INTERNET STANDARDS. SECURITY AND SAFETY COALITION (IS3C)	INTERNET STANDARDS. SECURITY AND SAFETY COALITION (IS3C)
MAKING THE INTERNET MORE SECURE AND SAFER	SPRAWIAMY, ŻE INTERNET STAJE SIĘ MIEJSCEM BARDZIEJ ZABEZPIECZONYM I BEZPIECZNYM

Zmniejszanie luki pomiędzy potrzebami branży cyberbezpieczeństwa a umiejętnościami absolwentów szkół wyższych

Raport z badań

Autorzy

Janice Richardson
Veronica Samara
Olena Styslavska
Teuntje Manders

Opublikowano przez ISC3C, październik 2022

Do 2025 r. 50% wszystkich pracowników będzie wymagało aktualizacji swoich kwalifikacji, w miarę jak wzrasta wykorzystanie technologii.

Źródło: Future of Jobs Report 2020, Światowe Forum Ekonomiczne.

Spis treści

Podsumowanie

W 2021 roku Grupa Robocza nr 2 koalicji IS3C (dynamiczna koalicja Internet Governance Forum skupiająca się na internetowych standardach, zabezpieczaniu i bezpieczeństwie Internetu) rozpoczęła badanie dotyczące edukacji i umiejętności związanych z cyberbezpieczeństwem. Celem było zrozumienie wagi, jaką sektor cyberbezpieczeństwa i instytucje szkolnictwa wyższego przywiązują do kompetencji przekrojowych i zawodowych, a także szacowanego poziomu kompetencji młodych ludzi wchodzących na rynek pracy w dziedzinie cyberbezpieczeństwa z obu perspektyw. W celu zdefiniowania zakresu badania i opracowania listy wymaganych kompetencji przekrojowych i zawodowych przeprowadzono 5 wywiadów z liderami branży z 5 różnych krajów UE, a następnie wyniki zostały potwierdzone w wywiadach z przedstawicielami sektora szkolnictwa wyższego w dwóch kolejnych krajach. Członkowie IGF Youth i AprIGF zostali przeszkoleni i w 2022 roku przeprowadzili kolejne 21 wywiadów w 9 krajach na całym świecie, zgodnie z ustalonym protokołem.

Z ogólnej liczby 235 respondentów, którzy wypełnili ankietę, 73% stanowili mężczyźni, 26% kobiety, a 1% wolał nie podawać swojej płci. 19% było w wieku poniżej 30 lat. Niedostateczna reprezentacja kobiet i osób poniżej 30 roku życia świadczy o obecnym braku różnorodności w sektorze cyberbezpieczeństwa. Pytania ankiety zostały dostosowane w zależności od tego, czy respondenci pochodzili z sektora biznesowo-przemysłowego, czy z sektora edukacji, chociaż w obu przypadkach zachowano tę samą listę kompetencji przekrojowych i zawodowych. Respondenci z sektora biznesowo-przemysłowego (64% ogółu) przywiązywali około 10% większą wagę do umiejętności przekrojowych i zawodowych niż przedstawiciele sektora edukacyjnego, uznając **myślenie krytyczne**, **umiejętność rozwiązywania problemów**, **umiejętność pracy zespołowej** i **kreatywność** za najważniejsze kryteria w zakresie umiejętności przekrojowych wraz z umiejętnościami zawodowymi takimi jak **zapobieganie ryzykom** i **zarządzanie ryzykami w zakresie ochrony Internetu**. Respondenci z grupy edukacyjnej (36%) wskazali **kreatywność** i **umiejętność rozwiązywania problemów** jako najważniejsze kompetencje przekrojowe, a **rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych** ocenili jako najważniejszy wymóg zawodowy.

Tylko 67% przedstawicieli przemysłu i biznesu - średnio - oceniło poziom kompetencji przekrojowych absolwentów jako dobry lub umiarkowany, najwyżej oceniając **umiejętności w zakresie komunikacji werbalnej** i **pisemnej** oraz **umiejętność pracy zespołowej**, a najniżej **myślenie holistyczne**. Prawie połowa tej grupy (44%) oceniła średni poziom kompetencji zawodowych absolwentów jako niski lub bardzo niski, przy czym najniżej oceniono **znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych** (ang. *cloud computing*). Grupa edukacyjna w podobny sposób oceniła kompetencje przekrojowe swoich absolwentów, przy czym najwyżej oceniono **umiejętności w zakresie komunikacji werbalnej** i **rozwiązywania problemów**, a nisko **myślenie strategiczne** i **myślenie holistyczne**. Średnio połowa respondentów z grupy edukacyjnej oceniła kompetencje absolwentów pozytywnie (*bardzo dobrze* lub *dobrze*), przy czym najwyżej oceniono **rozumienie zagadnień związanych z bezpieczną komunikacją w Internecie i technologiami internetowymi**, a najniżej **wiedzę na temat podatności systemów na ataki i eksploitów w systemach** oraz **znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych** (ang. *cloud computing*).

Obie grupy - przemysłowo-biznesowa i edukacyjna - przywiązują wagę do podobnych umiejętności przekrojowych (**krytyczne myślenie**, **umiejętność rozwiązywania problemów**,

umiejętność pracy zespołowej, **kreatywność** i **umiejętności komunikacyjne**), chociaż grupa edukacyjna systematycznie przywiązuje do nich mniejszą wagę. Ich ocena poziomu osiągnięć absolwentów jest znacznie bliższa, przy czym wyższe oceny dotyczą **myślenia etycznego**, **umiejętności rozwiązywania problemów**, **umiejętności pracy zespołowej** i **umiejętności komunikacyjnych**, a najniższe **myślenia holistycznego**, **strategicznego** i **interdyscyplinarnego** oraz **wiedzy biznesowej**. Rozbieżność między obiema grupami w kwestii znaczenia przypisywanego kompetencjom zawodowym jest znacznie większa. Grupa edukacyjna przywiązuje znacznie mniejszą wagę niż grupa przemysłowo-biznesowa do **rozumienia logiki systemów** i **znajomości zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT**, a większą do **umiejętności pisania skryptów lub kodowania**. Oceny kompetencji zawodowych absolwentów są do siebie zbliżone, przy czym obie grupy najwyżej oceniają **zrozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych**, a nisko oceniają **znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych** (ang. *cloud computing*).

Wnioski z całościowego badania pokazują, że priorytety środowisk przemysłu i edukacji w zakresie kompetencji przekrojowych różnią się, choć bardziej pod względem przypisywanego znaczenia niż obszaru zainteresowania. Z drugiej strony, środowisko edukacyjne wydaje się pozostawać w tyle, jeżeli chodzi, na przykład, o rozwój IoT, gdzie zachodzą szybkie zmiany. Sugestie przedstawione w wywiadach i w ankiecie podkreślają, że grupa edukacyjna powinna bardziej skupić się na podstawach, takich jak pomaganie studentom w lepszym zrozumieniu działania systemów i aplikacji oraz w radzeniu sobie z wprowadzającymi w błąd mechanizmami wyszukiwarek. Na podstawie badania sformułowano siedem zaleceń. Obejmują one poprawę współpracy między sektorami, unowocześnienie procedur rekrutacji w celu zwiększenia różnorodności, a także podnoszenie świadomości w celu zachęcenia użytkowników do bardziej odpowiedzialnego podejścia do własnego cyberbezpieczeństwa oraz zachęcenia większej liczby młodych ludzi do planowania kariery zawodowej w tym szybko rozwijającym się sektorze gospodarki.

Według danych (ISC)[2], międzynarodowego stowarzyszenia non-profit zrzeszającego certyfikowanych specjalistów ds. cyberbezpieczeństwa, branża cyberbezpieczeństwa musi zwiększyć liczbę pracowników o 2,7 miliona, aby wypełnić międzynarodową lukę kadrową.[1]

[1] https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

1. Wprowadzenie

Czym jest IS3C

IS3C - dynamiczna koalicja na rzecz internetowych standardów, zabezpieczania i bezpieczeństwa Internetu - to wspólne przedsięwzięcie zainteresowanych stron z całego świata, reprezentujących społeczność techniczną, społeczeństwo obywatelskie, decydentów rządowych, organy regulacyjne oraz firmy i osoby prywatne, mające na celu poprawę bezpieczeństwa i ochrony w Internecie poprzez szersze i szybsze wdrażanie istniejących standardów internetowych i dobrych praktyk ICT. Powstała ona w 2020 roku w ramach Forum Zarządzania Internetem (IGF),[2] międzynarodowego wydarzenia organizowanego przez ONZ i goszczącego co roku w innym kraju członkowskim. Skuteczne zarządzanie Internetem jest koniecznie wsparte globalną świadomością i poszanowaniem standardów bezpieczeństwa i zabezpieczeń, które mają na celu budowanie zaufania w środowisku internetowym i przyczyniają się do bezpieczeństwa i zabezpieczania jego użytkowników.

IS3C ustala roczny plan pracy realizowany przez 5 Grup Roboczych, z których każda posiada specjalistyczną wiedzę w dziedzinach od bezpieczeństwa w fazie projektowania, edukacji i umiejętności po zarządzanie łańcuchem dostaw i zarządzanie danymi. Celem jest identyfikacja i połączenie krytycznych czynników podaży i popytu na bezpieczeństwo oraz zaproponowanie najlepszych opcji wdrażania kluczowych standardów i najlepszych praktyk po obu stronach, w formie zaleceń politycznych i praktycznych wskazówek.

Grupa Robocza 2 posiada wiedzę specjalistyczną w zakresie edukacji i rozwoju kompetencji obywateli w każdym wieku w zakresie zachowania własnego bezpieczeństwa, prywatności i dobrego samopoczucia w Internecie oraz aktywnego udziału w postępie w zakresie produktów i usług cyfrowych, w których zastosowano wiodące standardy bezpieczeństwa i najlepsze praktyki. Badania opisane w niniejszym raporcie, poprzez określenie aktualnego poziomu wiedzy i umiejętności studentów i absolwentów szkół wyższych oraz oczekiwań ze strony sektora biznesowo-przemysłowego, są podstawowym krokiem do określenia kolejnych kroków w celu osiągnięcia celów IS3C.

Dlaczego cyberbezpieczeństwo jest ważne

Technologia cyfrowa stała się integralną częścią współczesnego życia, do tego stopnia, że trudno sobie wyobrazić bez niej życie. Na przykład ponad 83% ludności świata to użytkownicy smartfonów (2022), a liczba ta rośnie w tempie 4,9% rocznie.[3] Badania antropologiczne przeprowadzone na 4 kontynentach w latach 2020-2021 opisują sieć jako miejsce, *w którym obecnie żyjemy*.[4] Jednak, podczas gdy stałe połączenie z Internetem stało się powszechne, nasza obecność w sieci i ślady cyfrowe stanowią rosnące zagrożenie dla bezpieczeństwa osobistego, szczególnie dla osób młodszych lub niepiśmiennych cyfrowo. Niestety, wraz z rosnącą liczbą cyfrowych tubylców, wzrosła również liczba osób o złych zamiarach, często szukających korzyści finansowych. Dlatego cyberbezpieczeństwo, jako praktyka i norma społeczna, nabrało ogromnego znaczenia i jest jedynym sposobem zapobiegania naruszeniom

[2] https://www.intgovforum.org
[3] http://www.Statista.com
[4] https://www.weforum.org/agenda/2021/05/how-we-interact-with-smartphones-report/

prywatności i kradzieży tożsamości oraz innym cyberprzestępstwom.

Cyberbezpieczeństwo obejmuje wszystkie środki stosowane przez *osoby, organizacje lub państwa oraz ich informacje komputerowe przeciwko przestępstwom lub atakom przeprowadzanym za pośrednictwem Internetu*.[5] Podstawową funkcją cyberbezpieczeństwa jest ochrona danych, które osoby i organizacje udostępniają lub do których mają dostęp za pośrednictwem Internetu, a zatem dotyczy ono z konieczności zarówno bezpieczeństwa urządzeń służących do łączenia się, jak i środków służących do przechowywania danych. Większość interakcji i procesów społecznych, handlowych, finansowych, rozrywkowych, a także politycznych odbywa się obecnie w Internecie.

Szacuje się, że od 2007 roku ponad 99,9% wszystkich informacji jest generowanych w formie cyfrowej. Przeciętny człowiek wytwarza około 1,5 megabajta danych dziennie, a w 2021 roku wytworzyliśmy globalnie 2,5 kwintyliona bajtów danych dziennie.[6] Znaczenie cyberbezpieczeństwa będzie zatem nadal rosło w postępie geometrycznym, ponieważ staramy się chronić ogromne ilości informacji osobistych, biznesowych i rządowych przechowywanych w Internecie przed nieuprawnionym dostępem, kradzieżą, niewłaściwym wykorzystaniem i zniszczeniem.

Cyberprzestępczość wzrosła dramatycznie na całym świecie wraz z pandemią wirusa Covid-19 w latach 2020-21[7] , kiedy to szkoły, przedsiębiorstwa i miejsca pracy zwróciły się do Internetu, aby kontynuować swoją codzienną działalność w obliczu społecznego oddalenia i zamknięcia przestrzeni publicznej. Edukacja w zakresie cyberbezpieczeństwa jest niezbędna dla każdego użytkownika Internetu od wczesnego dzieciństwa i obejmuje złożony zestaw umiejętności i wiedzy, które stale się rozwijają, ponieważ urządzenia stają się coraz potężniejsze i coraz mocniej zintegrowane z każdym aspektem życia człowieka.

Chociaż za cyberbezpieczeństwo odpowiada każdy użytkownik Internetu, stało się ono centralnym punktem globalnego biznesu i w dużej mierze zależy od czujności, szybkości działania i reakcji oraz innowacyjności twórców oprogramowania, firm i organizacji zajmujących się bezpieczeństwem cybernetycznym. Jednak firma SAP, główny światowy gracz w dziedzinie cyberbezpieczeństwa, podkreśla, że branża ta boryka się z systemowym problemem zatrudniania i zatrzymywania pracowników, który musi być rozwiązany globalnie, aby zapewnić obsadzenie rosnącej liczby stanowisk, jeśli chcemy wyprzedzić stale ewoluujący krajobraz zagrożeń.[8]

Niniejsze badanie ma na celu przeanalizowanie niezbędnych umiejętności przekrojowych i zawodowych, które są wymagane, aby sprostać powyższym wyzwaniom, w ramach podejścia, które stawia na stałe podnoszenia świadomości znaczenia cyberbezpieczeństwa i budowanie odporności użytkowników poprzez edukację.

---

5 Słownik Cambridge. (28. września 2022 r.) definicja cyberbezpieczeństwa. Pobrano 4. października 2022 r. z https://dictionary.cambridge.org/dictionary/english/cybersecurity?q=cybersecurity+

6 Mapfre, F. (27 grudnia 2021 r.). *Ile informacji jest generowanych i przechowywanych na świecie?* Fundacja MAPFRE. Pobrano 5. października 2022 r. z https://www.fundacionmapfre.org/en/blog/how-much-information-is-generated-and-stored-in-the-world/

7 Europol (2020). Internet Organised Crime Threat Assessment (pol. O*cena zagrożenia przestępczością zorganizowaną w Internecie*) (IOCTA), dostępna na stronie: https://bit.ly/348XZKi

8 Elena Kvochko, dyrektor ds. ochrony zaufania w SAP. Na stronie https://www.scmagazine.com/news/careers/only-30-of-the-cyber-workforce-is-in-the-19-34-age-demographic%EF%BF%BC. Skonsultowano 7. października 2022 r.

2. Metodologia

Podejście dwufazowe

Niniejsze badanie opiera się na dwuetapowej metodologii, której celem jest udokumentowanie konkretnych kompetencji, jakich oczekuje się od absolwentów rozpoczynających karierę w branży cyberbezpieczeństwa oraz, z perspektywy zarówno sektora biznesowego, jak i edukacyjnego, podsumowanie obecnego średniego poziomu kompetencji, jakie absolwenci wnoszą do miejsca pracy. Celem dodatkowym jest zebranie istniejących dobrych praktyk biznesowych, które mogłyby pomóc szkolnictwu wyższemu i zawodowemu w wypełnieniu luki między podażą a popytem. W poniższym opisie metodologii i ustaleń zdefiniowano następujące kluczowe pojęcia:

- **Kompetencje** rozumiane są zgodnie z definicją Rady Europy jako „zdolność do mobilizowania i wykorzystywania odpowiednich wartości, postaw, umiejętności, wiedzy i/lub zrozumienia w celu odpowiedniego i skutecznego reagowania na wymagania, wyzwania i możliwości, jakie stwarza dany rodzaj kontekstu". Oprócz tego globalnego i całościowego użycia terminu „**kompetencja**", termin „**kompetencje**" (w liczbie mnogiej) odnosi się do „określonych zasobów indywidualnych (mianowicie specyficznych wartości, postaw, umiejętności, wiedzy i zrozumienia), które są mobilizowane i wykorzystywane w tworzeniu kompetentnych zachowań".[9]
- W **badaniu** skupiono się na interpretacji przedstawicieli biznesu, przemysłu i sektora edukacji na temat wiedzy i poziomu umiejętności wymaganych od kompetentnego pracownika w dzisiejszym sektorze cyberbezpieczeństwa, w porównaniu z opinią przedstawicieli z obszaru edukacji na temat znaczenia przypisywanego takim umiejętnościom i wiedzy oraz szacowanego poziomu kompetencji osiąganych przez ich absolwentów. Uwagę skupiono na dwóch rodzajach kompetencji - przekrojowych i zawodowych.
- **Kompetencje przekrojowe** rozumiano jako „kompetencje, które zazwyczaj uważa się za niezwiązane z konkretnym stanowiskiem, zadaniem, dyscypliną akademicką lub obszarem wiedzy, a które można wykorzystać w wielu różnych sytuacjach i środowiskach pracy".[10]
- **Kompetencje zawodowe** rozumiano jako „połączenie umiejętności, wiedzy, postaw i wartości, które są szczególnie cenione przez stowarzyszenia, organizacje i organy zawodowe w sektorze cyberbezpieczeństwa".

Oczekiwano, że ocena obecnej sytuacji z perspektywy zarówno sektora przemysłowego, jak i edukacyjnego przyczyni się do opisu potencjalnych rozwiązań, które pozwolą skrócić dystans między podażą a popytem i zachęcą do szerszego stosowania dobrych praktyk.

[9] Glosariusz RFCDC: na stronie https://www.coe.int/en/web/reference-framework-of-competences-for-democratic-culture/glossary

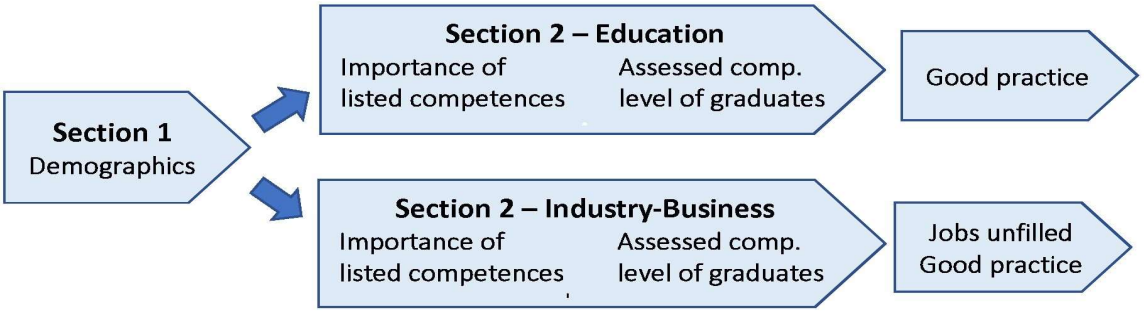
[10] UNESCO (2019). *Ocena kompetencji przekrojowych: aktualne narzędzia w regionie azjatyckim*, rys. 1. Na stronie https://unesdoc.unesco.org/arkV48223/pf0000368479

Narzędzia badawcze

Pierwszy etap badania obejmował wywiady bezpośrednie i internetowe przeprowadzone z liderami branży cyberbezpieczeństwa w okresie od października 2021 r. do czerwca 2022 r. w celu dopracowania pytań badawczych, określenia zakresu cyberbezpieczeństwa pod względem potrzeb i wyzwań oraz zebrania przykładów dobrych praktyk. 60-minutowe wywiady zostały przeprowadzone przez 10 ankieterów z różnych środowisk językowych i kulturowych. Ankieterzy mieli doświadczenie w dziedzinach pokrewnych i uczestniczyli w dwóch wstępnych sesjach szkoleniowych. Otrzymali oni szczegółowy przewodnik dla ankieterów i szablony nagrań, aby zapewnić porównywalność wyników. Podczas wywiadów zebrano wyniki w 3 kategoriach: wymagania dotyczące kompetencji, wyzwania i dobre praktyki. Wywiady zostały przeprowadzone w ścisłej współpracy z uczestnikami IGF Youth[11] i Youth Summit oraz przedstawicielami regionalnego forum IGF Azji i Pacyfiku (APrIGF). Na podstawie wywiadów opracowano model 14 kompetencji przekrojowych i 10 zawodowych uznanych za istotne z punktu widzenia pracodawców. Stanowiły one **listę kompetencji** wykorzystanych w drugiej fazie badania.

Druga faza została zorganizowana w formie internetowego kwestionariusza ankiety, który zbierał dane ilościowe tak, aby zweryfikować model kompetencji, określić luki i zebrać dalsze przykłady dobrych praktyk. Ankieta składała się z dwóch części, patrz rys. 1.

W pierwszej części uczestnicy odpowiadali na pytania demograficzne i musieli wybrać sektor zatrudnienia: przemysł-biznes lub edukacja (w tym szkolna i wyższa). Pytania w drugiej części zostały sformułowane nieco inaczej dla każdego z dwóch sektorów zatrudnienia, ale zachowano te same dwie **listy kompetencji przekrojowych i zawodowych** dla obu sektorów. Każde pytanie zawierało miejsce, w którym respondenci mogli dodać swoje własne sugestie. Dla grupy przemysłowo-biznesowej dodano dwa kolejne pytania otwarte.



Section 1 Demographics	Część nr 1 Dane demograficzne
Section 2 – Education	Część nr 2 - Grupa edukacyjna
Importance of listed competences	Znaczenie wymienionych kompetencji
Assessed comp. level of graduates	Oceniony poziom kompetencji absolwentów
Good practice	Dobra praktyka
Section 2 – Industry-Business	Część nr 2 - Grupa przemysłowo-biznesowa
Jobs unfilled Good practice	Nieobsadzone miejsca pracy Dobra praktyka

rys. 1. Struktura kwestionariusza

W kwestionariuszu dla przedstawicieli grupy przemysłowo-biznesowej poproszono

[11] IGF Youth and Youth Summit (pol. IGF - Szczyt Młodzieży), na stronie https://youthigf.com/

respondentów o:

- Ocenę znaczenia **listy kompetencji** w miejscu pracy;
- Ocenę poziomu absolwentów pracujących w ich organizacji według **wymienionych kompetencji**;
- Wskazanie, które stanowiska są dla nich **najtrudniejsze do obsadzenia** i jaki ma to wpływ na ich organizację;
- Podanie przykładów **dobrych praktyk** i zaproponowanie sposobów poprawy sytuacji.

Respondentów z sektora edukacji poproszono o:

- Ocenę znaczenia, jakie ich placówka przypisuje **liście kompetencji**;
- Ocenę poziomu absolwentów w zakresie **wymienionych kompetencji**;
- Podanie przykładów **dobrych praktyk** stosowanych w ich placówce oraz zaproponowanie rozwiązań mających na celu podniesienie kompetencji absolwentów.

Za pomocą 5-stopniowej skali Likerta zmierzono zarówno znaczenie wymienionych kompetencji przekrojowych i zawodowych, jak i oceniony poziom absolwentów w każdej z wymienionych kompetencji.

Badanie kwestionariuszem ankiety trwało od 5 lipca do 20 września 2022 r. i zostało rozpowszechnione online poprzez sieci osobiste członków IS3C, Youth IGF i APrIGF .

„Po pierwsze, trzeba przyciągać różnorodnych ludzi. Jeśli będziemy skoncentrowani tylko na jednym punkcie widzenia i jednej perspektywie, branża nie będzie atrakcyjna dla ludzi z różnych środowisk. Zespół traci wtedy różnorodny ogląd sytuacji i szersze spojrzenie na aspekty bezpieczeństwa, które są istotne. Różnorodność jest potrzebna, aby dostrzec różne rzeczy dla różnych klientów."

Konsultantka ds. cyberbezpieczeństwa w UE

3. Ustalenia

Wywiady

Przeprowadzono dwadzieścia osiem wywiadów w 16 różnych krajach na całym świecie (patrz rys. 2); do prowadzenia rozmów wykorzystano 5 pytań kluczowych. Główny badacz przeprowadził pierwszych siedem wywiadów z liderami przemysłu i szkolnictwa wyższego, z rozmówcami z sektora rządowego, przemysłowego i szkolnictwa wyższego; celem było określenie zakresu i stworzenie standardowego protokołu nagrywania wywiadów. Wywiady te odbyły się w siedmiu krajach takich jak: Belgia, Dania, Włochy, Luksemburg, Maroko, Holandia i Polska. Następnie przeprowadzono dwie sesje szkoleniowe online dla dziesięciu ankieterów-ochotników. Ankieterzy byli w większości absolwentami szkół wyższych, szczególnie zainteresowanymi cyberbezpieczeństwem i zarządzaniem Internetem; wszyscy byli członkami IGF Youth lub APrIGF. Przeprowadzili oni kolejnych dwadzieścia wywiadów z ważnymi osobami zajmującymi się cyberbezpieczeństwem w swoich krajach takich jak: Brazylia, Ghana, Indonezja, Polska, Samoa, Sri Lanka, Sudan i Wietnam oraz jeden wywiad z ekspertem technicznym z firmy Microsoft z USA. Wszystkie dane z wywiadów zostały zapisane we wspólnym dokumencie online przy użyciu wyżej wymienionego protokołu nagrywania wywiadów.

rys. 2: Wywiady przeprowadzono w 16 krajach na całym świecie

Wyniki wywiadów przyczyniły się do opracowania kwestionariuszy ankiety, zarówno pod względem struktury, jak i treści. Z wywiadów wynikło wiele interesujących kwestii, które będą nadal służyć jako wskazówki do obszarów wartych dalszego badania. Kilka takich kwestii zostało również poruszonych lub potwierdzonych przez wkład w otwarte pytania ankietowe, w tym:

- **Duży obraz**: chociaż wszystkie aspekty bezpieczeństwa wymagają różnych zestawów wiedzy specjalistycznej, istnienie silosów wiedzy spowalnia śledzenie i rozwiązywanie incydentów. Cyberbezpieczeństwo rozwija się bardzo szybko, a ludzie z różnych dziedzin muszą nauczyć się dzielić wiedzą specjalistyczną, umiejętnościami i doświadczeniem, tak aby połączyć ze sobą różne silosy i uzyskać pełny obraz sytuacji. Organizacje coraz częściej poszukują osób o kompetencjach przekrojowych, ponieważ są świadome tego wyzwania.
- **Różnorodność społeczna**: przynosi korzyści organizacjom, ponieważ wnosi wiele różnych punktów widzenia do wszystkich obszarów pracy i sprawia, że praca jest o wiele

bardziej interesująca. Zawężone spojrzenie nie pozostawia miejsca na różne punkty widzenia aspektów bezpieczeństwa. Ważne jest, aby zaangażować więcej młodych ludzi, ponieważ mają oni tendencję do korzystania z technologii w różny sposób, oraz aby zachęcać kobiety do podejmowania kariery w cyberbezpieczeństwie, ponieważ często przyjmują one bardziej szczegółowe podejście. Dzielenie się wiedzą, autentyczność i otwartość to podstawowe składniki udanej pracy zespołowej.

- **Umiejętność myślenia**: umiejętność krytycznego i abstrakcyjnego myślenia jest kluczowa. Zdolność do czerpania praktycznej wiedzy z pracy w laboratoriach, stosowania jej w innych sytuacjach i sprawdzania, jak można skalować wyniki, są ważniejsze niż nauka z książki. Projektowanie cyberbezpiecznych produktów i zwalczanie incydentów związanych z cyberbezpieczeństwem to złożone procesy, które wymagają również umiejętności przewidywania, jakie mogą być przyszłe zagrożenia i skąd mogą pochodzić.
- **Pisanie raportów**: raporty opisujące strategie rozwiązywania problemów lub wskazujące, jak poradzono sobie z danym problemem, muszą być szybkie, jasne i napisane przystępnym językiem. Zespoły ds. cyberbezpieczeństwa muszą być w stanie dotrzeć do użytkowników i przekonać ich do zintegrowania środków zapobiegawczych oraz do postrzegania siebie jako części rozwiązania. Wyzwaniem jest przekazanie silnych komunikatów z zachowaniem wrażliwości kulturowo-politycznej i bez technokratyzmu.
- **Braki w wiedzy**: dobre zrozumienie funkcjonowania szkieletu internetowego i systemów administracyjnych jest kluczowe dla wiedzy o tym, które środowiska są najbardziej odpowiednie. Studenci mają problemy z opanowaniem podstawowych elementów budowy, takich jak kontenery i jądra, ponieważ brakuje im wiedzy na temat historii rozwoju technologii cyfrowych. Często przeszkodą jest również słabe zrozumienie algorytmów oraz bezpieczeństwa mechanizmu blockchain, urządzeń mobilnych i rozwiązań chmurowych.
- **Edukacja**: musimy sprawić, aby dzieci z entuzjazmem uczyły się, jak działają ich urządzenia cyfrowe, i pomóc im dostrzec ewentualne minusy i zagrożenia związane z korzystaniem z darmowych narzędzi technicznych. Dużym wyzwaniem jest nauczenie ich, jak skutecznie wyszukiwać informacje. Wyszukiwarki internetowe zazwyczaj szeregują rzeczy według tego, ile razy były one przywoływane, co oznacza, że najstarsze rzeczy są wymieniane jako pierwsze i dostęp do najnowszych informacji może być trudny. Takie rzeczy jak poszukiwanie i dzielenie się wiedzą, autentyczność, współpraca, otwartość i zarządzanie sobą należy rozwijać w szkole od najmłodszych lat.

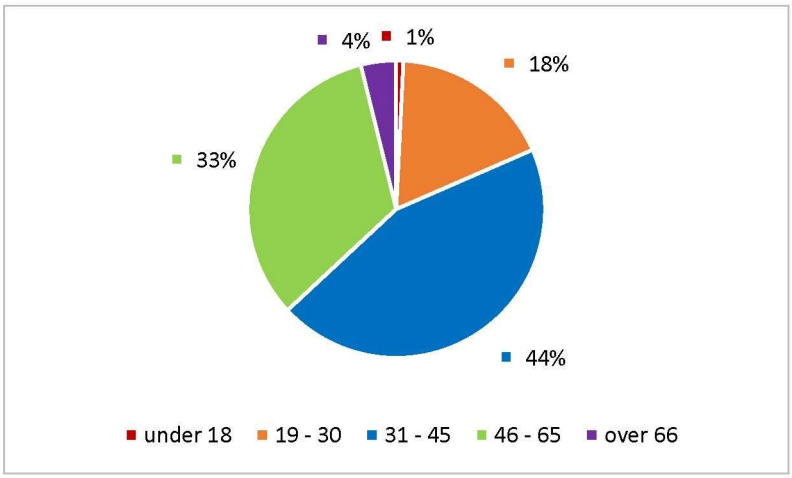
Kluczowe obawy zgłaszane przez większość rozmówców znalazły potwierdzenie w wynikach kwestionariusza ankietowego przeprowadzonego w drugiej fazie tego badania. Jedną z wielokrotnie poruszanych kwestii można podsumować słowami Grega Bianchi z Microsoft USA: *Potrzeby w branży cyberbezpieczeństwa są ogromne. W tej chwili liczba wakatów jest ogromna. Wynika to z potrzeby zapewnienia cyberbezpieczeństwa na wielu różnych poziomach. Brakuje wszelkiego rodzaju ekspertów. Problem małej liczby kobiet i innych osób historycznie wykluczonych ze społeczności sprawia, że bardzo trudno jest uzyskać odpowiedni poziom zróżnicowania kadr.*[12]

[12] https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/ oraz

Kwestionariusz online

Kwestionariusz wypełniło 235 respondentów, 64% z sektora biznesu i przemysłu oraz 36% z sektora edukacji. Odpowiedzi pochodziły z 65 różnych krajów[13] (patrz rys. 3).

rys. 3. Kraje zamieszkania respondentów kwestionariusza



under	poniżej
over	ponad

rys. 4. Reprezentacja wiekowa respondentów badania

73% respondentów to mężczyźni, 26% kobiety, a 1% wolał nie podawać swojej płci. Mężczyźni i kobiety byli dość równomiernie rozłożeni w obu grupach odpowiedzi. Niedostateczna reprezentacja kobiet biorących udział w badaniu świadczy o różnicach między płciami, które

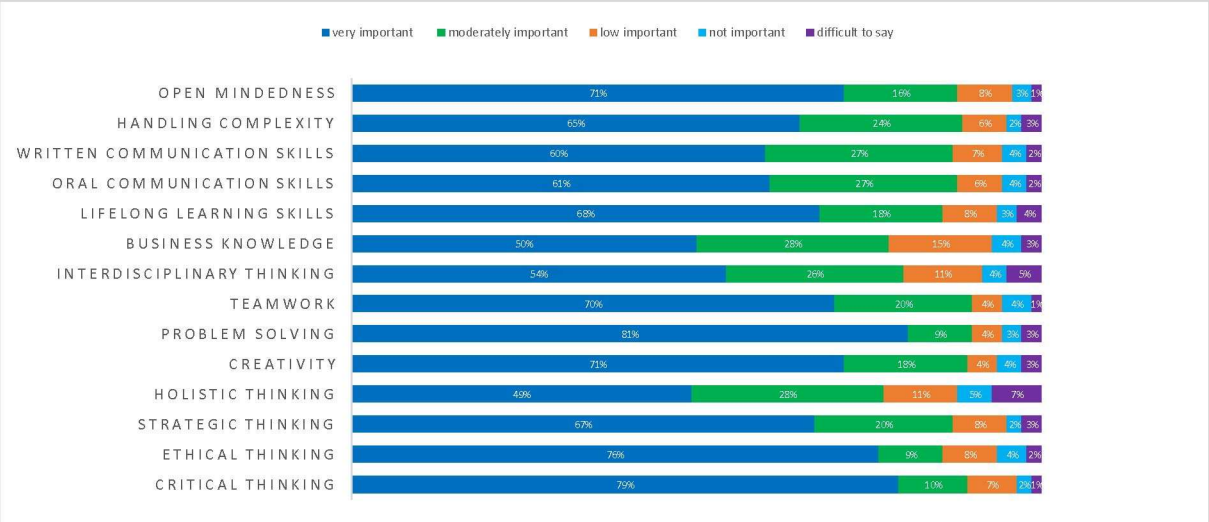
https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/

[13] Afganistan, Argentyna, Australia, Austria, Aruba, Bangladesz, Belgia, Botswana, Brazylia, Burkina Faso, Kamerun, Kanada, Czad, Chile, Kolumbia, Kongo, Wybrzeże Kości Słoniowej, Etiopia, Francja, Fidżi, Finlandia, Gambia, Niemcy, Ghana, Gwinea, Haiti, Islandia, Indie, Indonezja, Kenia, Liban, Madagaskar, Malawi, Malezja, Mali, Mauretania, Maroko, Mozambik, Meksyk, Nepal, Holandia, Nigeria, Norwegia, Panama, Filipiny, Polska, Portugalia, Rosja, Rwanda, Serbia, RPA, Senegal, Sudan, Szwecja, Szwajcaria, Tanzania, Togo, Turcja, Wielka Brytania, Uganda, Ukraina, USA, Zimbabwe, Zair, Zambia.

istnieją w całym sektorze cyberbezpieczeństwa. Według badań przeprowadzonych w 2022 roku przez (ISC)2, [14] tylko 24% wszystkich osób pracujących w sektorze cyberbezpieczeństwa stanowią kobiety. To już znacznie więcej niż w badaniu tej samej organizacji z 2017 r., które wskazywało, że w sektorze zatrudnionych jest tylko 11% kobiet. 44% respondentów było w wieku od 31 do 45 lat, 22% w przedziale wiekowym od 46 do 65 lat, a tylko 18% w wieku od 19 do 30 lat (patrz rys. 4). 1% respondentów miało mniej niż 18 lat, a 4% było w wieku 66 lat lub więcej. Podział wiekowy respondentów odzwierciedla ciągłe obawy biznesu i przemysłu: jak zachęcić więcej młodych ludzi do zainteresowania się karierą w sektorze cyberbezpieczeństwa. Ostatnie badania CompTIA dotyczące pracowników technicznych wykazały, na przykład, że 52% osób pracujących w branży cyberbezpieczeństwa należy do grupy wiekowej 35-54 lata, a tylko 30% takich pracowników należy do grupy wiekowej 19-34 lata.[15]

Ocena wymagań dotyczących kompetencji w miejscu pracy dokonana przez grupę przemysłowo-biznesową

Średnio 86% spośród grupy przedsiębiorstw ocenia wymienione kompetencje przekrojowe jako bardzo ważne lub umiarkowanie ważne (patrz rys. 5). Po zsumowaniu ocen *bardzo ważny* i *umiarkowanie ważny* okazuje się, że **umiejętność rozwiązywania problemów** i **pracy zespołowej** są oceniane jako najważniejsze kompetencje przez grupę biznesowo-przemysłową, a **radzenie sobie ze złożonością problemów**, **kreatywność** i **krytyczne myślenie** są oceniane jako mniej ważne.



OPEN MINDEDNESS	OTWARTOŚĆ UMYSŁU
HANDLING COMPLEXITY	RADZENIE SOBIE ZE ZŁOŻONOŚCIĄ PROBLEMÓW
WRITTEN COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI PISEMNEJ
ORAL COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI WERBALNEJ
LIFELONG LEARNING SKILLS	UMIEJĘTNOŚĆ UCZENIA SIĘ PRZEZ CAŁE ŻYCIE
BUSINESS KNOWLEDGE	WIEDZA BIZNESOWA
INTERDISCIPLINARY THINKING	MYŚLENIE INTERDYSCYPLINARNE

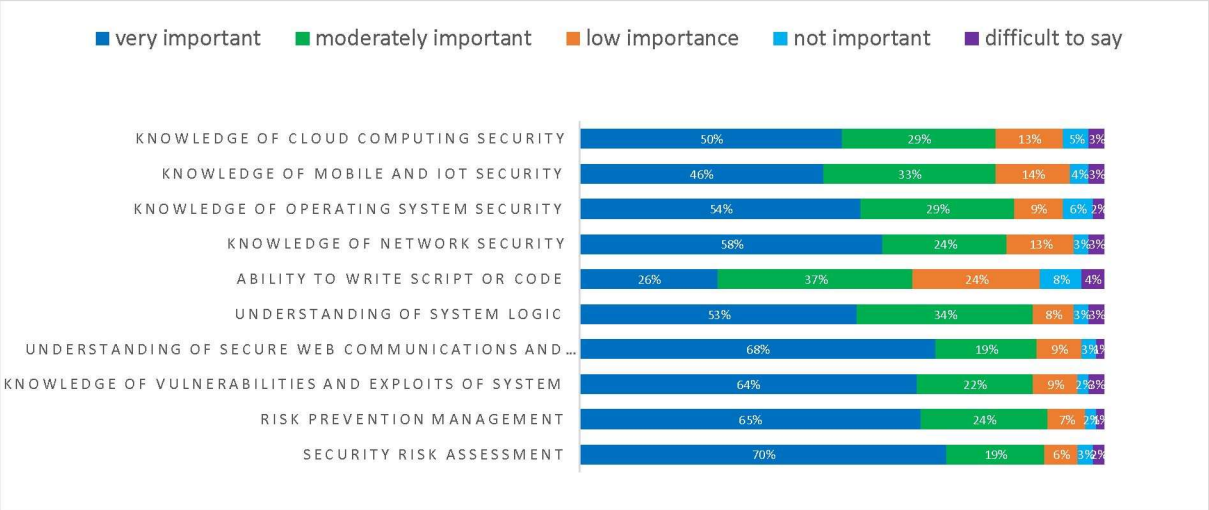
[14] https://www.isc2.org/research/women-in-cybersecurity. Skonsultowano 6. października 2022 r.

[15] Badanie przeprowadzone przez CompTIA, cytowane w https://www.scmagazine.com/news/careers/only-30-of-the-cyber-workforce-is-in-the-19-34-age-demographic%EF%BF%BC. Skonsultowano 6. października 2022 r.

TEAMWORK	UMIEJĘTNOŚĆ PRACY ZESPOŁOWEJ
PROBLEM SOLVING	UMIEJĘTNOŚĆ ROZWIĄZYWANIA PROBLEMÓW
CREATIVITY	KREATYWNOŚĆ
HOLISTIC THINKING	MYŚLENIE HOLISTYCZNE
STRATEGIC THINKING	MYŚLENIE STRATEGICZNE
ETHICAL THINKING	MYŚLENIE ETYCZNE
CRITICAL THINKING	MYŚLENIE KRYTYCZNE
very important	bardzo ważne
moderately important	umiarkowanie ważne
low important	mało ważne
not important	nieistotne
difficult to say	trudno powiedzieć

rys. 5. Grupa przemysłowo-biznesowa: Znaczenie kompetencji przekrojowych w miejscu pracy

Wszystkie 10 wymienionych kompetencji zawodowych zostało ocenionych jako *bardzo ważne* lub *umiarkowanie ważne* przez co najmniej 63%, a średnio przez 82% spośród grupy przemysłowo-biznesowej (patrz rys. 6). **Zapobieganie ryzykom** i **zarządzanie ryzykami w zakresie zabezpieczeń**, a następnie **rozumienie logiki systemów** oraz **rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych,** zostały ocenione jako najważniejsze wymagane kompetencje. Zaraz po nich uplasowało się **zarządzanie zapobieganiem ryzykom**.



KNOWLEDGE OF CLOUD COMPUTING SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW CHMUROWYCH
KNOWLEDGE OF MOBILE AND IOT SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM URZĄDZEŃ MOBILNYCH I IOT
KNOWLEDGE OF OPERATING SYSTEM SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW OPERACYJNYCH
KNOWLEDGE OF NETWORK SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SIECI
ABILITY TO WRITE SCRIPT OR CODE	UMIEJĘTNOŚĆ PISANIA SKRYPTÓW LUB KODOWANIA
UNDERSTANDING OF SYSTEM LOGIC	ROZUMIENIE LOGIKI SYSTEMÓW
UNDERSTANDING OF SECURE WEB COMMUNICATIONS AND...	ZROZUMIENIE ZAGADNIEŃ BEZPIECZNEJ KOMUNIKACJI W INTERNECIE ORAZ ...
KNOWLEDGE OF VULNERABILITIES AND EXPLOITS OF SYSTEM	WIEDZA NA TEMAT PODATNOŚCI SYSTEMÓW NA ATAKI I EKSPLOITÓW W SYSTEMACH
RISK PREVENTION MANAGEMENT	ZARZĄDZANIE ZAPOBIEGANIEM RYZYKOM
SECURITY RISK ASSESSMENT	OCENA RYZYK W ZAKRESIE ZABEZPIECZEŃ

very important	bardzo ważne
moderately important	umiarkowanie ważne
low importance	mało ważne
not important	nieistotne
difficult to say	trudno powiedzieć

rys. 6. Grupa przemysłowo-biznesowa: Znaczenie kompetencji zawodowych w miejscu pracy

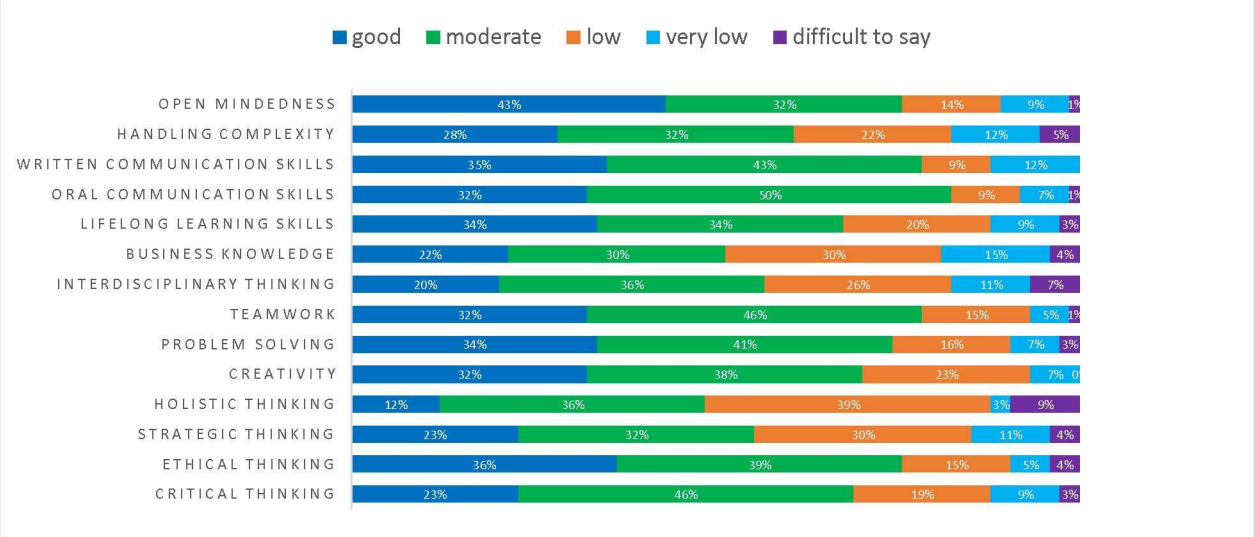
Jedenastu respondentów dodało własne propozycje do listy kompetencji przekrojowych, z których większość dotyczyła umiejętności uczenia się w zespole, samodzielnego uczenia się i otwartości na dzielenie się wiedzą. Odpowiedzialność, przywództwo, umiejętności negocjacyjne, wielojęzyczność, poszanowanie różnorodności kulturowej i psychologiczne aspekty zabezpieczeń (np. znajomość socjotechnik - inżynierii społecznej) zostały również wskazane - jeden lub kilka razy - jako elementy kompetencji przekrojowych.

Dla większości respondentów z grupy przemysłowo-biznesowej sugerowana **lista kompetencji** wydawała się wystarczająco obszerna, chociaż 21 respondentów sugerowało uzupełnienie listy. Jednak większość sugestii była bardzo podobna, choć bardziej szczegółowa, do tych zawartych na **liście kompetencji** i dotyczyła głównie zabezpieczeń danych, świadomości w zakresie zabezpieczeń, zabezpieczeń sieci i oceny ryzyka.

Ocena kompetencji absolwentów w miejscu pracy dokonana przez grupę przemysłowo-biznesową

Kiedy poproszono o ocenę poziomu kompetencji przekrojowych absolwentów szkół wyższych zatrudnionych w ich organizacjach, średnio 67% respondentów z sektora przemysłowo-biznesowego uznało, że absolwenci wykazali się akceptowalnym poziomem co pokazano na ogólnej liście (patrz rys. 7). Jednak za wyjątkiem dwóch kompetencji, **otwartości umysłu** i **umiejętności uczenia się przez całe życie**, większość respondentów oceniła poziom raczej jako *umiarkowany* niż *dobry*.

Najwyżej ocenionymi kompetencjami przekrojowymi były **umiejętności w zakresie komunikacji werbalnej** (82% oceniło je jako dobre lub umiarkowane) oraz **umiejętności w zakresie komunikacji pisemnej** i **pracy zespołowej** (obie na poziomie 78%). Najniżej ocenione kompetencje przekrojowe to **myślenie holistyczne** (tylko 48% uznało poziom absolwentów za dobry lub umiarkowany), **wiedza biznesowa** (52%) i **myślenie strategiczne** (55%).



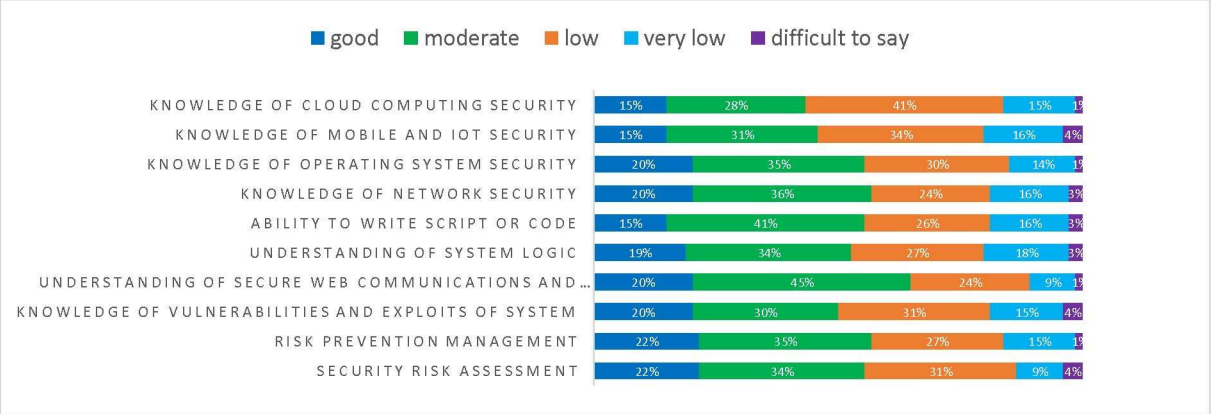
OPEN MINDEDNESS	OTWARTOŚĆ UMYSŁU
HANDLING COMPLEXITY	RADZENIE SOBIE ZE ZŁOŻONOŚCIĄ PROBLEMÓW
WRITTEN COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI PISEMNEJ
ORAL COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI WERBALNEJ
LIFELONG LEARNING SKILLS	UMIEJĘTNOŚĆ UCZENIA SIĘ PRZEZ CAŁE ŻYCIE
BUSINESS KNOWLEDGE	WIEDZA BIZNESOWA
INTERDISCIPLINARY THINKING	MYŚLENIE INTERDYSCYPLINARNE
TEAMWORK	UMIEJĘTNOŚĆ PRACY ZESPOŁOWEJ
PROBLEM SOLVING	UMIEJĘTNOŚĆ ROZWIĄZYWANIA PROBLEMÓW
CREATIVITY	KREATYWNOŚĆ
HOLISTIC THINKING	MYŚLENIE HOLISTYCZNE
STRATEGIC THINKING	MYŚLENIE STRATEGICZNE
ETHICAL THINKING	MYŚLENIE ETYCZNE
CRITICAL THINKING	MYŚLENIE KRYTYCZNE
good	dobre
moderate	umiarkowane
low	niskie
very low	bardzo niskie
difficult to say	trudno powiedzieć

rys. 7. Ocena kompetencji przekrojowych absolwentów dokonywana przez grupę biznesowo-przemysłową

Organizacje wykazały mniejsze zadowolenie z kompetencji zawodowych zatrudnianych przez nie absolwentów; średnio tylko 54% oceniło pozycje z ogólnej listy kompetencji zawodowych jako dobre lub umiarkowane (patrz rys. 8), przy czym więcej było ocen *umiarkowane* niż *dobre* w przypadku wszystkich 10 kompetencji. Średnio 44% respondentów z grupy przemysłowo-biznesowej oceniło kompetencje zawodowe absolwentów jako *niskie* lub *bardzo niskie*. Najwyżej oceniane kompetencje zawodowe to **rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych** (65% wybrało ocenę *dobrą* lub *umiarkowaną*), **zarządzanie zapobieganiem ryzykom** (57%), **zarządzanie ryzykami w zakresie zabezpieczeń** oraz **znajomość zagadnień związanych z zabezpieczaniem sieci** (obie na poziomie 56%).

Najniżej ocenianymi kompetencjami zawodowymi były: **znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych** (56% respondentów z grupy przemysłowo-biznesowej oceniło poziom absolwentów w zakresie tej kompetencji jako *niski* lub *bardzo niski*), z**najomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT** (50%)

oraz w**iedza na temat podatności systemów na ataki i eksploitów w systemach** (46% oceniło poziom absolwentów w zakresie tej kompetencji jako *niski* lub *bardzo niski*).

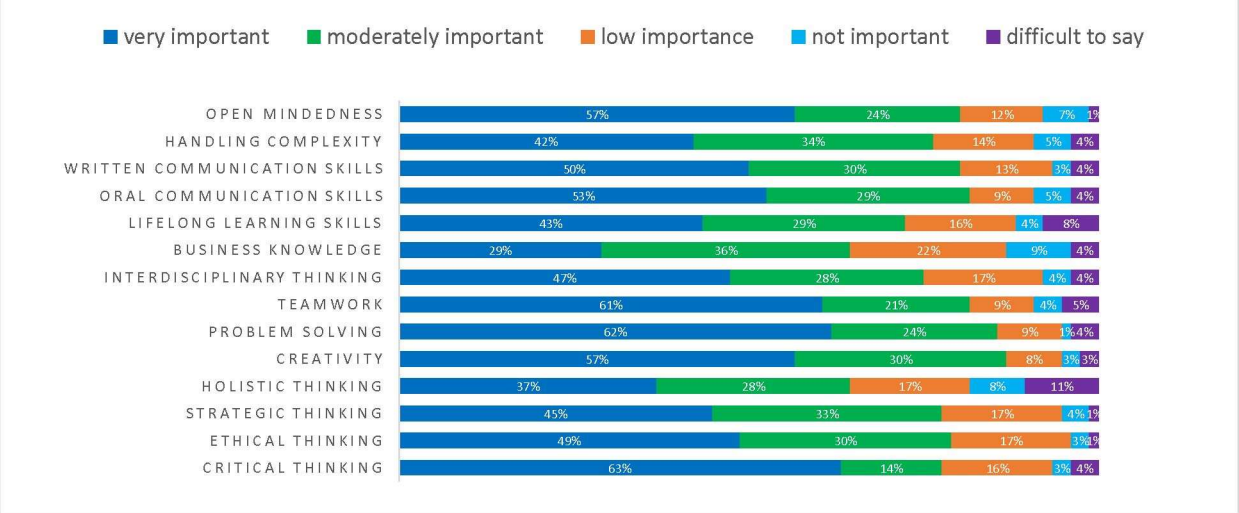


KNOWLEDGE OF CLOUD COMPUTING SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW CHMUROWYCH
KNOWLEDGE OF MOBILE AND IOT SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM URZĄDZEŃ MOBILNYCH I IOT
KNOWLEDGE OF OPERATING SYSTEM SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW OPERACYJNYCH
KNOWLEDGE OF NETWORK SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SIECI
ABILITY TO WRITE SCRIPT OR CODE	UMIEJĘTNOŚĆ PISANIA SKRYPTÓW LUB KODOWANIA
UNDERSTANDING OF SYSTEM LOGIC	ROZUMIENIE LOGIKI SYSTEMÓW
UNDERSTANDING OF SECURE WEB COMMUNICATIONS AND...	ZROZUMIENIE ZAGADNIEŃ BEZPIECZNEJ KOMUNIKACJI W INTERNECIE ORAZ ...
KNOWLEDGE OF VULNERABILITIES AND EXPLOITS OF SYSTEM	WIEDZA NA TEMAT PODATNOŚCI SYSTEMÓW NA ATAKI I EKSPLOITÓW W SYSTEMACH
RISK PREVENTION MANAGEMENT	ZARZĄDZANIE ZAPOBIEGANIEM RYZYKOM
SECURITY RISK ASSESSMENT	OCENA RYZYK W ZAKRESIE ZABEZPIECZEŃ
good	dobre
moderate	umiarkowane
low	niskie
very low	bardzo niskie
difficult to say	trudno powiedzieć

rys. 8. Ocena kompetencji zawodowych absolwentów ze strony grupy biznesowo-przemysłowej

Spojrzenie z punktu widzenia sektora edukacyjnego

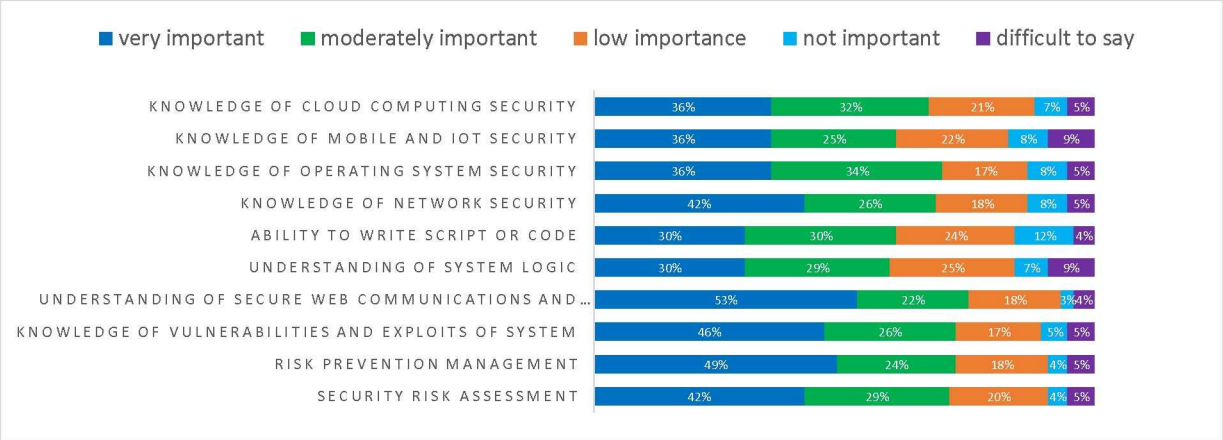
Odpowiedzi z sektora edukacji na temat znaczenia kompetencji przekrojowych były podobne do tych z grupy przemysłowo-biznesowej, przy czym 78% oceniło kompetencje z ogólnej listy jako *bardzo ważne* lub *umiarkowanie ważne* (rys. 9). Kompetencje przekrojowe uznane za najważniejsze to **kreatywność** (*bardzo ważna* lub *umiarkowanie ważna* dla 87% respondentów), **umiejętność rozwiązywania problemów** (dla 86% grupy), **umiejętności w zakresie komunikacji werbalnej** i **praca zespołowa** (dla 82%). Kompetencje przekrojowe ocenione jako *mało ważne* lub *nieważne* to **wiedza biznesowa** (*mało ważna* lub *nieistotna* dla 31%), **myślenie holistyczne** (25%) i **myślenie strategiczne** (21%). Te niskie oceny wydają się potwierdzać pogląd grupy przemysłowo-biznesowej, że absolwenci nie mają wystarczających kompetencji w tych dziedzinach (porównaj z rys. 7).



OPEN MINDEDNESS	OTWARTOŚĆ UMYSŁU
HANDLING COMPLEXITY	RADZENIE SOBIE ZE ZŁOŻONOŚCIĄ PROBLEMÓW
WRITTEN COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI PISEMNEJ
ORAL COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI WERBALNEJ
LIFELONG LEARNING SKILLS	UMIEJĘTNOŚĆ UCZENIA SIĘ PRZEZ CAŁE ŻYCIE
BUSINESS KNOWLEDGE	WIEDZA BIZNESOWA
INTERDISCIPLINARY THINKING	MYŚLENIE INTERDYSCYPLINARNE
TEAMWORK	UMIEJĘTNOŚĆ PRACY ZESPOŁOWEJ
PROBLEM SOLVING	UMIEJĘTNOŚĆ ROZWIĄZYWANIA PROBLEMÓW
CREATIVITY	KREATYWNOŚĆ
HOLISTIC THINKING	MYŚLENIE HOLISTYCZNE
STRATEGIC THINKING	MYŚLENIE STRATEGICZNE
ETHICAL THINKING	MYŚLENIE ETYCZNE
CRITICAL THINKING	MYŚLENIE KRYTYCZNE
very important	bardzo ważne
moderately important	umiarkowanie ważne
low importance	mało ważne
not important	nieistotne
difficult to say	trudno powiedzieć

rys. 9. Punkt widzenia grupy edukacyjnej na znaczenie kompetencji przekrojowych

Większość respondentów w grupie edukacyjnej pochodziła z sektora szkolnictwa wyższego. Na pytanie o znaczenie 10 wymienionych kompetencji zawodowych 75% przyznało, że **rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych** jest *bardzo ważne* lub *umiarkowanie ważne* (patrz rys. 10). **Zarządzanie zapobieganiem ryzykom** oraz **wiedza na temat podatności systemów na ataki i eksploitów w systemach** zostały uznane za *bardzo ważne* lub *umiarkowanie ważne* odpowiednio przez 73% i 72% respondentów z grupy edukacyjnej. Najniżej pod względem ważności oceniono **umiejętność pisania skryptów lub kodowania** (36% oceniło ją jako *mało ważną* lub *nieistotną*), **rozumienie logiki systemów** (32%) **oraz znajomość urządzeń mobilnych i IoT** (30%).



KNOWLEDGE OF CLOUD COMPUTING SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW CHMUROWYCH
KNOWLEDGE OF MOBILE AND IOT SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM URZĄDZEŃ MOBILNYCH I IOT
KNOWLEDGE OF OPERATING SYSTEM SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW OPERACYJNYCH
KNOWLEDGE OF NETWORK SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SIECI
ABILITY TO WRITE SCRIPT OR CODE	UMIEJĘTNOŚĆ PISANIA SKRYPTÓW LUB KODOWANIA
UNDERSTANDING OF SYSTEM LOGIC	ROZUMIENIE LOGIKI SYSTEMÓW
UNDERSTANDING OF SECURE WEB COMMUNICATIONS AND...	ZROZUMIENIE ZAGADNIEŃ BEZPIECZNEJ KOMUNIKACJI W INTERNECIE ORAZ ...
KNOWLEDGE OF VULNERABILITIES AND EXPLOITS OF SYSTEM	WIEDZA NA TEMAT PODATNOŚCI SYSTEMÓW NA ATAKI I EKSPLOITÓW W SYSTEMACH
RISK PREVENTION MANAGEMENT	ZARZĄDZANIE ZAPOBIEGANIEM RYZYKOM
SECURITY RISK ASSESSMENT	OCENA RYZYK W ZAKRESIE ZABEZPIECZEŃ
very important	bardzo ważne
moderately important	umiarkowanie ważne
low importance	mało ważne
not important	nieistotne
difficult to say	trudno powiedzieć

rys. 10. Punkt widzenia grupy edukacyjnej dotyczący znaczenia nadanego przez przedsiębiorstwo kompetencjom zawodowym

Warto zauważyć, że opinia grupy przemysłowo-biznesowej na temat znaczenia kompetencji przekrojowych, a zwłaszcza zawodowych absolwentów, niezależnie od ich regionu geograficznego, w pewnym stopniu odzwierciedla odpowiedzi sektora edukacji na temat znaczenia tych kompetencji.

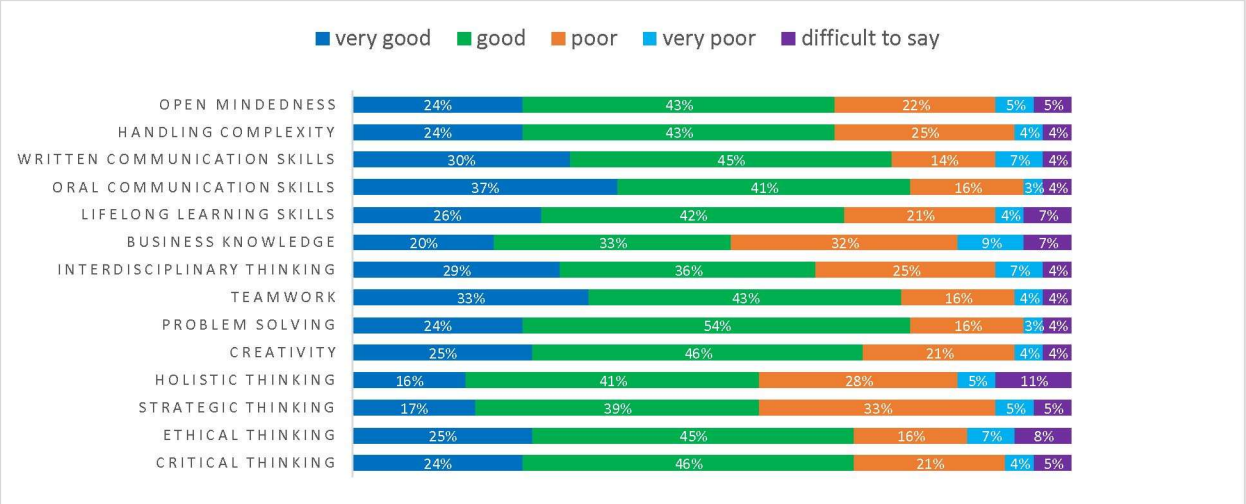
Dziewiętnastu respondentów z sektora edukacji dodało do listy inne kompetencje przekrojowe, w tym myślenie projektowe, umiejętność bezpiecznego działania w środowisku cyfrowym oraz umiejętność ochrony własnej prywatności w środowisku cyfrowym. Inne kompetencje zawodowe uznane za ważne to:

- Rozumienie środowiska cyfrowego i Internetu;
- Zgodność z zasadami, znajomość przepisów prawnych i prawa cybernetycznego;
- Rozumienie ekonomicznych aspektów zabezpieczeń;
- Umiejętność korzystania z pomocy informatycznej;
- Wiedza na temat pojawiających się trendów;
- Umiejętność efektywnego korzystania z nowoczesnych technologii.

Respondenci z grupy edukacyjnej wspomnieli również o znaczeniu **integracji cyfrowej**, w sytuacji gdy w klasach szkolnych ma miejsce transformacja technologiczna.

Ocena poziomu kompetencji absolwentów dokonana przez grupę edukacyjną

Grupa edukacyjna ogólnie umiarkowanie oceniła poziom kompetencji przekrojowych swoich absolwentów, średnio 68% oceniło wymienione kompetencje jako *bardzo dobre* lub *dobre* (patrz rys. 11). **Umiejętności w zakresie komunikacji werbalnej** i **rozwiązywania problemów** zostały ocenione najwyżej - 78% respondentów oceniło poziom swoich absolwentów jako *dobry* lub *bardzo dobry*, w dalszej kolejności była **praca zespołowa** - 76%. Najniżej oceniono następujące kompetencje przekrojowe: **wiedzę biznesową** (41% respondentów z dziedziny edukacji oceniło to kryterium *nisko* lub *bardzo nisko*), **myślenie strategiczne** i **myślenie holistyczne** (odpowiednio 38% i 33%).

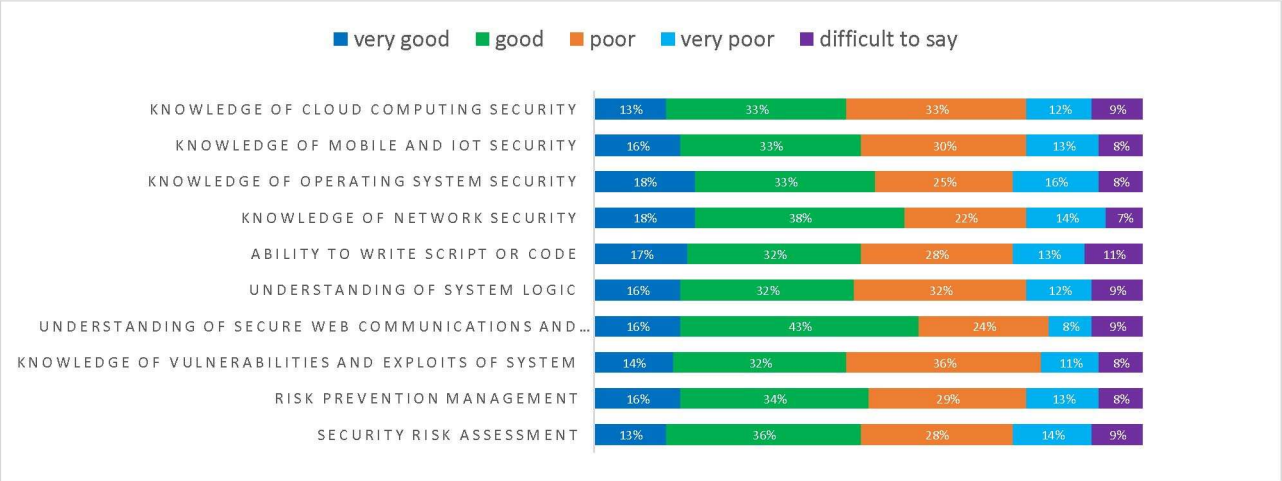


OPEN MINDEDNESS	OTWARTOŚĆ UMYSŁU
HANDLING COMPLEXITY	RADZENIE SOBIE ZE ZŁOŻONOŚCIĄ PROBLEMÓW
WRITTEN COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI PISEMNEJ
ORAL COMMUNICATION SKILLS	UMIEJĘTNOŚCI W ZAKRESIE KOMUNIKACJI WERBALNEJ
LIFELONG LEARNING SKILLS	UMIEJĘTNOŚĆ UCZENIA SIĘ PRZEZ CAŁE ŻYCIE
BUSINESS KNOWLEDGE	WIEDZA BIZNESOWA
INTERDISCIPLINARY THINKING	MYŚLENIE INTERDYSCYPLINARNE
TEAMWORK	UMIEJĘTNOŚĆ PRACY ZESPOŁOWEJ
PROBLEM SOLVING	UMIEJĘTNOŚĆ ROZWIĄZYWANIA PROBLEMÓW
CREATIVITY	KREATYWNOŚĆ
HOLISTIC THINKING	MYŚLENIE HOLISTYCZNE
STRATEGIC THINKING	MYŚLENIE STRATEGICZNE
ETHICAL THINKING	MYŚLENIE ETYCZNE
CRITICAL THINKING	MYŚLENIE KRYTYCZNE
very good	bardzo dobra
good	dobre
poor	słaba
very poor	bardzo słaba
difficult to say	trudno powiedzieć

rys. 11: Spojrzenie grupy edukacyjnej na kompetencje przekrojowe ich absolwentów

Ogólny poziom kompetencji zawodowych absolwentów, kluczowy aspekt z perspektywy branży cyberbezpieczeństwa, został oceniony jeszcze niżej przez przedstawicieli sektora

edukacyjnego niż sektora przemysłowo-biznesowego (patrz rys. 12). Średnio tylko połowa respondentów w grupie edukacyjnej oceniła kompetencje absolwentów pozytywnie (*bardzo dobrze* lub *dobrze*). Najwyżej oceniono **rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych** - 59% przyznało ocenę *bardzo dobrą* lub *dobrą*, następnie **znajomość zagadnień związanych z zabezpieczaniem sieci** (56%) i **znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych** (51%). **Wiedza na temat podatności systemów na ataki i eksploitów w systemach** oraz **znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych** zostały ocenione jako słabo przyswojone kompetencje, z ogólną oceną *niska* i *bardzo niska* odpowiednio 47% i 45%, w dalszej kolejności były **rozumienie logiki systemów** (44%) oraz **znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT** (43%). Może to świadczyć o rozbieżności między oczekiwaniami przemysłu a celami lub przynajmniej wynikami sektora edukacji.



KNOWLEDGE OF CLOUD COMPUTING SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW CHMUROWYCH
KNOWLEDGE OF MOBILE AND IOT SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM URZĄDZEŃ MOBILNYCH I IOT
KNOWLEDGE OF OPERATING SYSTEM SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SYSTEMÓW OPERACYJNYCH
KNOWLEDGE OF NETWORK SECURITY	ZNAJOMOŚĆ ZAGADNIEŃ ZWIĄZANYCH Z ZABEZPIECZANIEM SIECI
ABILITY TO WRITE SCRIPT OR CODE	UMIEJĘTNOŚĆ PISANIA SKRYPTÓW LUB KODOWANIA
UNDERSTANDING OF SYSTEM LOGIC	ROZUMIENIE LOGIKI SYSTEMÓW
UNDERSTANDING OF SECURE WEB COMMUNICATIONS AND ...	ZROZUMIENIE ZAGADNIEŃ BEZPIECZNEJ KOMUNIKACJI W INTERNECIE ORAZ ...
KNOWLEDGE OF VULNERABILITIES AND EXPLOITS OF SYSTEM	WIEDZA NA TEMAT PODATNOŚCI SYSTEMÓW NA ATAKI I EKSPLOITÓW W SYSTEMACH
RISK PREVENTION MANAGEMENT	ZARZĄDZANIE ZAPOBIEGANIEM RYZYKOM
SECURITY RISK ASSESSMENT	OCENA RYZYK W ZAKRESIE ZABEZPIECZEŃ
very good	bardzo dobra
good	dobre
poor	słaba
very poor	bardzo słaba
difficult to say	trudno powiedzieć

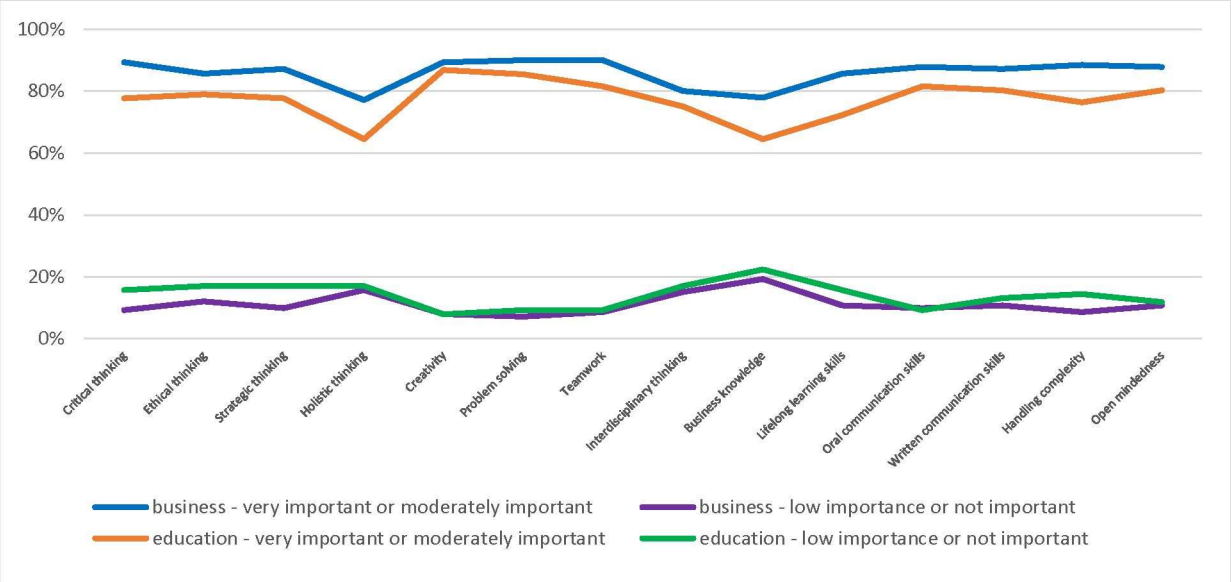
rys. 12. Punkt widzenia grupy edukacyjnej w zakresie kompetencji zawodowych absolwentów

Z małymi wyjątkami, punkty widzenia obu sektorów (biznesowo-przemysłowego i edukacyjnego) są w dużej mierze do siebie podobne. Prawie te same kompetencje przekrojowe i zawodowe były wskazywane jako najbardziej i najmniej rozwinięte. Niemniej jednak przedstawiciele sektora edukacyjnego wydają się być nieco bardziej optymistyczni, jeśli chodzi o poziom kompetencji swoich absolwentów, niż przedstawiciele sektora przemysłowo-biznesowego, jeśli chodzi o kompetencje zatrudnianych absolwentów.

4. Zdefiniowanie rozbieżności, zaproponowanie rozwiązań

Bliższe spojrzenie na braki w zakresie kompetencji przekrojowych

Odpowiedzi udzielone w kwestionariuszu ankiety online potwierdziły założenia wyciągnięte z wywiadów. Interesariusze zarówno z sektora edukacji, jak i przemysłowo-biznesowego wydają się zgodni co do znaczenia kompetencji przekrojowych i zawodowych, zawartych w tym modelu, dla potrzeb cyberbezpieczeństwa we współczesnym świecie. Jednakże respondenci z sektora przemysłowo-biznesowego przypisywali większe znaczenie obu listom kompetencji w porównaniu z sektorem edukacyjnym: 86% wobec 78% dla kompetencji przekrojowych i 82% wobec 68% dla kompetencji zawodowych (patrz rys. 13 i 15).

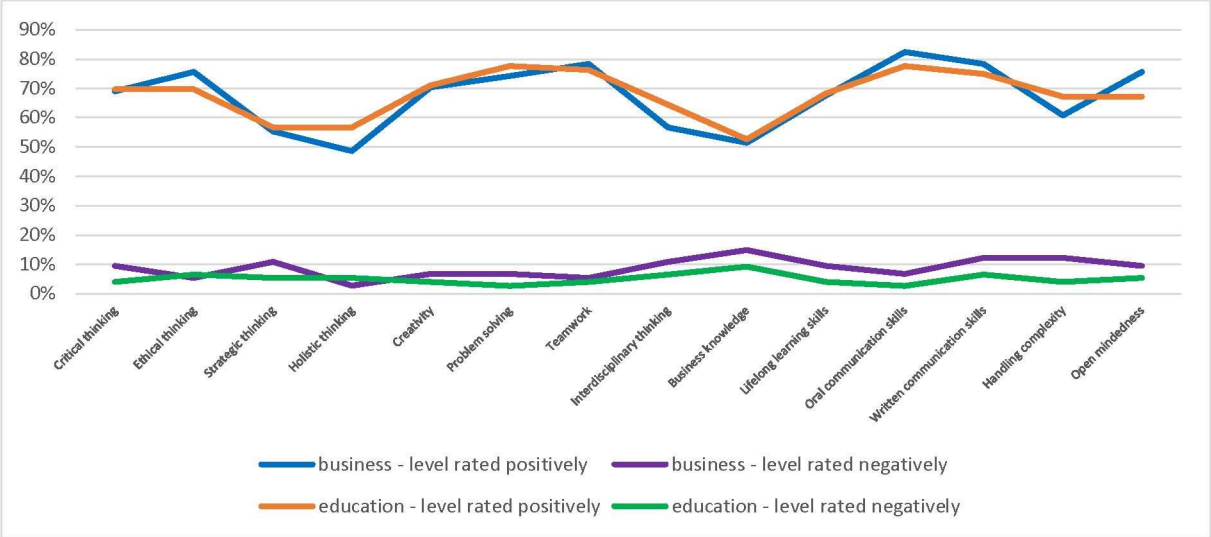


Critical thinking	Myślenie krytyczne
Ethical thinking	Myślenie etyczne
Strategic thinking	Myślenie strategiczne
Holistic thinking	Myślenie holistyczne
Creativity	Kreatywność
Problem solving	Umiejętność rozwiązywania problemów
Teamwork	Umiejętność pracy zespołowej
Interdisciplinary thinking	Myślenie interdyscyplinarne
Business knowledge	Wiedza biznesowa
Lifelong learning skills	Umiejętność uczenia się przez całe życie
Oral communication skills	Umiejętności w zakresie komunikacji werbalnej
Written communication skills	Umiejętności w zakresie komunikacji pisemnej
Handling complexity	Radzenie sobie ze złożonością problemów
Open mindedness	Otwartość umysłu
business - very important or moderately important	środowisko biznesowe - bardzo ważna lub umiarkowanie ważna

education - very important or moderately important	środowisko edukacyjne - bardzo ważna lub umiarkowanie ważna
business - low importance or not important	środowisko biznesowe - mało ważna lub nieistotna
education - low importance or not important	środowisko edukacyjne - mało ważna lub nieistotna

rys. 13. Porównanie odpowiedzi grup przemysłowo-biznesowych i edukacyjnych na temat znaczenia kompetencji przekrojowych

Oba sektory oceniają **etyczne myślenie**, **umiejętność rozwiązywania problemów**, **umiejętność pracy zespołowej** oraz **umiejętności w zakresie komunikacji werbalnej** i **pisemnej** jako dość dobre. **Myślenie krytyczne**, **kreatywność**, **umiejętność uczenia się przez całe życie**, **radzenie sobie ze złożonością problemów** i **otwartość umysłu** zostały ocenione jako kryteria umiarkowanie istotne. Najniżej oceniono myślenie strategiczne, holistyczne i interdyscyplinarne oraz wiedzę biznesową.

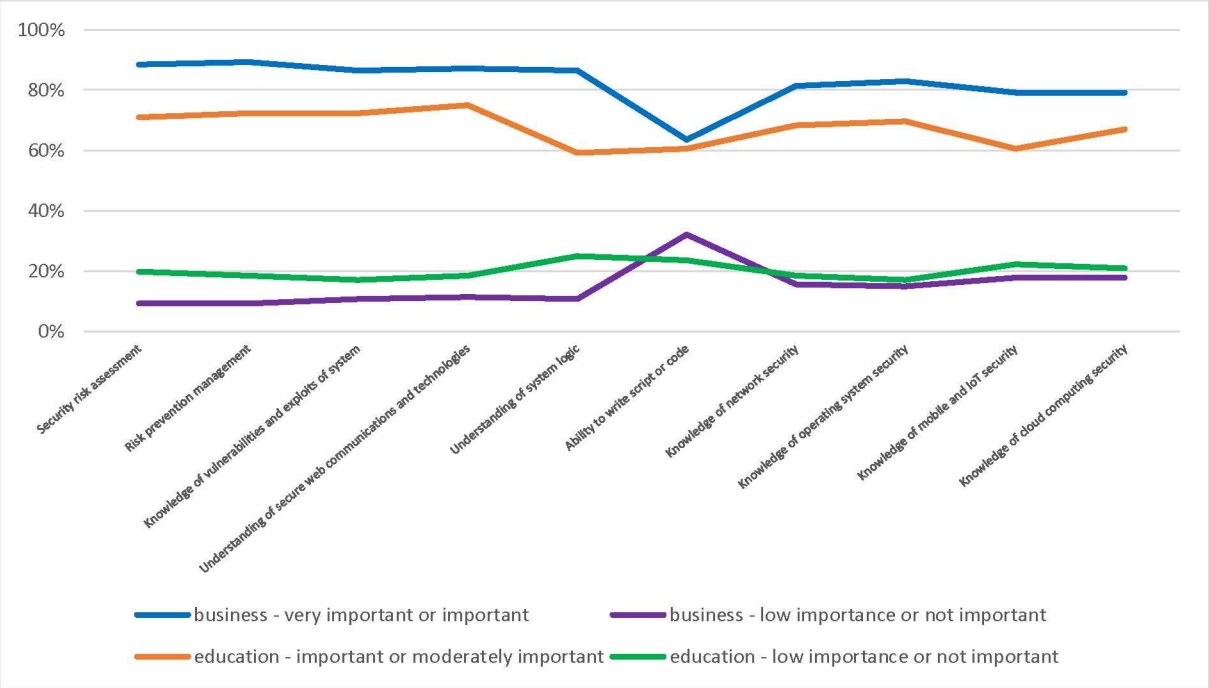


Critical thinking	Myślenie krytyczne
Ethical thinking	Myślenie etyczne
Strategic thinking	Myślenie strategiczne
Holistic thinking	Myślenie holistyczne
Creativity	Kreatywność
Problem solving	Umiejętność rozwiązywania problemów
Teamwork	Umiejętność pracy zespołowej
Interdisciplinary thinking	Myślenie interdyscyplinarne
Business knowledge	Wiedza biznesowa
Lifelong learning skills	Umiejętność uczenia się przez całe życie
Oral communication skills	Umiejętności w zakresie komunikacji werbalnej
Written communication skills	Umiejętności w zakresie komunikacji pisemnej
Handling complexity	Radzenie sobie ze złożonością problemów
Open mindedness	Otwartość umysłu
business - very important or moderately important	środowisko biznesowe - bardzo ważna lub umiarkowanie ważna
education - very important or moderately important	środowisko edukacyjne - bardzo ważna lub umiarkowanie ważna
business - low importance or not important	środowisko biznesowe - mało ważna lub nieistotna
education - low importance or not important	środowisko edukacyjne - mało ważna lub nieistotna

rys. 14. Porównanie odpowiedzi między grupami przemysłowo-biznesowymi i edukacyjnymi na temat poziomu kompetencji przekrojowych absolwentów

Bliższe spojrzenie na braki w zakresie kompetencji zawodowych

Chociaż respondenci z grupy edukacyjnej nadali mniejszą wagę rozwojowi kompetencji zawodowych (60% respondentów uznało ogólny zakres kompetencji zawodowych za ważny, a 30% oceniło je jako nieważne), wydaje się, że w obu sektorach istnieje, na rozsądnym poziomie, wspólne zrozumienie znaczenia kompetencji zawodowych (patrz rys. 15).



Security risk assessment	Ocena ryzyk w zakresie zabezpieczeń
Risk prevention management	Zarządzanie zapobieganiem ryzykom
Knowledge of vulnerabilities and exploits of system	Wiedza na temat podatności systemów na ataki i eksploitów w systemach
Understanding of secure web communications and technologies	Rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
Understanding of system logic	Rozumienie logiki systemów
Ability to write script or code	Umiejętność pisania skryptów lub kodowania
Knowledge of network security	Znajomość zagadnień związanych z zabezpieczaniem sieci
Knowledge of operating system security	Znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
Knowledge of mobile and IoT security	Znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
Knowledge of cloud computing security	Znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych
business - very important or important	grupa biznesowa - bardzo ważna lub ważna
education - important or moderately important	grupa edukacyjna - ważna lub umiarkowanie ważna
business - low importance or not important	środowisko biznesowe - mało ważna lub nieistotna
education - low importance or not important	środowisko edukacyjne - mało ważna lub nieistotna

rys. 15. Porównanie odpowiedzi między grupami przemysłowo-biznesowymi i edukacyjnymi na temat znaczenia kompetencji zawodowych

Obie grupy respondentów prezentowały podobne opinie na temat poziomu kompetencji zawodowych absolwentów. Jak widać na rys. 16,[16] średnio około połowa respondentów z obu

[16] Możesz również zapoznać się z rysunkami 8 i 11

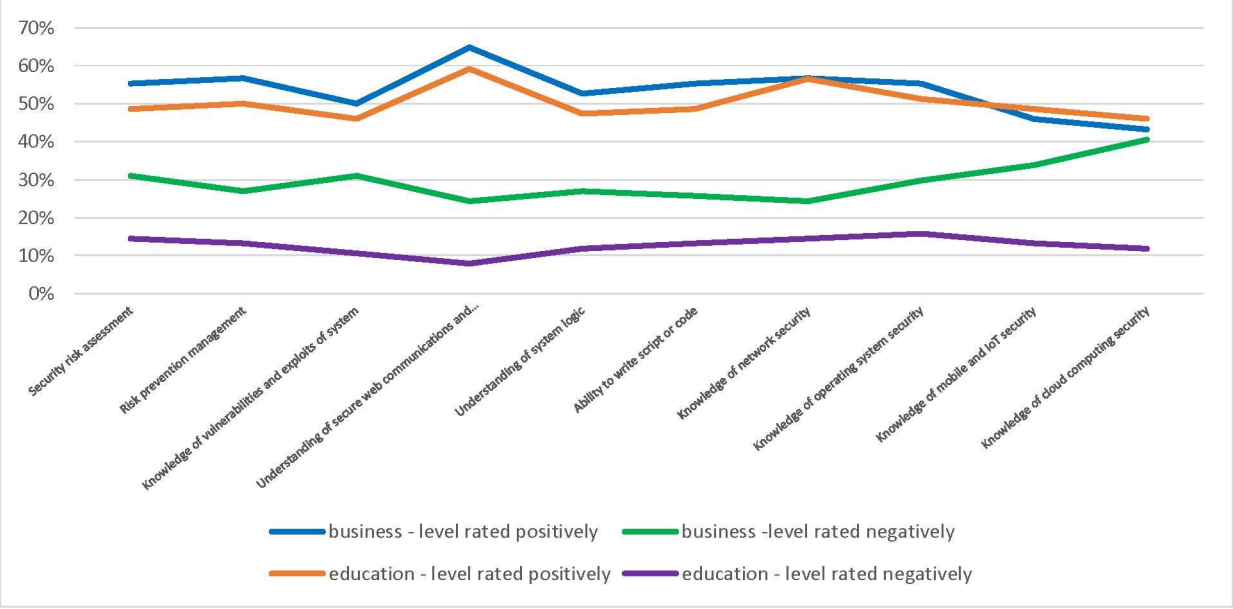
grup oceniła poziom rozwoju kompetencji zawodowych pozytywnie, natomiast średnio 44% respondentów z grupy biznesowej i 41% z grupy edukacyjnej oceniło ten poziom jako niski lub bardzo niski. Żadna z pozytywnych ocen (*bardzo dobra* lub *dobra*) dla jakiejkolwiek kompetencji nie osiągnęła 60%, z wyjątkiem **rozumienia zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych** (65% w sektorze przedsiębiorstw i 59% w sektorze edukacji).

Kolejne pięć kompetencji zawodowych ocenionych przez obie grupy na około 50%:

- Znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych;
- Znajomość zagadnień związanych z zabezpieczaniem sieci;
- Zarządzanie zapobieganiem ryzykom;
- Zrozumienie zagadnień bezpiecznej komunikacji w Internecie oraz ...
- Ocena ryzyk w zakresie zabezpieczeń
- Rozumienie logiki systemów;
- Umiejętność pisania skryptów lub kodowania.

Trzy kompetencje zawodowe zostały ocenione przez obie grupy jako słabe:

- Wiedza na temat podatności systemów na ataki i eksploitów w systemach;
- Znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT;
- Znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych.



Security risk assessment	Ocena ryzyk w zakresie zabezpieczeń
Risk prevention management	Zarządzanie zapobieganiem ryzykom
Knowledge of vulnerabilities and exploits of system	Wiedza na temat podatności systemów na ataki i eksploitów w systemach
Understanding of secure web communications and …	Zrozumienie zagadnień bezpiecznej komunikacji w Internecie oraz ...
Understanding of system logic	Rozumienie logiki systemów
Ability to write script or code	Umiejętność pisania skryptów lub kodowania
Knowledge of network security	Znajomość zagadnień związanych z zabezpieczaniem sieci
Knowledge of operating system security	Znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
Knowledge of mobile and IoT security	Znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT

Knowledge of cloud computing security	Znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych
business - level rated positively	grupa biznesowa - poziom oceniony pozytywnie
education - level rated positively	grupa edukacyjna - poziom oceniony pozytywnie
business -level rated negatively	grupa biznesowa - poziom oceniony negatywnie
education - level rated negatively	grupa edukacyjna - poziom oceniony negatywnie

rys. 16. Porównanie odpowiedzi między grupami przemysłowo-biznesowymi i edukacyjnymi na temat poziomu kompetencji zawodowych absolwentów

Szkolenia odpowiadające aktualnym i pojawiającym się potrzebom

Przeważająca większość sugestii (52) i dobrych praktyk (24) przedstawionych przez respondentów opisywała **Szkolenie** jako najbardziej skuteczne rozwiązanie. Wymieniano różne formy szkoleń, od online i hybrydowych, po szkolenia mieszane (ang. *blended learning*) i sesje offline. Respondenci wymieniali kursy, programy rozwojowe, warsztaty, spotkania, seminaria, projekty, wykłady, mentoring, aktualizację wiadomości i wymianę doświadczeń. Za konieczne uznano zarówno tryb offline, jak i online. Najpopularniejszymi metodami szkoleniowymi wydają się być: uczenie się w oparciu o problemy, współpraca i uczenie się od siebie nawzajem, w przeciwieństwie do szkoleń prowadzonych przez instruktorów. Za konieczne uznano zarówno długoterminowe programy rozwojowe dostosowane do potrzeb, jak i krótkoterminowe wydarzenia, a także kursy udostępniane przez Internet (ang. *MOOCs*), demonstracje, wykłady i prezentacje. Respondenci często wspominali o potrzebie kursów wewnętrznych, dostosowanych do potrzeb danej organizacji, choć doceniano rolę szkoleń zewnętrznych, zwłaszcza oferowanych przez renomowane ośrodki i organizacje zajmujące się problematyką cyberbezpieczeństwa.

Niektóre organizacje oferują szkolenia **regularne**, inne proponują je **ad hoc** i/lub dla nowo zatrudnionych pracowników. Niektórzy wolą realizować wewnętrzne programy szkoleniowe, na przykład prowadzone przez doświadczonego pracodawcę dla innych pracowników. Inni wolą odpowiadać na wewnętrzne potrzeby szkoleniowe, wysyłając pracowników na wydarzenia zewnętrzne, lub nawet zachęcają kierowników zespołów do wyboru kursów, które są finansowane z budżetu edukacyjnego firmy. Wymieniono certyfikację i staże, podając przykłady certyfikacji wewnętrznej opartej na polityce cyberbezpieczeństwa firmy oraz certyfikacji zewnętrznej oferowanej przez renomowane organizacje.

Skuteczne szkolenia opisywano jako takie, które:

- Są oparte na ocenie potrzeb;
- oferują szybko możliwe do zastosowania i wykonalne rozwiązania;
- zwiększają motywację i świadomość pracowników;
- oferują gotowy dostęp do zasobów i narzędzi, które pomagają w rozwijaniu niezbędnych kompetencji.

Inne przykłady dobrych praktyk związanych z rozwojem osobistym pracowników to:

- Praca nad projektem i uczenie się przez działanie;
- Podnoszenie świadomości w firmie;
- Opieka ze strony mentora;
- Wzajemne ocenianie i uczenie się przez samych pracowników;
- Obszerna dokumentacja;
- Wdrożenie ISO 27001 i 22301;
- Procesy rekrutacyjne z uwzględnieniem inżynierii społecznej w celu zatrudnienia

wysoko zmotywowanych kandydatów;
- Zasady organizowania zabezpieczeń i Podręcznik dla personelu;
- Dyskusje na temat oceny wyników;
- Współpraca z uniwersytetami;
- Wymiany (wiedzy, pracowników) pomiędzy podmiotami biznesowymi;
- Outsourcing.

Wyrażono również powszechne zrozumienie dla potrzeby przeznaczenia większego budżetu na rozwój zawodowy pracowników, chociaż istniała również obawa, że dobrze wyszkoleni specjaliści opuszczą swoje organizacje w poszukiwaniu lepszych możliwości.

Lepsza koordynacja pomiędzy edukacją a przemysłem

Drugim, bardzo ważnym czynnikiem sukcesu, wyrażonym przez ponad połowę respondentów, była **koordynacja i współpraca pomiędzy edukacją a przemysłem**. Cyberbezpieczeństwo jest uważane za ważny temat na wszystkich poziomach edukacji i wymaga aktualnych branżowych informacji, po to aby budować potencjał wszystkich obywateli, nie tylko tych, których ścieżka zawodowa jest ściśle związana z bezpieczeństwem cybernetycznym. Drugim jasno wyrażonym oczekiwaniem było to, że ścieżka edukacyjna powinna być mniej teoretyczna, a bardziej związana z codziennymi wyzwaniami. Edukacja powinna przygotowywać uczniów do rozwiązywania problemów, a nie do zapamiętywania faktów. „Byłby to sposób, aby absolwenci lepiej wykonywali swoje zadania i byli lepiej przygotowani do pracy w branży", stwierdził jeden z respondentów.

Komentarze respondentów dotyczące edukacji często poruszały takie aspekty jak:
- Nawiązanie ścisłej współpracy i stałego dialogu między instytucjami szkoleniowymi a pracodawcami w celu zapewnienia szkoleniowcom aktualnych informacji o bieżących potrzebach związanych z praktyką;
- Włączenie treści dotyczących cyberbezpieczeństwa do programów nauczania na poziomie podstawowym, średnim, wyższym i podyplomowym;
- Wdrażanie zaktualizowanych programów nauczania, które są zgodne z aktualnymi potrzebami przemysłu/biznesu;
- Wcześniejsze zaangażowanie studentów w działalność przemysłową i gospodarczą;
- Zapewnienie studentom możliwości obserwowania profesjonalistów w trakcie studiów.

Każda z poniższych sugestii została wyrażona przez co najmniej 3 respondentów:
- Bliższa współpraca między sektorem przemysłowo-biznesowym a ekspertami i organizacjami zajmującymi się cyberbezpieczeństwem;
- Dostawcy usług w zakresie cyberbezpieczeństwa mogliby zaoferować bezpłatną lub przystępną współpracę z dyrektorami ds. bezpieczeństwa (ang. Chief Security Officer - CSO);
- Zwiększona uwaga państw na kwestię cyberbezpieczeństwa i odpowiednia rewizja przepisów;
- Lepsza promocja kariery w dziedzinie cyberbezpieczeństwa wśród młodzieży;
- Wspieranie badań i rozwoju wiedzy w zakresie cyberbezpieczeństwa;
- Możliwość wymiany wiedzy między dostawcami usług w zakresie cyberbezpieczeństwa, aby uniknąć sytuacji, w której różne firmy koncentrują swoje wysiłki tam, gdzie rozwiązania już istnieją.

W dalszych komentarzach podkreślano znaczenie zachęcania większej liczby kobiet do podejmowania studiów w STEM (nauka, technologia, inżynieria, matematyka) - wszystkich szybko rozwijających się sektorach gospodarki, w których różnorodność jest niezbędna.

Zmniejszanie luki z punktu widzenia sektora edukacji

Trzydziestu czterech respondentów z sektora edukacji podzieliło się swoimi sugestiami, w jaki sposób można zniwelować lukę między poziomem kompetencji absolwentów a oczekiwaniami przemysłu. Podobnie jak w przypadku sugestii respondentów z grupy przemysłowo-biznesowej, najczęstszą propozycją było **nawiązanie ścisłej współpracy między edukacją a sektorem przemysłowo-biznesowym**, głównie w celu:

- Lepszego zrozumienia potrzeb pracodawców;
- Dostosowania wzajemnych oczekiwań;
- Włączenia zagadnień związanych z cyberbezpieczeństwem do programów nauczania poszczególnych przedmiotów;
- Modernizacji metod nauczania i uczenia się;
- Sprowadzenia ekspertów technologicznych z branży na seminaria dotyczące zabezpieczeń;
- Organizowania praktyk, wizyt w terenie, warsztatów, seminariów, staży i zatrudnienia studentów, programów mentorskich itp.

Respondenci uważają, że szkolenie wstępne powinno obejmować więcej:

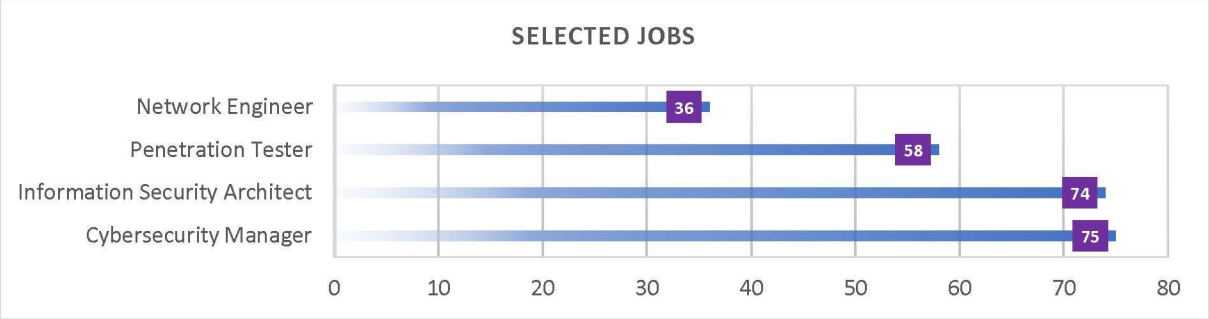
- Specyficznych modułów cyberbezpieczeństwa (np. zabezpieczenia rozwiązań chmurowych), na żądanie;
- Studiów przypadków z zakresu cyberbezpieczeństwa, które można włączyć do szerszych kursów;
- Rozwoju umiejętności praktycznych;
- Pracy w terenie (u klientów);
- Uwagi poświęconej umiejętnościom miękkim;
- Podnoszenia świadomości na temat znaczenia cyberbezpieczeństwa;
- Regularnych aktualizacji informacji;
- Możliwości zastosowania teorii w praktyce;
- Wykorzystania wirtualnych możliwości multimedialnych.

Niektórzy respondenci uważają, że wszystkie wyżej wymienione zmiany powinny być wprowadzone na wszystkich poziomach edukacji, od podstawowego i średniego do wyższego. Kilku naukowców przywołało znaczenie takich czynników jak:

- Doskonalenie zawodowe nauczycieli na poziomie podstawowym i średnim;
- Istotne zmiany w przepisach i standardach edukacyjnych;
- Szersze wsparcie dla zmian w zakresie informacji i komunikacji w systemach edukacyjnych;
- Większa uwaga poświęcona integracji cyfrowej;
- Niwelowanie różnic w zakresie równości płci i równości społeczno-ekonomicznej;
- Kwestie związane z certyfikacją;
- Monitorowanie i ocena zadań w sektorze edukacji.

Trudne do obsadzenia stanowiska i ich wpływ na organizacje

Jedno z pytań uzupełniających do grupy przemysłowo-biznesowej dotyczyło rodzajów stanowisk pracy w zakresie cyberbezpieczeństwa, które najtrudniej jest obsadzić. Na podstawie ustaleń z wywiadów z liderami w sektorze cyberbezpieczeństwa zaproponowano cztery kategorie miejsc pracy (patrz rys. 17). Siedemdziesięciu pięciu respondentów z grupy przemysłowo-biznesowej wskazało na menedżerów ds. cyberbezpieczeństwa jako najtrudniejszą do obsadzenia rolę, 74 respondentów wskazało na architektów bezpieczeństwa informacji, a 58 na testerów penetracyjnych. Dla 36 respondentów rola inżyniera sieci wydawała się trudna do obsadzenia.



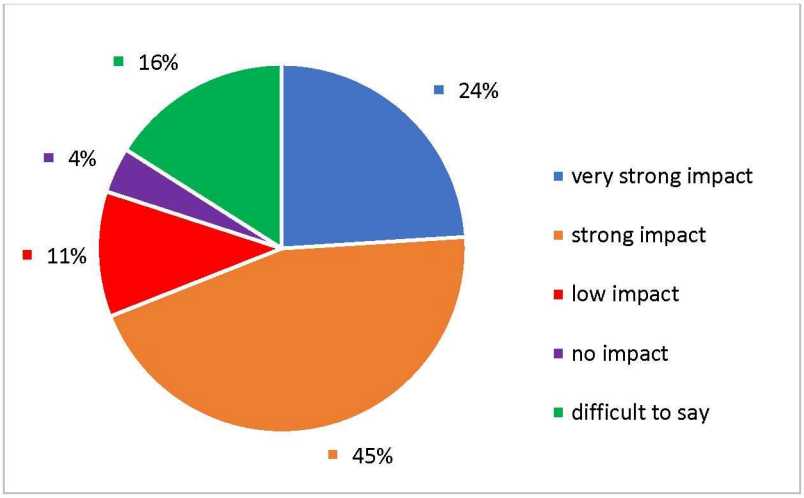
SELECTED JOBS	WYBRANE STANOWISKA PRACY
Network Engineer	Inżynier ds. sieci
Penetration Tester	Tester penetracyjny
Information Security Architect	Architekt bezpieczeństwa informacji
Cybersecurity Manager	Menedżer ds. cyberbezpieczeństwa

rys. 17: Spojrzenie sektora przemysłowo-biznesowego na stanowiska najtrudniejsze do obsadzenia

To pytanie pozwoliło respondentom uzupełnić listę. Pięć rodzajów pracy zostało wymienionych kilkakrotnie:

- Specjalista ds. zabezpieczania systemów chmurowych
- Inżynier backendowy systemów chmurowych
- Ekspert w dziedzinie uczenia maszynowego
- Analityk ds. informatyki śledczej
- Inżynier ds. Internetu 3 generacji (ang. *Web3*)

Według większości respondentów ten brak specjalistów ma *silny* (45%) lub *bardzo silny* (24%) wpływ na ich organizację; 15% uważa, że ten brak *nie ma wpływu* lub ma *niewielki wpływ*, a kolejne 16% ma trudności z oszacowaniem (patrz rys. 18).



very strong impact	bardzo silny wpływ
strong impact	silny wpływ
low impact	niewielki wpływ
no impact	nie ma wpływu
difficult to say	trudno powiedzieć

rys. 18: Wpływ trudności z rekrutacją na organizację

5. Wnioski i zalecenia

Zalecenia

Wyniki badania wskazują, że na poziomie globalnym sektory przemysłowo-biznesowe i edukacyjne są zgodne co do luki, jaka istnieje pomiędzy potrzebami i oczekiwaniami branży cyberbezpieczeństwa a poziomem kompetencji przekrojowych i zawodowych, jakie absolwenci wnoszą do miejsca pracy. Badanie potwierdza również zaproponowany model niezbędnych kompetencji przekrojowych i zawodowych w celu wypełnienia tej luki, który zostanie teraz nieco rozszerzony o sugestie wynikające z badania.

Z badań wynika siedem zaleceń, które zostaną przełożone na plan działania dla grupy roboczej nr 2 IS3C w 2023 roku:

1. **Poprawa edukacji i szkoleń:** uczestnicy badania niemal jednogłośnie zgadzają się, że większy, lepszy rozwój kompetencji jest antidotum na wiele wyzwań, przed którymi stoi sektor cyberbezpieczeństwa. Sugerują oni odejście od tradycyjnych form szkoleń bezpośrednich, internetowych i hybrydowych na rzecz uczenia się od siebie nawzajem i oceniania, mentoringu, pracy nad projektem, myślenia projektowego, uczenia się przez działanie i oceny formatywnej, aby sprostać szybko zmieniającym się potrzebom społeczeństwa w zakresie cyberbezpieczeństwa. Szczególną uwagę należy zwrócić na rozwój większej liczby szkoleń i możliwości certyfikacji w krajach takich jak Nepal, Wietnam, Samoa i w różnych regionach Afryki, gdzie zarówno ankieterzy, jak i respondenci podkreślają, że wiele miejsc pracy dla certyfikowanych ekspertów ds. cyberbezpieczeństwa pozostaje nieobsadzonych.
2. **Powrót do podstaw:** kreatywność młodych ludzi rozpoczynających pracę w dziedzinach związanych z technologią jest według wielu uczestników badań osłabiona przez brak wiedzy i zainteresowania tym, jak to wszystko działa. Sugerują oni, że młodzi ludzie stali się raczej użytkownikami i konsumentami niż budowniczymi, którzy tylko powierzchownie rozumieją technologię cyfrową, co także zostało podniesione w kilku innych badaniach. [17] Głębsze zrozumienie, jak działają takie rzeczy, jak szkielet Internetu, technologia chmurowa i blockchain, skutkowałoby większą innowacyjnością i zachęciłoby do myślenia lateralnego.

   Respondenci uważają, że zachęcanie dzieci do zastanowienia się nad tym, jak funkcjonują rzeczy, których używają w swoim codziennym życiu, powinno być integralną częścią edukacji w szkole podstawowej i średniej. Pomaga rozwinąć myślenie krytyczne i lepiej zrozumieć zjawiska powszechnie spotykane w sieci, takie jak manipulacja obrazem i informacją oraz strategie inżynierii społecznej. Powrót do podstaw wyszukiwania informacji również pomógłby ludziom lepiej zrozumieć działanie mechanizmów wyszukiwania, np. wyszukiwarki przynoszą efekt przeciwny do zamierzonego, gdy szuka się najnowszych informacji lub nowych pomysłów, ponieważ dane są uszeregowane według liczby wyświetleń danego dokumentu, co oznacza, że zazwyczaj starsze informacje

[17] OECD (2019). *Ramowy program twórczego myślenia PISA 2021.* Na stronie https://www.oecd.org/pisa/publications/PISA-2021-creative-thinking-framework.pdf, i UNESCO (2022). *Ponowne kształtowanie polityki na rzecz kreatywności - traktowanie kultury jako globalnego dobra publicznego.* Na stronie https://www.unesco.org/reports/reshaping-creativity/2022/en

wychodzą na pierwszy plan.

3. **Uświadamianie znaczenia cyberbezpieczeństwa na wszystkich poziomach edukacji:** cyberbezpieczeństwo jest naszą osobistą sprawą, tak jak zdrowie i dobre samopoczucie. Przedmioty IoT i cyfrowe gadżety do noszenia są obecnie codziennym aspektem życia większości ludzi i należy uświadomić im, że ochrona bezpieczeństwa ich urządzeń oraz świadomość praw i obowiązków w środowisku online jest nieodłącznym elementem zapewnienia cyberbezpieczeństwa. Jeżeli internet ma stać się miejscem zaufania, pojęcia te muszą być uwzględnione w programach nauczania. Uczynienie z cyberbezpieczeństwa przyjemnej części edukacji szkolnej mogłoby wzbudzić większe zainteresowanie tym tematem jako karierą zawodową i zapewniłoby solidne podstawy do przezwyciężenia powierzchowności wiedzy, która została skrytykowana w punkcie powyżej. Społeczeństwo jako całość musi zrozumieć znaczenie standardów internetowych związanych z bezpieczeństwem oraz najlepszych praktyk ICT dla własnego dobra i dla dobra ogółu. Bezpieczniejsze internetowe praktyki zmniejszyłyby zapotrzebowanie w sektorze cyberbezpieczeństwa, a być może także zwiększyłyby zainteresowanie karierami związanymi z cyberbezpieczeństwem.

4. **Usprawnienie współpracy między przemysłem a szkolnictwem** w celu zapewnienia, że edukacja dotrzymuje kroku pojawiającym się trendom technologicznym, ma większy dostęp do aktualnych narzędzi i zasobów oraz głębsze zrozumienie wymagań dotyczących kompetencji obywateli XXI wieku. Wyniki badania sugerują, że sektor edukacji przywiązuje mniejszą wagę do kompetencji przekrojowych i w większym stopniu do kompetencji zawodowych niż przemysł (patrz rys. 13), chociaż oba te sektory wyraziły podobne opinie, gdy zapytano je o poziom absolwentów (patrz rys. 12). Chociaż misja edukacji jest znacznie szersza niż zaspokajanie potrzeb przemysłu, bliższa współpraca może być korzystna dla obu partnerów.

   Aby młodzi ludzie mogli w pełni rozwinąć swój potencjał edukacyjny i swoją przyszłość, muszą korzystać i rozumieć technologię cyfrową, z której korzystają na co dzień, a pedagodzy potrzebują solidnej wiedzy na temat dzisiejszych narzędzi i platform informacyjno-komunikacyjnych. Respondenci sugerują, że bliższa współpraca z przemysłem mogłaby również ułatwić dzielenie się narzędziami i zasobami, a przy okazji otworzyć autentyczne możliwości dla placówek edukacyjnych w zakresie uczenia młodych ludzi, jak chronić ich prywatność i dane. Podczas jednego z wywiadów badawczych wymieniono duński CyberHub[18] jako trwały model współpracy między sektorem edukacji i przemysłu.

5. **Zwiększenie różnorodności:** niedostateczna reprezentacja młodych ludzi i kobiet w badaniach odzwierciedla ogólny brak różnorodności w zespołach zajmujących się cyberbezpieczeństwem.[19] A przecież różnorodność, jak wynika z najnowszych badań biznesowych, uwalnia innowacyjność, tworząc środowisko, w którym są widoczne pomysły „nieszablonowe”.[20] Pomaga zespołom podejmować lepsze decyzje, ponieważ mnoży punkty widzenia i sposoby patrzenia na problemy i zagrożenia, a także pozwala uniknąć niedopatrzeń przy wprowadzaniu środków bezpieczeństwa. Typowym

[18] https://cyberhub.dk/danish-cyberstartups-overview/danish-cyberstartups/
[19] https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[20] Harvard Business Review na stronie https://hbr.org/2013/12/how-diversity-can-drive-innovation

przykładem jest rozpoznawanie twarzy.[21] Kilku lat błędów sądowych można było uniknąć, gdyby wczesne wersje oprogramowania uwzględniały inne typy skóry i twarzy niż te, które posiadali głównie biali inżynierowie. W tak szybko rozwijającej się dziedzinie, jaką jest cyberbezpieczeństwo, kreatywność, innowacyjność i wieloaspektowe podejście są niezbędne, aby wyprzedzić hakerów i zagrożenia.

6. **Unowocześnienie procedur rekrutacyjnych:** kariera w cyberbezpieczeństwie byłaby bardziej atrakcyjna dla młodych ludzi, a zwłaszcza dla dziewcząt, gdyby w dzieciństwie i okresie nastoletnim mogły odkrywać ekscytujące wyzwania, możliwości i elastyczność, jakie oferuje ta dziedzina. Rozwiązaniem mogą być gry online, symulacje i zajęcia edukacyjne opracowane w ramach partnerstwa biznesu i edukacji. Na etapie zatrudniania algorytmiczne stronniczości dyskryminują populacje, które nie są jeszcze zainteresowane lub nie pracują w danym sektorze, eliminując dostęp grup mniejszościowych do danych możliwości zatrudnienia. Słaba wymiana wiedzy między sektorem edukacji i cyberbezpieczeństwa, szkolnictwem wyższym i zawodowym również ogranicza perspektywiczne podejście w dostosowywaniu edukacji i szkoleń do profili zawodowych, na które jest największe zapotrzebowanie. Wreszcie, procedury rekrutacyjne są, według kilku rozmówców, czasochłonne i często słabo przystosowane do zatrudniania pracowników o wysokim poziomie technicznym, chociaż wykorzystanie strategii inżynierii społecznej może rozwiązać ten ostatni problem.
7. **Zwiększenie skali dzielenia się wiedzą i dobrymi praktykami:** wymiana interesującymi dobrymi praktykami została podkreślona w badaniu zarówno przez przedstawicieli przemysłu, jak i edukacji, ale rzadko są one skalowane ze względu na brak odpowiednich mechanizmów. Zaproponowano utworzenie międzynarodowego obserwatorium dobrych praktyk, zbudowanego w oparciu o zaproponowaną powyżej ulepszoną współpracę międzysektorową. Skuteczne zarządzanie wiedzą i strategie dzielenia się nią, czyli docieranie na czas z właściwą informacją do właściwych osób, mogłyby stanowić rozwiązanie wielu problemów omawianych w trakcie badania poprzez unowocześnienie procesów rekrutacji, szkolenia i podnoszenia świadomości.

> *„Musimy przełamać ograniczenia nakładane przez silosy, zachęcając ludzi o różnym doświadczeniu do współpracy, tak aby widzieć rzeczy z szerokiej perspektywy."*
>
> Konsultantka ds. cyberbezpieczeństwa w UE

[21] https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Droga w przyszłość

Fakt, że zarówno sektor przemysłowo-biznesowy, jak i edukacyjny na całym świecie uznają istnienie luki kompetencyjnej i wyrażają podobne opinie na temat kompetencji kluczowych, jest pozytywnym krokiem. Ponadto oba sektory wydają się wyrażać potrzebę podobnych rozwiązań problemu i mają tendencję do proponowania komplementarnych sposobów osiągnięcia tych rozwiązań. Podczas gdy respondenci z grupy przemysłowo-biznesowej wykazywali większe zainteresowanie szkoleniami, respondenci z dziedziny edukacji preferowali współpracę i wymianę doświadczeń z biznesem, tak aby móc budować realistyczne, przyszłościowe programy nauczania. Respondenci z obu grup chętnie opisywali dobre praktyki, które wdrożyli lub z którymi się zetknęli, a które mogłyby ułatwić kolejne kroki w kierunku osiągnięcia celów.

Koalicja IS3C mogłaby odegrać ważną rolę w wypełnianiu luki kompetencyjnej poprzez:

- Utworzenie ośrodka, który mógłby pełnić rolę obserwatora dobrych praktyk i zapewnić stały dialog;
- Podnoszenie świadomość w sektorze przemysłowo-biznesowym na temat korzyści płynących z nawiązania bliższej współpracy z sektorami edukacyjnymi w zakresie wymiany informacji, wiedzy i rozwiązań dotyczących cyberbezpieczeństwa, w celu wspierania rozwoju lepiej dostosowanych programów nauczania;
- Budowanie potencjału w celu wspierania dzielenia się wiedzą między sektorami, na przykład poprzez programy typu „szkol trenera”;
- Zachęcanie i wspieranie udziału osób w wieku poniżej 30 lat i kobiet w programach budowania potencjału, opracowanych wspólnie z przedstawicielami sektora przemysłowo-biznesowego;
- Wspieranie przeglądu i aktualizacji programów nauczania oraz rozwój ukierunkowanych zasobów nauczania i uczenia się (na przykład pakietów edukacyjnych z treściami teoretycznymi i metodologicznymi dla osób szkolących się).

Załączniki

Załącznik I - Kwestionariusz wywiadu i tabela wywiadów

Przeprowadzono dwadzieścia osiem wywiadów w 16 krajach świata. W trakcie tych wstępnych wywiadów i dyskusji opracowano, pilotowano i kształtowano pięć pytań, aby ukierunkować rozmowę, która trwała średnio godzinę:

1. Jakie są główne kompetencje w zakresie cyberbezpieczeństwa, których Twoja firma szuka przy zatrudnianiu?
2. Jakie są główne luki kompetencyjne w zakresie cyberbezpieczeństwa, które dostrzegasz pomiędzy tym, czego poszukuje Twoja firma, a tym, co potrafią nowi absolwenci po ukończeniu studiów?
3. Jak poważny jest to problem dla Twojej organizacji?
4. Z obsadzeniem jakich profili zawodowych związanych z cyberbezpieczeństwem masz największe problemy?
5. Czy byłeś/aś w jakiś sposób zaangażowany w usuwanie tych luk w ministerstwie ds. edukacji lub placówkach edukacyjnych, a jeśli tak, to jakie są Twoje doświadczenia?

1	Brazylia	Brazylia	Brazylijskie Stowarzyszenie Komputerowe
2	Brazylia	Brazylia	Petrobas
3	Indonezja	Indonezja	Linknet
4	Indonezja	Indonezja	Xynesis International
5	Ghana	Ghana	Seltech Ghana
6	Ghana	Ghana	CyberGhana
7	Luksemburg	Niderlandy	Ministerstwo Zdrowia, Dobrobytu i Sportu
8	Luksemburg	Dania	KPMG
9	Luksemburg	Belgia	Konsultant ds. cyberbezpieczeństwa w UE
10	Luksemburg	Polska	Uniwersytet Łódzki, Polska
11	Luksemburg	Luksemburg	Ministerstwo Gospodarki
12	Luksemburg	Maroko	Krajowe Centrum Badań i Innowacji (CMRPI), Uniwersytet Kenitra
13	Luksemburg	Włochy	Konsultant ds. bezpieczeństwa informacji
14	Nepal	Nepal	InfoDevelopers Pvt. Ltd
15	Nepal	Nepal	Centrum Badań i Innowacji w zakresie Cyberbezpieczeństwa
16	Nepal	Nepal	Vairav Technology Security Pvt Ltd.
17	Polska	USA	Microsoft
18	Polska	Polska	NASK
19	Samoa	Samoa	Ministerstwo Komunikacji, Info Tech (MCIT)
20	Samoa	Samoa	Urząd Regulatora
21	Sri Lanka	Sri Lanka	Techone Global
22	Sri Lanka	Sri Lanka	Bank DFCC
23	Sudan	Sudan	SudanCERT
24	Sudan	Sudan	Krajowe Centrum Informacji - Sudan
25	Wietnam	Wietnam	TMG Solutions
26	Wietnam	Wietnam	Polaris Infosec
27	Wietnam	Wietnam	Bosch Global Software Technologies Co Ltd
28	Wietnam	Wietnam	Uniwersytet RMIT

Załącznik II - Kwestionariusz dla przedstawicieli biznesu

CZĘŚĆ NR 1

Cel tego badania

IS3C jest dynamiczną koalicją Forum Zarządzania Internetem, w skład której wchodzą interesariusze z sektorów biznesu i edukacji, a także społeczności obywatelskie, rządowe, regulacyjne i korporacyjne, szczególnie zainteresowane kompetencjami cyfrowymi. Zachęca do stosowania standardów, dzięki którym usługi i sieci internetowe staną się bezpieczniejsze, pewniejsze i bardziej godne zaufania.

Niniejsze badanie przyczyni się do zrozumienia i zniwelowania luk pomiędzy kompetencjami, jakie posiadają absolwenci kierunków związanych z cyberbezpieczeństwem/informatyką, a wymaganiami przemysłu lub biznesu.

Wypełnienie ankiety zajmie Ci 15 do 20 minut. Zgodnie z GDPR, żadne dane osobowe ani adres IP nie będą rejestrowane ani gromadzone.

CZĘŚĆ NR 2 [22]

O Tobie

(opcjonalnie - tekst swobodny)

Wiek *

O poniżej 18 O 18-30 O 31-45 O 46-65 O powyżej 65

Płeć *

O mężczyzna O kobieta O wolę nie podawać

Państwo *

(menu rozwijane „państwa")

Branża zawodowa *

O Biznes/przemysł O Szkolnictwo wyższe O Szkolnictwo O Inna (proszę podać)

CZĘŚĆ NR 3

Biznes / przemysł i pozostałe

(opis swobodnym tekstem)

1(a) Oceń, jakie znaczenie w miejscu pracy przypisałbyś poniższym kompetencjom przekrojowym *.

Skala: nieistotne, mało ważne, umiarkowanie ważne, bardzo ważne, trudno powiedzieć

- myślenie krytyczne
- myślenie etyczne
- myślenie strategiczne
- myślenie holistyczne
- kreatywność

[22] Pytania oznaczone gwiazdką * były obowiązkowe, wszystkie inne były opcjonalne

- umiejętność rozwiązywania problemów
- umiejętność pracy zespołowej
- myślenie interdyscyplinarne
- wiedza biznesowa
- umiejętność uczenia się przez całe życie
- umiejętności w zakresie komunikacji werbalnej
- umiejętności w zakresie komunikacji pisemnej
- radzenie sobie ze złożonością problemów
- otwartość umysłu

1(b) Oceń, jakie znaczenie w miejscu pracy przypisałbyś poniższym kompetencjom zawodowym *.

Skala: nieistotne, mało ważne, umiarkowanie ważne, bardzo ważne, trudno powiedzieć

- ocena ryzyk w zakresie zabezpieczeń
- zarządzanie zapobieganiem ryzykom
- wiedza na temat podatności systemów na ataki i eksploitów w systemach
- rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
- rozumienie logiki systemów
- umiejętność pisania skryptów lub kodowania
- znajomość zagadnień związanych z zabezpieczaniem sieci
- znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
- znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
- znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych

1(c) Wskaż tutaj wszelkie inne kompetencje przekrojowe lub zawodowe, których nie ma na liście, a które uważasz za bardzo ważne

(opcjonalnie - tekst swobodny)

2(a) Oceń średni poziom kompetencji absolwentów w Twojej placówce w zakresie poniższych kompetencji przekrojowych *.

Skala (poziom): bardzo niski, niski, umiarkowany, dobry, trudno powiedzieć

- myślenie krytyczne
- myślenie etyczne
- myślenie strategiczne
- myślenie holistyczne
- kreatywność
- umiejętność rozwiązywania problemów
- umiejętność pracy zespołowej
- myślenie interdyscyplinarne
- wiedza biznesowa
- uczenie się przez całe życie
- umiejętności w zakresie komunikacji werbalnej
- umiejętności w zakresie komunikacji pisemnej
- radzenie sobie ze złożonością problemów
- otwartość umysłu

2(b) Oceń średni poziom kompetencji zawodowych absolwentów w Twojej placówce w poniższych obszarach *.

Skala (poziom): bardzo niski, niski, umiarkowany, dobry, trudno powiedzieć

- ocena ryzyk w zakresie zabezpieczeń
- zarządzanie zapobieganiem ryzykom
- wiedza na temat podatności systemów na ataki i eksploitów w systemach
- rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
- rozumienie logiki systemów
- umiejętność pisania skryptów lub kodowania
- znajomość zagadnień związanych z zabezpieczaniem sieci
- znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
- znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
- znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych

CZĘŚĆ NR 4

Twoje pomysły i sugestie

(tekst swobodny)

3. **Podziel się przykładami dobrych praktyk, które Twoja organizacja wdraża w celu zniwelowania różnic między Twoimi oczekiwaniami a kompetencjami pracowników (jeżeli znasz takie przykłady). (Kompetencje przekrojowe i/lub zawodowe)**

   (tekst swobodny)

4. **W ramach sektora, w którym działasz zawodowo, które stanowiska uważasz za najtrudniejsze do obsadzenia (wybierz dowolną liczbę stanowisk, a w razie potrzeby dodaj kolejne stanowiska)**

   - Tester penetracyjny
   - Menedżer ds. cyberbezpieczeństwa
   - Inżynier sieci
   - Architekt bezpieczeństwa informacji
   - Inne stanowiska

5. **W jakim stopniu trudności w obsadzeniu tych stanowisk wpływają na Twoją organizację lub sektor, w którym działasz?**

   O nie ma wpływu O niewielki wpływ O silny wpływ O bardzo silny wpływ O trudno powiedzieć

6. **Jakie rozwiązania możesz zaproponować, aby zniwelować lukę pomiędzy Twoimi oczekiwaniami a kompetencjami pracowników?**

   (tekst swobodny)

Załącznik III - Kwestionariusz dla przedstawicieli edukacji

CZĘŚĆ NR 1

Cel tego badania

IS3C jest dynamiczną koalicją Forum Zarządzania Internetem, w skład której wchodzą interesariusze z sektorów biznesu i edukacji, a także społeczności obywatelskie, rządowe, regulacyjne i korporacyjne, szczególnie zainteresowane kompetencjami cyfrowymi. Zachęca do stosowania standardów, dzięki którym usługi i sieci internetowe staną się bezpieczniejsze, pewniejsze i bardziej godne zaufania.

Niniejsze badanie przyczyni się do zrozumienia i zniwelowania luk pomiędzy kompetencjami, jakie posiadają absolwenci kierunków związanych z cyberbezpieczeństwem/informatyką, a wymaganiami przemysłu lub biznesu.

Wypełnienie ankiety zajmie Ci 15 do 20 minut. Zgodnie z GDPR, żadne dane osobowe ani adres IP nie będą rejestrowane ani gromadzone.

CZĘŚĆ NR 2

O Tobie

(tekst swobodny)

Wiek *

O poniżej 18 O 18-30 O 31-45 O 46-65 O powyżej 65

Płeć *

O mężczyzna O kobieta O wolę nie podawać

Państwo *

(menu rozwijane „państwa")

Branża zawodowa *

O Biznes/przemysł O Szkolnictwo wyższe O Szkolnictwo O Inna (proszę podać)

CZĘŚĆ NR 3

Sektory edukacyjne

(opis swobodnym tekstem)

1(a) Jaką wagę przywiązuje się w Twojej placówce edukacyjnej do poniższych kompetencji przekrojowych? *

Skala: nieistotne, mało ważne, umiarkowanie ważne, bardzo ważne, trudno powiedzieć

- myślenie krytyczne
- myślenie etyczne
- myślenie strategiczne
- myślenie holistyczne
- kreatywność
- umiejętność rozwiązywania problemów
- umiejętność pracy zespołowej

- myślenie interdyscyplinarne
- wiedza biznesowa
- uczenie się przez całe życie
- umiejętności w zakresie komunikacji werbalnej
- umiejętności w zakresie komunikacji pisemnej
- radzenie sobie ze złożonością problemów
- otwartość umysłu

1(b) Jeśli ma to zastosowanie w tym przypadku, jakie znaczenie przypisuje się w Twojej placówce edukacyjnej poniższym kompetencjom zawodowym?

Skala: nieistotne, mało ważne, umiarkowanie ważne, bardzo ważne, trudno powiedzieć

- ocena ryzyk w zakresie zabezpieczeń
- zarządzanie zapobieganiem ryzykom
- wiedza na temat podatności systemów na ataki i eksploitów w systemach
- rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
- rozumienie logiki systemów
- umiejętność pisania skryptów lub kodowania
- znajomość zagadnień związanych z zabezpieczaniem sieci
- znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
- znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
- znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych

1(c) Wskaż tutaj wszelkie inne kompetencje przekrojowe lub zawodowe, których nie ma na liście, a które uważasz za bardzo ważne.

(opcjonalnie - tekst swobodny)

2(a) Oceń średni poziom kompetencji przekrojowych absolwentów Twojej placówki w poniższych obszarach *.

Skala: bardzo słaby, słaby, dobry, bardzo dobry, trudno powiedzieć

- myślenie krytyczne
- myślenie etyczne
- myślenie strategiczne
- myślenie holistyczne
- kreatywność
- umiejętność rozwiązywania problemów
- umiejętność pracy zespołowej
- myślenie interdyscyplinarne
- wiedza biznesowa
- uczenie się przez całe życie
- umiejętności w zakresie komunikacji werbalnej
- umiejętności w zakresie komunikacji pisemnej
- radzenie sobie ze złożonością problemów
- otwartość umysłu

2(b) Jeśli ma to zastosowanie w tym przypadku, oceń średni poziom kompetencji zawodowych absolwentów Twojej placówki w poniższych obszarach

Skala: bardzo słaby, słaby, dobry, bardzo dobry, trudno powiedzieć

- ocena ryzyk w zakresie zabezpieczeń
- zarządzanie zapobieganiem ryzykom
- wiedza na temat podatności systemów na ataki i eksploitów w systemach
- rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
- rozumienie logiki systemów
- umiejętność pisania skryptów lub kodowania
- znajomość zagadnień związanych z zabezpieczaniem sieci
- znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
- znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
- znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych

CZĘŚĆ NR 4

3. Jakie rozwiązania możesz zaproponować, aby wypełnić lukę między kompetencjami absolwentów Twojej placówki a oczekiwaniami przemysłu?

(tekst swobodny)

Załącznik IV - Model 14 kompetencji przekrojowych i 10 zawodowych

Kompetencje przekrojowe

1. myślenie krytyczne
2. myślenie etyczne
3. myślenie strategiczne
4. myślenie holistyczne
5. kreatywność
6. umiejętność rozwiązywania problemów
7. umiejętność pracy zespołowej
8. myślenie interdyscyplinarne
9. wiedza biznesowa
10. uczenie się przez całe życie
11. umiejętności w zakresie komunikacji werbalnej
12. umiejętności w zakresie komunikacji pisemnej
13. radzenie sobie ze złożonością problemów
14. otwartość umysłu

Kompetencje zawodowe

1. ocena ryzyk w zakresie zabezpieczeń
2. zarządzanie zapobieganiem ryzykom
3. wiedza na temat podatności systemów na ataki i eksploitów w systemach
4. rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych
5. rozumienie logiki systemów
6. umiejętność pisania skryptów lub kodowania
7. znajomość zagadnień związanych z zabezpieczaniem sieci
8. znajomość zagadnień związanych z zabezpieczaniem systemów operacyjnych
9. znajomość zagadnień związanych z zabezpieczaniem urządzeń mobilnych i IoT
10. znajomość zagadnień związanych z zabezpieczaniem systemów chmurowych

W 2021 r. IS3C (dynamiczna koalicja, powstała w ramach Internet Governance Forum, zajmująca się standardami internetowymi, zabezpieczeniami i bezpieczeństwem) rozpoczęła badanie mające na celu lepsze zrozumienie niedoboru umiejętności w sektorze cyberbezpieczeństwa. Po serii wywiadów przeprowadzonych z liderami przemysłu, biznesu i szkolnictwa wyższego w 14 krajach, określono krótką listę umiejętności przekrojowych i zawodowych, która stała się podstawą do przeprowadzenia ankiety mającej na celu poznanie punktu widzenia szerszej populacji. W badaniu wzięło udział 235 respondentów z 65 krajów świata.

Tylko co czwarty respondent był kobietą, a ponad 80% było w wieku powyżej 30 lat. Odzwierciedla to brak różnorodności w sektorze cyberbezpieczeństwa, co zdaniem wielu rozmówców i respondentów ankiety w dużej mierze przyczynia się do niedoboru umiejętności, z którym boryka się ten sektor.

Myślenie krytyczne, umiejętność rozwiązywania problemów, umiejętność pracy zespołowej i kreatywność pojawiły się jako główne kryteria dotyczące kompetencji przekrojowych zarówno dla edukatorów, jak i przedstawicieli biznesu. Co ciekawe, respondenci z sektora edukacji przywiązywali średnio o 10% mniejszą wagę do umiejętności przekrojowych niż ci z przemysłu. Szacunki z obu sektorów wskazują, że co trzeci młody człowiek wchodzący na rynek pracy nie opanował przedstawionej listy kompetencji przekrojowych.

Kompetencje takie jak zapobieganie ryzykom i zarządzanie zabezpieczeniami systemów i sieci, jak twierdzą respondenci, są nie tylko kompetencjami zawodowymi, ale są przede wszystkim niezbędne dla wszystkich użytkowników technologii cyfrowych. Niektórzy respondenci zwracają uwagę, że wyniki znacznie by się poprawiły, gdyby edukacja zachęcała młodych ludzi do głębszego zastanowienia się nad funkcjonowaniem narzędzi i platform, z których korzystają w życiu codziennym.

Jednym z 17 celów zrównoważonego rozwoju ONZ do osiągnięcia do 2030 r. jest zapewnienie dostępu do wymiaru sprawiedliwości dla wszystkich oraz budowanie skutecznych, odpowiedzialnych i inkluzywnych instytucji na wszystkich szczeblach (SDG16). Niezawodna, bezpieczna infrastruktura cyfrowa ma zasadnicze znaczenie dla utrzymania solidnych, dynamicznych instytucji, a integracja jest zagrożona wszędzie tam, gdzie brakuje różnorodności. Aby zapewnić zrównoważoną przyszłość, edukacja (SDG4) musi być dostosowana do celu, opierać się na potrzebach jednostki i uwzględniać przyszłe potrzeby społeczeństwa. *W niniejszej publikacji IS3C przedstawia siedem kluczowych zaleceń opracowanych na podstawie pomysłów, sugestii i dobrych praktyk zebranych od praktyków z branży, biznesu i edukacji podczas tego trwającego rok badania.*

Wydawnictwo Insight S.A.