideokonferencji
- Prezentacja zasad sieci IRC

Dla wyższego cyklu szkoły średniej, klasa 11 - jedynie kierunek kształcenia zawodowego Automatyka Elektroniczna dla specjalizacji Technik Telekomunikacji, Technik Operator Komputerowy, Technik Operator Telematyki, oferuje treści dotyczące instalowania aplikacji zabezpieczających. W klasie 12, wyłącznie na specjalizacji Technik Informatyk, moduł specjalizacyjny obejmuje treści takie jak:

- Podstawowe zasady bezpieczeństwa systemów komputerowych i sieci komputerowych
- Opracowywanie polityk bezpieczeństwa w sieci
- Zagrożenia bezpieczeństwa sieci
- Ochrona przeglądania Internetu
- Wirusy i aplikacje zabezpieczające

Jeśli chodzi o uczelnie, Uniwersytet Transylwanii w Braszowie wykazuje duże zaangażowanie w edukację w zakresie cyberbezpieczeństwa, oferując kompleksowy program magisterski z zakresu cyberbezpieczeństwa prowadzony w całości w języku angielskim. Zaangażowanie uniwersytetu w rozwijanie wiedzy specjalistycznej w tej krytycznej dziedzinie jest widoczne w obszernym programie nauczania przewidzianym w programie.

Ten program magisterski na Uniwersytecie Transilvania to doskonała okazja dla studentów poszukujących wszechstronnej edukacji w zakresie cyberbezpieczeństwa w międzynarodowym środowisku akademickim. Połączenie solidnego programu nauczania i instrukcji w języku angielskim zapewnia absolwentom sukces w dynamicznej i wymagającej dziedzinie cyberbezpieczeństwa.

Uniwersytet Babes-Bolyai w Kluż-Napoce, za pośrednictwem Wydziału Matematyki i Informatyki, zainicjował od roku akademickiego 2023-2024 studia magisterskie w języku angielskim w zakresie Cyberbezpieczeństwa, mające na celu przygotowanie przyszłych specjalistów w tej dziedzinie o istotnym znaczeniu w kontekście przejścia do społeczeństwa informacyjnego. Zajęcia na nowym kierunku rozpoczynają się w październiku tego roku wraz z

rokiem akademickim 2023-2024, którego przyjęcie przekracza oczekiwania. Ponad 40 studentów, w tym z zagranicy, przyjętych do programu zostanie specjalistami w dziedzinie Cyberbezpieczeństwa, przyjęci kandydaci mogą nawet zdecydować się na studia przez rok akademicki na innych renomowanych uczelniach w Europie.

Na Wydziale Matematyki i Informatyki studia magisterskie *Technologie Internetowe* (w języku angielskim) oferują również w drugim semestrze pierwszego roku kurs *Kryptografii i Bezpieczeństwa Systemów* , który wprowadza studentów w dziedzinę Cyberbezpieczeństwa oraz specyficzne metody szyfrowania danych.

Ponadto program magisterski Nowoczesne technologie w inżynierii systemów oprogramowania oferuje w pierwszym semestrze drugiego roku fakultatywny kurs zatytułowany Bezpieczeństwo systemów informatycznych, skupiony wokół głównych wyzwań cyberbezpieczeństwa.

Obydwa kierunki pozwalają studentom studiów magisterskich na Wydziale Matematyki i Informatyki zdobyć wiedzę i ekspertyzę w tej dziedzinie, która w aktualnym kontekście międzynarodowym ma istotne znaczenie, a także uświadomić sobie wyzwania, jakie niesie ze sobą szyfrowanie i bezpieczeństwo współczesnych systemów.

Uniwersytet w Bukareszcie, Wydział Matematyki i Informatyki, oferuje studia magisterskie dotyczące bezpieczeństwa i logiki stosowanej (w języku angielskim), które oferują serię kursów poświęconych kryptografii i bezpieczeństwu systemów. Studenci mogą zdobywać wiedzę z zakresu bezpieczeństwa systemów operacyjnych, kryptografii, bezpieczeństwa sieci i cyberbezpieczeństwa, przygotowując się tym samym do stawienia czoła wyzwaniom tej dziedziny.

W Hiszpanii większość studiów w zakresie cyberbezpieczeństwa odbywa się na poziomie szkolnictwa wyższego, uzyskując stopnie naukowe lub tytuł magistra. Według danych odzyskanych przez Hiszpański Narodowy Instytut Cyberbezpieczeństwa istnieją:

- Około 87 stopni magisterskich z zakresu cyberbezpieczeństwa oferowanych przez publiczne i prywatne uniwersytety oraz inne instytucje szkolnictwa wyższego.
- 4 specjalizacje, głównie specjalizacje z informatyki śledczej.
- 3 stopnie naukowe, wszystkie oferowane przez sektor prywatny.

Jeśli chodzi o szkolenie na poziomie VET, w hiszpańskich instytutach szkolenia zawodowego dostępnych jest około 60 kursów. Wszystkie są regulowane tym samym programem nauczania, zatwierdzonym przez Ministerstwo Edukacji w maju 2020 r. *Dekretem Królewskim nr 479/2020 z dnia 7 kwietnia, który ustanawia specjalizację z zakresu cyberbezpieczeństwa w środowiskach technologii informatycznych* .

Pomimo istniejących programów uznano potrzebę dalszych wysiłków. Hiszpania wdrożyła różne plany, w tym Krajowy Plan Umiejętności Cyfrowych, Plan Cyfryzacji MŚP na lata 2021–2025 i Hiszpania Plan Cyfryzacja 2025, skupiając się przede wszystkim na tworzeniu nowych talentów, aby sprostać rosnącemu zapotrzebowaniu na umiejętności cyfrowe, szczególnie w zakresie cyberbezpieczeństwa.

W Turcji zapotrzebowanie na cyberbezpieczeństwo gwałtownie wzrosło i stało się bardzo ważne w naszym kraju, a także na całym świecie, szczególnie w ostatnich latach. Równolegle z rozwojem technologii zagrożenia i zagrożenia cybernetyczne zmieniają się w tym samym tempie i stają się złożone. Ryzyka i zagrożenia cybernetyczne osiągnęły potencjał powodowania znacznie bardziej kompleksowych i negatywnych konsekwencji niż ataki fizyczne. W sektorach takich jak finanse, komunikacja elektroniczna, energetyka, transport i lotnictwo świadczenie usług w bezpiecznym środowisku cyfrowym, zapewnienie krajowego bezpieczeństwa cybernetycznego stało się jednym z najważniejszych priorytetów naszego kraju. W tym kontekście badania w dalszym ciągu rozpowszechniają szkolenia z zakresu cyberbezpieczeństwa w szkoleniu zawodowym i szkolnictwie wyższym zgodnie z potrzebami sektora oraz rozwijają i wzbogacają treści szkoleniowe.

W ramach tych studiów , w kształceniu zawodowym: Kurs Podstawy cyberbezpieczeństwa w działaniu sieci w zakresie technologii informatycznych. Z zakresu cyberbezpieczeństwa, podstaw programowania, bezpieczeństwa systemów, technologii sieciowych, tworzenia bezpiecznego oprogramowania, testów penetracyjnych i reagowania na incydenty cybernetyczne, informatyki śledczej itp. Osiągnięcia z przedmiotu są przyznawane studentom.

W szkolnictwie wyższym program studiów stowarzyszonych „Analityk i operator bezpieczeństwa cybernetycznego” w szkołach zawodowych zajmujących się bezpieczeństwem cybernetycznym, studia licencjackie z zakresu inżynierii komputerowej kryminalistycznej na uniwersytetach oraz odpowiednie programy magisterskie są oferowane na uniwersytetach.

Ponadto ośrodki kształcenia ustawicznego na uniwersytetach, publiczne centra edukacji w gminach, instytucje oficjalne, takie jak TÜBİTAK, TSE i prywatne instytucje edukacyjne również zapewniają szkolenia z zakresu cyberbezpieczeństwa.

2.1.2. WYZWANIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM I POTRZEBY BRANŻY

Na podstawie dokładnego przeglądu literatury wymieniliśmy wyzwania związane z cyberbezpieczeństwem, przed którymi stoją MŚP w krajach projektu. W zmieniającym się krajobrazie cyberbezpieczeństwa małe i średnie przedsiębiorstwa (MŚP) na Litwie stoją przed wieloma wyzwaniami w zakresie cyberbezpieczeństwa. Ponieważ przedsiębiorstwa te w coraz większym stopniu opierają swoją działalność na technologiach cyfrowych, stają się bardziej podatne na spektrum zagrożeń cybernetycznych, co wymaga wszechstronnego zrozumienia i strategicznego podejścia, aby skutecznie zarządzać tymi ryzykami.

W badaniu z 2022 r. Bukauskas i in. [8]wyróżniono typy organizacji ze względu na ich dojrzałość w zakresie cyberbezpieczeństwa i potrzeby kompetencyjne. Z badania wynika, że małe organizacje są porównywalne z pojedynczymi osobami w społeczeństwie, ponieważ głównym parametrem bezpieczeństwa cyfrowej przestrzeni pracy jest poziom higieny cyberbezpieczeństwa, na który wpływa ogólne zrozumienie zagrożeń cyberbezpieczeństwa. Na tym poziomie cyberbezpieczeństwo jest koordynowane wewnętrznie w organizacji, co prowadzi do potencjalnych naruszeń bezpieczeństwa w procesach biznesowych. W średnich przedsiębiorstwach zarządzanie i regulacja cyberbezpieczeństwa są również słabo skoordynowane. W organizacji nie kładzie się nacisku na reagowanie na incydenty lub inne działania związane z cyberbezpieczeństwem. Mając na uwadze, że małe przedsiębiorstwa na Litwie stanowią 97% wszystkich firm, Bukauskas i in. (2022) stwierdzili, że istnieje duże zapotrzebowanie na specjalistów IT, którzy świadczą usługi IT, konsultują się z użytkownikami, a których zadaniem jest zapewnienie podstawowych zasad cyberbezpieczeństwa. Podkreślili także, że obserwuje się zauważalny brak informacji o zagrożeniach i badaniach naukowych oraz widoczne zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa w zakresie inżynierii bezpieczeństwa i cyklu życia systemów.

Kilka lat wcześniej w ramach programu „Twórz dla Litwy" we współpracy z Ministerstwem Obrony Narodowej zorganizowano konsultacje społeczne na temat podnoszenia świadomości cyberbezpieczeństwa wśród małych i średnich przedsiębiorstw [9]. Inicjatywa doszła również do wniosku, że oczywiste jest, że poziom świadomości cyberbezpieczeństwa wśród MŚP na Litwie nie jest wysoki i że małe przedsiębiorstwa nie osiągnęły odpowiedniego poziomu odporności cybernetycznej ze względu na brak zrozumienia zagrożeń cyfrowych. Co więcej, w ramach inicjatywy zauważono, że ponad połowa (57%) liderów firm stwierdziła, że brakuje im wiedzy lub nie jest pewna, czy posiada wystarczającą wiedzę, aby wybrać rozwiązania w zakresie cyberbezpieczeństwa, a ponad trzy czwarte pracowników zgodziło się, że brakuje im łatwo zrozumiałych informacji.

Porównując wyniki Bukauskas i in. (2022) i wcześniejszą inicjatywę „Twórz dla Litwy" (2019) oczywiste jest, że sytuacja w zakresie cyberbezpieczeństwa wśród MŚP na Litwie wykazała ograniczony postęp. Obydwa badania podkreślają utrzymujący się niedobór podstawowej wiedzy i gotowości w zakresie cyberbezpieczeństwa w tych przedsiębiorstwach. Pomimo zwiększonej zależności od technologii cyfrowych MŚP w dalszym ciągu wykazują słabe punkty wynikające z niewystarczającej odporności cybernetycznej i ogólnego braku zrozumienia zagrożeń cyfrowych. To ciągłe wyzwanie uwydatnia pilną potrzebę poprawy świadomości i szkoleń w zakresie cyberbezpieczeństwa wśród MŚP – sektora krytycznego stanowiącego większość litewskiego krajobrazu biznesowego.

[8]Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. „Projekto „Kibernetinio saugumo kompetencijų žemėlapio kūrimas" ataskaita", Vilniaus universitetas Informatikos institutas. Dostępne pod adresem: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [dostęp: 12 stycznia 2024 r.]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

[9]Obrony Narodowej , 2019. SVV Kibernetinio Saugumo Apklausos Apžvalga . [online] Dostępne pod adresem: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

W Finlandii badanie przeprowadzone przez ETLA (Elinkeinoelämän tutkimuslaitos), fiński Instytut Badań Ekonomicznych wykazało, że liczba naruszeń danych w fińskich firmach, w tym MŚP, podwoiła się w ciągu dwóch lat. Fińskie firmy zgłosiły w 2019 r. trzy razy więcej naruszeń danych niż średnia europejska, przy czym większość incydentów dotyczyła oszustw, ataków phishingowych, naruszeń danych, złośliwego oprogramowania i luk w zabezpieczeniach. W badaniu tym podkreślono również, że głównym wyzwaniem dla fińskich MŚP jest niedobór wykwalifikowanych specjalistów ds. cyberbezpieczeństwa. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

Narodowe Centrum Cyberbezpieczeństwa w Finlandii (NCSC-FI) (**https://www.kyberturvallisuuskeskus.fi/en**) to inicjatywa kierowana przez rząd fiński. Działa w ramach Fińskiej Agencji Transportu i Komunikacji (Traficom), która jest agencją rządową odpowiedzialną za regulację sektora komunikacji i transportu w Finlandii. Dostarczają informacji na temat bieżącego stanu bezpieczeństwa cybernetycznego oraz oferują wskazówki i narzędzia zarówno dla osób fizycznych, jak i organizacji, umożliwiające ulepszenie praktyk w zakresie bezpieczeństwa cybernetycznego. Centrum angażuje się także w krajowe inicjatywy w zakresie bezpieczeństwa cybernetycznego, takie jak alerty o podatnościach na zagrożenia, a także promuje świadomość i gotowość na wypadek zagrożeń cybernetycznych.

Ich cotygodniowe przeglądy zapewniają dobry wgląd w wyzwania stojące przed MŚP. Dowiadujemy się, że fińskie MŚP, podobnie jak wiele innych, borykają się z tymi samymi problemami bezpieczeństwa, które zostały opisane przez instytut ETLA w związku z wieloma wiadomościami phishingowymi i oszustwami. Należą do nich próby podszywania się pod legalne usługi, takie jak Suomi.fi, w celu wyłudzenia danych uwierzytelniających lub innych poufnych informacji. Zasoby finansowe MŚP mogą stanowić ograniczenie we wdrażaniu nowoczesnych rozwiązań w zakresie cyberbezpieczeństwa w celu ochrony przed zagrożeniami cybernetycznymi. Z kolei już wyposażone MŚP mają trudności z byciem na bieżąco z pojawiającymi się zagrożeniami dla cyberbezpieczeństwa.

Starając się zrozumieć sytuację w zakresie cyberbezpieczeństwa, z jaką borykają się MŚP w Belgii, przeprowadziliśmy dokładne badanie. Uzyskanie kompleksowych danych lub źródeł dotyczących tego krytycznego problemu okazało się jednak trudne. Ten brak informacji utrudnia tworzenie skutecznych strategii i rozwiązań, które mogą pomóc MŚP chronić ich zasoby cyfrowe przed zagrożeniami cybernetycznymi.

Udało nam się dotrzeć do profesjonalistów aktywnie zaangażowanych w obszar cyberbezpieczeństwa w Belgii, dzięki rozbudowanej sieci Fundacji Women4Cyber. Eksperci ci dostarczyli nam ważnych spostrzeżeń i perspektyw, które pomogły nam zrozumieć różne wyzwania stojące przed MŚP w zakresie cyberbezpieczeństwa. Otrzymaliśmy uwagi od Ivy Tashevy, wybitnej członkini Women4Cyber Belgium, która podzieliła się swoim rozległym doświadczeniem i wiedzą na temat wyzwań stojących przed MŚP, próbując chronić swoją infrastrukturę cyfrową przed zagrożeniami cybernetycznymi.

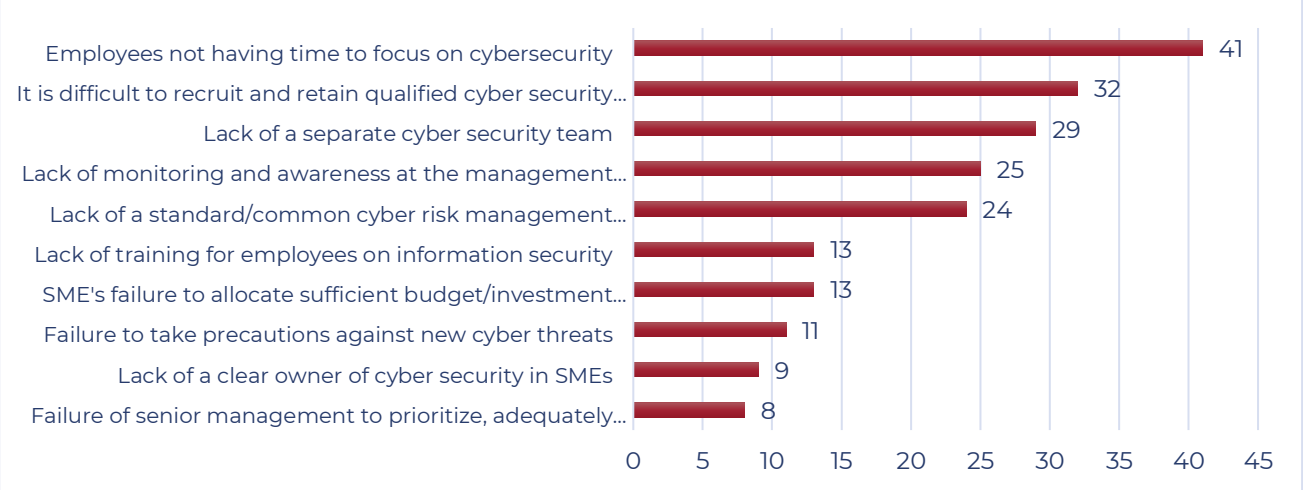
Przedsiębiorstwa stoją przed kilkoma wyzwaniami związanymi z cyberbezpieczeństwem, takimi jak trudności w dostępie do doraźnego wsparcia, brak szkoleń w zakresie zarządzania tożsamością i dostępem dla ich personelu oraz ograniczone zrozumienie ról i obowiązków w usługach w chmurze. Ponadto MŚP mają ograniczony dostęp do niedrogich rozwiązań do skanowania podatności i narzędzi monitorowania, co czyni je bardziej podatnymi na zagrożenia cybernetyczne. Wszechobecna hiperłączność w środowiskach biznesowych naraża MŚP na kradzież tożsamości i oszukańcze działania, podczas gdy phishing i oszustwa stwarzają ciągłe ryzyko. Aby sprostać tym wyzwaniom, MŚP muszą podjąć proaktywne działania, wdrożyć solidne protokoły bezpieczeństwa i zapewnić wszechstronną edukację pracowników, aby wzmocnić ich umiejętności i chronić przed potencjalnymi naruszeniami i stratami finansowymi.

Cyberbezpieczeństwo stało się jednym z głównych priorytetów przedsiębiorstw w Hiszpanii, w tym małych i średnich przedsiębiorstw (MŚP). Wzrost liczby telepracy i zajęć online doprowadził do powszechnego stosowania funkcji zdalnego pulpitu, przetwarzania w chmurze i narzędzi współpracy, między innymi zwiększając ryzyko i ataki komputerowe. Raport Narodowego Centrum Kryptologicznego (CCN-CERT) łączy wzrost telepracy i wykorzystania technologii ze wzrostem tych zagrożeń. Najczęstsze ataki, na jakie padają ataki na firmy, to ransomware i ataki na systemy zdalnego dostępu. Wzrost zagrożeń cybernetycznych doprowadził firmy do zwiększenia liczby osób przypisanych do zespołów ds. cyberbezpieczeństwa, zarówno wewnętrznie, jak i zewnętrznie. Jednak pomimo tego firmy nadal zlecają około 50% tych funkcji na zewnątrz.

Ponadto w Hiszpanii nadal 21% firm nie posiada centrów operacyjnych ds. bezpieczeństwa (SOC), które zajmowałyby się incydentami. W zakresie edukacji o cyberbezpieczeństwie w środowisku biznesowym z analizy Deloitte wynika, że w 2022 roku liczba godzin szkoleń online z zakresu cyberbezpieczeństwa dla pracowników analizowanych organizacji wzrosła o prawie 30% w porównaniu do danych za 2021 rok. Jednak prawie 50% firm w Hiszpanii nie posiada żadnych certyfikatów z zakresu cyberbezpieczeństwa, co jest wyraźnym wyzwaniem na przyszłość.

Niemniej jednak największym wyzwaniem, przed jakim stoją hiszpańskie firmy, nadal pozostaje brak talentów w zakresie cyberbezpieczeństwa. Jak wynika z raportu „Analiza i diagnoza talentów cyberbezpieczeństwa w Hiszpanii" przygotowanego przez ObservaCiber, w 2021 roku w Hiszpanii lukę talentów szacowano na 24.119. Szacuje się, że w 2024 r. Hiszpania będzie potrzebować ponad 83 000 ekspertów, co zwiększy lukę w talentach do 57,5%.

Wydaje się, że najsłabszym ogniwem, które sprawia, że MŚP stają przed wyzwaniami związanymi z cyberbezpieczeństwem, jest czynnik „ludzki" . Największym wyzwaniem dla MŚP jest to, że pracownicy odpowiedzialni za cyberbezpieczeństwo nie mogą przeznaczyć wystarczającej ilości czasu na dziedzinę cyberbezpieczeństwa, ponieważ mają obowiązki w więcej niż jednym obszarze. W związku z tym brak odrębnego zespołu ds. cyberbezpieczeństwa plasuje się na trzecim miejscu na liście trudności, jakie napotykają MŚP w zarządzaniu cyberbezpieczeństwem. MŚP mają problemy z rekrutacją i utrzymaniem wykwalifikowanych pracowników zajmujących się cyberbezpieczeństwem.



Rysunek 1– Wyzwania MŚP – badanie Türkiye.

W Rumunii środowisko internetowe stwarza możliwości biznesowe i powiązania, które mogą pomóc w rozwoju MŚP, ale niesie ze sobą także wiele zagrożeń.

Cyberbezpieczeństwo to już nie bajka, to rzeczywistość także w Rumunii, nawet jeśli do tej pory nie mieliśmy większego cyberataku.

Źródłem wykorzystanych informacji jest RAPORT VERIZON o zagrożeniach cybernetycznych w 2023 roku – główne kluczowe punkty dla MŚP (DATA BREACH INVESTIGATIONS RAPORT – DBIR), oparty na 16 312 incydentach bezpieczeństwa, z czego 5 199 zostało potwierdzonych jako naruszenia bezpieczeństwa danych.

Punkty zainteresowania dla MŚP:

- Powierzchnie ataku dla MŚP i korporacji są podobne, ponieważ korzystają z oprogramowania opartego na chmurze. Nieuprawniona penetracja systemu, techniki socjotechniki i podstawowe ataki na aplikacje internetowe stanowią 92% wszystkich typów ataków z powodu włamań odnotowanych przez MŚP (85% w przypadku korporacji).
- ransomware 24% przypadków (dane są kradzione przed zaszyfrowaniem)
- nieuprawniona penetracja systemu - złożone ataki oparte na złośliwym oprogramowaniu i/lub hakowaniu w celu osiągnięcia swoich celów.

- Osoby atakujące zewnętrznie stanowią największe zagrożenie, powodując 83% obecnych naruszeń bezpieczeństwa, osiągając 94% w przypadku ataków na MŚP. 94% podmiotów zaangażowanych w rozprzestrzenianie się zagrożeń ma charakter zewnętrzny w porównaniu z 89% w przypadku dużych organizacji, a 98% naruszeń ma podłoże finansowe w porównaniu z 97% w przypadku korporacji.
- Motywacja finansowa jest na pierwszym miejscu w 95% wszystkich przypadków, a w przypadku ataków na MŚP odsetek ten wzrasta do 98%. Tylko 1% ma motywację szpiegostwa.
- Pracownicy stanowią słabe ogniwo w łańcuchu bezpieczeństwa – 74% wszystkich przypadków (słaba świadomość zagrożeń cybernetycznych). Główną metodą włamania może być wykorzystanie skradzionych danych uwierzytelniających – 49% i phishing – 12% lub innych metod, takich jak błędna konfiguracja lub omyłkowe przesłanie wrażliwych danych.
- Naruszenie służbowych wiadomości e-mail — ofiara zostaje oszukana i przelewa duże sumy pieniędzy na konta atakujących.

W Norwegii małe i średnie przedsiębiorstwa (MŚP) stoją przed poważnymi wyzwaniami w zakresie cyberbezpieczeństwa. Wielu osobom brakuje głębokiego zrozumienia związanych z nimi zagrożeń, co prowadzi do potencjalnych luk w zabezpieczeniach. Zauważalna jest luka w skutecznym szkoleniu pracowników w zakresie cyberbezpieczeństwa, co sprawia, że błąd ludzki jest częstym czynnikiem ryzyka. MŚP, zwłaszcza te zgłaszające ograniczone zasoby, często mają trudności z inwestowaniem w zaawansowane środki cyberbezpieczeństwa i wykwalifikowany personel. Muszą także poruszać się po skomplikowanych przepisach dotyczących ochrony danych, co zwiększa złożoność zapewniania zgodności przy jednoczesnej ochronie wrażliwych informacji. Wzrost liczby ataków phishingowych i socjotechniki dodatkowo ukazuje ich podatność, podobnie jak niewystarczające bezpieczeństwo sieci i ryzyko zagrożeń wewnętrznych. Zarządzanie tym ryzykiem ma kluczowe znaczenie, jednak dla MŚP często skuteczna ocena ryzyka i zarządzanie nim stanowi wyzwanie. Ponadto poleganie na zewnętrznych dostawcach wprowadza kolejną warstwę złożoności, potencjalnie narażając MŚP na dodatkowe zagrożenia cyberbezpieczeństwa.

2.2. KOBIETY W CYBERBEZPIECZEŃSTWIE

Przeanalizowaliśmy potrzeby kobiet w zakresie szkoleń i wsparcia, istniejące kwalifikacje i kompetencje kobiet w zakresie cyberbezpieczeństwa oraz zalecenia dotyczące angażowania większej liczby pracownic w wyzwania związane z cyberbezpieczeństwem.

Firma Microsoft przeprowadziła ankietę, w której w 35 krajach Europy stwierdzono, że mniej niż 1 na 5 absolwentów informatyki to kobiety. Zainteresowanie naukami ścisłymi, technologią, inżynierią i matematyką (przedmioty STEM) spada zdecydowanie zbyt wcześnie. W rzeczywistości Program OECD dotyczący międzynarodowej oceny uczniów (PISA) pokazuje, że chłopcy znacznie częściej niż dziewczęta wyobrażają sobie siebie jako specjalistów, naukowców lub inżynierów w dziedzinie ICT. (Microsoft, 2017).

Patrząc na udział kobiet wśród zatrudnionych specjalistów ICT, w UE27 w 2020 r. jedynie 18,5% wszystkich specjalistów ICT stanowiły kobiety. Największy udział kobiet odnotowano w Bułgarii – 28,2%, Grecji – 26,6% i Rumunii – 26,2% (patrz wykres 5 (Kobiety wybierają technologie, 2021)). Kraje z regionu nordycko-bałtyckiego również w większości znalazły się w czołówce zestawienia, z wyjątkiem Norwegii, która znalazła się bardziej w środku rankingu. (Kobiety wybierają technologie, 2021).

Według Departamentu Statystyki Republiki Litewskiej w czwartym kwartale 2022 roku w kategorii informacja i komunikacja zatrudnionych było 29,4 tys. mężczyzn i 21,5 tys. kobiet. W I kwartale 2023 r. było to 34,6 tys. mężczyzn i 20,7 tys. kobiet. W drugim kwartale 2023 r. było to 36,8 tys. mężczyzn i 14,8 tys. kobiet, a w trzecim kwartale 2023 r. było to 34,5 tys. mężczyzn i 18,0 tys. kobiet. Od I do II kwartału 2023 r. zauważalny jest spadek liczby zatrudnionych kobiet, a następnie wzrost w III kwartale 2023 r. (Rodiklių Duomenų Bazė – Oficialiosios Statistikos Portalas, bd).

Do 11% kobiet pracuje w obszarze bezpieczeństwa cybernetycznego, przeprowadzono ankietę, aby poznać opinię publiczną na temat punktu widzenia kobiet w tej dziedzinie. W odpowiedziach 44,4% respondentów wskazało, że liczba kobiet zajmujących się cyberbezpieczeństwem powinna mieścić się w przedziale od 30 do 60%. Największa część respondentów odpowiedziała, że kobiety powinny stanowić od 30 do 60% kobiet pracujących zawodowo (35,2%). Analizując odpowiedzi w podziale na płeć i grupę wiekową można zauważyć, że kobiety, szczególnie te młodsze (poniżej 25. roku życia oraz 25-45 lat), najczęściej uważają, że liczba kobiet powinna wynosić około połowy. Młodzi mężczyźni (poniżej 25. roku życia) uważają, że aż 30% kobiet powinny stanowić kobiety. Można zauważyć, że same kobiety dostrzegają znacznie większą liczbę kobiet w obszarze Cyberbezpieczeństwa niż ma to obecnie miejsce na rynku. To dobra wiadomość, ponieważ przyciągnięcie kobiet do pracy w tym obszarze nie tylko pomogłoby zaradzić niedoborom specjalistów, ale także zwiększyłoby bezpieczeństwo samych organizacji. (Bukauskas i in., 2022).

W Finlandii, podobnie jak w wielu krajach europejskich, panuje powszechne zrozumienie co do braku równowagi płci w cyberbezpieczeństwie i ogólnie w dziedzinie IT. Wzrosła liczba inicjatyw i wysiłków mających na celu wspieranie kobiet w dziedzinie cyberbezpieczeństwa i promowanie ich zaangażowania w rozwiązywanie problemów związanych z cyberbezpieczeństwem. Większość z nich jest wspierana przez organizacje non-profit.

W dziedzinie cyberbezpieczeństwa podjęto szereg inicjatyw mających na celu opracowanie ścieżek edukacyjnych i zawodowych, programów szkoleniowych i wydarzeń służących tworzeniu sieci kontaktów. Strategia opiera się również na promowaniu wzorców do naśladowania poprzez podkreślanie ścieżek kariery kobiet odnoszących sukcesy w cyberbezpieczeństwie i dzielenie się ich historiami, aby zainspirować więcej kobiet do kontynuowania kariery w tej dziedzinie. Women4Cyber i wymienione inicjatywy podkreślają znaczenie różnorodności i włączenia społecznego, aby nie tylko zaradzić brakowi równowagi płci, ale także przyczynić się do ogólnej siły i odporności sektora cyberbezpieczeństwa. Instytucje publiczne i prywatne również wspierają tę strategię, włączając wymiar równości płci jako najwyższy priorytet do wszystkich swoich inicjatyw.

Women4Cyber Finlandia (W4CFI)

Założona w sierpniu 2021 roku W4CFI jest organizacją non-profit, której celem jest zwiększenie liczby kobiet zatrudnionych w fińskiej branży cyberbezpieczeństwa. Jest częścią większej, ogólnounijnej inicjatywy Women4Cyber i koncentruje się na wspieraniu bardziej zróżnicowanego i włączającego przemysłu w Finlandii. W4CFI angażuje się w różne działania, w tym zapewnianie wskazówek, wymianę wiedzy i podnoszenie świadomości w celu zwiększania i wspierania zaangażowania kobiet w cyberbezpieczeństwo **Women4Cyber Finlandia.**

Fińskie Ministerstwo Transportu i Komunikacji oraz projekt Uniwersytetu Aalto

Fińskie Ministerstwo Transportu i Komunikacji we współpracy z Uniwersytetem Aalto opracowuje pakiet edukacyjny, dzięki któremu cyberbezpieczeństwo stanie się umiejętnością obywatelską w całej Unii Europejskiej. Inicjatywa ta podkreśla rosnące znaczenie cyberbezpieczeństwa w życiu codziennym oraz potrzebę świadomości i umiejętności wśród wszystkich obywateli, w tym kobiet. Podkreśla rolę instytucji edukacyjnych w zapewnianiu dostępnej edukacji i szkoleń w zakresie cyberbezpieczeństwa, co ma kluczowe znaczenie dla wzmacniania pozycji kobiet w tej dziedzinie. Finlandia wspiera edukację w zakresie umiejętności w zakresie cyberbezpieczeństwa w UE. **Platforma umiejętności cyfrowych i zatrudnienia** (europa.eu).

Ruch „Mimmit koodaa" (Kodeks kobiet).

Inicjatywa ta oferuje warsztaty, szkolenia, możliwości nawiązywania kontaktów, seminaria internetowe i wsparcie zawodowe. Koncentruje się na przełamywaniu stereotypów i zachęcaniu większej liczby kobiet do odkrywania kariery w technologiach, w tym w cyberbezpieczeństwie. Celem tej organizacji jest stworzenie kobietom możliwości wejścia i osiągnięcia doskonałości w dziedzinie cyberbezpieczeństwa. **Mimit koodaa**

Jak wynika z pierwszego badania społeczno-ekonomicznego dotyczącego sektora cyberbezpieczeństwa w Belgii opublikowanego przez Agorię w 2022 r., w belgijskim krajobrazie cyberbezpieczeństwa kobiety stanowią 19% siły roboczej. Przy koordynacji belgijskiego Ministerstwa Gospodarki (FPS Belgium) kompetentni gracze polityczni z Belgii opracowali pięcioletni plan na rzecz kobiet w branży cyfrowej zatytułowany „Kobiety w branży cyfrowej – strategia krajowa i międzysektorowa na lata 2021–2026". Plan pięcioletni obejmuje wspólną, międzysektorową strategię opartą na pięciu celach strategicznych przydatnych w zwalczaniu uprzedzeń i przeszkodach strukturalnych uniemożliwiających kobietom udział w gospodarce cyfrowej. Pięć celów jest następujących:

1. Zapewnienie większej liczbie kobiet kończących studia w sektorze cyfrowym; 2. Stymulowanie wszystkich kobiet do udziału w cyfrowym rynku pracy i/lub w sektorze cyfrowym; 3. Poprawa zatrzymywania kobiet w sektorze cyfrowym; 4. Tworzenie nowych obrazów promujących rolę kobiet w terenie (na ekranie i poza nim); 5. Likwidacja zróżnicowania płci w poszczególnych grupach docelowych (**link do Strategii**).

Fundacja Women4Cyber z siedzibą w Brukseli organizuje i wspiera szeroki zakres działań skierowanych do kobiet pracujących lub rozpoczynających karierę w cyberbezpieczeństwie w Belgii i Europie. W Belgii Fundacja wspiera i współpracuje z Belgijskim Oddziałem Krajowym (**Women4Cyber Belgium**) w tych działaniach. Belgijska Kapituła Krajowa liczy około 20 aktywnych członków pracujących nad inicjatywami. Działania, wydarzenia i programy organizowane przez Oddział to na przykład: spotkania i wydarzenia networkingowe (wirtualne i osobiste), takie jak „wirtualna kawa", na którą Oddział W4C Belgia zaprasza do rozmowy ekspertów z różnych dziedzin związanych z bezpieczeństwem cybernetycznym i informacyjnym; seminaria internetowe i sesje informacyjne; programy mentorskie mające na celu pomoc kobietom w doskonaleniu umiejętności i rozwoju kariery w dziedzinie cyberbezpieczeństwa na wszystkich poziomach; projekty i wydarzenia we współpracy z Belgijską Koalicją Cyberbezpieczeństwa (np. organizacja **Międzynarodowego Dnia Kobiet 2023**); promocja stypendiów na programy edukacyjne związane z cyberprzestrzenią, np. organizowane przez Solvay Bruksela School of Economics & Management.

W Norwegii zajęcie się różnicą między płciami w cyberbezpieczeństwie ma kluczowe znaczenie dla budowania odpornej i zróżnicowanej siły roboczej. Odsetek kobiet w IT wynosi zaledwie 29%. Niska liczba jest w dużym stopniu powiązana z liczbą kobiet wybierających przedmioty matematyczne i techniczne w szkołach średnich.

Potrzeby w zakresie szkoleń i wsparcia oraz zalecenia dotyczące angażowania kobiet

Istnieje zapotrzebowanie na dostosowane programy cyberbezpieczeństwa, zaprojektowane specjalnie w celu zachęcania kobiet do udziału. Programy te powinny równoważyć aspekty techniczne z kwestiami cyberbezpieczeństwa organizacyjnymi i skupionymi na człowieku. W tej dziedzinie dostępnych jest kilka kierunków dalszego kształcenia technicznego, podczas gdy oferty dalszego kształcenia w większości typowych zawodów kobiecych (zawody pedagogiczno – zdrowotne) nie mają takich ofert, a opracowanie krótszych ofert szkoleń z zakresu

cyberbezpieczeństwa związanych z tymi zawodami mogłoby dotrzeć do większej liczby kobiet. Potwierdza to również sam sektor, który stwierdził, że różnorodność może zapewnić unikalne perspektywy w obliczu wyzwań związanych z cyberbezpieczeństwem. Zwiększanie świadomości kobiet na temat wewnętrznych karier związanych z cyberbezpieczeństwem mogłoby nastąpić poprzez warsztaty, seminaria i ukierunkowane programy informacyjne w szkołach i na uniwersytetach, które mogą zainspirować więcej kobiet do podjęcia pracy w tej dziedzinie.

Inne podejście sugerowane przez wiele z nominowanych 50 najlepszych norweskich kobiet-technologów 2022 polega na ustanowieniu programów mentorskich i możliwości nawiązywania kontaktów dla kobiet zajmujących się cyberbezpieczeństwem, aby zapewnić im niezbędne wskazówki i wsparcie, pomagając im poruszać się i rozwijać w tej dziedzinie.

Sam sektor cyberbezpieczeństwa sugeruje, że organizacje powinny wdrożyć inkluzywne praktyki i zasady zatrudniania, które aktywnie zachęcają do rekrutacji i zatrzymywania kobiet na stanowiskach związanych z cyberbezpieczeństwem. Według raportu McKinsey „Kobiety w miejscu pracy 2022" 32% kobiet na stanowiskach technicznych jest często „jedyną kobietą w pomieszczeniu" **.**

Wreszcie, promowanie kobiet na stanowiska kierownicze w dziedzinie cyberbezpieczeństwa może zapewnić wzorce do naśladowania i zainspirować inne kobiety do podążania podobnymi ścieżkami, jak na przykład **Mia Landsem** .

W Rumunii cyberbezpieczeństwo pozostaje jednym z najbardziej dynamicznych i ekscytujących sektorów technologii. Sektor ten potrzebuje jednak systemowej zmiany w reprezentacji i wynagradzaniu kobiet. Pomimo zwiększonego zainteresowania dziedziną cyberbezpieczeństwa, dysproporcje między płciami utrzymują się. Kobiety są nadal zdecydowanie niedostatecznie reprezentowane, choć większość stanowisk pracy zajmują głównie mężczyźni. Na przyszłość cyberbezpieczeństwa wpływa zdolność do przyciągania, zatrzymywania i promowania większej liczby specjalistów ds. cyberbezpieczeństwa, w tym większej liczby kobiet.

Przeprowadzono wiele badań, aby pokazać, jak niedoceniane są kobiety na całym świecie, ale także aby wszyscy zrozumieli znaczenie kobiet we wszystkich dziedzinach, a szczególnie w cyberbezpieczeństwie. Skrajne różnice między płciami wśród pracowników zajmujących się cyberbezpieczeństwem wskazują, że inne siły robocze wcale nie są równe. Kobiety stanowią 39% ogółu siły roboczej. Według Cybersecurity Ventures stanowią oni 38% pracowników na stanowiskach STEM, ale tylko około 25% pracowników zajmujących się cyberbezpieczeństwem.

Istnieją różne bariery, które uniemożliwiają kobietom dostęp do cyberbezpieczeństwa. Według badania przeprowadzonego przez (ISC)2, organizację non-profit skupiającą się na szkoleniach i certyfikacji w zakresie cyberbezpieczeństwa, większość kobiet, które pracowały w terenie, zgłasza dyskryminację ze względu na płeć. Prawie wszystkie kobiety (87%) zgłosiły, że doświadczyły nieświadomej dyskryminacji, a 19% stwierdziło, że padły ofiarą jawnej

dyskryminacji. Kobiety wskazywały także na niewyjaśnione opóźnienia w awansie zawodowym (53%) i przesadne reakcje na błędy (29%).

Dyskryminacja objawia się także luką w wynagrodzeniu. Badania (ISC)2 pokazują, że 32% mężczyzn pracujących w cyberbezpieczeństwie zarabia średnio od 50 000 do 100 000 dolarów rocznie, podczas gdy zaledwie 18% kobiet zajmujących się cyberbezpieczeństwem osiąga ten sam przedział dochodów. 25% mężczyzn w porównaniu z 20% kobiet zarabia od 100 000 do 500 000 dolarów rocznie.

Istnieją mocne argumenty przemawiające za zwiększeniem liczby kobiet zajmujących się cyberbezpieczeństwem, takie jak korzyści płynące z różnorodności, innowacyjności, empatii emocjonalnej i bezstronnej perspektywy, a wszystkie te umiejętności są cennymi umiejętnościami w miejscu pracy zajmującym się cyberbezpieczeństwem.

Członek zarządu Women in Cybersecurity, Jay Koehler, przedstawił kolejne spostrzeżenie: „Kobiety rezygnują, ponieważ jest to „klub dla chłopców" i panuje tam niskie poczucie przynależności. Problem ten można rozwiązać poprzez zaangażowanie i odpowiedzialność za zapewnienie bezpieczeństwa psychicznego i miejsca pracy przyjaznego płci, a także poprzez tworzenie sieci kobiet.

Istnieje nadzieja, że cyberbezpieczeństwo nie będzie już „zawodem zdominowanym przez mężczyzn", ale będzie pełnym utalentowanych ludzi każdej płci i pochodzenia.

Literatura na temat udziału kobiet w cyberbezpieczeństwie w Hiszpanii jest uboga. Większość istniejącej literatury wskazuje na wyraźną nierównowagę płci w szerszej społeczności naukowej, w tym w dyscyplinach STEM, przy zauważalnym spadku możliwości awansu kobiet na wyższe szczeble kariery, co jest powszechnie uważane za „zjawisko rurociągu". Jeśli chodzi o wykształcenie wyższe, różnice między płciami są nadal wyraźne – jedynie 18% osób kończących studia na tych kierunkach to kobiety. Liczba kobiet zatrudnionych w MŚP na stanowiskach związanych z I+D jest nadal bardzo niska i według danych GUS nie sięga nawet 30%. Jeśli chodzi o kobiety-badacze zajmujące się cyberbezpieczeństwem w uczelniach w Hiszpanii, bardzo niewiele z tych Uczelni charakteryzuje się zrównoważoną kadrą pod względem płci. Spośród 31 uczelni zweryfikowanych przez *Fundación Alternativas* w 11 z nich w zespołach badawczych nie uczestniczą kobiety, a tylko 5 z nich charakteryzuje się bardziej egalitarną kadrą. W odpowiedzi na te wyzwania analiza potrzeb szkoleniowych i wsparcia identyfikuje kluczowe obszary wymagające poprawy. Należy opracować inicjatywy zachęcające większą liczbę kobiet do podejmowania studiów doktoranckich i zapewniające zrównoważoną reprezentację w całej ścieżce edukacyjnej. Eliminowanie uprzedzeń w procesach awansu zawodowego ma kluczowe znaczenie, a programy mentorskie mogą odegrać kluczową rolę w prowadzeniu kobiet przez zawiłości dziedziny cyberbezpieczeństwa. Ponadto zaleca się współpracę z organizacjami z branży prywatnej w celu zbadania ścieżek kariery i stymulowania zaangażowania kobiet w role związane z cyberbezpieczeństwem w sektorach prywatnych. Ocena kwalifikacji i kompetencji podkreśla znaczenie zindywidualizowanych programów szkoleniowych, kładących nacisk na konkretne umiejętności i kompetencje w zakresie cyberbezpieczeństwa.

2.3. ANALIZA ZAWODÓW ESCO

Interpretujemy istniejącą klasyfikację ESCO (Europejska wielojęzyczna klasyfikacja umiejętności, kompetencji i zawodów) pod kątem zidentyfikowanych efektów uczenia się, w tym wiedzy, umiejętności i kompetencji. Celem jest:

- Analiza istniejących zawodów ESCO związanych z cyberbezpieczeństwem.
- Przyporządkowanie efektów uczenia się do zawodów ESCO pod względem wiedzy, umiejętności, kompetencji itp.

Dla każdego zawodu istnieje zestaw kompetencji, umiejętności i wiedzy. Poniżej znajdują się definicje i przykłady kompetencji, umiejętności, wiedzy i wartości.

Kompetencje odnoszą się do zdolności jednostki do skutecznego wykonywania określonego zadania lub pracy. Obejmuje połączenie wiedzy, umiejętności i zachowań stosowanych w celu poprawy wydajności. Przykład: Kompetencje w zarządzaniu projektami obejmują połączenie umiejętności organizacyjnych, znajomości procesów zarządzania projektami i umiejętności skutecznej komunikacji z członkami zespołu.

Umiejętności to określone zdolności lub możliwości nabyte w drodze praktyki, szkolenia lub doświadczenia, które umożliwiają jednostce wykonywanie zadań. Przykład: umiejętności testów penetracyjnych, umiejętność korzystania z narzędzi i oprogramowania zapewniającego cyberbezpieczeństwo, umiejętności programowania oraz zdolność do analizowania zagrożeń i reagowania na nie w czasie rzeczywistym.

Wiedza odnosi się do faktów, informacji i zrozumienia zdobytych poprzez edukację lub doświadczenie. Obejmuje teoretyczne zrozumienie faktów i zasad związanych z określoną dziedziną. Przykład: Zrozumienie sposobu przeprowadzania różnych rodzajów cyberataków (np. phishing, ransomware, ataki DDoS) lub znajomość różnych metod szyfrowania oraz znajomość najnowszych trendów i zmian w cyberbezpieczeństwie.

Analiza ta jest podzielona na 2 fazy:

Faza 1: Przegląd i wybór zawodów w ESCO

Konsultacje na portalu ESCO w celu filtrowania zawodów związanych z cyberbezpieczeństwem i dokumentowania w kolejnej sekcji każdego zawodu, zwracając szczególną uwagę na wymienione umiejętności, kompetencje, wiedzę.

Tytuł zawodowy ESCO	Wiedza	Umiejętności	Kompetencje
3512.3 - Technik bezpieczeństwa teleinformatycznego	• Sieci teleinformatyczne • wektory ataku sprzętowego • środki przeciwdziałania cyberatakom • zakup systemów	• krytycznie podchodzić do problemów • analizować system teleinformatyczny • zapewnić	• zintegrować komponenty systemu • dostarczyć dokumentację techniczną • rozwiązywać problemy

	operacyjnych dla ICT • sprzęt sieciowy • Aplikacja internetowa • zagrożenia bezpieczeństwa	prawidłowe zarządzanie dokumentacją • przeprowadzić testy oprogramowania, zidentyfikować słabe punkty systemów teleinformatycznych	systemów teleinformatycznych • korzystać z oprogramowania do kontroli dostępu
2529.1 – dyrektor ds. bezpieczeństwa teleinformatycznego – obejmuje osoby pełniące funkcje związane z bezpieczeństwem korporacyjnym.	• Zagrożenia bezpieczeństwa sieci teleinformatycznych • ustawodawstwo dotyczące bezpieczeństwa ICT • Standardy bezpieczeństwa teleinformatycznego • wektory ataku • techniki audytu • środki przeciwdziałania cyberatakom • bezpieczeństwo cybernetyczne • Ochrona danych • Systemy Wspomagania Decyzji • poufność informacji • strategia bezpieczeństwa informacji • wewnętrzna polityka zarządzania ryzykiem • odporność organizacyjna	• edukować na temat poufności danych • zapewnić przestrzeganie organizacyjnych standardów ICT • zapewnić zgodność z wymogami prawnymi • zapewnić współpracę międzyresortową • zapewnić prywatność informacji • identyfikować zagrożenia bezpieczeństwa ICT • wdrożyć zarządzanie ryzykiem ICT • wdrażać polityki bezpieczeństwa ICT • wdrożyć ład korporacyjny	• prowadzić ćwiczenia w zakresie odzyskiwania po awarii • utrzymać plan ciągłości działania • zarządzać zgodnością z bezpieczeństwem IT • zarządzać planami odzyskiwania po awarii • monitorować rozwój sytuacji w danej dziedzinie wiedzy specjalistycznej • monitorować trendy technologiczne korzystać z systemu wspomagania decyzji
2529.2 – ekspert z zakresu kryminalistyki cyfrowej – pobiera i analizuje informacje z komputerów i innych typów urządzeń do przechowywania danych; bada media cyfrowe, które mogły zostać ukryte, zaszyfrowane lub uszkodzone, w sposób kryminalistyczny w celu zidentyfikowania, zachowania, odzyskania, przeanalizowania i przedstawienia faktów i opinii na temat informacji cyfrowych.	• Zagrożenia bezpieczeństwa sieci teleinformatycznych • Standardy bezpieczeństwa teleinformatycznego • informatyka śledcza • środki przeciwdziałania cyberatakom • poufność informacji	• zastosować inżynierię odwrotną • opracować strategię bezpieczeństwa informacji • edukować na temat poufności danych	• zarządzać zgodnością z bezpieczeństwem IT • zarządzać danymi w celach prawnych • przeprowadzać kryminalistyczną konserwację urządzeń cyfrowych

	• narzędzie do testów penetracyjnych • języki zapytań • Język zapytań struktury opisu zasobów	• zbierać dane do celów kryminalistycznych • identyfikować zagrożenia bezpieczeństwa ICT • zidentyfikować słabe strony systemu ICT • wdrożyć narzędzia diagnostyki sieci teleinformatycznej • udzielać porad w zakresie doradztwa ICT • zabezpieczać wrażliwe dane klientów • używać programowania skryptowego • używać oprogramowania do przechowywania danych • przeprowadzić testy bezpieczeństwa teleinformatyczne go	
2529.3 - inżynier bezpieczeństwa systemów wbudowanych - inżynierowie bezpieczeństwa systemów wbudowanych skupiają się na połączonych produktach i obsługujących je sieciach, a mniej na bezpieczeństwie organizacji, jak w przypadku inżyniera bezpieczeństwa ICT.	• Zagrożenia bezpieczeństwa sieci teleinformatycznych • Standardy bezpieczeństwa teleinformatycznego • Internet przedmiotów • programowanie komputerowe • środki przeciwdziałania cyberatakom • systemy wbudowane • strategia bezpieczeństwa informacji • anomalie oprogramowania	• analizować system teleinformatyczny • Tworzyć diagram schematu blokowego • zdefiniować zasady bezpieczeństwa • opracować sterownik urządzenia ICT • opracować prototyp oprogramowania • wykonać testy oprogramowania • identyfikować zagrożenia bezpieczeństwa ICT	• być na bieżąco z najnowszymi rozwiązaniami systemów informatycznych • zarządzać zgodnością z bezpieczeństwem IT • monitorować wydajność systemu • przeprowadzić analizę ryzyka • raportować wyniki testów, korzystać ze wzorców projektowania oprogramowania • korzystać z bibliotek oprogramowania • korzystać z narzędzi

		• zidentyfikować słabe strony systemu ICT • interpretować teksty techniczne • udzielać porad w zakresie doradztwa ICT • przeprowadzić testy bezpieczeństwa teleinformatyczne go • dostarczyć dokumentację techniczną	inżynierii oprogramowania wspomaganego komputerowo • określić wymagania techniczne
2529.4 – haker etyczny – przeprowadza ocenę podatności na zagrożenia i testy penetracyjne zgodnie z metodami i protokołami przyjętymi w branży; analizuje systemy pod kątem potencjalnych luk, które mogą wynikać z nieprawidłowej konfiguracji systemu, wad sprzętu lub oprogramowania lub słabości operacyjnych.	• wektory ataku • informatyka śledcza • środki przeciwdziałania cyberatakom • etyka • wymagania prawne produktów ICT • narzędzie do testów penetracyjnych • anomalie oprogramowania • narzędzia do automatyzacji testów ICT • zagrożenia bezpieczeństwa aplikacji internetowych	• przeprowadzić testy bezpieczeństwa teleinformatyczne go • dostarczyć dokumentację techniczną • opracowywać exploity w kodzie • przeprowadzać audyty teleinformatyczne • wykonać testy oprogramowania • identyfikować zagrożenia bezpieczeństwa ICT • zidentyfikować słabe strony systemu ICT	• krytycznie podchodzić do problemów • analizować kontekst organizacji • monitorować wydajność systemu
2529.5 - Menedżer odporności ICT - bada, planuje i rozwija modele, zasady, metody, techniki i narzędzia, które zwiększają bezpieczeństwo cybernetyczne organizacji, jej odporność i odzyskiwanie po awarii	• Techniki odzyskiwania ICT • wewnętrzne bezpieczeństwo cybernetyczne • politykę zarządzania ryzykiem • odporność organizacyjna • najlepsze praktyki tworzenia kopii zapasowych systemu	• opracować plany awaryjne na wypadek sytuacji awaryjnych • opracować strategię bezpieczeństwa informacji • przeprowadzać audyty ICT • identyfikować zagrożenia bezpieczeństwa	• analizować procesy biznesowe • analizować kontekst organizacji • przestrzegać przepisów prawnych • prowadzić ćwiczenia w zakresie odzyskiwania po awarii • zarządzać zgodnością z bezpieczeństwem IT • zarządzać planami

		ICT • wdrożyć system odzyskiwania ICT • wdrożyć zarządzanie ryzykiem ICT	odzyskiwania po awarii • zarządzać bezpieczeństwem systemu • przeprowadzić testy bezpieczeństwa teleinformatycznego
2529.6 - Administrator bezpieczeństwa teleinformatycznego - planuje i realizuje środki bezpieczeństwa mające na celu ochronę informacji i danych przed nieuprawnionym dostępem, umyślnym atakiem, kradzieżą i korupcją.	• Zagrożenia bezpieczeństwa sieci teleinformatycznych • Internet przedmiotów • środki przeciwdziałania cyberatakom • narzędzia do tworzenia baz danych • zarządzanie Internetem • zarządzanie urządzeniami mobilnymi • system operacyjny • odporność organizacyjna • metodyki zapewniania jakości • najlepsze praktyki tworzenia kopii zapasowych systemu	• zidentyfikować słabe strony systemu ICT • interpretować teksty techniczne • utrzymać zarządzanie tożsamością ICT • utrzymać bezpieczeństwo bazy danych	• stosować politykę firmy • dbać o jakość systemów teleinformatycznych • zapewnić prawidłowe zarządzanie dokumentacją • zarządzać architekturą danych ICT • zarządzać zgodnością z bezpieczeństwem IT • rozwiązywać problemy związane z ICT • rozwiązywać problemy systemów teleinformatycznych
2529.7 - Inżynier bezpieczeństwa teleinformatycznego - doradza i wdraża rozwiązania kontroli dostępu do danych i programów oraz zapewnia ochronę misji organizacji i procesów biznesowych.	• ustawodawstwo dotyczące bezpieczeństwa ICT • Standardy bezpieczeństwa teleinformatycznego • wektory ataku • analiza biznesowa • środki przeciwdziałania cyberatakom • bezpieczeństwo cybernetyczne • nowe technologie • architektura informacji • strategia bezpieczeństwa informacji • system operacyjny • odporność organizacyjna • zarządzanie ryzykiem • dane nieustrukturyzowane	• opracować strategię bezpieczeństwa informacji • edukować na temat poufności danych • zapewnić bezpieczeństwo informacji • przeprowadzać audyty ICT • wykonać testy oprogramowania • identyfikować zagrożenia bezpieczeństwa ICT • zidentyfikować słabe strony systemu ICT • wdrożyć zarządzanie	• zdefiniować kryteria jakości danych • określić wymagania techniczne • przechowywać zapisy zadań • być na bieżąco z najnowszymi rozwiązaniami systemów informatycznych • zarządzać zgodnością z bezpieczeństwem IT • zarządzać planami odzyskiwania po awarii • monitorować wydajność systemu • przeprowadzić analizę danych • przeprowadzić analizę ryzyka • raportowanie wyników

		• ryzykiem ICT • udzielać porad w zakresie doradztwa ICT • analizować system teleinformatyczny • zdefiniować zasady bezpieczeństwa	• testów rozwiązywanie problemów • zweryfikować formalne specyfikacje ICT
2529.8 - Menedżer bezpieczeństwa teleinformatycznego - proponuje i wdraża niezbędne aktualizacje bezpieczeństwa; doradza, wspiera, informuje i zapewnia szkolenia i świadomość bezpieczeństwa oraz podejmuje bezpośrednie działania w sprawie całości lub części sieci lub systemu.	• Techniki zarządzania problemami ICT • Zarządzanie projektami teleinformatycznymi • Polityka jakości ICT • Standardy bezpieczeństwa teleinformatycznego • Wymagania użytkowników systemów teleinformatycznych • Internet przedmiotów • wektory ataku • informatyka śledcza • strategia bezpieczeństwa informacji • wewnętrzna polityka zarządzania ryzykiem • zarządzanie Internetem • wymagania prawne produktów ICT	• zdefiniować zasady bezpieczeństwa • opracować strategię bezpieczeństwa informacji • ustanowić plan zapobiegania bezpieczeństwu ICT • wdrożyć zarządzanie ryzykiem ICT	• prowadzić ćwiczenia w zakresie odzyskiwania po awarii • utrzymywać zarządzanie tożsamością ICT • zarządzać zgodnością z bezpieczeństwem IT • zarządzać planami odzyskiwania po awarii • rozwiązywać problemy systemów teleinformatycznych
2529.9 – inżynier wiedzy – integruje wiedzę strukturalną z systemami komputerowymi (bazami wiedzy) w celu rozwiązywania złożonych problemów, zwykle wymagających wysokiego poziomu wiedzy specjalistycznej człowieka lub metod sztucznej inteligencji.	• inteligencja biznesowa • modelowanie procesów biznesowych • narzędzia do tworzenia baz danych • ekstrakcja informacji • struktura informacji, przetwarzanie języka naturalnego • zasady sztucznej inteligencji • Język zapytań struktury opisu zasobów • cykl życia rozwoju systemów • teoria systemów • algorytmizacja zadań • Programowanie sieciowe	• Używać interfejsu specyficznego dla aplikacji • korzystać z baz danych • używać języków znaczników	• analizować wymagania biznesowe • stosować teorię systemów teleinformatycznych • ocenić wiedzę z zakresu ICT • tworzyć drzewa semantyczne • określić wymagania techniczne • zarządzać integracją semantyczną ICT • zarządzać wiedzą biznesową • zarządzać bazą danych

Faza 2: Mapowanie zawodów i efektów uczenia się w ESCO

W poprzedniej tabeli przeanalizowaliśmy udokumentowane zawody i zidentyfikowaliśmy efekty uczenia się powiązane z każdą rolą. Wykorzystaliśmy ramy ESCO, aby sklasyfikować te wyniki jako wiedzę, umiejętności i kompetencje.

Efekt uczenia się to jasne i konkretne stwierdzenie opisujące, czego od uczniów oczekuje się, że się nauczą i będą w stanie zrobić po zakończeniu okresu nauczania. W oświadczeniu zawarto wiedzę, umiejętności i postawy.

W sekcji klasyfikatora zawodów ESCO Specjaliści ds. technologii informacyjno-komunikacyjnych znajdują się w dwóch podsekcjach: Twórcy i analizy oprogramowania i aplikacji oraz Specjaliści od baz danych i sieci. Ta ostatnia składa się z czterech grup: Specjaliści od baz danych i sieci, Administratorzy systemów, Specjaliści od sieci komputerowych oraz Specjaliści od baz danych i sieci gdzie indziej niesklasyfikowani. W tej grupie jednostek znalazły się wszystkie zaprezentowane w tabeli zawody związane z cyberbezpieczeństwem. W skład tej grupy wchodzą na przykład specjaliści ds. bezpieczeństwa technologii informacyjno-komunikacyjnych.

W takich przypadkach do zadań należeć będzie:

a) opracowywanie planów zabezpieczenia plików komputerowych przed przypadkową lub nieuprawnioną modyfikacją, zniszczeniem lub ujawnieniem oraz zaspokojenie awaryjnych potrzeb w zakresie przetwarzania danych.

b) szkolenie użytkowników i promowanie świadomości bezpieczeństwa w celu zapewnienia bezpieczeństwa systemu oraz poprawy wydajności serwerów i sieci.

(c) naradzanie się z użytkownikami w celu omówienia takich kwestii, jak potrzeby w zakresie dostępu do danych komputerowych, naruszenia bezpieczeństwa i zmiany w programowaniu.

(d) monitorowanie bieżących raportów na temat wirusów komputerowych w celu ustalenia, kiedy należy zaktualizować systemy ochrony antywirusowej.

(e) modyfikowanie plików bezpieczeństwa komputera w celu włączenia nowego oprogramowania, skorygowania błędów lub zmiany indywidualnego statusu dostępu.

f) monitorowanie wykorzystania plików danych i regulowanie dostępu w celu zabezpieczenia informacji w plikach komputerowych.

(g) przeprowadzanie ocen ryzyka i przeprowadzanie testów systemu przetwarzania danych w celu zapewnienia funkcjonowania działań związanych z przetwarzaniem danych i środków bezpieczeństwa.

h) szyfrowanie transmisji danych i tworzenie zapór sieciowych w celu ukrycia poufnych informacji podczas ich przesyłania i zapobiegania skażonym transferom cyfrowym.

Opis efektów uczenia się dla każdego zawodu:

Zawód	Wyniki nauki
technik bezpieczeństwa teleinformatycznego (3512.3)	• Wykazać wszechstronną wiedzę na temat sieci ICT, wektorów ataków sprzętowych, środków zaradczych przed cyberatakami i systemów operacyjnych. • Krytycznie analizować i diagnozować luki w systemach ICT w celu zwiększenia bezpieczeństwa systemu. • Wdrażać i zarządzać solidnymi strategiami zarządzania dokumentami, które są zgodne z protokołami bezpieczeństwa ICT. • Opracować i realizować szczegółowe plany testowania oprogramowania w celu identyfikacji i usunięcia luk w oprogramowaniu. • Integrować komponenty systemów i korzystać z oprogramowania kontroli dostępu, aby budować bezpieczne i wydajne systemy teleinformatyczne .
Główny specjalista ds. bezpieczeństwa teleinformatycznego (2529.1)	• Rozumieć i analizować zagrożenia bezpieczeństwa sieci ICT, ustawodawstwo i standardy w celu ochrony informacji organizacyjnych. • Opracowywanie i wdrażanie strategii bezpieczeństwa informacji oraz wewnętrznych polityk zarządzania ryzykiem. • Prowadzić ćwiczenia w zakresie odzyskiwania po awarii i utrzymywać plany ciągłości operacyjnej. • Edukować personel w zakresie poufności danych i zapewniać współpracę między działami w celu zwiększenia praktyk bezpieczeństwa.
Ekspert ds. kryminalistyki cyfrowej (2529.2)	• Analizować i testować bezpieczeństwo systemów wbudowanych, szczególnie w środowisku Internetu Rzeczy (IoT). • Opracowywanie i wykonywanie prototypów i testów oprogramowania oraz wykorzystywanie narzędzi inżynierii oprogramowania wspomaganego

	komputerowo. • Zarządzać zgodnością z bezpieczeństwem IT oraz przeprowadzać analizę ryzyka i monitorowanie wydajności systemu. • Definiowanie i wdrażanie polityk bezpieczeństwa i wymagań technicznych dla systemów wbudowanych.
Inżynier bezpieczeństwa systemów wbudowanych (2529.3)	• Analizować i testować bezpieczeństwo systemów wbudowanych, szczególnie w środowisku Internetu Rzeczy (IoT). • Opracowywanie i wykonywanie prototypów i testów oprogramowania oraz wykorzystywanie narzędzi inżynierii oprogramowania wspomaganego komputerowo. • Zarządzać zgodnością z bezpieczeństwem IT oraz przeprowadzać analizę ryzyka i monitorowanie wydajności systemu. • Definiowanie i wdrażanie polityk bezpieczeństwa i wymagań technicznych dla systemów wbudowanych.
Etyczny haker (2529.4)	• Wykonywać oceny podatności na zagrożenia i testy penetracyjne, korzystając z metod przyjętych w branży. • Identyfikować i wykorzystywać potencjalne luki w systemach w celu poprawy środków bezpieczeństwa. • Tworzyć exploity w kodzie i przeprowadzać audyty ICT, aby zapewnić integralność systemu. • Analizować kontekst organizacji, aby skutecznie dostosować strategie bezpieczeństwa
Menedżer ds. odporności ICT (2529.5)	• Opracować i wdrażać plany awaryjne i strategie bezpieczeństwa informacji dla scenariuszy awaryjnych. • Wdrażać i zarządzać systemami odzyskiwania danych ICT oraz procesami zarządzania ryzykiem. • Prowadzić ćwiczenia w zakresie odtwarzania po awarii i zarządzaj bezpieczeństwem systemu podczas kryzysów.

	• Analizować procesy biznesowe w celu zwiększenia odporności organizacji i zgodności z przepisami prawa.
Administrator Bezpieczeństwa ICT (2529.6)	• Planować i wdrażać środki bezpieczeństwa w celu ochrony danych i zarządzania systemami tożsamości teleinformatycznej. • Utrzymywać bezpieczeństwo baz danych oraz zapewniać integralność i odporność systemu. • Rozwiązywanie problemów z systemami teleinformatycznymi oraz wdrażanie metod rozwiązywania problemów i zapewniania jakości. • Zarządzać architekturą danych i przestrzegać zasad organizacyjnych dotyczących ochrony danych.
Inżynier bezpieczeństwa teleinformatycznego (2529.7)	• Doradzać i wdrażać rozwiązania kontroli dostępu do danych i ochrony procesów biznesowych. • Analizować systemy teleinformatyczne i definiować polityki bezpieczeństwa oraz kryteria jakości danych. • Przeprowadzać analizę danych i analizę ryzyka oraz zarządzać zgodnością z bezpieczeństwem IT i planami odzyskiwania po awarii. • Być na bieżąco z pojawiającymi się technologiami i rozwiązaniami z zakresu systemów informatycznych
Menedżer ds. bezpieczeństwa teleinformatycznego (2529.8)	• Proponować i wdrażać aktualizacje zabezpieczeń oraz zarządzać bezpieczeństwem ICT w różnych projektach. • Prowadzić ćwiczenia w zakresie odzyskiwania po awarii i ustalać plany zapobiegania bezpieczeństwu ICT. • Utrzymanie i zarządzanie systemami zarządzania tożsamością ICT oraz rozwiązywanie złożonych problemów systemowych. • Opracować i wdrażać strategie bezpieczeństwa informacji oraz zarządzać

	planami odtwarzania po awarii.
Inżynier wiedzy (2529.9)	• Integrować ustrukturyzowaną wiedzę z systemami komputerowymi, korzystając z zaawansowanych narzędzi, takich jak język zapytań RDF i programowanie internetowe. • Zarządzać integracją semantyczną i systemami baz danych, aby usprawnić zarządzanie wiedzą biznesową. • Analizować wymagania biznesowe i stosować teorię systemów ICT do tworzenia efektywnych baz wiedzy. • Tworzyć drzewa semantyczne i oceniać wiedzę ICT, aby rozwiązywać złożone problemy przy użyciu metod AI.

3. ANALIZA I USTALENIA

3.1. ANALIZA BADAŃ TERENOWYCH

Analiza badań terenowych VET i HEI

Dane z ankiety „Mapowanie potrzeb szkoleniowych dla agentów zmian w zakresie bezpieczeństwa cybernetycznego MŚP" zawierają szereg pytań skupiających się na szkoleniach z zakresu cyberbezpieczeństwa w kontekście kształcenia i szkolenia zawodowego (VET) oraz instytucji szkolnictwa wyższego (HEI). Zebraliśmy dane na temat tematów objętych szkoleniami z zakresu cyberbezpieczeństwa, metod nauczania, inkluzywności płci i danych demograficznych respondentów.

Celem tego badania jest analiza odpowiedzi, aby zrozumieć obecny stan szkoleń z zakresu cyberbezpieczeństwa, stosowane metodologie oraz postrzeganie inkluzywności i skuteczności w tej dziedzinie.

Analiza odpowiedzi będzie opierać się na następującej strukturze kluczy:

- Demografia
- Program nauczania, potrzeby szkoleniowe i preferencje edukacyjne
- Wymagania kompetencyjne i przyszłe umiejętności
- Spostrzeżenia dotyczące płci

Demografia:

Podział płci wśród respondentów badania pomiędzy instytucjami kształcenia i szkolenia zawodowego (VET) a instytucjami szkolnictwa wyższego (HEI) jest następujący:

Całkowita liczba respondentów według typu instytucji

Typ instytucji	Odpowiedzi	Kobieta	Mężczyzna	Wolę nie mówić
HEI (Instytucje szkolnictwa wyższego)	104	28	73	3
VET (kształcenie i szkolenie zawodowe)	86	36	48	2
Całkowity	**190**	**64**	**121**	**5**

Chociaż zarówno w instytucjach szkolnictwa wyższego, jak i w instytucjach kształcenia i szkolenia zawodowego występuje brak równowagi między płciami, w instytucjach kształcenia i szkolenia zawodowego różnica jest mniejsza. Aby zapewnić jaśniejszy obraz reprezentacji płci w stosunku do całkowitej liczby odpowiedzi z każdej instytucji i dostosować wyniki pod względem liczby stronniczości odpowiedzi, obliczyliśmy odsetek każdej płci w obu typach instytucji.

Rozkład respondentów według typu instytucji

Typ instytucji	Kobieta %	Mężczyzna %	Wolę nie mówić %	Całkowity
HEI (Instytucje szkolnictwa wyższego)	27	70	3	**100%**
VET (kształcenie i szkolenie zawodowe)	42	56	2	**100%**

Analiza skorygowana o błąd odpowiedzi potwierdza, że chociaż w obu typach instytucji występuje wyższy odsetek respondentów płci męskiej, różnica między reprezentacją mężczyzn i kobiet pozostaje mniejsza w instytucjach VET. Przyczyna może być zróżnicowana (np. czynniki kulturowe, strukturalne lub polityczne wpływające na różnorodność płci w edukacji o cyberbezpieczeństwie w tych typach instytucji). Wyższy odsetek kobiet biorących udział w kształceniu i szkoleniu zawodowym sugeruje potencjalne obszary dalszych badań nad praktykami, które wspierają środowisko bardziej włączające płeć w szkoleniu zawodowym w porównaniu ze szkolnictwem wyższym.

Program nauczania, potrzeby szkoleniowe i preferencje edukacyjne

Tematy zawarte w istniejących szkoleniach z zakresu cyberbezpieczeństwa w uczelniach wyższych i kształceniu zawodowym

Temat	Odpowiedzi	HEI	VET
Podstawy cyberbezpieczeństwa	151	90	61
Bezpieczeństwo sieci	123	72	51
Analiza i zarządzanie zagrożeniami	99	65	34
Kryptografia	92	57	35
Reagowanie na incydenty	82	49	33
Zarządzanie ryzykiem	77	43	34
Przepisy i zasady dotyczące cyberbezpieczeństwa	73	42	31
Zaawansowane techniki łagodzenia zagrożeń	54	33	21

Wydaje się, że priorytetem jest podstawowa wiedza i umiejętności oraz bezpieczeństwo sieci. Analiza i zarządzanie zagrożeniami, kryptografia i reagowanie na incydenty sugerują kompleksowe omówienie zagrożeń cyberbezpieczeństwa podczas szkoleń. Zarządzanie ryzykiem oraz przepisy i polityki dotyczące cyberbezpieczeństwa, pomimo wskazania świadomości potrzeby holistycznego podejścia, które obejmuje zrozumienie kontekstu prawnego i skuteczne zarządzanie ryzykiem, nie zawsze są wybierane. Warto zauważyć, że zaawansowane techniki łagodzenia zagrożeń są rzadziej uwzględniane w szkoleniach.

Aby zapewnić wyniki bez błędu wynikającego z liczby respondentów z każdego typu instytucji (wyższej uczelni i kształcenia zawodowego), dane normalizowano w oparciu o całkowitą liczbę odpowiedzi dla każdego typu instytucji. Takie podejście pozwala nam zobaczyć odsetek instytucji, które uwzględniają każdy temat w swoich programach szkoleniowych z zakresu cyberbezpieczeństwa.

Tematy	**Proporcja uczelni (HEI)**	**Proporcja kształcenia i szkolenia zawodowego (VET)**
Podstawy cyberbezpieczeństwa	15,76%	15,48%
Bezpieczeństwo sieci	12,61%	12,94%
Analiza i zarządzanie zagrożeniami	11,38%	8,63%
Kryptografia	9,98%	8,88%
Reagowanie na incydenty	8,58%	8,38%
Zarządzanie ryzykiem	7,53%	8,63%
Przepisy i zasady dotyczące cyberbezpieczeństwa	7,36%	7,87%
Zaawansowane techniki łagodzenia zagrożeń	5,78%	5,33%

Co ciekawe, istnieją podobne priorytety z niewielkimi różnicami. Zarówno uczelnie, jak i instytucje zajmujące się kształceniem i szkoleniem zawodowym kładą duży nacisk na „Podstawy cyberbezpieczeństwa" i „Bezpieczeństwo sieci". Oznacza to, że tematy te są uznawane za kluczowe elementy edukacji w zakresie cyberbezpieczeństwa. Proporcje są ściśle dopasowane, przy czym w uczelniach wyższych kładzie się nieco większy nacisk na „podstawy cyberbezpieczeństwa" w porównaniu z kształceniem i szkoleniem zawodowym, a „bezpieczeństwo sieci" wykazuje podobny wzorzec, ale z węższymi różnicami.

Zauważalna jest różnica w nacisku na bardziej specjalistyczne tematy, takie jak „Analiza zagrożeń i zarządzanie nimi", „Kryptografia" oraz „Zaawansowane techniki łagodzenia zagrożeń". Uczelnie zazwyczaj przeznaczają na te tematy nieco większą część swoich programów szkoleniowych w porównaniu z kształceniem i szkoleniem zawodowym. Można to wytłumaczyć faktem, że uczelnie skupiają się na zapewnianiu bardziej wszechstronnego, opartego na teorii zrozumienia cyberbezpieczeństwa, które często obejmuje szerszy zakres specjalistycznych przedmiotów. Z drugiej strony instytucje kształcenia i szkolenia zawodowego, choć nadal obejmują szerokie spektrum tematów, mogą priorytetowo traktować praktyczne zastosowania i natychmiastową gotowość do pracy.

Metody nauczania

Metody nauczania	Proporcja uczelni (HEI)	Proporcja kształcenia i szkolenia zawodowego (VET)
Studium przypadku	60,91%	39,09%
Projekty grupowe	58,95%	41,05%
Laboratoria praktyczne	59,02%	40,98%
Wykłady	56,97%	43,03%
Odwrócona klasa	34,78%	65,22%
Symulacje on-line	51,35%	48,65%

Metody studiów przypadków, projektów grupowych, laboratoriów praktycznych i wykładów są powszechnie stosowane w obu typach instytucji, przy czym preferowane są uczelnie wyższe niż kształcenie i szkolenie zawodowe. Jeśli chodzi o metodę odwróconej klasy, jest ona bardziej rozpowszechniona w kształceniu i szkoleniu zawodowym (65,22%) niż w szkołach wyższych (34,78%), co wskazuje na skłonność do interaktywnego modelu uczenia się w kształceniu zawodowym. W odwróconych klasach priorytetem jest aktywne uczenie się i zaangażowanie uczniów, co dobrze wpisuje się w podejście praktyczne i oparte na umiejętnościach charakterystyczne dla kształcenia i szkolenia zawodowego.

Skuteczność metod nauczania

Metoda nauczania	Liczba
Praktyczne sesje praktyczne	141
Warsztaty stacjonarne	134
Interaktywne symulacje	104
Kursy online	100
Samouczki wideo	73
Webinaria	68

Przegląd ten podkreśla różnorodność preferowanych metod nauczania, ale z wyraźnym naciskiem na praktyczne, interaktywne i elastyczne doświadczenia edukacyjne. Praktyczne sesje i warsztaty na żywo są wysoko cenione, ponieważ zapewniają interaktywne i praktyczne doświadczenie edukacyjne. Interaktywne symulacje i kursy online również otrzymały istotne wzmianki, co pokazało znaczenie dostępnych sposobów uczenia się.

Wyzwania stojące przed placówkami szkolnymi.

Na pytanie o główne wyzwania stojące przed placówkami szkolnymi, oto podsumowanie najczęściej powracających tematów:

- **Różnorodność umiejętności i doświadczenia uczestników** : Trenerzy napotykają trudności ze względu na zróżnicowane pochodzenie i poziom wiedzy specjalistycznej wśród uczestników. Dopasowanie szkolenia tak, aby pasowało do całej grupy i zapewnienie, że z sesji skorzystają zarówno osoby techniczne, jak i nietechniczne, jest wyzwaniem.

- **Dbanie o aktualność materiałów szkoleniowych** : Szybka ewolucja zagrożeń cyberbezpieczeństwa wymaga ciągłej aktualizacji materiałów szkoleniowych i metod nauczania, aby zapewnić ich przydatność.
- **Ograniczenia w zakresie szkolenia praktycznego** : Zapewnienie praktycznego doświadczenia stanowi poważne wyzwanie. Ograniczenia obejmują niewystarczające zaplecze laboratoryjne, brak możliwości symulacji w świecie rzeczywistym oraz trudność w stworzeniu realistycznych scenariuszy cyberataków do celów praktycznych.
- **Ograniczenia zasobów** : Trenerzy często muszą radzić sobie z ograniczonymi zasobami finansowymi, brakiem wykwalifikowanego personelu, przestarzałymi materiałami do nauki oraz niewystarczającym sprzętem i oprogramowaniem niezbędnym do skutecznego szkolenia.
- **Zaangażowanie i motywacja uczniów** : Utrzymanie uwagi uczniów i motywowanie ich do aktywnego udziału w nauce jest trudne, szczególnie ze względu na konieczność omówienia złożonych i czasami suchych treści technicznych.
- **Program nauczania i struktura edukacji** : Istnieje potrzeba kompleksowych, multidyscyplinarnych programów nauczania obejmujących wszystkie aspekty cyberbezpieczeństwa. Ponadto istotnym wyzwaniem pozostaje włączenie cyberbezpieczeństwa do programów nauczania, zwłaszcza na poziomie szkół średnich.
- **Dostęp do aktualnych narzędzi i technologii** : Zapewnienie uczniom dostępu do najnowszych narzędzi i technologii związanych z cyberbezpieczeństwem na potrzeby praktycznej nauki często stanowi wyzwanie, co ma kluczowe znaczenie dla praktycznego zrozumienia.
- **Kwestie językowe i lokalizacyjne** : zasoby dotyczące cyberbezpieczeństwa mogą nie zawsze być dostępne w językach ojczystych uczniów, co dodatkowo komplikuje szkolenie w regionach nieanglojęzycznych.
- **Dostosowanie przemysłu i edukacji** : wyzwaniem jest zrównoważenie potrzeby nauczania podstaw teoretycznych z umiejętnościami praktycznymi odpowiadającymi potrzebom branży. Istnieje także konieczność przygotowania studentów do wejścia na rynek pracy poprzez posiadanie odpowiednich umiejętności.
- **Potencjał i rozwój nauczycieli** : Zapewnienie, że nauczyciele posiadają aktualną wiedzę i są w stanie skutecznie przekazywać złożone koncepcje, ma kluczowe znaczenie, ale stanowi wyzwanie.

Dostosowanie do konkretnych potrzeb MŚP

Opcja odpowiedzi	Liczba
Neutralny	82
Wyrównany	67
Trochę nie dopasowane	19
Wysoce wyrównane	17
Niewyrównane	5

Większość odpowiedzi wskazuje na neutralne podejście, co sugeruje, że istnieje pole do poprawy w tym zakresie. Znaczna liczba respondentów oceniła swoje programy jako dostosowane, podczas gdy bardzo niewielu nauczycieli uważa, że ich programy są w dużym stopniu dostosowane lub niezgodne z potrzebami branży. Odpowiedzi na dolnym końcu skali (niedopasowane i nieznacznie niedopasowane) odzwierciedlają obawy lub wyzwania związane z pełnym dostosowaniem treści edukacyjnych do ewoluującego charakteru cyberbezpieczeństwa

w branży. Taki rozkład odpowiedzi pokazuje, że wyzwanie, jakim jest zapewnienie edukacji w zakresie cyberbezpieczeństwa, dostosowanej do trendów i wymagań branżowych, jest nadal aktualne. Podkreśla znaczenie projektu CyberAgent, którego celem jest zapewnienie ciągłych aktualizacji programów nauczania, partnerstw branżowych i możliwości szkoleń praktycznych w celu lepszego dostosowania programów szkoleniowych w zakresie cyberbezpieczeństwa do potrzeb branży cyberbezpieczeństwa.

Dedykowane tematy dla MŚP

Temat/umiejętność	**Liczba**
Podstawowe cyberbezpieczeństwo dla MŚP	91
Ochrona danych i prywatność dla MŚP	75
Program nie obejmuje konkretnych tematów ani umiejętności MŚP	**64**
Reakcja na incydenty dla MŚP	58
Ocena ryzyka i zarządzanie ryzykiem w kontekście MŚP	53
Rozwój polityki cyberbezpieczeństwa dla MŚP	46

Duży nacisk kładzie się na podstawowe zasady cyberbezpieczeństwa i ochrony danych. Najczęściej wymieniane tematy, Podstawowe cyberbezpieczeństwo dla MŚP oraz Ochrona danych i prywatność dla MŚP, wskazują, że edukatorzy traktują priorytetowo wyposażenie MŚP w wiedzę niezbędną do ochrony ich danych i zrozumienia podstawowych koncepcji cyberbezpieczeństwa. Liczba odpowiedzi „Program nie obejmuje żadnego konkretnego tematu ani umiejętności MŚP" wskazuje na lukę w niektórych programach szkoleniowych z zakresu cyberbezpieczeństwa w zakresie treści dostosowanych do potrzeb małych i średnich przedsiębiorstw (MŚP). Podkreśla krytyczny obszar wymagający ulepszenia szkoleń z zakresu cyberbezpieczeństwa, szczególnie biorąc pod uwagę wyzwania i zagrożenia stojące przed MŚP.

MŚP często dysponują ograniczonymi zasobami i mogą nie mieć dostępu do specjalistycznej wiedzy w zakresie cyberbezpieczeństwa, co czyni je szczególnie podatnymi na zagrożenia cybernetyczne. Brak treści specyficznych dla MŚP w programach szkoleniowych w zakresie cyberbezpieczeństwa sugeruje, że programy te mogą nie w pełni odpowiadać odrębnym potrzebom MŚP, potencjalnie pozostawiając lukę w ich przygotowaniu i odporności na cyberataki. Zapełnienie tej luki wymaga integracji tematów i umiejętności zaprojektowanych specjalnie z myślą o zaspokojeniu potrzeb MŚP w zakresie cyberbezpieczeństwa, takich jak ocena ryzyka dostosowana do mniejszych operacji biznesowych, opłacalne praktyki w zakresie cyberbezpieczeństwa oraz strategie opracowania skutecznej polityki cyberbezpieczeństwa przy ograniczonych zasobach.

Deficyt kompetencji pracowników MŚP

Umiejętność/temat	Liczba
Wykrywanie zagrożeń i reagowanie	103
Wiedza specjalistyczna w zakresie bezpieczeństwa w chmurze	87
Reakcja na incydenty i odzyskiwanie	69
Prywatność i ochrona danych	67
Zarządzanie i analiza ryzyka	63
Pojawiające się technologie	58
Bezpieczeństwo sieci	41
Znajomość przepisów i zgodności	36

Analiza pokazuje, że pracownikom brakuje umiejętności w kluczowych obszarach, przy czym najczęściej wymienianym jest wykrywanie zagrożeń i reagowanie na nie. Podkreśla to znaczenie przygotowania studentów do identyfikowania zagrożeń cyberbezpieczeństwa i reagowania na nie, co jest podstawową umiejętnością w tej dziedzinie. Na drugim miejscu znajduje się wiedza o bezpieczeństwie chmur, pokazująca zależność od technologii chmurowych i potrzebę specjalistycznej wiedzy, aby zabezpieczyć środowiska chmurowe przed pracownikami. Cenione są również reakcja na incydenty i ich odzyskiwanie, prywatność i ochrona danych oraz zarządzanie ryzykiem i analiza. Uważa się, że w odniesieniu do nowych technologii potrzeba bycia na bieżąco z najnowszymi osiągnięciami w tej dziedzinie nie jest obszarem deficytowym. To samo dotyczy bezpieczeństwa sieci, które jest podstawowym obszarem stanowiącym część większości programów szkoleniowych z zakresu cyberbezpieczeństwa. Pokazuje to skuteczność szkoleń w tym zakresie.

Zagrożenia

Zagrożenia	Liczba
Cyberataki oparte na sztucznej inteligencji	117
Ataki ransomware	96
Phishing i inżynieria społeczna	87
Naruszenia bezpieczeństwa chmury	82
Luki w zabezpieczeniach IoT	75
Zagrożenia związane z użyciem deep-fake	51
Zagrożenia wewnętrzne	25

Analiza pokazuje, że na najczęściej wymienianym pojawiającym się zagrożeniu dla cyberbezpieczeństwa kładzie się znaczny nacisk na cyberataki oparte na sztucznej inteligencji, co wskazuje na obawy związane z wyrafinowaniem i złożonością zagrożeń cybernetycznych napędzanych sztuczną inteligencją. Ataki typu ransomware, phishing i inżynieria społeczna również uzyskały wysoką pozycję, co wskazuje na obecność tych wektorów ataków w przypadku MŚP. Naruszenia bezpieczeństwa chmury i luki w zabezpieczeniach IoT uwydatniają obawy związane z bezpieczeństwem usług w chmurze i rozwijającym się Internetem rzeczy, odzwierciedlając wyzwania związane z ochroną zróżnicowanych i rozproszonych ekosystemów

technologicznych dla MŚP. Zagrożenia typu deepfake i zagrożenia wewnętrzne nie są uważane za duże wektory zagrożeń. Programy szkoleniowe obejmujące 5 najważniejszych tematów mogą lepiej przygotować studentów i pracowników MŚP do radzenia sobie z napotykanymi zagrożeniami.

Pojawiające się trendy

Obszar	Liczba
Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie	160
Tożsamość cyfrowa i prywatność	96
Etyczne hakowanie i umiejętności obronne	82
Zagrożenia obliczeń kwantowych	67
Zdecentralizowane systemy bezpieczeństwa (np. Blockchain)	52
Skoncentrowanie się na umiejętnościach miękkich i szkoleniach interdyscyplinarnych	47

Duży nacisk kładzie się na sztuczną inteligencję i uczenie maszynowe w cyberbezpieczeństwie jako najczęściej wymieniany obszar, co odzwierciedla znaczenie tych technologii we wzmacnianiu środków cyberbezpieczeństwa oraz zapotrzebowanie na specjalistów wykwalifikowanych w tych obszarach. Tożsamość cyfrowa i prywatność to kolejny ważny obszar podkreślający znaczenie ochrony tożsamości cyfrowych i zapewniania prywatności. Wynik w zakresie etycznego hakowania i umiejętności obronnych wskazuje na zapotrzebowanie na praktyczne umiejętności, które umożliwiają profesjonalistom identyfikację słabych punktów i skuteczną obronę przed atakami. Zagrożenia w dziedzinie obliczeń kwantowych, zdecentralizowane systemy bezpieczeństwa, takie jak technologia blockchain oraz umiejętności miękkie i szkolenia interdyscyplinarne nie zostały uznane za pojawiające się trendy. Rozkład odpowiedzi podkreśla różnorodność dziedziny cyberbezpieczeństwa oraz znaczenie przygotowania specjalistów posiadających zróżnicowany zestaw umiejętności i wiedzy do sprostania obecnym i przyszłym wyzwaniom. Ale temat sztucznej inteligencji jest na szczycie listy.

Równość płci

Procent kobiet	Liczba odpowiedzi
Mniej niż 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Ponad 75%	3

Odsetek kobiet uczestniczących w programach szkoleniowych z zakresu cyberbezpieczeństwa wskazuje na dysproporcje w różnorodności płci, przy czym większość odpowiedzi wskazuje na niski udział kobiet. Mówiąc szczegółowo, w 79 odpowiedziach udział kobiet mieścił się w przedziale od 10% do 25%, a 57 odpowiedzi wskazywało, że było to mniej niż 10%. W niektórych

programach sugeruje się umiarkowany poziom różnorodności płci, przy czym 43 respondentów szacuje, że wskaźnik udziału kobiet mieści się w przedziale od 26% do 50%. Jednakże programy, w których uczestniczy duży odsetek kobiet, są szczególnie rzadkie, o czym świadczy zaledwie 8 odpowiedzi wskazujących zakres od 51% do 75% oraz minimalna liczba 3 odpowiedzi, w których szacuje się ponad 75%. Dane te podkreślają wyzwanie, jakim jest osiągnięcie różnorodności płci w programach szkoleniowych z zakresu cyberbezpieczeństwa, podkreślając znaczną różnicę w udziale kobiet w większości zgłaszanych programów.

Inicjatywy dotyczące płci

Odpowiedź	Liczba odpowiedzi
Tak	30
NIE	160

Dane wskazują, że zdecydowana większość respondentów, łącznie 160, nie stosuje konkretnych inicjatyw ani strategii zachęcających kobiety do udziału w szkoleniach z zakresu cyberbezpieczeństwa. Jedynie 30 respondentów potwierdziło wdrożenie takich działań. Sugeruje to, że choć istnieje pewna świadomość i wysiłki na rzecz zwiększenia udziału kobiet w szkoleniach z zakresu cyberbezpieczeństwa poprzez ukierunkowane inicjatywy, w większości programów może jeszcze nie ustalać priorytetów ani nie wdrażać konkretnych strategii mających na celu zajęcie się różnorodnością płci. Ten brak ukierunkowanych inicjatyw może przyczynić się do niskiego odsetka udziału kobiet, jak zauważono w odpowiedziach na poprzednie pytanie.

Szkolenia włączające płeć

Odpowiedź	Liczba odpowiedzi
Tak	47
NIE	44
Niepewny	72
Nie dotyczy mnie	27

Wyniki sugerują podzielone zdanie wśród respondentów na temat dostępności modułów szkoleniowych włączających płeć w zakresie cyberbezpieczeństwa. Największa grupa, licząca 72 respondentów, wyraziła niepewność („Nie wiem"), wskazując na brak jasnego konsensusu lub wiedzy na temat obecności materiałów inkluzywnych płci. Istnieje prawie równy podział między tymi, którzy uważają, że istnieje wystarczająca liczba modułów włączających płeć (47 odpowiedzi), a tymi, którzy tak nie uważają (44 odpowiedzi). Ponadto 27 respondentów uznało, że pytanie nie ma związku z ich doświadczeniem lub kontekstem.

Podział ten odzwierciedla toczącą się debatę i zróżnicowane postrzeganie inkluzywności treści szkoleń z zakresu cyberbezpieczeństwa. Duża liczba niepewnych odpowiedzi uwydatnia potencjalną lukę w świadomości lub dostępności zasobów szkoleniowych włączających płeć w ekosystemie edukacji i szkoleń w zakresie cyberbezpieczeństwa.

Bariery utrudniające włączenie płci

Bariera	Liczba
Stereotypy czy normy kulturowe	107
Brak świadomości możliwości w zakresie cyberbezpieczeństwa	86
Brak mentora i wzorców do naśladowania	74
Wyzwania dotyczące równowagi między życiem zawodowym a prywatnym	60
Postrzegane uprzedzenia ze względu na płeć w branży	58

Do najważniejszych barier utrudniających udział kobiet w cyberbezpieczeństwie, w opinii respondentek badania, należą stereotypy lub normy kulturowe (107 wskazań) oraz brak świadomości możliwości, jakie daje cyberbezpieczeństwo (86 wskazań). Te dwie bariery sugerują, że postrzeganie społeczne i niewystarczające informacje na temat ścieżek kariery znacząco utrudniają kobietom wejście do branży cyberbezpieczeństwa. Brak mentorstwa lub wzorców do naśladowania oraz wyzwania w zakresie równowagi między życiem zawodowym a prywatnym również stanowią istotne bariery, co podkreśla znaczenie sieci wsparcia i elastycznych środowisk pracy w zachęcaniu kobiet do udziału w życiu zawodowym. Ponadto postrzegane w branży uprzedzenia związane z płcią wskazują na potrzebę zmian kulturowych i systemowych w tej dziedzinie, aby uczynić ją bardziej przyjazną i sprawiedliwą dla kobiet.

Specjalny program promujący różnorodność i włączenie społeczne

Odpowiedź	Liczba odpowiedzi
Tak	44
NIE	85
Niepewny	61

Dane pokazują, że znaczna część ankietowanych instytucji (85 odpowiedzi) nie posiada konkretnych polityk ani programów promujących różnorodność i włączenie kobiet w szkoleniach z zakresu cyberbezpieczeństwa. Tymczasem 44 respondentów wskazało, że ich instytucje rzeczywiście wdrażają takie inicjatywy, podkreślając podejście do kwestii różnorodności płci w terenie. Jednak znaczna liczba respondentów (61) nie jest pewna, czy ich instytucje posiadają taką politykę lub programy, wskazując na potencjalny brak komunikacji lub świadomości w zakresie istniejących wysiłków na rzecz różnorodności i włączenia społecznego. Ponadto ta mieszana reakcja sugeruje, że chociaż niektóre instytucje podejmują kroki w kierunku włączania szkoleń w zakresie cyberbezpieczeństwa, pozostaje znaczna luka, zarówno we wdrażaniu programów różnorodności, jak i w świadomości takich inicjatyw wśród wykładowców, pracowników i studentów.

Sugestia ulepszeń

Sugestia	Liczba
Większa widoczność kobiet odnoszących sukcesy specjalistek ds. cyberbezpieczeństwa	95
Więcej kobiet-instruktorów lub personelu szkoleniowego ds. cyberbezpieczeństwa	89
Oferowanie stypendiów lub zachęt	81
Możliwości mentorskie	49
Treści szkoleniowe, które pozwalają uniknąć uprzedzeń związanych z płcią	33
Regularnie aktualizowane zasady, aby wspierać integrację	31
Studia przypadków i scenariusze uwzględniające płeć	24
Dopasowane programy szkoleniowe	21
Więcej szkoleń tylko dla kobiet	18

Analiza odpowiedzi dotyczących sugestii dotyczących uczynienia szkoleń z zakresu cyberbezpieczeństwa bardziej włączającymi płeć, pokazuje silny konsensus co do znaczenia kilku kluczowych strategii. Najbardziej popieraną sugestią (95 wzmianek) jest zwiększenie widoczności kobiet odnoszących sukcesy specjalistek ds. cyberbezpieczeństwa. Podkreśla to kluczową rolę wzorców do naśladowania i postaci z aspiracjami w inspirowaniu kobiet do kontynuowania kariery w cyberbezpieczeństwie. Tuż za nimi, z 89 wzmiankami, znajduje się wezwanie do zatrudnienia większej liczby kobiet instruktorów lub personelu szkoleniowego ds. cyberbezpieczeństwa, co podkreśla potrzebę reprezentacji w kadrze edukacyjnej. Oferowanie stypendiów lub zachęt, które otrzymało 81 wzmianek, uznano za kluczowe dla zwiększenia dostępności finansowej i atrakcyjności tej dziedziny dla kobiet. Możliwości mentoringu, które zauważyło 49 respondentów, podkreślają znaczenie poradnictwa i wsparcia ze strony doświadczonych specjalistów w tej dziedzinie. Potrzeba treści szkoleniowych pozwalających uniknąć uprzedzeń związanych z płcią oraz regularnie aktualizowanych polityk wspierających włączenie, wskazuje na konieczność dostosowania programów nauczania i polityk, które odzwierciedlają i promują różnorodność.

Analiza badania terenowego MŚP

Demografia:

W ankiecie otrzymano odpowiedzi od krajów partnerskich. Najwięcej respondentów ma Rumunia (28), następnie Norwegia (23), a następnie Litwa, Hiszpania i Belgia, po 21 respondentów. Finlandia i Turcja również uzyskały znaczną liczbę odpowiedzi – po 20 odpowiedzi, a Polska jest tuż za nimi z 19 respondentami.

Branża firmowa

Sektor firm	Liczba
IT	18
Edukacja	6
Budowa	4
Doradztwo	4
Bezpieczeństwo cybernetyczne	4

Dane wskazują na silną reprezentację sektora IT – 18 respondentów określiło swoją firmę jako działającą w tym sektorze. Sektory edukacji, budownictwa, konsultingu i cyberbezpieczeństwa również są godne uwagi reprezentacje, każdy z liczbą od 4 do 6. Poza pierwszą piątką istnieje długi ogon sektorów z mniejszą liczbą, co ilustruje szerokie podejście badania do różnych branż.

Profil respondentów

pozycja w firmie	Liczba
Menedżer	48
Wykonawczy/Właściciel	35
Techniczny (inżynier/programista/analityk)	27
Inny	25
Koordynator/Administrator	8
Sprzedaż i Marketing	8
Specjalista/Ekspert	8
Pracownik	8
Konsultant	3
Edukacja/Nauczanie	2
Finanse/Księgowość	1
Zarządzanie projektami	1
HR	1
Całkowity	**175**

Istnieje szeroka gama stanowisk pracy dla zróżnicowanej grupy odbiorców zawodowych oraz duży panel stanowisk, takich jak „Pracownik" i „Dyrektor", który wskazuje szerokie spektrum respondentów, obejmujących różne poziomy w hierarchii organizacyjnej. Cyberbezpieczeństwo to kwestia przekrojowa, która angażuje osoby pełniące różne role i obowiązki w firmach .

Płeć

Rozkład płci wśród respondentów badania wskazuje na większą reprezentację mężczyzn (102) w porównaniu z kobietami (69), przy czym niewielka część respondentów (4) woli nie ujawniać swojej płci. Rozkład ten sugeruje różnicę między płciami w dziedzinie reprezentowanej przez badanie, co odzwierciedla szersze trendy w sektorach cyberbezpieczeństwa i technologii, w

których często odnotowuje się dominację mężczyzn. Jednakże znaczna liczba respondentek wskazuje na znaczący udział kobiet w tej dziedzinie, co wskazuje na ciągłe zmiany w różnorodności płci w tym sektorze. Chociaż różnica między płciami jest ewidentna, różnorodność odpowiedzi wskazuje również na stopniowo zmieniający się krajobraz cyberbezpieczeństwa.

Podział płci według kraju

Kraj	Kobieta	Mężczyzna	Wolę nie mówić
Belgia	10	10	1
Finlandia	9	11	0
Litwa	9	12	0
Norwegia	8	15	0
Polska	8	9	2
Rumunia	12	16	0
Hiszpania	6	14	1
Turcja	7	13	0

Tabela pokazuje rozkład płci w różnych krajach. W każdym kraju liczba respondentów płci męskiej przewyższa liczbę kobiet, co jest zgodne z ogólnym rozkładem płci omówionym wcześniej. Różnica ta różni się jednak w zależności od kraju – w niektórych krajach, takich jak Belgia, liczba respondentów płci męskiej i żeńskiej jest równa (po 10), a w Polsce rozkład mężczyzn (9) i kobiet (8) jest bliższy, przy czym niewielka liczba respondentów preferuje nie mówiąc już o ich płci (2). Kraje takie jak Rumunia i Norwegia mają ogólnie większą liczbę respondentów i utrzymują wyższy stosunek liczby mężczyzn do kobiet. Podział na kraje ze względu na płeć pozwala na szczegółowe zrozumienie składu demograficznego respondentów ankiety, podkreślając zarówno dysproporcje ze względu na płeć, jak i różnorodność geograficzną w dziedzinie cyberbezpieczeństwa.

Rozmiar firmy

Rozmiar firmy	Liczba
Do 10 pracowników	64
11-50	60
51-250	51

Z odpowiedzi ankiety wynika, że wśród uczestników jest znaczna liczba małych i średnich przedsiębiorstw. Największą grupę stanowią firmy zatrudniające do 10 pracowników (64 ankietowanych), tuż za nimi plasują się firmy zatrudniające od 11 do 50 pracowników (60 respondentów), a następnie firmy zatrudniające od 51 do 250 pracowników (51 respondentów).

Przewaga mniejszych firm wśród respondentów podkreśla znaczenie dostosowanych do indywidualnych potrzeb rozwiązań w zakresie cyberbezpieczeństwa, które uwzględniają specyficzne potrzeby i ograniczenia MŚP.

Poziom wiedzy

Poziom wiedzy o cyberbezpieczeństwie	Liczba
Średniozaawansowany	85
Początkujący	64
Zaawansowany	26

Odpowiedzi na ankietę wskazują, że większość respondentów ocenia obecny poziom wiedzy swoich pracowników na temat cyberbezpieczeństwa jako „średniozaawansowany" (85), w dalszej kolejności znajdują się ci, którzy uważają go za „początkujący" (64), a mniejsza część postrzega swoich pracowników jako posiadanie „zaawansowanej" wiedzy na temat cyberbezpieczeństwa (26).

Rozkład ten sugeruje znaczny potencjał wzrostu i rozwoju umiejętności w zakresie cyberbezpieczeństwa w reprezentowanych organizacjach. Większość poziomów „średniozaawansowany" i „początkujący" wskazuje na konieczność ciągłych inicjatyw szkoleniowych i edukacyjnych w celu podniesienia bazy wiedzy tych pracowników w zakresie cyberbezpieczeństwa. Podkreśla szansę na ukierunkowane programy szkoleniowe w zakresie cyberbezpieczeństwa, które odpowiadają różnym poziomom wiedzy, zapewniając dobre zrozumienie podstawowych zasad cyberbezpieczeństwa przez początkujących.

Obecność pracowników z zaawansowaną wiedzą, choć mniejsza, jest zachęcająca, ponieważ wskazuje na podstawową warstwę wiedzy specjalistycznej w zakresie cyberbezpieczeństwa w niektórych organizacjach.

Poziom wiedzy w zależności od wielkości firmy.

Rozmiar firmy	Zaawansowany	Początkujący	Średniozaawansowany
Do 10 pracowników	6	25	33
11-50	10	20	30
51-250	10	19	22

Tabela pokazuje, jak poziomy wiedzy o cyberbezpieczeństwie (zaawansowany, początkujący, średniozaawansowany) rozkładają się w firmach różnej wielkości. Małe firmy (do 10 pracowników) wykazują tendencję do „średniego" poziomu wiedzy o cyberbezpieczeństwie, a następnie „początkującego". Sugeruje to, że chociaż małe firmy mogą mieć pewną wiedzę na temat cyberbezpieczeństwa, nadal znaczna ich część znajduje się na poziomie początkującym, co wskazuje na pole do poprawy i potrzebę bardziej podstawowego szkolenia. W średnich firmach (11–50 pracowników) rozkład poziomów wiedzy jest zrównoważony, z lekką preferencją dla wiedzy „średnio zaawansowanej". Może to odzwierciedlać bardziej zorganizowane podejście do szkoleń z zakresu cyberbezpieczeństwa w nieco większych organizacjach, ale podobnie wskazuje na obecność zarówno zaawansowanego zrozumienia, jak i podstawowych potrzeb edukacyjnych. Większe MŚP (51–250 pracowników) postępują podobnie jak średnie firmy, z

równą liczbą osób na poziomie zaawansowanym i początkującym oraz nieco mniejszą liczbą wiedzy średniozaawansowanej.

We wszystkich firmach wielkości „średnio zaawansowany" poziom wiedzy o cyberbezpieczeństwie jest najbardziej powszechny.

Pracownicy zajmujący się zadaniami z zakresu cyberbezpieczeństwa

Numer	Liczba
1-5	88
0	22
6-10	17
21+	12
11-20	5

Zakres pracowników w cyberbezpieczeństwie	Liczba
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Tabele przedstawiają rozkład liczby pracowników wykonujących prace związane z cyberbezpieczeństwem w różnych organizacjach. Zapewnia jaśniejszy obraz podziału obowiązków w zakresie cyberbezpieczeństwa pomiędzy różnymi zakresami liczby pracowników. Zdecydowana większość odpowiedzi mieści się w przedziale 0–4, co wskazuje na dużą liczbę organizacji posiadających bardzo małe zespoły ds. cyberbezpieczeństwa lub nawet takich, które nie zajmują się specjalnie cyberbezpieczeństwem. W miarę przechodzenia na wyższe zakresy następuje znaczny spadek częstotliwości, przy czym następuje pewien wzrost w organizacjach zatrudniających ponad 100 pracowników zajmujących się cyberbezpieczeństwem. Wyjaśnia to fakt, że głównym zajęciem tych firm jest cyberbezpieczeństwo .

W szczegółach dane sugerują szeroki zakres wielkości zespołów ds. cyberbezpieczeństwa, przy czym najczęstszą liczebnością jest pojedynczy pracownik, a w drugiej kolejności brak wyspecjalizowanych pracowników ds. cyberbezpieczeństwa, co wskazuje, że wiele organizacji w minimalnym stopniu lub wcale nie korzysta z wyspecjalizowanego personelu ds. cyberbezpieczeństwa. Wraz ze wzrostem wielkości zespołu zauważalny jest spadek częstotliwości.

Podział ten podkreśla potencjalną lukę w alokacji pracowników zajmujących się cyberbezpieczeństwem, w przypadku której znaczna liczba małych i średnich przedsiębiorstw (MŚP) może nie posiadać odpowiednich zasobów przeznaczonych na cyberbezpieczeństwo, co naraża je na większe ryzyko. Obecność większych zespołów w niektórych organizacjach sugeruje uznanie znaczenia cyberbezpieczeństwa w niektórych sektorach lub większych firmach.

Kobiety w cyberbezpieczeństwie

Zakres kobiet w cyberbezpieczeństwie	Liczba
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Wyniki pytania „Ilu spośród tych pracowników to kobiety?" podkreślają znaczną różnicę między płciami wśród pracowników zajmujących się cyberbezpieczeństwem w MŚP. Najbardziej uderzającą obserwacją jest to, że większość firm – w sumie 78 – zgłosiła, że na stanowiskach związanych z cyberbezpieczeństwem nie ma kobiet. Wskazuje to na powszechny problem niedostatecznej reprezentacji kobiet w tym krytycznym obszarze w badanych MŚP. Odnotowuje się stopniowy spadek tej liczby wraz ze wzrostem liczby kobiet na stanowiskach związanych z cyberbezpieczeństwem – w 31 firmach jedna kobieta jest zatrudniona na takim stanowisku. Obecność kilku firm zatrudniających co najmniej 10 kobiet na stanowiskach związanych z cyberbezpieczeństwem, choć jest pozytywna, pozostaje raczej wyjątkiem niż normą. Przypadki te mogą reprezentować organizacje posiadające większe zespoły ds. cyberbezpieczeństwa lub takie, które położyły szczególny nacisk na różnorodność płci wśród swoich pracowników zajmujących się cyberbezpieczeństwem. Podkreśla potrzebę inicjatyw mających na celu zachęcanie i wspieranie kobiet w kontynuowaniu kariery w cyberbezpieczeństwie. Znacząca liczba firm, w których nie ma kobiet na stanowiskach związanych z cyberbezpieczeństwem, wskazuje na kluczowy obszar interwencji mający na celu promowanie różnorodności płci i włączenia społecznego w sektorze. Zmniejszenie tej różnicy między płciami mogłoby przyczynić się do bardziej zróżnicowanych perspektyw w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem.

Korzystanie z usług zewnętrznych

Odpowiedź	Liczba
NIE	115
Tak	60

Odpowiedzi ujawniają istotny aspekt podejścia MŚP do cyberbezpieczeństwa. Większość ankietowanych firm, bo 115 ze 175, wskazuje, że nie korzysta z usług zewnętrznych w zakresie cyberbezpieczeństwa. Sugeruje to preferencję lub konieczność wewnętrznego zarządzania

wysiłkami w zakresie cyberbezpieczeństwa w dużej części populacji MŚP. Tendencję tę mogą napędzać różne czynniki, takie jak ograniczenia budżetowe, postrzegana kontrola nad praktykami w zakresie cyberbezpieczeństwa lub przekonanie, że istniejące zasoby wewnętrzne są wystarczające, aby zaspokoić ich potrzeby w zakresie cyberbezpieczeństwa. Ta sytuacja sprawia, że projekt CyberAgent jest bardzo istotny, jeśli chodzi o wyposażenie pracownika w podstawowe umiejętności i wiedzę.

60 firm zgłosiło zatrudnienie usług zewnętrznych do zadań związanych z cyberbezpieczeństwem. Ta grupa prawdopodobnie dostrzega korzyści płynące z outsourcingu, takie jak dostęp do specjalistycznych umiejętności, bycie na bieżąco z najnowszymi zagrożeniami i środkami zaradczymi dla cyberbezpieczeństwa czy uzupełnianie swoich wewnętrznych możliwości. Decyzja o zatrudnieniu usług zewnętrznych może również odzwierciedlać zrozumienie złożoności zagrożeń cyberbezpieczeństwa, których zarządzanie w całości we własnym zakresie może stanowić wyzwanie, szczególnie w przypadku MŚP o ograniczonych zasobach.

Podział ten uwypukla rozbieżności w strategii cyberbezpieczeństwa wśród MŚP, utrzymując równowagę między zarządzaniem wewnętrznym a zewnętrznym outsourcingiem funkcji cyberbezpieczeństwa. Podkreśla znaczenie dostosowanego podejścia do cyberbezpieczeństwa, uznając, że różne organizacje mogą mieć różne potrzeby, możliwości i zasoby, które wpływają na ich decyzje dotyczące tego, czy szukać zewnętrznego wsparcia dla wysiłków w zakresie cyberbezpieczeństwa.

Skuteczność programów szkoleniowych

Odpowiedź	Liczba
1 (nieskuteczny)	8
2	38
3	79
4	39
5 (bardzo skuteczny)	11

Odpowiedzi dostarczają wglądu w spostrzeżenia dotyczące skuteczności obecnych programów szkoleniowych w przygotowaniu studentów do rzeczywistych wyzwań związanych z cyberbezpieczeństwem w MŚP. Większość respondentów, bo aż 79, oceniło skuteczność dotychczasowych programów szkoleniowych na „3”, co oznacza neutralną lub umiarkowaną ocenę ich efektywności. Sugeruje to, że chociaż istnieje pewien poziom zaufania do tych programów, istnieje również znaczne pole do poprawy. Odpowiedzi również wykazują tendencję do dolnego krańca skali, gdzie „2” otrzymało 38 punktów, co wskazuje na sceptycyzm co do skuteczności tych programów szkoleniowych. W skrajnych przypadkach „1” (nieskuteczne) otrzymało najmniejszą liczbę selekcji (8 zliczeń), a „5” (bardzo skuteczne) otrzymało nieco więcej (11 zliczeń). Oznacza to, że bardzo niewielu respondentów uważa obecne programy szkoleniowe za całkowicie nieskuteczne lub bardzo skuteczne w przygotowaniu studentów do wyzwań związanych z cyberbezpieczeństwem w MŚP. Zrównoważona liczba odpowiedzi dla „4” (39

punktów) sugeruje, że znaczna część uczestników postrzega programy szkoleniowe jako stosunkowo skuteczne, choć nie pozbawione znaczących ograniczeń. Chociaż obecne programy szkoleniowe zapewniają pewne przygotowanie do rzeczywistych wyzwań związanych z cyberbezpieczeństwem w MŚP, istnieje rozbieżność między zapewnianymi szkoleniami a potrzebami branży. Luka ta może wynikać z kilku czynników, takich jak tempo ewolucji zagrożeń cyberbezpieczeństwa, praktyczne zastosowanie umiejętności czy specyfika wyzwań stojących przed MŚP.

3 najważniejsze obszary szkoleń z zakresu cyberbezpieczeństwa

Kategoria	Liczba
Wykrywanie zagrożeń i reagowanie	102
Zarządzanie i analiza ryzyka	81
Reakcja na incydenty i odzyskiwanie	72
Prywatność i ochrona danych	68
Wiedza specjalistyczna w zakresie bezpieczeństwa w chmurze	51
Bezpieczeństwo sieci	46
Znajomość przepisów i zgodności	31
Pojawiające się technologie	24

Analiza odpowiedzi pokazuje, że „wykrywanie zagrożeń i reagowanie" jest uważane za najważniejszy obszar szkoleń w zakresie cyberbezpieczeństwa (102 punkty), co wskazuje na silne przekonanie o jego znaczeniu dla rozwiązywania rzeczywistych wyzwań związanych z cyberbezpieczeństwem w MŚP. Tuż za tym obszarem znajdują się „Zarządzanie ryzykiem i analiza ryzyka" oraz „Reagowanie na incydenty i ich usuwanie", z odpowiednio 81 i 72 punktami, co podkreśla wagę, jaką przywiązuje się do zrozumienia ryzyka i możliwości skutecznego reagowania na incydenty. „Prywatność i ochrona danych" również poświęcono znaczny nacisk, co odzwierciedla rosnące znaczenie przepisów o ochronie danych oraz potrzebę ochrony danych osobowych i wrażliwych w epoce cyfrowej. 51 respondentów uznało „ekspertyzę w zakresie bezpieczeństwa chmury" za kluczowy obszar, prawdopodobnie ze względu na rosnące wykorzystanie usług w chmurze i związane z nimi wyjątkowe wyzwania w zakresie bezpieczeństwa. Bezpieczeństwo sieci, z 46 punktami, pozostaje podstawową kwestią, co podkreśla potrzebę silnej ochrony przed zagrożeniami sieciowymi. „Zgodność z przepisami i wiedza regulacyjna" oraz „Nowe technologie" są postrzegane jako mniej ważne.

Kompetencje i wiedza

Obszar kompetencji i wiedzy	Niezbędny (%)	Wysoka potrzeba (%)	Umiarkowana potrzeba (%)	Niskie zapotrzebowanie (%)	Nie są potrzebne (%)
Prywatność i ochrona danych	38,29	38,29	13.14	10.29	0,00*
Ocena i zarządzanie ryzykiem	34,86	36.00	24.00	4,57	0,57
Reagowanie na incydenty i odzyskiwanie	33.14	38,86	19.43	8.00	0,57
Umiejętności komunikacyjne	32,57	35,43	22.29	8.00	1,71
Wiedza techniczna	30.29	32.00	26.29	8,57	2,86
Analiza zagrożeń i monitorowanie	29.71	37.14	24.00	8,57	0,57
Opracowywanie i wdrażanie polityki	24.00	37.14	24.00	12.57	2.29

*: Odsetek „Niepotrzebne” dla „Prywatności i ochrony danych” nie jest dostępny (NaN), co może wynikać z tego, że wszyscy respondenci rozważają ten obszar przynajmniej w pewnym stopniu, dlatego można go uznać za 0%.

W tabeli przedstawiono średnie wyniki dla każdego obszaru kompetencji i wiedzy, uzyskane na podstawie odpowiedzi z ankiet oceniających ich znaczenie w skali od 1 (niepotrzebne) do 5 (niezbędne). Wyniki te zapewniają ilościowy wgląd w to, jak respondenci ustalają priorytety dla różnych obszarów w danej dziedzinie.

Poniższa tabela przedstawia jasne zestawienie tego, jak respondenci cenią każdy obszar kompetencji i wiedzy. Obszary takie jak „Prywatność i ochrona danych” oraz „Ocena i zarządzanie ryzykiem” mają najwyższy odsetek ocen „Niezbędnych”, co odzwierciedla ich kluczowe znaczenie w tej dziedzinie. Natomiast „Opracowywanie i wdrażanie polityki” wykazuje szerszy rozkład odpowiedzi, wskazując na bardziej zróżnicowane postrzeganie jej znaczenia. Wyniki podkreślają duży nacisk na wiedzę techniczną, świadomość zagrożeń i umiejętność reagowania na incydenty, a także kluczową potrzebę skutecznych praktyk w zakresie komunikacji i ochrony danych.

Pojawiające się zagrożenia cyberbezpieczeństwa

Pojawiające się zagrożenie cyberbezpieczeństwa	Częstotliwość
Phishing i inżynieria społeczna	105
Cyberataki oparte na sztucznej inteligencji	95
Ataki ransomware	90
Naruszenia bezpieczeństwa chmury	60
Zagrożenia deep-fake	57
Luki w zabezpieczeniach IoT	44
Zagrożenia wewnętrzne	31

Za najpilniejsze zagrożenia uznaje się phishing i socjotechnikę, przy czym dużą uwagę poświęca się także cyberatakom wykorzystującym sztuczną inteligencję i atakom ransomware. Sugeruje to dużą świadomość wśród MŚP konieczności ochrony zarówno przed tradycyjnymi, jak i pojawiającymi się zagrożeniami cybernetycznymi. Zwrócono także uwagę na naruszenia bezpieczeństwa chmury i zagrożenia typu deep fake, co odzwierciedla obawy dotyczące bezpieczeństwa usług w chmurze i potencjalnego niewłaściwego wykorzystania sztucznej inteligencji. Identyfikowane są również luki w zabezpieczeniach IoT i zagrożenia wewnętrzne, chociaż postrzega się je jako mniej nieuchronne niż inne kategorie. W szczególności istnieją odpowiedzi wskazujące, że niektórzy respondenci nie mają pewności co do konkretnych zagrożeń lub nie mają pomysłów na poziomie swojej działalności, co sugeruje potencjalną lukę w świadomości lub obawy dotyczące konkretnych pojawiających się zagrożeń wśród niektórych MŚP.

Luka w wiedzy lub umiejętnościach dotyczących cyberbezpieczeństwa

Luka w wiedzy lub umiejętnościach dotyczących cyberbezpieczeństwa	Częstotliwość
Niski poziom świadomości zagrożeń	105
Niski poziom regularnych szkoleń z zakresu cyberbezpieczeństwa	88
Niski poziom oceny podatności	80
Niski poziom umiejętności technicznych	71
Niski poziom zrozumienia zasad i przepisów	50
Niski poziom umiejętności miękkich	37

Najbardziej znaczące luki w wiedzy lub umiejętnościach dotyczących cyberbezpieczeństwa wśród pracowników dotyczą świadomości zagrożeń, regularnych szkoleń z zakresu cyberbezpieczeństwa, oceny podatności, umiejętności technicznych oraz zrozumienia polityki i przepisów. Częstotliwość tych odpowiedzi uwypukla kluczową potrzebę kompleksowej edukacji i szkoleń w zakresie cyberbezpieczeństwa, które dotyczą tych konkretnych obszarów. Najbardziej znaczącą luką jest świadomość zagrożeń, która wskazuje, że pracownicy mogą nie być w pełni świadomi zagrożeń cyberbezpieczeństwa, które mogą mieć wpływ na ich organizację. Ta luka podkreśla znaczenie doskonalenia programów i szkoleń uświadamiających, aby pomóc pracownikom skuteczniej rozpoznawać potencjalne zagrożenia. Za lukę

postrzegane są również regularne szkolenia z zakresu cyberbezpieczeństwa, co wskazuje na potrzebę ciągłej edukacji i aktualizacji na temat najnowszych praktyk i zagrożeń w zakresie cyberbezpieczeństwa, a nie jednorazowych sesji szkoleniowych.

Pojawiające się trendy

Pojawiające się trendy w szkoleniach z zakresu cyberbezpieczeństwa	Częstotliwość
Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie	134
Tożsamość cyfrowa i prywatność	108
Etyczne hakowanie i umiejętności obronne	86
Skoncentrowanie się na umiejętnościach miękkich i szkoleniach interdyscyplinarnych	54
Zagrożenia związane z komputerami kwantowymi	39
Zdecentralizowane systemy bezpieczeństwa (np. Blockchain)	28

Analiza pokazuje wyraźny nacisk na sztuczną inteligencję i uczenie maszynowe w cyberbezpieczeństwie jako najbardziej oczekiwany trend na najbliższe pięć lat. Wskazuje to na rosnące uznanie roli zaawansowanych technologii we wzmacnianiu obrony cyberbezpieczeństwa i opracowywaniu nowych rozwiązań w zakresie bezpieczeństwa. Wysoka częstotliwość odpowiedzi w tej kategorii sugeruje, że programy szkoleniowe będą w coraz większym stopniu musiały uwzględniać elementy sztucznej inteligencji i uczenia maszynowego, aby przygotować specjalistów ds. cyberbezpieczeństwa na przyszłość. Tożsamość cyfrowa i prywatność wyłaniają się jako drugi najbardziej oczekiwany trend, podkreślając obawy związane z ochroną danych osobowych i zarządzaniem tożsamościami cyfrowymi w świecie w coraz większym stopniu internetowym. Tendencja ta sugeruje zapotrzebowanie na szkolenia obejmujące złożoność przepisów dotyczących prywatności, technik ochrony danych i rozwiązań do zarządzania tożsamością. Jako trzeci kluczowy trend uznano etyczny hacking i umiejętności obronne, odzwierciedlające znaczenie proaktywnych strategii obronnych w cyberbezpieczeństwie. Nacisk na etyczne hakowanie pokazuje zwrot w kierunku szkoleń, które umożliwiają specjalistom ds. cyberbezpieczeństwa myślenie jak atakujący, aby lepiej chronić swoje organizacje.

Adekwatność programów szkoleniowych

Odpowiedź	Częstotliwość
Tak	81
Niepewny	65
NIE	29

Analiza pytania, które badało poglądy respondentów na temat adekwatności obecnych programów szkoleniowych w zakresie cyberbezpieczeństwa, ujawnia mieszaną perspektywę wśród uczestników. Znaczna część, stanowiąca większość respondentów, uważa, że obecne

programy szkoleń z zakresu cyberbezpieczeństwa są odpowiednie, na co wskazują odpowiedzi „Tak". Sugeruje to, że wiele osób uważa, że dostępne obecnie szkolenia odpowiadają potrzebom ich organizacji lub są zgodne z ich oczekiwaniami co do tego, co powinno obejmować szkolenie w zakresie cyberbezpieczeństwa. Jednakże znaczna liczba respondentów „nie jest pewna" co do adekwatności obecnych programów szkoleniowych, podkreślając pewien stopień niepewności lub braku informacji na temat dostępnych opcji szkoleniowych lub ich skuteczności w stawianiu czoła bieżącym wyzwaniom w zakresie cyberbezpieczeństwa. Tę niepewność można przypisać zmieniającemu się charakterowi zagrożeń cybernetycznych i trudnościom w aktualizowaniu programów szkoleniowych w oparciu o najnowsze osiągnięcia w tej dziedzinie. Odpowiedzi „Nie", choć reprezentują najmniejszą grupę, wskazują na wyraźną obawę, że istniejące programy szkoleniowe nie są wystarczające, aby sprostać bieżącym potrzebom w zakresie cyberbezpieczeństwa. Grupa ta może dostrzec luki w zakresie szkolenia dotyczącym pojawiających się zagrożeń, technologii lub metodologii.

Inkluzywność programów szkoleniowych

Odpowiedź	Częstotliwość
Tak	81
Niepewny	65
NIE	29

Analiza odpowiedzi wskazuje na zróżnicowane spojrzenie na inkluzywność obecnych programów szkoleniowych z zakresu cyberbezpieczeństwa w aspekcie płci. Wielu respondentów uważa, że obecne szkolenia mają charakter włączający i skutecznie zaspokajają potrzeby wszystkich płci, na co wskazują odpowiedzi „Tak". Sugeruje to, że znaczna część społeczności zajmującej się cyberbezpieczeństwem uważa, że obecne wysiłki szkoleniowe przyczyniają się do inkluzywności i równości płci. Jednak duża liczba respondentów „nie ma pewności" co do włączającego charakteru tych programów, co wskazuje na znaczną niepewność lub brak świadomości w zakresie włączania płci w szkoleniach z zakresu cyberbezpieczeństwa. Odpowiedź ta może uwypuklić lukę w komunikacji pomiędzy organizatorami szkoleń a uczestnikami lub zasugerować, że wysiłki na rzecz włączania mogą nie być tak widoczne lub skuteczne, jak zamierzono. Odpowiedzi „Nie" reprezentujące najmniejszą grupę wśród respondentów podkreślają jednak krytyczną obawę, że obecne szkolenia z zakresu cyberbezpieczeństwa w niewystarczającym stopniu uwzględniają potrzeby wszystkich płci. Informacje zwrotne wskazują na lukę w wysiłkach na rzecz włączenia społecznego w ramach programów szkoleniowych w zakresie cyberbezpieczeństwa, co sugeruje, że potrzeba więcej pracy, aby zapewnić, że programy te będą przyjazne i dostosowane do potrzeb osób bez względu na tożsamość płciową.

3.2. PREFERENCJE I POTRZEBY SZKOLENIOWE

Na podstawie wyników badań terenowych, poniżej znajduje się opis zidentyfikowanych cech i potrzeb szkoleniowych, preferencji edukacyjnych, szkoleń i wsparcia kobiet zaangażowanych w cyberbezpieczeństwo

Identyfikacja potrzeb szkoleniowych:

Obszar 1 – Podstawowa wiedza i umiejętności

Priorytet w edukacji o cyberbezpieczeństwie. Zwłaszcza tematy takie jak podstawy cyberbezpieczeństwa i bezpieczeństwo sieci. Istnieją znaczne luki w obszarach takich jak wykrywanie i reagowanie na zagrożenia, wiedza specjalistyczna w zakresie bezpieczeństwa chmury, reagowanie na incydenty i ich odzyskiwanie, prywatność i ochrona danych oraz zarządzanie ryzykiem i analiza. Programy szkoleniowe muszą uwzględniać te braki w umiejętnościach. Istnieje także duże zapotrzebowanie na cyberbezpieczeństwo treści przeznaczonych dla MŚP.

Obszar 2 – Tematy specjalistyczne

Wymaga to szkoleń obejmujących szerokie spektrum zagrożeń i środków zaradczych dla cyberbezpieczeństwa. Podkreślono niektóre specjalistyczne tematy, takie jak analiza zagrożeń i zarządzanie nimi, kryptografia i zaawansowane techniki łagodzenia zagrożeń. Szkolenia powinny obejmować treści dotyczące najczęściej wymienianych pojawiających się zagrożeń, w tym cyberataków opartych na sztucznej inteligencji, ataków oprogramowania ransomware, phishingu i inżynierii społecznej, naruszeń bezpieczeństwa chmury oraz luk w zabezpieczeniach IoT.

Obszar 3 – Zastosowanie praktyczne

Preferowanie metod nauczania, takich jak laboratoria praktyczne, studia przypadków i projekty grupowe, podkreśla znaczenie praktycznego, interaktywnego i rzeczywistego zastosowania w szkoleniach z zakresu cyberbezpieczeństwa.

Aktualne praktyki:

Jeśli chodzi o metodę nauczania, możemy zauważyć wykorzystanie różnych praktyk, takich jak studia przypadków, projekty grupowe, laboratoria praktyczne i wykłady. W obecnych programach szkoleniowych istnieje mieszanka podejść teoretycznych i praktycznych.

Obecne programy szkoleniowe obejmują szereg tematów związanych z cyberbezpieczeństwem, przy czym priorytetowo traktowane są przedmioty podstawowe. Jednakże w niektórych programach zauważalny jest brak treści specyficznych dla MŚP.

Jeśli chodzi o włączenie społeczne i równowagę płci, w niektórych programach wdrożono inicjatywy mające na celu zwiększenie udziału kobiet i utworzenie środowisk szkoleniowych włączających płeć, chociaż wysiłki te wydają się być mniejszościowe.

Wyzwania:

Główne wyzwania stojące przed edukacją o cyberbezpieczeństwie to:

- Dostosowanie szkolenia do różnych środowisk i poziomów wiedzy specjalistycznej jest wyzwaniem, ponieważ istnieje różnorodność umiejętności i doświadczenia
- Dbanie o aktualność materiałów szkoleniowych w celu radzenia sobie z szybką ewolucją zagrożeń cyberbezpieczeństwa. Wymaga to ciągłej aktualizacji materiałów szkoleniowych.
- Ograniczenia w zakresie szkolenia praktycznego wynikające z ograniczeń w zapleczu laboratoryjnym, możliwości symulacji w świecie rzeczywistym oraz tworzenia realistycznych scenariuszy cyberataków do celów praktycznych
- Utrzymanie zaangażowania i motywacji uczniów, szczególnie w przypadku złożonych treści technicznych, jest trudne.
- Wyzwaniem jest dostosowanie przemysłu i edukacji do równoważenia podstaw teoretycznych z umiejętnościami praktycznymi odpowiadającymi potrzebom przemysłu.

Sugestia dotycząca rozwoju szkolenia:

- Dopasowanie szkoleń do potrzeb MŚP: integrowanie tematów i umiejętności specjalnie zaprojektowanych w celu zaspokojenia potrzeb MŚP w zakresie cyberbezpieczeństwa.
- Poprawa praktycznego zastosowania poprzez rozszerzenie stosowania praktycznych, interaktywnych metod nauczania w celu poprawy umiejętności praktycznych i gotowości do działania w świecie rzeczywistym.
- Uwzględnianie nowych trendów, takich jak sztuczna inteligencja i uczenie maszynowe, tożsamość cyfrowa i prywatność oraz etyczne hakowanie. Obecnie uważa się je za kluczowe obszary, na których w przyszłości skupią się programy szkoleniowe.
- Rozwiązanie problemu niedoborów umiejętności poprzez skupienie się na obszarach, w których brakuje pracowników, takich jak wykrywanie i reagowanie na zagrożenia, bezpieczeństwo w chmurze i reagowanie na incydenty, aby lepiej przygotować ich do stawienia czoła wyzwaniom i stać się skutecznym i odpornym CyberAgentem.
- Opracowanie inicjatyw na rzecz różnorodności płci, aby zwiększyć udział kobiet poprzez ukierunkowane inicjatywy, mentoring i wzorce do naśladowania.

4. PROFIL KWALIFIKACJI AGENTA ZMIANY CYBERBEZPIECZEŃSTWA MŚP

W oparciu o wyniki badań biurowych i terenowych, oto przykład oczekiwanego zestawu wiedzy, umiejętności i kompetencji CyberAgenta. Wyniki te określają oczekiwane osiągnięcia uczestników na koniec odpowiednich programów szkoleniowych w zakresie cyberbezpieczeństwa, zapewniając rozwój od podstawowej wiedzy i umiejętności na poziomie 4/5 EQF do bardziej zaawansowanych i zorientowanych na przywództwo umiejętności na poziomie 6 EQF.

Profil kwalifikacyjny CyberAgent	Wiedza	Umiejętności	Kompetencje
Na poziomie 4/5 EQF	**Podstawy cyberbezpieczeństwa** - Podstawowe pojęcia z zakresu cyberbezpieczeństwa - Rodzaje zagrożeń cybernetycznych (phishing, ransomware, ataki ddos), wektory ataków - Znaczenie cyberbezpieczeństwa w ochronie majątku organizacji. **Ramy prawne i ramy danych dotyczące cyberbezpieczeństwa** - Przepisy, standardy i wymagania dotyczące bezpieczeństwa cybernetycznego - Strategie i polityki bezpieczeństwa informacji - Ochrona danych	**Bezpieczeństwo** - Identyfikacja potencjalnych zagrożeń i luk w zabezpieczeniach cyberbezpieczeństwa - Korzystanie z narzędzi i oprogramowania zapewniającego cyberbezpieczeństwo, aby chronić się przed zagrożeniami cybernetycznymi - Promowanie praktyczne stosowanie podstawowych praktyk w zakresie cyberbezpieczeństwa, bezpiecznego tworzenia haseł, bezpiecznego przeglądania, bezpieczeństwa poczty elektronicznej i bezpiecznego obchodzenia się z wrażliwymi danymi	**Zarządzanie ryzykiem i jego ograniczanie** - Ocenianie i łagodzenie potencjalnych zagrożeń bezpieczeństwa **Skuteczna komunikacja w kwestiach cyberbezpieczeństwa** - Umiejętność skutecznego komunikowania się w kwestiach związanych z cyberbezpieczeństwem, - Zgłaszanie zagrożeń i naruszeń do odpowiednich kanałów w organizacji.

	- Zasady zarządzania ryzykiem		
Na poziomie 6 EQF	**Zaawansowane koncepcje cyberbezpieczeństwa** - Zrozumienie zaawansowanych zasad cyberbezpieczeństwa, w tym wyrafinowanych zagrożeń cybernetycznych i wektorów ataków, - Świadomość najnowszych trendów w zakresie zagrożeń cyberbezpieczeństwa i mechanizmów obronnych. **Przepisy dotyczące cyberbezpieczeństwa i ich zgodność** - Znajomość krajowych i międzynarodowych przepisów, standardów i wymogów dotyczących bezpieczeństwa cybernetycznego, a także innych istotnych dla ich konkretnej branży.	**Zaawansowana ocena i zarządzanie ryzykiem** - Umiejętność przeprowadzania kompleksowych ocen ryzyka - Stosowanie zaawansowanych metodologii i narzędzi - Projektowanie i wdrażanie skutecznych strategii zarządzania ryzykiem w celu minimalizacji zidentyfikowanych ryzyk. **Specjalizacja w architekturze bezpieczeństwa i obronie sieci** - Projektowanie, wdrażanie i ocenianie bezpiecznej architektury sieciowej, w tym wykorzystanie zapór sieciowych, systemów wykrywania włamań (id) i systemów zapobiegania włamaniom (ips). **Reakcja na incydenty i odzyskiwanie** - Umiejętność przygotowania się na incydenty	**Planowanie i rozwój polityki** - Umiejętność opracowywania i wdrażania strategicznych polityk i ram cyberbezpieczeństwa zgodnych z celami organizacji i zobowiązaniami dotyczącymi zgodności. **Przywództwo w inicjatywach związanych z cyberbezpieczeństwem** - Kierowanie i zarządzanie projektami i zespołami zajmującymi się cyberbezpieczeństwem, w tym umiejętność inspirowania i wspierania pracowników we wdrażaniu strategii cyberbezpieczeństwa. **Podejmowanie decyzji** - Podejmowanie etycznych decyzji dotyczących praktyk w zakresie cyberbezpieczeństwa

		cyberbezpieczeństwa, reagowania na nie i odzyskiwania danych po nich, - Opracowywanie planów odzyskiwania i ciągłości działania.	

Na poziomie 4/5 EQF możliwe efekty uczenia się mogą być następujące:

- Uczestnicy poznają podstawowe pojęcia cyberbezpieczeństwa, w tym podstawową terminologię, rodzaje zagrożeń cybernetycznych, takich jak phishing, oprogramowanie ransomware i ataki DDoS, a także odpowiadające im wektory ataków.
- Uczestnicy kursu będą potrafili zidentyfikować potencjalne zagrożenia i luki w zabezpieczeniach cyberbezpieczeństwa, korzystać z odpowiednich narzędzi i oprogramowania, aby złagodzić te zagrożenia oraz wdrożyć podstawowe praktyki cyberbezpieczeństwa, takie jak bezpieczne tworzenie haseł i bezpieczne przeglądanie.
- Uczestnicy zdobędą wiedzę na temat przepisów prawnych, standardów i wymogów dotyczących bezpieczeństwa cybernetycznego, a także strategii i zasad dotyczących bezpieczeństwa informacji i zarządzania ryzykiem w organizacji.
- Uczestnicy kursu rozwiną kompetencje skutecznej oceny i łagodzenia potencjalnych zagrożeń bezpieczeństwa oraz jasnego i skutecznego komunikowania kwestii cyberbezpieczeństwa w organizacji, w tym zgłaszania zagrożeń i naruszeń odpowiednimi kanałami.

Na poziomie 6 EQF możliwymi efektami uczenia się mogą być:

- Uczestnicy kursu rozwiną zaawansowaną wiedzę na temat zasad cyberbezpieczeństwa, w tym umiejętność identyfikowania wyrafinowanych zagrożeń cybernetycznych i wektorów ataków, a także będą na bieżąco informowani o najnowszych trendach w zakresie zabezpieczeń cybernetycznych.
- Uczniowie zdobędą wszechstronną wiedzę na temat krajowych i międzynarodowych przepisów, standardów i wymagań dotyczących bezpieczeństwa cybernetycznego, dostosowując tę wiedzę do specyficznych potrzeb swojej branży.
- Uczniowie będą mogli przeprowadzać szczegółowe oceny ryzyka przy użyciu zaawansowanych metodologii i narzędzi oraz opracowywać skuteczne strategie zarządzania ryzykiem w celu ograniczenia tego ryzyka.
- Uczestnicy będą projektować, wdrażać i oceniać bezpieczne architektury sieciowe, w tym opanowywać wykorzystanie kluczowych technologii bezpieczeństwa, takich jak zapory ogniowe, IDS i IPS.
- Uczestnicy kursu będą biegli w planowaniu i wykonywaniu strategii reagowania na incydenty i odzyskiwania danych, zapewniając odporność organizacji poprzez skuteczne plany odzyskiwania i ciągłości działania.

- Uczestnicy kursu wykażą się przywództwem w dziedzinie cyberbezpieczeństwa, opracowując strategie, zarządzając projektami i zespołami zajmującymi się cyberbezpieczeństwem oraz podejmując świadome, etyczne decyzje pod presją.

5. ZAŁĄCZNIKI

5.1. ZAŁĄCZNIK A: LISTA PRZEGLĄDANEJ LITERATURY

Przegląd edukacji w zakresie cyberbezpieczeństwa w ramach kształcenia i szkolenia zawodowego i szkolnictwa wyższego

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj- napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4gNukWMvDPXICf62FqF
14. Analiza i diagnoza talentów w zakresie cyberbezpieczeństwa w Hiszpanii, marzec 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías Disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama aktualna de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de Competencias Digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan digitalizacji PYMES na lata 2021–2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020 z 7 kwietnia, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspektos básicos del currículo https://www.boe.es/diario_boe/ txt.php?id=BOE-A-2020-4963

Wyzwania związane z cyberbezpieczeństwem i potrzeby branży

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (koordynator). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país podatne, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana /**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 marca 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Analiza i diagnoza talentów w zakresie cyberbezpieczeństwa w Hiszpanii, marzec 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías Disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Aktualna panorama Ciberseguridad w Hiszpanii **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Plan España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**

10. Plan digitalizacji PYMES na lata 2021–2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
11. https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
12. http://data.europa.eu/esco/ockupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Kobiety w cyberbezpieczeństwie

1. Microsoftu. (2017, marzec). Dlaczego dziewczęta w Europie nie uczą się przedmiotów STEM. Wiadomości Microsoftu. Pobrano 20 stycznia 2024 r. z https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Kobiety wybierają technologię. (2021, wrzesień). Pracownicy ICT w Europie i wyzwania związane z płcią po Covid-19. Kobiety wybierają technologię. Pobrano 20 stycznia 2024 r. z https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (nd) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius i Lepaite. (2022, 5 sierpnia). Ataskaita Lietuvos kibernetinio saugumo kompetenciju žemelapis. Uniwersytet Wileński. Pobrano 20 stycznia 2024 r. z https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (koordynatorka). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas en ciencia y tecnología (reparto por sektores). Hiszpania, UE-27 i UE-28. Seria 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 marca 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Analiza i diagnoza talentów cyberbezpieczeństwa w Hiszpanii, marzec 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías Disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama aktualna de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. ZAŁĄCZNIK B: KWESTIONARIUSZ ANKIETY

Kwestionariusz VET i HEI

Ankieta ta ma na celu zebranie informacji na temat obecnego stanu i przyszłych potrzeb szkoleń z zakresu cyberbezpieczeństwa oraz pomoc w kształtowaniu skutecznego programu szkoleniowego z zakresu cyberbezpieczeństwa dostosowanego do wyzwań związanych z cyberbezpieczeństwem dla małych i średnich przedsiębiorstw (MŚP).

Ankieta podzielona jest na 4 sekcje:

- Demografia
- Program nauczania, potrzeby szkoleniowe i preferencje edukacyjne
- Wymagania kompetencyjne i przyszłe umiejętności
- Spostrzeżenia dotyczące płci

Wypełnienie ankiety zajmie około 8 minut.

DEMOGRAFIA

Z jakiego kraju pochodzisz?
▫ Litwa
▫ Belgia
▫ Norwegia
▫ Turcja
▫ Finlandia
▫ Rumunia
▫ Hiszpania
▫ Polska

W której placówce szkolnej obecnie uczysz?
▫ VET (kształcenie i szkolenie zawodowe)
▫ HEI (instytucja szkolnictwa wyższego)

Jaka jest twoja płeć?
▫ Mężczyzna
▫ Kobieta
▫ Wolę nie mówić

Od ilu lat zajmujesz się szkoleniami z zakresu cyberbezpieczeństwa?
▫ Mniej niż 1 rok
▫ 1-5 lat
▫ 6-10 lat
▫ Ponad 10 lat

PROGRAM NAUCZANIA, POTRZEBY SZKOLENIA I PREFERENCJE UCZENIA SIĘ

Które z poniższych tematów są uwzględnione w Twoim programie szkoleniowym z zakresu cyberbezpieczeństwa? (Wybierz wszystkie, które mają zastosowanie)

▫ Podstawy cyberbezpieczeństwa
▫ Analiza zagrożeń i zarządzanie nimi
▫ Zaawansowane techniki łagodzenia zagrożeń
▫ Kryptografia
▫ Bezpieczeństwo sieci
▫ Przepisy i zasady dotyczące cyberbezpieczeństwa
▫ Zarządzanie ryzykiem
▫ Reagowanie na incydenty
▫ Inne: _____

Jakich metod nauczania używasz przede wszystkim podczas szkoleń z zakresu cyberbezpieczeństwa? (Wybierz wszystkie, które mają zastosowanie)

▫ Wykłady
▫ Laboratoria praktyczne
▫ Studia przypadków
▫ Projekty grupowe
▫ Symulacje online
▫ Odwrócona klasa
Inny: _____

Jakie formaty nauczania byłyby najskuteczniejsze w przypadku szkoleń z zakresu cyberbezpieczeństwa? (Wybierz wszystkie, które mają zastosowanie)

▫ Warsztaty stacjonarne
▫ Kursy online
▫ Seminaria internetowe
▫ Interaktywne symulacje
▫ Samouczki wideo
▫ Praktyczne sesje praktyczne
▫ Inne: _____

Jakie są największe wyzwania, przed którymi stoisz, prowadząc skuteczne szkolenia z zakresu cyberbezpieczeństwa?

Pytanie otwarte

W skali od 1 do 5, jak skutecznie, Twoim zdaniem, obecne programy szkoleniowe przygotowują studentów do rzeczywistych wyzwań związanych z cyberbezpieczeństwem MŚP?

▫ Bardzo nieskuteczne
▫ Raczej nieskuteczne
▫ Neutralny
▫ Raczej skuteczne
▫ Bardzo skuteczny

Jak dobrze według Ciebie obecne szkolenia w zakresie cyberbezpieczeństwa odpowiadają konkretnym potrzebom MŚP?

1 (niewyrównany)
2 (Lekko wyrównane)

3 (wyrównane)
4 (Dobrze wyrównane)
5 (wysoce wyrównane)

Czy są jakieś konkretne tematy lub umiejętności, które uwzględniasz w swoim szkoleniu, aby zaspokoić wyjątkowe potrzeby MŚP w zakresie cyberbezpieczeństwa? (Wybierz wszystkie, które mają zastosowanie)

▫ Podstawowe cyberbezpieczeństwo dla MŚP
▫ Ocena i zarządzanie ryzykiem w kontekście MŚP
▫ Reagowanie na incydenty dla MŚP
▫ Ochrona danych i prywatność dla MŚP
▫ Rozwój Polityki Cyberbezpieczeństwa dla MŚP
▫ Inne: _____

Jak często adaptujesz lub dostosowujesz swoje szkolenia z zakresu cyberbezpieczeństwa, aby lepiej zaspokoić potrzeby MŚP?

▫ Zawsze
▫ Często
▫ Czasami
▫ Rzadko
▫ Nigdy

Czy otrzymujesz informację zwrotną lub kontaktujesz się z przedstawicielami MŚP lub specjalistami, aby upewnić się, że treść Twojego szkolenia odpowiada ich potrzebom?

▫ Tak, regularnie
▫ Czasami
▫ Rzadko
▫ Nigdy

Na podstawie swojego doświadczenia, jak myślisz, jak skuteczne jest obecne szkolenie z zakresu cyberbezpieczeństwa w wyposażaniu specjalistów z MŚP do radzenia sobie z wyzwaniami związanymi z cyberbezpieczeństwem?

▫ Bardzo nieskuteczne
▫ Raczej nieskuteczne
▫ Neutralny
▫ Raczej skuteczne
▫ Bardzo skuteczny

Jakie masz sugestie dotyczące poprawy przydatności i skuteczności szkoleń z zakresu cyberbezpieczeństwa dla MŚP?

Pytanie otwarte

<u>WYMAGANIA KOMPETENCYJNE I PRZYSZŁE UMIEJĘTNOŚCI</u>

Jakie są Twoim zdaniem największe braki umiejętności wśród obecnych pracowników MŚP zajmujących się cyberbezpieczeństwem? (Wybierz maksymalnie trzy)

▫ Wykrywanie i reagowanie na zagrożenia

▫ Specjalizacja w zakresie bezpieczeństwa w chmurze
▫ Znajomość przepisów i przepisów
▫ Reagowanie na incydenty i usuwanie skutków
▫ Zarządzanie i analiza ryzyka
▫ Prywatność i ochrona danych
▫ Nowe technologie
▫ Bezpieczeństwo sieci

Proszę ocenić w skali od 1 (niepotrzebne) do 5 (bardzo potrzebne) kompetencje i zapotrzebowanie na wiedzę:

	Ocena
Ocena i zarządzanie ryzykiem Zrozumienie rodzajów ryzyka i skutków.	
Wiedza techniczna Techniczne aspekty cyberbezpieczeństwa oraz znajomość systemów operacyjnych, sieci i zarządzania bazami danych.	
Reagowanie na incydenty i odzyskiwanie Identyfikowanie, reagowanie i usuwanie naruszeń i incydentów bezpieczeństwa.	
Opracowywanie i wdrażanie polityki Opracowywanie i wdrażanie skutecznych polityk i praktyk bezpieczeństwa.	
Analiza zagrożeń i monitorowanie Bycie na bieżąco z najnowszymi trendami, zagrożeniami i metodami ataków w cyberbezpieczeństwie.	
Umiejętności komunikacyjne Skuteczna komunikacja z personelem, kierownictwem i ewentualnie klientami w kwestiach związanych z cyberbezpieczeństwem.	
Prywatność i ochrona danych Zasady ochrony danych i sposoby ochrony informacji wrażliwych.	

Czy dostrzegasz jakiś odpowiedni zestaw umiejętności i wiedzy niewymieniony w poprzednim pytaniu, który mógłby być bardzo potrzebny MŚP?
Pytanie otwarte
Na jakie pojawiające się zagrożenia cyberbezpieczeństwa Twoim zdaniem MŚP muszą być przygotowane w ciągu najbliższych 5 lat? (Wybierz maksymalnie trzy)
▫ Ataki ransomware
▫ Luki w zabezpieczeniach IoT
▫ Naruszenia bezpieczeństwa chmury
▫ Cyberataki oparte na sztucznej inteligencji
▫ Zagrożenia wewnętrzne
▫ Inne: _____

Jakie według Ciebie są 3 najważniejsze pojawiające się trendy w szkoleniach z zakresu cyberbezpieczeństwa na najbliższe 5 lat? (Wybierz maksymalnie 3 opcje)

▫ Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie
▫ Koncentrowanie się na umiejętnościach miękkich i szkoleniach interdyscyplinarnych
▫ Zagrożenia związane z obliczeniami kwantowymi
▫ Etyczne umiejętności hakerskie i obronne
▫ Tożsamość cyfrowa i prywatność
▫ Zdecentralizowane systemy bezpieczeństwa (np. Blockchain)
▫ Inne: _____

Czy są jakieś szczególne metody, narzędzia lub platformy szkoleniowe, które Twoim zdaniem są wyjątkowo skuteczne w edukacji w zakresie cyberbezpieczeństwa?

Pytanie otwarte

Jakieś dodatkowe uwagi lub sugestie dotyczące ulepszenia szkoleń z zakresu cyberbezpieczeństwa dla MŚP?

Pytanie otwarte

WNIOSKI DOTYCZĄCE PŁCI

Jaki jest szacunkowy odsetek kobiet wśród uczestniczek Państwa programów szkoleniowych z zakresu cyberbezpieczeństwa?

▫ Mniej niż 10%
▫ 10% - 25%
▫ 26% - 50%
▫ 51% - 75%
▫ Ponad 75%

Czy stosujecie jakieś konkretne inicjatywy lub strategie, aby zachęcić kobiety do udziału w szkoleniach z zakresu cyberbezpieczeństwa?

▫ Tak
▫ Nie

Jeśli tak, proszę podać: _____

Czy uważasz, że w zakresie cyberbezpieczeństwa dostępna jest wystarczająca liczba modułów szkoleniowych włączających płeć?

▫ Tak
▫ Nie
▫ Nie jestem pewien
▫ Nie dotyczy mnie

Z Twojego doświadczenia wynika, że jakie są główne bariery uniemożliwiające kobietom udział w szkoleniach i karierze w zakresie cyberbezpieczeństwa lub awansowanie w nich? (Wybierz wszystkie, które mają zastosowanie)

▫ Brak świadomości możliwości w zakresie cyberbezpieczeństwa
▫ Stereotypy lub normy kulturowe
▫ Brak mentoringu i wzorców do naśladowania

▫ Wyzwania dotyczące równowagi między życiem zawodowym a prywatnym
▫ Postrzegane uprzedzenia związane z płcią w branży
▫ Inne: _____

Czy Twoja instytucja posiada specjalne zasady lub programy promujące różnorodność i włączenie, zwłaszcza kobiet, w szkoleniach z zakresu cyberbezpieczeństwa?

▫ Tak
▫ Nie
▫ Nie jestem pewien

Co może sprawić, że szkolenia z zakresu cyberbezpieczeństwa będą bardziej włączające płeć? (Wybierz maksymalnie trzy)

▫ Więcej kobiet-instruktorów lub personelu szkoleniowego ds. cyberbezpieczeństwa
▫ Oferowanie stypendiów lub zachęt
▫ Treści szkoleniowe, które pozwalają uniknąć uprzedzeń związanych z płcią
▫ Większa widoczność kobiet odnoszących sukcesy specjalistek ds. cyberbezpieczeństwa
▫ Więcej sesji szkoleniowych tylko dla kobiet
▫ Studia przypadków i scenariusze uwzględniające płeć
▫ Indywidualne programy szkoleniowe
▫ Możliwości mentorskie
▫ Inne: _____

KWESTIONARIUSZ MŚP

Celem tej ankiety jest określenie potrzeb szkoleniowych agentów ds. zmian w zakresie bezpieczeństwa cybernetycznego MŚP. Twoje odpowiedzi pomogą w zrozumieniu obecnego stanu wiedzy i umiejętności w zakresie cyberbezpieczeństwa w różnych MŚP, zidentyfikowaniu luk w szkoleniach z zakresu cyberbezpieczeństwa oraz zwiększeniu skuteczności przyszłych programów szkoleniowych.

Ankieta podzielona jest na 3 sekcje:

- Demografia
- Potrzeby szkoleniowe
- Włączenie społeczne i potrzeby kobiet w zakresie cyberbezpieczeństwa.

Wypełnienie ankiety zajmie około 5 minut.

DEMOGRAFIA

Z jakiego kraju pochodzisz?

▫ Litwa
▫ Belgia
▫ Norwegia
▫ Turcja
▫ Finlandia
▫ Rumunia
▫ Hiszpania
▫ Polska

Jakie jest Twoje obecne stanowisko i dział w firmie?

Stanowisko: _____
Dział: _____

Jaka jest twoja płeć?

▫ Mężczyzna
▫ Kobieta
▫ Wolę nie mówić

Ilu pracowników pracuje w firmie?

▫ do 10 pracowników
▫ 11-50
▫ 51-250

Jak oceniłbyś obecny poziom wiedzy i umiejętności pracowników w zakresie cyberbezpieczeństwa?

▫ Początkujący
▫ Średnio zaawansowany
▫ Zaawansowane

Ilu pracowników wykonuje prace związane z cyberbezpieczeństwem?

Wstaw numer: _____

Czy zatrudniasz usługi zewnętrzne do prac związanych z cyberbezpieczeństwem?

▫ Tak
▫ Nie

POTRZEBY SZKOLENIOWE

W skali od 1 (nieskuteczne) do 5 (bardzo skuteczne), jak skutecznie, Twoim zdaniem, obecne programy szkoleniowe przygotowują studentów do rzeczywistych wyzwań związanych z cyberbezpieczeństwem MŚP?

1- Nieskuteczne
5- Bardzo skuteczny

Jakie są Twoim zdaniem największe braki umiejętności wśród obecnych pracowników MŚP zajmujących się cyberbezpieczeństwem? (Wybierz maksymalnie trzy)

▫ Wykrywanie i reagowanie na zagrożenia
▫ Doświadczenie w zakresie bezpieczeństwa w chmurze
▫ Znajomość przepisów i przepisów
▫ Reagowanie na incydenty i usuwanie skutków
▫ Zarządzanie i analiza ryzyka
▫ Prywatność i ochrona danych
▫ Nowe technologie
▫ Bezpieczeństwo sieci
▫ Inne: _____

Proszę ocenić w skali od 1 (niepotrzebne) do 5 (niezbędne) kompetencje i zapotrzebowanie na wiedzę:

	Ocena				
Ocena i zarządzanie ryzykiem Zrozumienie rodzajów ryzyka i skutków.					
Wiedza techniczna Techniczne aspekty cyberbezpieczeństwa oraz znajomość systemów operacyjnych, sieci i zarządzania bazami danych.					
Reagowanie na incydenty i odzyskiwanie Identyfikowanie, reagowanie i usuwanie naruszeń i incydentów bezpieczeństwa.					

Opracowywanie i wdrażanie polityki Opracowywanie i wdrażanie skutecznych polityk i praktyk bezpieczeństwa.					
Analiza zagrożeń i monitorowanie Bycie na bieżąco z najnowszymi trendami, zagrożeniami i metodami ataków w cyberbezpieczeństwie.					
Umiejętności komunikacyjne Skuteczna komunikacja z personelem, kierownictwem i ewentualnie klientami w kwestiach związanych z cyberbezpieczeństwem.					
Prywatność i ochrona danych Zasady ochrony danych i sposoby ochrony informacji wrażliwych.					

Czy dostrzegasz jakiś odpowiedni zestaw umiejętności i wiedzy niewymieniony w poprzednim pytaniu, który mógłby być bardzo potrzebny MŚP?
Pytanie otwarte

Na jakie pojawiające się zagrożenia cyberbezpieczeństwa Twoim zdaniem MŚP muszą być przygotowane w ciągu najbliższych 5 lat? (Wybierz maksymalnie trzy)
▫ Ataki ransomware
▫ Luki w zabezpieczeniach IoT
▫ Naruszenia bezpieczeństwa chmury
▫ Cyberataki oparte na sztucznej inteligencji
▫ Zagrożenia wewnętrzne
▫ Inne: _____

Jakie konkretne luki, jeśli w ogóle, Twoim zdaniem istnieją w obecnym stanie wiedzy lub umiejętności pracowników w zakresie cyberbezpieczeństwa?
▫ Niski poziom umiejętności technicznych
▫ Niski poziom umiejętności miękkich
▫ Niski poziom oceny podatności
▫ Niski poziom zrozumienia Polityki i przepisów
▫ Niski poziom świadomości zagrożeń
▫ Niski poziom regularnych szkoleń z zakresu cyberbezpieczeństwa
▫ Inne: _____

Jakie są według Ciebie 3 najważniejsze pojawiające się trendy w szkoleniach z zakresu cyberbezpieczeństwa na najbliższe 5 lat? (Wybierz maksymalnie 3 opcje)
▫ Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie
▫ Koncentrowanie się na umiejętnościach miękkich i szkoleniach interdyscyplinarnych
▫ Zagrożenia związane z obliczeniami kwantowymi
▫ Etyczne umiejętności hakerskie i obronne
▫ Tożsamość cyfrowa i prywatność
▫ Zdecentralizowane systemy bezpieczeństwa (np. Blockchain)
▫ Inne: _____

INKLUZYWNOŚĆ I POTRZEBY KOBIET W CYBERBEZPIECZEŃSTWIE

Czy uważasz, że obecne szkolenia z zakresu cyberbezpieczeństwa mają charakter włączający i skutecznie uwzględniają potrzeby wszystkich płci?

▫ Taka
▫ Nie
▫ Nie jestem pewien

Jeśli identyfikujesz się jako kobieta, czy napotkałaś jakieś bariery lub wyzwania w dostępie do szkoleń/studiów z zakresu cyberbezpieczeństwa lub uczestnictwie w nich?

▫ Tak
▫ Nie
▫ Wolę nie mówić
▫ Jeśli tak, proszę określić: _____

Czy znasz jakieś inicjatywy lub programy w Twojej organizacji, które konkretnie wspierają lub promują udział kobiet w cyberbezpieczeństwie?

▫ Tak
▫ Nie
▫ Nie jestem pewien

Jakie rodzaje wsparcia lub zasobów zachęciłyby więcej kobiet w Twojej organizacji do udziału w szkoleniach z zakresu cyberbezpieczeństwa? (Otwarty)

Pytanie otwarte

Jakie ulepszenia lub innowacje zasugerowałbyś w celu zwiększenia efektywności szkoleń z zakresu cyberbezpieczeństwa?

Pytanie otwarte

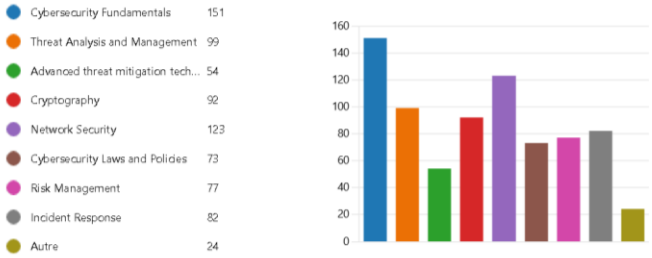
5.3. ZAŁĄCZNIK C: WYNIKI ANKIETY

kształcenie i szkolenie zawodowe

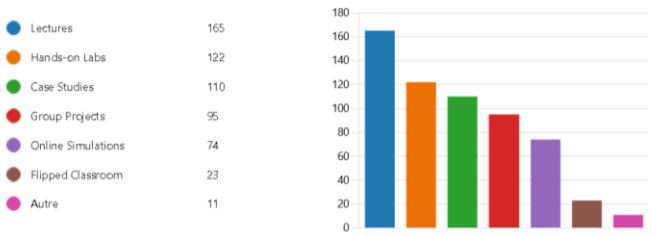
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

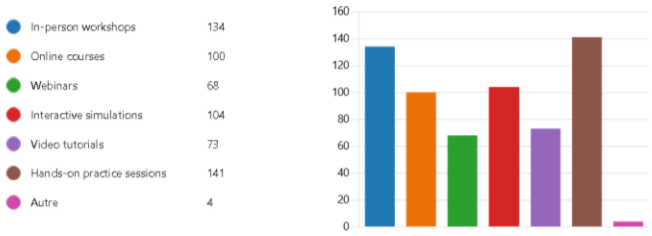
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

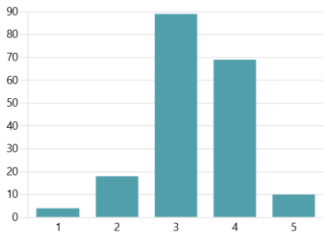
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

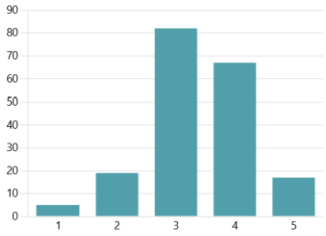
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



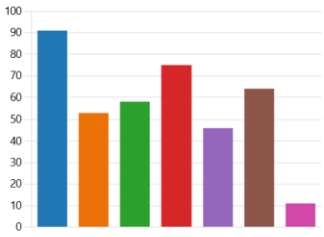
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

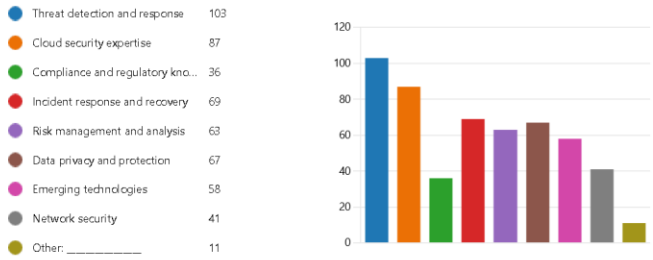
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

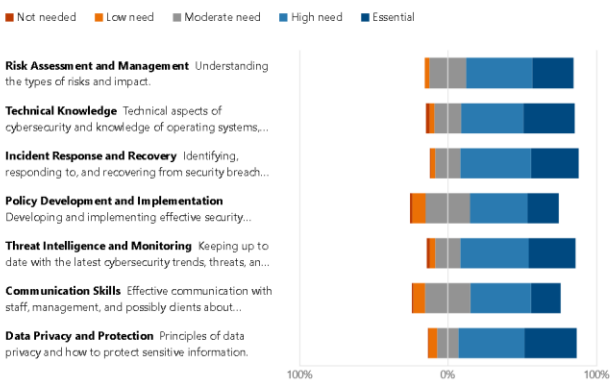
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

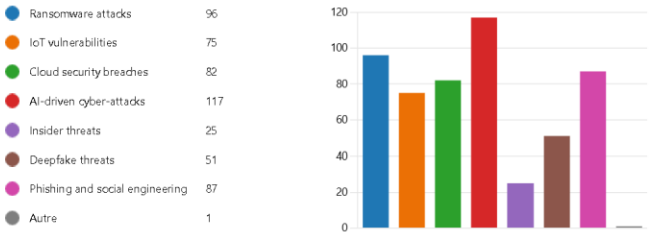
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

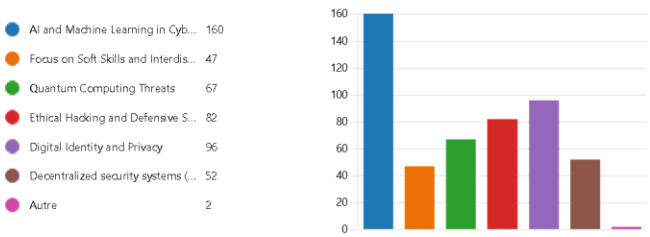
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

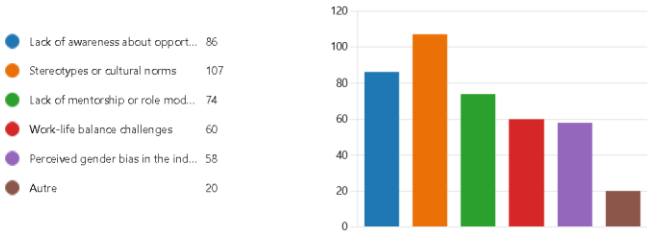
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

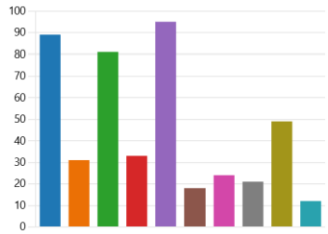
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

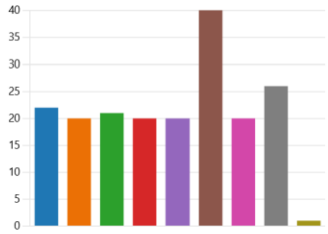
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

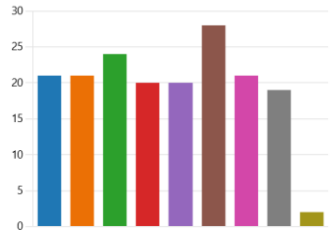
MŚP

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

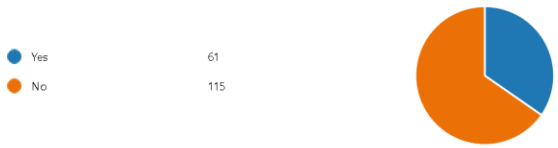
176
Réponses

Dernières réponses
"1"
"1"
"0"

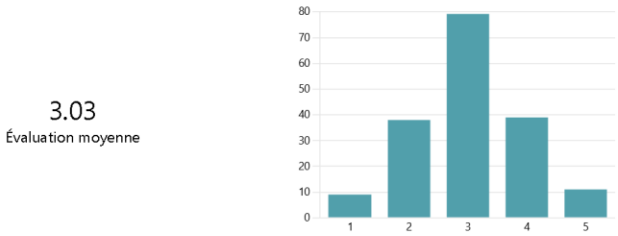
Mettre à jour

31 répondants (**18**%) répondu **1** pour cette question.

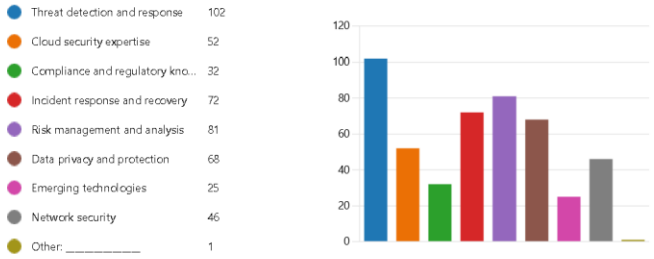
9. **Do you hire external services for cybersecurity work?**



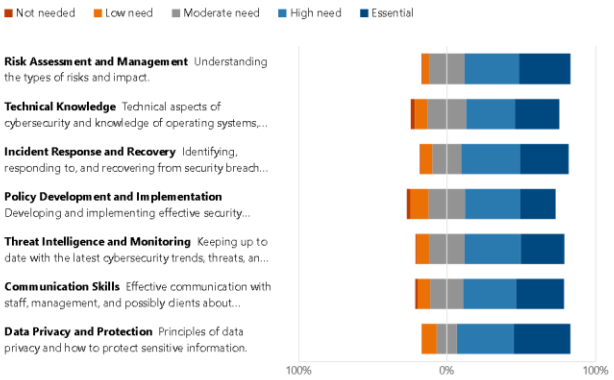
10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**



11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

Dernières réponses

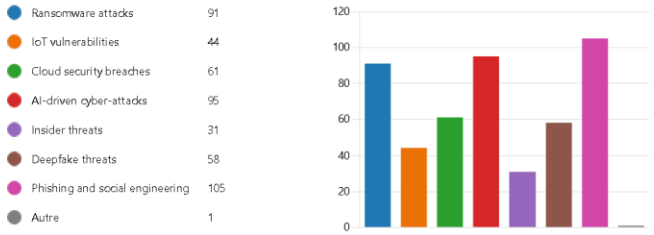
"My assumption is that Subject matter experts (SME's) in a big company are ...

"Cyber Security on all these topics arround Generative AI - which is complete...

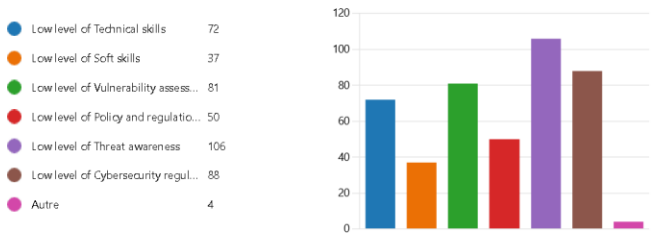
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

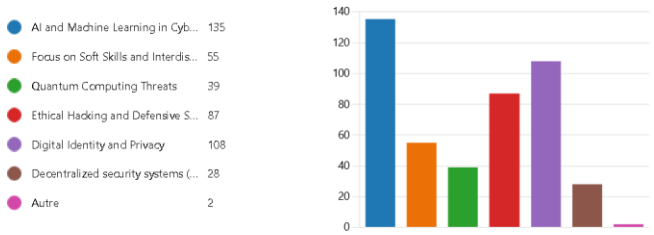
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**

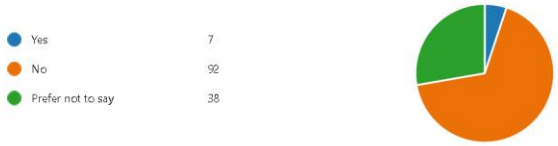


16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. ZAŁĄCZNIK D: LISTA ZWERYFIKOWANYCH ZAWODÓW ESCO

Bibliografia:

2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529.3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

kontakt@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDx

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau