RAPORT

Mapa MŚP sektora cyberbezpieczeństwa w Polsce: diagnoza, potrzeby, rekomendacje

Charakterystyka branży, kluczowe czynniki wzrostu i rekomendacje dla stworzenia Społeczności Kompetentnej

W ramach projektu NATIONAL COORDINATION CENTER – POLAND (NCC-PL) współfinansowanego ze środków Programu Cyfrowa Europa

| Czerwiec 2025

O raporcie

Ministerstwo Cyfryzacji

Szanowni Państwo,

Małe i średnie przedsiębiorstwa stanowią fundament polskiej gospodarki oraz kluczowy element rozwoju innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa. To właśnie w tych firmach rodzą się przyszłe liderki i przyszli liderzy polskiego cyberbezpieczeństwa, tworzący innowacyjne technologie, budując usługi i wspierając odporność cyfrową zarówno sektora prywatnego, jak i publicznego. Ich rola w kształtowaniu przyszłości cyberbezpieczeństwa w Polsce jest nie do przecenienia.
W ramach projektu National Coordination Centre - Poland [NCC-PL] współfinansowanego ze środków Programu Cyfrowa Europa, realizowanego przez Krajowe Centrum Kompetencji Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, została opracowana Mapa MŚP sektora cyberbezpieczeństwa w Polsce: diagnoza, potrzeby, rekomendacje pokazująca wieloaspektowy obraz tego sektora. Wnioski prezentowane w raporcie posiadają wysoką wiarygodność i wartość analityczną gdyż oparte są na bardzo dużej próbie obejmującej znaczą część branży cyberbezpieczeństwa, zaś wypracowane rekomendacje powstały przy udziale przedstawicieli ekosystemu cyberbezpieczeństwa.
Jestem przekonany, że prezentowane Państwu badanie potencjału i potrzeb msp z branży cyberbezpieczeństwa to nie tylko wiedza ale również przydatne narzędzie do tworzenia skutecznej polityki publicznej wspierającej branżę cyberbezpieczeństwa w Polsce, oparte nie na intuicji ale na wiarygodnych danych oraz bezpośrednim głosie (nie zawsze przychylnym) małych i średnich przedsiębiorców, który musi być usłyszany a potrzeby realnie adresowane.
Mam nadzieję, że lektura tego dokumentu zainspiruje Państwa do własnych przemyśleń a podmioty posiadające motywację i potencjał do włączenia się w prace na rzecz rozwoju cyberbezpieczeństwa Polski i Europy poprzez Społeczność kompetentną wspierającą cele i zadania Europejskiego Centrum Kompetencji Cyberbezpieczeństwa oraz Krajowego Centrum Kompetencji Cyberbezpieczeństwa. Zapraszam do współpracy i kontaktu z Krajowym Centrum, wszystkie informacje znajdziecie Państwo na stronie www.gov.pl/web/cyber-nccpl.
Na zakończenie chciałbym wyrazić swoją wdzięczność wszystkim Ekspertkom i Ekspertom oraz Przedstawicielkom i Przedstawicielom małych i średnich przedsiębiorstw, którzy bezinteresownie poświęcili swój czas biorąc udział w badaniu. Bez Państwa zaangażowania Mapa MŚP sektora cyberbezpieczeństwa w Polsce nie miałaby szansy powstać.

Dziękuję!

Paweł Olszewski

Sekretarz Stanu w Ministerstwie Cyfryzacji

Szanowni Państwo,

W raporcie skoncentrowaliśmy się w szczególności na ukazaniu obrazu sektora MŚP branży cyberbezpieczeństwa w Polsce. Sprawdziliśmy, jak polskie małe i średnie spółki organizują swoją działalność operacyjną i kadrową, a także jak podchodzą do internacjonalizacji, pozyskiwania finansowania i wdrażania regulacji unijnych. Niestety aż 77% firm przyznaje, że nigdy nie korzystało z żadnej formy wsparcia publicznego na rozwój działalności w obszarze cyberbezpieczeństwa. Co trzecia firma zadeklarowała chęć ekspansji zagranicznej, jednak w praktyce działania te ograniczają się do pojedynczych projektów lub pozostają na etapie planowania. Jaki jest aktualny obraz branży? Jak możemy rozwijać MŚP i wzmacniać krajowy potencjał branży cyberbezpieczeństwa? To jest przedmiotem niniejszego raportu.

Życzę Państwu ciekawej lektury oraz wielu refleksji, wierząc jednocześnie, że wnioski z badania przełożą się na wzrost i sprawniejszy rozwój sektora.

Emilian Kołodziej

Prezes Zarządu IBC Advisory S.A.

Spis treści

O raporcie 2
Spis treści 4
Wstęp 5
Najważniejsze wnioski i rekomendacje 8
1. Kluczowe wnioski 10
2. Rekomendacje 11
Charakterystyka polskiej branży cyberbezpieczeństwa 14
1.1. Mapa branży cyberbezpieczeczeństwa 15
1.2. Analiza ekosystemu 18
1.3. Charakterystyka przedsiębiorstw MŚP w branży cyberbezpieczeństwa w Polsce 20
1.4. Model biznesowy 29
Potencjał krajowych MŚP w obszarze cyberbezpieczeństwa 32
2.1. Zasoby kadrowe i kompetencje (na podstawie ECSF) 33
2.2. Potencjał technologiczny i infrastrukturalny 42
2.3. Certyfikacja 50
2.4. Rodzaje finansowania 54
2.5. Internacjonalizacja firm 66
2.6. Analiza powiązań kooperacyjnych 69
Bariery i potrzeby rozwojowe polskich małych i średnich firm sektora cyberbezpieczeństwa 70
3.1. Bariery wzrostu – finansowe, organizacyjne, regulacyjne 71
3.2. Regulacje polskiego rynku cyberbezpieczeństwa 82
3.3. Oczekiwania wobec otoczenia instytucjonalnego i legislacyjnego 87
Bibliografia 94
Spis wykresów i rysunków 96

Wstęp

Rozwój sektora cyberbezpieczeństwa jest jednym z kluczowych elementów zapewnienia odporności cyfrowej kraju i jego gospodarki. W szczególności dotyczy to małych i średnich przedsiębiorstw (MŚP), które – mimo rosnącej roli – często napotykają na istotne ograniczenia rozwojowe, finansowe i kadrowe. Wobec postępującej cyfryzacji, złożoności zagrożeń oraz dynamicznych zmian regulacyjnych, konieczne jest kompleksowe zrozumienie kondycji i potrzeb krajowych MŚP w branży cyberbezpieczeństwa.

Celem niniejszego badania jest identyfikacja potencjału, barier oraz kierunków rozwoju sektora MŚP działających w obszarze cyberbezpieczeństwa w Polsce. Raport stanowi podstawę do sformułowania rekomendacji dla administracji publicznej oraz innych interesariuszy zaangażowanych w budowanie krajowego i europejskiego ekosystemu cyberbezpieczeństwa. Szczególna uwaga została poświęcona identyfikacji podmiotów, które – ze względu na posiadane zasoby, kompetencje i profil działalności – mogą zostać włączone do tzw. Społeczności Kompetentnej, zgodnie z art. 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r.

Społeczność Kompetentna, rozwijana przez Krajowe Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL), to inicjatywa mająca na celu integrację podmiotów posiadających wiedzę i doświadczenie w dziedzinie cyberbezpieczeństwa. Przyłączenie się do Społeczności pozwoli przedsiębiorcom uzyskać dostęp do specjalistycznej wiedzy, innowacyjnych technologii oraz umożliwi nawiązanie współpracy z kluczowymi podmiotami z sektora publicznego, naukowego i biznesowego – zarówno na poziomie krajowym, jak i europejskim. Udział w Społeczności ułatwi firmom, zwłaszcza MŚP, nawiązywanie kontaktów z partnerami, dostęp do informacji o dostępnych źródłach finansowania oraz zwiększy ich widoczność na rynku cyberbezpieczeństwa. Członkostwo w Społeczności będzie również sprzyjać wymianie doświadczeń, wspólnemu rozwiązywaniu problemów branżowych oraz lepszemu przygotowaniu się do wdrażania nowych regulacji, takich jak dyrektywa NIS2. Dzięki udziałowi w tej inicjatywie firmy zyskają realne wsparcie w rozwijaniu kompetencji kadrowych, wdrażaniu innowacyjnych produktów i usług oraz budowaniu swojej pozycji konkurencyjnej na rynku europejskim.

Zakres i cele badania

Badanie miało charakter przekrojowy i objęło zarówno analizę strukturalną krajowego rynku cyberbezpieczeństwa MŚP, jak i diagnozę potrzeb oraz ograniczeń na poziomie operacyjnym, strategicznym i systemowym. Cele ogólne badania obejmowały:

1. Opracowanie mapy branży cyberbezpieczeństwa w segmencie MŚP, z uwzględnieniem podziału na specjalizacje, zasięg terytorialny, formy działalności i skalę operacyjną.
2. Określenie krótkoterminowych i średniookresowych perspektyw rozwoju sektora.
3. Diagnozę barier wzrostu – w tym finansowych, organizacyjnych i regulacyjnych – ograniczających ekspansję i innowacyjność firm.
4. Opracowanie rekomendacji dla instytucji publicznych, mających na celu poprawę warunków prowadzenia działalności i zwiększenie konkurencyjności krajowych przedsiębiorstw.
5. Zidentyfikowanie podmiotów o wysokim potencjale rozwojowym, które mogą być zainteresowane aktywnym uczestnictwem w inicjatywach Społeczności Kompetentnej.

Do celów szczegółowych należało m.in. opracowanie odpowiednich narzędzi badawczych (kwestionariuszy, scenariuszy wywiadów), wypracowanie kryteriów przynależności do sektora, analiza zakresu certyfikacji, doświadczeń międzynarodowych oraz gotowości firm do udziału w projektach akceleracyjnych i kooperacyjnych.

Metodologia

Badanie miało charakter nowatorski.

Do realizacji badania wykorzystano podejście mieszane, łączące komponenty ilościowe i jakościowe:

- Desk research – analiza dokumentów źródłowych, danych statystycznych, raportów branżowych oraz przepisów prawnych. Stanowiło punkt wyjścia do rozpoznania kontekstu rynkowego i regulacyjnego. W ramach tego narzędzia, na podstawie danych o ponad 400 przedsiębiorstwach, powstała Mapa Małych i Średnich Przedsiębiorstw z branży cyberbezpieczeństwa.
- Badanie CAWI/CATI – ilościowe badanie ankietowe przeprowadzone na próbie 197 przedsiębiorstw z sektora cyberbezpieczeństwa, zróżnicowanych pod względem formy działalności, lokalizacji i wielkości.
- Wywiady pogłębione (IDI) – 20 indywidualnych rozmów z przedstawicielami firm, które pozwoliły na pogłębienie diagnozy i uchwycenie subtelnych zależności wpływających na decyzje strategiczne przedsiębiorców.
- Panele eksperckie – w ramach badania zostały przeprowadzone 2 panele eksperckie – na początku procesu badawczego w ramach tworzenia narzędzi badawczych, a także na końcu w ramach tworzenia rekomendacji. W panelach udział wzięli przedstawiciele polskich MŚP działających w branży cyberbezpieczeństwa, w tym prezesi i dyrektorzy tych przedsiębiorstw.

Takie podejście umożliwiło triangulację danych oraz uzyskanie zarówno przekroju ilościowego branży, jak i wglądu w perspektywy decydentów, bariery instytucjonalne oraz obawy firm dotyczące ekspansji, certyfikacji i współpracy międzynarodowej.

Struktura raportu

Raport został podzielony na **trzy główne części**, obejmujące zarówno analizę kontekstową, jak i szczegółowe wyniki badań empirycznych oraz wnioski operacyjne. Każda z części zawiera podrozdziały skupiające się na kluczowych aspektach funkcjonowania krajowego sektora MŚP w branży cyberbezpieczeństwa.

1. Charakterystyka polskiej branży cyberbezpieczeństwa (desk research)

Pierwsza część raportu przedstawia syntetyczną analizę rynku cyberbezpieczeństwa w Polsce. Zawiera m.in.:

- definicje i uwarunkowania terminologiczne,
- analizę wielkości i struktury rynku (w tym jego wartość i dynamikę wzrostu),
- identyfikację kluczowych instytucji ekosystemu (takich jak NASK, CSIRT-y, Ministerstwo Cyfryzacji),
- opis obowiązujących regulacji krajowych i unijnych wpływających na działalność firm (NIS2, DORA, RODO, CRA),
- wskazanie czynników stymulujących popyt na usługi i produkty cyberbezpieczeństwa,
- przegląd dostępnych form finansowania oraz kierunków internacjonalizacji.

Ta część raportu stanowi fundament merytoryczny dla dalszych analiz oraz ramy kontekstowe dla interpretacji danych zebranych w badaniach.

Opis branży opiera się na zgromadzonych danych badawczych od 417 podmiotów zidentyfikowanych w ramach mappingu, spełniających kryteria polskich MŚP z branży cyberbezpieczeństwa zgodnie z przyjętą definicją oraz metodologią, a także od 201 podmiotów zbadanych szczegółowo w badaniach CAWI/CATI/IDI.

2. Potencjał krajowych MŚP w obszarze cyberbezpieczeństwa

W drugim rozdziale zaprezentowano analizę potencjału firm w ujęciu zasobowym, technologicznym, kadrowym i organizacyjnym. Skoncentrowano się na:

- strukturze zatrudnienia i kompetencjach (zgodnie z ramą ECSF – European Cybersecurity Skills Framework),

- wykorzystywanej infrastrukturze technicznej i rozwiązaniach technologicznych,
- posiadanych certyfikacjach, patentach i doświadczeniach międzynarodowych,
- modelach finansowania i inwestycjach w innowacje.

Celem tej części jest ocena, w jakim stopniu przedsiębiorstwa są przygotowane do rozwoju i uczestnictwa w europejskim ekosystemie cyberbezpieczeństwa.

3. Bariery i potrzeby rozwojowe sektora

Trzecia część raportu przedstawia wyniki analizy głównych barier i ograniczeń hamujących rozwój MŚP w branży cyberbezpieczeństwa. Na podstawie danych jakościowych (IDI) i ilościowych (CAWI/CATI) opisano:

- przeszkody finansowe, regulacyjne i organizacyjne,
- oczekiwania przedsiębiorców wobec otoczenia instytucjonalnego,
- trudności związane z certyfikacją produktów i ekspansją zagraniczną,
- wpływ regulacji NIS2 i CRA na działalność operacyjną.

Rozdział ten dostarcza szczegółowych insightów na temat wyzwań strukturalnych i systemowych stojących przed firmami, które potencjalnie mogą stanowić przedmiot interwencji publicznej.

Najważniejsze wnioski i rekomendacje

Raport prezentuje kompleksową analizę sektora cyberbezpieczeństwa w Polsce, przygotowaną w oparciu o zlecone badanie, ze szczególnym uwzględnieniem małych i średnich przedsiębiorstw. Badanie zostało przeprowadzone w oparciu o desk research, wywiady pogłębione z przedstawicielami firm z branży cyberbezpieczeństwa oraz badanie ilościowe przedsiębiorstw metodą CAWI/CATI, co pozwoliło uchwycić zarówno uwarunkowania strukturalne jak i realne wyzwania operacyjne oraz strategiczne.

Rynek małych i średnich przedsiębiorstw w sektorze cyberbezpieczeństwa w Polsce charakteryzuje się dużym zróżnicowaniem pod względem wielkości, stażu, źródeł kapitału i zakresu działalności. Zdecydowaną większość populacji badawczej stanowiły małe firmy (160 z 197), z których większość funkcjonuje na rynku ponad 4 lata, a znaczna część również powyżej dekady. Przedsiębiorstwa te w większości opierają się na kapitale krajowym, a tylko nieliczne są częścią struktur zagranicznych. Profil działalności MŚP w branży cyberbezpieczeństwa jest rozbudowany – wiele firm świadczy równolegle usługi doradcze, szkoleniowe, integracyjne, testy penetracyjne i produkuje oprogramowanie, co świadczy o wysokim stopniu specjalizacji i elastyczności operacyjnej.

Terytorialnie największe zagęszczenie firm z sektora cyberbezpieczeństwa odnotowano w województwie mazowieckim, które pełni rolę krajowego centrum tej branży, a także w województwach wielkopolskim, śląskim, małopolskim i dolnośląskim. Dominują firmy o profilu usługodawców i integratorów, oferujące usługi monitorowania incydentów, zarządzania tożsamością i dostępem, testów bezpieczeństwa oraz zgodności z regulacjami. W strukturze sektora przeważają przedsiębiorstwa działające w kilku segmentach jednocześnie, co wskazuje na ich dążenie do kompleksowej obsługi klientów. Mimo rosnącego znaczenia technologii chmurowych i bezpieczeństwa OT, nadal dominują klasyczne obszary bezpieczeństwa IT, takie jak ochrona sieci, endpointów i zarządzanie podatnościami.

Z badań wyłania się obraz dynamicznie rosnącej branży, cechującej się wysoką elastycznością organizacyjną, ale jednocześnie obciążonej wieloma barierami rozwojowymi. Przedsiębiorstwa stosują hybrydowe modele zatrudnienia i często współpracują z ekspertami zewnętrznymi oraz środowiskiem naukowym. Kluczowym problemem jest niedobór wysoko wykwalifikowanych specjalistów, szczególnie na stanowiskach przekrojowych, łączących kompetencje techniczne, strategiczne i sprzedażowe.

Wyzwania kadrowe pogłębiają również braki w kompetencjach wspierających, takich jak marketing, sprzedaż czy zarządzanie produktem. Równolegle, zróżnicowanie zespołów (płciowe, wiekowe, dostępność dla osób z niepełnosprawnościami) pozostaje na niskim poziomie, a działania inkluzywne są w większości deklaratywne.

Sektor zmaga się z ograniczonym dostępem do środków finansowych – 77% badanych przedsiębiorstw nie korzystało z dotacji B+R, a 87% z nich nie aplikowało o wsparcie na ekspansję międzynarodową. Deklarowanym powodem są m.in. złożoność procedur, brak wiedzy o programach i niewystarczające zasoby organizacyjne. Przedsiębiorstwa rzadko sięgają też po kapitał prywatny, wykazując niechęć do oddawania udziałów i brak zaufania do funduszy.

Branża cyberbezpieczeństwa stoi przed rosnącymi wymaganiami regulacyjnymi (NIS2, CRA, DORA), które z jednej strony wymuszają profesjonalizację i porządkowanie procesów, z drugiej zaś stanowią wyzwanie kosztowe i organizacyjne – szczególnie dla MŚP. Jednocześnie wymagania regulacyjne z obszaru cyberbezpieczeństwa pozytywnie przyczyniają się do wzrostu popytu na produkty i usługi cyberbezpieczeństwa.

Mimo barier, przedsiębiorstwa deklarują gotowość do inwestycji – 42% badanych planuje rozwój usług i produktów, w tym automatyzację, SaaS oraz ekspansję zagraniczną, głównie do UE, USA, Bliskiego Wschodu i Azji. Wskazywane są także potrzeby rozwoju rozwiązań w obszarze threat intelligence, audytów AI/ML oraz bezpieczeństwa środowisk chmurowych.

Większość firm z sektora cyberbezpieczeństwa uważa, że bariery rozwojowe można pokonać samodzielnie, choć wielu dostrzega potrzebę wsparcia państwa w obszarach regulacyjnych, finansowych i promocyjnych. Ponad połowa respondentów wskazuje, że działania publiczne wymagają usprawnień – najczęściej krytykowane są zbyt wysokie koszty certyfikacji, nieczytelne procedury i symboliczny charakter wsparcia. Przedsiębiorcy oczekują od państwa roli partnera – nie kontrolera – który tworzy równe warunki konkurowania z firmami wspieranymi przez zagraniczne rządy. Szczególne znaczenie przypisuje się wsparciu eksportu, promocji krajowych rozwiązań, ułatwieniom w zamówieniach publicznych oraz

współpracy nauki i biznesu. Firmy postulują długofalowe, wieloetapowe programy wsparcia zamiast pojedynczych grantów oraz lepszą koordynację działań między instytucjami. Wzrasta też świadomość roli AI jako narzędzia wspierającego rozwój, choć część firm pozostaje sceptyczna. Bez aktywnej i przemyślanej strategii państwa, Polska może utracić cyfrową suwerenność i rolę innowatora, stając się jedynie odbiorcą obcych technologii.

Na podstawie wyników badania sformułowano 16 szczegółowych rekomendacji, obejmujących m.in. uproszczenie systemu wsparcia finansowego, rozwój kompetencji miękkich i sprzedażowych, wsparcie certyfikacji, promocję programów akceleracyjnych, budowę platform współpracy nauki i biznesu, oraz profesjonalizację komunikacji branżowej i działań rzeczniczych.

Raport stanowi punkt wyjścia do dalszych działań strategicznych – wskazuje konkretne obszary interwencji i potrzebę wypracowania trwałych mechanizmów wsparcia dla MŚP, które mogą stanowić fundament odpornej, innowacyjnej i konkurencyjnej gospodarki cyfrowej w Polsce.

1. Kluczowe wnioski

1. Sektor cyberbezpieczeństwa charakteryzuje się elastycznym modelem zatrudnienia – firmy coraz częściej rezygnują z etatów na rzecz współpracy B2B i projektowej, co pozwala im sprawnie reagować na zmienne potrzeby rynkowe i optymalizować koszty. Skala i forma zatrudnienia zależą od etapu rozwoju firmy i rodzaju projektów – nawet większe organizacje opierają się na zewnętrznych ekspertach i współpracy z uczelniami. Stabilne, długo budowane zespoły są postrzegane jako kluczowy atut, ale rośnie problem z pozyskiwaniem specjalistów o kompetencjach przekrojowych – łączących wiedzę techniczną z biznesową i komunikacyjną. Trudności dotyczą głównie ról hybrydowych, takich jak architekci, liderzy pre-sales czy konsultanci rozwoju biznesu. Choć wiele firm deklaruje neutralność płciową, kobiety są nadal nieliczne w zespołach technicznych, a osoby 65+ i z niepełnosprawnościami prawie nie występują.

2. Badania CAWI i IDI pokazują, że głównym wyzwaniem polskiego sektora cyberbezpieczeństwa jest brak rozwiniętej predykcji zagrożeń – firmy koncentrują się na reakcji, zaniedbując threat intelligence. Rosnące znaczenie mają bezpieczeństwo chmury i systemy IAM, a rozwój AI generatywnej rodzi ryzyka związane z jakością kodu i potrzebą nowych standardów audytu. Firmy borykają się z niedoborem specjalistów łączących kompetencje techniczne i biznesowe. Mimo to blisko połowa (CAWI) planuje inwestycje – głównie w B+R, nowe produkty, zgodność z NIS2/DORA (Pomimo, że DORA jest regulacją typu *lex specialis* i dotyczy bezpośrednio sektora finansowego, jej obecność w raporcie jest uzasadniona wpływem pośrednim na rynek dostawców ICT, w tym polskie MŚP z sektora cyberbezpieczeństwa. Firmy te jako podwykonawcy instytucji objętych DORA, muszą dostosować swoje działania do wymogów narzucanych przez klientów – m.in. w zakresie ciągłości działania, zarządzania incydentami czy zgodności z politykami bezpieczeństwa informacji. W praktyce oznacza to, że choć DORA formalnie nie nakłada obowiązków na wszystkie MŚP, to wprowadza nowe wymagania rynkowe, które realnie wpływają na ich działalność operacyjną i inwestycje w obszarze compliance i ekspansję (UE, USA, Bliski Wschód). Respondenci IDI wskazują na rolę sektora publicznego jako odbiorcy innowacji, ale bariery stanowią przeregulowanie i biurokracja. Aż 81% firm nie korzystało z akceleratorów – to niewykorzystany potencjał. Sektor rośnie, ale wymaga inwestycji w kompetencje, przewidywanie zagrożeń i lepsze otoczenie prawne.

3. Zasięg działalności firm cyberbezpieczeństwa w Polsce jest zróżnicowany – większość działa krajowo, ale wiele rozwija ekspansję międzynarodową. Główne kierunki to UE, USA, Azja Południowo-Wschodnia i Bliski Wschód, gdzie rynki są chłonne i mniej nasycone konkurencją. Modele ekspansji obejmują eksport, partnerstwa, targi branżowe i spółki zależne. Mimo ambicji firmy napotykają bariery – wysokie koszty, przetargi, różnice kulturowe i trudność w budowie relacji. 64% firm oferuje rozwiązania w modelu hybrydowym (cloud/on-premise), a 39% korzysta z pośredników sprzedaży. Duża część przedsiębiorstw integruje produkty innych polskich firm, wspierając lokalny ekosystem. Tylko 44% planuje certyfikację produktów, mimo że 72% deklaruje znajomość procesu – co może ograniczać konkurencyjność. Zabezpieczenie własności intelektualnej jest niskie – większość firm nie posiada patentów czy znaków towarowych.

4. Polski sektor cyberbezpieczeństwa rozwija się dynamicznie, ale jego potencjał hamują liczne bariery. Firmy zmagają się z brakiem finansowania, deficytem kadr i niską świadomością rynku na temat zagrożeń cyfrowych. Mniejsze podmioty mają trudności z pozyskaniem klientów i konkurowaniem z globalnymi markami, które dominują w przetargach i cieszą się większym zaufaniem. Wiele organizacji nie dysponuje narzędziami do predykcji ryzyk, co ogranicza skuteczność działań prewencyjnych. Wysokie koszty certyfikacji, złożone regulacje (np. NIS2, CRA) i brak wsparcia eksportowego dodatkowo ograniczają rozwój MŚP. Firmom brakuje kompetencji sprzedażowych i biznesowych, co utrudnia skalowanie i wejście na rynki zagraniczne. Sektor publiczny nie wykorzystuje swojego potencjału jako odbiorcy i promotora krajowych rozwiązań. Konieczne są uproszczenia regulacyjne, wsparcie finansowe i silniejsza współpraca branżowa, by wzmocnić konkurencyjność polskich firm na rynku międzynarodowym.

2. Rekomendacje

1. Uproszczenie procedur dostępu do finansowania publicznego

Obecne procedury ubiegania się o fundusze krajowe i unijne są zbyt skomplikowane, czasochłonne i niedostosowane do realiów działania małych i średnich przedsiębiorstw. Rekomenduje się uproszczenie formularzy, skrócenie terminów rozpatrywania wniosków oraz wdrożenie systemu wsparcia (np. punktów konsultacyjnych, mobilnych doradców projektowych), który ułatwi firmom aplikowanie i kosztorysowanie projektów. Rekomenduje się także uproszczenie i uelastycznienie zasad dotyczących wkładu własnego w programach finansowania publicznego, szczególnie tych skierowanych do sektora MŚP. Obecne wymogi często przewyższają możliwości organizacyjne i finansowe mniejszych firm, skutecznie zniechęcając je do aplikowania o środki. Warto rozważyć wprowadzenie mechanizmów różnicujących poziom wymaganego wkładu własnego w zależności od wielkości przedsiębiorstwa, poziomu innowacyjności projektu lub etapu rozwoju firmy. Takie podejście zwiększy dostępność wsparcia, umożliwiając szerszemu gronu firm realizację inwestycji w obszarze cyberbezpieczeństwa i zwiększy skuteczność wykorzystania dostępnych instrumentów publicznych. Ułatwienia te powinny dotyczyć szczególnie programów B+R, internacjonalizacji i wdrażania rozwiązań zgodnych z regulacjami (NIS2, DORA, CRA).

Adresaci rekomendacji: Ministerstwo Funduszy i Polityki Regionalnej, Polska Agencja Rozwoju Przedsiębiorczości, Narodowe Centrum Badań i Rozwoju (NCBR), Komisja Europejska (w zakresie funduszy unijnych).

2. Rozwój programów edukacyjnych i reskillingowych

Brakuje systemowych inicjatyw podnoszących kwalifikacje techniczne i strategiczne w sektorze. Rekomenduje się rozwój wyspecjalizowanych ścieżek edukacyjnych na uczelniach technicznych i uniwersytetach (np. kierunki typu „cyberbezpieczeństwo dla menedżerów", „threat intelligence", „cloud security"), a także finansowanie kursów reskillingowych dla osób chcących zmienić branżę. Współpraca z firmami powinna być obowiązkowym elementem tych programów.

Adresaci rekomendacji: Ministerstwo Edukacji i Nauki, uczelnie wyższe, PARP, pracodawcy / firmy technologiczne.

3. Wsparcie dla certyfikacji i zgodności regulacyjnej MŚP

Koszty uzyskania certyfikatów (np. ISO 27001, ENISA, Common Criteria, CE) są bardzo wysokie, przez co nieosiągalne dla małych firm. Rekomenduje się utworzenie funduszy lub bonów wspierających proces certyfikacji oraz opracowanie uproszczonych standardów zgodności dostosowanych do możliwości mniejszych podmiotów. Powinno to obejmować także wsparcie doradcze i audytorskie.

Adresaci rekomendacji: PARP, Urząd Dozoru Technicznego, Ministerstwo Rozwoju i Technologii, instytucje certyfikujące.

4. Budowa systemowej polityki różnorodności i inkluzywności

Sektor powinien wdrażać spójne polityki DEI (diversity, equity, inclusion), promujące zatrudnienie kobiet, osób starszych i z niepełnosprawnościami. Zaleca się tworzenie inkluzywnych kampanii rekrutacyjnych, dostosowanie miejsc pracy oraz szkolenia antydyskryminacyjne dla kadry zarządzającej. Takie działania mogą również być warunkiem dostępu do wybranych form wsparcia publicznego.

Adresaci rekomendacji: Ministerstwo Rodziny, Pracy i Polityki Społecznej, Rzecznik Praw Obywatelskich, PARP, organizacje pozarządowe zajmujące się DEI.

5. Zwiększenie współpracy między nauką a biznesem

Brakuje trwałych mechanizmów transferu wiedzy i wspólnych projektów badawczo-wdrożeniowych. Rekomenduje się tworzenie wspólnych centrów kompetencji, laboratoriów oraz inkubatorów przy uczelniach wyższych, w których firmy mogłyby testować swoje technologie w środowisku eksperymentalnym. Uczelnie powinny być również partnerem naukowym w projektach komercyjnych i eksportowych.

Adresaci rekomendacji: uczelnie wyższe, NCBR, Ministerstwo Nauki i Szkolnictwa Wyższego, firmy prywatne.

6. Promocja i rozwój programów akceleracyjnych i inkubatorów

Wiele firm nie korzysta z usług akceleratorów. Rekomenduje się wsparcie finansowe i organizacyjne dla rozwoju silnych programów akceleracyjnych, dedykowanych wyłącznie cyberbezpieczeństwu. Powinny one łączyć mentoring, testowanie MVP, dostęp do inwestorów oraz ścieżki ekspansji zagranicznej.

Adresaci rekomendacji: PARP, fundusze VC/akceleratory.

7. Profesjonalizacja kompetencji sprzedażowych i zarządczych

Firmy technologiczne często nie posiadają kompetencji w zakresie sprzedaży, marketingu oraz rozwoju modeli biznesowych. Rekomenduje się wdrożenie krajowego programu szkoleniowego z obszaru „cyber business management", który byłby kierowany do założycieli firm technologicznych i liderów technicznych. Programy powinny zawierać moduły dotyczące strategii, pozyskiwania klientów, storytellingu technologicznego oraz wyceny firm.

Adresaci rekomendacji: PARP, uczelnie ekonomiczne/biznesowe, Ministerstwo Rozwoju i Technologii, branżowe organizacje szkoleniowe.

8. Utworzenie funduszu ekspansji międzynarodowej

Polskie firmy posiadają silny potencjał eksportowy, jednak brakuje narzędzi wspierających wejście na rynki zagraniczne. Rekomenduje się utworzenie dedykowanego funduszu ekspansji dla firm z branży cyberbezpieczeństwa, który finansowałby m.in. udział w targach, lokalne badania rynku, certyfikację produktów oraz zakładanie zagranicznych oddziałów.

Adresaci rekomendacji: Polska Agencja Inwestycji i Handlu, Ministerstwo Spraw Zagranicznych, Ministerstwo Rozwoju i Technologii, PARP.

9. Rozwój mechanizmów zamówień publicznych wspierających innowacje

Sektor publiczny i obronny może odegrać rolę katalizatora innowacji, o ile wdrożone zostaną mechanizmy preferujące krajowe technologie i innowacje. Rekomenduje się m.in. tworzenie „piaskownic regulacyjnych" (regulatory sandboxes), zamówień przedkomercyjnych oraz zamówień testowych (proof-of-concept) dla MŚP. Zaleca się odstąpienie od obligatoryjnego powoływania się na zagraniczne rankingi (np. "Magic Quadrant" firmy Gartner) zwłaszcza gdy nie mają one bezpośredniego przełożenia na rzeczywiste potrzeby danego zamówienia. W zamian, rekomenduje się stosowanie neutralnych, otwartych kryteriów technicznych i funkcjonalnych oraz preferencję dla rozwiązań opartych o lokalne technologie.

Adresaci rekomendacji: Urząd Zamówień Publicznych, Ministerstwo Cyfryzacji, Ministerstwo Rozwoju i Technologii, Ministerstwo Obrony Narodowej.

10. Ujednolicenie interpretacji i wsparcie wdrożeń regulacji unijnych

Nowe regulacje takie jak NIS2, DORA czy CRA są postrzegane jako szansa, ale i duże obciążenie organizacyjne. Rekomenduje się utworzenie portalu informacyjnego z praktycznymi wytycznymi, aktualizowanymi na bieżąco interpretacjami prawnymi, wzorami dokumentów oraz bazą doradców i audytorów pomagających w ich wdrożeniu.

Adresaci rekomendacji: Ministerstwo Cyfryzacji, Urząd Ochrony Danych Osobowych, UOKiK, organizacje branżowe i izby gospodarcze.

11. Wzmocnienie roli organizacji branżowych i konsorcjów

Polski sektor jest rozproszony i słabo zorganizowany wewnętrznie. Rekomenduje się wspieranie tworzenia konsorcjów tematycznych (np. cyberbezpieczeństwo, chmura, IoT, SI), które będą wspólnie realizować projekty badawcze, eksportowe i rzecznicze. Organizacje branżowe powinny otrzymać środki na rozwój zaplecza analityczno-lobbingowego. Rekomenduje się także, zapewnienie wsparcia we wdrażaniu produktów do krajowego systemu cyberbezpieczeństwa oraz instytucji odpowiedzialnych za bezpieczeństwo Państwa.

Adresaci rekomendacji: organizacje branżowe, Ministerstwo Rozwoju i Technologii, Ministerstwo Cyfryzacji, PARP.

12. Stworzenie „cyber sandboxów" do testowania produktów

Potrzebne są środowiska testowe, w których firmy mogłyby symulować zagrożenia, testować nowe produkty i prowadzić audyty w kontrolowanych warunkach. Rekomenduje się utworzenie kilku regionalnych centrów testowych, dostępnych także dla uczelni i wojska.

Adresaci rekomendacji: Ministerstwo Cyfryzacji, NASK, uczelnie techniczne, Ministerstwo Obrony Narodowej, PARP.

13. Budowa wspólnego systemu promocji sektora za granicą

Rekomenduje się stworzenie wspólnej marki promującej polskie technologie cyberbezpieczeństwa (np. "Polish CyberTech"), z jednolitym stoiskiem narodowym na targach, katalogiem firm, promocją eksportu oraz wsparciem komunikacyjnym i prawnym dla wejścia na rynki międzynarodowe.

Adresaci rekomendacji: Ministerstwo Cyfryzacji, NASK, uczelnie techniczne, PARP.

14. Zachęty podatkowe dla inwestorów branżowych i prywatnych

Aby zachęcić rynek do inwestowania w firmy cyberbezpieczeństwa, warto wprowadzić ulgi podatkowe dla funduszy VC/PE inwestujących w ten sektor. Dodatkowo można rozważyć preferencje dla aniołów biznesu oraz mechanizmy współinwestowania publiczno-prywatnego.

Adresaci rekomendacji: Ministerstwo Finansów, Ministerstwo Rozwoju i Technologii, Polska Agencja Inwestycji i Handlu.

15. Edukacja rynku i promocja wartości cyberbezpieczeństwa

Wciąż wielu odbiorców traktuje cyberbezpieczeństwo jako zbędny koszt. Potrzebna jest kampania świadomościowa skierowana do sektora MŚP, jednostek samorządu i administracji, pokazująca zagrożenia, koszty incydentów oraz konkretne korzyści z inwestycji w bezpieczeństwo. Powinna ona obejmować również działania PR dla branży – pokazujące sukcesy, liderów i innowacje.

Adresaci rekomendacji: NASK, Ministerstwo Cyfryzacji, PARP, organizacje branżowe, media / agencje PR.

16. Wzmocnienie współpracy z europejskimi strukturami

Należy wzmocnić współpracę z europejskimi strukturami koordynującymi, takimi jak Europejskie Centrum Kompetencji w Dziedzinie Cyberbezpieczeństwa (ECCC), poprzez zapewnienie lepszej komunikacji, obecności przedstawicieli instytucji finansujących na wydarzeniach branżowych oraz zwiększenie działań promujących projekty współfinansowane ze środków unijnych. Skuteczna promocja rezultatów projektów i ich szeroka widoczność na rynku europejskim mogą istotnie przyczynić się do zwiększenia ich oddziaływania oraz wspierać skalowanie innowacyjnych rozwiązań opracowywanych przez polskie MŚP.

Adresaci rekomendacji: Ministerstwo Cyfryzacji, Narodowe Centrum Badań i Rozwoju (NCBR), Polska Agencja Rozwoju Przedsiębiorczości (PARP), przedstawiciele Polski w Radzie Zarządzającej ECCC, Ministerstwo Funduszy i Polityki Regionalnej.

Rozdział 1

Charakterystyka polskiej branży cyberbezpieczeństwa

1.1. Mapa branży cyberbezpieczeczeństwa

Sektor cyberbezpieczeństwa w Polsce dynamicznie się rozwija, napędzany rosnącą liczbą zagrożeń, nowymi regulacjami prawnymi oraz zwiększonym zapotrzebowaniem na specjalistyczne usługi ochrony cyfrowej. W tym kontekście małe i średnie przedsiębiorstwa działające w branży cyberbezpieczeństwa odgrywają kluczową rolę w dostarczaniu innowacyjnych rozwiązań, jednak same napotykają liczne wyzwania związane z rozwojem i skalowaniem działalności

Cyberbezpieczeństwo definiowane jest na poziomie krajowym w ustawie o krajowym systemie cyberbezpieczeństwa z 2018 r. jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[1].

Dlatego też za przedsiębiorstwo działające w branży cyberbezpieczeństwa można uznać firmę, która dostarcza produkty, usługi lub procesy chroniące poufność, integralność, dostępności i autentyczność danych w organizacji lub systemów, w których przetwarzane są dane, w tym dane osobowe również dane wrażliwe. Należy jednak zaznaczyć, że wiele firm działających w szeroko pojętym obszarze technologii informacyjnych (IT) posiada w swojej ofercie produkty lub usługi cyberbezpieczeństwa jednak nie są to dominujące w firmie obszary działalności. Na rynku działa również wiele firm zajmujących się odsprzedażą produktów cyberbezpieczeństwa (głównie zagranicznych firm) co pokazuje, że rynek cyberbezpieczeństwa w Polsce jest niejednorodny i trudny w potencjalnej analizie.

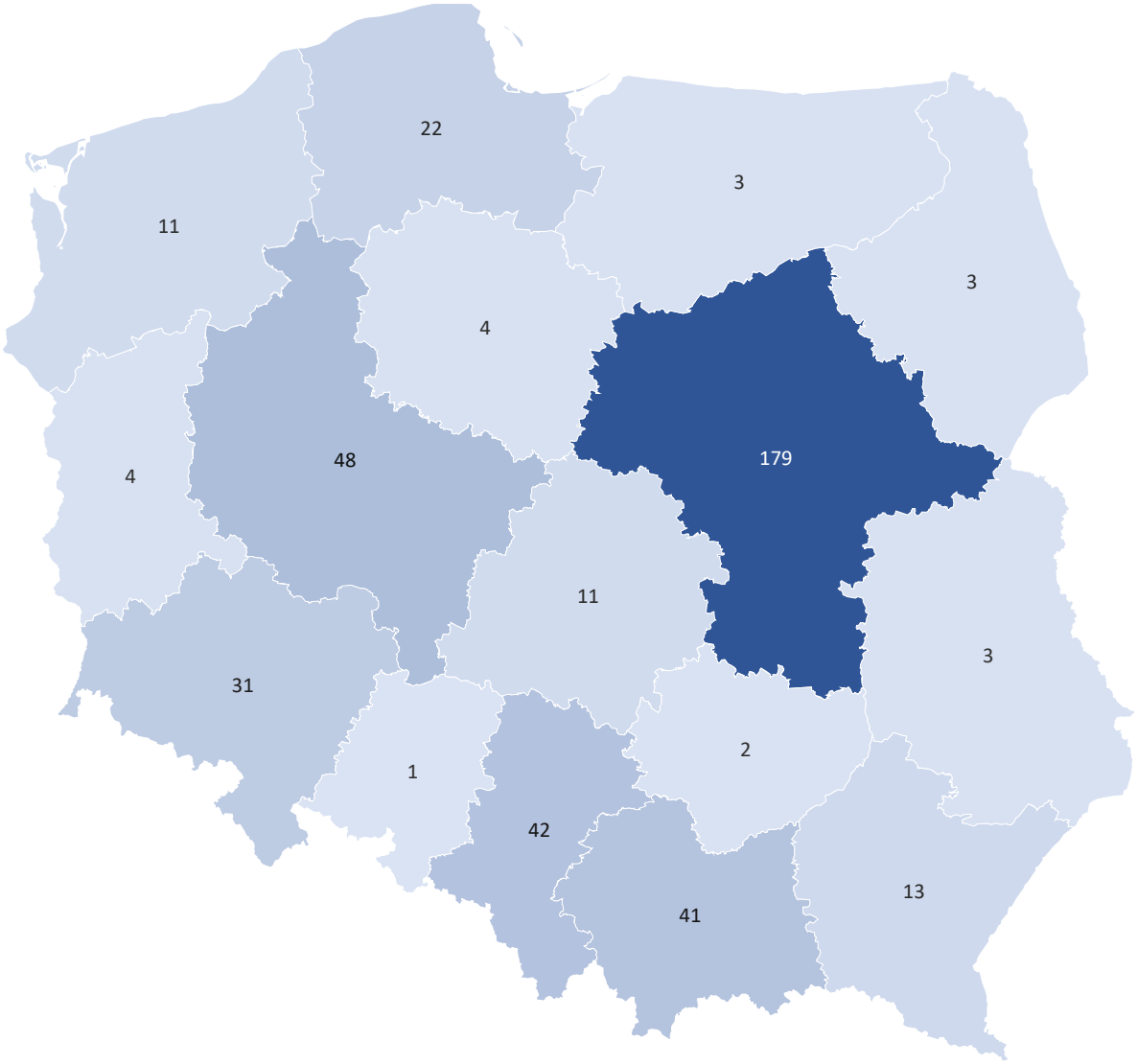
Według szacunków The Insights Partners globalny rynek cyberbezpieczeństwa w 2022 r. wart był ok. 203 mld USD[2]. Szacunki te pokrywają się również z danymi portalu Statista, który szacuje wartość globalnego rynku cyberbezpieczeństwa na 200 mld USD[3]. Co ważne w zależności od niektórych źródeł przewidywany globalny wzrost tego rynku (CAGR) szacowany jest między 7,5 a nawet 15% co w perspektywie do 2030 r. podniesie wartość rynku do 660 mld USD globalnie[4].

Wartość polskiego rynku cyberbezpieczeństwa w 2025 r. szacowana jest na 1 mld USD (ok. 3 mld PLN) co stanowi ok. 0,5% wartości światowego rynku cyberbezpieczeństwa. Gdyby do wartości rynku cyberbezpieczeństwa dodać chmurę obliczeniową, rynek usług data centrowych, backup, hosting oraz inne obszary, takie jak zapewnienie bezpieczeństwa fizycznego, zasilanie awaryjne i informatykę śledczą, możemy już mówić o skali rzędu 12 mld zł[5]. W latach 2021 - 2024 polski rynek cyberbezpieczeństwa notował stabilne kilkunastoprocentowe wzrosty (kolejno 11, 20, 15, 10%) co potwierdza wzrost popytu na rozwiązania z obszaru cyberbezpieczeństwa w Polsce. W latach 2025 - 2030 przewiduje się CAGR na poziomie ok. 6% co w przeciągu pięciu lat ma podnieść wartość rynku do 4 mld PLN[6]. Statystyki pokazują więc wyraźnie, że polski rynek cyberbezpieczeństwa będzie rósł wolniej w porównaniu do globalnej średniej przyrostu.

Na poniższej mapie przedstawiono rozkład przestrzenny 417 MŚP firm z branży cyberbezpieczeństwa w Polsce.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560.
[2] Artykuł "Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners." GlobeNewswire, 8 Nov. 2023. [Dostęp: 17.04.2025]
[3] "Cybersecurity – Worldwide." *Statista Market Forecast*. [Dostęp: 17.04.2025]
[4] Artykuł "Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners." GlobeNewswire, 8 Nov. 2023. [Dostęp: 17.04.2025]
[5] Artykuł "Ekosystem rozwiązań cyberbezpieczeństwa w Polsce wart jest 12 mld zł." *ITwiz*, 2024. [Dostęp: 17.04.2025]
[6] Artykuł "Poland Cybersecurity Market Size & Share Analysis – Growth Trends & Forecasts (2025–2030)." Mordor Intelligence. [Dostęp: 17.04.2025]

Mapa 1. Rozkład przestrzenny przedsiębiorstw z branży cyberbezpieczeństwa



Źródło: Analizy IBC Advisory S.A.

Najwięcej firm z branży cyberbezpieczeństwa działa w województwie mazowieckim, co czyni ten region liderem w skali kraju pod względem liczby przedsiębiorstw działających w tym sektorze. W pozostałych województwach liczba firm jest wyraźnie mniejsza: w wielkopolskim zarejestrowano 48 firm, w śląskim – 42, małopolskim – 41, a w dolnośląskim – 31.

W Polsce najliczniejszą grupę podmiotów działających w sektorze cyberbezpieczeństwa stanowią usługodawcy – 199 przedsiębiorstw. Na drugim miejscu znajdują się integratorzy – 129 przedsiębiorstw, a następnie vendorzy (producenci rozwiązań) – 67 przedsiębiorstw. Kolejną, mniej liczną grupę stanowią dystrybutorzy – 13 przedsiębiorstw, natomiast najmniejszą kategorię tworzą dystrybutorzy typu VAD (Value Added Distributors) – 10 przedsiębiorstw. Strukturę tę należy odczytywać jako odzwierciedlenie dominującego w Polsce modelu opartego na świadczeniu usług i integracji technologii, przy stosunkowo niewielkiej liczbie podmiotów prowadzących działalność produkcyjną lub dystrybucyjną.

Najwięcej przedsiębiorstw z sektora cyberbezpieczeństwa w Polsce zajmuje się monitorowaniem i reagowaniem na incydenty – 209 przedsiębiorstw. Kolejne najczęściej reprezentowane obszary działalności to: zgodność i zarządzanie bezpieczeństwem (compliance) – 195, bezpieczeństwo sieci – 172, ochrona urządzeń końcowych – 162, zarządzanie tożsamością i dostępem – 116 oraz szkolenia i działania z zakresu security awareness – 101. Mniej licznie reprezentowane specjalizacje to: testy penetracyjne, red teaming i audyty – 107, zarządzanie podatnościami – 71 oraz bezpieczeństwo chmury – 51. Najrzadziej występujące obszary to bezpieczeństwo przemysłowe (OT) – 45 przedsiębiorstw oraz prowadzenie Security Operation Center (SOC) – 44 przedsiębiorstwa.

Warto podkreślić, że jedno przedsiębiorstwo może świadczyć usługi w więcej niż jednym obszarze – zestawienie nie oznacza przypisania jednej kategorii do jednego podmiotu. Przedsiębiorstwa często działają równolegle w wielu segmentach rynku.

Łącznie 117 przedsiębiorstw specjalizuje się tylko w jednym typie usług. Pozostałe prowadzą działalność w dwóch lub więcej obszarach. Najwięcej przedsiębiorstw świadczy dwa – 102 przedsiębiorstwa, trzy – 59 przedsiębiorstw, cztery – 45 przedsiębiorstw lub pięć – 44 przedsiębiorstwa typów usług równocześnie. Zidentyfikowano również przedsiębiorstwa oferujące aż jedenaście różnych rodzajów usług – 3 przedsiębiorstwa – co pokazuje obecność silnie zdywersyfikowanych podmiotów w branży.

W toku badania zmapowano profil działalności firm z branży cyberbezpieczeństwa w podziale na województwa. Analiza wykazała wyraźne zróżnicowanie regionalne, zarówno pod względem liczby firm, jak i typów prowadzonej działalności. Szczególnej uwagi wymagają województwa, w których koncentruje się największa liczba podmiotów, tj. mazowieckie, wielkopolskie, dolnośląskie, śląskie oraz małopolskie.

Województwo mazowieckie wyróżnia się zdecydowaną dominacją w skali kraju – działa tu aż 179 firm z branży cyberbezpieczeństwa. Reprezentowane są praktycznie wszystkie typy działalności: usługodawcy, vendorzy, integratorzy, a także dystrybutorzy i firmy typu value added distributor (VAD). Przewagę liczebną mają zdecydowanie **usługodawcy**, co sugeruje silne zapotrzebowanie na doradztwo, wdrożenia i outsourcing usług cyberbezpieczeństwa w regionie. Obecność vendorów i integratorów potwierdza również rozwój autorskich rozwiązań oraz ofert kompleksowej obsługi technicznej. Znacząca liczba firm oraz ich zróżnicowany profil świadczy o dojrzałości rynku w stolicy i jej otoczeniu, gdzie znajduje się również największe skupisko instytucji publicznych, centrów danych i podmiotów regulowanych.

Województwo wielkopolskie to trzeci region pod względem liczby firm (48), przy czym dominującym modelem działalności także jest świadczenie usług. Występują również integratorzy i vendorzy, jednak w zdecydowanie mniejszej liczbie. Firmy w tym regionie najczęściej specjalizują się w testach penetracyjnych, zarządzaniu incydentami i reagowaniu na zagrożenia. Obszar ten rozwija się dynamicznie, choć w sposób bardziej wyspecjalizowany niż mazowiecki – skupia się na konkretnych segmentach usług.

Województwo dolnośląskie cechuje się dużą różnorodnością działalności przy stosunkowo mniejszej liczbie firm (31). Obok 21 usługodawców działają tu również vendorzy (6), integratorzy (2) oraz dystrybutorzy (2). W porównaniu do innych regionów, dolnośląskie wyróżnia się stosunkowo wysokim udziałem firm oferujących autorskie rozwiązania oraz pełniących funkcję pośredników technologicznych. Może to wynikać z lokalnej koncentracji ośrodków technologicznych i akademickich, zwłaszcza we Wrocławiu.

Województwo śląskie w którym działa 42 firmy z branży cyberbezpieczeństwa, stanowi jeden z ważniejszych regionalnych ośrodków sektora. Na szczególną uwagę zasługuje wysoki udział integratorów (18 firm), co wskazuje na silne zapotrzebowanie na kompleksowe wdrożenia i integrację systemów zabezpieczeń, szczególnie w dużych organizacjach przemysłowych i produkcyjnych. W regionie działają także usługodawcy (16) oraz vendorzy (7), co świadczy o istnieniu lokalnego zaplecza technicznego i kompetencyjnego. Profil rynku w województwie śląskim sugeruje koncentrację na praktycznych rozwiązaniach wspierających bezpieczeństwo infrastruktury przemysłowej oraz systemów OT (Operational Technology), co wpisuje się w charakter gospodarczy regionu.

Województwo małopolskie (41 firm) wykazuje podobny profil do wielkopolskiego. Przeważają usługodawcy świadczący szeroki zakres usług doradczych, audytowych oraz technicznych. W regionie występuje również kilku vendorów i integratorów. Obecność rozwiniętego sektora edukacji i technologii w Krakowie sprzyja rozwojowi lokalnych kompetencji i powstawaniu firm oferujących innowacyjne, specjalistyczne usługi.

1.2. Analiza ekosystemu

Aby w pełni zrozumieć dynamikę rynku oraz potrzeby i wyzwania polskich MŚP z branży cyberbezpieczeństwa należy rozpatrywać je w kontekście całego ekosystemu. Poniżej znajduje się podstawowa analiza, w której wyróżnione zostały najważniejsze i najaktywniejsze z punktu widzenia kształtowania rynku instytucje i organizacje działające w Polsce. Do nich zaliczają się m.in. Ministerstwo Cyfryzacji, Ministerstwo Rozwoju i Technologii, Narodowe Centrum Badań i Rozwoju, NASK-PIB, IŁ-PIB oraz Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa – Łukasiewicz - AI.

Ministerstwo Cyfryzacji (MC) realnie wpływa na MŚP w sektorze cyberbezpieczeństwa przede wszystkim poprzez tworzenie ram prawnych, które nakładają konkretne obowiązki na podmioty nimi objęte. Należy rozpatrywać tę kwestię w kategorii szans i zagrożeń dla MŚP w sektorze cyberbezpieczeństwa - regulacje w znacznym stopniu mogą przyczynić się do stymulacji popytu na rozwiązania z tej dziedziny, niemniej z drugiej strony ich nadmiar może spowodować chaos organizacyjny i zwiększenie kosztów związanych z budową cyberbezpieczeństwa wśród klientów końcowych[7]. Ministerstwo ponadto opracowuje, aktualizuje i wdraża Strategię Cyberbezpieczeństwa RP. Ważnym aspektem działalności MC dla MŚP w Polsce jest program PW Cyber, który funkcjonuje jako platforma integrująca sektor publiczny z prywatnym i umożliwia zwiększenie widoczności i wiarygodności na rynku. Dodatkowo, działania edukacyjne i promocyjne Ministerstwa podnoszą ogólną świadomość cyberbezpieczeństwa w gospodarce, co przekłada się na rosnące zapotrzebowanie na usługi MŚP, a współpraca międzynarodowa otwiera polskim firmom drogę do harmonizacji standardów i potencjalnej ekspansji na rynki zagraniczne[8]. Istotną rolę w tym działaniu pełni również NCC-PL, które aktywnie wspiera polskich przedsiębiorców działających na rynku europejskim, ale także jest punktem kontaktowym w zakresie działań i inicjatyw ECCC (The European Cybersecurity Competence Centre).

Ministerstwo Rozwoju i Technologii (MRiT) jako główna instytucja kształtująca politykę gospodarczą i innowacyjną państwa jest istotnym elementem ekosystemu cyberbezpieczeństwa, zwłaszcza w kontekście wsparcia finansowego i programowego dla MŚP, które chcą inwestować w cyberbezpieczeństwo lub rozwijać własne produkty i usługi w tej dziedzinie. Służą temu programy dotacyjne, ulgi podatkowe czy ułatwienia w dostępie do kapitału. Ponadto, MRiT kształtuje politykę handlową i inwestycyjną, działanie na rzecz zwiększania konkurencyjności polskiej gospodarki na arenie międzynarodowej, czy prowadzenie dialogu z przedsiębiorcami i partnerami społecznymi[9]. Ministerstwo sprawuje nadzór nad: Polską Agencją Rozwoju i Przedsiębiorczości oraz Polską Agencją Inwestycji i Handlu. Obie te instytucje posiadają dedykowane programy wsparcia rozwoju i ekspansji MŚP.

Narodowe Centrum Badań i Rozwoju (NCBR) to agencja wykonawcza Ministra Nauki i Szkolnictwa Wyższego, kluczowa dla finansowania i wspierania badań naukowych oraz prac rozwojowych w Polsce. NCBR aktywnie wspiera projekty z wielu obszarów, identyfikując strategiczne kierunki rozwoju i inwestując w innowacyjne rozwiązania. Instytucja ta jest niezwykle ważnym źródłem finansowania dla MŚP, które prowadzą własne projekty badawczo-rozwojowe w obszarze cyberbezpieczeństwa. Dzięki tym środkom możliwy jest rozwój innowacyjnych produktów i usług, zwiększanie swoich kompetencji i umacnianie pozycji na rynku. NCBR umożliwia również MŚP nawiązywanie współpracy z jednostkami naukowymi[10].

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) działa pod nadzorem **Ministerstwa Cyfryzacji.** Jako państwowy instytut badawczy, NASK-PIB realizuje zadania z pogranicza nauki, technologii i administracji publicznej, wspierając państwo w zakresie monitorowania zagrożeń w cyberprzestrzeni, podnoszenia poziomu świadomości cyfrowej, ochrony dzieci w sieci, a także wdrażania innowacyjnych rozwiązań w dziedzinie bezpieczeństwa teleinformatycznego. Zgodnie ze statutem NASK-PIB prowadzi badania naukowe i prace rozwojowe w określonym zakresie, przystosowuje ich wyniki do potrzeb praktyki, a także wdraża w usługach świadczonych m.in. na potrzeby organów bezpieczeństwa i porządku publicznego. Ponadto, Instytut dokonuje oceny zgodności, prowadzi procesy certyfikacji oraz działalność normalizacyjną.

[7] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 128.
[8] Strona internetowa Ministerstwa Cyfryzacji - Działania, Gov.pl. [Dostęp: 26.06.2025]
[9] Strona internetowa Ministerstwa Rozwoju i Technologii - działania ministerstwa, Gov.pl. [Dostęp: 26.06.2025]
[10] Strona internetowa Narodowego Centrum Badań i Rozwoju, Gov.pl. [Dostęp: 26.06.2025]

NASK–PIB pełni istotną funkcję w zakresie certyfikacji bezpieczeństwa, posiadając kompetencje w obszarze Common Criteria (CC) – międzynarodowego standardu oceny bezpieczeństwa produktów i systemów IT. Jednostka Certyfikująca NASK to jedyna instytucja w Polsce, która może wydawać międzynarodowe certyfikaty Common Criteria. Oceniają one, jak bezpieczne są produkty i systemy IT. Standard CC jest używany przez rządy i firmy na całym świecie do sprawdzania bezpieczeństwa technologii. W ramach wsparcia dla MŚP, instytut realizuje również program „Firma Bezpieczna Cyfrowo", którego celem jest podnoszenie poziomu cyberbezpieczeństwa w małych i średnich przedsiębiorstwach poprzez audyty, szkolenia i dobre praktyki. Po zakończeniu działań doskonalących, firma może zgłosić się do Jednostki Certyfikującej NASK w celu rozpoczęcia procesu certyfikacji w ramach niniejszego programu.

W strukturze krajowego systemu cyberbezpieczeństwa NASK prowadzi CSIRT NASK – jeden z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego, obok CSIRT GOV (prowadzony przez ABW) i CSIRT MON (prowadzony przez MON).

Z art. 26 ustawy o KSC wynikają m.in. następujące zadania dla CSIRT-NASK:

- Koordynacja obsługi incydentów zgłaszanych przez określone jednostki.
- Tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach.
- Zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzących działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych.

Oraz

- Monitorowanie zagrożeń cyberbezpieczeństwa w zakresie sieci i systemów teleinformatycznych.
- Przyjmowanie zgłoszeń o incydentach i wspieranie podmiotów w ich obsłudze.
- Analiza incydentów i zagrożeń oraz ich skutków.
- Wymiana informacji o zagrożeniach z innymi podmiotami krajowego systemu cyberbezpieczeństwa oraz z CSIRT GOV i CSIRT MON.
- Współpraca z sektorem prywatnym i międzynarodowym w zakresie cyberbezpieczeństwa[11].

Dodatkowo, NASK-PIB może być zaangażowany w szkolenia, ćwiczenia, kampanie edukacyjne oraz działania prewencyjne, w celu zwiększenia świadomości w zakresie cyberbezpieczeństwa.

Instytut Łączności - Państwowy Instytut Badawczy (IŁ-PIB) to niezależna, krajowa jednostka badawczo-rozwojowa specjalizująca się w telekomunikacji oraz technologiach informacyjnych. Instytut aktywnie współpracuje z krajowymi i międzynarodowymi ośrodkami naukowymi, wspierając integrację środowiska badawczego i uczestnicząc w tworzeniu Europejskiej Przestrzeni Badawczej (European Research Area). Wśród działań Instytutu dedykowanych sektorowi prywatnemu w głównej mierze wyróżnia się jego działalność związaną z procesem certyfikacji, badaniem zgodności z normami czy wsparcie przy tworzeniu dokumentacji technicznej oraz deklaracji zgodności. Jego działalność naukowa ma zarówno charakter rozwojowy, jak i aplikacyjny[12].

Sieć Badawcza Łukasiewicz - Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa – Łukasiewicz – AI to jeden z czołowych instytutów badawczych w Polsce, wchodzący w skład Sieci Badawczej Łukasiewicz. Instytut prowadzi badania naukowe i prace rozwojowe, tworząc rozwiązania dla przemysłu, administracji publicznej oraz sektora obronnego. Instytut jest potencjalnym partnerem badawczo-rozwojowym dla MŚP, oferującym dostęp do specjalistycznej wiedzy i infrastruktury badawczej. Instytut AI oferuje również usługi przygotowania do procesu certyfikacji Common criteria i razem z IŁ jest jednostką oceniającą zgodność w ramach tego schematu. MŚP mogą współpracować z instytutem przy tworzeniu innowacyjnych produktów i usług w obszarze cyberbezpieczeństwa, szczególnie w kontekście przemysłowym (OT/ICS). Instytut może również oferować szkolenia i konsultacje, pomagając MŚP w podnoszeniu ich kompetencji technologicznych i biznesowych[13].

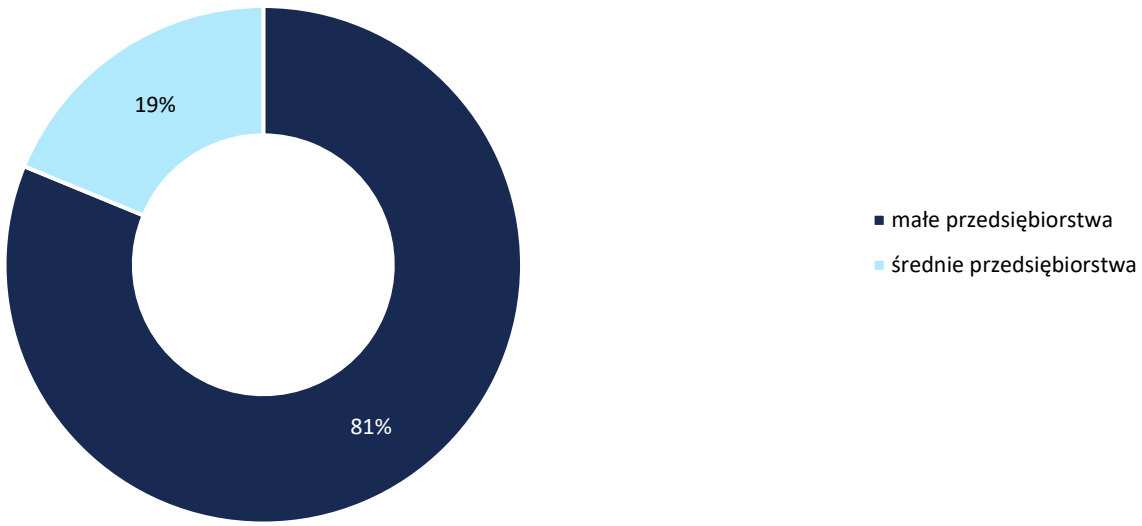
[11] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560, s. 26-28.
[12] Strona internetowa Instytutu Łączności – Państwowego Instytutu Badawczego, Gov.pl. [Dostęp: 18.04.2025]
[13] Strona internetowa Łukasiewicz – AI, Gov.pl. [Dostęp: 04.07.2025]

1.3. Charakterystyka przedsiębiorstw MŚP w branży cyberbezpieczeństwa w Polsce

W badaniu ilościowym wzięło udział 201 przedsiębiorstw, zaklasyfikowanych według ich wielkości. Ankietę wypełniło 197 firm, natomiast w wywiadach pogłębionych uczestniczyło 20 przedstawicieli przedsiębiorstw – w tym cztery podmioty, które nie brały udziału w badaniu ankietowym. Respondenci zostali podzieleni na dwie kategorie: małe oraz średnie przedsiębiorstwa. Rozkład firm w próbie prezentuje się następująco:

- Małe przedsiębiorstwa – 160 firm – przez które rozumie się podmiot zatrudniający średniorocznie do 50 pracowników oraz osiągający roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 10 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 milionów euro.
- Średnie przedsiębiorstwa – 37 firm – przez które rozumie się podmiot jednocześnie zatrudniający średniorocznie mniej niż 250 pracowników oraz osiągający roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro i który nie jest małym przedsiębiorstwem).

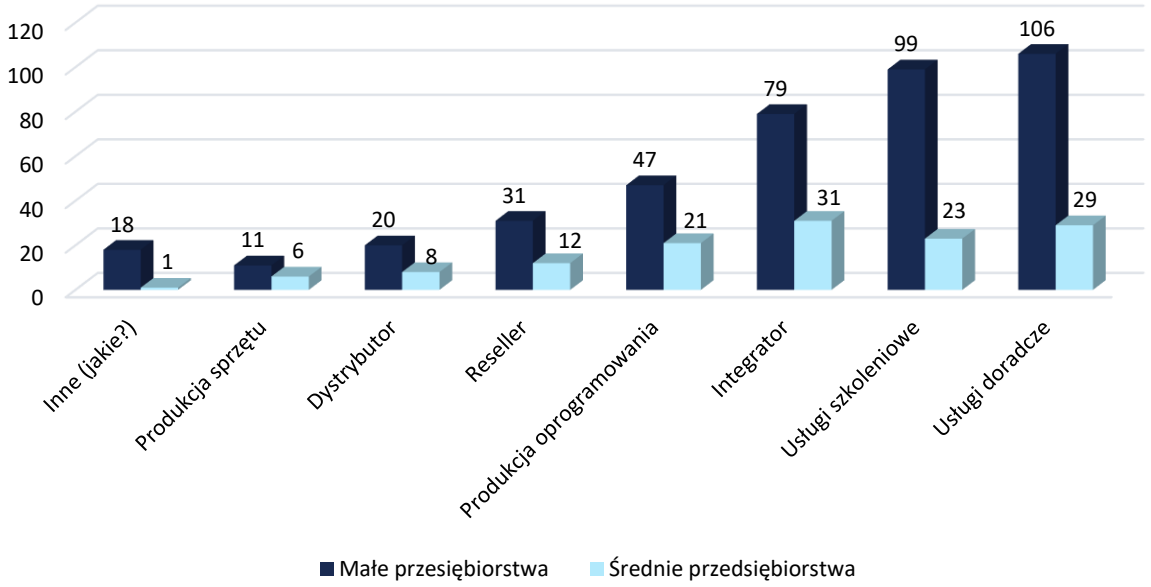
Wykres 1. Jaki status posiada przedsiębiorstwo? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Następnie respondenci w badaniu CAWI zostali zapytani o rodzaj działalności prowadzonej w ramach branży cyberbezpieczeństwa. Pytanie miało charakter wielokrotnego wyboru, co pozwoliło firmom wskazać wszystkie obszary, w których są aktywne.

Wykres 2. Rodzaj działalności w branży cyberbezpieczeństwa (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Uzyskane odpowiedzi wskazują na dużą różnorodność świadczonych usług i oferowanych produktów. Najczęściej wskazywane przez małe i średnie przedsiębiorstwa były:

- usługi doradcze (łącznie 135),
- usługi szkoleniowe (łącznie 122),
- integracja rozwiązań bezpieczeństwa (łącznie 110),
- produkcja oprogramowania (47 wskazań przez małe oraz 21 przez średnie przedsiębiorstwa),
- działalność resellerska i dystrybucyjna (łącznie 71),
- produkcja sprzętu (11 wskazań przez małe oraz 6 przez średnie przedsiębiorstwa).

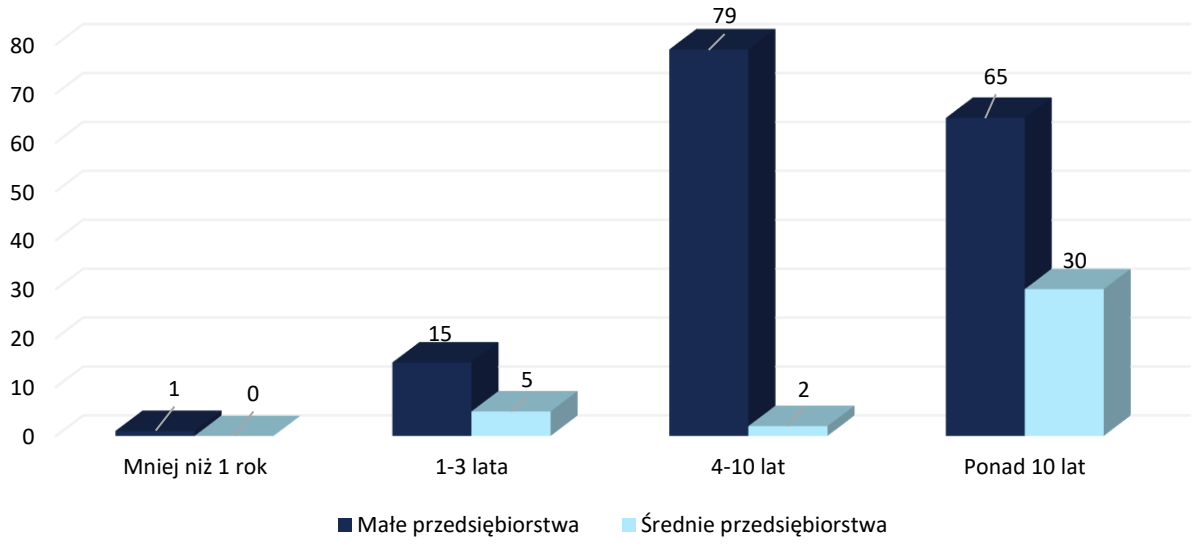
W odpowiedziach otwartych pojawiły się m.in.:

- zarządzane usługi bezpieczeństwa (MSSP, SOC, MDR),
- testy bezpieczeństwa i testy penetracyjne,
- outsourcing usług IT,
- specjalistyczne usługi związane z infrastrukturą krytyczną (NIS2),
- działalność telekomunikacyjna oraz testowanie oprogramowania.

Wyniki te pokazują, że wiele firm działa równolegle w kilku segmentach rynku, oferując zarówno usługi, jak i produkty, co potwierdza złożony charakter polskiego rynku cyberbezpieczeństwa.

Na wykresie 3. przedstawiono staż firm na rynku, czyli informację o tym, jak długo badane przedsiębiorstwa funkcjonują w obrocie rynkowym.

Wykres 3. Ile lat firma działa na rynku? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

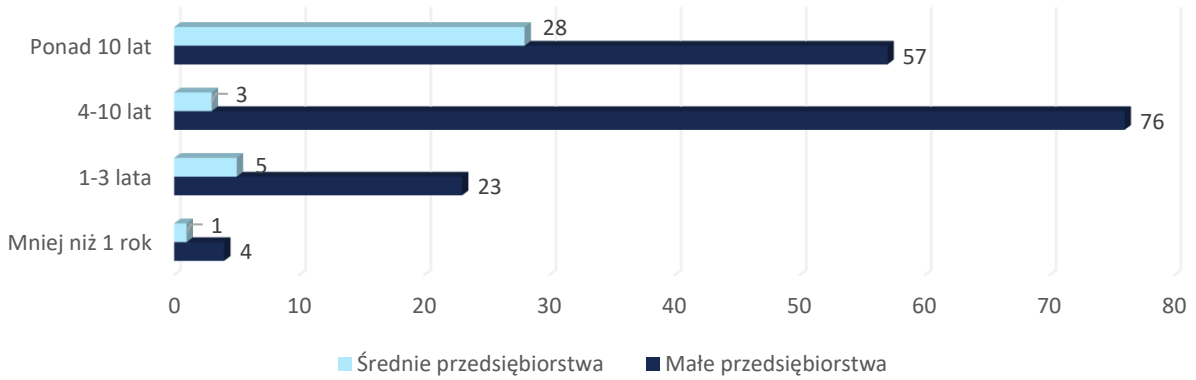
Zdecydowana większość firm obecnych na rynku cyberbezpieczeństwa to podmioty funkcjonujące od wielu lat. Wśród małych przedsiębiorstw największą grupę stanowią firmy, które istnieją od 4 do 10 lat – jest ich 79, a kolejne 65 działa ponad 10 lat. Mniej liczne są firmy młodsze: 15 działa od 1 do 3 lat, a tylko 1 krócej niż rok.

W przypadku średnich przedsiębiorstw dominują firmy o najdłuższym stażu – 30 z nich istnieje ponad 10 lat. Znacznie mniej jest podmiotów młodszych: 5 działa od 1 do 3 lat, a tylko 2 od 4 do 10 lat. Nie odnotowano żadnej średniej firmy funkcjonującej krócej niż rok.

Dane te pokazują, że w grupie MŚP działających w branży cyberbezpieczeństwa przeważają firmy z kilkuletnim lub wieloletnim stażem, a udział nowo powstałych podmiotów jest niewielki. Może to świadczyć o tym, że działalność w obszarze cyberbezpieczeństwa rozwijają przede wszystkim firmy z ugruntowaną pozycją i doświadczeniem na rynku.

Na poniższym wykresie przedstawiono, jak długo firmy działają w obszarze cyberbezpieczeństwa. Dane pokazują doświadczenie przedsiębiorstw w tej konkretnej dziedzinie, co może mieć wpływ na ich kompetencje, ofertę usług oraz pozycję na rynku.

Wykres 4. Ile lat firma działa w obszarze cyberbezpieczeństwa? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

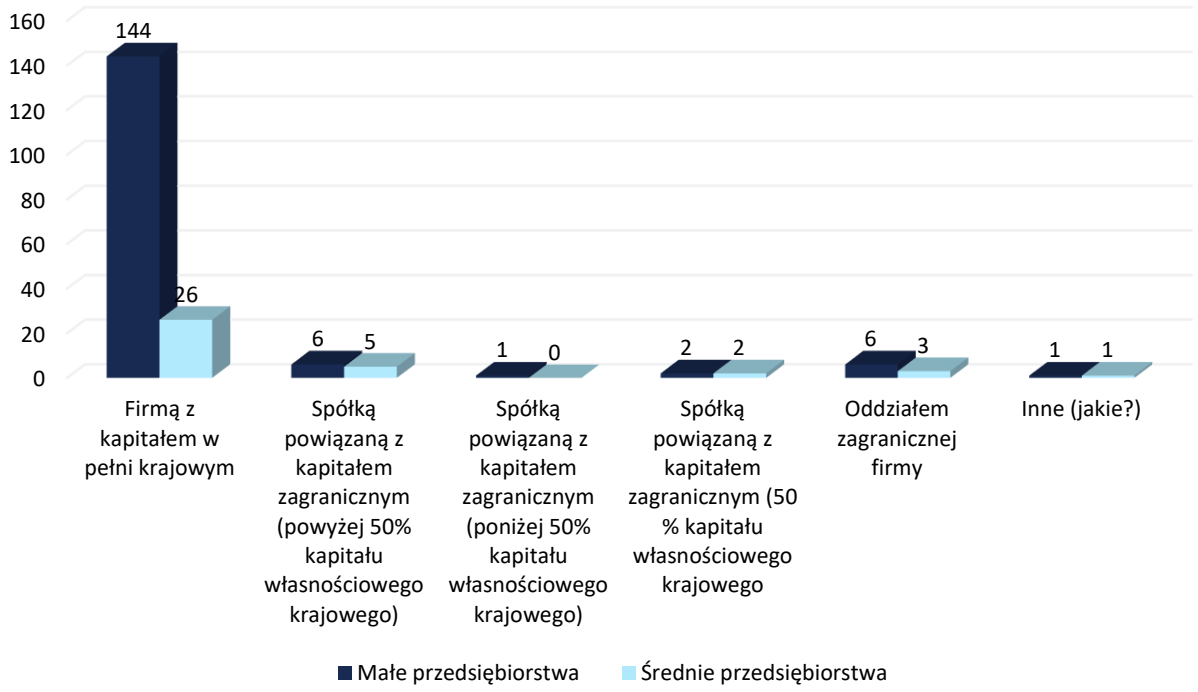
Wśród małych przedsiębiorstw największą grupę stanowią firmy, które działają w branży cyberbezpieczeństwa od 4 do 10 lat – jest ich 76. Kolejną liczną kategorią są podmioty aktywne w tym obszarze ponad 10 lat (57 firm). 23 małe firmy rozpoczęły działalność w cyberbezpieczeństwie w ciągu ostatnich 1–3 lat, a 4 prowadzą ją krócej niż rok. Oznacza to, że choć część firm mogła istnieć wcześniej, ich aktywność w obszarze cyberbezpieczeństwa rozpoczęła się dopiero na późniejszym etapie rozwoju.

W przypadku średnich przedsiębiorstw najwięcej firm (28) prowadzi działalność w cyberbezpieczeństwie ponad 10 lat. Znacznie mniej firm rozpoczęło działalność w tym obszarze 1–3 lata temu (5 firm) lub 4–10 lat temu (3 firmy), a tylko 1 firma działa w branży od mniej niż roku.

Dane pokazują, że zarówno małe, jak i średnie przedsiębiorstwa najczęściej posiadają wieloletnie doświadczenie w obszarze cyberbezpieczeństwa, chociaż niekoniecznie od początku istnienia firmy. Najwięcej firm rozpoczęło działalność w tej branży co najmniej cztery lata temu, co może świadczyć o stabilizacji rynku i rozwijaniu specjalizacji w odpowiedzi na rosnące zapotrzebowanie na usługi związane z bezpieczeństwem cyfrowym.

Poniższy wykres ilustruje szczegółowy podział struktury własności kapitałowej badanych przedsiębiorstw. Zdecydowaną większość wszystkich respondentów, stanowiły firmy z kapitałem w pełni krajowym. Udział podmiotów z jakąkolwiek formą kapitału zagranicznego był relatywnie niewielki.

Wykres 5. Firma jest: (N=197)

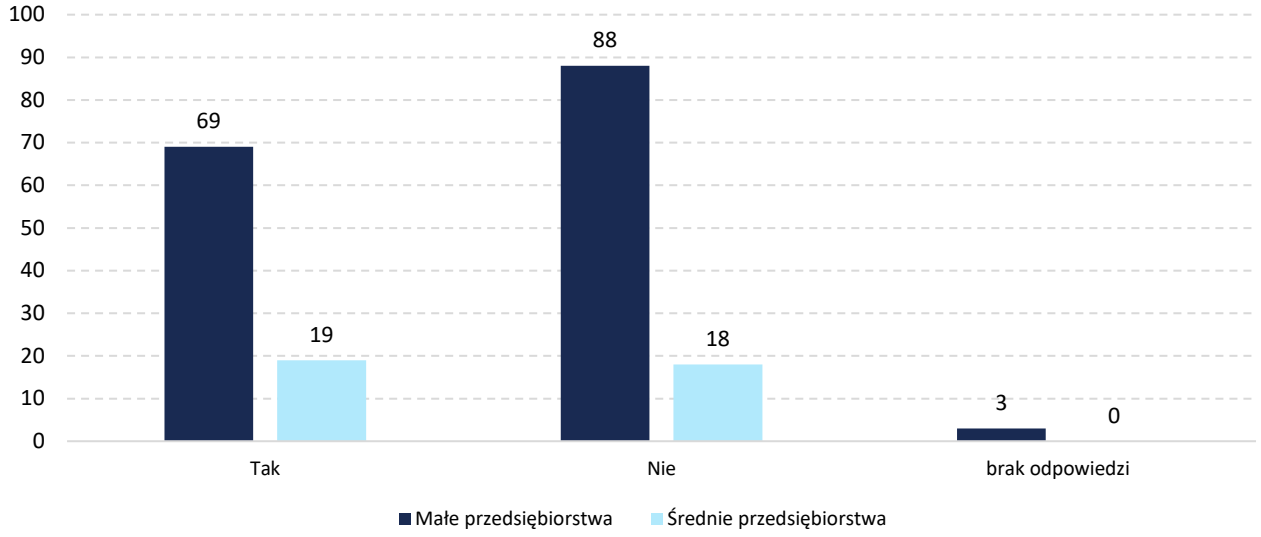


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość firm będących respondentami badania to podmioty z kapitałem w pełni krajowym. Taką formę własności zadeklarowało 144 małych oraz 26 średnich przedsiębiorstw. Oznacza to, że sektor MŚP w obszarze cyberbezpieczeństwa w Polsce opiera się przede wszystkim na firmach krajowych.
Pozostałe formy własności kapitałowej występowały znacznie rzadziej. Spółki powiązane z kapitałem zagranicznym, w których ponad 50% kapitału pozostaje w rękach właścicieli krajowych, wskazało 6 małych i 5 średnich firm. Firmy, w których poniżej 50% kapitału ma pochodzenie krajowe, reprezentowane były tylko przez 1 małe przedsiębiorstwo, a wśród średnich nie odnotowano żadnego przypadku. Po 2 małe i 2 średnie firmy zadeklarowały równy udział kapitału krajowego i zagranicznego (50/50).

W badaniu wzięło też udział 6 małych i 3 średnie przedsiębiorstwa, które są oddziałami zagranicznych firm. Kategorie niestandardowe, określone jako „inne", wskazało po 1 respondencie z każdej grupy.
Wyniki te pokazują, że wśród firm MŚP działających w obszarze cyberbezpieczeństwa dominują podmioty o krajowym kapitale, a powiązania zagraniczne występują jedynie incydentalnie.
Kolejnym z badanych aspektów było członkostwo firm w organizacjach branżowych, takich jak klastry czy izby przemysłowe. Przynależność do tego typu struktur może sprzyjać wymianie wiedzy, współpracy oraz wspólnemu podejmowaniu działań z zakresu cyberbezpieczeństwa. W ankiecie zapytano respondentów, czy ich firma należy do takiej organizacji.

Wykres 6. Czy firma należy do jakiejś organizacji branżowej (np. klastrów, izb przemysłowych)? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość firm biorących udział w badaniu nie należy do żadnej organizacji branżowej, takiej jak klastry czy izby przemysłowe. Brak przynależności zadeklarowało 88 małych oraz 18 średnich przedsiębiorstw. Członkostwo w organizacjach branżowych potwierdziło 69 małych i 19 średnich firm. Oznacza to, że choć pewna część przedsiębiorstw dostrzega wartość w uczestnictwie w strukturach branżowych, to jednak nadal dominuje postawa niezależności organizacyjnej. Warto również odnotować, że 3 małe firmy nie udzieliły odpowiedzi na to pytanie, natomiast wśród średnich przedsiębiorstw nie odnotowano przypadków braku odpowiedzi.

Wyniki te sugerują, że mimo istnienia struktur wspierających współpracę i reprezentację interesów branżowych, znaczna część firm MŚP działających w branży cyberbezpieczeństwa w Polsce funkcjonuje poza tego typu organizacjami.

Następnie respondenci zostali zapytani o technologie i usługi rozwijane w ich firmach w zakresie cyberbezpieczeństwa.

Wśród firm specjalizujących się w rozwiązaniach z zakresu cyberbezpieczeństwa można wyróżnić wiele kategorii oferowanych usług i produktów. Rynek cyberbezpieczeństwa w Polsce jest mocno rozdrobniony, dlatego na potrzeby niniejszej analizy małe i średnie przedsiębiorstwa z branży cyberbezpieczeństwa zostały sklasyfikowane w 12 najpopularniejszych kategoriach.

1. **Ochrona urządzeń końcowych (Endpoint Security)** - to klasa rozwiązań koncentrujących się na zabezpieczeniu wszelkich urządzeń używanych przez użytkowników do uzyskiwania dostępu do zasobów organizacji – takich jak komputery stacjonarne, laptopy, tablety czy smartfony. Urządzenia te są jednymi z najczęstszych wektorów ataku, dlatego stanowią krytyczny punkt w strategii bezpieczeństwa IT. Rozwiązania z tej kategorii mają na celu wykrywanie i blokowanie złośliwego oprogramowania, zapobieganie nieautoryzowanemu dostępowi oraz monitorowanie nietypowych zachowań użytkowników.
   Systemy ochrony endpointów rozwiązują problem podatności urządzeń na ataki typu ransomware, phishing, złośliwe oprogramowanie (malware), a także niezamierzone wycieki danych spowodowane przez użytkowników. Współczesne rozwiązania nie ograniczają się jedynie do tradycyjnych antywirusów – coraz częściej wykorzystują

zaawansowane techniki analizy zachowań (behavioural analysis), sztuczną inteligencję oraz zautomatyzowaną odpowiedź na incydenty[14].

2. **Bezpieczeństwo sieci (Network Security)** - obejmuje zestaw technologii, polityk i praktyk, które chronią integralność, poufność i dostępność infrastruktury sieciowej oraz danych w niej przesyłanych. Współczesne organizacje – niezależnie od wielkości – polegają na sieciach jako podstawowym nośniku danych i usług, dlatego ich ochrona jest kluczowym elementem systemu cyberbezpieczeństwa. Rozwiązania w tej kategorii zapobiegają nieautoryzowanemu dostępowi, atakom typu DDoS, infekcjom malware czy wyciekom danych poprzez kontrolę przepływu informacji i analizę ruchu sieciowego.
   Do głównych technologii zaliczamy zapory sieciowe (firewalle), które filtrują ruch na podstawie zdefiniowanych reguł, systemy IDS/IPS (Intrusion Detection/Prevention Systems) służące do wykrywania i blokowania podejrzanych działań, oraz systemy segmentacji sieci, które ograniczają możliwość rozprzestrzeniania się zagrożeń. Coraz częściej stosowane są także rozwiązania typu NDR (Network Detection and Response), które zapewniają zaawansowaną analizę i reagowanie w czasie rzeczywistym[15].
3. **Zarządzanie tożsamością i dostęp (Identity and Access Management, IAM)** - obejmuje zestaw polityk, procesów i technologii, które umożliwiają firmom kontrolowanie, kto ma dostęp do jakich zasobów cyfrowych, w jakich warunkach i z jakim poziomem uprawnień. Rozwiązania IAM mają kluczowe znaczenie dla zapobiegania nieautoryzowanemu dostępowi, ograniczania ryzyka wycieku danych oraz spełniania wymogów regulacyjnych. Systemy IAM wspierają zarządzanie pełnym cyklem życia tożsamości – od tworzenia kont użytkowników, przez nadawanie ról, aż po ich dezaktywację[16].
4. **Bezpieczeństwo chmury (Cloud Security)** - obejmuje zbiór narzędzi, technologii i praktyk, które chronią dane, aplikacje oraz usługi przechowywane w chmurze przed zagrożeniami, takimi jak utrata danych, nieautoryzowany dostęp czy ataki DDoS. Ze względu na rosnącą popularność rozwiązań chmurowych, zapewnienie odpowiedniego poziomu bezpieczeństwa jest kluczowe, zwłaszcza przy przechowywaniu wrażliwych informacji. W ramach bezpieczeństwa chmury wykorzystywane są mechanizmy takie jak szyfrowanie danych, kontrola dostępu, zarządzanie tożsamościami (IAM) oraz monitorowanie i audyt działań użytkowników[17].
5. **Testy penetracyjne, Red Taming, audyty** - to kluczowe techniki oceny bezpieczeństwa, które pomagają organizacjom w identyfikowaniu słabości systemów przed ich wykorzystaniem przez cyberprzestępców. Testy penetracyjne polegają na symulowaniu ataków zewnętrznych w celu wykrycia luk w zabezpieczeniach aplikacji, sieci i infrastruktury. Red Teaming to bardziej kompleksowe podejście, które imituje działania zaawansowanych zagrożeń, takich jak zorganizowane grupy cyberprzestępcze, testując nie tylko technologie, ale również procesy i ludzi. Audyty bezpieczeństwa to szczegółowe przeglądy systemów i procedur w organizacji, mające na celu ocenę zgodności z normami, politykami i najlepszymi praktykami branżowymi[18].
6. **Zarządzanie podatnościami (Vulnerability Management)** - Zarządzanie podatnościami to proces identyfikacji, oceny, klasyfikowania i eliminowania luk w zabezpieczeniach systemów informatycznych, mający na celu minimalizację ryzyka związanego z ich wykorzystaniem przez cyberprzestępców. Kluczowe elementy tego procesu to inwentaryzacja zasobów, regularne skanowanie w poszukiwaniu podatności, analiza ryzyka, priorytetyzacja oraz remediacja poprzez stosowanie odpowiednich poprawek i łatek. Narzędzia związane z zarządzaniem podatnościami wspierają automatyczne wykrywanie i zarządzanie podatnościami, umożliwiając efektywne monitorowanie i zabezpieczanie infrastruktury IT[19].
7. **Monitorowanie i reagowanie na incydenty (Incident Monitoring and Response)** - polega na ciągłym nadzorowaniu aktywności systemów IT w celu wykrywania podejrzanych działań oraz szybkiej reakcji na zaistniałe zagrożenia. Celem jest jak najszybsze zidentyfikowanie i neutralizowanie incydentów, takich jak ataki hakerskie, złośliwe oprogramowanie czy nieautoryzowane dostępy. Narzędzia do monitorowania, umożliwiają gromadzenie, analizowanie i korelowanie danych z różnych źródeł, co pozwala na szybsze wykrycie i odpowiedź na incydenty.

[14] Artykuł "Threat Landscape for Endpoint Security". ENISA, 2023. [Dostęp: 17.04.2025]
[15] Artykuł "Network and Information Security Threat Landscape". ENISA, 2023. [Dostęp: 17.04.2025]
[16] Artykuł "Co to jest zarządzanie dostępem i tożsamościami?". Microsoft, 2025. [Dostęp: 17.04.2025]
[17] Artykuł "Bezpieczeństwo w chmurze". Microsoft, 2025. [Dostęp: 17.04.2025]
[18] Artykuł "Penetration Testing and Red Teaming". ENISA, 2023. [Dostęp: 17.04.2025]
[19] Publikacja "Vulnerability Management". Qualys, 2023.[Dostęp: 17.04.2025]

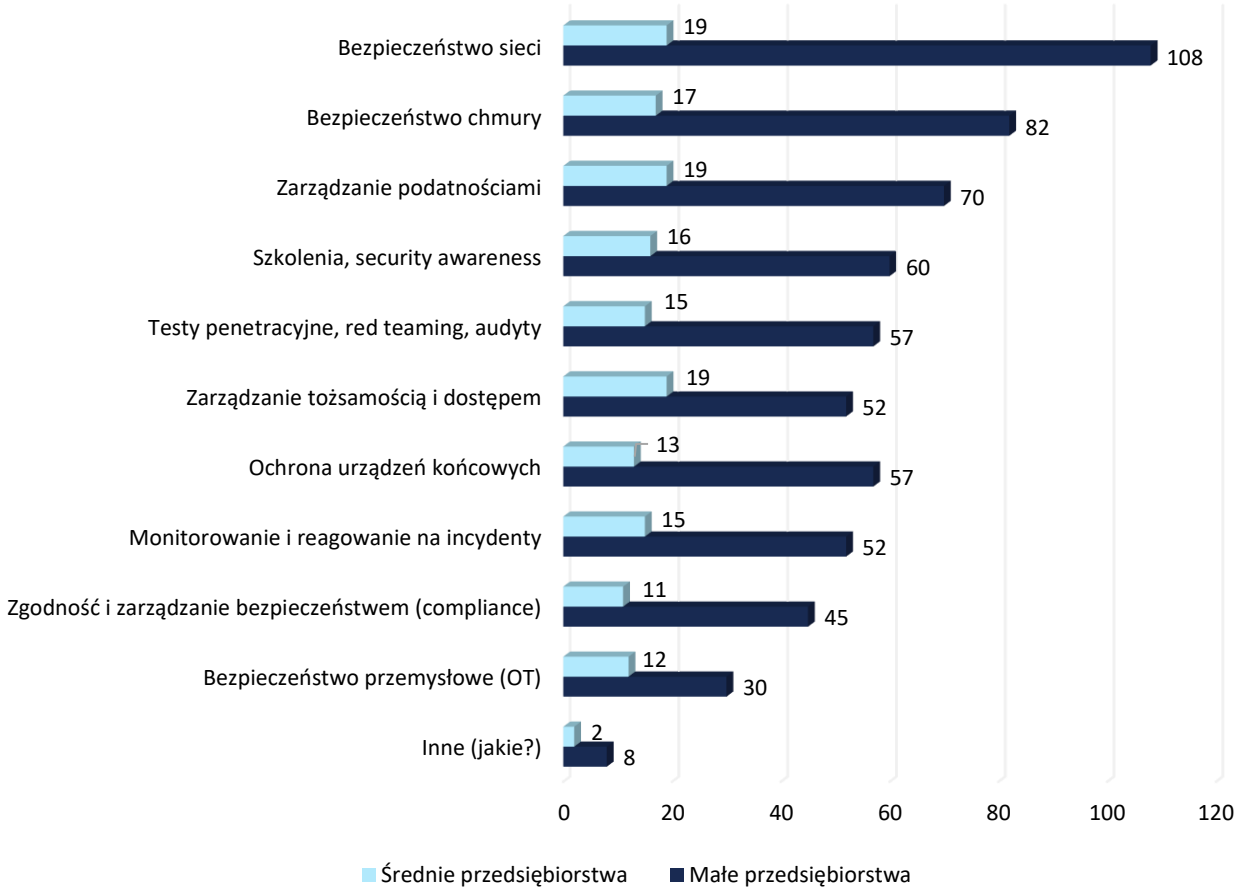
W ramach reakcji na incydent podejmuje się działania takie jak izolacja zagrożonych systemów, przeprowadzenie dochodzenia oraz wdrożenie działań naprawczych[20].

8. **Szkolenia, security awarness (Security Awareness and Training)** - Szkolenia z zakresu bezpieczeństwa oraz podnoszenie świadomości pracowników to kluczowe elementy w ochronie organizacji przed zagrożeniami, które mogą wynikać z błędów ludzkich. Celem tych działań jest edukowanie pracowników na temat najlepszych praktyk w zakresie bezpieczeństwa, rozpoznawania zagrożeń, takich jak phishing czy socjotechnika oraz właściwego reagowania na podejrzane sytuacje. Programy szkoleniowe mogą obejmować kursy e-learningowe, warsztaty, testy na próbnych scenariuszach oraz symulacje ataków. Właściwie zaplanowane i regularne szkolenia zwiększają świadomość bezpieczeństwa w organizacji, co znacząco zmniejsza ryzyko związane z atakami skierowanymi na użytkowników[21].
9. **Zgodność i zarządzanie bezpieczeństwem, compliance, konsulting** - pomagają organizacjom przestrzegać obowiązujących regulacji prawnych oraz zapewniają bezpieczeństwo informacji w firmach. Główne aspekty to wdrażanie polityk, procedur oraz standardów ochrony danych, takich jak RODO (ochrona danych osobowych) czy ISO/IEC 27001 (systemy zarządzania bezpieczeństwem informacji). Firmy przeprowadzają audyty zgodności, monitorują przestrzeganie przepisów, a także oceniają ryzyko związane z bezpieczeństwem informacji. Działania te pomagają w minimalizowaniu ryzyka naruszeń i zapewnieniu ciągłości działalności organizacji. W tym obszarze wykorzystuje się także usługi konsultingowe, które wspierają organizacje w dostosowywaniu procesów do zmieniających się wymogów prawnych[22].
10. **Bezpieczeństwo przemysłowe (OT security)** - Bezpieczeństwo technologii operacyjnej (OT security) dotyczy ochrony systemów i urządzeń wykorzystywanych w infrastrukturze przemysłowej, takich jak urządzenia sterujące, czujniki i systemy monitorujące. Celem jest zapewnienie integralności, dostępności i poufności tych systemów przed zagrożeniami cybernetycznymi. Składa się na to zarządzanie dostępem, monitorowanie i detekcję incydentów, a także zapewnienie zgodności z przepisami. Ochrona OT jest kluczowa, szczególnie w sektorach takich jak energetyka, produkcja czy transport, gdzie awaria systemów może mieć poważne konsekwencje[23].
11. **Security Operation Center (SOC)** - to dedykowane centrum odpowiedzialne za monitorowanie, analizowanie i reagowanie na incydenty bezpieczeństwa w organizacji. Zespół SOC, składający się z analityków i inżynierów bezpieczeństwa, pracuje 24/7, aby zapewnić ochronę przed zagrożeniami cybernetycznymi. Ich zadania obejmują monitorowanie sieci i systemów, analizowanie zdarzeń bezpieczeństwa oraz koordynację reakcji na incydenty, co pozwala na szybkie wykrywanie i łagodzenie potencjalnych ataków[24].
12. **Inne (other)** - kategoria inne obejmuje wszystkie usługi, rozwiązania i procesy, które nie kwalifikują się do żadnej z powyższych kategorii. Ponadto kategoria inne obejmuje firmy, które w swojej ofercie mają rozwiązania, które nie są związane bezpośrednio z cyberbezpieczeństwem jak np. dostarczanie systemów klasy ERP, CRM, serwerów, usług hostingowych itp.

[20] Artykuł "Digital Forensics and Incident Response Retainer Services Reviews and Ratings". Gartner, 2025. [Dostęp: 17.04.2025]
[21] Artykuł "Security Awareness Training". SANS Institute, 2025. [Dostęp: 17.04.2025]
[22] Artykuł "Building Trust for Today and Tomorrow". PwC, 2025. [Dostęp: 17.04.2025]
[23] Artykuł "What Is Operational Technology (OT) Security?". Cisco, 2025. [Dostęp: 17.04.2025]
[24] Artykuł "What Is a Security Operations Center (SOC)?". IBM, 2024. [Dostęp: 17.04.2025]

Poniższe dane pokazują, które obszary cieszą się największym zainteresowaniem i inwestycjami, a także jakie niszowe rozwiązania są obecne w sektorze.

Wykres 7. Jakie technologie/usługi są rozwijane przez Państwa firmę? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci badania, reprezentujący małe i średnie przedsiębiorstwa z sektora cyberbezpieczeństwa, najczęściej wskazywali rozwój technologii i usług związanych z bezpieczeństwem sieciowym. Tę kategorię zadeklarowało 82 małe oraz 19 średnich firm, co czyni ją najczęściej rozwijaną dziedziną wśród badanych podmiotów.

Na kolejnych miejscach znalazły się: zarządzanie tożsamością i dostępem (70 małych i 17 średnich firm), szkolenia oraz usługi typu security awareness (60 małych i 19 średnich firm), testy penetracyjne i audyty bezpieczeństwa (57 małych i 16 średnich firm), a także ochrona urządzeń końcowych (57 małych i 13 średnich firm).

Znacząca liczba respondentów rozwija również rozwiązania z zakresu monitorowania i wykrywania zagrożeń (52 małe i 15 średnich firm) oraz zarządzania incydentami bezpieczeństwa (52 małe i 19 średnich firm). Mniej popularne, choć nadal istotne, są usługi związane ze zgodnością i audytem (45 małych i 11 średnich firm) oraz ogólne rozwiązania z zakresu bezpieczeństwa informacji (30 małych i 12 średnich firm).

Mniej liczne, ale ciekawe są odpowiedzi w kategorii Inne (10 firm), gdzie wymieniono m.in.:

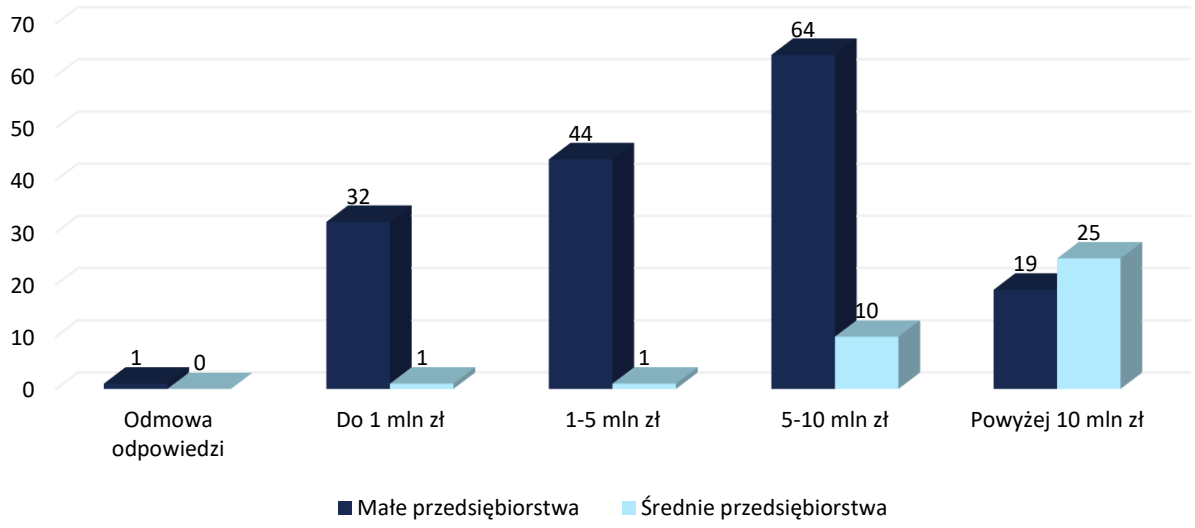
- niszczenie danych,
- technologie synchronizacji odporne na jamming/spoofing GPS,
- rozwiązania ISAC i CTI,
- Managed Security i SOC 24/7,
- narzędzia do szyfrowania end-to-end,

- obsługę prawną twórców AI,
- oraz niszowe oprogramowanie np. dla kolei.

Największy nacisk firmy kładą na klasyczne filary bezpieczeństwa IT – ochronę sieci, chmury i zarządzanie podatnościami. Coraz większe znaczenie mają również działania edukacyjne i prewencyjne. Mniej liczne, ale innowacyjne rozwiązania pokazują z kolei rozwój specjalistycznych i niszowych technologii w branży. Warto zaznaczyć, że w przypadku średnich przedsiębiorstw odpowiedzi dotyczące rozwijanych technologii i usług rozłożyły się stosunkowo równomiernie pomiędzy poszczególne kategorie. Choć bezpieczeństwo sieciowe, zarządzanie podatnością i zarządzanie tożsamością i dostępem były najczęściej wskazywaną dziedziną (każde 19 wskazań), to pozostałe obszary – takie jak szkolenia, testy penetracyjne, zarządzanie incydentami czy monitorowanie zagrożeń – również cieszyły się porównywalnym zainteresowaniem, z różnicami liczbowymi nieprzekraczającymi kilku wskazań. Może to świadczyć o równomiernym rozłożeniu zróżnicowania profilu działalności średnich firm w badanej grupie.

Respondenci następnie określili przedział rocznych dochodów ich przedsiębiorstw. Informacja ta pozwala lepiej zrozumieć profil finansowy badanych podmiotów.

Wykres 8. W jakim przedziale mieszczą się roczne dochody przedsiębiorstwa? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci zostali zapytani o roczne dochody swoich firm. Największa liczba firm zadeklarowała roczne dochody mieszczące się w przedziale 5–10 mln zł. Próg ten wskazały 64 małe oraz 10 średnich przedsiębiorstw.

Kolejną najczęściej wybieraną kategorią wśród małych firm był przedział 1–5 mln zł (44 wskazania), a następnie dochody do 1 mln zł (32 wskazania). W przypadku średnich przedsiębiorstw te przedziały były reprezentowane marginalnie – po jednym wskazaniu w każdej z tych kategorii.

Najwyższy przedział dochodów, czyli powyżej 10 mln zł, został wskazany przez 19 małych i aż 25 średnich firm, co sugeruje, że wśród średnich przedsiębiorstw biorących udział w badaniu dominują podmioty o relatywnie wysokich przychodach.

Brak odpowiedzi odnotowano jedynie w przypadku jednej małej firmy.

Wyniki te pokazują, że choć wśród małych firm występuje większe zróżnicowanie poziomu dochodów, to średnie przedsiębiorstwa w badanej grupie częściej osiągają przychody przekraczające 10 mln zł rocznie.

Branża MŚP działających w obszarze cyberbezpieczeństwa w Polsce jest niejednorodna i mocno zróżnicowana. Na rynku działa zarówno wiele podmiotów oferujących produkty ściśle związane z zapewnieniem bezpieczeństwa informacji i ochrony prywatności, firmy oferujące usługi związane m.in z audytami czy zapewnieniem zgodności z najbardziej aktualnymi aktami prawnymi, jak i firmy, które zajmują się integracją wielu rozwiązań w ramach jednego systemu informatycznego.

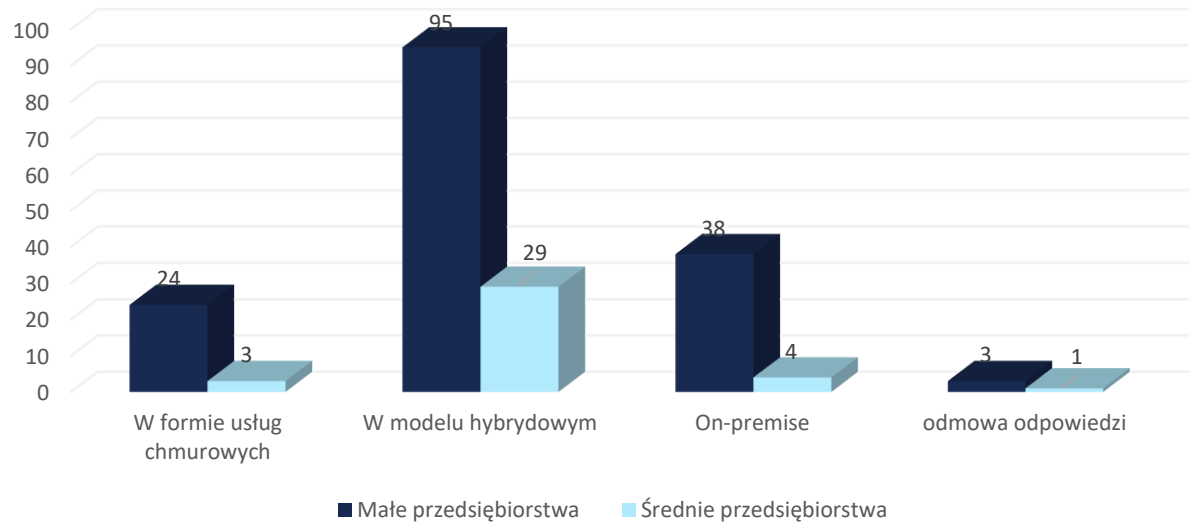
Dodatkowo, produkty i usługi cyberbezpieczeństwa często oferowane są przez firmy, w których cyberbezpieczeństwo nie jest działalnością dominującą a związaną m.in. z tworzeniem oprogramowania, budową środowisk chmury obliczeniowej czy hostingu.

1.4. Model biznesowy

Sposób oferowania produktów i usług, a także modele sprzedaży i współpracy w zakresie dystrybucji, odgrywają kluczową rolę w strategiach rozwoju przedsiębiorstw z sektora cyberbezpieczeństwa. Wraz z rosnącą popularyzacją rozwiązań chmurowych i zmianami w sposobach zakupu technologii przez klientów, firmy muszą elastycznie dostosowywać swoje podejście do oczekiwań rynku. Równocześnie, współpraca z partnerami handlowymi i dystrybucja rozwiązań innych krajowych producentów mogą stanowić ważny element budowania pozycji konkurencyjnej oraz wspierania ekosystemu innowacji. Poniższe wykresy prezentują najczęściej stosowane modele dostarczania produktów, korzystania z pośredników sprzedaży oraz współpracy z innymi polskimi firmami w zakresie oferowanych rozwiązań. Wyniki te pozwalają zidentyfikować dominujące podejścia rynkowe oraz potencjalne obszary dalszego rozwoju.

Poniższy wykres przedstawia preferowane modele oferowania produktów przez firmy z branży cyberbezpieczeństwa. Najczęściej stosowanym modelem jest podejście hybrydowe, łączące rozwiązania chmurowe i on-premise, co może świadczyć o elastycznym podejściu firm do potrzeb klientów.

Wykres 9. Czy oferują Państwo swoje produkty w formie usług chmurowych, on-premise, czy w modelu hybrydowym? (N=197)



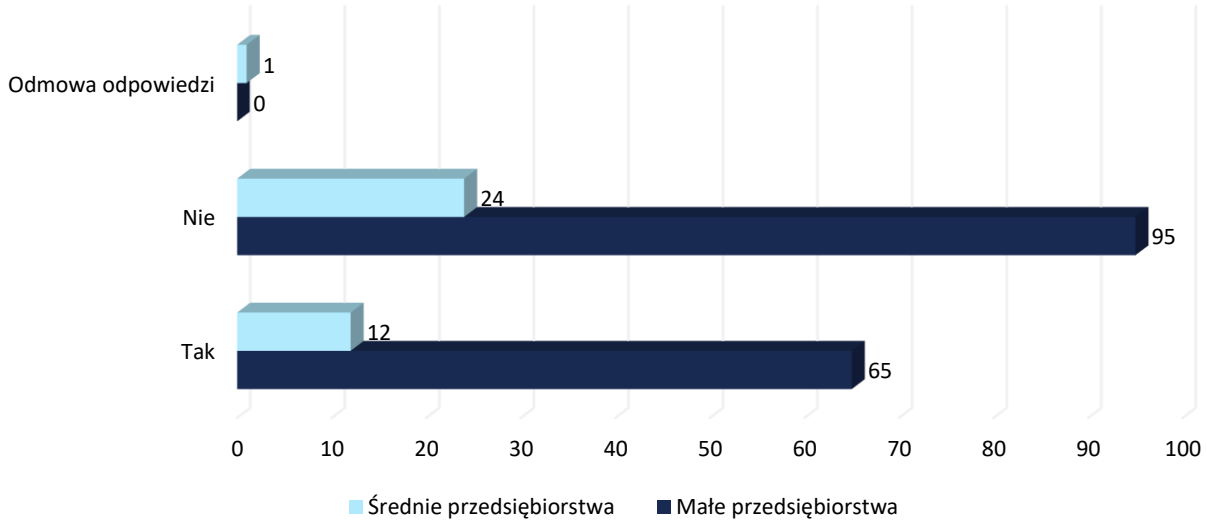
Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Najczęściej wskazywaną formą była oferta w modelu hybrydowym, łączącym rozwiązania lokalne i chmurowe. Taką odpowiedź zadeklarowało 95 małych oraz 29 średnich przedsiębiorstw.

Rozwiązania wyłącznie on-premise oferuje 38 małych i 4 średnie firmy, natomiast wyłącznie w formie usług chmurowych – 24 małe i 3 średnie przedsiębiorstwa.

Wyniki te pokazują, że rynek cyberbezpieczeństwa preferuje podejście mieszane, co odzwierciedla zróżnicowane potrzeby klientów i stopniową, ale niepełną adaptację usług chmurowych.

Wykres 10. Czy korzystają Państwo z pośredników sprzedaży, takich jak integratorzy, dystrybutorzy lub resellerzy? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

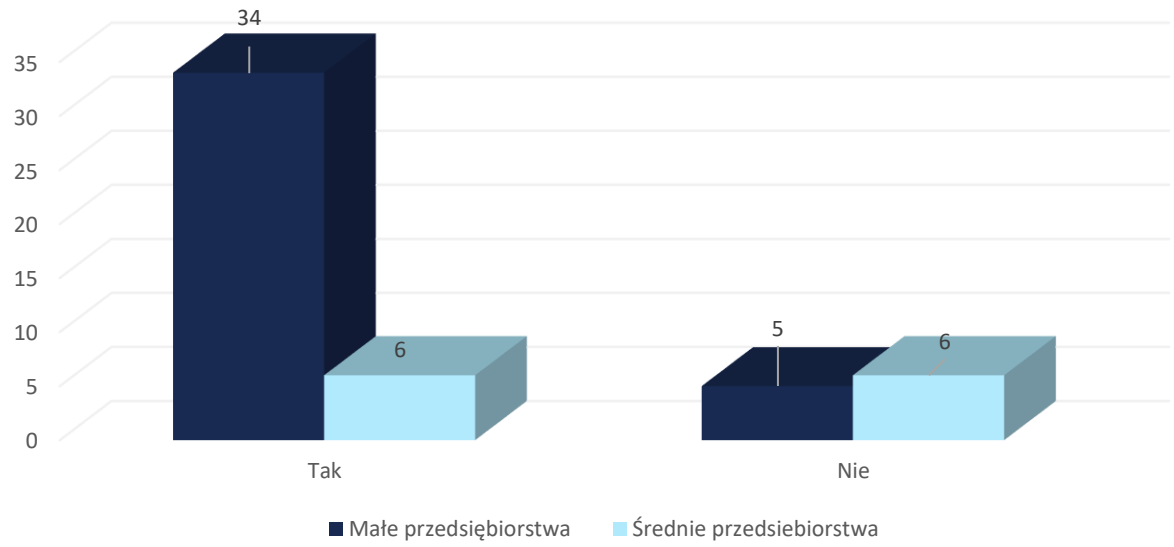
Większość firm – zarówno małych, jak i średnich – zadeklarowała, że nie korzysta z tego typu kanałów dystrybucji. Odpowiedź „nie" wskazało 95 małych oraz 24 średnie przedsiębiorstwa.

Z pośredników sprzedaży korzysta 65 małych i 12 średnich firm, co oznacza, że choć jest to mniej popularna forma dystrybucji, to nadal znajduje zastosowanie w istotnej części badanych podmiotów.

Wyniki te sugerują, że choć bezpośredni model sprzedaży dominuje, znaczna część firm korzysta z sieci partnerów handlowych, co może być związane z chęcią dotarcia do szerszego rynku, optymalizacją kosztów sprzedaży lub ograniczeniami zasobowymi. Model pośredni może również świadczyć o rozwiniętych strukturach dystrybucyjnych w sektorze cyberbezpieczeństwa.

Następnie zapytano respondentów czy oferują produkty/usługi/technologie innych krajowych przedsiębiorstw. Jak można zaobserwować z przedstawionych poniżej wyników, większość przedsiębiorców oferuje takie produkty.

Wykres 11. Czy oferują Państwo produkty/usługi/technologie innych krajowych przedsiębiorstw? (N=51)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Spośród 51 firm, które udzieliły odpowiedzi na to pytanie, większość zadeklarowała współpracę w zakresie dystrybucji lub integracji rozwiązań pochodzących od innych polskich podmiotów. Takie produkty oferuje 34 małych firm i 6 średnich firm. W sumie jest to 40 firm. Z kolei 11 firm (5 małych i 6 średnich) nie oferuje polskich produktów.

Wyniki te mogą sugerować, że większość przedsiębiorstw nie ogranicza się wyłącznie do rozwiązań zagranicznych, lecz aktywnie korzysta z dorobku krajowych firm, co może wspierać rozwój innowacji i zwiększać konkurencyjność całego sektora.

Rozdział 2

Potencjał krajowych MŚP w obszarze cyberbezpieczeństwa

2.1. Zasoby kadrowe i kompetencje (na podstawie ECSF)

W indywidualnych wywiadach pogłębionych uczestniczyły zarówno bardzo małe firmy, liczące od kilkunastu do kilkudziesięciu pracowników, jak i bardziej rozwinięte technologiczne spółki. Jak opisał to jeden z respondentów:

„[…] firma do dzisiejszego dnia zatrudnia kilkadziesiąt osób. Są to z reguły inżynierowie, wsparcie techniczne, osoby odpowiedzialne za nowe produkty, za rozwiązania […]" ~ powiedział Respondent 3.

Inna z firm, operująca na pograniczu MŚP, wskazała na zatrudnienie blisko stu osób, w tym współpracę z kadrą naukową:

„W tej chwili jest to około 80 osób zatrudnionych w ramach działalności spółki. Nie wszyscy są pracownikami na pełen etat, mamy też współpracę z naukowcami, z profesorami, doktorami habilitowanymi […]" ~ powiedział Respondent 15.

Wielu przedstawicieli firm zaznaczało, że tradycyjny model etatowy przestaje być dominującą formą zatrudnienia. W szczególności w małych i średnich firmach preferowane są elastyczne modele współpracy, oparte na umowach B2B, zadaniowości, zleceniu lub projektowym modelu rozliczeń.

„Jeżeli chodzi o zatrudnienie, nie mamy takiego klasycznego zatrudnienia etatowego […] wszystkie osoby, które z nami pracują, to są osoby sprawdzone i pracujące bardzo długo [...]" ~ powiedział Respondent 7.

Większość firm uczestniczących w badaniu deklarowała stosowanie zróżnicowanych form zatrudnienia i współpracy, co wpisuje się w coraz powszechniejszy trend elastycznego podejścia do zarządzania zasobami ludzkimi. Obok tradycyjnych umów o pracę coraz częściej funkcjonują umowy B2B, współpraca na podstawie kontraktów cywilnoprawnych, praca zadaniowa czy model projektowy. Takie zróżnicowanie umożliwia organizacjom szybkie dostosowanie struktury zatrudnienia do bieżących potrzeb operacyjnych oraz lepszą kontrolę nad kosztami personalnymi. Firmy mogą w ten sposób zwiększać lub zmniejszać liczbę współpracowników w zależności od natężenia prac, unikając jednocześnie długoterminowych zobowiązań kadrowych.

W praktyce przekłada się to na istotne różnice między liczbą pracowników zatrudnionych na stałe, a całkowitą liczbą osób faktycznie zaangażowanych w realizację projektów i bieżącą działalność operacyjną. Jak wynika z wypowiedzi respondentów, podstawowy zespół etatowy w niektórych firmach liczy zaledwie kilkanaście osób, natomiast w okresach intensywnej pracy – na przykład przy realizacji dużych projektów – liczba współpracowników może wzrosnąć nawet dwukrotnie.

„W tym momencie zatrudniamy na umowę o pracę około 12 osób, natomiast również zatrudniamy osoby na B2B" ~ powiedział Respondent 1.

Takie podejście jest w pełni uzasadnione specyfiką branży, która często charakteryzuje się wysokim stopniem specjalizacji oraz dużą dynamiką i nieprzewidywalnością zleceń – zarówno ze strony klientów prywatnych, jak i instytucji publicznych. Różnorodność wymagań projektowych oraz zmienność ich harmonogramów wymuszają na firmach elastyczność i zdolność do szybkiego reagowania. Tym samym przyjęcie elastycznego modelu zatrudnienia nie tylko wspiera efektywność operacyjną, ale też stanowi wyraz dojrzałości organizacyjnej – świadczy o strategicznym podejściu do zarządzania kapitałem ludzkim w kontekście optymalizacji procesów i maksymalizacji efektywności biznesowej.

Skala zatrudnienia zależy od fazy rozwoju firmy i profilu działalności

Większe organizacje, obsługujące zarówno rynek krajowy, jak i zagraniczny, z reguły dysponują szerszym portfolio projektów i usług, co znajduje odzwierciedlenie w znacznie większej liczbie współpracowników – od 60 do nawet 100 osób. Warto zaznaczyć, że w tych przypadkach liczba ta obejmuje nie tylko etatowych pracowników, ale również osoby zatrudnione w modelu B2B oraz ekspertów zewnętrznych, w tym przedstawicieli środowisk naukowych.

„W tej chwili jest to około 80 osób zatrudnionych w ramach działalności spółki. Nie wszyscy są pracownikami na pełen etat […] ” ~ powiedział Respondent 15.

Coraz większe znaczenie zyskuje współpraca z uczelniami wyższymi, jednostkami badawczymi oraz niezależnymi ekspertami akademickimi. Firmy rozwijają te relacje w formie doradztwa eksperckiego, szczególnie w projektach badawczo-rozwojowych (R&D), a także w procesach związanych z certyfikacją produktów i analizą zagrożeń na poziomie systemowym. Współpraca ta wnosi do organizacji aktualną wiedzę naukową, wspiera innowacje oraz wzmacnia pozycję firm jako kompetentnych partnerów dla instytucji publicznych i międzynarodowych.

Kompetencje zespołów pracowniczych są zazwyczaj oceniane bardzo wysoko – zwłaszcza tam, gdzie zespoły rozwijane były organicznie, na drodze wieloletniej, świadomej budowy zasobów ludzkich. Firmy, które postawiły na długofalowe relacje z pracownikami oraz zainwestowały w wewnętrzne inicjatywy edukacyjne (np. akademie cyberbezpieczeństwa), podkreślają silne więzi wewnętrzne, wysoki poziom zaufania do kompetencji zespołu oraz zgodność wartości i kultury pracy.

„od kilku lat, mamy stały zespół i tak naprawdę nie mamy czasu jakiejś aktywne rekrutacje w tym zakresie, więc nie mogę tu powiedzieć, co się dzieje na rynku, ponieważ mamy ten stały zespół, który z nami jest i on tutaj jakby spełnia swoje zadania” ~ powiedział Respondent 1.

Dodatkowo wiele firm wdraża programy rozwojowe, które pełnią funkcję pomostu między środowiskiem akademickim a rynkiem pracy. Akademie wewnętrzne czy specjalistyczne kursy dla studentów i młodych profesjonalistów mają na celu przygotowanie przyszłych specjalistów do realiów pracy w branży, z uwzględnieniem jej specyfiki i aktualnych potrzeb.

„Prowadzimy Akademię od 10 lat […]. Akademia była takim elementem też zaproszenia do współpracy z nami potencjalnych studentów, którzy byli zainteresowani branżą cyber security.” ~ powiedział Respondent 3.

Akademie pełnią więc podwójną funkcję: z jednej strony dostarczają firmom lepiej przygotowanych kandydatów, z drugiej – wzmacniają wizerunek organizacji jako podmiotu zaangażowanego w rozwój rynku i wspierającego edukację. Część firm oferuje uczestnikom takich programów opiekę mentorską, dostęp do realnych projektów oraz możliwość zdobycia pierwszego doświadczenia zawodowego pod okiem ekspertów.

Mimo pozytywnej oceny istniejących zespołów i działań rozwojowych, respondenci wskazują na istotny i coraz bardziej odczuwalny problem – systemowy niedobór wykwalifikowanych specjalistów w obszarze cyberbezpieczeństwa. Braki kadrowe są zauważalne nie tylko w skali krajowej, ale również na poziomie europejskim i dotyczą w szczególności najbardziej zaawansowanych ról – takich jak architekci bezpieczeństwa, eksperci ds. strategii czy osoby łączące wysokie kompetencje techniczne z umiejętnościami sprzedażowymi, zarządczymi lub komunikacyjnymi.

Wyzwania rekrutacyjne i braki kadrowe

Większość respondentów deklarowała brak istotnych problemów rekrutacyjnych w ostatnim roku. Wskazywano na skuteczność działań wewnętrznych, silne zespoły zbudowane w przeszłości oraz współpracę z uczelniami jako sposób pozyskiwania młodych talentów. Jednak nawet w tych przypadkach zwracano uwagę na trudności z pozyskaniem specjalistów do ról łączących różne kompetencje – np. techniczne i strategiczne.

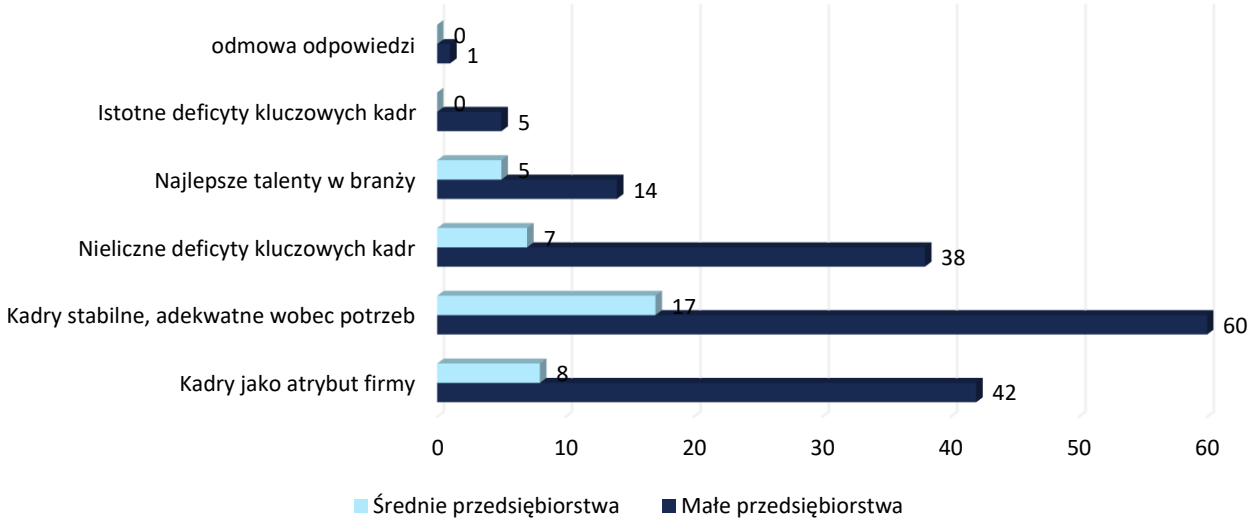
„W tej chwili nie mamy takich problemów. Nie mieliśmy dotąd takich problemów. My tutaj też mocno współpracujemy z uczelniami. Realizujemy różnego rodzaju projekty też studenckie. To też jest dobry sposób na poznanie osób, które gdzieś tam są bardziej może ambitne, zdolne i chętne do realizacji też trudniejszych projektów” ~ powiedział Respondent 15.

„[…] Kiedyś, czyli na przykład 3 czy 4 lata temu rekrutacja była dużym wyzwaniem, dlatego, że to był moment jeszcze po pandemii czy też w pandemii i po pandemii. […] Dzisiaj ostatnią rekrutację, którą robiliśmy 2 miesiące temu, nie mieliśmy możliwości przejrzenia tych wszystkich CV […] ~ powiedział Respondent 9.

Aktualna sytuacja rekrutacyjna w wielu organizacjach jest stabilna, to trudności z pozyskaniem specjalistów o profilach łączących kompetencje techniczne i strategiczne mogą stanowić istotne wyzwanie w kontekście dalszego rozwoju i specjalizacji zespołów.

Zasoby ludzkie stanowią jeden z kluczowych czynników warunkujących skuteczność działań w obszarze cyberbezpieczeństwa. Dlatego respondentów zapytano o subiektywną ocenę potencjału merytorycznego ich kadry. Odpowiedzi pozwalają określić, na ile firmy postrzegają swoje zespoły jako wystarczająco przygotowane do wyzwań stojących przed branżą.

Wykres 12. Jak oceniają Państwo potencjał merytoryczny swojej kadry? (N=197)

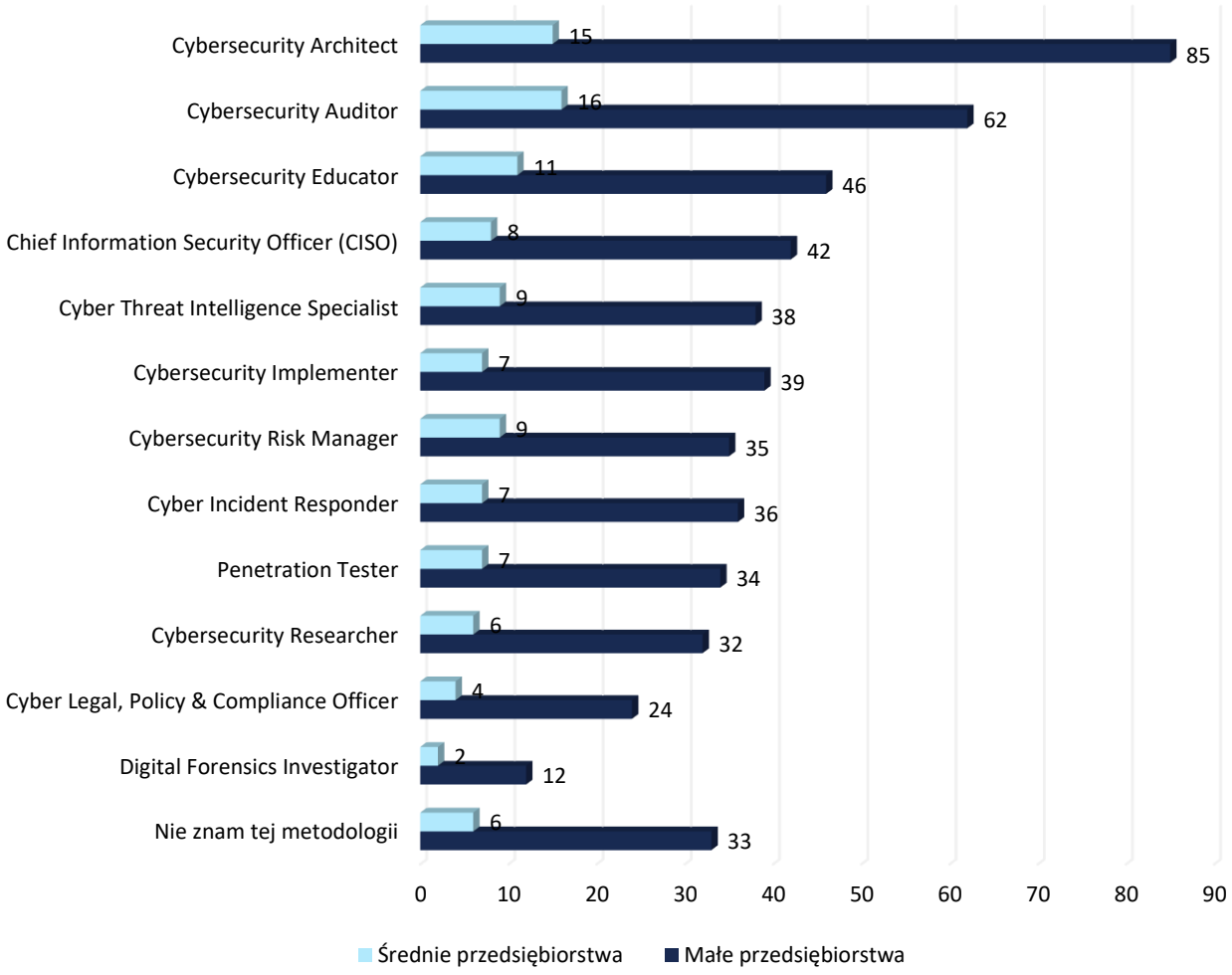


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci w większości pozytywnie oceniają potencjał merytoryczny swojej kadry. Najczęściej wybieraną odpowiedzią była ocena „kadry stabilne, adekwatne wobec potrzeb", którą wskazało 60 małych oraz 17 średnich firm. Znacząca liczba respondentów uznała również, że kadry stanowią istotny atut firmy – tę opinię wyraziły 42 małe i 8 średnich przedsiębiorstw. Nieco mniej licznie reprezentowana była odpowiedź „nieliczne deficyty kluczowych kadr" (38 małych i 7 średnich firm), co może wskazywać na pewne, choć ograniczone, trudności w pozyskaniu specjalistów. Najwyższą ocenę – „najlepsze talenty w branży" – zadeklarowało 14 małych i 5 średnich firm, co sugeruje, że tylko część badanych postrzega swoją kadrę jako wyróżniającą się na tle konkurencji.

Wyniki te pokazują, że zdecydowana większość respondentów postrzega swoje zespoły jako wystarczająco kompetentne i dopasowane do potrzeb działalności.

Wykres 13. Jakie role wymienione w Europejskiej Ramie Umiejętności w zakresie Cyberbezpieczeństwa (ECSF) występują w Pana/Pani firmie? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Wśród respondentów badania najczęściej występującą rolą w firmie, którą reprezentują, zgodnie z Europejską Ramą Umiejętności w zakresie Cyberbezpieczeństwa (ECSF), był Cybersecurity Architect. Obecność tej roli zadeklarowało 85 małych oraz 15 średnich firm.

Kolejne najczęściej wskazywane role to: Cybersecurity Auditor (62 małe i 16 średnich firm), Cybersecurity Educator (46 małych i 11 średnich), a także Chief Information Security Officer (CISO) (42 małe i 8 średnich firm). W dalszej kolejności pojawiały się takie funkcje jak: Cyber Threat Intelligence Specialist, Cybersecurity Implementer, Cybersecurity Risk Manager, Cyber Incident Responder oraz Penetration Tester – każda z nich została wskazana przez od 34 do 39 małych firm oraz od 7 do 9 średnich.

Rzadziej występującymi rolami były: Cybersecurity Researcher (32 małe i 6 średnich firm), Cyber Legal, Policy & Compliance Officer (24 małe i 4 średnie), a także Digital Forensics Investigator, obecny jedynie w 12 małych i 2 średnich przedsiębiorstwach.

Jednocześnie 39 firm (33 małych i 6 średnich) zadeklarowało brak znajomości metodologii ECSF, co może świadczyć o jej rosnącej rozpoznawalności wśród podmiotów z branży.

Wyniki te pokazują, że w badanych firmach najczęściej występują role techniczne, a także te dotyczące tworzenia architektury bezpieczeństwa, natomiast funkcje związane z analizą prawną, zgodnością czy informatyką śledczą są reprezentowane w mniejszym stopniu.

Największe wyzwania dotyczą ról interdyscyplinarnych: liderów techniczno-biznesowych, architektów, osób z kompetencjami sprzedażowymi

W firmach, które napotkały trudności rekrutacyjne, szczególnie często wskazywano na brak dostępnych kandydatów do tzw. ról hybrydowych – czyli stanowisk wymagających zarówno głębokich kompetencji technicznych, jak i zdolności komunikacyjnych, strategicznych oraz biznesowych. Przykładami takich ról są:

- architekci systemów bezpieczeństwa,
- liderzy pre-sales i konsultanci sprzedażowi,
- eksperci ds. integracji technologii z procesami biznesowymi,
- osoby umiejące tłumaczyć język technologii na język wartości biznesowej.

To właśnie te stanowiska stały się szczególnie istotne w kontekście transformacji cyfrowej i rosnącego znaczenia bezpieczeństwa informacji jako elementu przewagi konkurencyjnej. Organizacje, które chcą skutecznie wdrażać złożone rozwiązania IT i zarządzać nimi w sposób zintegrowany z celami biznesowymi, potrzebują pracowników o kompetencjach przekrojowych – zdolnych do prowadzenia dialogu zarówno z inżynierami, jak i decydentami po stronie klienta.

> *„[…] my szukamy konkretnych osób, które już rynek trochę zweryfikował […]. Są świetni specjaliści w różnych dziedzinach […], tylko my potrzebujemy tych bardziej uniwersalnych, o bardziej tych artysty, architektach albo osoby, które potrafią zaprojektować proces, dostarczyć dokumentacje" ~ powiedział Respondent 7.*

> *„[…] wcale nie jest łatwo znaleźć osoby o dużej wiedzy biznesowej z tego obszaru IT. Mówię tu o liderach z zakresu sprzedaży właśnie rozwoju biznesu czy eksportu, marketingu, czy pre-sales, czyli osób, które potrafią rozmawiać biznesowo o technologiach" ~ powiedział Respondent 13.*

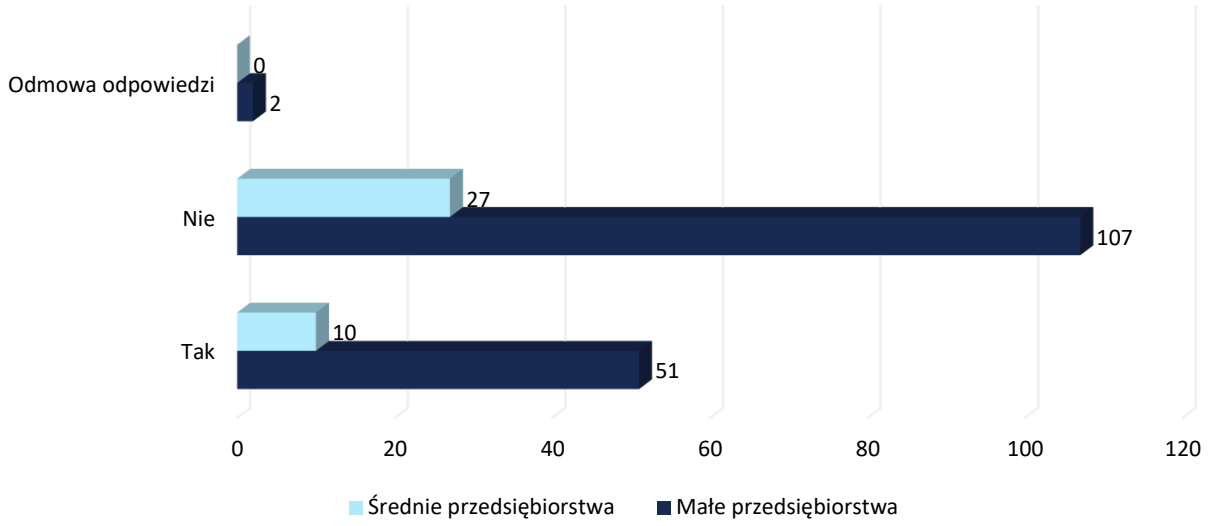
Tego rodzaju konkurencja o talenty sprawia, że mniejsze organizacje – mimo często ciekawszego środowiska pracy i większej elastyczności – mają ograniczone możliwości w przyciąganiu i utrzymywaniu specjalistów. W dłuższej perspektywie może to pogłębiać nierównowagi na rynku pracy i utrudniać budowanie zrównoważonego ekosystemu kompetencji w sektorze.

Część firm podkreślała, że największe problemy dotyczą nie zespołów R&D czy inżynierów, ale stanowisk „bliżej rynku" – w tym specjalistów sprzedaży technologii i komunikacji z klientem końcowym. Wskazywano tu na wysoki poziom rotacji, trudności z utrzymaniem motywacji i brak kandydatów rozumiejących zarówno produkt, jak i potrzeby biznesowe odbiorców.

> *„[…] wcale nie jest łatwo znaleźć osoby o dużej wiedzy biznesowej z tego obszaru IT. Mówię tu o liderach z zakresu sprzedaży, właśnie rozwoju biznesu czy eksportu, marketingu, czy pre-sales, czyli osób, które potrafią rozmawiać biznesowo o technologiach" ~ powiedział Respondent 13.*

Dostęp do odpowiednio wykwalifikowanej kadry to jeden z kluczowych czynników warunkujących rozwój przedsiębiorstw w sektorze cyberbezpieczeństwa. W związku z tym respondentów zapytano, czy w ostatnich 12 miesiącach napotykali trudności w zatrudnianiu specjalistów o wymaganych kompetencjach.

Wykres 14. Czy w ostatnim roku napotykali Państwo trudności w zatrudnieniu odpowiednio wykwalifikowanych pracowników? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Wśród respondentów badania większość firm nie napotkała w ostatnim roku trudności w zatrudnieniu odpowiednio wykwalifikowanych pracowników. Brak takich problemów zadeklarowało 107 małych oraz 27 średnich przedsiębiorstw.

Trudności w rekrutacji odpowiednich specjalistów zgłosiło natomiast 51 małych i 10 średnich firm. Choć stanowią one mniejszość, wyniki te wskazują, że wyzwania kadrowe są obecne w części badanych podmiotów, szczególnie wśród małych firm.

W kontekście rosnącego znaczenia bezpieczeństwa cyfrowego, ten wynik może być sygnałem dla instytucji edukacyjnych, podmiotów szkoleniowych oraz decydentów polityki rynku pracy.

Rozproszenie wiedzy i specjalizacji utrudnia pełną ocenę kompetencji

Cyberbezpieczeństwo, choć często traktowane z zewnątrz jako jednolity obszar kompetencyjny, w rzeczywistości stanowi wysoce zróżnicowaną i rozproszoną dziedzinę wiedzy, obejmującą szeroki wachlarz specjalizacji – od aspektów technologicznych i infrastrukturalnych, przez procesy organizacyjne, po zarządzanie ryzykiem, audyt, compliance i komunikację kryzysową.

Respondenci badania byli zgodni, że oczekiwanie tzw. „ogólno-cyberbezpieczeństwowych" kompetencji – czyli sytuacji, w której jeden specjalista zna się na wszystkim – jest nierealistyczne i nieadekwatne do rzeczywistości rynkowej. Każdy ekspert rozwija swoją wiedzę w wybranym segmencie, nierzadko wąsko wyspecjalizowanym, co wynika zarówno z rosnącej złożoności technologii, jak i z tempa zmian w otoczeniu prawnym i operacyjnym.

> *„[...] cyberbezpieczeństwa też jest taką dziedziną bardzo mocno rozproszoną i to nie jest tak, że jak ktoś mówi znam się na cyberbezpieczeństwie, to znaczy, że się będzie znał na wszystkim tak, po prostu każdy ma jakąś swoją dziedzinę" ~ powiedział Respondent 8.*

Respondenci byli zgodni co do faktu, że choć obecna sytuacja rekrutacyjna jest w wielu firmach stabilna, to rynek jako całość wciąż zmaga się z deficytem wykwalifikowanej kadry w wybranych obszarach. Obraz rynku pracy jest zróżnicowany – część firm nie odnotowała trudności w zatrudnieniu, inne wskazywały konkretne problemy związane z pozyskiwaniem specjalistów zarówno technicznych, jak i sprzedażowo-biznesowych.

Różnorodność zespołów - płeć, wiek, niepełnosprawność

Choć temat różnorodności płci i inkluzywności nie był dominującym wątkiem w wypowiedziach respondentów, pojawił się jako ważny sygnał świadczący o dojrzewaniu kultury organizacyjnej w części firm sektora cyberbezpieczeństwa. W kilku przypadkach respondenci świadomie odnosili się do kwestii reprezentacji kobiet w strukturach swoich zespołów, podkreślając potrzebę budowania środowiska pracy opartego na otwartości, równych szansach i świadomym zarządzaniu różnorodnością.

„Natomiast w moim zespole ja zatrudniałam 25 osób, tylko to już były osoby pode mną i miałam diversity prawie 50%" ~ powiedział Respondent 8.

Tak wysoki poziom zróżnicowania płciowego w zespole technologicznym – szczególnie w branży postrzeganej jako tradycyjnie zdominowana przez mężczyzn – stanowi godny uwagi przykład dobrej praktyki. Świadczy o tym, że inkluzywność może być realnie wdrażana w działaniu, a nie tylko deklarowana w dokumentach HR-owych. Przykłady te wskazują, że przy odpowiednim podejściu możliwe jest tworzenie przestrzeni, w której kompetencje, a nie płeć, decydują o przydziale zadań i awansach.

Pomimo pojedynczych pozytywnych przykładów, przeciętny udział kobiet w strukturach organizacyjnych firm technologicznych wciąż oscyluje wokół 20–40%, przy czym największe ich skupienie przypada na działy wspierające: sprzedaż, marketing, komunikację oraz relacje z klientami. W tych obszarach kobiety nie tylko są bardziej widoczne, ale też częściej pełnią funkcje koordynacyjne i kierownicze.

„To i tak trochę się podzieliło, że w developmencie nie ma żadnej kobiety w tej części sprzedażowej. Za rynek Polski (imię), mamy (imię) w dziale marketingu, a ponieważ w ogóle jest nas mało, to można powiedzieć, że się siły rozkładają, jeżeli chodzi o tę część reprezentacyjną, taką biznesową." ~ powiedział Respondent 2.

Znacznie rzadziej kobiety występują w zespołach stricte inżynieryjnych, developerskich lub analitycznych – a jeśli już, to najczęściej na stanowiskach niższego i średniego szczebla. Ten stan rzeczy nie wynika z braku kompetencji, lecz z szeregu utrwalonych barier kulturowych, braku odpowiednich wzorców i systemowych niedociągnięć w procesie kształcenia i rekrutacji.

Mimo że kobiety nadal stanowią mniejszość w działach technicznych firm z sektora cyberbezpieczeństwa, pojawiają się coraz wyraźniejsze przykłady ich obecności na stanowiskach kierowniczych, architektonicznych i eksperckich. Z wypowiedzi respondentów wynika, że choć zespoły developerskie i inżynieryjne wciąż są zdominowane przez mężczyzn, w niektórych organizacjach kobiety osiągają istotną reprezentację w strukturach wyższego szczebla – zwłaszcza tam, gdzie o awansie decydują rzeczywiste kompetencje i doświadczenie, a nie schematyczne wyobrażenia o „typowym inżynierze".

„To jest ciekawe, bo właśnie przez lata zauważyliśmy taki trend, u nas jest dość sporo kobiet. […] Struktura tych wyższych stanowisk, takich architektów, czy też takich liderów usług, to są przeważnie kobiety, […]." ~ powiedział Respondent 7.

To ważne sygnały – świadczące o tym, że realne kompetencje mogą skutecznie przełamywać stereotypy płciowe, a kobiety są w stanie z sukcesem funkcjonować w rolach wymagających zarówno zaawansowanej wiedzy technicznej, jak i zdolności zarządczych. Takie przypadki przeczą przekonaniu, że kobiety „naturalnie" lepiej odnajdują się w funkcjach wspierających (np. HR, marketing) niż w twardych domenach inżynierskich.

Z wypowiedzi respondentów jasno wynika, że udział kobiet w zespołach firm z sektora cyberbezpieczeństwa w dużej mierze zależy od specyfiki danej organizacji, jej modelu działania oraz lokalnego rynku rekrutacyjnego. Większość firm deklaruje podejście neutralne pod względem płci – podkreślając, że w procesach rekrutacyjnych kluczowym kryterium są kompetencje kandydatów, a nie ich płeć.

„Tak, pracują u nas kobiety, ale niestety jest to dość niski procent. (…) Widocznie w rekrutacjach głównie mężczyźni się zgłaszali i takie decyzje były podejmowane. Kierujemy się przede wszystkim kompetencjami danej osoby, która się zgłasza" ~ powiedział Respondent 10.

Jednak pomimo tej deklarowanej neutralności, w praktyce większość zespołów technicznych pozostaje silnie zmaskulinizowana. Przewaga mężczyzn nie wynika z jawnej dyskryminacji czy świadomego wykluczania kobiet, ale z faktu, że kobiety rzadziej aplikują na stanowiska techniczne, zwłaszcza w obszarach takich jak rozwój oprogramowania, inżynieria systemowa czy bezpieczeństwo operacyjne.

Mimo że udział kobiet w zespołach technicznych w wielu firmach pozostaje niski, większość badanych organizacji deklaruje świadomość potrzeby wspierania różnorodności oraz zgodność z formalnymi wymaganiami w zakresie równouprawnienia. W szczególności dotyczy to firm uczestniczących w projektach unijnych, gdzie obowiązują określone standardy w obszarze polityk równościowych, dostępności i przeciwdziałania dyskryminacji. Zespoły często działają w trybie zdalnym lub hybrydowym, co z założenia ogranicza bariery związane z lokalizacją, mobilnością czy elastycznością czasu pracy.

„Generalnie realizując każdy projekt unijny, my musimy spełniać wszystkie dyrektywy dotyczące równouprawnienia w zakresie […] płci, czy w zakresie niepełnosprawności, czy nawet sterowania obszarów wiejskich, to są te elementy i my spełniamy te kryteria w 100%" ~ powiedział Respondent 3.

W wielu firmach kobiety pełnią różnorodne funkcje – od operacyjnych po specjalistyczne i techniczne – co potwierdza, że formalnych ograniczeń dotyczących ról zawodowych nie ma, a w strukturach istnieją realne możliwości rozwoju zawodowego niezależnie od płci.

Wysoka rozpiętość wiekowa – ale niekoniecznie z udziałem najstarszych grup

Z przeprowadzonych wywiadów jednoznacznie wynika, że osoby powyżej 65. roku życia są praktycznie nieobecne w strukturach firm działających w sektorze cyberbezpieczeństwa. W żadnym z badanych przypadków nie wskazano aktywnego zatrudnienia specjalistów z tej grupy wiekowej na stanowiskach technicznych, operacyjnych czy menedżerskich. Nawet tam, gdzie deklarowano współpracę z seniorami w przeszłości, dotyczyło to głównie obszarów wspierających – takich jak księgowość, kadry, administracja czy doradztwo okazjonalne.

Branża pozostaje wyraźnie sfokusowana na pokolenia aktywne zawodowo (25–55 lat), a osoby zbliżające się do wieku emerytalnego – nawet jeśli posiadają istotne doświadczenie i wiedzę – nie są traktowane jako realna grupa docelowa w działaniach rekrutacyjnych czy rozwojowych. Najstarsze osoby w zespołach to zwykle pracownicy ok. 60. roku życia, często pełniący funkcje doradcze lub nadzorujące, jednak bez kontynuacji po przekroczeniu progu 65+.

„Jest to zespół w bardzo różnym wieku, w bardzo różnym rozstrzale. Sądzę, że można powiedzieć, że ten rozstrzał jest ponad 30 – letni pomiędzy pracownikami […]" – powiedział Respondent 8.

Można to interpretować jako przejaw niewykorzystanego potencjału eksperckiego – szczególnie w obszarach takich jak mentoring, audyt bezpieczeństwa, analiza ryzyk systemowych czy dokumentacja projektowa. W dobie niedoboru specjalistów i wysokiego zapotrzebowania na wiedzę instytucjonalną, aktywizacja zawodowa doświadczonych profesjonalistów mogłaby stanowić istotne uzupełnienie zasobów kadrowych – jednak obecnie nie jest to w praktyce realizowane.

Brak obecności pracowników 65+ w zespołach technicznych wynika więc przede wszystkim z dynamiki i charakteru sektora. Szybkość rozwoju technologii sprawia, że doświadczenie zawodowe, choć cenne, często musi ustępować miejsca biegłości w nowych narzędziach, językach programowania czy metodykach pracy. Mimo braku formalnych barier, starsi specjaliści mogą napotykać trudności w utrzymaniu tempa rozwoju kompetencji wymaganych na stanowiskach stricte operacyjnych.

Zupełnie marginalna pozostaje natomiast obecność osób z niepełnosprawnościami w firmach z sektora cyberbezpieczeństwa. W przeważającej liczbie przypadków badane organizacje nie zatrudniają obecnie takich pracowników. Część respondentów przyznała, że w przeszłości zdarzały się pojedyncze przypadki zatrudnienia osób z niepełnosprawnościami, jednak nie miały one charakteru systemowego i najczęściej były incydentalne. Jedynie jeden respondent zadeklarował aktualną współpracę z osobą z niepełnosprawnością w obszarze technicznym:

„[…] mamy niepełnosprawną w tym obszarze developmentu" ~ powiedział Respondent 2.

Zebrane dane sugerują, że zatrudnienie osób z niepełnosprawnościami w sektorze cyberbezpieczeństwa nie stanowi elementu świadomie prowadzonej polityki różnorodności czy inkluzywności. Mimo że część firm deklaruje doświadczenia w tym zakresie, brakuje instytucjonalnych mechanizmów, które mogłyby wspierać trwałe włączenie tej grupy pracowników w struktury organizacyjne. Szczególnie niewykorzystany pozostaje potencjał pracy zdalnej i zadaniowej, która w naturalny sposób mogłaby otworzyć przestrzeń dla osób z ograniczeniami mobilności czy potrzebą elastycznego środowiska pracy. Brak takich rozwiązań oznacza, że możliwości aktywizacji zawodowej osób z niepełnosprawnościami – mimo deklaratywnej otwartości niektórych firm – pozostają w dużej mierze niewykorzystane.

Respondenci często wskazywali, że charakter zadań realizowanych w firmach – obejmujący konieczność wyjazdów służbowych, pracy w terenie, elastyczności czasowej oraz fizycznej obecności u klienta – może stanowić istotną barierę w zatrudnianiu osób z niepełnosprawnościami, zwłaszcza w przypadku znacznych ograniczeń ruchowych czy zdrowotnych. Zwracano uwagę, że wiele projektów wymaga wysokiego poziomu mobilności oraz bezpośredniego zaangażowania na miejscu realizacji działań, co może utrudniać włączenie pracowników o szczególnych potrzebach.

„[…] zastanawialiśmy się z tej perspektywy. Może dlatego, że te projekty znowu wymagają dużej aktywności, czasem też fizycznej, pojechania do klienta i te takie disabilities" ~ powiedział Respondent 7.

Wypowiedzi te uwidaczniają jedno z kluczowych wyzwań związanych z inkluzywnością w sektorze – trudność w dopasowaniu specyfiki pracy projektowej do zróżnicowanych możliwości funkcjonalnych kandydatów. W firmach działających w modelu zadaniowym, opartym na dużej dynamice działań i wymagającym gotowości do szybkiego reagowania, pojawia się obawa, że zatrudnienie osoby z ograniczeniami fizycznymi może wiązać się z koniecznością reorganizacji pracy lub obniżeniem tempa i jakości realizacji zadań.

Znaczenie kapitału ludzkiego i kompetencji

Na koniec warto zaznaczyć, że nawet najlepsze rozwiązania technologiczne nie będą miały szansy się rozwinąć, jeśli nie zadbamy o odpowiednie kompetencje. Wielu respondentów zwracało uwagę, że największym wyzwaniem nie są same technologie, lecz brak ludzi zdolnych je rozwijać, wdrażać i utrzymywać. Stąd potrzeba inwestycji w edukację, popularyzację cyberbezpieczeństwa i tworzenie klarownych ścieżek kariery.

„Uważam, że kompetencje odnośnie cyberbezpieczeństwa zawsze mogą być zwiększone. […] myślę poziom tej wiedzy naszych pracowników wzrósł" ~ powiedział Respondent 10.

Wnioski te jednoznacznie wskazują, że rozwój sektora cyberbezpieczeństwa wymaga równoległego wzmacniania zaplecza kadrowego – zarówno na poziomie technicznym, jak i strategicznym. Bez inwestycji w kompetencje, ludzki potencjał innowacyjny pozostanie niewykorzystany, a firmy nie będą w stanie sprostać rosnącemu zapotrzebowaniu rynku. Kluczowe staje się więc stworzenie spójnego systemu kształcenia, rozwoju zawodowego i upowszechniania wiedzy, który umożliwi skuteczne odpowiadanie na dynamiczne potrzeby branży.

Podsumowanie:

Analiza struktury zatrudnienia i wyzwań kadrowych w sektorze cyberbezpieczeństwa ujawnia złożony i zróżnicowany obraz funkcjonowania firm operujących w tej branży. Przedsiębiorstwa wykazują dużą elastyczność organizacyjną, dostosowując modele współpracy do zmiennych warunków rynkowych i projektowych. Powszechnie stosowane są hybrydowe formy zatrudnienia, łączące etaty z kontraktami B2B i współpracą zadaniową, co pozwala efektywnie zarządzać zasobami ludzkimi i ryzykiem kosztowym.

Skala zatrudnienia pozostaje silnie uzależniona od specjalizacji i etapu rozwoju firmy – od kilku do ponad stu współpracowników – przy czym nawet większe organizacje często opierają się na rozbudowanej sieci ekspertów zewnętrznych oraz współpracy z uczelniami i środowiskiem naukowym. Stabilne zespoły, budowane w oparciu

o długoterminową współpracę, są postrzegane jako kluczowy atut – szczególnie w kontekście lojalności, dopasowania kulturowego i wysokiej oceny kompetencji.

Jednocześnie, mimo lokalnej stabilności w części firm, rynek jako całość mierzy się z narastającym niedoborem wysoko wykwalifikowanych specjalistów. W szczególności dotyczy to ról o charakterze przekrojowym – takich jak architekci systemów, liderzy pre-sales czy eksperci łączący wiedzę techniczną z kompetencjami strategicznymi i sprzedażowymi. Trudności rekrutacyjne są pogłębiane przez silną konkurencję ze strony dużych korporacji i centrów technologicznych, oferujących wyższe wynagrodzenia i szersze możliwości rozwoju.

Wskazano także na lukę kompetencyjną w obszarach wspierających, takich jak marketing i sprzedaż rozwiązań z zakresu cyberbezpieczeństwa. Firmom trudno jest znaleźć osoby, które potrafią skutecznie komunikować wartość usług technologicznych i tłumaczyć je na język biznesu.

Na tle powyższych wyzwań, kwestie różnorodności płciowej, wiekowej i dostępności dla osób z niepełnosprawnościami pozostają w dużej mierze nierozwiązane. Choć zauważalna jest rosnąca świadomość w zakresie różnorodności i równości szans, działania w tym obszarze mają głównie charakter deklaratywny. Udział kobiet w zespołach technicznych nadal jest niski, a osoby 65+ i osoby z niepełnosprawnościami są w strukturach organizacyjnych obecne sporadycznie, najczęściej w rolach administracyjnych lub wspierających. Firmy rzadko prowadzą systemowe działania sprzyjające inkluzywności – brak kampanii rekrutacyjnych, dostosowanych stanowisk pracy czy polityk DEI.

Podsumowując, sektor cyberbezpieczeństwa cechuje się wysoką adaptacyjnością i świadomością organizacyjną, ale stoi przed wyzwaniami o charakterze strukturalnym i systemowym. Rozwój nowoczesnej, odpornej kadrowo branży wymaga nie tylko wzmacniania kompetencji technicznych, ale także inwestycji w rozwój kompetencji miękkich, polityki różnorodności i inkluzywności oraz partnerskiej współpracy z sektorem edukacji.

2.2. Potencjał technologiczny i infrastrukturalny

Sektor cyberbezpieczeństwa w Polsce dynamicznie się rozwija, a jego kształtowanie determinują zarówno nowe technologie, jak i czynniki geopolityczne. Na podstawie przeprowadzonego badania jakościowego i ilościowego wskazano najważniejsze trendy i potrzeby, które będą wpływać na branżę w najbliższych latach.

- Jednym z kluczowych wyzwań jest etap predykcji – przewidywania potencjalnych zagrożeń. Choć technologie detekcji i reakcji są coraz skuteczniejsze, wiele organizacji wciąż nie dysponuje narzędziami do analizy scenariuszy ryzyk. Dlatego rośnie znaczenie threat intelligence i analityki predyktywnej, które mogą przesunąć akcent z reagowania na zapobieganie.
- Kolejnym obszarem wymagającym uwagi jest bezpieczeństwo środowisk chmurowych. Rozproszone architektury IT wymagają nowych podejść do zarządzania tożsamością i dostępem. Rozwiązania z obszaru IAM (identity & access management) stają się nieodzownym elementem ochrony zasobów cyfrowych.
- Rozwój technologii opartych na sztucznej inteligencji, w tym generatywnej AI, niesie ze sobą nowe ryzyka związane z jakością i bezpieczeństwem generowanego kodu. Wymusza to potrzebę wdrażania nowych standardów audytu oraz edukacji programistów w zakresie cyberbezpieczeństwa.
- W kontekście bezpieczeństwa strategicznego Polska zyskuje przewagę wynikającą z położenia geograficznego i doświadczeń operacyjnych. Praktyczna wiedza zdobyta w warunkach realnego zagrożenia może stać się atutem na arenie międzynarodowej.
- Sektor publiczny może odegrać rolę katalizatora innowacji, stając się ważnym klientem i środowiskiem testowym dla krajowych rozwiązań. Potrzebne są jednak inwestycje w kompetencje – zarówno techniczne, jak i strategiczne – które umożliwią efektywne wykorzystanie potencjału sektora.

- Wreszcie, respondenci podkreślają znaczenie różnorodności – szczególnie w kontekście udziału kobiet i tworzenia inkluzywnych zespołów. To właśnie zróżnicowanie kulturowe i kompetencyjne może stymulować innowacyjność i odporność branży na przyszłe wyzwania.

Rozwój sektora wymaga działań systemowych – od edukacji, przez wsparcie legislacyjne i promocyjne, po wzmacnianie pozycji na rynkach zagranicznych. Tylko wspólne działania firm, administracji, uczelni i organizacji branżowych pozwolą na pełne wykorzystanie potencjału polskiego cyberbezpieczeństwa.

Predykcja zagrożeń i cyber threat intelligence (CTI)

Zdaniem części ekspertów, najsłabszym ogniwem w procesie ochrony organizacji przed cyberzagrożeniami jest etap predykcji, czyli prognozowania możliwych incydentów. O ile technologie detekcji (EDR, antywirusy) i reakcji są coraz bardziej zaawansowane, o tyle niewiele firm posiada procedury i narzędzia do analizowania możliwych scenariuszy zagrożeń. Stąd rosnące zainteresowanie obszarem threat intelligence – zarówno na poziomie usług doradczych, jak i rozwiązań automatyzujących zbieranie, analizę i korelację danych o zagrożeniach.

„[…] najwięcej firm ma źle zorganizowaną fazę właśnie PREDICT, znaczy w ogóle mało firm w ogóle robi tą predykcję cyberincydentów […]" ~ powiedział Respondent 7.

Powyższe obserwacje wskazują, że rozwój kompetencji i narzędzi w obszarze predykcji zagrożeń staje się jednym z priorytetów dla dalszego wzmacniania odporności cyfrowej organizacji. Luka na tym etapie cyklu bezpieczeństwa – pomiędzy identyfikacją zagrożeń a ich aktywną neutralizacją – może prowadzić do opóźnionej reakcji i zwiększonej podatności na incydenty. Dlatego konieczne wydaje się zarówno inwestowanie w analitykę predyktywną i cyber threat intelligence, jak i promowanie kultury przewidywania, opartej na systematycznym rozpoznawaniu i modelowaniu ryzyk. Tylko w ten sposób możliwe będzie przesunięcie punktu ciężkości z reagowania na zagrożenia ku ich skutecznemu zapobieganiu.

Bezpieczeństwo chmury i tożsamości cyfrowej

Jednym z najczęściej wskazywanych obszarów rozwojowych jest bezpieczeństwo rozwiązań chmurowych. Respondenci zauważają, że coraz więcej firm przenosi swoje systemy do środowisk cloudowych, jednak nie idzie to w parze z odpowiednią świadomością i kontrolą nad tym, co faktycznie dzieje się w tych systemach. W szczególności wskazywano na potrzebę rozwoju narzędzi do zarządzania tożsamością cyfrową (identity & access management), która w środowisku rozproszonym staje się kluczowym elementem architektury bezpieczeństwa.

„[…] coraz więcej firm korzysta z rozwiązań chmurowych, i nie jest to takie trywialne, żeby panować nad wszystkim, co tam się dzieje w tych systemach" ~ powiedział Respondent 10.

Z perspektywy respondentów, skuteczność systemów bezpieczeństwa w środowiskach chmurowych będzie w coraz większym stopniu zależna od zdolności organizacji do zarządzania tożsamością i dostępem w sposób dynamiczny, kontekstowy i zautomatyzowany. Rozproszona architektura IT, typowa dla nowoczesnych modeli biznesowych, wymusza odejście od klasycznych metod ochrony perymetrycznej na rzecz podejścia zorientowanego na użytkownika i jego prawa dostępu. W tym kontekście rozwiązania IAM zyskują rangę kluczowego ogniwa, integrującego aspekty technologiczne, procesowe i organizacyjne. Ich rozwój – zarówno pod względem funkcjonalnym, jak i dostępności dla mniejszych podmiotów – będzie miał istotny wpływ na poziom bezpieczeństwa całych ekosystemów cyfrowych.

Zagrożenia związane z generatywną sztuczną inteligencją

Pojawia się również refleksja dotycząca ryzyk generowanych przez sztuczną inteligencję, w szczególności w kontekście generowania kodu źródłowego. Zwracano uwagę, że nowe generacje deweloperów, wspomaganych systemami no-code i automatycznym kodowaniem, mogą nie być w stanie właściwie ocenić jakości i bezpieczeństwa wygenerowanego kodu. To rodzi nowe zagrożenia związane z infekowaniem bibliotek, ukrytymi podatnościami i błędami trudnymi do wykrycia – zwłaszcza przez te same algorytmy, które je wygenerowały.

„[…] ciężko uczyć systemy LLM wyłapywania błędów, które same wygenerowały, bo trudno jest testować swoje własne błędy" ~ powiedział Respondent 6.

W kontekście dynamicznego rozwoju narzędzi opartych na sztucznej inteligencji, szczególnie generatywnej, pojawiają się nowe wyzwania dotyczące zapewnienia bezpieczeństwa kodu źródłowego. Wskazane przez respondentów ryzyka ujawniają lukę pomiędzy tempem wdrażania nowoczesnych technologii a zdolnością ich bezpiecznego wykorzystania. Obserwowany deficyt kompetencji wśród młodszych programistów, wspieranych przez systemy no-code i AI, rodzi potrzebę wypracowania nowych standardów audytu kodu, mechanizmów kontroli jakości oraz edukacji z zakresu bezpieczeństwa aplikacji.
W przeciwnym razie sektor IT może stanąć wobec narastającego problemu „czarnych skrzynek" – rozwiązań tworzonych przez modele, których działania są nieprzejrzyste nawet dla ich użytkowników.

Cyberbezpieczeństwo w kontekście geopolitycznym

Respondenci wielokrotnie wskazywali, że sytuacja geopolityczna – zwłaszcza wschodnia granica Polski i trwająca wojna w Ukrainie – ma realny wpływ na postrzeganie polskich rozwiązań bezpieczeństwa jako szczególnie istotnych i „bliskich praktyce". Podkreślano, że Polska jako kraj graniczny ma szczególne kompetencje w zakresie reagowania na zagrożenia cyfrowe, co może być dodatkowym atutem we współpracy z partnerami zagranicznymi i sektorem publicznym.

„Nasz produkt jako system ochrony przed cyberatakami przez naszych partnerów z zagranicy widziany właśnie w tym kolorycie, że my jako Polacy o tym wiemy" ~ powiedział Respondent 2.

Wnioski płynące z wypowiedzi respondentów wskazują, że położenie geograficzne Polski oraz bezpośrednie doświadczenia związane z konfliktem za wschodnią granicą stwarzają unikalne warunki do rozwoju kompetencji w obszarze cyberbezpieczeństwa. W sytuacji zwiększonego ryzyka geopolitycznego, praktyczna wiedza i gotowość operacyjna zyskują szczególne znaczenie – co może stanowić przewagę konkurencyjną polskich firm na arenie międzynarodowej. Potencjał ten warto wzmacniać poprzez systemowe wspieranie współpracy międzynarodowej, a także budowanie narracji o Polsce jako wiarygodnym i doświadczonym partnerze w dziedzinie bezpieczeństwa cyfrowego.

Współpraca z sektorem publicznym i obronnym

Kilku respondentów wyraziło przekonanie, że przyszłość rozwoju technologii cyberbezpieczeństwa w Polsce może być silnie związana z rosnącym zapotrzebowaniem instytucji publicznych, wojska oraz sektora bezpieczeństwa narodowego. Istnieją już przykłady projektów realizowanych dla MON-u, jednak ich liczba powinna wzrosnąć, by w pełni wykorzystać potencjał innowacyjnych rozwiązań.

„Generalnie uważam, że państwo powinno wspierać rozwój technologii, żebyśmy byli właśnie krajem, czy też Unia, żebyśmy byli krajami, które są samowystarczalne i wsparcie państwa w tym zakresie rozwoju, no też rozwoju takiego ekonomiczno-gospodarczego, krótko mówiąc" ~ powiedział Respondent 7.

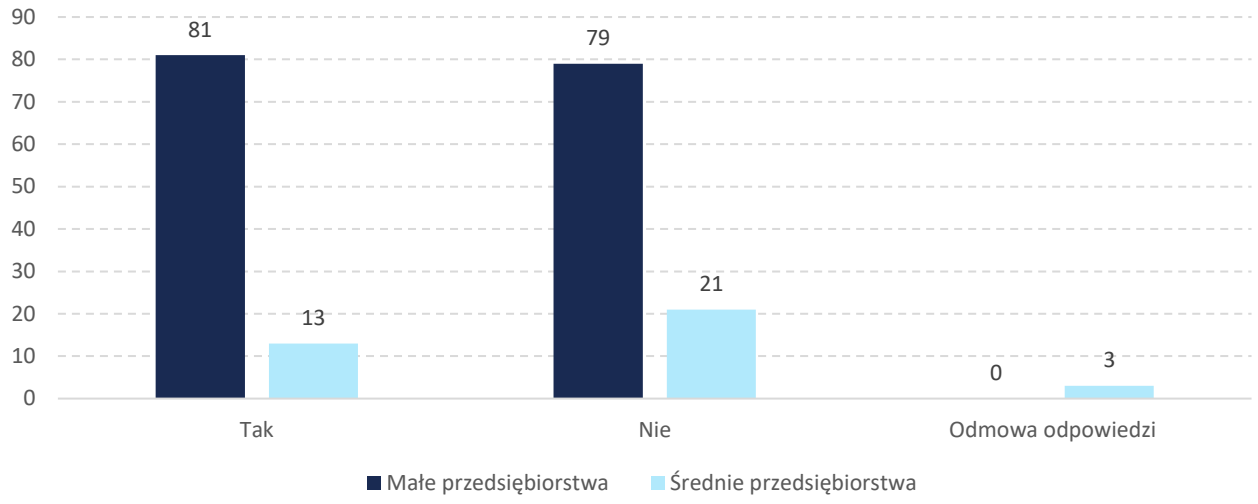
„[…] Państwo patrzy z perspektywy Państwa, no to wydaje mi się, że tutaj wykorzystanie tej naszej sytuacji geopolitycznej […] to są takie przewagi i też współpraca z sektorem właśnie publicznym, czyli ze wszystkimi cywilami, z wojskiem. Mamy takie w sumie przykłady już ciekawych rozwiązań, które realizują projekty właśnie dla MON-u. No to potrzebujemy tego więcej, żeby tego było więcej" ~ powiedział Respondent 8.

Wypowiedzi te potwierdzają, że sektor publiczny – w tym administracja państwowa i instytucje związane z obronnością – może odegrać kluczową rolę jako odbiorca i promotor innowacyjnych technologii cyberbezpieczeństwa. Zwiększenie liczby wdrożeń w tym obszarze nie tylko umożliwi firmom pozyskanie stabilnych kontraktów, ale również stworzy środowisko testowe dla rozwiązań o wysokim poziomie złożoności. W dłuższej perspektywie może to przyczynić się do zbudowania krajowego ekosystemu kompetencji i rozwiązań, zdolnego do konkurowania z zagranicznymi dostawcami również na innych rynkach strategicznych cyfrowych.

Rozwój produktów i nowych funkcjonalności jako priorytet inwestycyjny

Jednym z istotnych elementów badania było określenie planów inwestycyjnych firm z sektora cyberbezpieczeństwa w nadchodzącym roku. Analiza odpowiedzi respondentów pozwala ocenić ogólny klimat inwestycyjny w branży oraz zidentyfikować poziom gotowości do rozwoju technologicznego i biznesowego. W szczególności zweryfikowano, czy przedsiębiorstwa planują przeznaczyć środki na nowe projekty, innowacje produktowe, rozbudowę infrastruktury czy ekspansję zagraniczną. Wykres 15 prezentuje rozkład odpowiedzi na pytanie o planowane inwestycje, ukazując aktualne nastroje i strategie rozwojowe firm działających na polskim rynku cyberbezpieczeństwa.

Wykres 15. Czy w najbliższym roku planują Państwo inwestycje? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

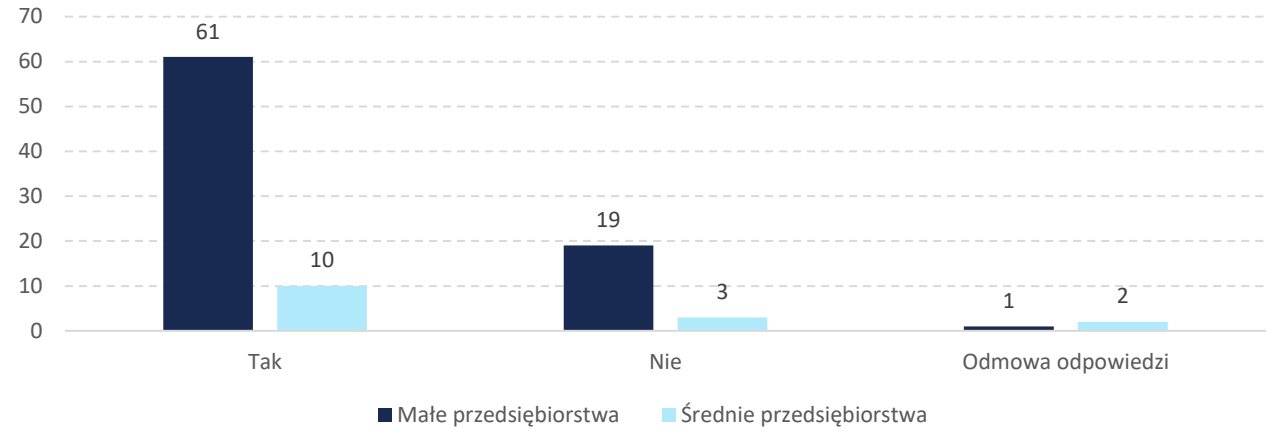
Respondenci badania zostali zapytani o plany inwestycyjne na najbliższy rok. Odpowiedzi rozłożyły się niemal równomiernie, szczególnie wśród małych firm.

Inwestycje w nadchodzącym roku planuje 81 małych oraz 13 średnich przedsiębiorstw. Z kolei brak takich planów zadeklarowało 79 małych i 21 średnich firm.

Wyniki te wskazują na umiarkowany optymizm inwestycyjny wśród respondentów – choć znaczna część firm planuje rozwój, równie liczna grupa nie przewiduje nowych nakładów w najbliższym czasie.

Wśród firm deklarujących zamiar inwestowania w najbliższym roku szczególną uwagę poświęcono celom tych nakładów. Wykres 16 przedstawia odpowiedzi na pytanie, czy planowane inwestycje obejmują infrastrukturę badawczo-rozwojową (B+R). Analiza tego aspektu pozwala lepiej zrozumieć, w jakim stopniu firmy koncentrują się na tworzeniu innowacyjnych rozwiązań technologicznych, dostosowywaniu produktów do zmieniających się regulacji oraz wdrażaniu automatyzacji i sztucznej inteligencji. Dane te pokazują również, jakie priorytety inwestycyjne dominują w sektorze cyberbezpieczeństwa i jaką rolę odgrywa rozwój B+R w strategiach rozwojowych przedsiębiorstw.

Wykres 16. Czy planowane inwestycje, dotyczą infrastruktury R+B? (N=96)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Spośród respondentów badania, którzy zadeklarowali plany inwestycyjne na najbliższy rok (N=99), zdecydowana większość małych przedsiębiorstw wskazała, że planowane inwestycje będą dotyczyć infrastruktury badawczo-rozwojowej (R+B). Taką odpowiedź udzieliło 61 małych firm oraz 10 firm z drugiej grupy (najprawdopodobniej średnich przedsiębiorstw).

Brak planów inwestycyjnych w obszarze R+B zadeklarowało 19 małych oraz 3 średnie firmy.

Zdecydowana większość firm planuje kontynuację lub intensyfikację działań badawczo-rozwojowych (B+R), skupionych na tworzeniu nowoczesnych rozwiązań oraz aktualizacji istniejących produktów. Szczególne znaczenie mają projekty obejmujące automatyzację usług z wykorzystaniem sztucznej inteligencji, rozwój mechanizmów uwierzytelniania (np. MFA, bezhasłowe logowanie), a także zgodność z nowymi regulacjami europejskimi, w tym dyrektywą NIS2.

Wskazania respondentów pokazują, że są to inwestycje wieloetapowe, rozciągnięte w czasie i wymagające znacznych nakładów pracy zespołów programistycznych i technologicznych:

„[…] w tym roku planujemy wprowadzić na rynek dwa kompletne i również zrobić taki refresh jednego z naszych urządzeń, który do tej pory funkcjonuje od kilku lat […]" ~ powiedział Respondent 1.

„[…], na pewno planujemy zakończyć obecną inwestycję, czyli wersję trzecią systemu. To jest tak jak powiedziałem 2,5 roku pracy, dodatkowy zespół programistów" ~ powiedział Respondent 9.

„[…] staramy się zbudować obecnie coś, czego myślę, że jakby taką usługę unikalną, której nie ma tak naprawdę na rynku, czyli ISAC dla właśnie małych, średnich przedsiębiorstw oraz NGOs […] pozwoli jakby im zbudować podstawy cyberbezpieczeństwa bez jakichś tam ogromnych nakładów finansowych […]" ~ powiedział Respondent 13.

Nowe produkty mają być nie tylko technologicznie innowacyjne, ale również bardziej dostępne cenowo i skalowalne, szczególnie z myślą o segmencie MŚP – który dotychczas był często niedostatecznie chroniony.

Rozbudowa i dostosowanie oferty produktowo-usługowej

Równolegle z ekspansją geograficzną postępuje rozwój oferty – zarówno poprzez tworzenie nowych produktów, jak i dostosowywanie istniejących rozwiązań do specyfiki poszczególnych rynków. Szczególny nacisk kładzie się na usługi i narzędzia zgodne z nowymi regulacjami, takie jak:

- wieloskładnikowe uwierzytelnianie (MFA),
- rozwiązania typu SaaS w modelu samoobsługowym,
- platformy wymiany informacji o zagrożeniach (np. ISAC dla MŚP),
- produkty zgodne z NIS2, EIDAS 2.0 czy DORA.

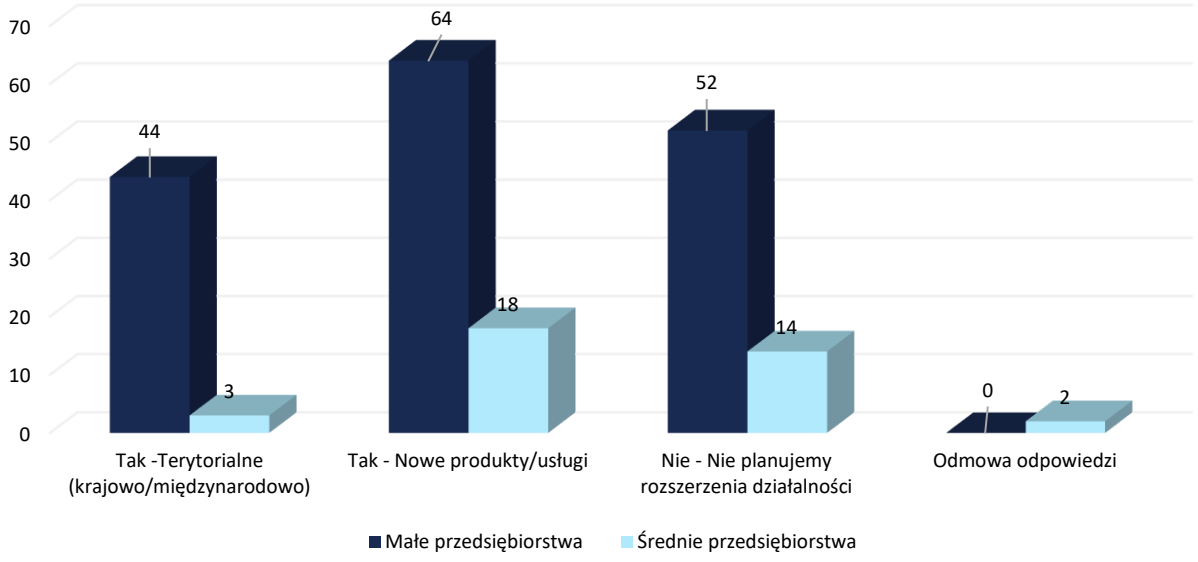
Warto podkreślić, że strategia rozwoju oferty nie ogranicza się wyłącznie do aspektów technologicznych. Firmy prowadzą aktywną rekrutację partnerów handlowych, rozwijając sieci dystrybucji oraz systemy wsparcia lokalnych klientów. Tworzenie kanałów partnerskich (partnerzy, resellerzy, integratorzy) w poszczególnych krajach jest postrzegane jako kluczowy element skutecznego skalowania działalności.

> *„[…], jeśli chodzi o dystrybutorów to oczywiście mamy ich pięćdziesięciu, no, ale krajów jest wiele i w każdym kraju może być kilku dystrybutorów, więc jakby cały czas aktywnie poszukujemy tych dystrybutorów" ~ powiedział Respondent 1.*

Ekspansja terytorialna: Europa, Bliski Wschód i Ameryka Północna

Poniższy wykres prezentuje plany ekspansji firm działających w branży cyberbezpieczeństwa, zarówno pod względem terytorialnym, jak i rozwoju oferty produktowej. Wyniki te obrazują aktualne nastawienie rynku do wzrostu i skalowania działalności, uwzględniając zarówno ambicje rozwojowe, jak i czynniki ograniczające.

Wykres 17. Czy planowane jest rozszerzenie działalności: (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Najczęściej deklarowanym kierunkiem rozwoju było wprowadzenie nowych produktów lub usług. Taką odpowiedź wskazało 64 małych oraz 18 średnich firm. Rozszerzenie działalności w ujęciu terytorialnym (na poziomie krajowym lub międzynarodowym) planuje 44 małe i 3 średnie przedsiębiorstwa. Z kolei brak planów rozwojowych zadeklarowało 52 małych oraz 14 średnich firm.

Wyniki te wskazują, że wśród badanych firm rozwój oferty produktowej i usługowej stanowi najczęściej wybierany kierunek ekspansji, podczas gdy ekspansja geograficzna jest rozważana rzadziej – szczególnie wśród średnich przedsiębiorstw.

Firmy planują rozszerzenie działalności przede wszystkim na kraje europejskie – w szczególności region DACH (Niemcy, Austria, Szwajcaria), Europę Wschodnią oraz państwa, w których wdrożone lub planowane są zaawansowane regulacje z zakresu cyberbezpieczeństwa. Jednocześnie pojawiają się coraz śmielsze plany ekspansji poza Europę – m.in. na Bliski Wschód oraz do Ameryki Północnej.

Przedstawiciele firm podkreślają, że zainteresowanie ich ofertą płynie także z rynków zagranicznych, co dodatkowo mobilizuje do podejmowania konkretnych kroków w kierunku internacjonalizacji:

„Zdecydowanie na razie ekspansja na terenie Europy Wschodniej. […], ale również też się Bliski Wschód odzywa do nas […]" ~ powiedział Respondent 4.

W kontekście ekspansji firmy uwzględniają nie tylko kwestie formalno-prawne, ale także technologiczne. Szczególną uwagę poświęcają lokalizacji infrastruktury chmurowej, dostosowaniu centrów danych (np. data center w USA) oraz zapewnieniu zgodności z lokalnymi wymogami compliance. Wszystkie te działania wymagają nakładów inwestycyjnych, dostosowania struktur sprzedażowych i reorganizacji działań operacyjnych.

Inwestycje w infrastrukturę i rozwój zespołów

Trzecim strategicznym obszarem inwestycyjnym jest rozbudowa zasobów technicznych i ludzkich. Firmy planują zwiększenie zatrudnienia – głównie w działach badawczo-rozwojowych, sprzedaży i marketingu – oraz inwestycje w fizyczną infrastrukturę. Przykłady obejmują budowę nowych przestrzeni produkcyjnych, powiększenie biur czy stworzenie wyspecjalizowanych zespołów do obsługi nowych rynków.

„[…] środki również zamierzamy inwestować w rozwój naszego zespołu oraz działania marketingowo-sprzedażowe na nowych rynkach" ~ powiedział Respondent 11.

Działania te mają wzmocnić zdolność operacyjną firm i przygotować je na obsługę większej liczby klientów oraz projektów – zarówno w kraju, jak i za granicą.

Brak aktywnych planów rozwoju – przyczyny

Część badanych firm przyznała, że mimo otwartości na okazjonalne inicjatywy rozwojowe, ich obecna strategia zakłada koncentrację na głównych rynkach uznanych za kluczowe z punktu widzenia przychodów i stabilności. Najczęściej wskazywanymi kierunkami są Europa Zachodnia (w szczególności kraje regionu DACH) oraz Stany Zjednoczone. Firmy te świadomie ograniczają skalę nowych działań, kierując dostępne zasoby – kadrowe, technologiczne i finansowe – na wzmocnienie pozycji w wybranych lokalizacjach.

Wypowiedzi przedstawicieli firm potwierdzają, że takie podejście wynika z potrzeby optymalizacji działań i maksymalizacji zwrotu z inwestycji:

„Nie mamy w tej chwili tych działań skomunikowanych w tym zakresie, jeśli trafi się oczywiście klient, to jesteśmy w stanie go obsłużyć, natomiast naszym głównym fokusem jest jednak Europa i Stany Zjednoczone na tą chwilę" ~ powiedział Respondent 6.

Inną przyczyną ograniczenia aktywności ekspansyjnych jest oczekiwanie na ukończenie bieżących prac badawczo-rozwojowych. Dla wielu firm nowe kierunki rozwoju – zarówno geograficzne, jak i produktowe – są uzależnione od powodzenia aktualnie realizowanych projektów. Szczególnie dotyczy to podmiotów inwestujących w autorskie platformy, rozwiązania automatyzujące procesy bezpieczeństwa lub narzędzia zgodne z nowymi regulacjami.

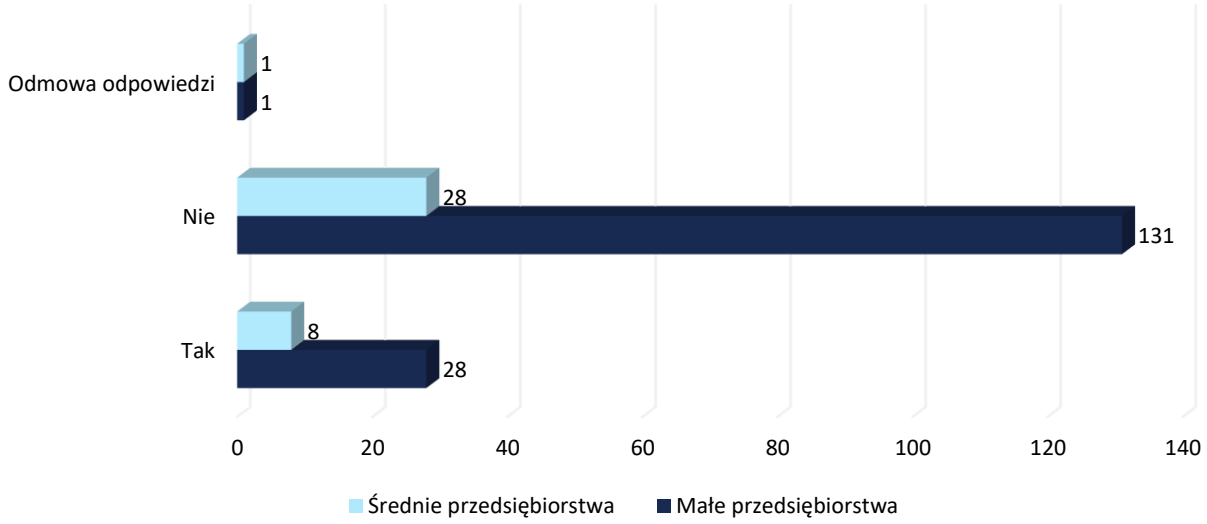
Firmy deklarują, że decyzje strategiczne zostaną podjęte dopiero po uzyskaniu mierzalnych rezultatów i przetestowaniu nowych produktów w praktyce:

„[…] rozszerzona ta nasza paleta takich capabilities samej platformy, chociażby w ramach tego, czy jak już będą wyniki tego projektu B+R, ale to dopiero za dwa lata nastąpi" ~ powiedział Respondent 10.

Niektóre przedsiębiorstwa znajdują się na etapie planowania i analizy możliwych scenariuszy rozwoju. Zamiast podejmować pochopne decyzje o ekspansji, firmy starają się dokładnie przemyśleć kwestie modelu wdrożenia (np. rozwój usług wewnętrznie czy poprzez nową spółkę), oczekiwań klientów, a także potencjalnych skutków organizacyjnych i wizerunkowych. Dotyczy to zwłaszcza podmiotów, które rozważają wejście w nowe obszary usługowe, takie jak testy penetracyjne, monitoring infrastruktury cloudowej czy zautomatyzowane audyty bezpieczeństwa.

W kontekście wspierania innowacyjności i rozwoju technologicznego, respondenci zostali zapytani o korzystanie z usług akceleratorów lub inkubatorów technologicznych. Tego typu instytucje odgrywają istotną rolę w przyspieszaniu rozwoju młodych firm, szczególnie w sektorze nowych technologii, oferując wsparcie doradcze, finansowe oraz dostęp do sieci kontaktów.

Wykres 18. Czy korzystali Państwo z usług akceleratorów lub inkubatorów technologicznych? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci badania zostali zapytani czy ich przedsiębiorstwa korzystały z usług akceleratorów lub inkubatorów technologicznych. Zdecydowana większość firm – zarówno małych, jak i średnich – zadeklarowała brak takiego doświadczenia. Odpowiedź „nie" wskazało 131 małych oraz 28 średnich przedsiębiorstw.

Z usług akceleratorów lub inkubatorów skorzystało 28 małych i 8 średnich firm, co stanowi mniejszość wśród badanych.

Wyniki te sugerują, że choć mechanizmy wsparcia w postaci akceleratorów i inkubatorów są dostępne, to ich wykorzystanie wśród firm z sektora cyberbezpieczeństwa pozostaje ograniczone.

Podsumowanie:

Aby wykorzystać potencjał rozwojowy, konieczne są działania systemowe: od reformy edukacji, przez odpowiednie regulacje i mechanizmy wsparcia publicznego, po wzmocnienie współpracy między firmami, uczelniami i administracją. Prawie połowa firm biorących udział w badaniu planuje inwestycje w cyberbezpieczeństwo w najbliższym roku – głównie w rozwój produktów, automatyzację usług i dostosowanie się do unijnych regulacji, takich jak NIS2 czy DORA.

Wysokim priorytetem są projekty badawczo-rozwojowe, które obejmują rozwój mechanizmów MFA, systemów zgodnych z regulacjami europejskimi, oraz usług w modelu SaaS dla MŚP. Firmy deklarują także zainteresowanie ekspansją na rynki zagraniczne, w tym Europę Wschodnią, region DACH, Bliski Wschód oraz Amerykę Północną. Ważnym czynnikiem ekspansji są zgodność z lokalnymi przepisami oraz dostępność infrastruktury chmurowej.

Pomimo optymizmu inwestycyjnego, firmy wskazują na liczne bariery rozwoju – przede wszystkim przeregulowanie, biurokrację oraz nieprzewidywalność prawa. Nowe regulacje unijne wymagają czasochłonnych dostosowań umownych i prawnych, co obciąża zespoły wewnętrzne i opóźnia rozwój produktów.

Część firm podejmuje bardziej ostrożną strategię – koncentrując się na rynkach głównych i bieżących projektach. Takie podejście ma na celu optymalizację wykorzystania zasobów i zwiększenie efektywności inwestycji. Niektóre firmy odkładają decyzje o ekspansji do momentu zakończenia prac B+R lub uzyskania wyników z projektów pilotażowych.

Respondenci podkreślają również potrzebę strategicznego planowania i dostosowywania modelu działalności do oczekiwań klientów oraz lokalnych uwarunkowań. Zamiast pochopnych działań, firmy starają się dokładnie analizować możliwości, m.in. poprzez testowanie modeli usługowych, takich jak monitoring infrastruktury chmurowej czy automatyczne audyty bezpieczeństwa.

Na koniec warto zwrócić uwagę na niskie wykorzystanie usług akceleratorów i inkubatorów technologicznych – aż 81% firm nie miało z nimi kontaktu. To pokazuje niewykorzystany potencjał tych instytucji jako narzędzia wspierającego innowacyjność w sektorze cyberbezpieczeństwa. Promocja i rozwój programów akceleracyjnych mogłyby znacząco przyspieszyć rozwój młodych firm i zwiększyć odporność cyfrową całej gospodarki.

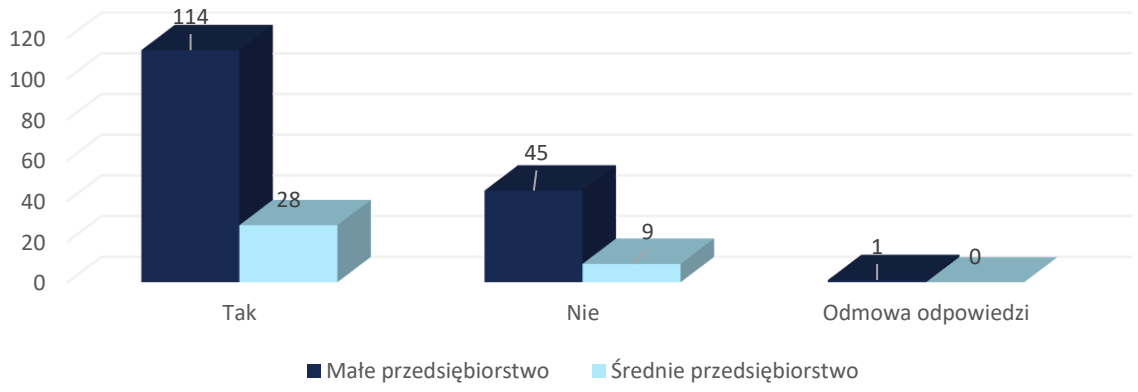
Podsumowując, sektor cyberbezpieczeństwa w Polsce stoi przed szansą na międzynarodowy sukces, pod warunkiem dalszych inwestycji, strategicznej współpracy i zdolności do szybkiego adaptowania się do globalnych wyzwań technologicznych i regulacyjnych.

2.3. Certyfikacja

Certyfikacja, ochrona własności intelektualnej oraz zgodność z międzynarodowymi standardami stanowią istotne elementy budowania wiarygodności i konkurencyjności firm z sektora cyberbezpieczeństwa – zarówno na rynku krajowym, jak i zagranicznym. W kontekście rosnących wymagań regulacyjnych (np. NIS2, CRA, DORA), a także coraz wyższych oczekiwań ze strony partnerów biznesowych i instytucji publicznych, kluczowe znaczenie zyskują takie obszary jak świadomość certyfikacyjna, gotowość do formalizacji jakości oferowanych rozwiązań oraz podejście do ochrony innowacji.

Poniższy wykres przedstawia poziom świadomości firm w zakresie procesu certyfikacji, który odgrywa istotną rolę w budowaniu zaufania klientów i spełnianiu wymagań regulacyjnych w obszarze cyberbezpieczeństwa.

Wykres 19. Czy w Państwa przedsiębiorstwie istnieje wiedza na temat procesu certyfikacji? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

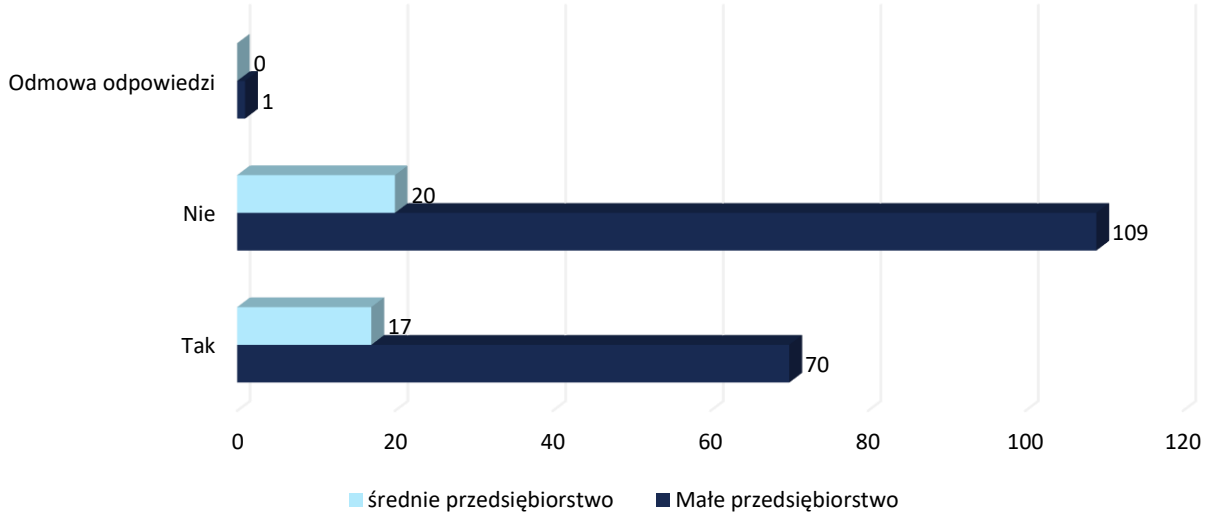
Zdecydowana większość firm – zarówno małych, jak i średnich – zadeklarowała posiadanie takiej wiedzy. Odpowiedź „tak" wskazało 114 małych oraz 28 średnich przedsiębiorstw.

Brak wiedzy w tym zakresie zadeklarowało 45 małych i 9 średnich firm, co pokazuje, że choć świadomość certyfikacyjna jest wysoka, nadal istnieje grupa podmiotów, które mogą wymagać dodatkowego wsparcia informacyjnego lub edukacyjnego.

Wynik ten może być impulsem dla instytucji publicznych, izb gospodarczych i organizacji branżowych do prowadzenia działań informacyjnych i szkoleniowych, które ułatwią przedsiębiorstwom zdobycie kompetencji niezbędnych do rozpoczęcia procesu certyfikacji.

Poniższy wykres ilustruje podejście firm do kwestii certyfikacji oferowanych produktów i usług. Wyniki te pozwalają ocenić gotowość rynku do wdrażania formalnych standardów jakości i bezpieczeństwa, które coraz częściej stają się wymogiem we współpracy z partnerami biznesowymi i instytucjami publicznymi.

Wykres 20. Czy mają Państwo plany certyfikacji produktów/usług? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

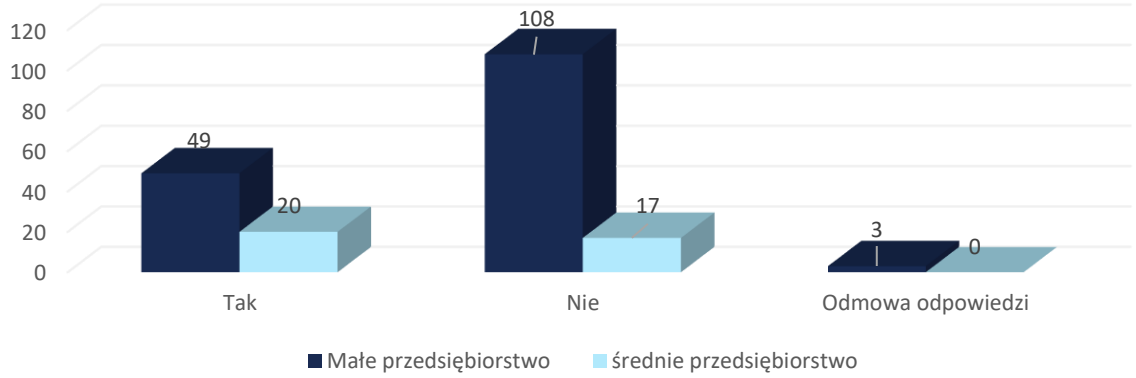
Respondenci badania zostali także zapytani, czy planują certyfikację swoich produktów lub usług. Większość firm – szczególnie wśród małych przedsiębiorstw – zadeklarowała brak takich planów. Taką odpowiedź wskazało 109 małych oraz 20 średnich firm.

Plany certyfikacyjne zadeklarowało 70 małych i 17 średnich przedsiębiorstw, co stanowi istotną część badanych podmiotów, choć nadal mniejszość. Może to świadczyć o rosnącym zainteresowaniu formalnym potwierdzaniem jakości i zgodności oferowanych rozwiązań, szczególnie w kontekście wymagań rynkowych i regulacyjnych.

Wynik ten wskazuje na istnienie realnej bariery wdrożeniowej w obszarze standaryzacji i zgodności z normami.

Poniższy wykres przedstawia stopień formalnego zabezpieczania własności intelektualnej przez firmy działające w sektorze cyberbezpieczeństwa. Analiza pozwala ocenić, w jakim zakresie przedsiębiorstwa korzystają z narzędzi prawnych służących ochronie innowacji i budowaniu przewagi konkurencyjnej.

Wykres 21. Czy przedsiębiorstwo posiada patenty/ licencje/ znaki towarowe/ wzory użytkowe, etc. związane z produktami/usługami? (N=197)

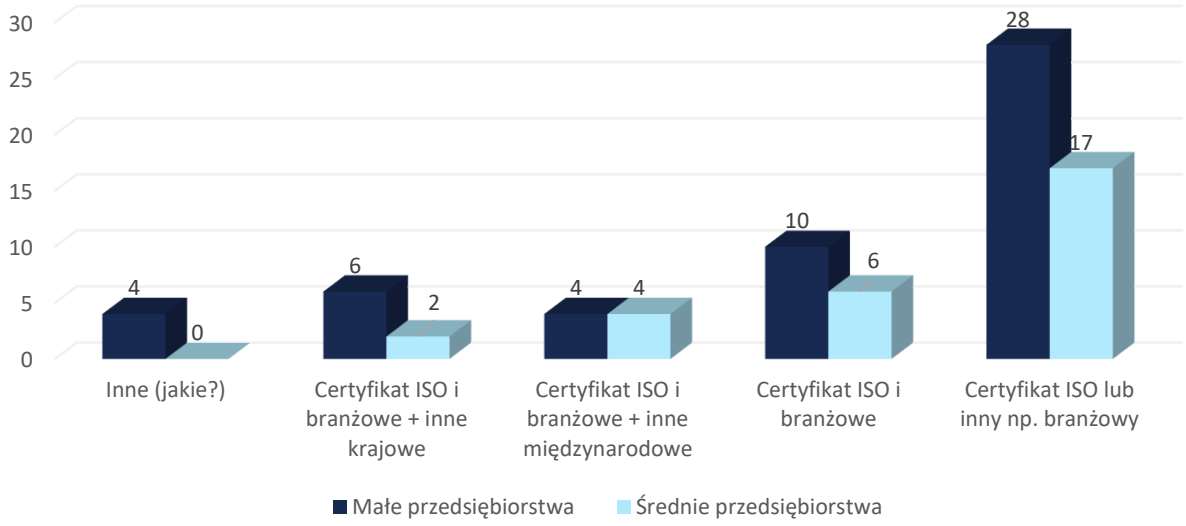


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Posiadanie takich praw zadeklarowało 49 małych oraz 20 średnich firm. Z kolei brak tego typu zabezpieczeń własności intelektualnej wskazało 108 małych i 17 średnich przedsiębiorstw. Taki wynik może świadczyć o ograniczonym zaangażowaniu przedsiębiorstw w formalne zabezpieczanie rezultatów prac rozwojowych i innowacyjnych. Może to być efektem zarówno braku świadomości na temat możliwości ochrony własności intelektualnej, jak i stosunkowo niskiego poziomu innowacyjności lub przewagi konkurencyjnej opartej na innych czynnikach, np. szybkości wdrożeń czy relacjach z klientem.

Poniższy wykres obrazuje, jakie certyfikaty, akredytacje i inne formalne dokumenty jakościowe posiadają firmy z sektora cyberbezpieczeństwa. Dane te pozwalają zidentyfikować, które standardy są najczęściej wdrażane i jakie podejście do formalnej zgodności przyjmują przedsiębiorstwa w tej branży.

Wykres 22 Liczba certyfikatów/ akredytacje/ jakość / dopuszczenia (N=71)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci badania zostali zapytani o posiadane certyfikaty, akredytacje, oznaczenia jakości lub dopuszczenia związane z działalnością ich przedsiębiorstw. Najczęściej wskazywaną odpowiedzią – zarówno wśród małych, jak i średnich firm – było posiadanie certyfikatu ISO lub innego, np. branżowego. Tę kategorię zaznaczyło 28 małych oraz 17 średnich przedsiębiorstw.

Kolejną grupę stanowiły firmy posiadające zarówno certyfikat ISO, jak i certyfikaty branżowe – 10 małych i 6 średnich firm. Nieco mniej liczne były podmioty deklarujące posiadanie certyfikatów ISO i branżowych wraz z dodatkowymi certyfikatami międzynarodowymi (4 małe i 4 średnie firmy), a także z dodatkowymi certyfikatami krajowymi (6 małych i 2 średnie firmy).

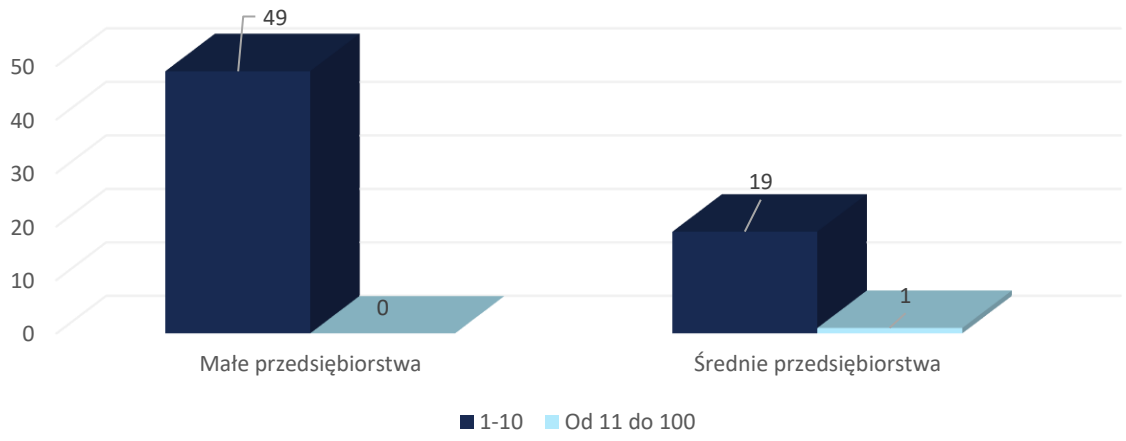
Najrzadziej wskazywaną kategorią były inne formy certyfikacji, niewymienione w głównych grupach – tę odpowiedź zaznaczyły jedynie 4 małe firmy, bez udziału średnich przedsiębiorstw.

Wyniki te pokazują, że certyfikacja – szczególnie w formie ISO i branżowej – jest powszechnie stosowana wśród respondentów, co może świadczyć o dążeniu do zapewnienia wysokiej jakości i zgodności z normami w sektorze cyberbezpieczeństwa.

Dane te pokazują, że choć duża część firm nie posiada żadnych formalnych certyfikacji, to wśród tych, które je wdrażają, dominują dokumenty potwierdzające zgodność z międzynarodowymi standardami zarządzania bezpieczeństwem informacji. Może to świadczyć o wysokiej świadomości znaczenia standaryzacji oraz chęci zwiększenia konkurencyjności i wiarygodności wobec klientów oraz partnerów instytucjonalnych.

Wykres prezentuje liczbę posiadanych przez firmy praw własności intelektualnej powiązanych z ich ofertą produktową lub usługową. Dane pozwalają ocenić, w jakim stopniu przedsiębiorstwa formalnie zabezpieczają rezultaty swojej działalności innowacyjnej i rozwojowej.

Wykres 23 Ile patentów/ licencji/ znaków towarowych/ wzorów użytkowych, etc., związane z produktami/usługami posiada Państwa firma? (N=69)



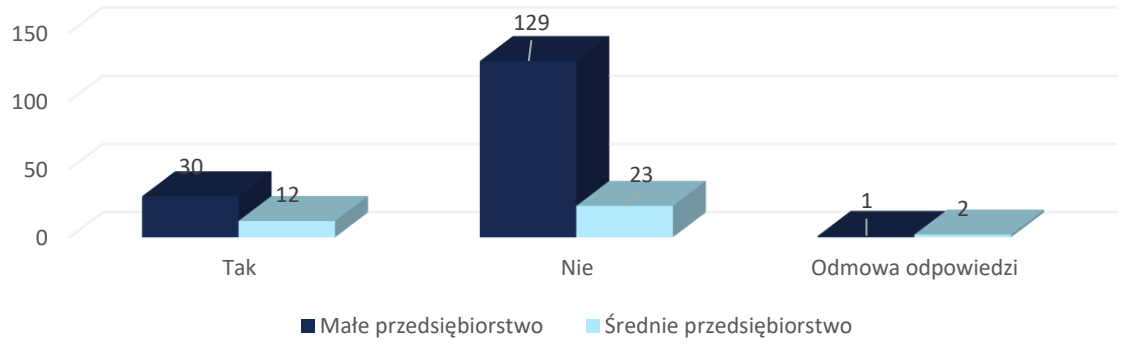
Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Większość firm zadeklarowała posiadanie od 1 do 10 patentów, licencji, znaków towarowych lub wzorów użytkowych związanych z oferowanymi produktami lub usługami. W tej kategorii znalazło się 49 małych oraz 19 średnich przedsiębiorstw. Tylko jedno średnie przedsiębiorstwo wskazało, że dysponuje od 11 do 100 takich form ochrony. Wśród małych firm żaden respondent zadeklarował przekroczenia progu 10. Dane te sugerują, że działania związane z ochroną własności intelektualnej są obecne, jednak ich skala jest zazwyczaj ograniczona do kilku rozwiązań.

2.4. Rodzaje finansowania

Poniższy wykres przedstawia czy wykorzystane są środki unijne przez firmy działające w branży cyberbezpieczeństwa, ze szczególnym uwzględnieniem projektów badawczo-rozwojowych. Wyniki te pozwalają ocenić, na ile przedsiębiorstwa sięgają po dostępne instrumenty wspierające innowacyjność, rozwój technologiczny i wdrażanie nowych rozwiązań.

Wykres 24. Czy firma korzystała wcześniej ze wsparcia krajowego lub unijnego w celu wsparcia rozwoju (np. projekty R+B)? (N=197)



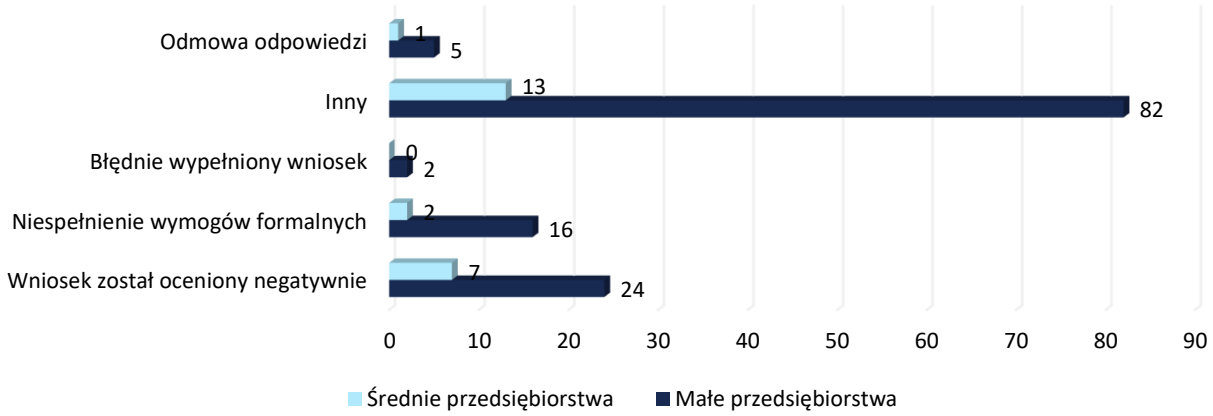
Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość firm nie korzystała dotychczas ze wsparcia krajowego ani unijnego w celu rozwoju działalności, w tym realizacji projektów badawczo-rozwojowych. Taką odpowiedź wskazało 129 małych oraz 23 średnie przedsiębiorstwa. Z pomocy publicznej lub unijnej skorzystało łącznie 42 respondentów — w tym 30 małych i 12 średnich firm.

Wyniki te mogą świadczyć o ograniczonym dostępie do instrumentów wsparcia lub niskim poziomie ich wykorzystania, szczególnie wśród mniejszych podmiotów.

Poniższy wykres przedstawia najczęściej wskazywane powody, dla których firmy nie skorzystały z dostępnego wsparcia krajowego lub unijnego w zakresie rozwoju, w tym projektów badawczo-rozwojowych. Dane pochodzą zarówno z odpowiedzi zamkniętych, jak i otwartych, co pozwala lepiej zrozumieć bariery utrudniające udział przedsiębiorstw w programach wspierających innowacyjność i rozwój technologiczny.

Wykres 25. Jaki był powód niekorzystania z takiej formy wsparcia (wsparcie rozwoju np. projekty R+B)? (N=152)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Najczęściej wskazywaną przyczyną niekorzystania ze wsparcia krajowego lub unijnego na cele rozwojowe były inne, niesprecyzowane powody. Taką odpowiedź zaznaczyło aż 82 małych oraz 13 średnich przedsiębiorstw. Znacząca liczba firm (24 małe i 7 średnich) wskazała również, że ich wnioski zostały ocenione negatywnie. Kolejną barierą okazało się niespełnienie wymogów formalnych — ten problem dotyczył 16 małych i 2 średnich firm. Sporadycznie pojawiały się przypadki błędnie wypełnionych wniosków (2 małe firmy) oraz odmowy udzielenia odpowiedzi (5 małych i 1 średnie przedsiębiorstwo).

Ponadto w ramach odpowiedzi otwartych najczęściej pojawiającym się powodem był brak wiedzy o dostępnych programach, ich zasadach, warunkach udziału oraz potencjalnych korzyściach. Respondenci wielokrotnie wskazywali, że nie byli świadomi istnienia takich form wsparcia, nie mieli dostępu do odpowiednich informacji lub nie posiadali danych niezbędnych do przygotowania aplikacji. Taki brak podstawowej wiedzy skutecznie uniemożliwia podjęcie decyzji o uczestnictwie w programach rozwojowych i wskazuje na potrzebę lepszej komunikacji ze strony instytucji oferujących pomoc.

Drugą istotną barierą okazały się skomplikowane procedury aplikacyjne i rozliczeniowe. Respondenci zwracali uwagę na formalizm, nadmiar dokumentacji, nieintuicyjne zasady i brak jasnych ścieżek postępowania. Pojawiały się głosy, że pozyskiwanie środków przypomina loterię, a jeden błąd formalny – często niezależny od firmy – może przekreślić cały wysiłek. Takie doświadczenia skutecznie zniechęcają do ponownych prób ubiegania się o wsparcie, zwłaszcza wśród mniejszych firm.

Kolejną grupę stanowiły odpowiedzi wskazujące na brak zasobów organizacyjnych i czasowych. Firmy często deklarowały, że nie mają odpowiednich kadr, czasu ani struktury, która mogłaby zająć się obsługą projektu – od napisania wniosku, przez jego realizację, po rozliczenie. Dla części respondentów barierą była także bieżąca działalność operacyjna, która nie pozostawiała przestrzeni na zaangażowanie się w działania rozwojowe.

Warto także odnotować wypowiedzi wskazujące na brak potrzeby lub motywacji do korzystania z dostępnego wsparcia. Niektóre firmy przyznały wprost, że nie widzą sensu w aplikowaniu o środki zewnętrzne, ponieważ nie mają projektów, które kwalifikowałyby się do dofinansowania lub uważają, że samodzielnie są w stanie sfinansować niezbędny rozwój.

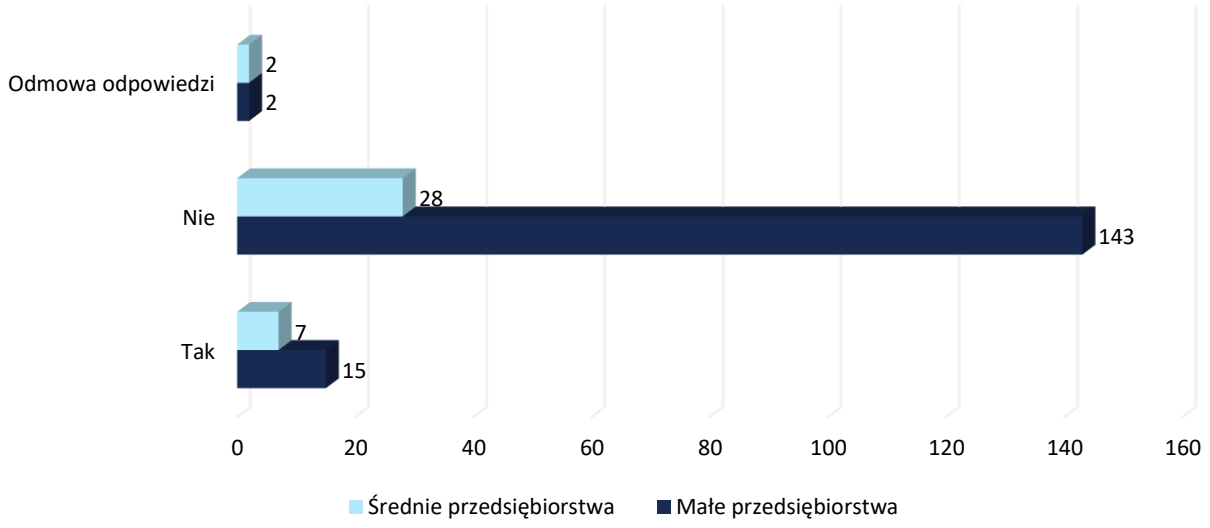
Pojawiły się również głosy wyrażające nieufność wobec systemu wsparcia. Część respondentów odwoływała się do złych doświadczeń, np. odrzucenia wniosku z powodów proceduralnych, czy problemów, jakie inne firmy miały z rozliczeniem środków i późniejszymi kontrolami. Dla niektórych taka sytuacja była wystarczającym powodem, by całkowicie zrezygnować z ubiegania się o dofinansowanie.

Wreszcie, w kilku przypadkach wskazano na brak kwalifikowalności, wynikający np. ze statusu dużego przedsiębiorstwa lub niedopasowania działalności firmy do tematyki dostępnych programów. Wypowiedzi tego typu pokazują, że nie wszystkie firmy mają realną możliwość skorzystania z oferowanych narzędzi wsparcia, nawet jeśli są ich świadome.

Część firm aktywnie pozyskuje środki z programów unijnych i wykorzystuje je na projekty B+R oraz ekspansję

Poniższy wykres przedstawia, w jakim stopniu firmy z sektora cyberbezpieczeństwa korzystały dotychczas z dostępnych instrumentów wsparcia publicznego – zarówno krajowego, jak i unijnego – w kontekście ekspansji rynkowej. Dane te pozwalają ocenić poziom zaangażowania branży w pozyskiwanie zewnętrznych źródeł finansowania na rozwój działalności.

Wykres 26. Czy firma korzystała wcześniej ze wsparcia krajowego lub unijnego w celu ekspansji firmy z branży cyberbezpieczeństwa? (N=197)



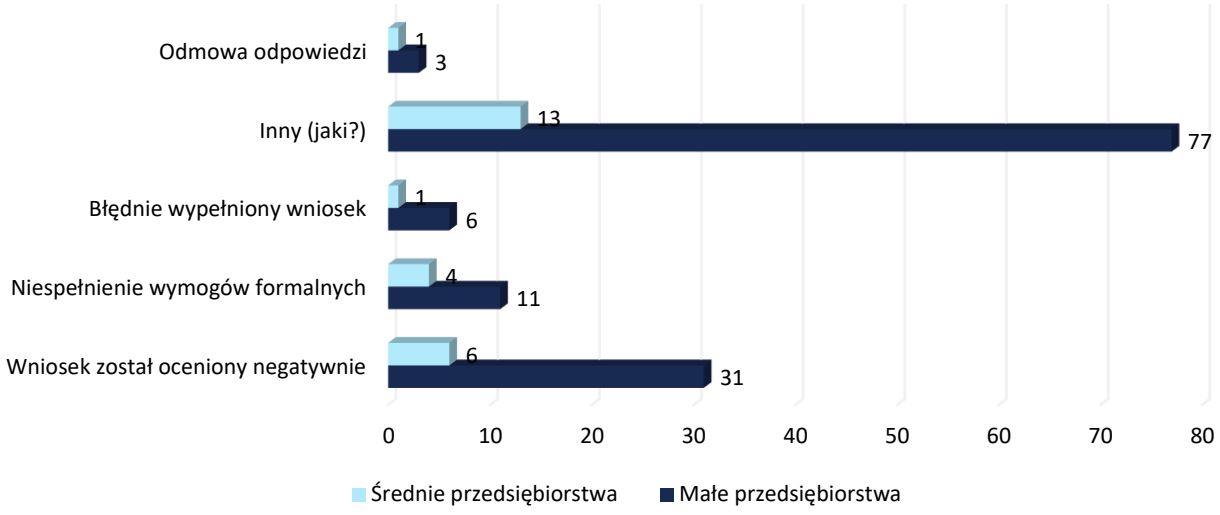
Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość firm nie korzystała dotychczas ze wsparcia krajowego ani unijnego w celu ekspansji działalności. Taką odpowiedź wskazało 143 małych oraz 28 średnich przedsiębiorstw. Z możliwości takiego wsparcia skorzystało jedynie 15 małych i 7 średnich firm.

Niski poziom wykorzystania wsparcia w kontekście ekspansji jest istotnym sygnałem dla instytucji odpowiedzialnych za projektowanie instrumentów wsparcia – wskazuje on na potrzebę intensyfikacji działań informacyjnych, uproszczenia zasad oraz uruchomienia dedykowanych mechanizmów wspierających wzrost firm działających w obszarze cyberbezpieczeństwa.

Poniższy wykres przedstawia główne powody, dla których firmy z sektora cyberbezpieczeństwa nie skorzystały z krajowego lub unijnego wsparcia na cele ekspansji rynkowej. Wyniki opierają się zarówno na odpowiedziach zamkniętych, jak i otwartych, ujawniając istotne bariery takie jak brak wiedzy o dostępnych programach, złożoność procedur, niedopasowanie oferty wsparcia do specyfiki działalności czy ograniczenia organizacyjne.

Wykres 27. Jaki był powód niekorzystania z takiej formy wsparcia (ekspansja firmy)? (N=153)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Najczęściej wskazywaną przyczyną niekorzystania ze wsparcia krajowego lub unijnego na cele ekspansji były inne, niesprecyzowane powody. Tę odpowiedź zaznaczyło 77 małych oraz 13 średnich przedsiębiorstw. Wśród barier formalnych najczęściej pojawiały się negatywne oceny złożonych wniosków (31 małych i 6 średnich firm), a także niespełnienie wymogów formalnych (11 małych i 4 średnie firmy). Sporadycznie wskazywano również na błędne wypełnienie dokumentacji aplikacyjnej (6 małych i 1 średnie przedsiębiorstwo). Odmowę udzielenia odpowiedzi zadeklarowały łącznie 4 firmy. Dane te pokazują, że choć część firm podejmowała próby pozyskania wsparcia, to często napotykały one na bariery proceduralne lub inne trudności, które uniemożliwiały skuteczne skorzystanie z dostępnych instrumentów.

Analiza odpowiedzi otwartych dotyczących powodów niekorzystania z krajowego lub unijnego wsparcia w zakresie ekspansji firm wskazuje na kilka dominujących barier, które ograniczają aktywność przedsiębiorstw w tym obszarze. Najczęściej wskazywaną przyczyną był brak wiedzy o istnieniu takich programów – respondenci deklarowali, że nie byli świadomi dostępnych możliwości, nie wiedzieli, gdzie szukać informacji, ani jakie instrumenty wsparcia mogłyby być dla nich odpowiednie. Wskazywano również, że wsparcie nie było komunikowane w sposób czytelny i przystępny dla firm z sektora MŚP.

Drugą najczęściej pojawiającą się grupą odpowiedzi były deklaracje, że firma nigdy nie składała wniosku – często bez podania konkretnej przyczyny. W wielu przypadkach wypowiedzi ograniczały się do prostego stwierdzenia: „nie aplikowaliśmy", „nie korzystaliśmy", „nie składaliśmy wniosków". Niekiedy było to uzasadniane brakiem potrzeby, brakiem planów rozwoju w tym kierunku lub skupieniem się na bieżącej działalności operacyjnej.

Istotną barierą okazało się również niedopasowanie programów do profilu działalności lub statusu firmy. Część respondentów wskazywała, że oferowane formy wsparcia nie były przeznaczone dla firm o ich charakterystyce, np. dla większych podmiotów lub firm działających w specyficznych niszach. Wskazywano na brak projektów odpowiadających potrzebom firm, zwłaszcza tych o nietypowym profilu technologicznym.

Niektórzy badani zwracali uwagę na zbyt duże obciążenie proceduralne, wskazując, że proces aplikacyjny jest czasochłonny, skomplikowany i obarczony dużym ryzykiem niepowodzenia. Pojawiały się głosy, że nawet jeśli firma byłaby zainteresowana wsparciem, nie dysponuje odpowiednią kadrą lub zasobami, by skutecznie przygotować i przeprowadzić wniosek.

Wskazywano również na brak wiedzy dotyczącej samego procesu aplikowania, w tym trudności z prawidłowym wypełnieniem dokumentacji.

Wśród respondentów pogłębionych wywiadów indywidualnych znalazły się także nieliczne, ale wyraziste opinie o charakterze ideologicznym, wyrażające niechęć do korzystania z pomocy publicznej. Niektórzy respondenci deklarowali brak zaufania do instytucji państwowych lub postrzegali mechanizmy wsparcia jako nieefektywne, nieuczciwe bądź dostępne tylko dla wybranych.

Firmy mające doświadczenie w realizacji projektów z udziałem środków unijnych wskazują na ich istotne znaczenie dla rozwoju infrastruktury badawczo-rozwojowej, budowy kompetencji i skalowania działalności, również na rynki zagraniczne. Wśród przykładów pojawiają się inwestycje w centra R&D oraz projekty o wartości kilku milionów złotych.

„[…] jedno dofinansowanie nawet obejmowało budowę naszego Centrum Badawczo- Rozwojowego i zawsze byliśmy bardzo zadowoleni, nigdy nie mieliśmy problemów na tej linii. Ja osobiście nie zgłaszam żadnych zastrzeżeń co do działania. Z różnych programów" ~ powiedział Respondent 1.

„[…] w tej chwili realizujemy projekt właśnie z funduszy europejskich. On w kwietniu się rozpoczął. Wartość projektu: 4 miliony 600 tysięcy" ~ powiedział Respondent 10.

Niektóre firmy dopiero planują aplikowanie o środki – wcześniej nie miały odpowiedniego profilu projektowego

Część firm nie korzystała jeszcze z dostępnych form wsparcia, najczęściej z powodu niedopasowania oferty programowej do ich etapu rozwoju lub modelu działania (np. brak gotowego produktu lub dominacja usług w ofercie). Wskazywano jednak zainteresowanie aktualnymi naborami i potrzebę lepszego rozeznania w dostępnych możliwościach.

„Nie, do tej pory nie, dlatego że nie mieliśmy produktu, a na usługi nie było. Teraz myślimy o tym, żeby poszukać wśród obecnych jakichś programów finansowania […]" ~ powiedział Respondent 7.

Zgłaszane są postulaty większego wsparcia sprzedaży i promocji zamiast bezpośredniego finansowania produkcji

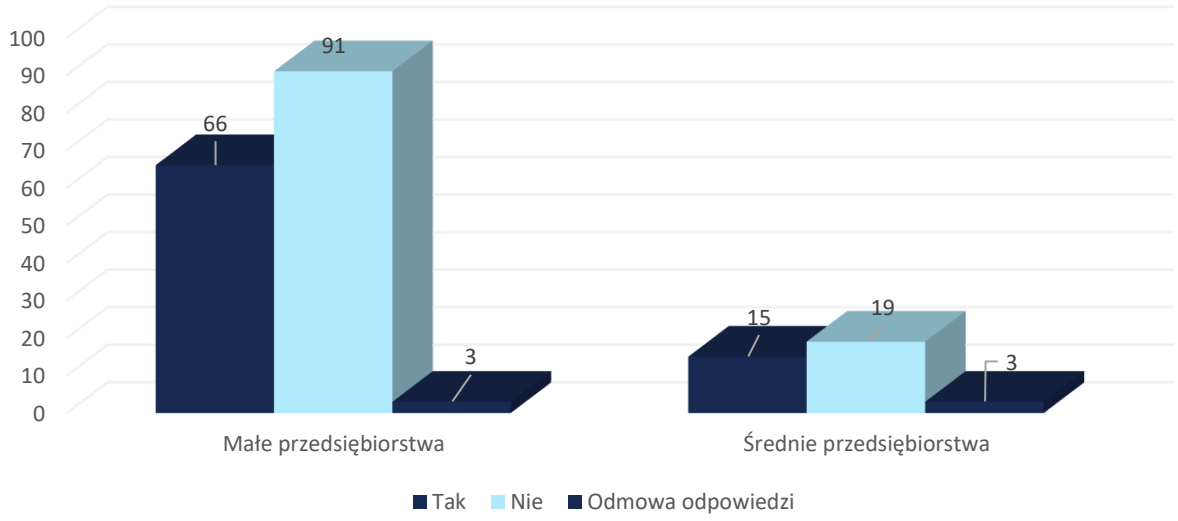
Pojawiły się głosy, że zamiast finansować same procesy wytwórcze, większy efekt prorozwojowy mogłoby przynieść wspieranie ekspansji sprzedażowej, promocji i obecności międzynarodowej. Zwracano także uwagę na konieczność lepszego celowania wsparcia – w oparciu o realny potencjał komercyjny produktów.

„[…] najlepszym źródłem finansowania jest sprzedaż. […] Będziemy dążyć do sytuacji sztucznie wykreowanych produktów, które później się będziemy zastanawiać, że mamy taki świetny produkt za 100 milionów złotych, ale nikt go nie chce kupić" ~ powiedział Respondent 13.

Środki unijne

Poniższy wykres prezentuje poziom znajomości unijnych programów wspierających rozwój innowacyjnych produktów i usług wśród firm z sektora cyberbezpieczeństwa.

Wykres 28. Czy firma zna programy unijne wspierające rozwój produktów/usług (np. Horyzont Europa, FENG, Cyfrowa Europa)? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Znajomość unijnych programów wspierających rozwój produktów i usług, takich jak Horyzont Europa, FENG czy Cyfrowa Europa, zadeklarowało łącznie 81 firm — w tym 66 małych i 15 średnich przedsiębiorstw. Większość respondentów nie zna jednak tych inicjatyw: odpowiedź „nie" wskazało 91 małych oraz 19 średnich firm. Wyniki te mogą świadczyć o potrzebie intensyfikacji działań informacyjnych i edukacyjnych dotyczących dostępnych źródeł wsparcia rozwoju innowacji.

Część firm aktywnie korzysta z dostępnych programów wsparcia (np. Digital Europe, Horyzont Europa), traktując je jako ważne źródło współfinansowania projektów innowacyjnych w obszarze R&D oraz rozwoju produktów. Dofinansowanie – nawet częściowe – pozwala im szybciej skalować inwestycje oraz budować przewagę technologiczną.

> *„Jeśli my nie mamy możliwości zrealizowania projektu w sumie własnym, ponieważ środki finansowe w firmie nie dają możliwości pokrycia tego projektu, to uzyskanie finansowania nawet w wysokości 20-50% daje tą możliwość. […], gdybyśmy nawet mieli możliwość uzyskania czy realizacji takiego projektu o wartości 100% jego wartości, to możliwość uzyskania dofinansowania w wysokości 50% daje handicap do realizowania drugiego projektu, bo wkład własny w tym momencie sumarycznie daje wartość 50% dwóch projektów, w związku z tym jesteśmy w stanie szybciej realizować nasze zamierzenia" ~ powiedział Respondent 3.*

Trudności proceduralne i ograniczone zaufanie do systemu oceny wniosków

Część respondentów wskazywała na bariery formalne i niską przejrzystość procesu aplikacyjnego jako czynnik zniechęcający do udziału w programach. Krytykowano złożoność dokumentacji, długi czas oczekiwania na transze środków oraz – w pojedynczych przypadkach – wątpliwości co do rzetelności oceny wniosków.

> *„[…] Natomiast jeżeli chodzi o wsparcie takie finansowe, stricte, ja do tych programów nie podchodziłam […] też średnio ufam, jak one są rozpatrywane, mam bardzo niski poziom zaufania do oceny tych programów, bardzo niski. […] Generalnie ja nie wierzę, że to się dzieje fair i nie wiem czy nie byłoby mi szkoda czasu się po prostu za to zabierać, bo prawdopodobieństwo wygrania oceniam bardzo nisko, ale może się mylę, nie wiem" ~ powiedział Respondent 8.*

Potrzeba lepszej koordynacji i promocji inicjatyw na poziomie centralnym

Część firm sygnalizowała ograniczoną efektywność współpracy z europejskimi strukturami koordynującymi (np. ECCC), a także niedostateczne wsparcie promocyjne dla realizowanych projektów. Brak obecności przedstawicieli instytucji finansujących na wydarzeniach branżowych ogranicza widoczność i potencjał skalowania efektów projektów.

> *„[...] brakuje jakby tego wsparcia takiego promocyjnego tych projektów […] skoro już Unia przekazuje jakieś tam miliony euro na to, żeby takie projekty realizować, no to powinna się zainteresować, żeby jak najszerzej to wypromować, a tutaj tak naprawdę współpraca na tym poziomie jest zerowa" ~ powiedział Respondent 14.*

Większość firm unika prywatnych źródeł finansowania ze względu na chęć zachowania kontroli i obawy o niedopasowanie celów

Zdecydowana część respondentów deklaruje, że nie korzystała z finansowania VC/PE, mimo że miała świadomość istnienia takiej możliwości. Kluczowymi barierami okazały się: niechęć do oddawania udziałów, przekonanie o zbyt niskiej wycenie ze strony funduszy oraz różnice w rozumieniu specyfiki branży cyberbezpieczeństwa.

> *„Nie chcieliśmy oddawać udziałów i wydawało nam się, że taka nasza wewnętrzna wycena naszej spółki będzie raczej wyższa niż wycena takiego zewnętrznego funduszu […]" ~ powiedział Respondent 10.*

> *„[…] cyberbezpieczeństwa to też zaufanie, zaufanie klientów do produktu i do marki. I tego nie da rady zbudować w tydzień, ani w rok, ani w dwa lata. […] rynek venture, teraz w dzisiejszych czasach promuje się jako taka siła wspierająca rozwój firmy z sektora cyberbezpieczeństwa, że to jest po prostu ich marketing" ~ powiedział Respondent 9.*

Współpraca z funduszami bywa rozważana, ale z dużą ostrożnością – brak doświadczenia i zaufania do rynku inwestycyjnego

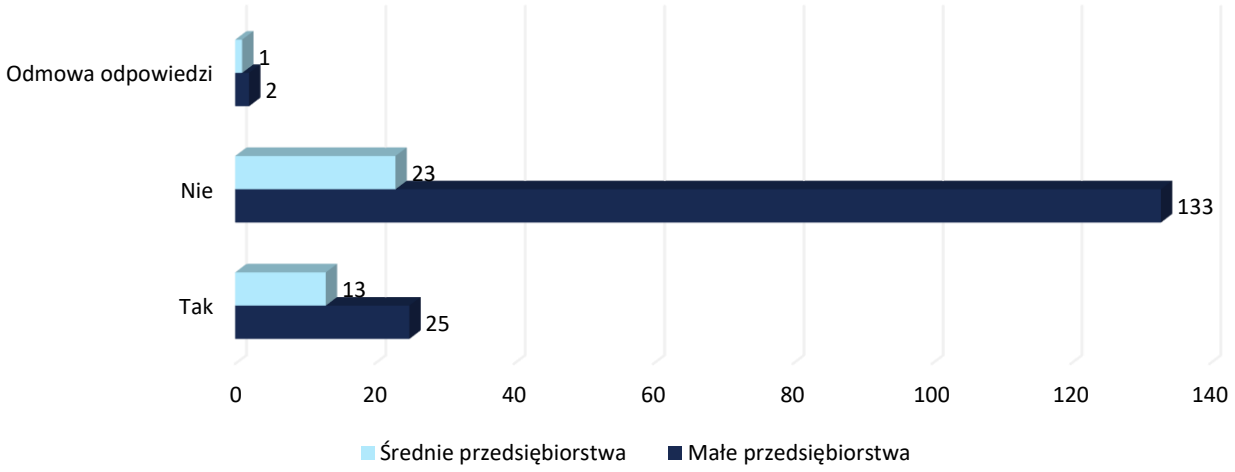
W niektórych przypadkach firmy prowadziły rozmowy z funduszami, jednak nie doszło do współpracy – najczęściej z powodu zbyt inwazyjnych warunków (np. wymóg przejęcia większościowego pakietu) lub braku przekonania co do korzyści pozafinansowych. Wśród respondentów dominuje przekonanie, że wsparcie powinno obejmować więcej niż tylko kapitał – np. realną pomoc w internacjonalizacji czy strategii.

> *„[…] dostaliśmy kilka ofert w ogóle współfinansowania działalności, ale to włączyło się zawsze z przejęciem większościowego pakietu spółki i na to się nie, znaczy nie potrzebowaliśmy, bo tak jak mówię, nie do końca nas interesuje sam kapitał" ~ powiedział Respondent 2.*

Nieliczne firmy skorzystały z finansowania prywatnego – głównie w modelu PE

Poniższy wykres prezentuje skalę korzystania z prywatnych źródeł finansowania wśród firm z branży cyberbezpieczeństwa w ciągu ostatnich trzech lat. Analiza pozwala ocenić, w jakim stopniu przedsiębiorstwa poszukiwały lub uzyskały wsparcie ze strony inwestorów prywatnych, takich jak fundusze venture capital czy private equity.

Wykres 29. Czy w ostatnich 3 latach przedsiębiorstwo otrzymało wsparcie z prywatnego finansowanie (np. venture capital, private equity)? (N=197)

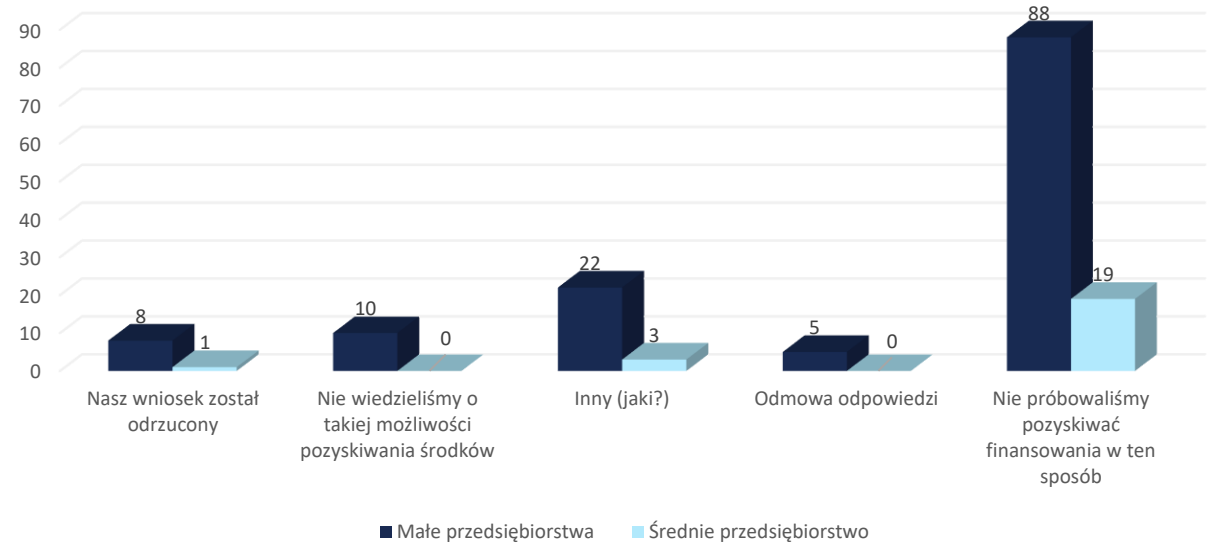


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość firm nie korzystała w ostatnich trzech latach z prywatnych źródeł finansowania, takich jak venture capital czy private equity. Brak takiego wsparcia zadeklarowało 133 małe oraz 23 średnie przedsiębiorstwa. Zewnętrzne finansowanie prywatne pozyskało łącznie 38 firm — w tym 25 małych i 13 średnich. Dane te wskazują, że choć dostęp do prywatnego kapitału jest możliwy, to nadal pozostaje relatywnie rzadką formą wsparcia rozwoju firm.

Poniżej przedstawiono z jakiego powodu firmy nie ubiegały się o takie finansowanie.

Wykres 30. Jeśli nie, jaki był tego powód? (N=156)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Najczęstszym powodem niekorzystania z prywatnych form finansowania, takich jak venture capital czy private equity, był brak prób ich pozyskania. Taką odpowiedź wskazało aż 88 małych oraz 19 średnich przedsiębiorstw. Kolejną istotną barierą była nieświadomość istnienia takiej możliwości — ten powód podało 10 małych firm. Część respondentów wskazała inne przyczyny (22 małe i 3 średnie firmy), a łącznie 9 firm (8 małych i 1 średnia) zadeklarowało, że ich wniosek został odrzucony. Dane te sugerują, że główną przeszkodą w korzystaniu z prywatnego finansowania nie są negatywne doświadczenia, lecz raczej brak inicjatywy lub wiedzy na temat dostępnych możliwości.

Na podstawie analizy odpowiedzi otwartych na pytanie o powody niekorzystania z prywatnego finansowania (np. venture capital, private equity), można wyróżnić kilka głównych kategorii przyczyn, przy czym przeważają wypowiedzi lakoniczne, odmowy odpowiedzi oraz brak szczegółowych uzasadnień.

Najczęściej wskazywanym powodem była niechęć lub brak potrzeby sięgania po zewnętrzny kapitał. Respondenci pisali wprost: „brak chęci", „brak zainteresowania", „not interested", „we didn't really need it" czy „korzystamy z własnych środków". Tego typu wypowiedzi sugerują, że część firm świadomie wybiera samofinansowanie, nie postrzegając udziału inwestorów jako niezbędnego lub pożądanego elementu rozwoju. Może to być efektem komfortowej sytuacji finansowej, przywiązania do niezależności właścicielskiej lub braku przekonania co do wartości dodanej współpracy z inwestorami.

Pojawiły się również głosy wskazujące na ryzyko i bariery negocjacyjne, np. „za duże ryzyko" czy „brak porozumienia na wczesnym etapie rozmów". Takie odpowiedzi pokazują, że nawet w przypadku firm, które rozważały współpracę z inwestorem, proces ten może zakończyć się niepowodzeniem z powodu niezgodności oczekiwań lub niepewności co do konsekwencji takiej decyzji. Z kolei odpowiedź: „specyfika produktów cyber (dual-use) wymaga zachowania ostrożności w pozyskiwaniu kapitału" sugeruje, że niektóre podmioty z branży cyberbezpieczeństwa ograniczają możliwość wejścia zewnętrznych inwestorów ze względu na wrażliwy charakter działalności.

W pozostałych przypadkach udzielono odpowiedzi ogólnych („nie korzystaliśmy z takiej formy finansowania") lub odmówiono odpowiedzi – co miało miejsce w zdecydowanej większości przypadków. Może to wskazywać na niechęć do ujawniania motywacji, brak refleksji nad tematem lub marginalne znaczenie tej formy finansowania w strategiach firm.

Pojedyncze przykłady wskazują na korzystanie z prywatnego kapitału w modelu private equity – głównie od doświadczonych inwestorów branżowych. Były to jednak wyjątki, nie dominujący trend. Wskazuje to na selektywność w podejściu do tego typu finansowania i potrzebę zbudowania większego zaufania między inwestorami a podmiotami z branży cyberbezpieczeństwa.

„Tak, Private Equity głównie, bo to jest Warsaw Equity Group, jest kapitałem prywatnym"
~ powiedział Respondent 6.

Podsumowanie:

Zebrane wyniki wskazują na pilną potrzebę uproszczenia procedur aplikacyjnych, poprawy komunikacji programów wsparcia oraz lepszego dopasowania instrumentów finansowych do realiów i potrzeb firm z sektora. Potrzebne są też działania promujące kulturę innowacji, współpracy z inwestorami oraz większe zaufanie do mechanizmów oceny i wdrażania projektów wspieranych środkami publicznymi lub prywatnymi.

Pomimo dostępności środków z różnych programów czy dofinansowań, nie wszystkie polskie firmy zajmujące się cyberbezpieczeństwem efektywnie korzystają z tego wsparcia. Powodem może być brak wiedzy o możliwościach finansowania, złożoność procedur aplikacyjnych oraz wymagania administracyjne związane z uzyskaniem dofinansowania. Dodatkowo, barierą dla niektórych firm – zwłaszcza MŚP – jest brak wystarczających zasobów organizacyjnych i eksperckich do skutecznego zarządzania projektami B+R, co sprawia, że trudniej im konkurować o fundusze z większymi podmiotami.

W przyszłości, dalszy rozwój programów wsparcia cyfryzacji i cyberbezpieczeństwa powinien uwzględniać uproszczenie procedur aplikacyjnych oraz lepszą informację i doradztwo dla przedsiębiorstw. Może to zwiększyć stopień wykorzystania dostępnych środków, przyczyniając się do dynamiczniejszego rozwoju polskiego sektora cyberbezpieczeństwa i jego konkurencyjności na arenie międzynarodowej.

Głównymi programami finansowania działalności, z których korzystają polskie firmy z przemysłu cyberbezpieczeństwa są w znacznej większości programy nastawione na projekty B+R. Uwarunkowane jest to wysoką kapitałochłonnością wymaganą do rozwoju produktu do MVP (Minimum Viable Product), mogącego konkurować na rynku. Pozostałe środki pozyskiwane ze strony firm opierają się w głównej mierze na konsorcjach tworzących wspólne projekty lub dostarczające określoną wartość rynkową dla klienta.

Programami finansowania z funduszy publicznych z których korzystały polskie MŚP z branży cyberbezpieczeństwa są m.in:

CyberSecIdent – program badawczo-rozwojowy nakierowany na podniesienie bezpieczeństwa cyberprzestrzeni RP poprzez rozwój rozwiązań sprzętowych i programistycznych. Celem projektu był rozwój nowych rozwiązań technologicznych i metodologicznych w zakresie:

- wykrywania, prezentacji i ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa,
- rozwiązań tożsamości cyfrowej, z uwzględnieniem aspektów prywatności,
- metodyki, techniki i procesów w obszarze analizy cyberbezpieczeństwa i cyfrowej tożsamości oraz ich wdrożenia.

W ramach programu założono budżet w wysokości 234 027 000 zł. Wnioskodawcą programu mogły być konsorcja naukowe w rozumieniu Ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki[25]. Finansowanie zostało podzielone na 4 konkursy w latach 2017 - 2020, natomiast monitoring i ewaluacja programu ma potrwać do 2030 roku[26]. W ramach programu CyberSecIndent dofinansowano we wskazanym okresie 23 projekty[27].

Szybka Ścieżka – innowacje cyfrowe. Fundusze z programu Szybkiej Ścieżki można było przeznaczyć na realizację badań przemysłowych, prac rozwojowych (obowiązkowych w projekcie) oraz prac przedwdrożeniowych[28]. Całościowy budżet programu wyniósł 811 301 837,90 zł. W ramach projektu dofinansowano 8 projektów nastawionych na aspekty cyberbezpieczeństwa na łączną kwotę 42 460 140,93 zł (całkowita wartość projektów wyniosła 61 653 829,34 zł).

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) to jeden z kluczowych instrumentów finansowych mających na celu wsparcie transformacji cyfrowej Polski. Program ten koncentruje się na rozwoju nowoczesnej infrastruktury cyfrowej, wzmacnianiu odporności na cyberzagrożenia oraz zwiększaniu kompetencji w obszarze cyberbezpieczeństwa zarówno w sektorze publicznym, jak i prywatnym[29]. W ramach FERC finansowane były m.in. projekty związane z rozwojem krajowych systemów zabezpieczeń, rozwiązaniami wspierającymi ochronę danych, a także narzędziami zwiększającymi odporność przedsiębiorstw i instytucji publicznych na cyberataki. Przykładem może być wsparcie dla inicjatyw rozwijających systemy wykrywania i reagowania na incydenty w cyberprzestrzeni, a także platform do monitorowania i analizowania zagrożeń w czasie rzeczywistym.

European Digital Innovation HUBs – program umożliwiający utworzenie regionalnych HUBów transformacji cyfrowej, których celem jest zwiększenie konkurencyjności małych i średnich przedsiębiorstw (MŚP) na rynku globalnym poprzez wspieranie ich w procesie wdrażania najnowszych rozwiązań cyfrowych. Połowa środków dofinansowania EDIH pochodzi z Funduszy Europejskich (DEP), druga połowa z funduszy krajowych (FENG). W Polsce powstały 4 EDIHy, które mają w swojej ofercie usługi z zakresu cyberbezpieczeństwa (w jednym przypadku cały EDIH skupiony jest na aspektach cyberbezpieczeństwa):

- **EDIH - Silesia Smart Systems** - całkowita wartość projektu - 21 424 118,47 zł. Dofinansowanie projektu z Funduszy Unijnych - 10 165 502,54 zł. W ramach projektu jeden Partner z siedmiu świadczy usługi cyberbezpieczeństwa[30].

[25] Założenia programu B+R CyberSecIdent: Cyberbezpieczeństwo i eTożsamość, aktualizacja nr 4, s. 34. Narodowe Centrum Badań i Rozwoju. [Dostęp: 11.04.2025]
[26] Tamże, s. 40-41.
[27] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s.113.
[28] Artykuł "Szybka ścieżka – Innowacje cyfrowe (1/1.1.1/2022)." Narodowe Centrum Badań i Rozwoju. [Dostęp: 11.04.2025]
[29] Informacja o programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027. [Dostęp: 18.04.2025]
[30] Artykuł "O SIlesia Smart Systems", Silesia Smart Systems. [Dostęp: 17.04. 2025]

- **EDIH - Cybersec** - całkowita wartość projektu - 15 813 409,27 zł. Dofinansowanie projektu z Funduszy Unijnych – 7 312 708,43 zł. W ramach projektu wszyscy Partnerzy (siedem podmiotów konsorcjum) świadczą usługi cyberbezpieczeństwa.
- **EDIH - Smart Secure Cities** - całkowita wartość projektu - 11 675 329,68 zł. Dofinansowanie projektu z Funduszy Unijnych - 5 569 261,20 zł. W ramach projektu jeden Partner z dziesięciu świadczy usługi cyberbezpieczeństwa.
- **EDIH - WRO4digITal** - całkowita wartość projektu - 5 055 491,06 EUR. Dofinansowanie projektu z Funduszy Unijnych - 2 527 745,49 EUR. W ramach projektu czterech z dwudziestu dwóch Partnerów świadczy usługi cyberbezpieczeństwa.

Firmy z branży cyberbezpieczeństwa korzystały również z dotacji z Regionalnych Programów Operacyjnych nastawionych w głównej mierze na działalność B+R, wśród beneficjentów można wskazać m.in:

- Digital Core Design pozyskało środki z Regionalnego Programu Operacyjnego Województwa Śląskiego na projekt: QBASS – Kwantowo odporny Blokowy Asymetryczny System Szyfrowania i autoryzacji[31].
- Perceptus pozyskał środki w ramach Regionalnego Programu Operacyjnego - Lubuskie 2020 na realizację projektu - Opracowanie bezpiecznego zarządzalnego managera haseł[32].

Patrząc na wysokość środków po jakie aplikowały firmy z branży cyberbezpieczeństwa w programach B+R można założyć, że optymalnym pułapem są środki w przedziale o 1 mln - 10 mln złotych (nie wliczając wkładu własnego wynikającego ze specyfiki danego konkursu).

Finansowanie rozwoju z wykorzystaniem środków prywatnych

Analiza danych zastanych wskazuje, że finansowanie polskich przedsiębiorstw z branży cyberbezpieczeństwa ze środków prywatnych choć wciąż rzadkie stale się zwiększa pozwalając firmom na bardziej dynamiczny rozwój działalności oraz ekspansję międzynarodową. Wśród firm, które pozyskały fundusze z środków prywatnych można wymienić m.in:

1. Sagenso (dawniej CyberStudio) - Status Starter VC zainwestował 2 mln złotych w 2021 roku w dalszy rozwój firmy[33].
2. ICsec - firma ICsec pozyskała w 2022 roku finansowanie z funduszu inwestycyjnego należącego do PKN Orlen. ORLEN VC samodzielnie objął emisję akcji firmy ICsec. Nie wskazano wysokości zainwestowanego kapitału[34].
3. Secfense - firma Secfense pozyskała w 2022 roku 2 miliony dolarów w swojej kolejnej rundzie finansowania. Wśród inwestorów są fundusze VC z Estonii, Czech, Polski oraz inwestorzy indywidualni tacy jak Tera Ventures, Presto Ventures, RKKVC oraz aniołowie biznesu[35].
4. Resquant - w 2023 roku fundusz Invento VC zainwestował 1,1 mln złotych w firmę ResQuant na dalszy rozwój organizacji[36].
5. Authologic - w 2024 roku YCombinator, Peak Capital oraz SMOK VC zainwestowały 8,2 mln dolarów w firmę Authologic, nastawiając inwestycję na zwiększenie oferty firmy na rynkach międzynarodowych[37].
6. Xopero Software - w 2024 roku Warsaw Equity Group zainwestował 20 mln zł (z możliwością rozszerzenia do 30 mln zł) w Xopero Software. Inwestycja ma przyspieszyć ekspansję zagraniczną firmy[38].
7. Fudo Security - z początkiem 2025 roku fundusz bValue zainwestował 40 mln złotych w firmę Fudo Security. Celem inwestycji jest dynamiczny rozwój działalności, w tym w szczególności, na rynku amerykańskim[39].
8. CyCommSec - firma pozyskała w 2025 roku inwestorów. Wartość inwestycji nie jest znana[40].

[31] Informacja o firmie "DCD. Company. R&D", DCD, 2025. [Dostęp: 18.04.2025]
[32] Informacja o firmie "Perceptus. Projekty Unijne", Perceptus, 2025.[Dostęp: 18.04.2025]
[33] Artykuł w portalu branżowym "Satus Starter VC zainwestował 2 miliony zł w Cybersecurity Studio". MamStartup, 2021. [Dostęp: 18.04.2025]
[34] Artykuł „ORLEN VC z pierwszą polską inwestycją bezpośrednią." PKN ORLEN, 2022. [Dostęp: 18.04.2025]
[35] Artykuł „Secfense pozyskuje 2 miliony dolarów w kolejnej rundzie inwestycyjnej." Secfense, 2022. [Dostęp: 18.04.2025]
[36] Artykuł w portalu branżowym „ResQuant z branży cybersecurity pozyskał finansowanie od Invento VC." MamStartup, 2023. [Dostęp: 18.04.2025]
[37] Artykuł w portalu branżowym „Authologic z pomocą SMOK VC pozyskuje 8,2 mln dolarów na rozwój globalnej platformy weryfikacji tożsamości cyfrowej." MyCompany Polska, 2022. [Dostęp: 18.04.2025]
[38] Artykuł w portalu branżowym „Inwestycja 20 mln zł w Xopero." CRN, 2024. [Dostęp: 18.04.2025]
[39] Artykuł w portalu branżowym „40 mln zł na cyberbezpieczeństwo od bValue. Fudo Security rozwinie skrzydła w USA." XYZ, 2025. [Dostęp: 18.04.2025]
[40] Wpis na stronie kancelarii prawnej „We advised CyCommSec." LLW Lewczuk Łyszczarek Szymczyk, 2025. [Dostęp: 18.04.2025]

Patrząc na informacje wskazywane w komunikatach odnośnie inwestycji wynika wprost, że inwestorzy chętniej inwestują w firmy, które gotowe są na skalowanie się na rynkach zagranicznych. Efektem gotowości do skalowania mogą być wspomniane wcześniej granty na działalność B+R pozwalające rozwinąć produkt.

Na polskim rynku doszło także do kilku przejęć firm z branży cyberbezpieczeństwa. Wśród przejęć można wskazać:

1. ComCERT - w 2019 roku firma Asseco Poland zakupiła 69,01% akcji spółki ComCERT stając się właścicielem wspomnianej firmy[41].
2. Famoc - w 2021 roku firma Techstep przejęła wszystkie akcji firmy Famoc za kwotę około 47 mln złotych[42].
3. Digital Fingerprints - w 2022 roku Biuro Informacji Kredytowej włączył do swojego portfolio markę Digital Fingerprints w wyniku porozumienia z poprzednim inwestorem - funduszem mAkcelerator. Wartość zakupu spółki nie jest znana[43].
4. Cryptomage - w 2023 firma Atende przejęła 20% udziałów w spółce Cryptomage. Docelowo Atende planuje przejąć 31,63% udziałów od fundusz Starfinder Capital[44].

Rola inkubatorów i akceleratorów branżowych w podnoszeniu innowacyjności i konkurencyjności polskich firm cyberbezpieczeństwa

Inkubatory i akceleratory odgrywają istotną rolę w ekosystemie innowacji, wspierając rozwój startupów i młodych firm w sektorze cyberbezpieczeństwa. Przykładem jest Krakowski Park Technologiczny, który wspólnie z AGH prowadzi polski oddział akceleratora innowacji obronnych NATO – DIANA – nazywany Fortem Kraków. Celem tego projektu jest integracja kompetencji naukowców, innowatorów oraz startupów z potrzebami sektora obronnego i wojskowego. Ponadto, w lipcu 2023 r. uruchomiony został fundusz inwestycyjny NATO - NIF, który jest pierwszym na świecie wielonarodowym funduszem kapitałowym (venture capital). DIANA oraz NIF mają posłużyć wsparciu rozwoju innowacji w obszarze nowych i przełomowych technologii (EDT), które w momencie pisania raportu zgodnie z klasyfikacją NATO obejmują m.in.: sztuczną inteligencję, technologie autonomiczne, technologie kosmiczne, technologie hipersoniczne, informatykę kwantową, czy sieci komunikacyjne nowej generacji[45].

Ponadto, Polska Agencja Rozwoju Przedsiębiorczości (PARP) uruchomiła programy takie jak Startup Booster Poland – Smart UP, mające na celu wsparcie nowych akceleratorów, które pomagają startupom w szybkim rozwoju i komercjalizacji innowacyjnych rozwiązań. Ostatni nabór do programu Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) wyłonił 17 zwycięskich projektów o łącznej wartości ponad 260 mln złotych - to programy rozwojowe i charakterze akceleracyjnym i post-akceleracyjnym oferowane przez doświadczonych operatorów[46].

Analiza opublikowanych raportów, np. Dealroom CEE 2025 potwierdza konieczność tworzenia programów wspierających ekspansję zagraniczną oraz rozwój tzw. soft-landing hubs (centra wsparcia dla startupów wchodzących na nowe rynki), które miałyby ułatwić wejście na strategiczne rynki, takie jak Stany Zjednoczone, Wielka Brytania czy Niemcy. Wśród kolejnych zaleceń mających na celu wzmocnienie innowacyjności pojawiło się również: inwestowanie w rozwój innych miast, takich jak Wrocław, Poznań czy Gdańsk, aby zrównoważyć ich postęp technologiczny z takimi miastami jak Kraków, czy Warszawa, które są głównymi ośrodkami start-upowymi. Ponadto, niezbędne są inwestycje w infrastrukturę startupową, w tym rozwój przestrzeni coworkingowych, inkubatorów i programów mentoringowych dedykowane akceleratory dla firm rozwijających technologie obronne i cyberbezpieczeństwa.

Współpraca startupów z NATO i sektorem publicznym może otworzyć nowe kanały finansowania i przyspieszyć wdrażanie innowacyjnych rozwiązań. Dodatkowo, fundusze inwestycyjne skierowane do startupów rozwijających technologie związane z bezpieczeństwem mogą wzmocnić pozycję Polski jako lidera w tym obszarze[47].

[41] Wpis w portalu branżowym „Asseco Poland kupiło 69,01% akcji spółki ComCERT." *Money.pl*, 2019. [Dostęp: 18.04.2025]
[42] Strona internetowa firmy „Techstep acquires software company Famoc, adding MMS capabilities." Techstep, 10 maja 2021. [Dostęp: 18.04.2025]
[43] Artykuł w portalu branżowym „Biuro Informacji Kredytowej inwestuje w polski fintech Digital Fingerprints." MamStartup, 2022. [Dostęp: 18.04.2025]
[44] Strona internetowa firmy „Atende inwestuje w Cryptomage – spółkę łączącą AI z cyberbezpieczeństwem sieciowym." Atende, 2023. [Dostęp: 18.04.2025]
[45] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 141-142.
[46] Artykuł w portalu branżowym „To będą nowe polskie akceleratory. PARP ogłasza wyniki Startup Booster Poland – Smart UP." MamStartup, 2024. [Dostęp: 18.04.2025]
[47] Strona internetowa PFR "Dla działań wspierających rozwój technologii o potencjale podwójnego przeznaczenia". Polski Fundusz Rozwoju S.A., 2024. [Dostęp: 18.04.2025]

Współpraca z inkubatorami i akceleratorami umożliwia polskim firmom cyberbezpieczeństwa nie tylko rozwój technologiczny, ale także zdobycie doświadczenia w zakresie zarządzania, marketingu oraz ekspansji na rynki zagraniczne, co znacząco podnosi ich konkurencyjność.

2.5. Internacjonalizacja firm

Jednym z kluczowych czynników różnicujących analizowane organizacje jest również zasięg geograficzny ich działalności. Choć część firm skupia się wyłącznie na rynku krajowym, wiele aktywnie rozwija działalność zagraniczną – zarówno w ramach Unii Europejskiej, jak i na rynkach pozaeuropejskich. Niektóre z firm wciąż koncentrują się na umacnianiu pozycji lokalnej, jednak niemal wszystkie deklarują ambicje międzynarodowe:

„Na razie polskim, ale oczywiście z planami na ekspansję" ~ powiedział Respondent 4.

Firmy realizujące sprzedaż poza Polską budują modele działalności oparte na sprzedaży eksportowej, dystrybucji międzynarodowej, uczestnictwie w zagranicznych wydarzeniach branżowych lub zakładaniu spółek zależnych. Ich obecność rynkowa często obejmuje kilkanaście krajów.

„Międzynarodowo. W tej chwili jesteśmy na około 12 rynkach, sprzedając rozwiązania decapu i disaster recovery, na zachodzie głównie rozwiązania ochrony kodu źródłowego. Europa i Stany Zjednoczone, Ameryka Południowa" ~ powiedział Respondent 6.

Kierunki ekspansji najczęściej obejmują Europę Środkowo-Wschodnią, Unię Europejską, USA, Azję Południowo-Wschodnią, Bliski Wschód oraz wybrane rynki Afryki. Dla wielu firm są to obszary mniej nasycone, bardziej chłonne na nowe technologie i relatywnie otwarte na innowacyjne podejścia.

„[…] to są rynki rozwijające się lub rynki na jakimś obszarze wzrostu. Jeszcze rynki nie tak skrajnie pokryte produktami, niezabetonowane" ~ powiedział Respondent 13.

Nie bez znaczenia pozostają także aspekty regulacyjne. Unifikacja przepisów w UE (np. RODO, NIS2) oraz powszechność zagrożeń cybernetycznych sprawiają, że firmy traktują swoje produkty jako naturalnie skalowalne.

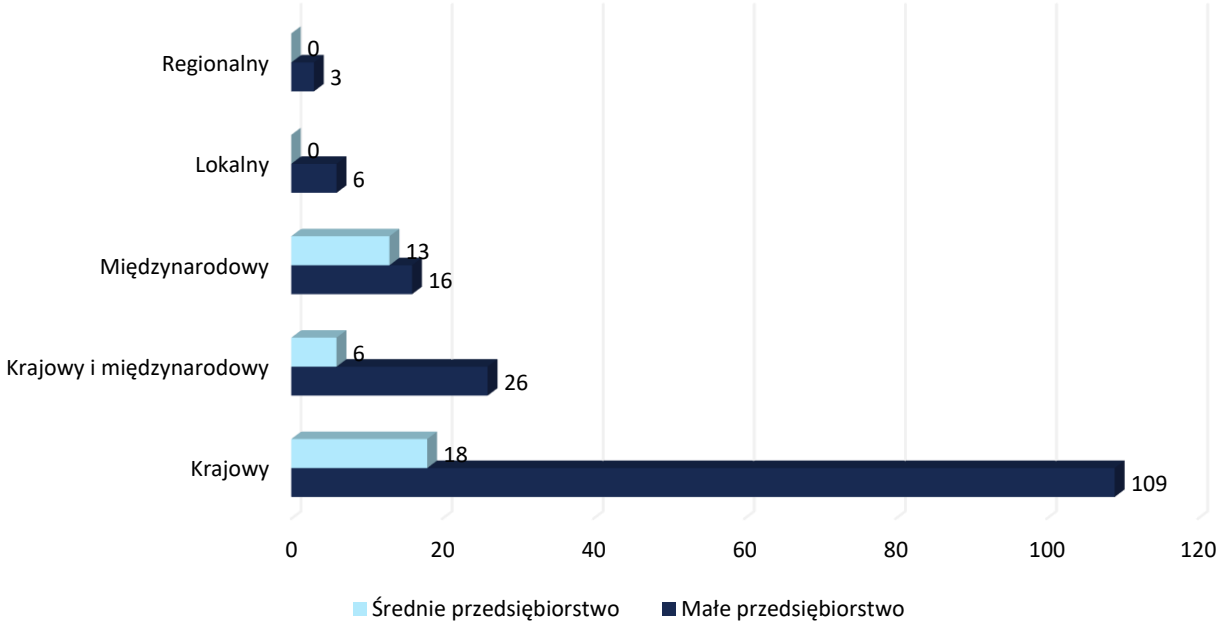
„Produkt jest cały napisany w języku angielskim […], to znaczy wspiera tylko język angielski, więc właściwie nasza ekspansja polska to jest dla nas taka trochę rozbiegówka" ~ powiedział Respondent 8.

Mimo rosnącej aktywności zagranicznej, wiele firm zmaga się z realnymi barierami wejścia na nowe rynki. Trudności obejmują złożone procedury przetargowe, różnice kulturowe i organizacyjne, a także wysokie koszty sprzedaży i promocji.

„Są kultury, które są nastawione na kulturę biznesowo- relacyjną i tam na przykład znalezienie dobrego partnera może dać szybkie przełożenie na przychody […]. A są kultury bardzo transakcyjne, gdzie znowu to będzie miało marginalne znaczenie i będą patrzyli zero- jedynkowo na te produkty" ~ powiedział Respondent 13.

Poniższy wykres przedstawia rozkład zasięgu działalności firm uczestniczących w badaniu dotyczącym cyberbezpieczeństwa. Zdecydowana większość respondentów działa głównie na rynku krajowym, choć znaczna część posiada również zasięg międzynarodowy.

Wykres 31. Jaki jest zasięg działalności Państwa firmy? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Zdecydowana większość małych przedsiębiorstw zadeklarowała działalność o zasięgu krajowym – odpowiedź tę wskazało 109 firm. Wśród średnich przedsiębiorstw również dominował zasięg krajowy, wskazany przez 18 respondentów.

Działalność o charakterze zarówno krajowym, jak i międzynarodowym prowadzi 26 małych oraz 6 średnich firm. Z kolei wyłącznie międzynarodowy zasięg zadeklarowało 16 małych i 13 średnich przedsiębiorstw.

Znacznie rzadziej wskazywano działalność lokalną (6 małych firm) oraz regionalną (3 małe firmy). Wśród średnich przedsiębiorstw nie odnotowano żadnych odpowiedzi w tych dwóch kategoriach.

Wyniki te pokazują, że choć dominującym modelem działania wśród respondentów pozostaje działalność krajowa, to istotna część firm – zarówno małych, jak i średnich – rozwija również aktywność na rynkach zagranicznych.

Analiza wskazań pokazuje, że firmy z branży cyberbezpieczeństwa najczęściej deklarują prowadzenie działalność na rynkach zachodnio- i północnoeuropejskich oraz w Stanach Zjednoczonych. Strategia internacjonalizacji polskich przedsiębiorstw opiera się na modelu sprzedaży przez kanał partnerski (w przypadku firm produktowych), oraz sprzedaży bezpośredniej (w przypadku firm usługowych). Dominującymi kierunkami są:

- Niemcy i Francja, co wiąże się z dużym popytem na usługi bezpieczeństwa IT w tych krajach;
- Wielka Brytania i Holandia, gdzie funkcjonują liczne centra technologiczne i huby startupowe;
- Szwajcaria i Czechy, atrakcyjne zarówno pod względem regulacyjnym, jak i inwestycyjnym;
- USA jako kluczowy rynek globalny dla rozwiązań cyberbezpieczeństwa;
- Kraje bałtyckie (Litwa, Łotwa) oraz Szwecja, które zyskują na znaczeniu dzięki wsparciu unijnych programów cyfryzacji.

Jednocześnie analiza Klastra #CyberMadeInPoland, wskazuje też na kierunki mniej eksponowane w ankiecie. Wśród głównych krajów, którymi zainteresowane są przedsiębiorstwa do prowadzenia działalności zagranicznej są (w kolejności od wskazywanego największego zainteresowania do najmniejszego)[48]:

1. Stany Zjednoczone (największe zainteresowanie, przy czym niewielkiej liczbie firm udało się skutecznie przeprowadzić działania sprzedażowe w USA);
2. Kraje DACH w tym głównie Niemcy;
3. Kraje Europy Środkowo Wschodniej (Rumunia, Czechy, Bułgaria, Węgry, Litwa, Łotwa);
4. Wielka Brytania;
5. Pozostałe kraje Europy Zachodniej (Włochy, Benelux, Hiszpania, Francja);
6. Kraje Skandynawskie;
7. Bałkany;
8. Kraje Postsowieckie (Uzbekistan, Kazachstan);
9. Zjednoczone Emiraty Arabskie (oraz pozostałe kraje Zatoki Perskiej);
10. Turcja;
11. Azja (Filipiny, Malezja, Mongolia);
12. Afryka;
13. Kraje Ameryki Południowej.

W celu nawiązywania relacji na rynkach zagranicznych z potencjalnymi Partnerami firmy biorą udział w głównych imprezach targowych na poszczególnych rynkach. Ponadto coraz częściej angażują się w działania wspierające koordynowane przez m.in. Ambasady RP.

Wśród form wsparcia, z których korzystały polskie przedsiębiorstwa przy ekspansji zagranicznej można wskazać:

- Grant “Go to Brand” realizowany przez PARP. Program Go to Brand skupiał się na promocji polskich marek produktowych firm z sektora MŚP na rynkach zagranicznych. Dofinansowanie można było wykorzystać m.in. na zakup stoiska lub miejsca na zagranicznych targach, podróży służbowych, uczestnictwa w konferencjach i seminariach oraz działań marketingowych[49].
- Program “Polskie Mosty Technologiczne” - to program Polskiej Agencji Inwestycji i Handlu, którego celem jest wsparcie promocji oraz internacjonalizacji innowacyjnych przedsiębiorstw. W ramach programu eksperci PAIH oferują usługi doradczo warsztatowe wspierające budowę strategii ekspansji zagranicznej na wybrany rynek[50].
- Udział w stoiskach narodowych organizowanych przez PAIH.
- Udział w stoiskach regionalnych organizowanych przez poszczególne Województwa.
- Udział w misjach handlowych realizowanych przez lokalne Zagraniczne Biura Handlowe.

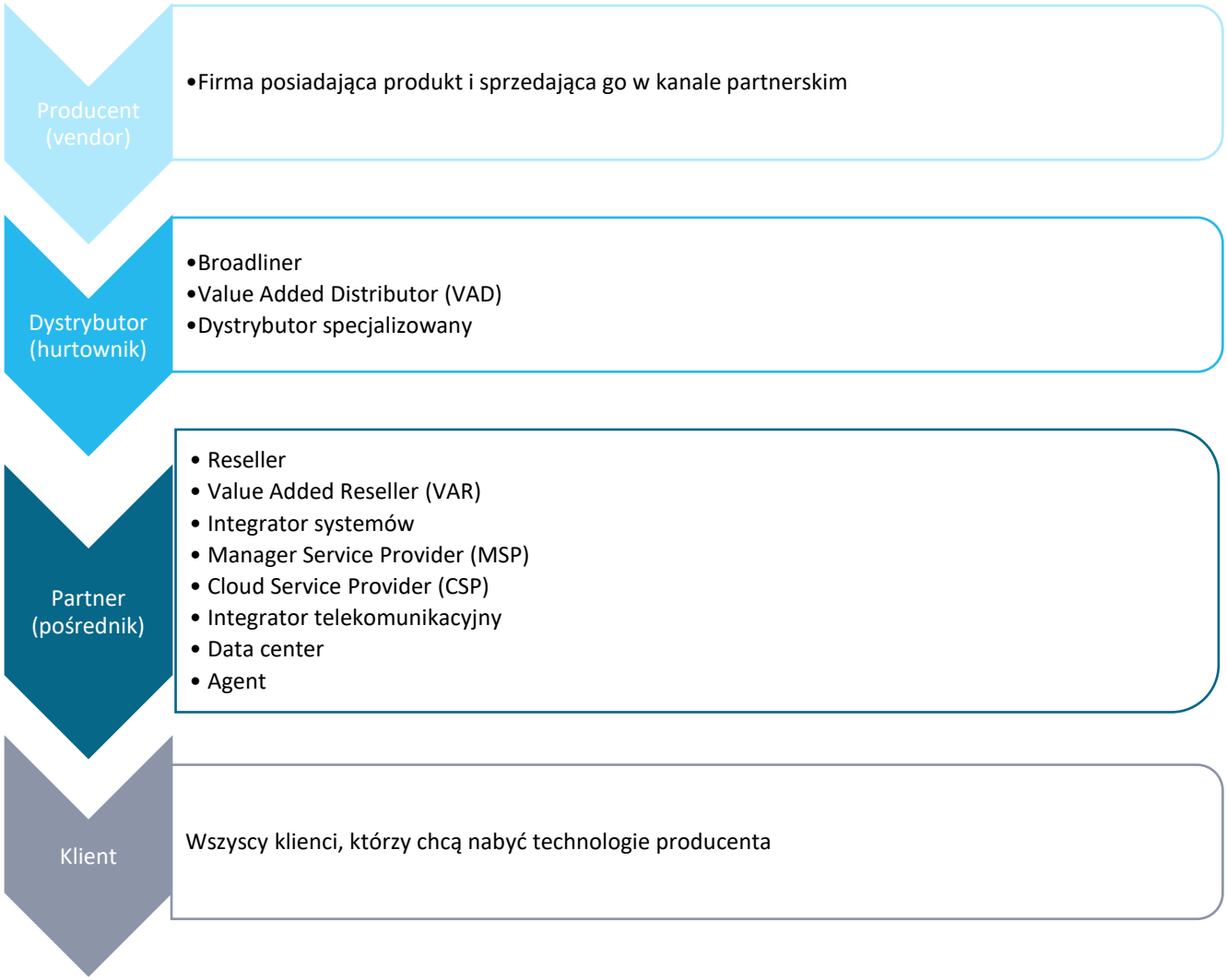
Cyberprzestrzeń nie ma granic, dlatego sprzedaż i implementacja rozwiązań z obszaru cyberbezpieczeństwa nie napotyka wielkich trudności. Zwykle sprzedaż zagraniczna wymaga dostosowania do lokalnych regulacji, choć w przypadku sprzedaży w ramach UE przepisy z zakresu cyberbezpieczeństwa są zwykle ujednolicone (jako przykład można wskazać tutaj transpozycję dyrektywy NIS2 w UE, której główne zapisy są niezmienne, natomiast każdy kraj członkowski może rozszerzyć zapisy dyrektywy tworząc konieczność zapoznania się z nimi oraz dostosowania przez firmę). **Największą barierą sprzedaży zagranicznej jest znalezienie odpowiedniego partnera (integratora, dystrybutora lub resellera) oraz dostosowania produktu lub usługi do lokalnych uwarunkowań prawnych oraz języka** (jeśli jest to wymagane).

[48] Na podstawie wewnętrznych materiałów Klastra #CyberMadeInPoland.
[49] Strona internetowa PARP “Go to Brand.” Polska Agencja Rozwoju Przedsiębiorczości (PARP). [Dostęp: 18.04.2025]
[50] Strona internetowa PAIH “O projekcie – Polskie Mosty Technologiczne.” Polska Agencja Inwestycji i Handlu (PAIH). [Dostęp: 18.04.2025]

2.6. Analiza powiązań kooperacyjnych

Kooperacja na polskim rynku wśród firm odbywa się głównie poprzez tworzenie kanałów partnerskich, integrację produktów oraz wzajemną sprzedaż usług. Kooperacja poprzez kanały partnerskie odbywa się na standardowych zasadach, vendor poszukuje dystrybutora lub Partnera, którzy w dalszej kolejności docierają z jego rozwiązaniem do szerokiego rynku klientów.

Rysunek 1. Powiązania kooperacyjne



Źródło: Analizy IBC.

Integracja produktów firm polega na wzajemnym dostosowywaniu oprogramowania z innym produktem, co przekłada się na komplementarność w działaniu u klienta oraz zwiększa możliwości sprzedażowe dla obu firm (firmy mogą wtedy polecać rozwiązania swoim klientom jako produkt komplementarny). Ponadto integratorzy realizujący szeroko zakrojone projekty posiadają większy wybór możliwości pod kątem poszczególnych wdrożeń.

Kolejną praktyką działań kooperacyjnych jest wzajemna sprzedaż usług. W momencie, kiedy firma nie posiada kompetencji w którymś aspekcie, którego wymaga klient, poszukuje stosownego Partnera do ich realizacji. Przykładem mogą być tutaj kancelarie prawne, świadczące usługi z zakresu zgodności z poszczególnymi przepisami prawnymi. Widząc niedociągnięcia bądź potrzeby klienta mogą bezpośrednio polecić Partnera, który jest w stanie zrealizować poszczególną usługę.

Rozdział 3

Bariery i potrzeby rozwojowe polskich małych i średnich firm sektora cyberbezpieczeństwa

3.1. Bariery wzrostu – finansowe, organizacyjne, regulacyjne

Sektor cyberbezpieczeństwa w Polsce rozwija się w szybkim tempie, a jego kierunki rozwoju kształtowane są przez postęp technologiczny oraz zmieniający się kontekst geopolityczny. Na podstawie przeprowadzonych badań jakościowych i ilościowych zidentyfikowano kluczowe trendy oraz potrzeby, które będą miały istotny wpływ na funkcjonowanie i transformację branży w nadchodzących latach.

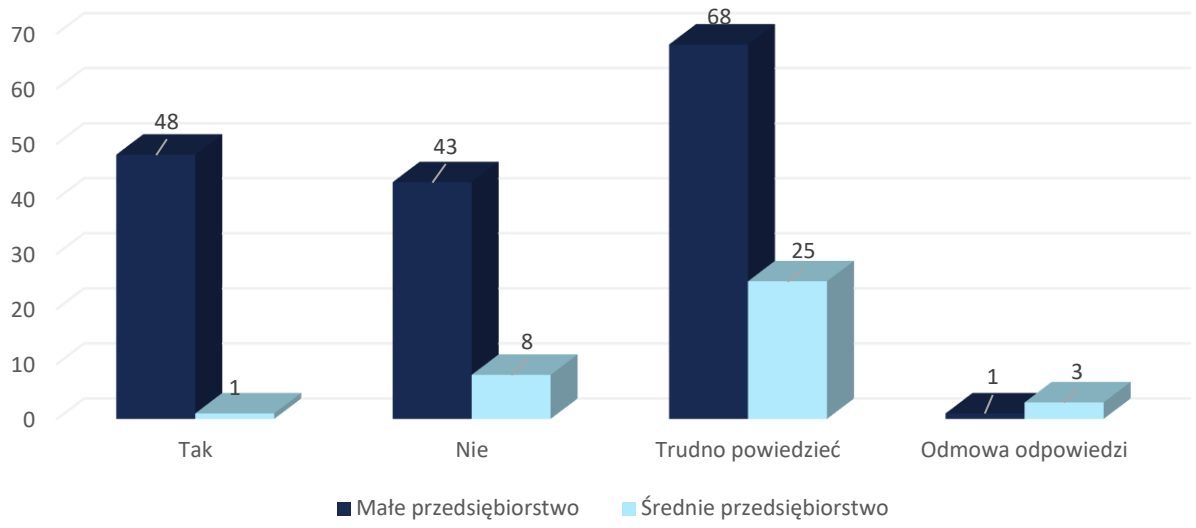
Badanie ujawniło istotne bariery rozwoju: niską świadomość rynku, trudności sprzedaży rozwiązań niewidocznych dla użytkownika, brak systemowego wsparcia ekspansji zagranicznej oraz dominację globalnych marek. Dodatkowe wyzwania to braki kadrowe, niedobór kompetencji sprzedażowych, niski poziom współpracy branżowej i nieprzejrzyste otoczenie prawno-podatkowe.

Aby w pełni wykorzystać potencjał polskiego sektora cyberbezpieczeństwa, potrzebne są działania systemowe łączące edukację, wsparcie legislacyjne, promocję i profesjonalizację firm. Tylko zintegrowane wysiłki wszystkich interesariuszy mogą stworzyć silny, odporny i innowacyjny ekosystem bezpieczeństwa cyfrowego.

Poniższy wykres prezentuje najczęściej wskazywane przyczyny rezygnacji z planów ekspansji przez firmy działające w sektorze cyberbezpieczeństwa. Analiza obejmuje zarówno bariery rynkowe i finansowe, jak również czynniki organizacyjne i strategiczne. Dane pochodzą z odpowiedzi zamkniętych oraz otwartych, co pozwala uchwycić zróżnicowane motywacje i ograniczenia wpływające na decyzje firm dotyczące kierunków rozwoju.

Wykres przedstawia, w jakim stopniu firmy z sektora cyberbezpieczeństwa identyfikują istnienie barier rozwojowych, które mogą ograniczać ich dalszy wzrost.

Wykres 32. Czy Państwa firma ma bariery rozwojowe? (N=197)



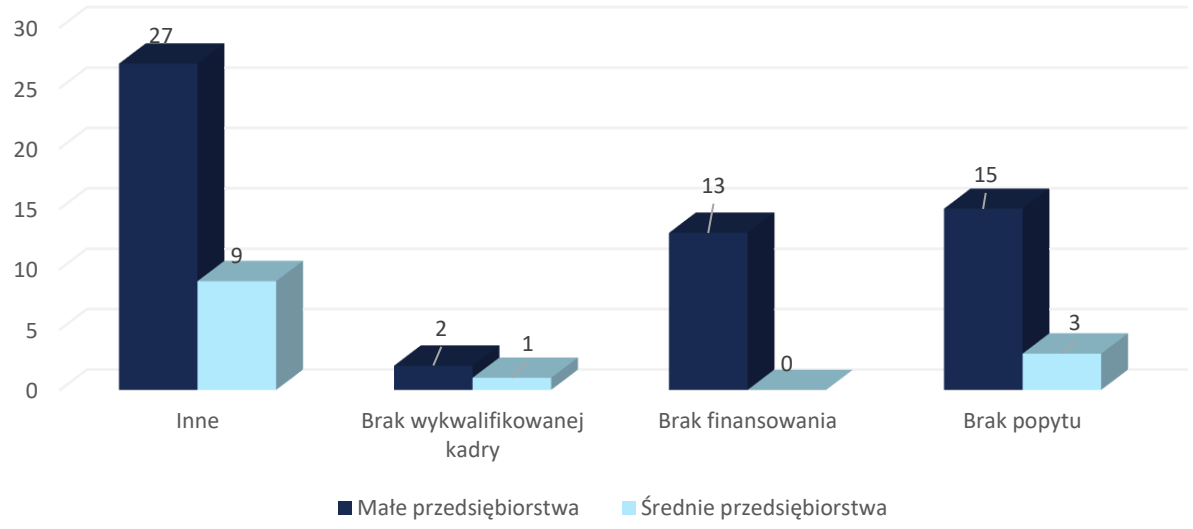
Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Wśród respondentów najczęściej pojawiającą się odpowiedzią na pytanie o występowanie barier rozwojowych było „trudno powiedzieć". Takiej odpowiedzi udzieliło aż 68 małych oraz 25 średnich przedsiębiorstw. Istnienie barier rozwojowych potwierdziło 48 małych firm, natomiast wśród średnich tylko jedna wskazała na ich obecność. Brak barier zadeklarowało łącznie 51 firm — 43 małych i 8 średnich. Nieliczni respondenci odmówili udzielenia odpowiedzi (1 małe i 3 średnie

przedsiębiorstwa). Dane te mogą sugerować, że wiele firm nie ma jednoznacznej opinii na temat przeszkód w rozwoju, co może wynikać z braku systematycznej analizy barier lub z ich trudnej identyfikowalności.

Firmy, które nie planują rozszerzenia działalności zostały poproszone o doprecyzowanie powodu takiego stanu rzeczy.

Wykres 33. Jeśli nie planują Państwo rozszerzenia działalności, co jest głównym powodem? (N=70)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

18 firm zadeklarowało, że brak popytu na oferowane produkty lub usługi wstrzymuje ich w rozszerzeniu działalności. Oznacza to, że znaczna część podmiotów dostrzega ograniczenia rynkowe, które uniemożliwiają im efektywną ekspansję — brak zapotrzebowania może wynikać z nasycenia rynku, specyfiki branży lub barier wejścia na nowe segmenty.

13 firm zadeklarowało brak finansowania, co wskazuje na realne ograniczenia kapitałowe i trudności w pozyskaniu środków niezbędnych do rozwoju. Ograniczony dostęp do zewnętrznego finansowania (publicznego lub prywatnego) może skutecznie blokować inwestycje rozwojowe, nawet jeśli firma posiada odpowiedni potencjał i know-how.

Dla 3 firm barierą był brak wykwalifikowanego personelu, co podkreśla problem niedoboru kadr, zwłaszcza w sektorach wymagających wysokospecjalistycznych kompetencji, takich jak cyberbezpieczeństwo czy nowe technologie.

Analiza otwartych odpowiedzi udzielonych w kategorii „Inne (jakie?)" na pytanie o powody nieplanowania rozszerzenia działalności pokazuje, że wiele firm nie odrzuca rozwoju jako takiego, lecz realizuje alternatywne strategie wzrostu lub koncentruje się na utrwaleniu i optymalizacji bieżącej działalności.

Część respondentów wskazała na skupienie się na obecnym modelu biznesowym, jego skalowaniu i doskonaleniu. Wypowiedzi takie jak „koncentracja na wdrażanym modelu biznesowym", „udoskonalanie świadczonych usług" czy „skalowanie dotychczasowego modelu" sugerują, że firmy podejmują działania rozwojowe, lecz niekoniecznie w formie terytorialnej lub operacyjnej ekspansji.

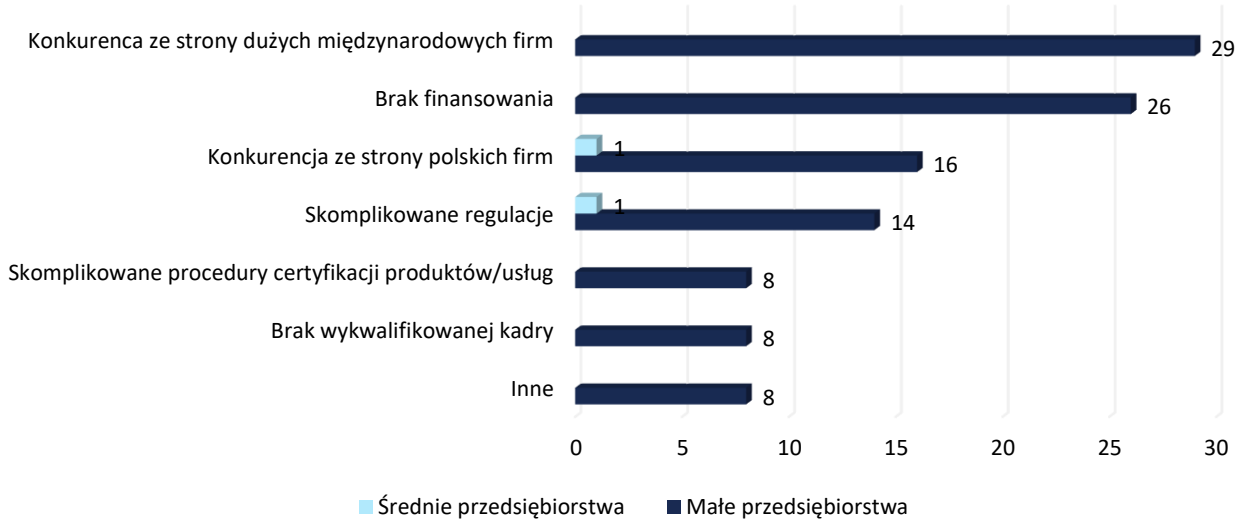
Wielokrotnie pojawiała się również motywacja związana z utrzymaniem obecnego rozmiaru firmy, który postrzegany jest jako optymalny – „rozmiar firmy w obecnym kształcie jest dla nas wystarczający", „rozwijamy organizację w obecnym wymiarze". Tego typu odpowiedzi świadczą o świadomym wyborze strategii stabilizacji i ostrożnego zarządzania ryzykiem.

Inni respondenci deklarowali priorytetyzację działań inwestycyjnych o innym charakterze, jak np. „inne plany inwestycyjne", „dodatkowe źródło dochodu" czy „reorganizacja", co może oznaczać, że środki i zasoby są skierowane na działania modernizacyjne, restrukturyzacyjne lub dywersyfikacyjne, a nie na ekspansję geograficzną lub produktową.

Pojawiły się też pojedyncze odpowiedzi wskazujące na ograniczenia zewnętrzne, np. „brak terenów do wybudowania sieci telekomunikacyjnych. Dublowanie sieci jest nieekonomiczne”, co pokazuje, że w niektórych branżach rozwój może być ograniczony nie przez brak woli, ale przez warunki rynkowe lub infrastrukturalne.

Poniższy wykres przedstawia najczęściej wskazywane bariery, które utrudniają rozwój firm działających w sektorze cyberbezpieczeństwa. Respondenci identyfikowali zarówno ograniczenia zewnętrzne (takie jak konkurencja czy regulacje), jak i wewnętrzne (np. brak finansowania, kadr czy kompetencji).

Wykres 34. Jakie bariery rozwoju Państwa firmy są obecnie największym wyzwaniem? (N=49)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Wśród barier rozwojowych najczęściej wskazywanym wyzwaniem była konkurencja ze strony dużych międzynarodowych firm, na ten problem zwróciło uwagę 29 respondentów. Firmy z sektora MŚP mają trudności z rywalizacją z globalnymi graczami, dysponującymi większymi zasobami, marką i skalą działania.

Na drugim miejscu znalazł się brak finansowania – 26 wskazań. Przedsiębiorstwa często napotykają trudności w pozyskaniu kapitału na rozwój, innowacje czy ekspansję, zarówno w formie środków publicznych, jak i prywatnych.

Konkurencję ze strony polskich firm jako barierę wskazało 17 firm. Może to świadczyć o wysokim nasyceniu rynku, presji cenowej lub rywalizacji w niszowych segmentach.

Skomplikowane regulacje stanowią wyzwanie dla 15 respondentów. Firmy postrzegają przepisy jako nieprzejrzyste, zmienne lub niedostosowane do rzeczywistości rynkowej, co utrudnia planowanie i wdrażanie działań rozwojowych.

Na dalszych miejscach znalazły się:

- Skomplikowane procedury certyfikacji produktów/usług – 9 wskazań,
- Brak wykwalifikowanej kadry – 8 wskazań,
- Inne czynniki – również 8 wskazań, obejmujące m.in. wysokie koszty działalności (w tym podatki i Polski Ład), brak specjalistów – zwłaszcza ds. sprzedaży, problemy z finansowaniem projektów B+R (konieczność wkładu własnego) oraz opóźnienia i niespójność regulacji. Dodatkowo zwrócono uwagę na niską świadomość instytucji publicznych w zakresie cyberbezpieczeństwa oraz ograniczony rozwój krajowych technologii infrastrukturalnych. Barierami są także braki kompetencyjne wewnątrz zespołów zarządzających i wysokie koszty skutecznych rozwiązań.

Niska świadomość rynku i trudność sprzedaży „niewidzialnego produktu”

Jednym z najczęściej przywoływanych przez respondentów problemów jest wciąż zbyt niska świadomość rynku – zarówno wśród małych, jak i dużych przedsiębiorstw – dotycząca skali zagrożeń cyfrowych oraz realnej wartości inwestycji w cyberbezpieczeństwo. Dla wielu klientów ochrona danych i systemów IT jest postrzegana bardziej jako niepotrzebny koszt niż jako istotny element strategii biznesowej. W szczególności dotyczy to organizacji spoza sektorów regulowanych, dla których certyfikacja lub wdrażanie zaawansowanych rozwiązań bezpieczeństwa nie generuje bezpośredniego zysku, przez co schodzi na dalszy plan. Jak ujął to jeden z respondentów:

> *„[…] to nie jest żaden benefit posiadanie certyfikacji cyberbezpieczeństwa. Więc dla nas, myślę, że takim głównym takim blokerem […] to jest właśnie wskazanie, jak cybersecurity może być, jakim może być benefitem, bo benefit pod tytułem nie bycie ofiarą ataku się po prostu nie sprzedaje” ~ powiedział Respondent 14.*

Tego rodzaju percepcja znacząco utrudnia komercjalizację rozwiązań oraz zmniejsza skłonność organizacji do inwestycji w profilaktykę i długofalowe bezpieczeństwo.

W wielu korporacjach działy cyberbezpieczeństwa nie dysponują własnym budżetem ani niezależnością decyzyjną. Wydatki na bezpieczeństwo są realizowane tylko wtedy, gdy są prawnie wymagane.

> *„Jeśli korporacja w Polsce, czyli międzynarodowa firma […], w ogóle ma dział cyberbezpieczeństwa, to ten dział cyberbezpieczeństwa bardzo rzadko ma własny budżet” ~ powiedział Respondent 5.*

Takie podejście nie tylko ogranicza popyt na zaawansowane rozwiązania, ale też utrwala przekonanie, że bezpieczeństwo cyfrowe jest kosztem, a nie inwestycją.

Presja ze strony globalnej konkurencji dodatkowo pogłębia trudności. Firmy z USA i Azji, wspierane kapitałowo i politycznie przez swoje państwa, dominują nie tylko na rynkach światowych, ale coraz częściej również w samej Unii Europejskiej. Lokalni dostawcy mają ograniczony dostęp do przetargów i budżetów publicznych. Jeden z przedsiębiorców trafnie podsumował obawy całej branży:

> *„Więc na końcu dnia może takich instytucjach publicznych, europejskich o bezpieczeństwo częściowo dbają o rozwiązania produkowane w Indiach, sprzedawane przez amerykańskie podmioty i nie jest to wydaje mi się idealne, choć nie zawsze tak oczywiście jest, […], ale żebyśmy jako organizacja mogli być tak samo efektywni na świecie, tak jak duże amerykańskie spółki, no to po prostu musimy mieć dużo więcej klientów, więcej przychodów, żebyśmy mogli inwestować w rozbudowanie tej naszej prezentacji na świecie […]” ~ powiedział Respondent 10.*

Pułapka stagnacji i bariery innowacyjności

Wyzwaniem pozostaje także tempo zmian technologicznych. Cyberzagrożenia ewoluują błyskawicznie, co wymusza stałą aktualizację rozwiązań i inwestowanie w badania. Mniejsze firmy, nie dysponując wystarczającymi zasobami, mogą nie nadążać za tym rytmem, co prowadzi do marginalizacji.

> *„[…] zagrożeniem może być szybkie tempo zmian ewolucyjnych i ewolucji samych cyberzagrożeń, ponieważ wymaga to ciągłych inwestycji i nakładów finansowych w research and development. […] konkurencja jest też zdrowa dla rynku” ~ powiedział Respondent 11.*

Ryzyko stagnacji jest czynnikiem, który zagraża dalszemu rozwojowi branży. W odróżnieniu od wielu innych sektorów, cyberbezpieczeństwo nie toleruje bezruchu. Jak ujął to jeden z przedstawicieli firm: „To nie jest branża, w której można się zatrzymać. Jak nie będziemy się rozwijać, to za chwilę wypchnie nas konkurencja.” Brak inwestycji w badania, rozwój i nieustanne doskonalenie produktów mogą prowadzić do szybkiej utraty pozycji rynkowej – nawet w przypadku firm, które wcześniej odniosły sukces.

Brak systemowego wsparcia i ograniczone możliwości ekspansji

Drugim istotnym ograniczeniem jest brak instytucjonalnego wsparcia dla firm planujących ekspansję zagraniczną. W odróżnieniu od takich krajów jak USA czy Chiny, gdzie eksport technologii cyberbezpieczeństwa jest elementem polityki państwowej (obejmującym finansowanie, lobbying, wsparcie legislacyjne czy obecność na rynkach strategicznych), w Polsce przedsiębiorstwa pozostawione są same sobie. Brakuje spójnej infrastruktury eksportowej, wsparcia w zakresie certyfikacji międzynarodowej, obecności w zagranicznych projektach publicznych czy doradztwa strategicznego.

> *„[…] barierą jest przede wszystkim możliwość pozyskiwania finansowania na rozwój danej technologii […] popatrzmy sobie na Stany Zjednoczone i ich ekspansję międzynarodową […] Ta ekspansja międzynarodowa nie byłaby możliwa bez zapewnienia wsparcia czy finansowania, czy umożliwienia tej ekspansji bez możliwości rządowych […] jest duża rola rządu […] ta rola jest niezbędna" ~ powiedział Respondent 3.*

Nawet firmy dysponujące silnym zapleczem technologicznym często nie są w stanie zdobywać dużych kontraktów zagranicznych, ponieważ decyzje zakupowe podejmowane są poza Polską – w centralach międzynarodowych klientów.

Krytycznym problemem jest brak spójnego systemu wsparcia dla firm chcących rozwijać się międzynarodowo. Przedsiębiorcy zwracają uwagę, że mimo formalnego zaproszenia do udziału w zagranicznych wydarzeniach, brak jest realnych instrumentów, które umożliwiałyby efektywne uczestnictwo.

> *„[…] PAIH, który zaprasza właśnie już nas nawet bezpośrednio, jesteśmy gdzieś tam na listach kontaktowych PAIH-u, zaprasza nas tak wybiórczo, pojedynczo na poszczególne wydarzenia branżowe, na targi, natomiast to nie wiąże się z finansowaniem. […] dla nas akurat barierą jest rzeczywiście wejście ze względu na to, że nie ma tych kosztów właśnie dojazdu kosztów zakwaterowania, a więc fajnie by było jakby tutaj gdzieś te środki się pojawiły" ~ powiedział Respondent 4.*

W tej sytuacji polskie firmy, nawet jeśli oferują konkurencyjne rozwiązania technologiczne, często przegrywają z amerykańskimi czy azjatyckimi podmiotami, które działają w znacznie korzystniejszych warunkach finansowych i regulacyjnych. Firmy potrzebują nie tylko okazjonalnych wyjazdów na wydarzenia, ale całych programów misji gospodarczych, szkoleń z zakresu eksportu oraz wsparcia w zakresie marketingu międzynarodowego. Bez takich działań szanse konkurowania z globalnymi gigantami są ograniczone – nawet przy najlepszej technologii.

Przewaga globalnych graczy – dominacja zagranicznych marek

Polski rynek zdominowany jest przez duże, rozpoznawalne podmioty – głównie z USA – które posiadają nie tylko znacznie większe zasoby kapitałowe i kadrowe, ale również międzynarodową renomę potwierdzoną obecnością w raportach branżowych. Firmy te cieszą się wysokim poziomem zaufania nawet w Polsce, co powoduje, że krajowi dostawcy często są ignorowani, mimo porównywalnych (lub lepszych) kompetencji. Jak wskazuje jeden z respondentów:

> *„[…] jest bardzo duża konkurencja amerykańskich spółek i bardzo często nie dochodzimy do głosu. […] tam, gdzie się naprawdę pojawiają bardzo duże pieniądze, to mamy we własnym kraju ciężej, dlatego, że my tego problemu nie mamy za granicą. Za granicą jesteśmy spółką międzynarodową i chociażby we wspomnianej Ruandzie realizujemy bardzo strategiczny projekt dla obrony w Polsce chcemy zyskać to myślę, żeby było to szalenie trudne." ~ powiedział Respondent 2.*

Problemem jest także brak widoczności medialnej i marketingowej polskich firm, które rzadko trafiają do branżowych raportów czy porównań, przez co nie są brane pod uwagę w procesach zakupowych – nawet na rodzimym rynku.

Wielkość firmy a skala wyzwań – „gracz za mały, by grać globalnie"

Jedną z najbardziej zauważalnych i najczęściej wskazywanych barier rozwoju jest niewielka skala działalności wielu firm funkcjonujących na rynku cyberbezpieczeństwa w Polsce. Przede wszystkim dotyczy to młodych, innowacyjnych podmiotów, takich jak start-upy oraz wyspecjalizowane mikro i małe przedsiębiorstwa, które ze względu na ograniczone

zasoby finansowe, kadrowe oraz organizacyjne nie są w stanie konkurować na równi z dużymi graczami – zarówno na rynku krajowym, jak i międzynarodowym.

Firmy te borykają się z brakiem środków na niezbędne certyfikacje, rozwój infrastruktury marketingowej, uczestnictwo w targach i konferencjach branżowych oraz prowadzenie działań lobbingowych i sprzedażowych poza granicami Polski.

> *„Start-upów w zasadzie w Polsce nie ma […], dlaczego nie ma produktów? Dlatego, że jest to […] ciężkie, bo do tych wszystkich nudnych rzeczy PR-owo-biznesowych trzeba dorzucić stworzenie produktu, a stworzenie produktu co do zasady zawsze jest obarczone pomyłką o 50%, czyli jeśli założyliśmy, że coś nam zajmie pół roku, to zajmie rok, jeśli założyliśmy, że coś będzie kosztowało pół miliona, to będzie kosztowało milion itd" ~ powiedział Respondent 5.*

> *„Jeśli chodzi o rozwój produktu, to tutaj jest poprzeczka bardzo wysoko postawiona, bo cyberbezpieczeństwo to są najdrożsi fachowcy na rynku, więc projekty R&D to tak naprawdę, tu bym nie stawiała jakichś limitów. Na pewno musi być duża otwartość, natomiast te programy dotacje na certyfikację to tak minimum 1,5-2 mln zł na firmę, żeby to zrobić tak bardzo profesjonalnie" ~ powiedział Respondent 4.*

Podczas gdy duże firmy z kapitałem i zasobami potrafią sprawnie dostosować się do zmian regulacyjnych (np. dyrektywy NIS2 czy rozporządzenia CRA), mniejsze podmioty często nie nadążają za tempem zmian legislacyjnych, co realnie grozi ich wykluczeniem z łańcuchów dostaw. W praktyce prowadzi to do marginalizacji innowacyjnych, ale niedofinansowanych rozwiązań.

Lokalizacja: Polska jako peryferie decyzyjne

Kolejną istotną barierą rozwojową jest lokalizacja geograficzna – nie tylko w sensie fizycznego położenia, ale przede wszystkim w kontekście systemu decyzyjnego dominującego na europejskim rynku technologicznym. Polskie firmy, mimo że operują w obrębie wspólnego rynku Unii Europejskiej, bardzo często wskazują, że realne decyzje zakupowe, przetargowe i inwestycyjne zapadają w zagranicznych centralach korporacyjnych – głównie w Europie Zachodniej.

Ten układ sił sprawia, że lokalne oddziały klientów działających w Polsce nie mają decyzyjności, a wejście do globalnych struktur przetargowych wymaga ogromnych nakładów pracy, kontaktów, obecności i środków finansowych.

> *„[…] Nie możemy pójść do oddziału jakiegoś banku w Polsce, bo oddział to oddział, ale on ma swoją centralę, która jest we Francji, w Portugalii, w jakiejś Norwegii. I tutaj mamy mało takich firm, które mają tutaj swoje centra decyzyjne. I dlatego Państwo nas powinno wesprzeć w tej ekspansji międzynarodowej, bo my sami tutaj po prostu mamy bardzo ograniczone możliwości […]" ~ powiedział Respondent 8.*

Sytuację dodatkowo pogarsza fakt, że wiele postępowań przetargowych prowadzonych lokalnie w Polsce konstruowane jest w sposób, który wyklucza mniejsze podmioty z udziału. Kryteria bywają nieproporcjonalnie wyśrubowane – tak, jakby były projektowane z myślą o dostawcach klasy enterprise, co znacznie utrudnia firmom z sektora MŚP realny udział w rynku zamówień publicznych.

> *„Pojawia się postępowanie na system klasy naszej, gdzie my jesteśmy w zasadzie wykluczeni, bo zapisy wyglądają jakby ktoś konstruował rakietę kosmiczną i trzy razy był na Marsie i mniej więcej takiego statku kosmicznego oczekiwał. […] na naszym rodzinnym rynku my musimy trochę udowadniać, że nie jesteśmy wielbłądem, mimo tego, że mamy bardzo silne referencje poza Polską, […]" ~ powiedział Respondent 2.*

Braki kadrowe i niedobór specjalistów

W sektorze cyberbezpieczeństwa coraz bardziej odczuwalny staje się deficyt wykwalifikowanych specjalistów. Pomimo że Polska posiada silny sektor IT, to w wąskiej dziedzinie bezpieczeństwa cyfrowego brakuje ekspertów o wysokim poziomie

technicznego przygotowania i zdolnościach strategicznych. Problem ten dotyczy nie tylko zatrudnienia, ale również zarządzania wiedzą i kompetencjami w organizacjach.

> *„[…] barierą będzie pozyskiwanie jednak specjalistów, ponieważ Ci specjaliści też się skończą i będzie trzeba wprowadzać bardzo dobrą edukację, taką edukację wewnętrzną, która umożliwi kalibrację wiedzy wewnątrz organizacji […]" ~ powiedział Respondent 6.*

Odpowiedzią na ten problem powinno być rozwijanie dedykowanych ścieżek edukacyjnych, kursów, programów certyfikacji oraz współpraca uczelni z przemysłem, która pozwoli na kalibrację oczekiwań rynku z rzeczywistymi umiejętnościami absolwentów.

Na przeszkodzie w innowacji stoi też brak realnego połączenia między światem akademickim a biznesem. Mimo otwartości po stronie firm, brakuje mechanizmów umożliwiających współpracę z uczelniami czy ośrodkami naukowymi. Jeden z ekspertów branżowych zauważył wprost:

> *„[…] na pewno trzeba zainwestować więcej w to połączenie biznesu z nauką. My bardzo dużo pracujemy z nauką, mamy różne doświadczenia, ale rzeczywiście nie ma takiej platformy, łączenia tych dwóch środowisk w tej domenie cyberbezpieczeństwa tak stricte i to by było bardzo wskazane" ~ powiedział Respondent 4.*

Bez systemowych programów współpracy, akceleratorów technologii i zachęt dla naukowców, wiedza pozostaje zamknięta w murach uczelni i nie znajduje zastosowania w realnych produktach.

Równocześnie branża zmaga się z deficytem kompetencji. Liczba dostępnych ekspertów nie pokrywa rosnącego zapotrzebowania, a uczelnie nie nadążają za zmianami w technologii. Przedsiębiorcy coraz częściej rezygnują z szukania gotowych kandydatów i decydują się na szkolenie pracowników z innych sektorów. Jak powiedział jeden z rozmówców:

> *„[...] Biorę ludzi, ja właśnie jak zatrudniam ludzi, to ja biorę ludzi niekoniecznie, którzy znają się na cyberbezpieczeństwie i pokończyli studia z cyberbezpieczeństwa, chociaż będą dalej na stanowisku, że uważam, że powinny być takie szkoły, to biorę ludzi z jakiegoś sektora na przykład z finansowego albo energetyki […] i ja wolę go douczyc w obszarze cyberbezpieczeństwa […]" ~ powiedział Respondent 8.*

Brakuje również państwowych programów reskillingowych, które mogłyby skutecznie łagodzić tę lukę kadrową.

Specjalizacja – przewaga technologiczna czy pułapka rozwojowa?

Wiele polskich firm z sektora cyberbezpieczeństwa wyróżnia się wysokim poziomem specjalizacji technologicznej. Tworzą one unikalne, często przełomowe rozwiązania z zakresu bezpieczeństwa informatycznego, jednak ich profil działalności – skoncentrowany na produktach, a nie usługach czy outsourcingu – powoduje, że zderzają się one z barierą skalowalności.

Brakuje im nie tylko środków finansowych na promocję i ekspansję, ale także kompetencji sprzedażowych, doświadczenia biznesowego i dostępu do odpowiednich kanałów dystrybucji. W efekcie, mimo technologicznej przewagi, firmy te mają trudności z monetyzacją swoich innowacji.

> *„[…] problem jest to z małymi przedsiębiorstwami, że przedsiębiorstwo […] potencjał ma, nie ma bardzo możliwości rozwinięcia skrzydeł, bo to zawsze jest kapitał, bez którego się nie ruszy, a bez pieniędzy nie jest w stanie zatrudniać fachowców" ~ powiedział Respondent 12.*

Dodatkowym problemem jest niedopasowanie systemów dotacyjnych i grantowych do rzeczywistości technologicznej tych firm. Publiczne wsparcie często kierowane jest ogólnie, bez uwzględnienia niuansów technicznych, specyfiki kosztów certyfikacyjnych czy iteracyjnego charakteru badań i testów w dziedzinie bezpieczeństwa cyfrowego.

Brak równości rynkowej i szklany sufit rozwoju

Polskie firmy technologiczne, mimo innowacyjności i wysokiej jakości swoich rozwiązań, często napotykają na strukturalny brak równości w dostępie do zamówień publicznych i programów wsparcia. Pomimo że ich produkty są obecne w setkach lokalizacji na całym świecie, nie mają one takiej samej szansy na realizację projektów na rynku krajowym.

„[…] zapewnić wsparcie czy przewagę konkurencyjną, czy przewagę w przetargach publicznych dla polskich przedsiębiorstw, to jest na pewno za dużo powiedziane, bo nie da się tego zrobić dla polskich przedsiębiorstw, ale zastanawiam się czy Unia Europejska jako cała Unia nie powinna bardziej premiować po prostu europejskich firm. I nie chodzi o to tutaj, że firma z Ameryki ma oddział w Europie, tylko, że po prostu firma jest europejska. […] W Stanach Zjednoczonych te firmy lokalne są zawsze lepiej premiowane. […] Są lepiej postrzegane. […] To wsparcie widziałbym raczej w zasięgu europejskim, bardziej jeżeli chodzi o konkurencyjność niż w jakimś polskim, lokalnym" ~ powiedział Respondent 9.

Dodatkowo, brak preferencji dla krajowych podmiotów w przetargach publicznych stoi w kontrze do praktyk stosowanych w państwach takich jak Stany Zjednoczone czy Izrael, gdzie instytucje rządowe aktywnie wspierają krajowych producentów technologii.

Bariery organizacyjne i komunikacyjne

Wiele firm, zwłaszcza tych mniejszych, zakładanych przez inżynierów i ekspertów technicznych, napotyka trudność w komercjalizacji swoich rozwiązań. Kluczowym problemem okazuje się brak umiejętności „opowiedzenia historii" swojego produktu w języku biznesu – zrozumiałym dla decydentów odpowiedzialnych za budżety i strategie IT.

„[…] Te firmy na przestrzeni 6-10 lat urosły do 3, 6, może 10 milionów i nie rosną dalej. Dlaczego? Najczęściej dlatego, że założone są przez specjalistów cyberbezpieczeństwa, którzy o biznesie mają równie duże pojęcie co ja o czołgach, czyli żadne, i przynieśli jakichś swoich klientów, rekomendacje zadziałały, że to urosło, ale w pewnym momencie tracą kontakt z tym, po co założyli tą firmę" ~ powiedział Respondent 5.

Brakuje kompetencji sprzedażowych, marketingowych i strategicznych, które pozwoliłyby na skalowanie działań i skuteczne dotarcie do klientów z różnych branż. Potrzebna jest profesjonalizacja komunikacji rynkowej oraz wsparcie w zakresie zarządzania cyklem sprzedażowym i rozwoju partnerstw biznesowych.

Niski poziom współpracy i brak branżowego lobbying'u

Polska branża cyberbezpieczeństwa charakteryzuje się również niskim poziomem współpracy wewnętrznej. Brakuje wspólnych inicjatyw, działań rzeczniczych i spójnej reprezentacji interesów sektora wobec instytucji państwowych oraz na forum międzynarodowym. Firmy działają w rozproszeniu, skupiając się na bieżących leadach, zamiast budować trwałe struktury współpracy, konsorcja czy fundusze rozwojowe.

Niedojrzałość branżowa skutkuje brakiem wpływu na politykę regulacyjną, co z kolei przekłada się na chaos legislacyjny, nieuwzględnianie głosu rynku przy tworzeniu przepisów oraz utratę szansy na systemowe preferencje w krajowych i europejskich zamówieniach publicznych.

Braki finansowe

Jednym z najczęściej wskazywanych problemów jest niedostateczny kapitał rozwojowy – zwłaszcza dla start-upów i młodych firm technologicznych. Przedsiębiorcy zauważają, że polski rynek venture capital jest wciąż w fazie wczesnego rozwoju, a finansowanie B+R nadal pozostaje poza zasięgiem wielu innowacyjnych, ale niewielkich firm.

„[…] W Polsce cały czas jeszcze te poziomy finansowania, inwestowania w start-up technologiczny jest bardzo niski w porównaniu chociażby ze Stanami […]" ~ powiedział Respondent 4.

Ten przekłada się na niemożność dokończenia prac nad produktem, przeprowadzenia kosztownej certyfikacji czy podjęcia ryzyka wejścia na nowe rynki. W efekcie wiele polskich firm, choć technologicznie gotowych, nie jest w stanie wyjść poza etap niszowego działania.

Dodatkowo, przedsiębiorcy zwracają uwagę na brak skutecznych mechanizmów pomostowych, które wspierałyby firmy już po etapie MVP, ale jeszcze przed osiągnięciem rentowności. Często powtarzają się postulaty stworzenia funduszy rozwojowych – ukierunkowanych na technologie wrażliwe i o wysokiej wartości strategicznej.

Bariery biurokratyczne, prawne i podatkowe

Warto wskazać także na problematyczne otoczenie prawno-gospodarcze, które dla wielu firm stanowi poważne obciążenie. Uciążliwa biurokracja, zmienność przepisów, nieprzejrzyste regulacje dotyczące bezpieczeństwa IT oraz wysokie koszty podatkowe – szczególnie dotkliwe dla małych i średnich przedsiębiorstw – to czynniki, które skutecznie zniechęcają do inwestycji i ekspansji.

Firmy zgłaszają również chaos wokół wdrażania przepisów unijnych (np. RODO, NIS2, CRA), które nierzadko są interpretowane niejednolicie, co prowadzi do niepewności prawnej oraz nieefektywnego alokowania zasobów na niepotrzebne lub źle zdefiniowane wymagania.

Jednym z najpoważniejszych zagrożeń, wskazywanych w rozmowach z przedstawicielami sektora, jest zjawisko przeregulowania. Choć potrzeba zwiększania standardów bezpieczeństwa jest oczywista, sposób wdrażania regulacji – w ocenie firm – często prowadzi do nadmiernego obciążenia, zwłaszcza dla mniejszych podmiotów. Szczególnie dotkliwe są koszty certyfikacji wymagane przez sektor publiczny i instytucje europejskie. Jak mówi jeden z respondentów:

> *„[...] polska administracja państwowa może kupić każdy dowolny produkt związany z cyberbezpieczeństwem pod warunkiem, że ma on certyfikat właśnie na przykład EL4 albo Common Criteria. […] to przeregulowanie na różnych poziomach uważam za dość spore zagrożenie […] My mówimy o sektorze małych i średnich polskich firm, a taki lobbing międzynarodowych graczy może doprowadzić do stworzenia niepożytecznych regulacji" ~ powiedział Respondent 9.*

Pojawiają się również obawy, że nowe przepisy powstają nie tyle z troski o bezpieczeństwo, co pod wpływem silnego lobbingu zagranicznych korporacji, które tym samym eliminują lokalną konkurencję.

W zamówieniach publicznych polskie firmy nadal spotykają się z barierami systemowymi, które utrudniają im skuteczny udział w postępowaniach. Często wygrywają duże, zagraniczne koncerny, ponieważ dokumentacja przetargowa jest tworzona według ich specyfikacji.

> *„[…] mamy we własnym kraju ciężej […] Za granicą jesteśmy spółką międzynarodową i chociażby we wspomnianej Ruandzie realizujemy bardzo strategiczny projekt dla obrony kraju, w Polsce […] myślę, żeby było to szalenie trudne" ~ powiedział Respondent 2.*

Potrzebna jest głęboka rewizja zasad zamówień – taka, która premiowałaby lokalne innowacje, bezpieczeństwo kodu, transparentność procesu certyfikacji i zgodność z europejskimi regulacjami.

> *„[…] Ministerstwo zidentyfikowało istnienie polskich dostawców rozwiązań, chciało je poznać, stworzyło jakąś przestrzeń sprzedażowo- zakupową […]" ~ powiedział Respondent 13.*

Wyzwania inwestycyjne: regulacje, biurokracja, niepewność

Pomimo wyraźnej chęci do inwestowania i rozwoju, przedstawiciele firm wskazują na poważne bariery, które spowalniają lub komplikują realizację planów. Na pierwszy plan wysuwają się trudności związane z nadmiarem regulacji i biurokratycznym charakterem systemów wsparcia publicznego – zwłaszcza w kontekście wnioskowania o dotacje.

> *„Na pewno jako zagrożenia postrzegam przeregulowanie tej branży, czyli niepotrzebne regulacje" ~ powiedział Respondent 9.*

Firmy zwracają również uwagę na znaczne obciążenia związane z wdrażaniem nowych przepisów unijnych. Przykładem są wymagania dyrektyw DORA czy EIDAS 2.0, które powodują konieczność renegocjacji umów, zaangażowania zespołów prawnych i dostosowania dokumentacji dla setek klientów – co przekłada się na spowolnienie rozwoju produktowego:

> *„[…] jeśli chodzi o nowe regulacje, to jest w tej chwili ogromny wysiłek. Jednym z takich tematów jest między innymi konieczność podpisania choćby na przykład ze wszystkimi istniejącymi klientami zobowiązanymi aneksów, co pochłonęło nam ogromną ilość czasu działu prawnego, żeby to wszystko przetworzyć i zrealizować" ~ powiedział Respondent 15.*

Dodatkowo, respondenci podkreślają nieprzewidywalność otoczenia prawnego oraz brak jednoznacznych interpretacji przepisów, co prowadzi do ostrożności inwestycyjnej i wstrzymywania niektórych projektów.

Mentalność zarządzania ryzykiem: „jakoś to będzie"

Na koniec warto wskazać również barierę o charakterze kulturowym i mentalnym – związaną z podejściem do zarządzania ryzykiem, planowania strategicznego oraz inwestycji w bezpieczeństwo. Wiele firm w Polsce funkcjonuje nadal w duchu operacyjnym, skoncentrowanym na bieżącym przetrwaniu, a nie na długoterminowym rozwoju.

> *„Jesteśmy społeczeństwem, które było nauczone, że musi sobie poradzić przez lata tej biedy, że wszystko było tam robione […] na przysłowiową gumkę od majtek, że jakoś to zrobimy, jakoś to będzie się będzie trzymało. Więc jakby to jest nasza cecha, która się utrzymuje" ~ powiedział Respondent 7.*

Dodatkowo, niska świadomość zagrożeń wśród małych i średnich przedsiębiorstw utrudnia sprzedaż cyberbezpieczeństwa jako realnej, mierzalnej wartości. W wielu przypadkach ochrona danych postrzegana jest bardziej jako kosztowna fanaberia niż realna konieczność biznesowa.

Polski sektor cyberbezpieczeństwa rozwija się dynamicznie, jednak tempo wzrostu hamują liczne bariery o charakterze systemowym, rynkowym i organizacyjnym. Jednym z głównych wyzwań jest brak powszechnego dostępu do finansowania – zarówno publicznego, jak i prywatnego. Mimo obecności różnych programów wsparcia, większość firm nie korzysta z nich z powodu skomplikowanych procedur, braku informacji lub zasobów organizacyjnych.

Problemem pozostaje także niska świadomość rynku na temat realnych zagrożeń i wartości cyberbezpieczeństwa. Wielu klientów nie traktuje inwestycji w bezpieczeństwo jako priorytetu strategicznego, a raczej jako zbędny koszt. Dotyczy to zwłaszcza podmiotów spoza sektorów regulowanych, gdzie brak wymogów prawnych skutkuje niską skłonnością do wdrażania rozwiązań zabezpieczających. Działy cyberbezpieczeństwa w dużych organizacjach często nie posiadają własnych budżetów, co znacznie utrudnia rozwój rynku.

Wielu respondentów wskazywało również na silną konkurencję ze strony globalnych graczy, zwłaszcza firm amerykańskich i azjatyckich. Podmioty te dysponują większymi zasobami, lepszym dostępem do rynków i wsparciem państwowym. Polska, nie posiada spójnej polityki wspierania eksportu rozwiązań z zakresu cyberbezpieczeństwa. Firmy wskazują, że brakuje misji gospodarczych, realnego wsparcia w certyfikacjach i promocji na rynkach zagranicznych. Nawet zaproszenia na targi i wydarzenia często nie są powiązane z finansowaniem uczestnictwa.

Wielką barierą pozostaje również skala działalności. Większość polskich firm to podmioty MŚP, które nie mają zasobów potrzebnych do konkurowania na globalnym rynku. Mniejsze przedsiębiorstwa nie są w stanie ponieść kosztów związanych z certyfikacją, PR-em czy obecnością w raportach branżowych. W zamówieniach publicznych dominują wymagania dostosowane do dużych korporacji, co skutecznie eliminuje z rynku lokalnych dostawców. Nawet jeśli polskie firmy realizują strategiczne projekty za granicą, w kraju napotykają bariery formalne i brak zaufania.

Istotnym problemem jest także niedobór specjalistów. Branża zmaga się z deficytem kadrowym, szczególnie w obszarach wymagających zaawansowanych kompetencji technicznych i strategicznych. Uczelnie nie nadążają z kształceniem kadr, a programy reskillingowe są niewystarczające. Przedsiębiorcy coraz częściej inwestują w wewnętrzne programy rozwojowe i doszkalanie pracowników z innych branż. Jednocześnie brakuje platform współpracy pomiędzy nauką a biznesem, co utrudnia komercjalizację innowacji.

Dodatkową barierą rozwojową jest brak kompetencji sprzedażowych i strategicznych w wielu firmach technologicznych. Przedsiębiorstwa założone przez inżynierów mają trudności w skalowaniu, ponieważ brakuje im umiejętności tworzenia spójnych modeli biznesowych i narracji sprzedażowych. Potrzebna jest profesjonalizacja komunikacji rynkowej, wsparcie mentoringowe i edukacja w zakresie zarządzania rozwojem.

Równie poważnym ograniczeniem jest brak współpracy wewnątrz sektora. Firmy rzadko tworzą konsorcja, nie prowadzą wspólnych działań rzeczniczych i nie wpływają aktywnie na kształtowanie polityki regulacyjnej. Brakuje reprezentacji

branżowej, która mogłaby skutecznie komunikować potrzeby rynku wobec administracji państwowej. Niski poziom współdziałania powoduje rozproszenie zasobów i osłabia pozycję sektora w debacie publicznej.

Problematyczne jest także otoczenie regulacyjne. Wprowadzanie przepisów unijnych często odbywa się chaotycznie, a wymagania certyfikacyjne są kosztowne i nieadekwatne do możliwości MŚP. Firmy wskazują na zjawisko przeregulowania oraz lobbing dużych korporacji, które wpływają na kształt regulacji, eliminując konkurencję. Brak równych szans w przetargach publicznych i nieuwzględnianie lokalnych dostawców to poważne bariery systemowe.

Na koniec warto podkreślić, że wiele z opisanych problemów wynika również z kulturowego podejścia do ryzyka. Polskie firmy często działają reaktywnie, skupiając się na bieżącym funkcjonowaniu, a nie na długofalowym rozwoju. Brakuje strategicznego myślenia o cyberbezpieczeństwie jako inwestycji i elemencie przewagi konkurencyjnej. Mentalność „jakoś to będzie" oraz niski poziom planowania utrudniają tworzenie skalowalnych i odpornych modeli biznesowych.

W badaniu przeprowadzonym przez Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland w 2023 r. ponad 60% respondentów wskazało, że to zbyt wysoka cena rozwiązań jest jedną z kluczowych barier rozwojowych polskiego rynku cyberbezpieczeństwa, kolejne uplasowały się: brak zaufania do mniej znanych rozwiązań (47,5%), brak kompetencji z zakresu cyberbezpieczeństwa w organizacji (47,5%), niska świadomość użytkowników końcowych (45,5%), czy nieznajomość istniejących rozwiązań (40,6%), zbyt dużo regulacji (38,6%), czy niewystarczająca liczba specjalistów cyber (17,8%)[51]. Ponadto, podczas zainicjowanej przez NCC-PL dyskusji panelowej (konferencja CYBERSEC Forum/EXPO, Katowice, 2023 r.) o szansach i barierach, jakie napotykają małe i średnie przedsiębiorstwa działające w obszarze cyberbezpieczeństwa w Polsce prelegenci wskazali najistotniejsze bariery wejścia na rynek, które pokrywają się z tymi wskazanymi w raporcie. Wśród nich pojawiły się: silna konkurencja, stosunkowo małe budżety promocyjne krajowych MŚP w stosunku do większych graczy rynkowych, postrzeganie przez klientów produktów krajowych, jako gorszej jakości i brak zaufania klientów do rozwiązań krajowych, ograniczona dostępność do specjalistów z branży cyberbezpieczeństwa z powodu wysokich kosztów ich zatrudnienia, trudności z wydatkowaniem środków pochodzących z UE na wsparcie MŚP, brak świadomości klientów o zagrożeniach i potrzebie wprowadzenia rozwiązań z obszaru cyberbezpieczeństwa[52]. Wśród innych barier wymieniane są także: zdobywanie referencji, czy brak wiedzy o zwiększaniu konkurencyjności (panel dyskusyjny podczas VI Forum Cyberbezpieczeństwa w Karpaczu)[53].

Choć wszystkie firmy działające w sektorze cyberbezpieczeństwa mierzą się z podobnymi wyzwaniami, ich charakter zmienia się wraz z wielkością organizacji. Małe firmy mają problemy ze zdobyciem klientów i budowaniem wiarygodności oraz finansowaniem, podczas gdy duże podmioty borykają się z presją regulacyjną, złożonością infrastruktury IT i kosztami operacyjnymi. W obu przypadkach kluczowe są inwestycje w rozwój technologii, kadrę oraz odpowiednie strategie sprzedażowe i marketingowe.

[51] Raport "Polski rynek cyberbezpieczeństwa 2023–2028". Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 125-126.
[52] Opis panelu „Szanse i Bariery dla MŚP działających w obszarze cyberbezpieczeństwa w Polsce" podczas Cybersec Forum w Katowicach, 2023 r. Gov.pl. [Dostęp: 18.04.2025]
[53] Panel "Jak uczynić polskie cyber MŚP bardziej konkurencyjnymi", podczas VI Forum Cyberbezpieczeństwa w Karpaczu, 2024.

3.2. Regulacje polskiego rynku cyberbezpieczeństwa

Wpływ regulacji na działalność firm sektora cyberbezpieczeństwa

Poniższy wykres prezentuje poziom znajomości dwóch kluczowych regulacji unijnych wśród przedstawicieli firm z sektora cyberbezpieczeństwa – CRA (Cyber Resilience Act) oraz NIS2 (dyrektywa w sprawie bezpieczeństwa sieci i informacji).

Wykres 35. Czy wie Pan/Pani, czym są regulacje CRA i NIS2? (N=197)

Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci badania zostali zapytani o znajomość regulacji CRA (Cyber Resilience Act) oraz NIS2 (dyrektywa w sprawie bezpieczeństwa sieci i informacji). Większość firm zadeklarowała, że zna te regulacje – odpowiedź „tak" wskazało 94 małych oraz 19 średnich przedsiębiorstw.

Brak znajomości regulacji zadeklarowało jedynie 7 małych i 2 średnie firmy, co może świadczyć o rosnącej świadomości w zakresie nadchodzących wymogów prawnych wśród podmiotów z branży cyberbezpieczeństwa.

Warto jednak zwrócić uwagę na stosunkowo wysoki odsetek odmów udzielenia odpowiedzi – 59 małych i 16 średnich firm nie określiło swojego poziomu wiedzy w tym zakresie. Może to sugerować niepewność co do interpretacji pytania lub brak jednoznacznej wiedzy na temat tych regulacji.

Zdecydowana większość firm w wywiadach pogłębionych deklaruje znajomość zarówno NIS2, jak i CRA, przy czym dyrektywa NIS2 jest znacznie lepiej rozumiana i w wielu przypadkach już implementowana. CRA jako regulacja nowsza, jest często traktowana jako wyzwanie na nadchodzące miesiące – firmy są świadome wymagań, ale nie wszystkie rozpoczęły proces wdrożenia.

Wpływ regulacji oceniany jest jako znaczący, choć niejednoznaczny. Część firm wskazuje, że same regulacje stanowią pozytywny impuls rozwojowy, zmuszają do uporządkowania procesów, inwestycji w cyberbezpieczeństwo i przyczyniają się do wzrostu świadomości na rynku – zarówno po stronie klientów, jak i partnerów.

„W związku z NIS2 widzimy większe zainteresowanie naszymi produktami. […] Widzimy troszkę większy ruch na rynku i zainteresowanie naszymi urządzeniami, ponieważ tutaj wszystko to obraca się w obszarze bezpieczeństwa danych" ~ powiedział Respondent 1.

Z drugiej strony, rosnące obciążenia formalne, wymagania dokumentacyjne i niejasności interpretacyjne są wskazywane jako poważne bariery rozwoju.

„[…] jeżeli chodzi o nowe regulacje, to jest to w tej chwili ogromny wysiłek. […] Wykonujemy ogromną pracę tylko po to, żeby odpowiedzieć na pytania, bo te instytucje są zobowiązane do tego, żeby taką informację otrzymać, ale nikt nie wie do końca, jak to w ogóle należy interpretować […]" ~ powiedział Respondent 15.

Wielokrotnie pojawia się również temat konieczności dostosowania produktów oraz budowy nowych funkcjonalności zgodnych z wymaganiami dyrektyw, jak również potrzeby rozbudowy zespołów prawnych, audytowych i compliance.

„[…] na pewno podlegamy właśnie pod CRA, wiadomo, to będzie taki tym bardziej zaawansowany znak CE, więc musimy się tym wymaganiom przyglądać. Oczywiście gotowi jeszcze nie jesteśmy, natomiast mamy świadomość, więc to już jest połowa sukcesu. Potem mamy dyrektywę NIS2, gdzie prawdopodobnie też będziemy podlegać, aczkolwiek nie wiadomo do końca, […] mamy wdrożone ISO 27001 u siebie i certyfikowani jesteśmy, natomiast mamy też wdrożone 22301, czyli ciągłość działania, ale tutaj jeszcze nie jesteśmy certyfikowani" ~ powiedział Respondent 4.

Jednocześnie regulacje są uznawane za szansę rynkową, szczególnie w kontekście rosnących potrzeb sektora MŚP, którzy dopiero teraz zaczynają inwestować w cyberbezpieczeństwo.

„Wszystkie regulacje zawsze są takim pozytywnym otoczeniem, dlatego, że samo ich wydawanie, samo ich istnienie sprawia, że nawet przez podmioty, których one bezpośrednio nie dotyczą, widzą, że to są ważne rzeczy" ~ powiedział Respondent 9.

Podsumowując, regulacje NIS2 i CRA są postrzegane jako konieczne i nieuniknione, ale jednocześnie obciążające i czasochłonne. Ich wpływ na działalność firm ocenia się jako duży – zarówno w kontekście wyzwań, jak i możliwości rynkowych.

DORA – standardy finansowe wpływające na całą branżę

Wpływ DORA jest odczuwalny przede wszystkim w kontekście rosnących wymagań ze strony instytucji finansowych. Firmy wskazują, że nowe przepisy dotyczące bezpieczeństwa cyfrowego i odporności operacyjnej stają się de facto rynkowym standardem – nawet jeśli formalnie ich nie obejmują.

„DORA tak naprawdę jest normą w tym obszarze. My niestety nie mamy lekko […] tutaj jest bardzo duża konkurencja amerykańskich spółek i bardzo często my nie dochodzimy do głosu" ~ powiedział Respondent 2.

Najsilniej zauważalny efekt DORA dotyczy zainteresowania klientów – szczególnie banków i ubezpieczycieli – rozwiązaniami wspierającymi ciągłość działania, disaster recovery oraz bezpieczeństwo łańcucha dostaw.

„[…] DORA bezpośrednio skierowana jest ku instytucjom finansowym i w związku z tym te instytucje dla nas w celu dokładnie tak jak te pozostałe spełniające lub chcące spełnić NIS2, w celu zabezpieczenia tych danych" ~ powiedział Respondent 6.

Regulacja ta postrzegana jest jako ewolucja, a nie rewolucja – szczególnie w kontekście firm, które już wcześniej współpracowały z branżą finansową i miały do czynienia z wymogami KNF. Zmiana polega głównie na uporządkowaniu i formalizacji oczekiwań względem dostawców technologii.

„[…] Sektor finansowy to jest sektor, który ma cyberbezpieczeństwo może nie w małym palcu, ale można by było tak powiedzieć" ~ powiedział Respondent 9.

Jednocześnie podkreślany jest aspekt konkurencyjności – mniejsze firmy europejskie mają trudność w przebiciu się w przetargach obok dużych graczy z USA, którzy często mają większe zasoby i silniejszą pozycję rynkową.

„[…] My niestety nie mamy lekko, można tak powiedzieć kolokwialnie, dlatego że tutaj jest bardzo duża konkurencja amerykańskich spółek i bardzo często my nie dochodzimy do głosu" ~ powiedział Respondent 2.

Regulacja DORA znacząco podnosi poprzeczkę w zakresie wymagań bezpieczeństwa i odporności operacyjnej – nie tylko dla sektora finansowego, ale także dla jego dostawców technologicznych. W praktyce staje się ona uniwersalnym standardem rynkowym, warunkującym możliwość współpracy z instytucjami finansowymi i zwiększającym presję na profesjonalizację procesów. Dla firm z sektora cyberbezpieczeństwa oznacza to zarówno nowe wyzwania organizacyjne, jak i szansę na budowanie przewagi konkurencyjnej poprzez dostosowanie oferty do oczekiwań najbardziej wymagających klientów. Jednak bez wsparcia dla mniejszych podmiotów – szczególnie w zakresie interpretacji przepisów i dostępu do środków na adaptację – istnieje ryzyko dalszego pogłębiania się nierówności rynkowych.

Wśród firm z branży cyberbezpieczeństwa obserwuje się relatywnie wysoki poziom świadomości na temat unijnych regulacji – 58% respondentów deklaruje znajomość aktów CRA i NIS2. Mimo to, aż 38% nie udzieliło jednoznacznej odpowiedzi, co może sugerować niepewność lub brak decyzyjności u respondentów.

W wywiadach pogłębionych firmy znacznie częściej i lepiej rozumieją wymogi dyrektywy NIS2, która bywa już implementowana. Z kolei CRA postrzegana jest jako nowe, złożone wyzwanie, które dopiero zaczyna być analizowane pod kątem wdrożeń.

Firmy wskazują, że regulacje, choć wymagające, mogą stanowić impuls prorozwojowy. Porównywane są do RODO – wymuszają uporządkowanie procesów, zwiększają popyt na usługi i podnoszą świadomość klientów. Regulacje motywują również do inwestycji w compliance, rozbudowę zespołów prawnych i dostosowanie produktów do wymagań formalnych.

Jednocześnie pojawia się krytyka: firmy obawiają się rosnących kosztów wdrożeń, niejasnych interpretacji prawnych oraz wysokiego obciążenia dokumentacyjnego. Szczególnie problematyczne okazuje się przygotowanie do CRA, którego wymogi (np. oznakowanie CE) wymagają głębokich zmian w procesach i ofercie.

Regulacja DORA, choć formalnie skierowana do instytucji finansowych, ma wyraźny wpływ na cały ekosystem dostawców technologii. Firmy zauważają, że DORA staje się de facto rynkowym standardem, który warunkuje współpracę z bankami i ubezpieczycielami. Wzmacnia to nacisk na zapewnienie odporności operacyjnej, disaster recovery i bezpieczeństwa łańcucha dostaw.

DORA postrzegana jest jako ewolucja dotychczasowych wymagań sektora finansowego, ale zyskuje większą moc formalną. Dla firm oznacza to konieczność dalszej profesjonalizacji działań i rozbudowy systemów bezpieczeństwa – często przy ograniczonych zasobach.

Wielu rozmówców podkreśla, że choć regulacje tworzą szanse rynkowe, sprzyjają dużym, międzynarodowym graczom – szczególnie ze Stanów Zjednoczonych. Mniejsze firmy mają problem z przebiciem się, co grozi dalszym pogłębianiem nierówności konkurencyjnych.

Branża cyberbezpieczeństwa oczekuje wsparcia państwowego w zakresie edukacji, interpretacji przepisów oraz dostępu do środków na wdrożenie nowych wymogów. Potrzebne są również instrumenty certyfikacyjne, które będą dopasowane do realiów MŚP, a nie wyłącznie dużych podmiotów.

Ostatecznie firmy zgadzają się, że NIS2, CRA i DORA są nieuniknione i ważne, ale jednocześnie wymagają znacznego wysiłku organizacyjnego, finansowego i kompetencyjnego. Ich skuteczna implementacja wymaga współpracy sektora prywatnego z administracją oraz wprowadzenia instrumentów wsparcia dostosowanych do potrzeb firm o różnej skali działania.

Cyberbezpieczeństwo stanowi jedno z kluczowych wyzwań dla funkcjonowania współczesnej gospodarki cyfrowej. W obliczu dynamicznie rozwijających się zagrożeń w cyberprzestrzeni, kraje Unii Europejskiej, w tym Polska, wdrażają kompleksowe regulacje prawne, które definiują ramy ochrony danych, cyberbezpieczeństwa oraz cyfrowej odporności instytucji i przedsiębiorstw. Dla małych i średnich przedsiębiorstw działających na rynku cyberbezpieczeństwa (MŚP cyber), nowe wymogi prawne oznaczają konieczność dostosowania działalności zarówno w roli producenta/dystrybutora rozwiązań, jak i uczestnika cyfrowego ekosystemu.

Kluczowe polskie regulacje kształtujące rynek cyberbezpieczeństwa:

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)

Ustawa KSC nakłada obowiązki na podmioty kluczowe, w tym dostawców usług cyfrowych, co oznacza, że MŚP cyber tworzące oprogramowanie lub świadczące usługi IT muszą zapewnić zgodność z wymogami zarządzania ryzykiem, wykrywania incydentów i ich zgłaszania, a także stosowania odpowiednich środków ochrony. Obecnie trwają prace nad nowelizacją ustawy KSC, która ma dostosować ją do wymagań unijnej dyrektywy NIS2, m.in. poprzez rozszerzenie katalogu podmiotów objętych regulacją, zaostrzenie wymagań dotyczących cyberodporności oraz zwiększenie sankcji za naruszenia.[54]

Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO)

Dla MŚP cyber jako producentów rozwiązań IT przetwarzających dane osobowe, RODO wymusza projektowanie i wdrażanie zabezpieczeń zgodnych z zasadą "privacy by design". MŚP jako część łańcucha dostaw IT zobowiązane są do zagwarantowania zgodności ze standardami ochrony danych oraz do zapewnienia klientom wsparcia w realizacji obowiązków informacyjnych i reagowania na incydenty naruszenia danych[55].

Strategia Cyberbezpieczeństwa RP

W Polsce obowiązuje również Strategia Cyberbezpieczeństwa - dokument określający długoterminowe strategiczne cele polityki państwa w zakresie cyberbezpieczeństwa, podmioty zaangażowane we wdrażanie strategii, czy środki potrzebne na jej realizację.

Głównym celem Strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym[56].

Ponadto, dokument doprecyzowuje kwestie związane m.in. z działaniami na rzecz podnoszenia odporności infrastruktury IT, współpracą międzynarodową, budowaniem świadomości społecznej oraz wspieraniem innowacyjności w sektorze cyberbezpieczeństwa. Aktualna wersja na lata 2019 - 2024 obowiązuje do czasu opublikowania nowej strategii na lata 2025 - 2029, która w momencie pisania raportu jest w trakcie konsultacji międzyresortowych.[57]

Kluczowe unijne regulacje kształtujące polski rynek cyberbezpieczeństwa:

Cybersecurity Act

Rozporządzenie to ma szczególne znaczenie dla MŚP cyber, które są producentami sprzętu i oprogramowania. Obowiązek spełnienia wymogów europejskich systemów certyfikacji (który będzie odwoływać się do jednego z trzech poziomów: podstawowego, istotnego lub wysokiego) oznacza konieczność inwestycji w testowanie bezpieczeństwa, dokumentację techniczną i zgodność z procedurami certyfikacyjnymi. Uzyskanie certyfikatu może być jednak przewagą konkurencyjną i umożliwić dostęp do rynku usług publicznych lub zagranicznych[58].

[54] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Dz.U. 2018, poz. 1560.
[55] Artykuł "Na czym polega ochrona danych osobowych RODO? Rozporządzenie RODO w pigułce". EY, 2025. [Dostęp: 15.04.2025]
[56] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Ministerstwo Cyfryzacji, 2019. [Dostęp: 18.04.2025]
[57] Tamże.
[58] Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019, s. 15-69.

DORA (Digital Operational Resilience Act)

Choć bezpośrednio dotyczy sektora finansowego, DORA oddziałuje również na MŚP cyber jako dostawców ICT. Firmy dostarczające usługi lub produkty dla instytucji finansowych muszą wykazać się zgodnością z ich strategiami zarządzania ryzykiem ICT, co oznacza m.in. konieczność wdrażania procedur monitoringu incydentów, planów ciągłości działania oraz polityk bezpieczeństwa informacji. Dla wielu MŚP oznacza to potrzebę budowy wewnętrznych zdolności w obszarze compliance i cyber risk management[59].

Dyrektywa NIS2

Dyrektywa NIS2 rozszerza zakres regulacji dotyczących cyberbezpieczeństwa, obejmując więcej sektorów i firm, w tym niektóre MŚP. MŚP mogą być objęte NIS2 bezpośrednio, jeśli świadczą usługi w sektorze objętym dyrektywą i są uznane za podmiot kluczowy lub ważny, albo pośrednio, jako dostawcy lub klienci podmiotów objętych NIS2. Dla MŚP oznacza to nowe obowiązki w zakresie cyberbezpieczeństwa, w tym zarządzanie ryzykiem, zabezpieczanie łańcuchów dostaw, szkolenia pracowników i raportowanie incydentów[60].

Dyrektywa CER

Dyrektywa CER (Critical Entities Resilience) w sprawie odporności podmiotów krytycznych, nie ma bezpośredniego wpływu na małe i średnie przedsiębiorstwa (MŚP) w zakresie cyberbezpieczeństwa, ale jej wdrożenie może pośrednio wpłynąć na niektóre z nich. Dyrektywa CER skupia się na zwiększeniu odporności podmiotów świadczących usługi kluczowe dla gospodarki i społeczeństwa (podmioty krytyczne). Jeśli MŚP są dostawcami lub podwykonawcami podmiotów krytycznych, mogą być zobligowane do spełnienia pewnych wymagań dotyczących cyberbezpieczeństwa, aby zapewnić ciągłość dostaw i bezpieczeństwo procesów[61]. Wraz z dyrektywą NIS 2 tworzą one komplementarne, zharmonizowane ramy prawne w zakresie zapewniania ciągłości usług kluczowych dla państwa oraz odporności (fizycznej i w cyberprzestrzeni) podmiotów je świadczących.

Cyber Resilience Act (CRA)

Wdrożenie CRA ma na celu zwiększenie bezpieczeństwa użytkowników oraz ograniczenie liczby kluczowych podatności w oprogramowaniu i urządzeniach elektronicznych. Nowe regulacje zobowiązują producentów do uwzględniania zasad cyberbezpieczeństwa już na etapie projektowania swoich produktów i usług oraz do zapewnienia ich ochrony przez cały cykl życia. Ponadto, producenci będą zobligowani do skutecznego zarządzania podatnościami, gwarantując, że przez określony czas po wprowadzeniu produktu na rynek wszelkie luki w zabezpieczeniach będą odpowiednio identyfikowane i usuwane. Wprowadzono również wymóg natychmiastowego raportowania incydentów – producenci będą zobligowani do powiadomienia Agencji UE ds. Bezpieczeństwa Cybernetycznego (ENISA) w ciągu 24 godzin od wykrycia aktywnie wykorzystywanej podatności lub zdarzenia mającego wpływ na bezpieczeństwo produktu[62].

Szanse dla MŚP z sektora cyberbezpieczeństwa

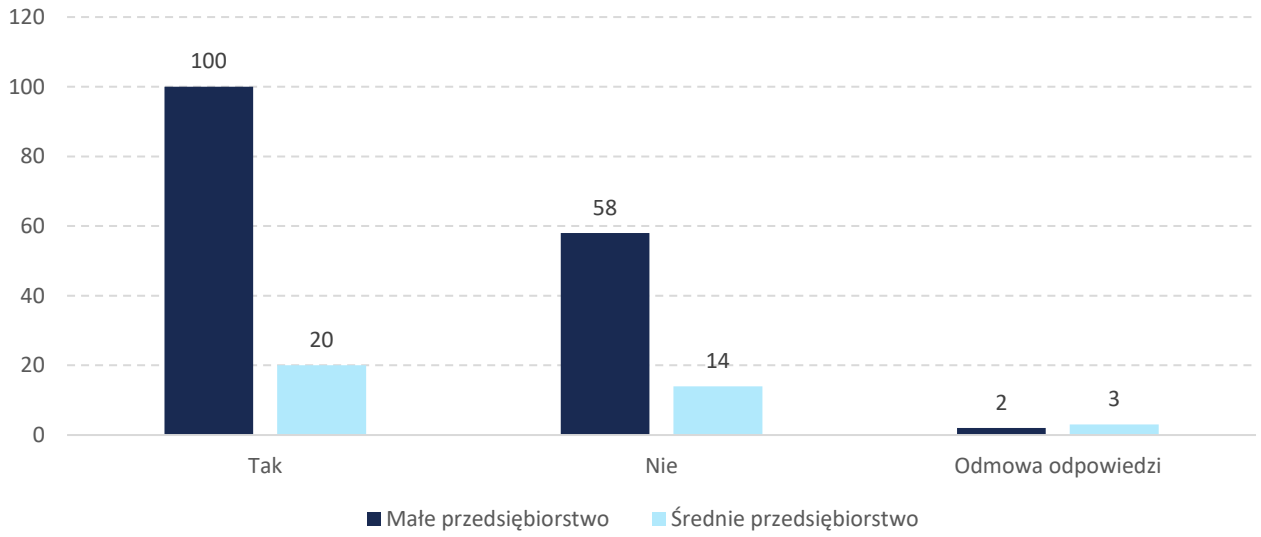
Pomimo rosnących obowiązków regulacyjnych, nowa legislacja tworzy znaczną przestrzeń rozwoju dla MŚP. Zdecydowanie wpłynie na to wzrost zapotrzebowania na usługi audytorskie, testy penetracyjne i doradztwo w zakresie zgodności, ale też możliwość certyfikacji produktów pod kątem wymagań UE, co ułatwi ekspansję na rynki zagraniczne. MŚP będą mogły liczyć także na współpracę z sektorem publicznym i podmiotami, które objęte zostaną wyróżnionymi aktami prawnymi.

[59] Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022, s. 1-65.
[60] Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS2). Dz.U. L 333 z 27.12.2022, s. 80– 152.
[61] Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Dz.U. L 333 z 27.12.2022, s. 164–196.
[62] Rozporządzenie (UE) 2024/2847 z dnia 12 marca 2024 r. w sprawie horyzontalnych wymagań dotyczących cyberbezpieczeństwa dla produktów z elementami cyfrowymi oraz zmieniające rozporządzenie (UE) 2019/1020. Dz.U. L 333 z 27.12.2024, s. 1–65.

3.3. Oczekiwania wobec otoczenia instytucjonalnego i legislacyjnego

Badanie obejmowało także analizę możliwości przezwyciężania barier rozwojowych samodzielnie w analizowanych firmach.

Wykres 36. Czy Pana/Pani zdaniem, bariery rozwojowe mogą zostać pokonane na szczeblu przedsiębiorstwa? (N=197)

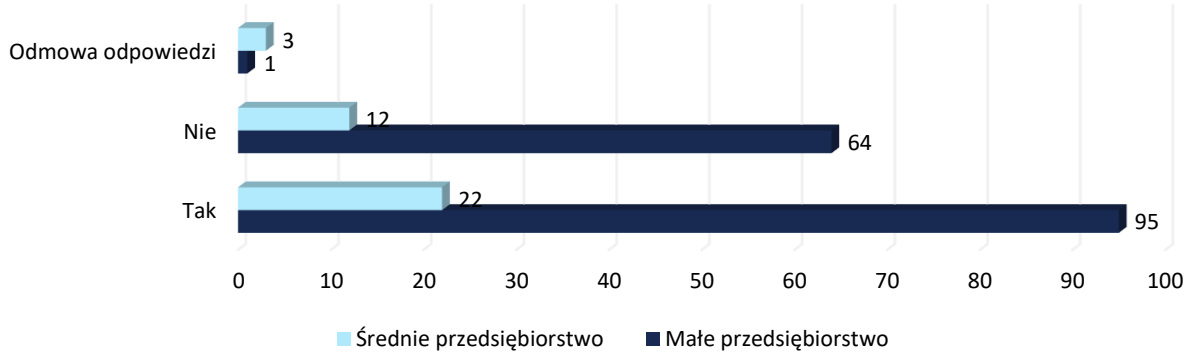


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Większość respondentów uważa, że bariery rozwojowe mogą zostać pokonane na poziomie przedsiębiorstwa. Taką opinię wyraziło 100 małych oraz 20 średnich firm. Przeciwnego zdania było łącznie 72 respondentów — 58 z sektora małych i 14 ze średnich przedsiębiorstw. Wyniki te wskazują, że mimo istniejących wyzwań, znaczna część firm dostrzega możliwość przezwyciężenia barier rozwojowych poprzez działania podejmowane wewnętrznie, bez konieczności wsparcia zewnętrznego.

Na wykresie poniżej przedstawiono opinie przedstawicieli firm z sektora cyberbezpieczeństwa na temat roli państwa w przezwyciężaniu barier rozwojowych. Dane pozwalają określić, na ile przedsiębiorcy ufają we własne możliwości oraz działania rynku, a na ile oczekują wsparcia instytucjonalnego i systemowego w pokonywaniu przeszkód utrudniających rozwój.

Wykres 37. Czy Pana/Pani zdaniem, bariery rozwojowe mogą być pokonane bez interwencji państwa? (N=197)

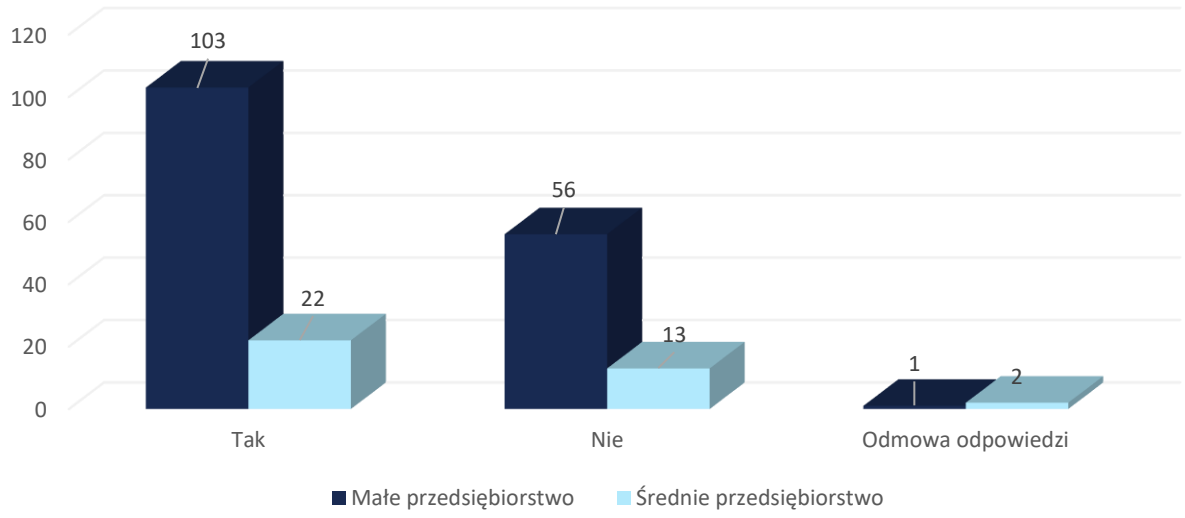


Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Większość respondentów uważa, że bariery rozwojowe mogą zostać pokonane bez konieczności interwencji państwa. Taką opinię wyraziło łącznie 117 firm — 95 małych oraz 22 średnie przedsiębiorstwa. Przeciwnego zdania było 76 respondentów (64 małych i 12 średnich firm). Dane te wskazują, że znaczna część firm dostrzega możliwość samodzielnego przezwyciężania barier, choć jednocześnie istotna grupa nadal widzi potrzebę wsparcia ze strony instytucji publicznych.

Dodatkowo zapytano o opinie respondentów na temat potencjału sztucznej inteligencji w kontekście pokonywania barier rozwojowych w firmach. Analiza pozwala zrozumieć, w jakim stopniu przedsiębiorcy dostrzegają rolę AI w optymalizacji procesów, automatyzacji, podejmowaniu decyzji oraz zwiększaniu efektywności operacyjnej.

Wykres 38. Czy Pana/Pani zdaniem, sztuczna inteligencja może przyczynić się do pokonania barier rozwojowych? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Większość respondentów uważa, że sztuczna inteligencja może przyczynić się do pokonania barier rozwojowych. Taką opinię wyraziło łącznie 125 firm — 103 małe oraz 22 średnie przedsiębiorstwa. Przeciwnego zdania było 69 respondentów (56 małych i 13 średnich firm). Wyniki te wskazują na świadomość potencjału technologii AI w kontekście wspierania rozwoju firm, choć część przedsiębiorstw pozostaje sceptyczna wobec jej skuteczności.

Państwo jako katalizator – oczekiwany model wsparcia

Paradoksalnie, mimo wyraźnej potrzeby interwencji państwowej, wielu przedsiębiorców ma dystans do samego pojęcia „interwencjonizmu". Nie chodzi im jednak o zastępowanie rynku, lecz o stworzenie warunków umożliwiających uczciwą konkurencję i rozwój.

> *„Nie chodzi o to, żeby państwo robiło za nas robotę. Ale jak mamy walczyć z firmami, które są wspierane politycznie, prawnie i finansowo przez swoje rządy, to potrzebujemy chociaż równych warunków gry."*

Potrzebne jest partnerstwo – państwo jako katalizator innowacji, inicjator wspólnych działań i promotor lokalnych kompetencji, a nie kontroler lub decydent.

Przedsiębiorstwa nie są w stanie samodzielnie pokonać wszystkich barier. Aby polska branża cyberbezpieczeństwa mogła realnie konkurować z globalnymi liderami, potrzebna jest świadoma, długofalowa polityka państwa, obejmująca nie tylko finansowanie i certyfikację, ale również promocję eksportu, wsparcie edukacyjne, preferencje w zamówieniach publicznych oraz zmianę narracji wokół pojęcia „polska technologia".

Potrzeba systemowego wsparcia i strategii przemysłowej

Jak podkreślają wszyscy rozmówcy, Polska ma potencjał, by stać się znaczącym graczem w dziedzinie cyberbezpieczeństwa. **Ale bez zaplecza instytucjonalnego, mądrej polityki przemysłowej i skutecznej strategii budowania zaufania do rodzimych rozwiązań – firmy będą nadal funkcjonować na marginesie globalnych łańcuchów wartości, realizując zlecenia jako podwykonawcy, a nie jako właściciele innowacji.**

Ocena aktywności państwa w zakresie wspierania polskiego sektora cyberbezpieczeństwa – choć częściowo pozytywna – wciąż budzi szereg zastrzeżeń i oczekiwań. Wśród przedstawicieli firm z branży widoczny jest zarówno umiarkowany optymizm, jak i rozczarowanie – zależne od poziomu szczegółowości działań, ich skuteczności oraz dostępu do realnego wsparcia. Zgromadzone wypowiedzi jednoznacznie pokazują, że choć w ostatnich latach poprawił się poziom dialogu między administracją a sektorem, to wiele potrzeb branży nadal pozostaje niezaspokojonych.

Dialog z administracją: postęp i ograniczenia

Część respondentów wskazuje, że w zakresie kontaktów z administracją widoczna jest pozytywna zmiana. Przedsiębiorcy zwracają uwagę na fakt, że instytucje państwowe częściej inicjują konsultacje i spotkania, a tematyka cyberbezpieczeństwa zyskuje na znaczeniu w agendzie publicznej. W ten sposób jeden z przedstawicieli firmy, podkreślając znaczenie realnych instrumentów wsparcia, zwłaszcza tych związanych z certyfikacją i rozwojem produktów:

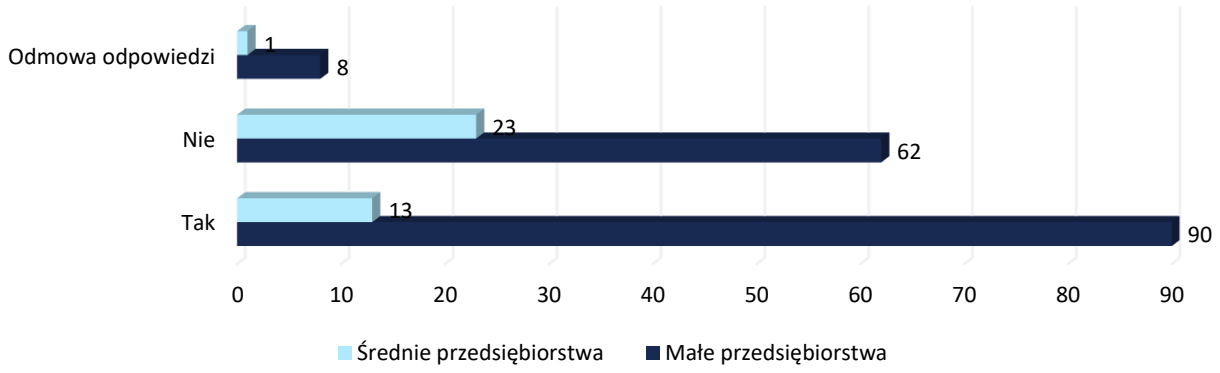
> *„To na pewno pozytywnie oceniam ten dialog, który jest prowadzony między rządem a firmami z tego ekosystemu cyberbezpieczeństwa. Oczywiście widać taką otwartość, chęć spotkania się, chęć rozmów. […] Na pewno wartościowe było stworzenie programu na rozwój właśnie produktów cyberbezpieczeństwa i certyfikacje. […] sama idea jest świetna, tylko by trzeba było ją wyskalować” ~ powiedział Respondent 4.*

Dla części firm takie inicjatywy stanowią ważny krok w kierunku poprawy konkurencyjności na rynku europejskim i globalnym.

Nieskuteczność i fragmentacja działań państwa

Wykres przedstawia ocenę respondentów dotyczącą skuteczności dotychczasowych działań podejmowanych na rzecz rozwoju rynku cyberbezpieczeństwa w Polsce. Odpowiedzi firm pozwalają ocenić, na ile inicjatywy legislacyjne, instytucjonalne czy finansowe są adekwatne do potrzeb sektora oraz gdzie mogą występować istotne luki wymagające usprawnienia.

Wykres 39. Czy uważa, Pan/Pani, że zostały podjęte działania dotyczące rynku cyberbezpieczeństwa, które wymagają usprawnienia? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Większość respondentów uważa, że działania podejmowane na rzecz rynku cyberbezpieczeństwa wymagają usprawnienia. Taką opinię wyraziło łącznie 103 przedsiębiorstwa — 90 małych oraz 13 średnich. Przeciwnego zdania było 85 firm (62 małe

i 23 średnie). Nieliczni respondenci (8 małych i 1 średnie przedsiębiorstwo) odmówili udzielenia odpowiedzi. Wyniki te wskazują na wyraźne oczekiwanie względem poprawy istniejących mechanizmów i inicjatyw w obszarze cyberbezpieczeństwa.

Jednakże mimo tych pozytywnych ocen, wielu respondentów wyraża silne zastrzeżenia co do skuteczności i przejrzystości działań państwa. Pojawia się zarzut, że wsparcie ma często charakter deklaratywny lub marketingowy, a nie operacyjny. Krytykowano m.in. małą skalę dostępnych programów, brak przejrzystości w kryteriach oraz długie i uciążliwe procedury aplikacyjne.

> *„[…] Ministerstwo Cyfryzacji, to jest z mojego punktu widzenia bardzo dużo marketingu, bardzo mało działania. […] Zakończono prace konsultacyjne […] nad projektem ustawy o krajowym systemie certyfikatów i cyberbezpieczeństwa. Wszyscy w sensie ministerstwa i rządu chwalą się, że jest to krok w dobrą stronę {…} Otrzymaliśmy informację, ile czasu to trwa i jakie to są koszty. Nie wierzę, że jeżeli taki system certyfikacji zostanie utrzymany, jeżeli to będą koszty, które będą opiewały na dziesiątki, a czasem setki tysięcy złotych […] to będzie wydatek, na który wielu z tych przedsiębiorstw nie będzie stać" ~ powiedział Respondent 9.*

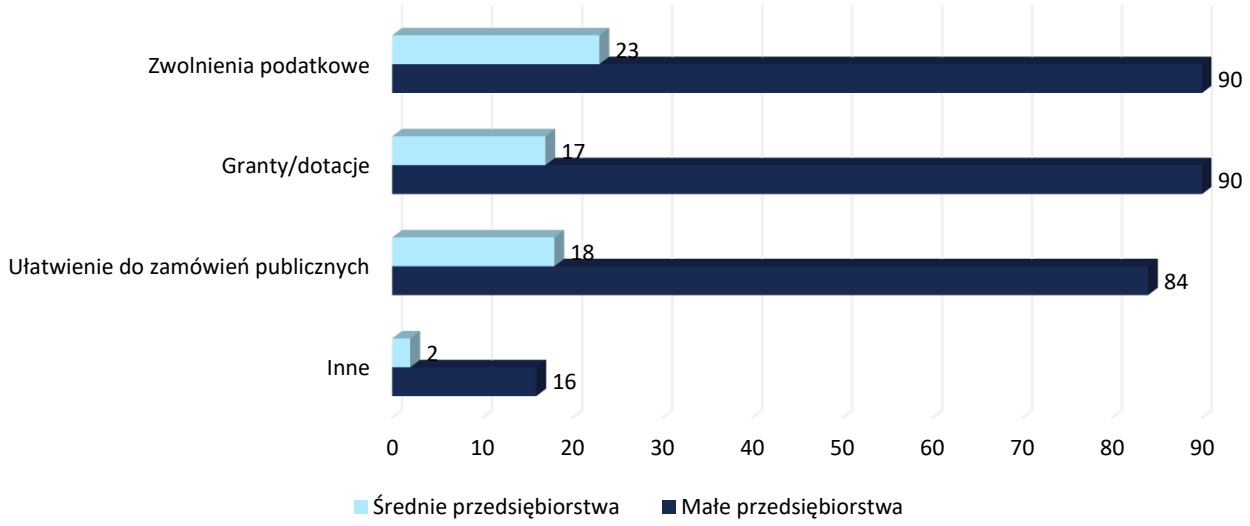
W tym kontekście szczególnie krytycznie oceniano projekty, które – mimo deklarowanej misji wsparcia polskich rozwiązań – często w praktyce służą promowaniu produktów i podmiotów reprezentujących zagraniczne interesy.

> *„[…] inicjatywa PW Cyber, […] czasami mam wrażenie, że jest trochę martwa albo wybiórcza" ~ powiedział Respondent 4.*

Potrzeba ciągłości i strukturyzacji instrumentów wsparcia

Wykres 40 prezentuje oczekiwania firm z branży cyberbezpieczeństwa wobec działań publicznych, które mogłyby najskuteczniej wspierać ich rozwój. Dane wskazują, że przedsiębiorcy największą wagę przywiązują do wsparcia finansowego w postaci ulg podatkowych i dotacji, ale równie istotne są działania systemowe, takie jak ułatwienie dostępu do zamówień publicznych, promocja krajowych rozwiązań oraz poprawa współpracy między administracją, nauką i biznesem.

Wykres 40. Jakie działania publiczne byłyby najbardziej pomocne? (N=197)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Wśród działań publicznych, które zdaniem respondentów byłyby najbardziej pomocne, najczęściej wskazywano na zwolnienia podatkowe oraz granty i dotacje — obie formy wsparcia uzyskały po 90 wskazań od małych przedsiębiorstw. Wśród średnich firm zwolnienia podatkowe wskazało 23 respondentów, a granty i dotacje — 17. Na trzecim miejscu

znalazły się ułatwienia w dostępie do zamówień publicznych, które uzyskały łącznie 102 wskazania (84 od małych i 18 od średnich firm).

Analiza otwartych odpowiedzi wskazuje, że firmy oczekują od państwa nie tylko wsparcia finansowego, lecz przede wszystkim systemowego i strategicznego zaangażowania w rozwój krajowego sektora cyberbezpieczeństwa.

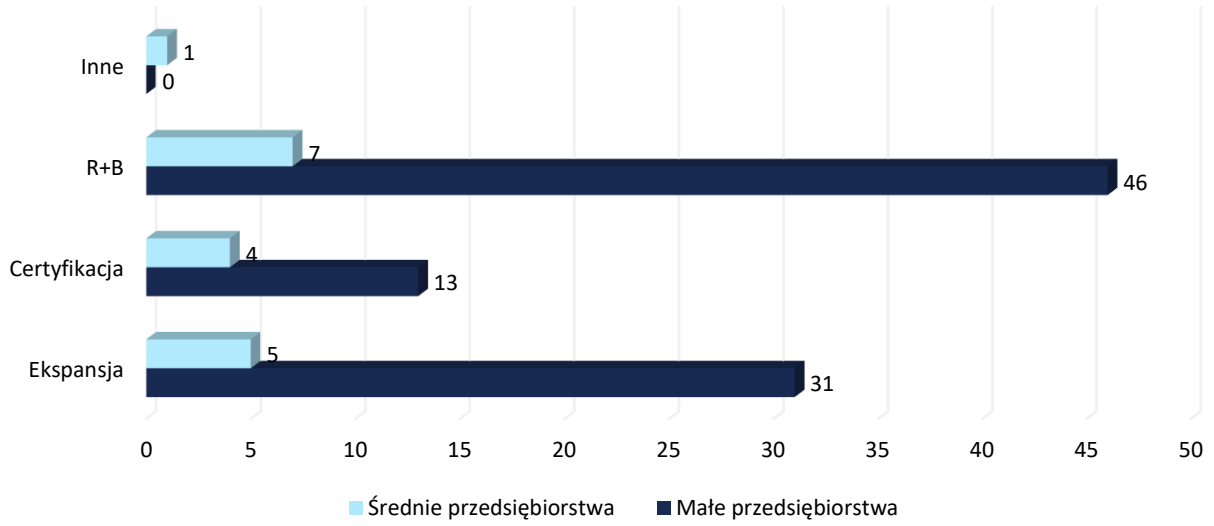
Najczęściej powtarzające się postulaty obejmują:

1. Promocję i wspieranie polskich firm technologicznych – postulowano międzynarodową promocję marek z udziałem państwa, wsparcie PR-owe i certyfikacyjne, a także rekomendacje instytucjonalne zachęcające do korzystania z lokalnych rozwiązań.
2. Lepszą koordynację instytucjonalną i legislacyjną – respondenci podkreślali potrzebę większej świadomości i kompetencji po stronie administracji rządowej, uproszczenia przepisów (w tym podatkowych), szybszego wdrażania regulacji (np. NIS2), a także stworzenia jasnych i skutecznych mechanizmów współpracy między resortami.
3. Budowę ekosystemu współpracy nauki i biznesu – postulowano obowiązkowe angażowanie firm prywatnych w projekty B+R, tworzenie wspólnych „use case'ów" z administracją, wskaźniki współpracy jednostek naukowych z przemysłem, oraz wsparcie klastrów i instytucji otoczenia biznesu (np. w finansowaniu udziału w targach, konferencjach, publikacjach itp.).
4. Wsparcie regulacyjne i sektorowe – pojawiły się też postulaty dotyczące konkretnych kwestii infrastrukturalnych, np. zakazu dublowania sieci telekomunikacyjnych i ochrony małych operatorów.

W mniejszym stopniu wskazywano na potrzebę klasycznych działań dotacyjnych – nacisk przesunął się w stronę długofalowych polityk wspierających konkurencyjność i obecność polskich firm na rynkach międzynarodowych.

Poniższy wykres przedstawia preferencje firm z sektora cyberbezpieczeństwa dotyczące kierunków alokacji środków publicznych w formie dotacji. Odpowiedzi respondentów wskazują, że największe znaczenie ma wsparcie działalności badawczo-rozwojowej, ekspansji międzynarodowej oraz procesów certyfikacyjnych – czyli obszarów kluczowych dla innowacyjności, konkurencyjności i zgodności z wymaganiami rynkowymi.

Wykres 41. Na jakie działania powinny być przeznaczone dotacje? (N=107)



Źródło: Analizy IBC Advisory S.A. na podstawie badania CAWI.

Respondenci najczęściej wskazywali, że dotacje powinny być przeznaczane na działania badawczo-rozwojowe (R+B). Taką odpowiedź wybrało łącznie 53 przedsiębiorstwa — 46 małych i 7 średnich. Kolejnym istotnym obszarem była ekspansja

działalności, wskazana przez 31 małych i 5 średnich firm. Certyfikację jako priorytet wskazało łącznie 17 firm (13 małych i 4 średnie). Kategoria „inne" pojawiła się jedynie w jednej odpowiedzi, udzielonej przez średnie przedsiębiorstwo. Wyniki te pokazują, że firmy oczekują przede wszystkim wsparcia w zakresie innowacji i rozwoju, a także w działaniach umożliwiających wejście na nowe rynki.

W odpowiedziach na pytanie o oczekiwaną lub wystarczającą wysokość dotacji pojawiło się wiele zróżnicowanych wskazań. Część respondentów podała konkretne kwoty, najczęściej mieszczące się w przedziale od 1 do 10 milionów złotych. Najniższe wskazane wartości to 3 000 zł, 100 000 zł oraz 200 000 zł, zarówno w złotych, jak i euro. Wskazywano również 300 000 zł rocznie, 500 000 zł, a także wartości w przedziale 1–2 milionów złotych (np. 1 mln, 2 mln, 2–5 mln). Pojawiły się też kwoty rzędu 3 mln, 6 mln oraz 10 mln zł, a pojedyncze odpowiedzi odnosiły się do jeszcze większych zakresów, takich jak „kilkanaście milionów złotych", „15–50 mln" czy nawet 50 mln zł. Niektóre odpowiedzi wskazywały ogólnikowo na „miliony" lub „x set tysięcy złotych".

Część wypowiedzi odnosiła się do wysokości dotacji w sposób procentowy lub warunkowy, np. jako 10% rocznego zysku netto, do 50% wartości projektu, w granicach pomocy de minimis lub do 200 000 zł w przypadku firm z rocznym przychodem do 1 miliona złotych. Kilku respondentów zaznaczało, że wysokość wsparcia powinna być dostosowana do rodzaju projektu, jego skali lub specyfiki branży R&D. Wskazywano również, że nie sama wysokość dotacji stanowi problem, ale konieczność wniesienia wkładu własnego oraz niestabilność otoczenia instytucjonalnego i politycznego.

Wypowiedzi wskazują także na potrzebę stworzenia lepiej zaprojektowanych, wieloetapowych programów wsparcia. Obecny model – oparty na pojedynczych grantach – jest uznawany za niewystarczający, zwłaszcza dla firm, które potrzebują ciągłości finansowania i systemowego modelu wzrostu. Jak ujął to jeden z respondentów:

> *„Grant się skończy, firma upada, a te osoby idą potem po kolejny grant. Nie ma takiej kontynuacji w ten sposób, bo jak są te wszystkie finansowania z serii A, B […]" ~ powiedział Respondent 8.*

W tym kontekście pojawiły się również postulaty silniejszego promowania europejskich dostawców – zwłaszcza w kontekście zamówień publicznych – tak jak czynią to inne kraje względem swoich firm narodowych.

> *„[...] zapewnić wsparcie czy przewagę konkurencyjną, czy przewagę w przetargach publicznych dla polskich przedsiębiorstw […] nie da się tego zrobić dla polskich przedsiębiorstw, ale zastanawiam się, czy Unia Europejska jako cała Unia nie powinna bardziej premiować po prostu europejskich firm. I nie chodzi o to tutaj, że firma z Ameryki ma oddział w Europie, tylko, że po prostu firma jest europejska. [..] W Stanach Zjednoczonych te firmy lokalne są zawsze lepiej premiowane. [..] Są lepiej postrzegane. I czemu my mielibyśmy tak nie robić? To wsparcie widziałbym raczej w takim zasięgu europejskim, bardziej jeżeli chodzi o konkurencyjność niż w jakimś polskim, lokalnym" ~ powiedział Respondent 9.*

Ryzyko utraty suwerenności cyfrowej

Publiczne środki przeznaczane na wdrażanie rozwiązań z zakresu cyberbezpieczeństwa – szczególnie w instytucjach publicznych takich jak szpitale – zostały ocenione pozytywnie jako ważny impuls inwestycyjny. Jednak nawet w tym obszarze pojawiły się istotne zastrzeżenia. Obawy budzi fakt, że środki te często trafiają w praktyce do zagranicznych producentów, co w dłuższej perspektywie może marginalizować lokalne firmy i osłabiać suwerenność cyfrową. Jak zauważył jeden z rozmówców:

> *„[…] właśnie te granty, które są udostępniane publicznym instytucjom tak jak obecnie np. szpitale, to nie do końca miałyby potencjał finansowy, żeby takie rozwiązania wdrażać u siebie. […] jeżeli doszłoby do tego, że zamiast stosowania naszych rozwiązań produkowanych tutaj w Polsce doszłoby do tego, że rozwiązania właśnie tych producentów amerykańskich byłby zastosowane, no to dla nas byłoby to oczywiście negatywne" ~ powiedział Respondent 10.*

Podsumowanie:

Polski sektor cyberbezpieczeństwa dostrzega szereg barier ograniczających jego rozwój, ale jednocześnie wykazuje wysokie poczucie sprawczości. Większość firm uważa, że wiele z tych przeszkód można pokonać na poziomie przedsiębiorstwa. Wskazuje się na potencjał reorganizacji, innowacji, inwestycji w kompetencje i nowe technologie. Wśród tych rozwiązań coraz większą rolę przypisuje się sztucznej inteligencji, której wdrożenie może zoptymalizować procesy i zwiększyć efektywność. AI postrzegana jest jako narzędzie wspierające automatyzację, analizę danych i podejmowanie decyzji. Mimo to, znaczna część firm podkreśla, że bariery systemowe – jak prawo, podatki czy certyfikacje – wymagają interwencji państwa.

Nie chodzi jednak o ingerencję w wolny rynek, lecz o stworzenie równych warunków konkurencji. Przedsiębiorcy oczekują od państwa roli katalizatora – partnera, a nie regulatora czy właściciela. Zwracają uwagę, że bez wsparcia instytucjonalnego trudno konkurować z firmami subsydiowanymi przez zagraniczne rządy. Uważają, że Polska powinna – podobnie jak USA, Francja czy Niemcy – promować i chronić rodzimy sektor cyberbezpieczeństwa. Postulują też długofalową strategię przemysłową oraz spójne działania instytucji państwowych.

Choć niektórzy doceniają poprawę dialogu z administracją, wielu respondentów wskazuje na brak przejrzystości, niewystarczającą skalę działań i zbyt skomplikowane procedury. Istnieje przekonanie, że część publicznych programów wsparcia ma charakter jedynie deklaratywny, a nie realnie operacyjny. Firmy narzekają na nadmiar dokumentacji, nieintuicyjne kryteria oraz długi czas oczekiwania na decyzje. Krytykowany jest również brak promocji polskich produktów i niewystarczające wsparcie eksportowe.

Najczęściej postulowane działania publiczne to ulgi podatkowe, dotacje oraz ułatwienia w dostępie do zamówień publicznych. Przedsiębiorcy chcą również uproszczenia procedur certyfikacyjnych oraz wsparcia promocji międzynarodowej. Wskazują na konieczność koordynacji między instytucjami, resortami oraz lepszą współpracę nauki z biznesem. Równolegle oczekują angażowania firm w projekty badawczo-rozwojowe oraz budowy infrastruktury wspierającej testowanie i wdrażanie rozwiązań.

Wielu respondentów zwraca uwagę na ryzyko marginalizacji polskich firm, jeśli wsparcie publiczne będzie trafiać głównie do zagranicznych dostawców. Ostrzegają, że może to prowadzić do utraty suwerenności cyfrowej i uzależnienia od zewnętrznych technologii. Podkreślają, że państwo powinno aktywnie promować europejskie i polskie rozwiązania, szczególnie w instytucjach publicznych. Zgłaszają także potrzebę stworzenia długofalowych programów wspierających rozwój – nie opartych na jednorazowych grantach, ale na wieloetapowym modelu finansowania.

Zauważalna jest również potrzeba zwiększenia edukacji na temat dostępnych instrumentów wsparcia. Firmy często nie aplikują o fundusze z powodu braku wiedzy, kompetencji lub zaufania do systemu oceny. Dodatkowo wskazują, że nawet najbardziej zaawansowane produkty technologiczne nie mają szans rozwoju bez odpowiedniego zaplecza sprzedażowego, promocyjnego i certyfikacyjnego. W tym kontekście promowanie startupów i MŚP wymaga działań wspierających ich profesjonalizację i skalowanie.

Część firm aktywnie korzysta z unijnych programów – takich jak Horyzont Europa czy Cyfrowa Europa – traktując je jako ważne źródło rozwoju. Inne dopiero planują aplikowanie, wskazując na wcześniejszy brak dopasowania oferty programowej do ich profilu. Firmy postulują też promowanie lokalnych rozwiązań przez administrację – poprzez rekomendacje, udział w wydarzeniach branżowych i wsparcie PR. Wspólnym mianownikiem wszystkich głosów jest oczekiwanie, że państwo przestanie być biernym obserwatorem, a stanie się aktywnym promotorem sektora.

Podsumowując, firmy z sektora cyberbezpieczeństwa wykazują silną wolę samodzielnego rozwoju, ale dostrzegają granice swoich możliwości bez systemowego wsparcia. Aby wykorzystać potencjał tej branży, konieczne jest zbudowanie partnerskiego ekosystemu, w którym państwo, biznes i nauka współpracują w sposób skoordynowany, długofalowy i transparentny.

Bibliografia

1. Artykuł ”Na czym polega ochrona danych osobowych RODO? Rozporządzenie RODO w pigułce”. EY, 2025.
2. Artykuł w portalu branżowym “Ekosystem rozwiązań cyberbezpieczeństwa w Polsce wart jest 12 mld zł.” ITwiz, 2024.
3. Artykuł w portalu branżowym “Poland Cybersecurity Market Size & Share Analysis – Growth Trends & Forecasts (2025–2030).” Mordor Intelligence.
4. Artykuł w portalu branżowym “Satus Starter VC zainwestował 2 miliony zł w Cybersecurity Studio”. MamStartup, 2021.
5. Artykuł w portalu branżowym „40 mln zł na cyberbezpieczeństwo od bValue. Fudo Security rozwinie skrzydła w USA.” XYZ, 2025.
6. Artykuł w portalu branżowym „Authologic z pomocą SMOK VC pozyskuje 8,2 mln dolarów na rozwój globalnej platformy weryfikacji tożsamości cyfrowej.” MyCompany Polska, 2022.
7. Artykuł w portalu branżowym „Biuro Informacji Kredytowej inwestuje w polski fintech Digital Fingerprints.” MamStartup, 2022.
8. Artykuł w portalu branżowym „Inwestycja 20 mln zł w Xopero.” CRN, 2024.
9. Artykuł w portalu branżowym „ResQuant z branży cybersecurity pozyskał finansowanie od Invento VC.” MamStartup, 2023.
10. Artykuł w portalu branżowym „To będą nowe polskie akceleratory. PARP ogłasza wyniki Startup Booster Poland – Smart UP.” MamStartup, 2024.
11. Artykuł “Bezpieczeństwo w chmurze”. Microsoft, 2025.
12. Artykuł “Building Trust for Today and Tomorrow”. PwC, 2025.
13. Artykuł “Co to jest zarządzanie dostępem i tożsamościami?”. Microsoft, 2025.
14. Artykuł “Cybersecurity Market Growth to Hit 15.9% CAGR Globally by 2030 – Exclusive Report by The Insight Partners.” GlobeNewswire, 8 Nov. 2023.
15. Artykuł “Digital Forensics and Incident Response Retainer Services Reviews and Ratings”. Gartner, 2025.
16. Artykuł “Network and Information Security Threat Landscape”. ENISA, 2023.
17. Artykuł “O SIlesia Smart Systems”, Silesia Smart Systems.
18. Artykuł “Penetration Testing and Red Teaming”. ENISA, 2023.
19. Artykuł “Security Awareness Training”. SANS Institute, 2025.
20. Artykuł “Szybka ścieżka – Innowacje cyfrowe (1/1.1.1/2022).” Narodowe Centrum Badań i Rozwoju.
21. Artykuł “Threat Landscape for Endpoint Security”. ENISA, 2023.
22. Artykuł “What Is a Security Operations Center (SOC)?”. IBM, 2024.
23. Artykuł “What Is Operational Technology (OT) Security?”. Cisco, 2025.
24. Artykuł „ORLEN VC z pierwszą polską inwestycją bezpośrednią.” PKN ORLEN, 2022.
25. Artykuł „Secfense pozyskuje 2 miliony dolarów w kolejnej rundzie inwestycyjnej.” Secfense, 2022.
26. Cybersecurity – Worldwide. Statista Market Forecast.
27. Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS2). Dz.U. L 333 z 27.12.2022.
28. Dyrektywa (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Dz.U. L 333 z 27.12.2022.
29. Informacja o firmie "DCD. Company. R&D", DCD, 2025.
30. Informacja o firmie "Perceptus. Projekty Unijne”, Perceptus, 2025.
31. Informacja o programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
32. Opis panelu „Szanse i Bariery dla MŚP działających w obszarze cyberbezpieczeństwa w Polsce” podczas Cybersec Forum w Katowicach, 2023 r. Gov.pl.
33. Publikacja “Vulnerability Management”. Qualys, 2023.

34. Raport “Polski rynek cyberbezpieczeństwa 2023–2028”. Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Październik. 2023, s. 128.
35. Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019.
36. Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022.
37. Rozporządzenie (UE) 2024/2847 z dnia 12 marca 2024 r. w sprawie horyzontalnych wymagań dotyczących cyberbezpieczeństwa dla produktów z elementami cyfrowymi oraz zmieniające rozporządzenie (UE) 2019/1020. Dz.U. L 333 z 27.12.2024.
38. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Ministerstwo Cyfryzacji, 2019.
39. Strona internetowa firmy „Atende inwestuje w Cryptomage – spółkę łączącą AI z cyberbezpieczeństwem sieciowym.” Atende, 2023.
40. Strona internetowa firmy „Techstep acquires software company Famoc, adding MMS capabilities.” Techstep, 10 maja 2021.
41. Strona internetowa PAIH “O projekcie – Polskie Mosty Technologiczne.” Polska Agencja Inwestycji i Handlu (PAIH).
42. Strona internetowa PARP “Go to Brand.” Polska Agencja Rozwoju Przedsiębiorczości (PARP).
43. Strona internetowa PFR “Dla działań wspierających rozwój technologii o potencjale podwójnego przeznaczenia”. Polski Fundusz Rozwoju S.A., 2024.
44. Strona internetowa Instytutu Łączności – Państwowego Instytutu Badawczego, Gov.pl.
45. Strona internetowa Łukasiewicz – AI, Gov.pl.
46. Strona internetowa Ministerstwa Cyfryzacji - Działania, Gov.pl.
47. Strona internetowa Ministerstwa Rozwoju i Technologii - działania ministerstwa, Gov.pl.
48. Strona internetowa Narodowego Centrum Badań i Rozwoju, Gov.pl.
49. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560.
50. Wpis na stronie kancelarii prawnej „We advised CyCommSec.” LLW Lewczuk Łyszczarek Szymczyk, 2025.
51. Wpis w portalu branżowym „Asseco Poland kupiło 69,01% akcji spółki ComCERT.” Money.pl, 2019.
52. Założenia programu B+R CyberSecIdent: Cyberbezpieczeństwo i eTożsamość, aktualizacja nr 4. Narodowe Centrum Badań i Rozwoju.

Spis wykresów i rysunków

Wykresy

***Wykres 1**. Jaki status posiada przedsiębiorstwo? (N=197) 20*
***Wykres 2.** Rodzaj działalności w branży cyberbezpieczeństwa (N=197) 21*
***Wykres 3.** Ile lat firma działa na rynku? (N=197) 22*
***Wykres 4.** Ile lat firma działa w obszarze cyberbezpieczeństwa? (N=197) 22*
***Wykres 5.** Firma jest: (N=197) 23*
***Wykres 6.** Czy firma należy do jakiejś organizacji branżowej (np. klastrów, izb przemysłowych)? (N=197) 24*
***Wykres 7.** Jakie technologie/usługi są rozwijane przez Państwa firmę? (N=197) 27*
***Wykres 8.** W jakim przedziale mieszczą się roczne dochody przedsiębiorstwa? (N=197) 28*
***Wykres 9.** Czy oferują Państwo swoje produkty w formie usług chmurowych, on-premise, czy w modelu hybrydowym? (N=197) 29*
***Wykres 10.** Czy korzystają Państwo z pośredników sprzedaży, takich jak integratorzy, dystrybutorzy lub resellerzy? (N=197) 30*
***Wykres 11.** Czy oferują Państwo produkty/usługi/technologie innych krajowych przedsiębiorstw? (N=51) 30*
***Wykres 12.** Jak oceniają Państwo potencjał merytoryczny swojej kadry? (N=197) 35*
Wykres 13. Jakie role wymienione w Europejskiej Ramie Umiejętności w zakresie Cyberbezpieczeństwa (ECSF) występują w Pana/Pani firmie? (N=197) 36
***Wykres 14.** Czy w ostatnim roku napotykali Państwo trudności w zatrudnieniu odpowiednio wykwalifikowanych pracowników? (N=197) 38*
***Wykres 15.** Czy w najbliższym roku planują Państwo inwestycje? (N=197) 45*
***Wykres 16.** Czy planowane inwestycje, dotyczą infrastruktury R+B? (N=96) 46*
***Wykres 17.** Czy planowane jest rozszerzenie działalności: (N=197) 47*
***Wykres 18.** Czy korzystali Państwo z usług akceleratorów lub inkubatorów technologicznych? (N=197) 49*
***Wykres 19.** Czy w Państwa przedsiębiorstwie istnieje wiedza na temat procesu certyfikacji? (N=197) 50*
***Wykres 20.** Czy mają Państwo plany certyfikacji produktów/usług? (N=197) 51*
***Wykres 21.** Czy przedsiębiorstwo posiada patenty/ licencje/ znaki towarowe/ wzory użytkowe, etc. związane z produktami/usługami? (N=197) 52*
***Wykres 22** Liczba certyfikatów/ akredytacje/ jakość / dopuszczenia (N=71) 52*
***Wykres 23** Ile patentów/ licencji/ znaków towarowych/ wzorów użytkowych, etc., związane z produktami/usługami posiada Państwa firma? (N=69) 53*
***Wykres 24.** Czy firma korzystała wcześniej ze wsparcia krajowego lub unijnego w celu wsparcia rozwoju (np. projekty R+B)? (N=197) 54*
***Wykres 25.** Jaki był powód niekorzystania z takiej formy wsparcia (wsparcie rozwoju np. projekty R+B)? (N=152) 54*
***Wykres 26.** Czy firma korzystała wcześniej ze wsparcia krajowego lub unijnego w celu ekspansji firmy z branży cyberbezpieczeństwa? (N=197) 56*
***Wykres 27.** Jaki był powód niekorzystania z takiej formy wsparcia (ekspansja firmy)? (N=153) 57*
***Wykres 28.** Czy firma zna programy unijne wspierające rozwój produktów/usług (np. Horyzont Europa, FENG, Cyfrowa Europa)? (N=197) 59*
***Wykres 29.** Czy w ostatnich 3 latach przedsiębiorstwo otrzymało wsparcie z prywatnego finansowanie (np. venture capital, private equity)? (N=197) 61*
***Wykres 30.** Jeśli nie, jaki był tego powód? (N=156) 61*
***Wykres 31.** Jaki jest zasięg działalności Państwa firmy? (N=197) 67*
***Wykres 32.** Czy Państwa firma ma bariery rozwojowe? (N=197) 71*
***Wykres 33.** Jeśli nie planują Państwo rozszerzenia działalności, co jest głównym powodem? (N=70) 72*
***Wykres 34.** Jakie bariery rozwoju Państwa firmy są obecnie największym wyzwaniem? (N=49) 73*
***Wykres 35.** Czy wie Pan/Pani, czym są regulacje CRA i NIS2? (N=197) 82*
***Wykres 36.** Czy Pana/Pani zdaniem, bariery rozwojowe mogą zostać pokonane na szczeblu przedsiębiorstwa? (N=197) 87*
***Wykres 37.** Czy Pana/Pani zdaniem, bariery rozwojowe mogą być pokonane bez interwencji państwa? (N=197) 87*
***Wykres 38.** Czy Pana/Pani zdaniem, sztuczna inteligencja może przyczynić się do pokonania barier rozwojowych? (N=197) 88*

Wykres 39. *Czy uważa, Pan/Pani, że zostały podjęte działania dotyczące rynku cyberbezpieczeństwa, które wymagają usprawnienia? (N=197)* *89*
Wykres 40. *Jakie działania publiczne byłyby najbardziej pomocne? (N=197)* *90*
Wykres 41. *Na jakie działania powinny być przeznaczone dotacje? (N=107)* *91*

Mapy

Mapa 1. *Rozkład przestrzenny przedsiębiorstw z branży cyberbezpieczeństwa* *16*

Rysunki

Rysunek 1. *Powiązania kooperacyjne* *69*

Raport *„Mapa MŚP sektora cyberbezpieczeństwa w Polsce: diagnoza, potrzeby, rekomendacje*" jest autorską publikacją IBC Advisory S.A., przygotowaną przez ekspertów IBC na zamówienie Ministra Cyfryzacji.

Cytowanie: Kołodziej E., Grzęda Ł., Gawron Ł., Pardyak O., Kamińska E., Wojtyczek K., Kolorz R., Jacak, P. (2025), *Mapa MŚP sektora cyberbezpieczeństwa w Polsce: diagnoza, potrzeby, rekomendacje*, IBC Advisory S.A., Warszawa.

Kontakt w sprawie badania:
ibc@ibc-advisory.pl

Autorzy
Emilian Kołodziej
dr Łukasz Grzęda
Łukasz Garwon
Oskar Pardyak
Ewa Kamińska
Karolina Wojtyczek
Rafał Kolorz
Paweł Jacak

Opracowanie

IBC Advisory Spółka Akcyjna

ZESPÓŁ REDAKCYJNY

Ewa Kamińska
Oskar Pardyak

WSPÓŁPRACA MERYTORYCZNA

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland

PROJEKT GRAFICZNY I SKŁAD

Krystian Ścipień

Warszawa, 2025

Wszelkie dane i projekcje zawarte w niniejszej publikacji dokonane zostały w oparciu o badania pierwotne i najnowsze dane z baz i rejestrów publicznych. Przedmiotem prac firmy IBC w ramach opracowania niniejszego raportu, była kompleksowa analiza polskiego sektora małych i średnich przedsiębiorstw prowadzących działalność w branży cyberbezpieczeństwa. Analizy zostały wykorzystane w oryginalnym kształcie do zasilenia mapy polskiej branży cyberbezpieczeństwa MŚP w Polsce.

Niniejszy raport został sporządzony przez konsultantów IBC na zlecenie Ministerstwa Cyfryzacji. Został sporządzony z należytą starannością, jednak z konieczności pewne informacje zostać mogły podane w nim w skróconej lub ogólnej formie. Publikacja ma charakter informacyjny. Zawarte w niej dane przed podjęciem decyzji inwestycyjnych nie powinny zastąpić profesjonalnego doradztwa. IBC dostarcza dane do projektowania oraz ewaluacji interwencji i polityk publicznych. Wspieramy działania strategiczne ministerstw, największych instytucji sektora publicznego i biznesowych liderów polskiej gospodarki aktywnych w obszarach inteligentnych specjalizacji. Dane, które gromadzimy są analizowane w zaawansowanych aplikacjach statystycznych w oparciu o dedykowane każdemu projektowi algorytmy. Wykorzystując własną metodologię gromadzenia i analityki danych, stworzyliśmy ofertę badawczą, która pozwala dotrzeć do informacji i danych o beneficjentach, konsumentach oraz 27 rynkach UE.

IBC

| Badania społeczne i ewaluacyjne| Analityka danych | Modelowanie ekonometryczne | Badania Ekonomiczne

www.ibc-advisory.pl

NCC-PL Krajowe Centrum Kompetencji Cyberbezpieczeństwa

Ministerstwo Cyfryzacji

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE