NCBR
Narodowe Centrum Badań i Rozwoju

Raport 1

Cyberbezpieczeństwo:
Strategiczna rola sektora w państwie

CYBERBEZPIECZEŃSTWO

Michał Baranowski
Robert Kostka-Zawadzki
Katarzyna Krok
Paweł Maj
Bartosz Mirowski

Warszawa, czerwiec 2025

Sekcja Analiz i Ewaluacji, NCBR

SPIS TREŚCI

Kluczowe wnioski	4
Wprowadzenie: Znaczenie cyberbezpieczeństwa we współczesnym świecie	7
Łańcuch wartości i główni gracze na rynku cyberbezpieczeństwa	13
Kluczowe segmenty usług	19
Wyzwania dla rozwoju technologii na rzecz cyberbezpieczeństwa	24
Trendy B+R w cyberbezpieczeństwie	32
Cyberbezpieczeństwo – priorytety Polski	39
Potencjał sektora prywatnego w Polsce	46
Stan cyberbezpieczeństwa przedsiębiorstw w Polsce	52
Wsparcie publiczne	60
Wsparcie NCBR obszaru cyberbezpieczeństwa	63
Obszary wymagające wsparcia	68
Podsumowanie i rekomendacje dla NCBR	72
Aneks 1: Metodologia	76

Niniejsze opracowanie jest kolejną częścią szerszego projektu realizowanego w Sekcji Ewaluacji i Analiz tzw. **Projektu analiz sektorowych**. Projekt ten ma dwa główne cele:

1. identyfikację i analizę kluczowych branż i sektorów o dużym potencjale wzrostu;
2. uzyskanie odpowiedzi na pytanie, czy należy wspierać polski biznes przede wszystkim w oparciu o strategię szerokiej dywersyfikacji, czy też bardziej efektywnym działaniem jest skupienie się na kilku wybranych branżach o największy potencjale rozwojowym?

Realizacja projektu opiera się w dużym stopniu na wcześniej zaproponowanej autorskiej metodologii.

Składa się ona z kilku zazębiających się ze sobą etapów:

- oceny branży od strony finansowej,
- oceny branży od strony potencjału strategicznego, na ile dana branża ma w sobie tzw. potencjał interwencyjny (czyli np. potencjał rozwojowy wynikający np. z narastającego zapotrzebowania społecznego, zdrowotnego, wynikający z narastających problemów, jak np. niż demograficzny, chorób podeszłego wieku (Alzhaimer), czy też rosnącej liczby osób cierpiących na otyłość),
- oceny branży od strony od strony potencjału technologicznego,
- oceny branży dokonanej w szerszym kontekście, czyli „trendów” (np. tzw. analiz typu PEST itp.).
- potencjału naukowo –badawczego

Wskazaliśmy, że naszym zdaniem **obecnie mamy do czynienia z czterema tzw. kluczowymi mega trendami,** tworzącymi kontekst dla rozwoju nowoczesnych technologii właściwe we wszystkich branżach. Na każdy z tych trendów można spojrzeć od strony potencjału różnych branż, które wykorzystują lub mogą w najbliższej przyszłości wykorzystać je do swojego rozwoju.

1. bardzo dynamicznym rozwojem sztucznej inteligencji,
2. narastającą niepewnością geopolityczną,
3. widocznymi coraz silniej zmianami klimatu
4. systematycznym spadkiem dzietności i starzeniem się społeczeństw.

Dotychczas zaprezentowaliśmy opracowania tematyczne dla następujących sektorów:

- metali ziem rzadkich
- Technologii krytycznych wchodzących w zakres instrumentu STEP (instrument wdrażany w ramach programu FENG) – biotechnologii, technologii zasobooszczędnych i technologii cyfrowych

W tym raporcie postanowiliśmy przyjrzeć się uważniej **rynkowi cyberbezpieczeństwa** pod kątem trendów, niezbędnych obszarów wsparcia i zasadności wsparcia publicznego, szczególnie w obszarze rozwoju nowych technologii i zastosowań dla krajowych rozwiązań cyberbezpieczeństwa . Wychodzimy bowiem z założenia, że obszar ten jest kluczowy z punktu widzenia bezpieczeństwa narodowego i zapewnienia ciągłości funkcjonowania strategicznych obszarów życia publicznego.
Jednocześnie jesteśmy świadkami nieustającego wyścigu między przestępcami a cyberobrońcami, co wymusza ciągłe doskonalenie i tym samym inwestowanie w ten obszar ze strony państwa.

Narodowe Centrum Badań i Rozwoju

Kluczowe wnioski

Najważniejsze wnioski

- **Wraz z dynamicznym wzrostem wydatków na cyberbezpieczeństwo rośnie również liczba cyberataków**, co czyni inwestycje w ten obszar, szczególnie w nowe rozwiązania technologiczne nieustająco ważnym
- **Rynek odbiorców** cyberbezpieczeństwa zdominowany jest przez duże firmy (ok 60% rynku) , ale **najszybciej rosnącym segmentem jest sektor MŚP m.in za sprawą dostępności tanich rozwiązań chmurowych oraz rosnącej świadomość zagrożeń.**
- Wśród usług o najwyższym potencjale wzrostu są **te związane z elastycznym wykyrwaniem i reagowaniem na zagrożenia, zapewnieniem bezpieczeństwa sieci i zapobieganiem utracie danych**
- Tematyka cyberbepieczeństwa jest dość powszechnie reprezentowana zarówno w publikacjach naukowych (155 tys. w latach 2021-2024) jak i patentach (345 tys. w latach 2021-2024). Pośrednio **świadczy to o intensyfikacji aktywności B+R+I w tym obszarze**.
- W przeciągu ostatniego dziesięciolecia roczna liczba nowych publikacji podwoiła się, a liczba patentów zwiększyła trzykrotnie.
- Najwięcej publikacji naukowych powstaje w Chinach, Stanach Zjednoczonych i w Unii Europejskiej
- Stany Zjednoczone dominują jeśli chodzi o pochodzenie patentów
- Najpopularniejszą tematyką zarówno w artykułach naukowych jak i w patentach są **protokoły bezpieczeństwa (kryptograficzne)**
- Najczęściej występującymi zagrożeniami, które są wskazywane w artykułach naukowych i patentach z ostatnich dziesięciu lat są **trojany** i złośliwe oprogramowanie – **malware**
- Strategia Polski w obszarze cyberbezpieczeństwa kładzie nacisk na **budowę odpornego systemu narodowego cyberbezpieczeństwa, ochronę usług kluczowych i infrastruktury krytycznej oraz inwestycje w krajowe technologie i kompetencje**
- Kwestia cyberbezpieczeństwa wymusza integrację obrony cywilnej i militarnej oraz współpracę na rzecz rozwiązań podwójnego zastosowania.
- **Wsparcie publiczne** ze środków **w Polsce** w obszarze cyberbezpieczeństwa służy **przede wszystkim rozbudowie i wzmocnieniu Krajowego Systemu Cyberbezpieczeństwa**, tj włączeniu nowych podmiotów, zwiększeniu skuteczności operacyjnej jego działania - są to zatem działania o charakterze systemowym. Jest to działanie wprost wynikające i spójne ze strategią Państwa.
- W obecnej perspektywie finansowej na cele związane z cyberbezpieczeństwa zostanie przekazanych w Polsce **ponad 1 mld EUR**. **Brakuje jednak wsparcia publicznego ukierunkowanego wprost na działalność B+R i wykorzystanie nowych technologii**
- Tego typu wsparcie – m.in. wykorzystanie **technologii AI, big data i szyfrowanie postkwantowe jest natomiast w agendzie działań finansowanych ze środków Komisji Europejskiej**
- W Polsce obszar cyberbezpieczeństwa, w tym **działania B+R+I i kształcenie kadr, wspierany jest przez wojsko m.in. w ramach programu Ministerstwa Obrony Narodowej CyberMil.PL**

- Wyniki ewaluacji programu wdrażanego w NCBR - CyberSecident wskazują również na potrzebę **wsparcia w większym stopniu rozwiązań na rzecz zapobiegania zagrożeniom bezpośrednio dotykającym obywateli** oraz procedur postępowania dla obywateli w momencie zetknięcia się z cyberprzestępstwem lub jego następstwami

- **NCBR od 2007 dofinansowało ponad 130 projektów** mających związek z cyberbezpieczeństwem **na kwotę około 1,8 mld zł**, w tym w ramach programu tematycznego –CyberSecIdent dofinansowano 22 projekty na kwotę 240 mln zł.

- Najwięcej projektów było skierowanych na ochronę końcowych odbiorców/urządzeń narażonych na cyberataki - tzw endpoint security

- Potencjał firm polskich do wprowadzania na rynek nowych rozwiązań z obszaru cyberbezpieczeństwa rośnie. Sam **rynek cyberbezpieczeństwa w Polsce w 2024 r osiągnął ok 3 mld zł, a dwucyfrowy wzrost obserwujemy na nim od kilku lat.**

- W szerokim ujęciu obejmującym także działalność związaną z **chmurą obliczeniową, rynkiem usług data centrowych, backup, hosting powoduje wzrost do poziomu ok 12 mld zł**

- Obserwujemy także **wzrost inwestycji związanych z cyberbezpieczeństwem przez polskie fundusze Venture Capital .** W 2024 był to czwarty pod względem znaczenia obszar inwestycyjny

- Zdecydowana większość firm w Polsce deklaruje działania na rzecz zwiększania cyberbezpieczeństwa w procesie wdrażania nowych technologii, w tym AI, ale obserwujemy **dysproporcję miedzy świadomością zagrożeń, a realnymi działaniami zaradczymi.**

- **Tylko 2% przedsiębiorstw wykorzystuje nowoczesne technologie AI do wzmocnienia swojego cyberbezpieczeństwa. Wśród dużych firm udział ten wzrasta do 17,5%**

- Około **13% planuje inwestować w rozszerzenie** rozwiązań na rzecz cyberbezpieczeństwa wykorzystujących **AI i deep learning, a około 1/5 planuje w ogóle ich wdrożenie. W jeszcze mniejszym stopniu firmy są gotowe** do wdrożenia nowoczesnych technologii UBA/UEBA wykorzystujących m.in. analizy behawioralne i uczenie maszynowe **do detekcji nietypowych zachowani użytkowników**

- MŚP wymaga znacznych inwestycji w obszarze cyberbezpieczeństwa. Jedynie około 80% tej grupy zabezpiecza swoje zasoby ICT przez uwierzytelnienie hasła dostępowego, a **tylko ok. 60% kontroluje w ogóle dostęp przedsiębiorstwa do sieci.**

- W ujęciu branżowym **krytyczne jest wsparcie c**yberzabezpieczeń podmiotów **zajmujących się dostawą kluczowych usług dla społeczeństwa – dostawą energii i dostawą wody**, z których 20% **nie stosuje zabezpieczeń kontroli dostępu do sieci.**

- Istotne jest także **wzmocnię zabezpieczeń dla operatorów infrastruktury sieciowej i transportowej w powietrzu, na lądzie i w wodzie,** które są chronione w niewystarczającym stopniu w całej UE

NCBR
Narodowe Centrum Badań i Rozwoju

Wprowadzenie: Znaczenie cyberbezpieczeństwa we współczesnym świecie

Cyberbezpieczeństwo to dziedzina zajmująca się ochroną systemów komputerowych, sieci, urządzeń oraz danych przed nieautoryzowanym dostępem, atakami, kradzieżą lub uszkodzeniem. Obejmuje zarówno technologie, jak i procesy oraz praktyki mające na celu zapewnienie bezpieczeństwa cyfrowego.

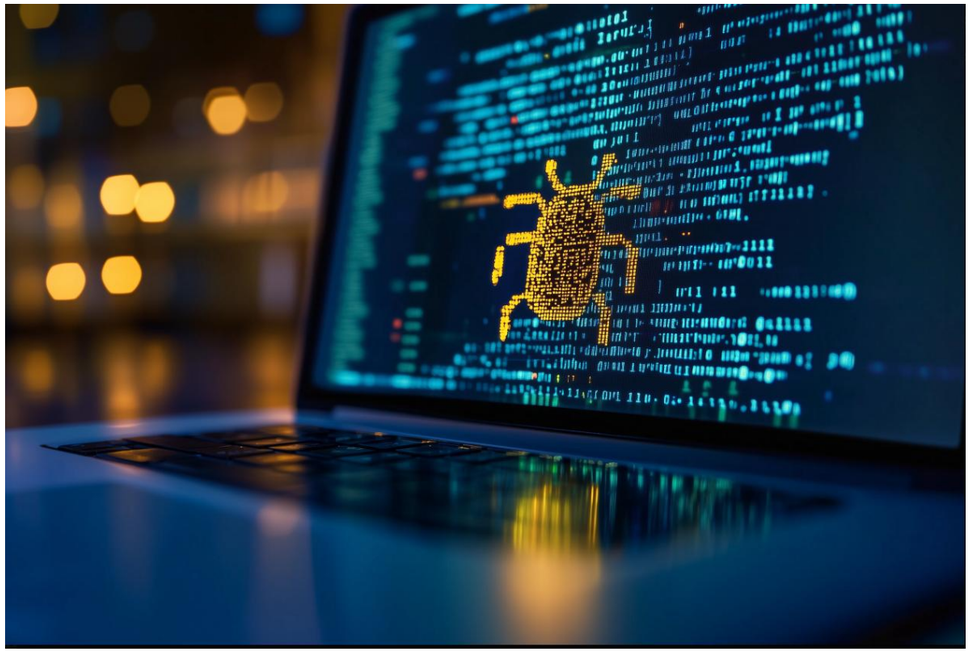
Celem cyberbezpieczeństwa jest zapewnienie poufności, integralności i dostępności danych, określanych jako **triada CIA (ang. Confidentiality, Integrity, Availability)**. Poufność chroni dane przed nieuprawnionym dostępem, integralność zapewnia, że informacje nie są zmieniane w nieautoryzowany sposób, a dostępność gwarantuje, że systemy i dane są dostępne dla uprawnionych użytkowników w odpowiednim czasie.

Realizacja tych celów wymaga stosowania zaawansowanych technologii, takich jak szyfrowanie, firewalle czy systemy wykrywania intruzów, a także edukacji użytkowników w zakresie bezpiecznych praktyk.

Cyberzagrożenia stanowią **jedno z najistotniejszych wyzwań dla sfery publicznej i prywatnej** w związku z postępującą cyfryzacją. Ich katalog nieustannie się rozszerza, a to wymaga ciągłego monitorowania trendów oraz doskonalenia rozwiązań i systemów cyberbezpieczeństwa.
Rosnące zagrożenie ze strony cyberprzestępców w Polsce potwierdzają dane Ministerstwa Cyfryzacji, które wskazują że **w samym 2024 roku zarejestrowano łącznie 111 660 potwierdzonych incydentów bezpieczeństwa na poziomie krajowym, co stanowi wzrost o 23%** w stosunku do roku wcześniejszego. Wiele z tych ataków **nakierowanych jest na infrastrukturę krytyczną państwa**, a to zagraża bezpieczeństwu kraju.

W związku z tym na cyberbezpieczeństwo należy patrzeć z kilku różnych perspektyw. **Dzisiaj bowiem problemy cyberbezpieczeństwa przestają być tylko domeną technologii informatycznych, a stają się nierozerwalne z bezpieczeństwem**.. Skala rażenia cyberataków może być bardzo dotkliwa dla fizycznej egzystencji całych państw: ich infrastruktury energetycznej, wodociągowej, nie wspominając już o tych związanych z komunikacją, dostępnością i bezpieczeństwem kluczowych danych itd. **Tradycyjne modele bezpieczeństwa często nie nadążają za nowymi formami cyberzagrożeń i wymagają stałego rozwoju i nowych narzędzi**

Cyberbezpieczeństwo to zestaw praktyk, procesów i technologii, które mają na celu ochronę systemów komputerowych, sieci i danych przed nieautoryzowanym dostępem, atakami czy zniszczeniem.



Cyberbezpieczeństwo jest istotne dla a wszelkich sfer życia publicznego

Kluczowe zadania cyberbezpieczeństwa

- **ochrona danych** – prywatne i firmowe informacje są narażone na wyciek i kradzież;
- **zapewnienie ciągłości działania** – skuteczne zabezpieczenia minimalizują ryzyko przerw w pracy systemów;
- **budowanie zaufania** – zabezpieczone systemy IT zwiększają wiarygodność firmy w oczach klientów i partnerów.

Wpływ na różne sfery życia publicznego

- **infrastruktura krytyczna -** przerwy w dostawach usług i utrata danych klientów oraz danych przemysłowych, narażenie bezpośrednio bezpieczeństwa państwa oraz zdrowia życia obywateli.
- **instytucje rządowe i administracja publiczna -** utrata danych obywateli oraz zakłócenie w świadczeniu usług publicznych, narażenie bezpieczeństwa obywateli i ciągłości funkcjonowania państwa.
- **przemysł -** przerwy w produkcji, utrata danych oraz wielomilionowymi straty finansowe
- **finanse -** kradzież danych, straty finansowe oraz oszustwa związane z transakcjami online.
- **edukacja i Badania -** utrata danych osobowych uczniów i pracowników, szpiegostwo technologicznego, zakłócenia w procesach edukacyjnych.

W ostatnich latach nasiliły się następujące zagrożenia:

- **Ataki ransomware**: polegające na zablokowaniu dostępu do danych i żądaniu okupu za ich odblokowanie, stały się coraz bardziej powszechne i zaawansowane.
  W 2024 roku znaczący wzrost takich incydentów
- **Ataki sponsorowane przez państwa**: grupy hakerskie wspierane przez państwa, takie jak „Midnight Blizzard" (prawdopodobnie rosyjski), prowadzą ataki mające na celu kradzież poufnych informacji.
  W 2024 roku wzrost takich działań w kontekście konfliktów geopolitycznych.
- **Phishing i social engineering**: metody manipulacji użytkownikami w celu uzyskania dostępu do danych lub systemów pozostają jednymi z najczęstszych form ataków.
  W 2024 roku -odpowiedzialny za ponad 60% zgłoszonych incydentów w Polsce.
- **Ataki na infrastrukturę krytyczną**: coraz częstsze są ataki na systemy energetyczne, transportowe i inne kluczowe dla funkcjonowania państwa.
  W 2024 roku o wzrost takich incydentów, co podkreśla Ministerstwo Cyfryzacji.
- **Wykorzystanie sztucznej inteligencji przez cyberprzestępców**: AI jest używane do automatyzacji i personalizacji ataków, co czyni je bardziej skutecznymi i trudniejszymi do wykrycia.

Przyszłe zagrożenia:

- **Ataki wykorzystujące kwantowe obliczenia**: kwantowe komputery mogą potencjalnie złamać obecne metody szyfrowania, co wymaga opracowania nowych, odpornych na ataki kwantowe metod ochrony danych.
- **Zaawansowane ataki na urządzenia IoT**: zwiększająca się liczba urządzeń Internetu Rzeczy (IoT) stwarza nowe możliwości dla cyberprzestępców do przeprowadzenia masowych ataków, szczególnie w smart cities i systemach przemysłowych.

Odpowiedź rynku na zagrożenia

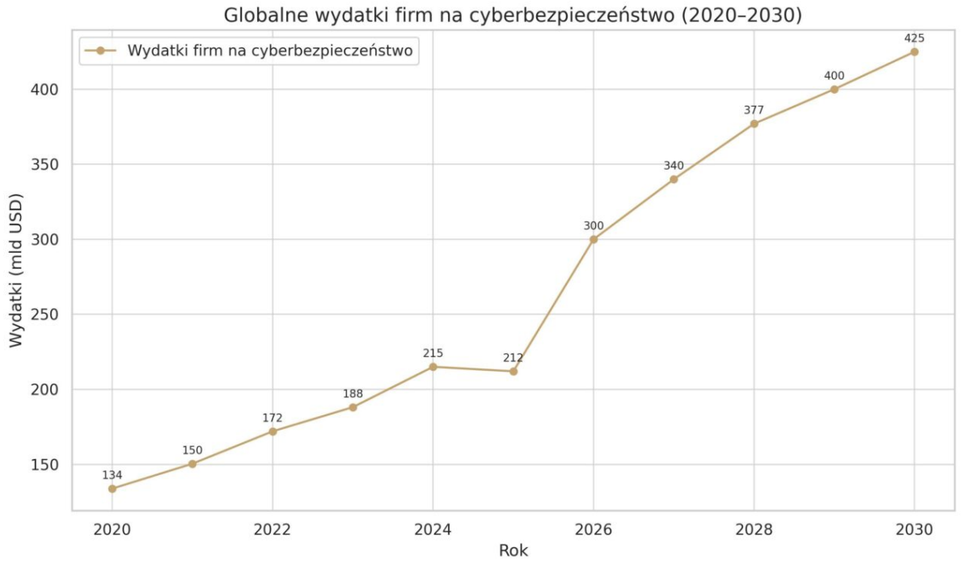
Sektor prywatny

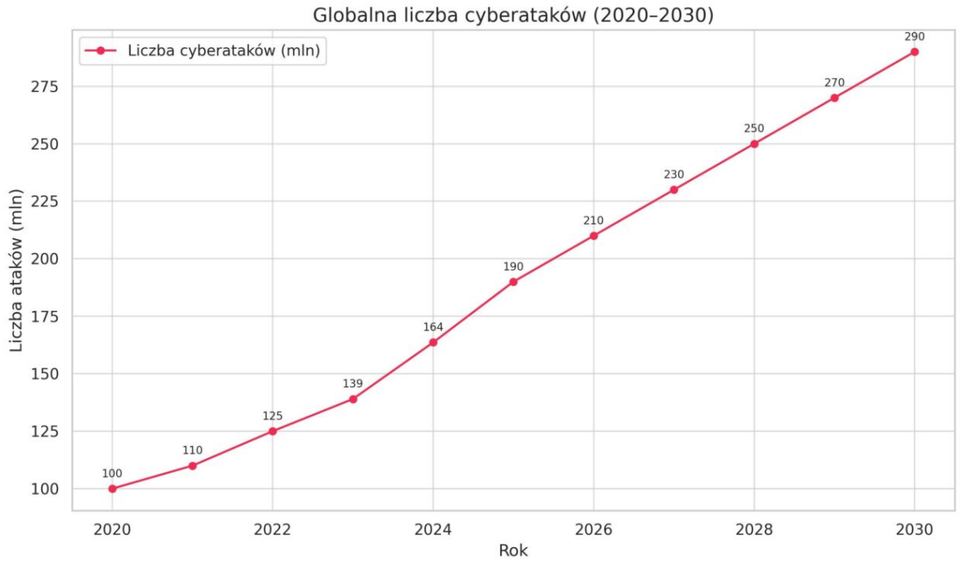
- **Wdrażanie zaawansowanych technologii**: firmy takie jak Microsoft czy SentinelOne inwestują w technologie takie jak sztuczna inteligencja do wykrywania zagrożeń, architektura zero trust oraz zabezpieczenia chmurowe (Microsoft, SentinelOne).
- **Rozwój usług doradczych**: firmy konsultingowe, takie jak EY, oferują usługi w zakresie analizy ryzyka i zarządzania incydentami, dostosowane do polskich realiów
- **Instytucje badawcze i uczelnie**
- Badania i rozwój: instytucje takie jak NASK (Państwowy Instytut Badawczy) prowadzą badania nad nowymi narzędziami, takimi jak Artemis czy Snitch, które wspierają ochronę cyberprzestrzeni (CERT Polska).
- **Edukacja**: uczelnie, takie jak Uniwersytet Ekonomiczny we Wrocławiu, oferują programy szkoleniowe i kursy z zakresu cyberbezpieczeństwa, aby zwiększyć liczbę wykwalifikowanych specjalistów (Uniwersytet Ekonomiczny).

Sektor publiczny

- **Regulacje i strategie**: w Polsce obowiązuje Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r., a Ministerstwo Cyfryzacji przygotowuje jej nowelizację, aby dostosować się do unijnej dyrektywy NIS2 (Ministerstwo Cyfryzacji).
- **Fundusz Cyberbezpieczeństwa**: utworzony w 2021 r., wspiera wynagrodzenia specjalistów w sektorze publicznym, aby konkurować z sektorem prywatnym (Portal Gov.pl).
- **CSIRT i CERT**: zespoły takie jak CSIRT NASK, CSIRT GOV i CSIRT MON koordynują obsługę incydentów i prowadzą działania prewencyjne (Ministerstwo Cyfryzacji).

Dynamicznemu wzrostowi wydatków na cyberbezpieczeństwo towarzyszy rosnąca liczba cyberataków



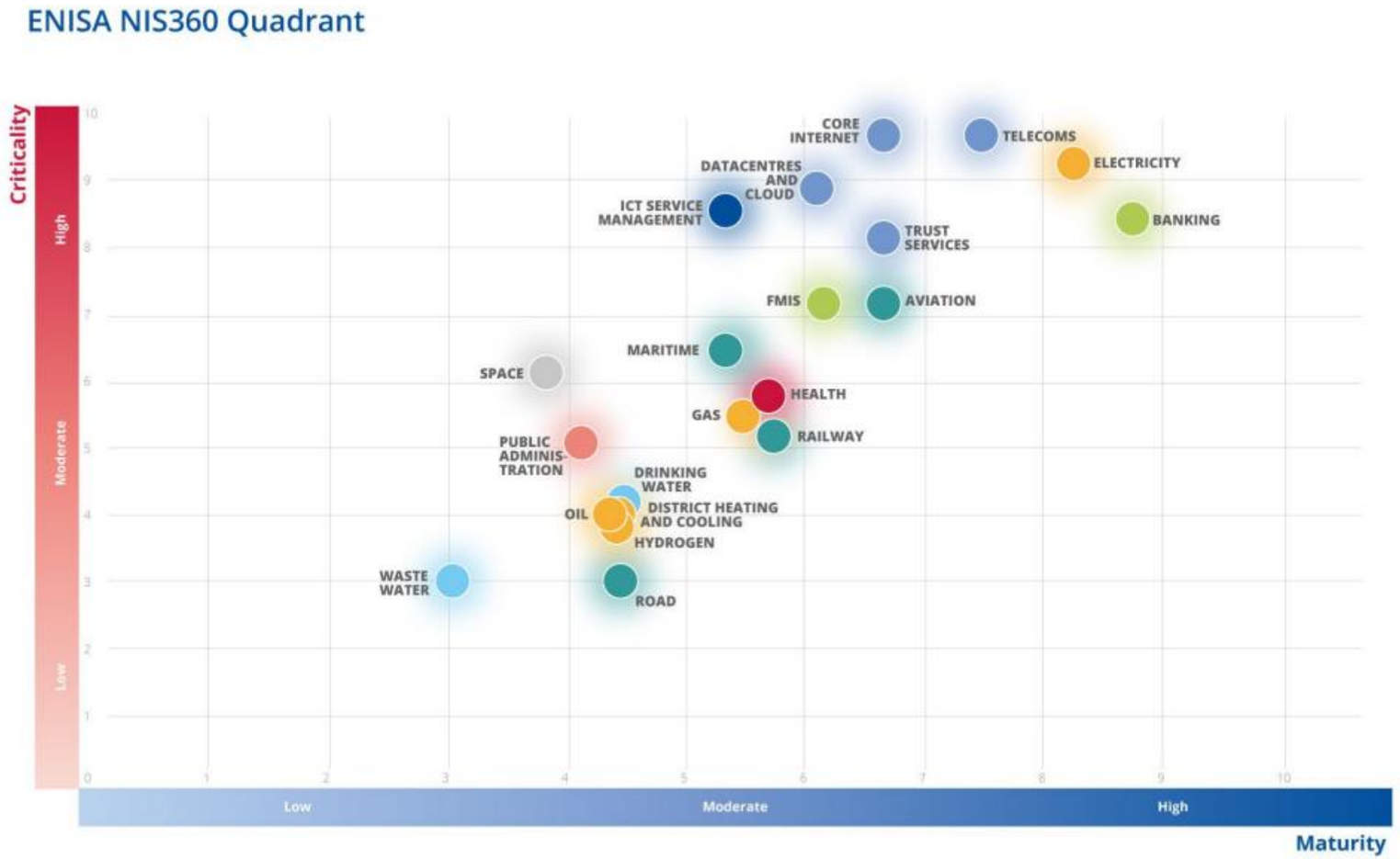


https://brandsit.pl/cyberparadoks-dlaczego-mimo-miliardow-na-cyberbezpieczenstwo-firmy-sa-coraz-bardziej-narazone/

Rosnącą liczbę cyberataków przy jednoczesnym wzrostem wydatków na cyberbezpieczeństwo można tłumaczyć, m.in.:

- **Wzroste, złożoności i dostępności technologii:** wraz z rozwojem technologii (np. chmura, IoT, AI) rośnie powierzchnia ataku. Cyberprzestępcy wykorzystują nowe technologie i ich luki, co sprawia, że nawet większe inwestycje w zabezpieczenia nie zawsze nadążają za nowymi zagrożeniami.
- **Profesjonalizacją**: ataki są coraz bardziej wyrafinowane, a cyberprzestępcy działają jak zorganizowane grupy, często finansowane przez państwa lub grupy przestępcze. Oferują narzędzia i usługi (np. ransomware-as-a-service) na czarnym rynku, co obniża barierę wejścia dla nowych atakujących.
- **Asymetrią kosztów**: atak jest tańszy niż obrona. Cyberprzestępca musi znaleźć tylko jedną lukę, podczas gdy firmy muszą zabezpieczyć wszystkie możliwe punkty wejścia. Wydatki na cyberbezpieczeństwo są więc wysokie, ale nie gwarantują pełnej ochrony.
- **Czynnikiem ludzkim**: nawet najlepsze systemy mogą zostać naruszone przez błąd człowieka, np. phishing czy słabe hasła. Szkolenia pracowników są kosztowne i nie zawsze skuteczne.
- **Opóźnieniem w adaptacji**: organizacje często inwestują w rozwiązania reaktywne, zamiast proaktywnych. Gdy nowe zagrożenie zostanie zidentyfikowane, wdrożenie zabezpieczeń zajmuje czas, co daje przewagę atakującym.
- **Wzrostem liczby celów**: rosnąca digitalizacja sprawia, że coraz więcej firm i urządzeń jest podłączonych do sieci, co zwiększa liczbę potencjalnych celów dla hakerów.
- **Niedoborem specjalistów**: pomimo większych budżetów, brakuje wykwalifikowanych ekspertów ds. cyberbezpieczeństwa, co ogranicza efektywność inwestycji.

Poziom cyberzabezpieczenia krytycznych sektorów funkcjonowania państwa w UE jest zróżnicowany szczególnego wsparcia wymaga nadal ochrona infrastruktura transportowej i przesyłowej



ENISA NIS360 2024; ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors, luty 2025

Trzy sektory wyróżniają się pod względem ogólnej dojrzałości w zakresie cyberbezpieczeństwa i jednocześnie kluczowego znaczenia dla stabilności społecznej i gospodarczej: **energia elektryczna, telekomunikacja i bankowość**.

Sektor infrastruktury cyfrowej obejmujący m.in. podstawowe usługi internetowe, centra danych i usługi w chmurze oraz zarzadzanie usługami ICT mają również krytyczne znaczeniu dla stabilności funkcjonowania państwa, wymagają nadal działań w celu zapewnienia pełnej dojrzałości pod względem zapewnienie cyberbezpieczeństwa

Sektory: przestrzeń kosmiczna, sektor morski, zdrowie i gaz mają ponadprzeciętne znaczenie dla zapewnienia ciągłości funkcjonowania speołeczno – gospodarczego ,ale charakteryzują się niższym niż średnia poziomem dojrzałości w zakresie cyberbezpieczeństwa.

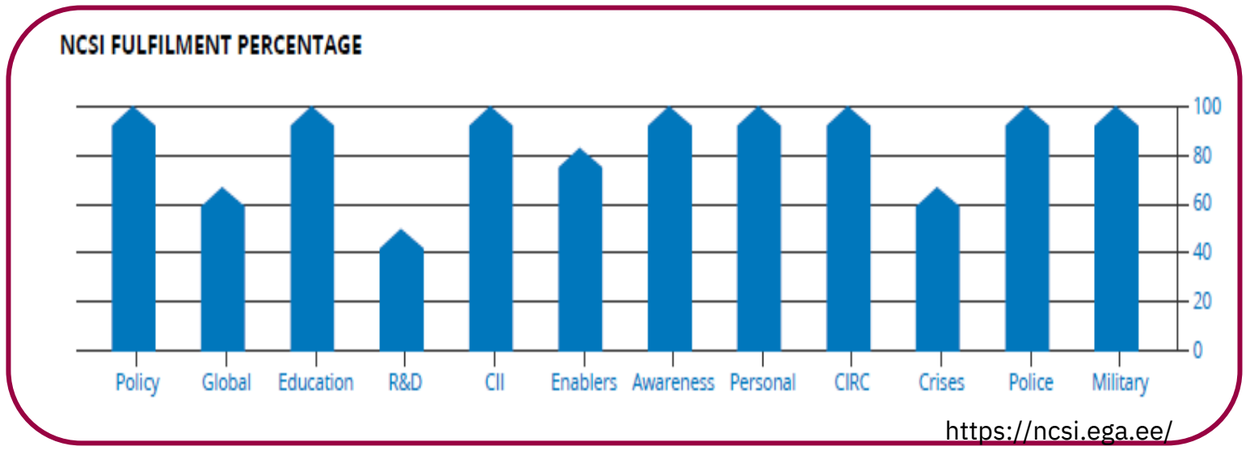
Pozycja Polski w światowym rankingu cyberbezpieczeństwa jest bardzo wysoka – 4 miejsce, choć obszar B+R wymaga zdecydowanej poprawy

Narodowy Indeks Bezpieczeństwa Cybernetycznego opracowany przez estońską Akademię e-Governance

4. Poland 92.50

Population	36.7 million
Area (km²)	312.7 thousand
GDP per capita ($)	46.6 thousand

4th	National Cyber Security Index	93 %
N/A	Global Cybersecurity Index	94 %
37th	E-Government Development Index	86 %
32nd	Network Readiness Index	60 %



https://ncsi.ega.ee/

Polska zajmuje **4 miejsce na świecie w rankingu bezpieczeństwa cyfrowego i tą wysoką** pozycję utrzymuje się na przestrzeni lat.

Większość z 12 obszarów, które obejmuje indeks oceniona została najwyżej (100 na 100 pkt) .

Obszary ocenione **najniżej to te związane z prowadzeniem działalności B+R+I** (50 na 100 pkt) oraz – w mniejszym stopniu - z włączeniem się w międzynarodowe działania na rzecz cyberbezpieczeństwa (67 na 100pkt) i publicznym zarządzaniem w obszarze świadomości w zakresie cyberzagrożeń (67 na 100 pkt)

Wskaźniki w obszarze B+R+I dla Polski wskazują na niższe niż w innych, wiodących krajach (wg danych z rankingu) finansowanie publiczne i wsparcie dla programów badawczych. Niską ocenę uzyskał też wskaźnik dostępności sprofilowanych na rzecz cyberbezpieczeństwa programów studiów doktoranckich, które pozwalają studentom rozwijać merytoryczną wiedzę z zakresu cyberbezpieczeństwa oraz projektować i prowadzić oryginalne, specjalistyczne badania w tym zakresie

NCSI to globalny **indeks, który mierzy gotowość krajów do zapobiegania zagrożeniom cybernetycznym i zarządzania incydentami cybernetycznymi.**

Indeks monitoruje wyniki krajów w 3 strategicznych filarach cyberbezpieczeństwa, w ramach których **wyróżniono 12 obszarów,** a łącznie 47 wskaźników składowych:

1. **zdolności strategiczne**, w tym m.in zarządzanie cyberbezpieczeństwem i polityką, globalne zaangażowanie, edukacja oraz **badania i innowacje**;
2. **zdolności prewencyjne**, które obejmują bezpieczną infrastrukturę cyfrową i analizę zagrożeń cybernetycznych;
3. **zdolności reagowania**, obejmujące zarządzanie incydentami cybernetycznymi i reagowanie na zagrożenia cybernetyczne o różnym charakterze.

Narodowe Centrum Badań i Rozwoju

Łańcuch wartości i główni gracze na rynku cyberbezpieczeństwa

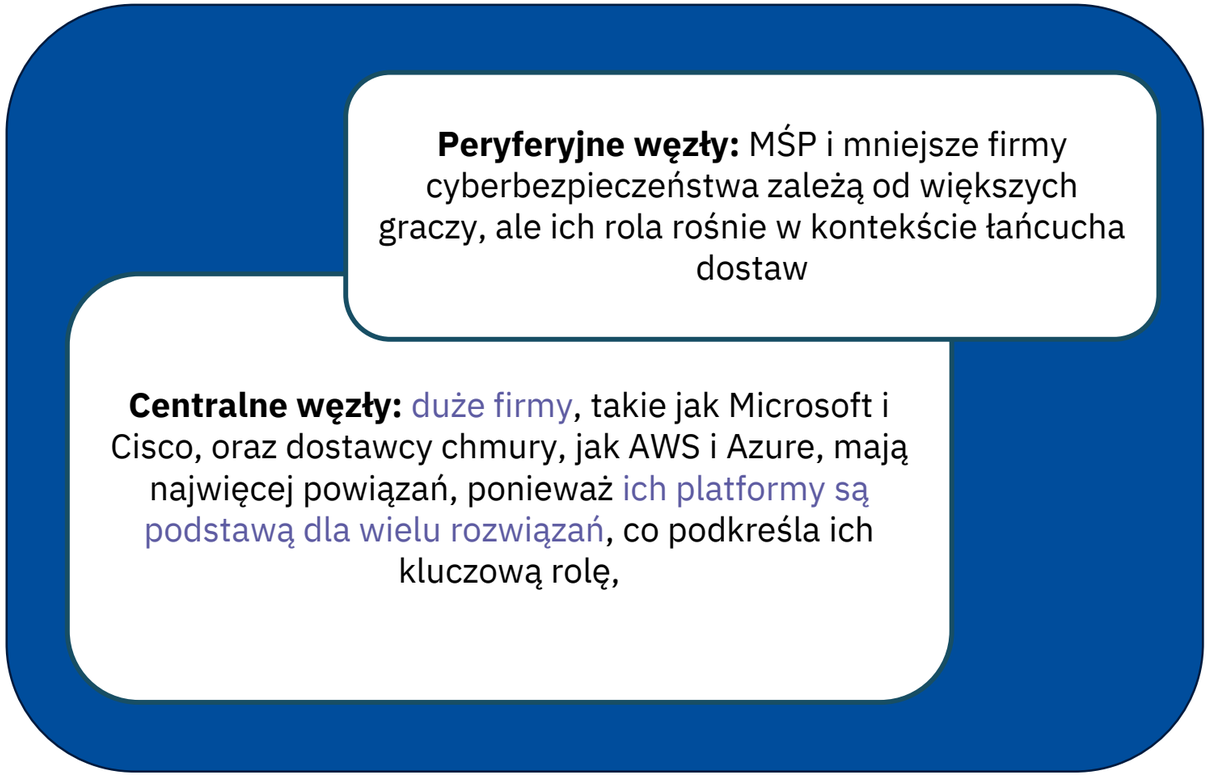
Łańcuch wartości na rynku cyberbezpieczeństwa

Badania i rozwój (R&D)	**Inwestycje w badania nad nowymi zagrożeniami** (np. ransomware, ataki zero-day, phishing oparty na AI) oraz rozwój technologii ochronnych, takich jak systemy wykrywania i reagowania (XDR), firewalle nowej generacji, czy rozwiązania oparte na sztucznej inteligencji. **Kluczowe działania**: analiza podatności, testy penetracyjne, tworzenie algorytmów uczenia maszynowego do wykrywania anomalii, rozwój oprogramowania zabezpieczającego. **Tworzona wartość**: innowacje, które pozwalają wyprzedzać cyberprzestępców i dostosowywać się do dynamicznie zmieniającego się krajobrazu zagrożeń.
Produkcja i integracja	**Tworzenie produktów** (np. oprogramowanie antywirusowe, systemy SIEM) oraz ich integrację z istniejącymi infrastrukturami klientów. Firmy współpracują z dostawcami sprzętu (np. producenci serwerów, urządzeń IoT) i oprogramowania (np. systemy operacyjne, chmura), aby zapewnić kompatybilność. **Tworzona wartość**: gotowe, skalowalne rozwiązania dostosowane do potrzeb różnych sektorów.
Marketing i sprzedaż	**Firmy promują swoje usługi poprzez budowanie świadomości o zagrożeniach cybernetycznych**, organizację konferencji (np. Black Hat, RSA Conference) oraz kampanie edukacyjne. Sprzedaż odbywa się bezpośrednio (B2B dla dużych przedsiębiorstw) lub przez partnerów, takich jak dystrybutorzy i integratorzy systemów. **Tworzona wartość**: dotarcie do klientów i dopasowanie oferty do ich specyficznych wymagań.
Wdrożenie i usługi zarządzane	**Etap obejmuje instalację rozwiązań, konfigurację systemów oraz świadczenie usług zarządzanych** (np. SOC – Security Operations Center, monitorowanie w czasie rzeczywistym). Firmy oferują również szkolenia dla pracowników klientów, audyty bezpieczeństwa i konsulting. **Tworzona wartość**: zapewnienie skutecznej ochrony i minimalizacja ryzyka incydentów.
Wsparcie posprzedażowe i reagowanie na incydenty	Obejmuje **aktualizacje oprogramowania, łatanie podatności oraz usługi reagowania na incydenty** (IR – Incident Response). Firmy współpracują z zespołami CSIRT (Computer Security Incident Response Team, np. CSIRT NASK w Polsce) w przypadku poważnych incydentów. **Tworzona wartość**: ciągłość działania klientów i szybkie przywracanie normalności po atakach.
Recykling i doskonalenie	Na podstawie danych z incydentów i feedbacku od klientów firmy doskonalą swoje produkty i usługi. Analiza łańcucha dostaw i partnerów pozwala minimalizować ryzyko ataków na dostawców.

Główni gracze na rynku cyberbezpieczeństwa – wzajemnie powiązania

Głowni gracze komercyjni	globalni liderzy, jak: Accenture, Palo Alto Networks, Cisco, Microsoft, CrowdStrike i Fortinet, oraz specjalistyczne firmy, takie jak Check Point (firewalle) i Splunk (SIEM); firmy te współpracują z integratorami systemów, takimi jak Deloitte i EY, oraz dostawcami chmury, takimi jak AWS i Azure. Przykładem jest integracja rozwiązań CrowdStrike z Azure,
Dostawcy infrastruktury	firmy takie jak Amazon (AWS), Google Cloud i Microsoft Azure dostarczają infrastrukturę chmurową, na której opierają się rozwiązania cyberbezpieczeństwa. Zależność od tych dostawców rośnie, ale sami oferują własne rozwiązania, takie jak Azure Sentinel, konkurując z niezależnymi firmami
Cyberpzrestępcy	choć nie są tradycyjnymi graczami, grupy ransomware, takie jak LockBit, i aktorzy państwowi, np. rosyjskie APT, wpływają na rynek, zmuszając firmy do innowacji. Niektóre grupy sprzedają narzędzia mniejszym podmiotom, tworząc „rynek" usług cyberprzestępczych, co wymaga
Łańcuch dostaw i partnerzy	obejmują dostawców i odbiorców - zależności między firmami cyberbezpieczeństwa, ich dostawcami i klientami. Firmy muszą audytować dostawców, co prowadzi do tworzenia konsorcjów i standardów, takich jak NIST SP 800-161
Instytucje publiczne i regulacyjne	obejmują Ministerstwo Cyfryzacji, CSIRT NASK i ABW, a w UE ENISA i Komisję Europejską. Te instytucje narzucają regulacje,, oraz współpracują z sektorem prywatnym w ramach zespołów CSIRT, co wspiera narodową obronę cybernetyczną.
Organizacje non-profit i badawcze	obejmuje MITRE (twórca frameworku ATT&CK), OWASP i akademickie centra badawcze, takie jak NASK. Dostarczają standardy, badania i narzędzia open-source, które są wykorzystywane przez firmy komercyjne i sektor publiczny, co wspiera innowacje.

Sieciowa struktura sieci na rynku cyberbezpieczeństwa ciągle ewoluuje – wzajemnie powiązania



Dynamiczna natura:
sieć ewoluuje i nieustannie dostosowuje się w odpowiedzi na nowe zagrożenia, takie jak GenAI w atakach, i regulacje, takie jak Dyrektywa NIS2

Przykłady głównych graczy i ich powiązań

Grupa	Przykłady firm/instytucji	Rodzaje powiązań
Firmy komercyjne	Microsoft, Cisco, CrowdStrike	Partnerstwa z integratorami, integracja z chmurą
Dostawcy infrastruktury	AWS, Google Cloud, Azure	Oferowanie własnych rozwiązań, konkurencja z firmami komercyjnymi
Instytucje publiczne	CSIRT NASK, ENISA	Regulacje, współpraca z sektorem prywatnym
Organizacje badawcze	MITRE, OWASP	Dostarczanie standardów, narzędzi open-source
Łańcuch dostaw	Dostawcy, MŚP	Audyty, konsorcja, standardy bezpieczeństwa

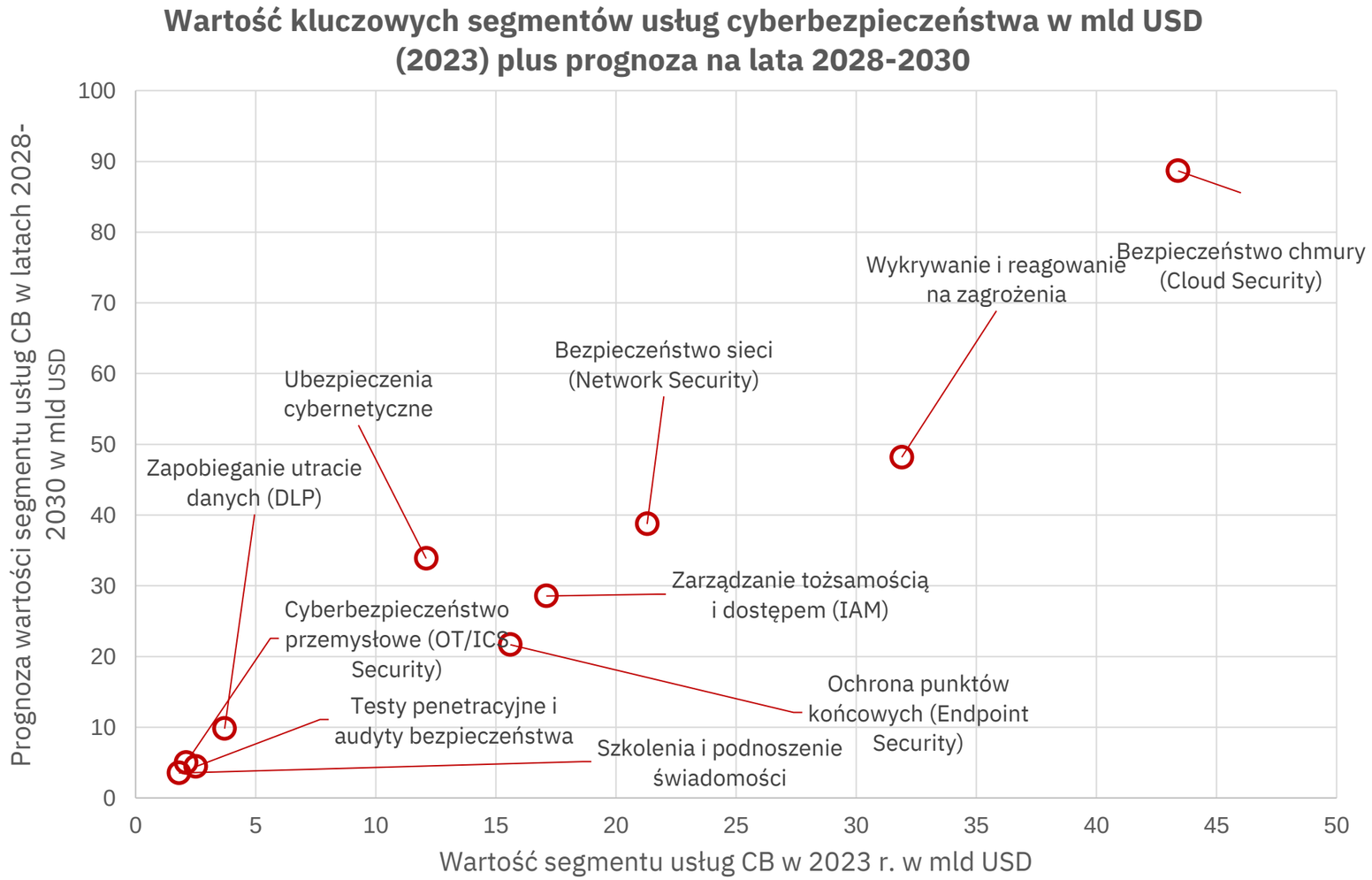
Główne grupy odbiorców na rynku cyberbezpieczeństwa

Duże przedsiębiorstwa	Sektor publiczny	Małe i średnie przedsiębiorstwa	Konsumenci indywidualni
Duże przedsiębiorstwa dominują, **odpowiadając za ponad 60% rynku** w 2024 roku, dzięki złożonej infrastrukturze i wysokim wymaganiom bezpieczeństwa.	**Udział w rynku: Ok. 10–15%**, z rosnącym znaczeniem w regionów o wysokim poziomie regulacji (np. USA, UE).	Udział w rynku: **szacowany na 20–30% rynku** w 2024 roku, z szybko rosnącym znaczeniem.	Udział w rynku: najmniejszy segment, szacowany na **mniej niż 5% rynku**.
Największe **inwestycje w rozwiązania takie jak IAM (Identity and Access Management**), SIEM, NGFW, DLP **oraz ochronę infrastruktury krytycznej.** Sektory kluczowe: BFSI (bankowość, finanse, ubezpieczenia) z największym udziałem, IT/telekom, opieka zdrowotna, energetyka i produkcja.	**Inwestycje w ochronę infrastruktury krytycznej** (energetyka, transport, zdrowie) i **danych wrażliwych** (np. dane obywateli, informacje wojskowe). Popularne rozwiązania: network security, IAM, SIEM, cloud security. Kluczowe inicjatywy: w USA programy jak CNAP i Cyber Trust Mark, w UE dyrektywa NIS2.	MŚP są bardziej narażone na ataki (np. ransomware, phishing), ale mają ograniczone budżety i brak specjalistów. **Popularne rozwiązania: chmurowe usługi bezpieczeństwa (**IaaS, SaaS), **podstawowe antywirusy, VPN i endpoint security.** Sektory kluczowe: e-commerce, retail, finanse.	Obejmuje **antywirusy, VPN, oprogramowanie do ochrony danych osobowych i smart urządzeń** (np. IoT). Wzrost popytu napędzany przez e-commerce, m-commerce i ataki phishingowe. Innowacje, takie jak U.S. Cyber Trust Mark, wspierają ochronę urządzeń konsumenckich.
Wzrost napędzany transformacją cyfrową, migracją do chmury (hybrid/multicloud) i rosnącą liczbą ataków, problemami z zabezpieczeniem łańcucha dostaw). Trendy obejmują adopcję Zero Trust, AI/ML w analizie zagrożeń i zwiększone inwestycje w managed security services (MSS).	**Wzrost napędzany przez rosnące zagrożenia geopolityczne i regulacje**. Wzrost inwestycji w sektorowe CSIRT-y, ochronę przed dezinformacją i zabezpieczenia chmurowe (np. rządowe chmury w UE). Wyzwania: biurokracja, ograniczone budżety w niektórych regionach (np. Ameryka Łacińska).	Potencjał wzrostu: CAGR: **15–20%, najwyższy wśród segmentów**, **dzięki cyfryzacji i większej dostępności tanich rozwiązań chmurowych.** **Wzrost napędzany przez regulacje** (np. GDPR, CCPA) i rosnącą świadomość zagrożeń. Kluczowe trendy: outsourcing usług bezpieczeństwa, adopcja SASE (Secure Access Service Edge) i prostych rozwiązań AI-driven.	**Wzrost popytu napędzany przez e-commerce, m-commerce i ataki phishingowe.** Innowacje, takie jak U.S. Cyber Trust Mark, wspierają ochronę urządzeń konsumenckich.

Narodowe Centrum Badań i Rozwoju

Kluczowe segmenty usług

Rosnące znaczenie aktywnego i elastycznego podejścia do reagowania na zagrożenia i tym samym rozwiązań zdolnych do uczenia się w czasie rzeczywistym



Źródła: Mordor Intelligence, Statista, Fortune Business Insights, Netscout, Gartner, MarketsandMarkets, IDC, PwC, Global Cyber Insurance Market Report, MarketsandMarkets 2023

Tradycyjne podejście do cyberbezpieczeństwa nadaje priorytet przewidywaniu, **kładąc nacisk na rozwiązania mające zapobiegać przewidywanym zagrożeniom**. Jednak w coraz bardziej złożonym cyfrowym otoczeniu ten reaktywny sposób myślenia może nie być wystarczający. **Na rynku usług cyberbezpieczeństwa zdecydowanie**, co wymusza proaktywne podejście do cyberbezpieczeństwa i **wzmocnienie narzędzi ochrony, które będą dostosowywać się i uczyć na bieżąco wraz z pojawianiem się nowych zagrożeń**.

Wyraźny wzrost rynku usług bezpieczeństwa w sieci i ochrony przeciw utracie danych jest spójne z tendencją do coraz większego zabezpieczenia aktywów firm w postaci danych i informacji przez nie gromadzonych. Z punktu widzenia dużych firm **utrata dostępów do danych to absolutnie największe zagrożenie dla prowadzonej działalności**. Wpływa to na rozwój bardziej zaawansowanych metod backupu- w chmurze i zewnętrznych lokalizacjach oraz zabezpieczenia ich w taki sposób, aby nie doszło do zaszyfrowania także kopii zapasowych.

Charakterystyki poszczególnych segmentów usług cyberbezpieczeństwa

Wykrywanie i reagowanie na zagrożenia (Threat Detection and Response)	
Opis	Segment obejmuje narzędzia takie jak SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response) oraz threat intelligence, które umożliwiają wykrywanie, analizę i reagowanie na incydenty w czasie rzeczywistym.
Znaczenie	Wzrost ataków APT i deepfake'ów (napędzanych przez generatywną AI) zwiększa zapotrzebowanie na zaawansowane wykrywanie.
Zagrożenia	Ataki APT, ransomware, backdoory (21% incydentów w 2023 roku), deepfake'i, ataki sponsorowane przez państwa.
Przykłady usług	SIEM (Security Information and Event Management, Zarządzanie Informacją i Zdarzeniami Bezpieczeństwa, SOAR (Security Orchestration, Automation, and Response / systemy, które integrują i automatyzują procesy reagowania na incydenty bezpieczeństwa w organizacji, threat intelligence (wywiad dotyczący zagrożeń to proces zbierania, analizowania i wykorzystywania informacji o zagrożeniach cybernetycznych, aby zrozumieć, przewidzieć i skutecznie przeciwdziałać atakom, analiza behawioralna.

Zarządzanie danymi i zapobieganie utracie danych (DLP - Data Loss Prevention)	
Opis	Segment obejmuje rozwiązania chroniące przed utratą lub kradzieżą danych, w tym szyfrowanie, klasyfikację danych i monitorowanie transferu danych. DLP jest kluczowe dla zgodności z regulacjami, takimi jak RODO czy NIS2.
Znaczenie	Wzrost liczby naruszeń danych (np. 2,6 mln rekordów z Facebooka w Polsce) podkreśla potrzebę DLP (Data Loss Prevention, czyli ochrona przed utratą danych. Jest to zestaw technologii i praktyk mających na celu zapobieganie wyciekowi, utracie lub niewłaściwemu użyciu poufnych informacji.
Zagrożenia	Wycieki danych (zamierzone i niezamierzone), naruszenia danych (60% incydentów w Europie zawiera element socjotechniki).
Przykłady usług	Szyfrowanie, klasyfikacja danych, ochrona przed wyciekami.
Kluczowe firmy	Symantec (Broadcom, USA), Forcepoint (USA), Next DLP (USA)

Charakterystyki poszczególnych segmentów usług cyberbezpieczeństwa

Bezpieczeństwo sieci (Network Security)	
Opis	Segment koncentruje się na ochronie infrastruktury sieciowej, w tym firewalli nowej generacji (NGFW), VPN, SD-WAN i systemów IDS/IPS (Intrusion Detection/Prevention Systems). Rozwiązania te zapobiegają nieautoryzowanemu dostępowi i zapewniają bezpieczną łączność.
Znaczenie	Ataki DDoS, podkreślają potrzebę ochrony sieci, szczególnie w erze 5G i IoT.
Zagrożenia	Ataki DDoS, przejmowanie infrastruktury sieciowej, manipulacja danymi w sieci, ataki na 5G.
Przykłady usług	Firewalle, VPN, IDS/IPS, ochrona przed DDoS (np. AWS Shield, Akamai).
Kluczowe firmy	Palo Alto Networks (USA), Fortinet (USA), Check Point Software (Izrael), Juniper Networks (USA)

Bezpieczeństwo chmury (Cloud Security)	
Opis	Segment obejmuje ochronę danych i aplikacji w środowiskach chmurowych (publicznych, prywatnych, hybrydowych) za pomocą narzędzi takich jak CASB (Cloud Access Security Broker), CWPP (Cloud Workload Protection Platform) i CSPM (Cloud Security Posture Management).
Znaczenie	Migracja do chmury (np. 90% firm z Fortune 100 używa Splunk w chmurze) zwiększa zapotrzebowanie na dedykowane rozwiązania bezpieczeństwa.
Zagrożenia	Naruszenia danych w chmurze, błędna konfiguracja chmury, ataki na API, przejmowanie kont chmurowych.
Przykłady usług	CASB (Cloud Access Security Broker, czyli broker zabezpieczeń dostępu do chmury)., CSPM (Cloud Security Posture Management, czyli Zarządzanie Stanem Bezpieczeństwa w Chmurze) , ochrona API, szyfrowanie danych w chmurze.
Kluczowe firmy	Microsoft (USA), Zscaler (USA), Amazon (USA), Lacework (USA)

Charakterystyki poszczególnych segmentów usług cyberbezpieczeństwa

Zarządzanie tożsamością i dostępem (IAM - Identity and Access Management)	
Opis	Segment obejmuje rozwiązania do zarządzania tożsamością, uwierzytelnianiem (np. MFA – Multi-Factor Authentication) i dostępem, w tym Zero Trust. Chroni przed kradzieżą danych uwierzytelniających i nieautoryzowanym dostępem.
Znaczenie	33% ataków w 2023 roku wykorzystywało wykradzione dane uwierzytelniające, co podkreśla kluczową rolę IAM
Zagrożenia	Kradzież tożsamości, ataki phishingowe, nieautoryzowany dostęp, ataki typu spearphishing (40% ataków w 2023 roku)
Przykłady usług	MFA (Multi-Factor Authentication, czyli uwierzytelnianie wieloskładnikowe), SSO (Single Sign-On, czyli logowanie jednokrotne. Jest to mechanizm, który pozwala użytkownikom na dostęp do wielu aplikacji i systemów za pomocą jednego zestawu danych uwierzytelniających, PAM (Privileged Access Management - rozwiązanie służące do zabezpieczania tożsamośc), Zero Trust (model bezpieczeństwa, który zakłada, że żadnemu użytkownikowi, urządzeniu ani aplikacji nie należy ufać domyślnie, niezależnie od tego, czy znajduje się wewnątrz czy na zewnątrz sieci organizacji. .
Kluczowe firmy	Okta (USA), CyberArk (USA/Izrael), Microsoft (USA), Ping Identity (USA)

Ochrona punktów końcowych (Endpoint Security)	
Opis	Segment obejmuje ochronę urządzeń końcowych, takich jak laptopy, smartfony czy urządzenia IoT, przed nieautoryzowanym dostępem i złośliwym oprogramowaniem. Rozwiązania takie jak EDR (Endpoint Detection and Response) i EPP (Endpoint Protection Platform) wykorzystują AI do wykrywania i reagowania na zagrożenia w czasie rzeczywistym.
Znaczenie	Wzrost liczby urządzeń IoT (prognoza: 41 mld urządzeń do 2025 roku) zwiększa zapotrzebowanie na ochronę punktów końcowych.
Zagrożenia	Malware (np. wirusy, ransomware), kradzież tożsamości, exploity zero-day, ataki na urządzenia IoT.
Przykłady usług	Antywirusy, EDR, ochrona przed ransomware, zabezpieczenia IoT.
Kluczowe firmy	CrowdStrike (USA), SentinelOne (USA), Bitdefender (Rumunia), Kaspersky (Rosja/Szwajcaria)

NCBR
Narodowe Centrum Badań i Rozwoju

Wyzwania dla rozwoju technologii na rzecz cyberbezpieczeństwa

Zmiany w technologiach stosowanych w filmach powodują pojawienie się nowych potrzeb w zakresie rozwiązań cyberbezpieczeństwa

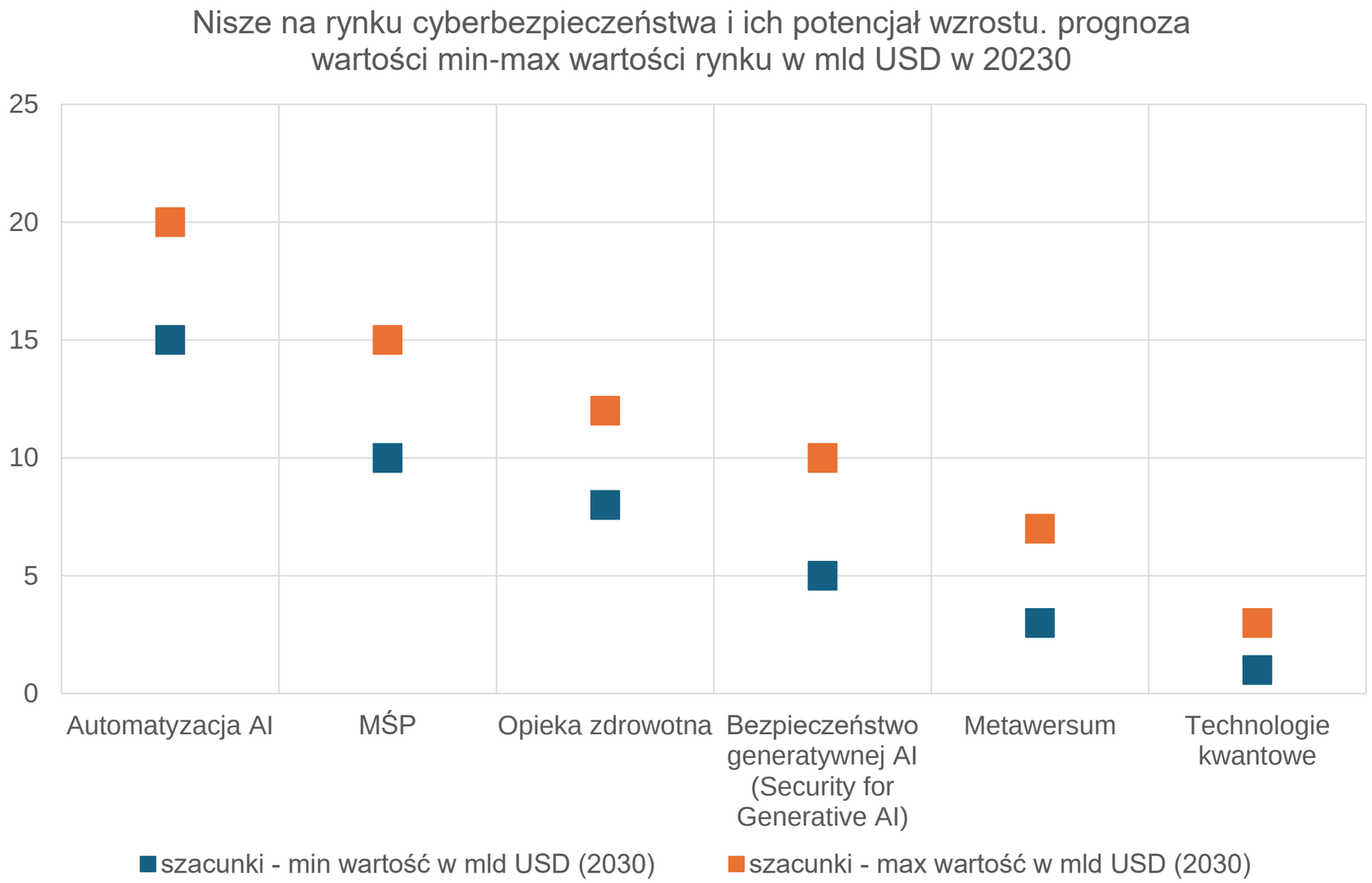
WYZWANIA TECHNOLOGICZNE

- **Zaawansowane ataki AI i automatyzacja**: cyberprzestępcy coraz częściej wykorzystują sztuczną inteligencję do tworzenia zaawansowanych ataków, takich jak deepfake, ataki phishingowe oparte na AI. Obrona wymaga równie zaawansowanych narzędzi AI do wykrywania i reagowania w czasie rzeczywistym.
- **Rozwój technologii chmurowych**: migracja do chmury zwiększa ryzyko związane z błędną konfiguracją, brakiem widoczności danych i atakami na interfejsy API. Zabezpieczenie środowisk hybrydowych i multi-cloud jest skomplikowane.
- **Zagrożenia związane z IoT**: rosnąca liczba urządzeń Internetu Rzeczy (IoT) tworzy nowe wektory ataków. Wiele z nich ma słabe zabezpieczenia, co utrudnia ich ochronę.
- **Zagrożenia kwantowe**: rozwój komputerów kwantowych zagraża obecnym standardom kryptograficznym, co wymusza przejście na kryptografię post-kwantową.
- **Ransomware i szyfrowanie danych**: ewolucja ransomware, w tym podwójne wymuszenia (szyfrowanie i kradzież danych), wymaga zaawansowanych strategii backupu i wykrywania.

WYZWANIA ORGANIZACYJNE

- **Ataki na łańcuch dostaw**: ataki na dostawców oprogramowania i usług (np. SolarWinds) pokazują, jak trudno zabezpieczyć złożone ekosystemy technologiczne.
- **Brak specjalistów**: niedobór wykwalifikowanych ekspertów w dziedzinie cyberbezpieczeństwa utrudnia wdrażanie i zarządzanie nowoczesnymi technologiami ochronnymi.
- **Zero Trust i tożsamość cyfrowa**: wdrożenie modelu Zero Trust wymaga zaawansowanych systemów zarządzania tożsamością (IAM) i ciągłego monitorowania, co jest technicznie wymagające.
- **Złożoność regulacji**: spełnienie wymogów regulacyjnych (np. RODO, NIS2) wymaga integracji technologii zapewniających zgodność, co zwiększa obciążenie firm.
- **Szybkość reakcj**i: wzrost liczby ataków w czasie rzeczywistym wymaga technologii umożliwiających błyskawiczne wykrywanie i neutralizację zagrożeń, co jest trudne w dużych, rozproszonych systemach.

Główny obszar innowacji związany jest z rosnącą automatyzacją wywołaną AI



Źródła: Gartner, McKinsey, BCG, Mordor Intelligence, Frost & Sullivan, IDC

Nisze na rynku cyberbezpieczeństwa

Automatyzacja cyberbezpieczeństwa oparta na AI	
Potencjał	Wzrost liczby incydentów (80 267 w Polsce w 2023 roku) przytłacza specjalistów, co zwiększa zapotrzebowanie na automatyczne systemy wykrywania i reagowania oparte na AI. AI pomaga w szybszym wykrywaniu zagrożeń i redukcji fałszywych alarmów.
Dlaczego nisza?	Choć firmy jak Darktrace czy Vectra AI oferują takie rozwiązania, rynek wciąż potrzebuje bardziej skalowalnych i przystępnych cenowo opcji.
Przykłady usług	Automatyczne SOAR (Security Orchestration, Automation and Response. Jest to technologia, która integruje i automatyzuje procesy związane z bezpieczeństwem, pozwalając na efektywniejsze zarządzanie zagrożeniami i reagowanie na incydenty.), AI-driven threat hunting (polowanie na zagrożenia napędzane sztuczną inteligencją), analiza behawioralna.
Źródła nowych graczy	Startupy AI z Indii, Izraela i Polski, a także działy R&D dużych firm (np. Microsoft, Google).

Cyberbezpieczeństwo dla MŚP (małych i średnich przedsiębiorstw)	
Potencjał	MŚP często nie stać na zaawansowane rozwiązania dużych graczy, takich jak Palo Alto czy Microsoft. W Polsce 70% firm doświadczyło cyberataku, ale brakuje przystępnych cenowo i łatwych w obsłudze narzędzi dla MŚP.
Dlaczego nisza?	Duże firmy skupiają się na korporacjach i sektorze publicznym, pozostawiając MŚP z ograniczonymi opcjami.
Przykłady usług	Uproszczone platformy DLP (Data Loss Prevention, zapobieganie utracie danych lub ochrona przed wyciekiem danych), IAM (Identity and Access Management, Zarządzanie Tożsamością i Dostępem), dla MŚP, outsourcing cyberbezpieczeństwa.
Źródła nowych graczy	Lokalne firmy IT z Polski (np. Comarch, TestArmy), startupy z Europy Wschodniej, dostawcy SaaS z USA.

Nisze na rynku cyberbezpieczeństwa

Bezpieczeństwo generatywnej AI i dużych modeli językowych	
Potencjał	Generatywna AI (np. ChatGPT) jest wykorzystywana do tworzenia deepfake'ów, złośliwego oprogramowania i zaawansowanych ataków socjotechnicznych (np. spearphishing). Gartner szacuje, że do 2027 roku 17% cyberataków będzie wykorzystywać generatywną AI. Brakuje dedykowanych rozwiązań do zabezpieczania modeli AI przed manipulacją, kradzieżą danych treningowych czy atakami typu „data poisoning".
Dlaczego nisza?	Technologie AI rozwijają się szybciej niż ich zabezpieczenia. Firmy takie jak Vectra AI już eksplorują ten obszar, ale rynek jest wciąż niedojrzały.
Przykłady usług	Narzędzia do wykrywania deepfake'ów, zabezpieczanie modeli AI, audyty bezpieczeństwa AI.
Źródła nowych graczy	Startupy z Doliny Krzemowej, Izraela i Europy Wschodniej (np. Polska, Estonia), które specjalizują się w AI i ML. Przykłady: Deepfence, Protect AI.

Cyberbezpieczeństwo w metawersum	
Potencjał	Rozwój metawersum (Meta, Microsoft) otwiera nowe wektory ataków, takie jak kradzież tożsamości w wirtualnych światach, manipulacja danymi VR/AR czy ataki na blockchainy obsługujące metawersum.
Dlaczego nisza?	Metawersum jest nowym ekosystemem, a obecne rozwiązania (np. IAM) nie są w pełni dostosowane do jego specyfiki.
Przykłady usług	Zabezpieczanie platform VR/AR, ochrona cyfrowych tożsamości, audyty blockchain.
Źródła nowych graczy	Firmy gamingowe (np. Epic Games), startupy blockchain (np. z Singapuru, Estonii) oraz giganci technologiczni eksplorujący VR/AR.

Nisze na rynku cyberbezpieczeństwa

Bezpieczeństwo technologii kwantowych	
Potencjał	Informatyka kwantowa (np. szyfrowanie kwantowe) może złamać obecne metody kryptograficzne (np. RSA) do 2030 roku, co wymaga nowych rozwiązań, takich jak kryptografia post-kwantowa. UE inwestuje w szyfrowanie kwantowe, co podkreśla potencjał tego rynku.
Dlaczego nisza?	Technologia jest w fazie badań, a liderzy (np. IBM, Google) dopiero zaczynają rozwijać zabezpieczenia kwantowe.
Przykłady usług	Kryptografia post-kwantowa, zabezpieczanie komunikacji kwantowej, audyty systemów kwantowych.
Źródła nowych graczy	Firmy technologiczne z USA i Chin, instytuty badawcze (np. CERN, NASK w Polsce), startupy z Izraela i Singapuru.

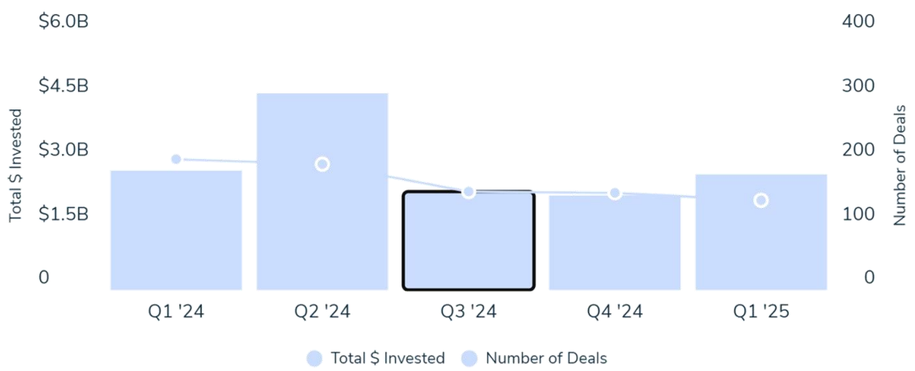
Cyberbezpieczeństwo w metawersum	
Potencjał	Rozwój metawersum (Meta, Microsoft) otwiera nowe wektory ataków, takie jak kradzież tożsamości w wirtualnych światach, manipulacja danymi VR/AR czy ataki na blockchainy obsługujące metawersum.
Dlaczego nisza?	Metawersum jest nowym ekosystemem, a obecne rozwiązania (np. IAM) nie są w pełni dostosowane do jego specyfiki.
Przykłady usług	Zabezpieczanie platform VR/AR, ochrona cyfrowych tożsamości, audyty blockchain.
Źródła nowych graczy	Firmy gamingowe (np. Epic Games), startupy blockchain (np. z Singapuru, Estonii) oraz giganci technologiczni eksplorujący VR/AR.

Nisze na rynku cyberbezpieczeństwa

Cyberbezpieczeństwo w opiece zdrowotnej	
Potencjał	Sektor zdrowia jest coraz częściej atakowany (9 incydentów w Polsce w 2023 roku) z powodu wrażliwych danych i przestarzałej infrastruktury. UE wprowadza plan działania na 2025–2026 dla szpitali, co zwiększa popyt na dedykowane rozwiązania.
Dlaczego nisza?	Sektor zdrowia wymaga specyficznych regulacji i rozwiązań, których większość firm jeszcze nie oferuje w pełni.
Przykłady usług	Ochrona systemów medycznych, zabezpieczanie IoT w szpitalach, audyty zgodności z RODO.
Źródła nowych graczy	Firmy med-tech z USA i Europy, startupy z Izraela, polskie firmy jak ICSEC z doświadczeniem w infrastrukturze krytycznej.

Mimo globalnego stałego wzrostu rynku spadek liczby inwestycji funduszy VC w cyberbezpieczeństwo na świecie – może to być jednak chwilowe zawahanie

Kwartalna wartość i liczba inwestycji venture w zakresie cyberbezpieczeństwa



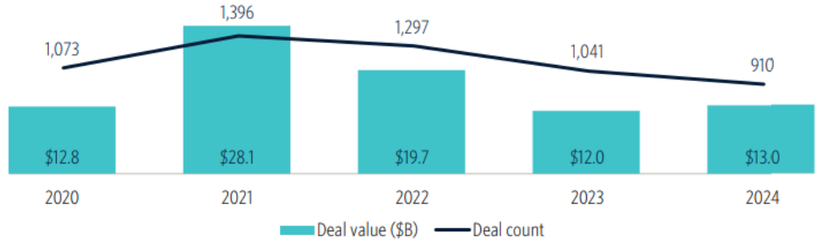
Źródło: Crunchbase

Wsparcie VC w sektorze CyberSec na świecie...

Venture capital jest jednym z bardziej efektywnych sposobów finansowania innowacyjnych przedsięwzięć we wczesnej fazie wzrostu. W ten sposób finansowane są także młode przedsiębiorstwa wdrażające rozwiązania z zakresu cyberbezpieczeństwa. Choć nie jest to tradycyjna branża, według której analizuje się inwestycje (lub dezinwestycje) funduszy, to są firmy analityczne dysponujące także danymi dotyczącymi tego sektora.

Według Crunchbase **w I kwartale 2025 roku mieliśmy do czynienia ze niewielkim wzrostem wartości inwestycji** dokonywanych w spółki z zakresu cyberbezpieczeń-stwa (do 2,7 mld USD), aczkolwiek **liczba transakcji zmniejsza się od czterech kwartałów** (do ok. 140 transakcji kwartalnie ponad 200 rok wcześniej).

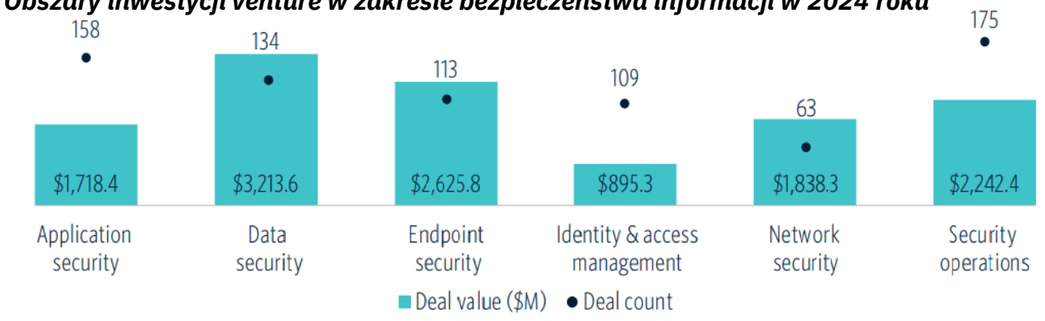
Roczna wartość i liczba inwestycji venture w zakresie bezpieczeństwa informacji



Źródło: Pitchbook

Dane firmy Pitchbook dla bezpieczeństwa informacji (InfoSec) dla Europy i Ameryki Północnej także pokazują tendencję spadkową w liczbie i wartości inwestycji w ten obszar, choć należy także pamiętać o ogólnym spadku inwestycji funduszy VC w tym okresie.

Obszary inwestycji venture w zakresie bezpieczeństwa informacji w 2024 roku



Źródło: Pitchbook

Według Pitchbook, obszarami, w które przede wszystkim inwestowano w 2024 roku było bezpieczeństwo danych (*data security*), działania związane z bezpieczeństwem (*security operations*) i tzw. ochrona punktów końcowych (*endpoint security*), czyli obszar cyberbezpieczeństwa skupiony na zabezpieczaniu urządzeń, takich jak komputery stacjonarne, laptopy i urządzenia mobilne.

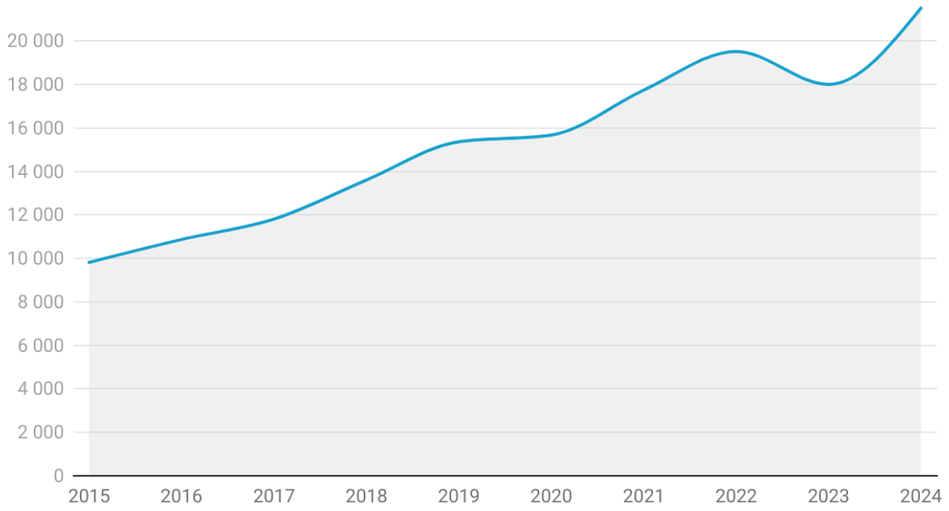
Narodowe Centrum Badań i Rozwoju

Cyberbezpieczeństwo – trendy w B+R

Cyberbezpieczeństwo jest przedmiotem intensywnych badań naukowych

Publikacje naukowe w zakresie systemów bezpieczeństwa

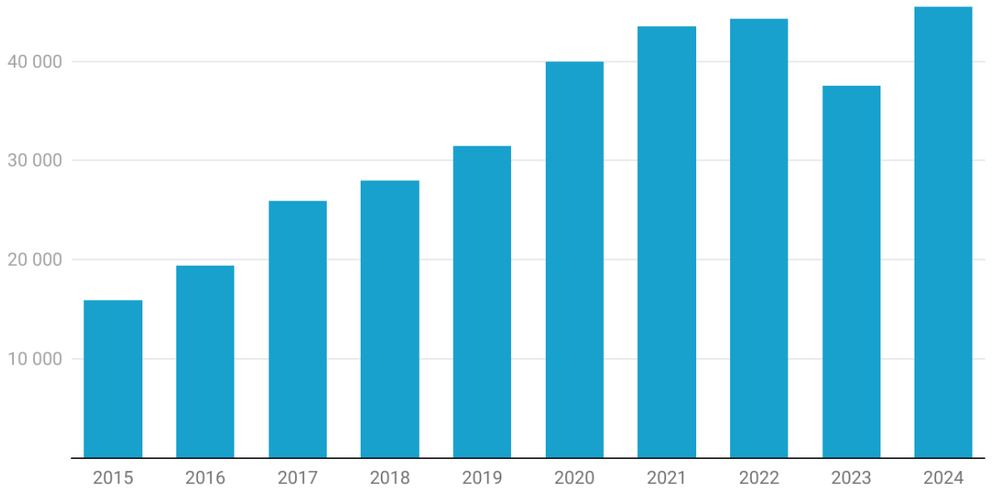
w latach 2015-2024



Źródło: opracowanie własne na podstawie danych Web of Science • Narzędzie: Datawrapper

Liczba patentów w związanych z cyberbezpieczeństwem

w ramach grupy G06F21 i H04L63 klasyfikacji CPC w latach 2015-2024



Źródło: opracowanie własne na podstawie danych EPO (espacenet) • Narzędzie: Datawrapper

Artykuły naukowe i patenty w zakresie cyberbezpieczeństwa

Cyberbezpieczeństwo jest przedmiotem intensywnych badań naukowych, a prace naukowe jakie powstają w tym obszarze można zaliczyć do stosunkowo licznych. Przedstawione dane uwzględniają różnego typu artykuły naukowe (w tym early access i proceeding paper) w kategorii „systemów bezpieczeństwa” według podziału tematycznego stosowanego w bazie Web of Science.

W 2024 roku opublikowano ich ponad 20 tys. co oznacza dwukrotny wzrost w stosunku do roku 2015. Natomiast w całym okresie 2015-2025 ukazało się ich ponad 155 tys.

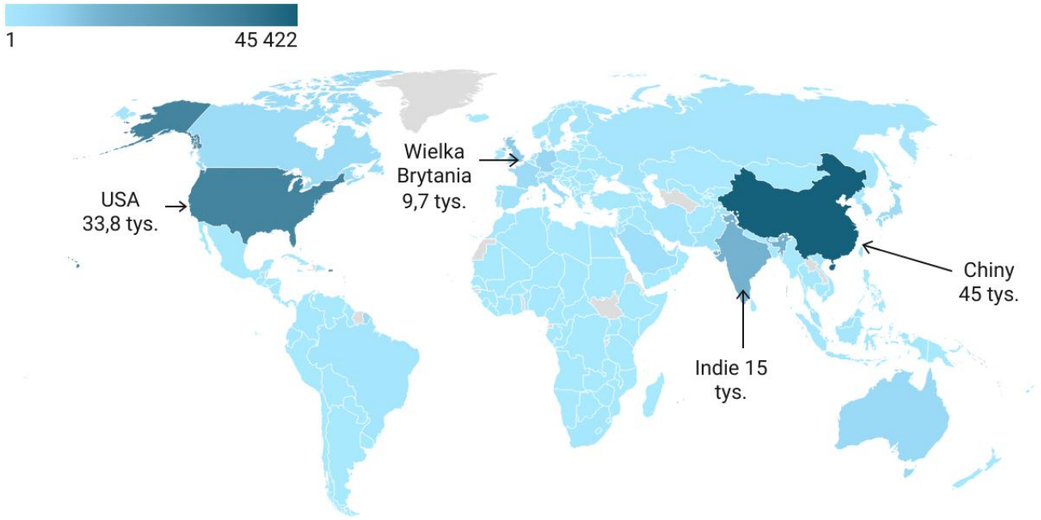
Dane pochodzące ze statystyk patentowych należy traktować jako orientacyjne, pokazujące trendy lub zależności. Liczba patentów krajowych zależy od wielu czynników takich jak np. regulacje prawne, poziom rozwoju gospodarczego, sprawność systemu sądownictwa, normy kulturowe itp.

Podobnie sytuacja wygląda w zakresie materialnego przejawu ochrony własności przemysłowej czyli patentów. Liczba patentów (właściwie rodzin patentowych) oznaczonych kodami klasyfikacji patentowej CPC odnoszącymi się do cyberbezpieczeństwa (grupa G06F21 - Układy zabezpieczające do ochrony komputerów lub systemów komputerowych przed działaniami nieupoważnionymi i H04L63 - architektura sieci lub protokoły komunikacji sieciowej dla bezpieczeństwa sieci) w ostatnim dziesięcioleciu sięgnęła 345 tys. Ich liczba wzrosła w tym okresie z 16 tys. do 45 tys. rocznie.

Poza względnie wysokim przyrostem w obydwu przypadkach widać niewielkie spadki w 2023 roku, które przypisywane jest problemom gospodarczym będącym opóźnionym efektem pandemii Covid-19 oraz wyższym stopom referencyjnym banków centralnych (wyższym kosztem pieniądza), które niekorzystnie oddziałują na inwestycje w nowe technologie.

Liczba artykułów naukowych w podziale na kraje

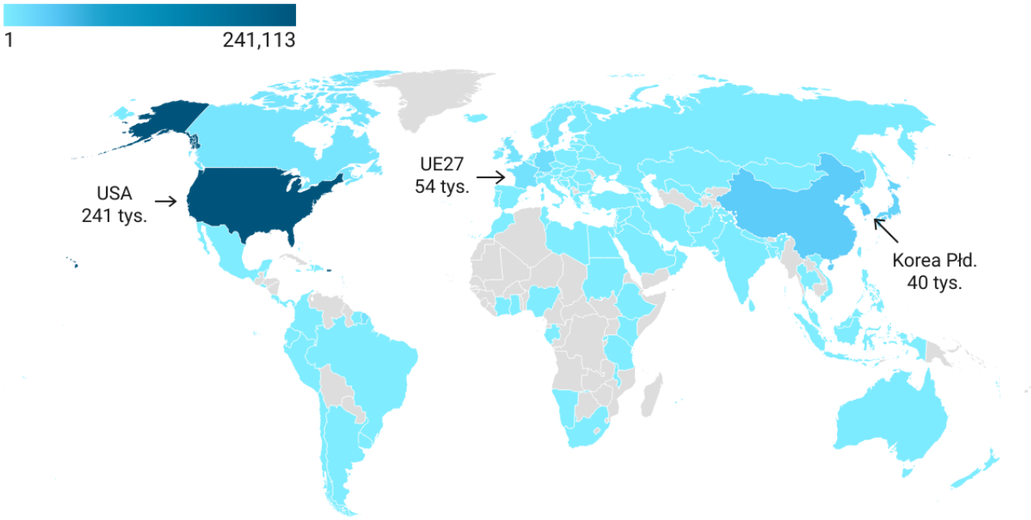
odnoszących się do cyberbezpieczeństwa, 2015-2025



Źródło: Opracowanie własne na podstawie danych Web of Science • Narzędzie: Datawrapper

Kraje pochodzenia podmiotów patentujących

osób fizycznych lub prawnych (liczba jednostek)



Source: Opracowanie własne na podstawie danych EPO (espacenet) • Created with Datawrapper

Rozkład przestrzenny

Tematyka cyberbezpieczeństwa jest na tyle powszechna, że w praktycznie każdym kraju są autorzy publikujący w tej tematyce (co przy innych tematykach nie jest powszechne). Liczebność artykułów naukowych w podziale na kraje w dużej mierze determinowana jest potencjałem ludnościowym i naukowym danego państwa oraz politykom naukowym. Stąd też w latach 2015-24 najwięcej ich pochodziło z Chin (ponad 45 tys.), a w drugiej kolejności ze Stanów Zjednoczonych (blisko 39 tys.). Trzecie miejsce zajmowały, posiadające stosunkowo prężny sektor ICT, Indie (15 tys.). Unii Europejska potraktowana jako całość także znajduje się stosunkowo wysoko z ponad 41 tys. publikacji.

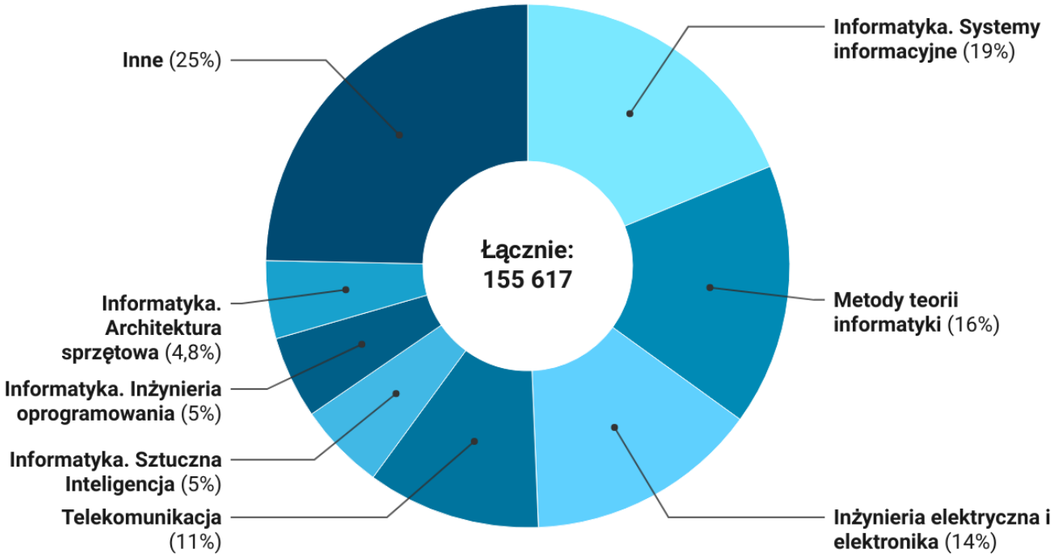
Polska na tej liście znajduje się stosunkowo daleko z blisko 1500 publikacji. W UE w przeliczeniu na głowę mieszkańca wyróżniają się Luksemburg, Estonia i Finlandia. Polska w takim ujęciu jest na trzecim miejscu od końca. W przypadku pochodzenia podmiotów patentujących (osób fizycznych lub prawnych) widoczna jest silna dominacja Stanów Zjednoczonych (241 tys. z 75 tys. patentów). Po części wynika to także ze specyfiki systemu patentowego w Stanach Zjednoczonych, w którym uznaje się, że oprogramowanie komputerowe może podlegać ochronie patentowej. W Unii Europejskiej (UE-27) takich patentów jest ponad 18 tys. z 54 tys. podmiotów. Trzecie miejsce zajmuje Korea Południowa z blisko 18 tys. patentów i 40 tys. podmiotów. Przy interpretacji danych warto zwrócić uwagę, że patenty pochodzące z ChRL dotyczą tych, które zostały otrzymane poza tym krajem.

Polska znajduje się dość daleko na tej liście, za Czechami, Litwą czy Cyprem. Właścielelami/ współwłaścicielami patentów 111 patentów są 284 podmioty. 1/3 z nich powstała we współpracy z podmiotami ze Stanów Zjednoczonych.

Najczęściej pojawiającą się tematyką w artykułach naukowych są protokoły kryptograficzne

Najpopularniejsze dziedziny w których prowadzi się badania

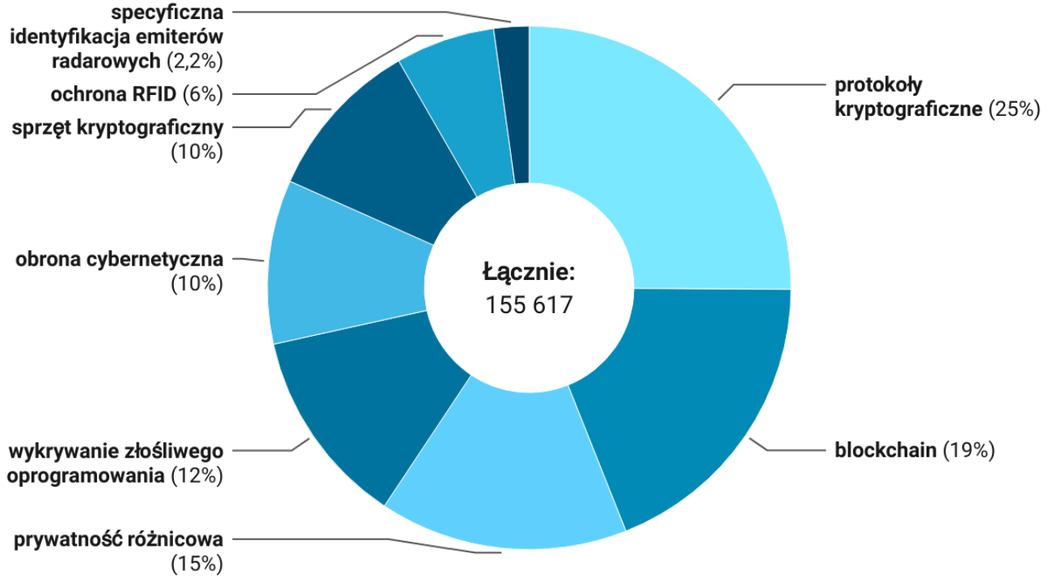
wg kategorii Web of Science, 2015-2025



Źródło: Opracowanie własne na podstawie Web of Science • Narzędzie: Datawrapper

Najpopularniejsze tematy badań

na poziomie mikro w artykułach z obszaru systemów bezpieczeństwa, 2015-2025



Źródło: Opracowanie własne na podstawie Web of Science • Narzędzie: Datawrapper

Obszary i tematyka

Badania zdecydowanie, co nie zaskakuje, są domeną nauk o komputerach i informatyce. Około połowy artykułów opublikowano w dziedzinach (według podziału stosowanego w Web of Science) mieszczących się w tych naukach. Poza nimi przypisano jest także do nauk inżynieryjnych z zakresu elektrotechniki i elektroniki (14%) oraz telekomunikacji (11%). W mniejszym stopniu dotyczy to także innych dziedzin, wśród których znajdują się np. matematyka stosowana, systemy sterowania i kontroli, multidyscyplinarne nauki inżynieryjne i techniczne, instrumenty czy zarządzanie.

Najważniejszą tematyką poruszaną w artykułach naukowych (według tzw. podziału mikrowątków bazy Web of Science) **są protokoły kryptograficzne (25%)**, które dotyczą realizacji sposobu wymiany informacji z użyciem szyfrowania. Popularną tematyką jest także **zastosowanie technologii blokchain (19%), tzw. prywatność różnicowa czyli zaawansowana technologia anonimizacji, która pozwala** nam uzyskać wgląd w dane bez naruszania anonimowości naszych użytkowników (15%). Ważną kwestią jest też **wykrywanie złośliwego oprogramowania (malware) oraz obrona cybernetyczna**. Mniej popularne wątki dotyczą transmisji danych i sprzętu kryptograficznego.

Rozwiązania dotyczące protokołów kryptograficznych są także najczęściej chronionymi patentami na świecie

Najpopularniejsze obszary patentowania

Według grup klasyfikacji IPC w latach 2015-2024

Podgrupa IPC	Nazwa	Liczba
H04L29/06	Sterowanie łącznością; Przetwarzanie telekomunikacyjne znamienne protokołem	109 490
H04L9/40	Protokoły bezpieczeństwa sieci	87 559
G06F21/62	Ochrona dostępu do danych za pomocą platformy, np. z zastosowaniem kluczy lub zasad kontroli dostępu	58 238
G06F21/60	Ochrona danych	52 123
H04L9/32	Układy do łączności utajnionej lub chronionej obejmujące środki do sprawdzania tożsamości lub uprawnienia użytkownika systemu	39 602
H04L29/08	Procedura sterowania transmisją, np. procedura sterowania poziomem łącza danych	36 806
H04L9/08	Rozkład kluczy	27 175
G06F21/64	Ochrona integralności danych, np. z zastosowaniem sum kontrolnych, certyfikatów lub podpisów	24 677
G06F21/31	Autoryzacja użytkownika	23 790
G06F21/32	Autoryzacja użytkownika poprzez użycie danych biometrycznych, np. odcisków palców, skanów tęczówki lub próbek głosu	22 522
G06F21/57	Certyfikowanie lub utrzymywanie zaufanych platform komputerowych	20 191
G06F21/56	Wykrywanie lub zarządzanie złośliwym oprogramowaniem, np. układy antywirusowe	14 826
G06F21/55	Wykrywanie lokalnego wtargnięcia lub realizacja środków zaradczych	13 421
H04W12/06	Sieci komunikacji bezprzewodowej. Uwierzytelnianie	13 015

Źródło: Opracowanie własne na podstawie danych EPO (espacenet) • Narzędzie: Datawrapper

Tematyka patentów określona podgrupami klasyfikacji patentowej jest mocno zróżnicowana, choć ze względu na wcześniejsze przypisanie do dwóch grup mocno tym zdeterminowana. W związku z tym najczęściej występująca **tematyka jest związana z protokołami bezpieczeństwa (109 tys.) a także ochroną danych (52 tys.) , dostępu do danych (58 tys.) i ich integralnością (24,6 tys.)** . Część z patentów związana jest także z autoryzacją użytkownika (23 tys.), z tym poprzez dane biometryczne (22,5 tys.) , czy certyfikowaniem (20 tys.) oraz kluczami kryptograficznymi (27 tys.) . Do popularnej tematyki odnosi się także przeciwdziałanie cyberzagrożeniom, takim jak wykrywania lub zarządzanie złośliwym oprogramowaniem (15 tys.) czy wykrywanie wtargnięcia i związane z tym środki zaradcze (13 tys.).

Spoza powyżej opisanej tematyki najczęściej występują kwestie uwierzytelnia w sieci komunikacji bezprzewodowej (13 tys.), urządzenia lub metody obliczeń cyfrowych lub przetwarzania danych (9,5 tys.). Inną grupą jest odtwarzanie, dystrybucja lub synchronizacja danych pomiędzy bazami danych lub w obrębie rozproszonych systemów baz danych (13 tys.). Jeszcze inną są sieci transmisji danych (9,5 tys.).

Pewne przybliżenie o polach zastosowań dają stosunkowo duża grupa patentów związanych ze strukturami, planami lub protokołami płatności (8,7 tys.), zatwierdzeniem, np. identyfikacją płatnika lub odbiorcy, weryfikacja danych uwierzytelniających klienta lub sklepu (6,8 tys.) czy automatyzacją pracy biurowej, czyli narzędziami biurowymi wykorzystywanymi przez przedsiębiorstwa (7 tys.).

Cyberzagrożenia w artykułach naukowych i patentach

Najczęściej występujące zagrożeniami które są wskazywane w artykułach naukowych i patentach z ostatnich dziesięciu lat są trojany i złośliwe oprogramowanie – malware.

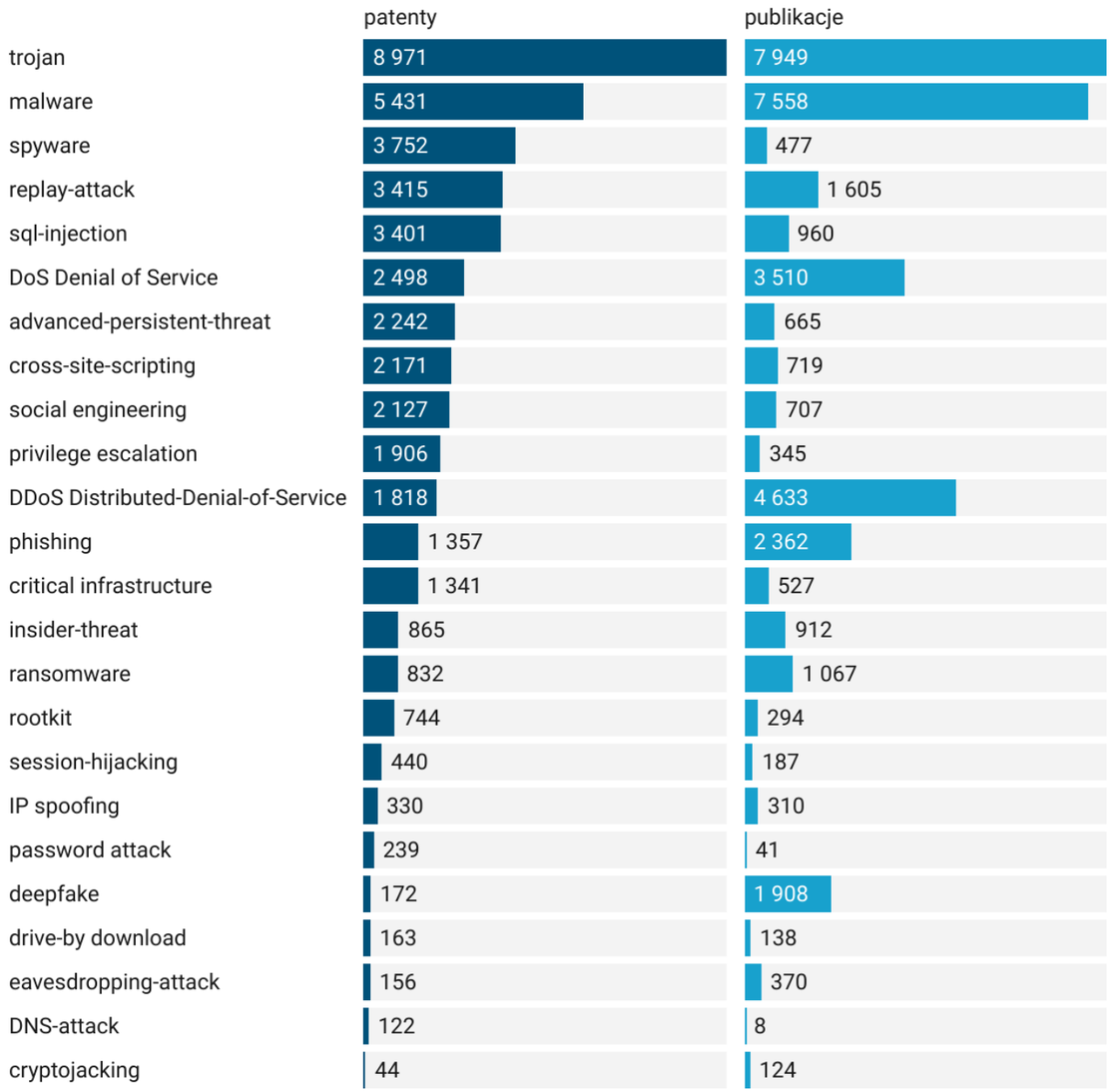
W przypadku pozostałych cyberzagrożeń występują pewne różnice między często-tliwością występowania w opisach patentów i w abstraktach artykułów naukowych. W tych drugich dużo częściej wymieniane są ataki typu DoS i DDoS, a także zagroże-nia związane z technologią deepfake i oprogramowaniem ransomware.
W patentach z kolei dużo częściej wymieniane są zagrożenia typu spyware (oprogramowanie szpiegujące), replay-attack (przechwycenie i retransmisja danych przez sieć), SQL-injection (umieszczenie złośliwego kodu SQL przy zapytaniach do bazy danych), tzw. eskalacja uprawnień (privilage escalation), czy advanced persistent threat (APT) – złożone, długotrwałe cyberataki. Widoczna jest także mała popularność takich cyber-zagrożeń jak cryptojacking, atak DNS czy atak na hasło.

Powyższe różnice mogą (ale nie muszą) wskazywać na pewne rozbieżności pomiędzy gotowanymi do opatentowania technologiami przeciwdziałającymi danemu zagrożeniu, a dopiero wskazywaniem na pewne dopiero rozwijające się technologie. Dotyczy to np. związanego z generatywną AI techniką deepfake, która jest także wykorzystywana do popełniania przestępstw.

Odnosząc to do obszarów cyberbezpieczeństwa, widoczne jest zainteresowanie rozwiązaniami odnoszącymi się do ochrony punktów końcowych (*Endpoint Security*) i wykrywania i reagowania na zagrożenia (*Threat Detection and Response*), a w trochę mniejszym zakresie do bezpieczeństwa sieci (*Network Security*).

Cyberzagrożenia w patentach i publikacjach

liczba dokumentów w których występują dane słowa kluczowe, 2015-2024



Źródło: opracowanie własne na podstawie Espacenet i Web of Science • Narzędzie: Datawrapper

Jednostki naukowe z największą liczbą afiliacji

z zakresu cyberbezpieczeństwa ("security systems") 2015-2024

	Instytucja	Kraj	Liczba
1	Chinese Academy of Sciences		4 471
2	University of California System		2 850
3	Xidian University		2 455
4	Centre National de la Recherche Scientifique CNRS		2 373
5	Indian Institute of Technology System IIT System		2 122
6	State University System of Florida		2 071
7	University of Chinese Academy of Sciences CAS		1 974
8	University of Electronic Science Technology of China		1 930
9	Institute of Information Engineering CAS		1 907
10	University of Texas System		1 835
11	Beijing University of Posts Telecommunications		1 795
12	Nanyang Technological University		1 698
13	National Institute of Technology NIT System		1 669
14	Tsinghua University		1 639
15	University System of Georgia		1 492

Źródło: Opracowanie własne na podstawie Web of Science • Narzędzie: Datawrapper

Najbardziej aktywne jednostki

Wśród instytucji przy których najwięcej afiliowano artykułów naukowych dominują na ogół sieci jednostek naukowych, takich jak Chińska Akademia Nauk, czy w przypadku Stanów Zjednoczonych systemy uniwersytetów stanowych. Dotyczy to np. Uniwersytetu Kalifornijskiego w skład którego wchodzi dziesięć uniwersytetów, w tym Uniwersytet Kalifornijski w Los Angeles i Uniwersytet w Berkeley. Podobne systemy funkcjonują m.in. w Georgii, Teksasie i na Florydzie. Analogiczny system instytutów technologicznych funkcjonuje w Indiach (w 23 lokalizacjach). Poza tymi instytucjami na liście występują też pojedyncze uniwersytety chińskie, a z Europy francuski CNRS. Na liście jednostek patentujących dominują natomiast duże przedsiębiorstwa z zakresu ICT, głównie z Chin i ze Stanów Zjednoczonych.

Najwięcej patentów jest własnością IBM (5,2 tys.). Inne amerykańskie przedsiębiorstwa chroniące na masową skalę swoją własność przemysłową to korporacje z sektora ICT takie jak Microsoft, Amazon, Cisco czy Dell. Uwagę zwraca natomiast obecność wśród liderów korporacji z zakresu finansów – Bank of Amercica. Analogicznie po stronie chińskiej także jest bank – ICBC, choć większość to korporacje zakresu technologii cyfrowych i komunikacji mobilnej. Jedynym przedsiębiorstwem spoza USA i Chin jest koreański Samsung.

Jednostki z największą liczbą patentów

z zakresu cyberbezpieczeństwa (CPC: G06F21, H04L63) 2015-2024

	nazwa jednostki	kraj	liczba patentów
1	IBM		5 248
2	TENCENT TECH SHENZHEN CO LTD		3 897
3	HUAWEI TECH CO LTD		3 636
4	MICROSOFT TECHNOLOGY LICENSING LLC		3 046
5	SAMSUNG ELECTRONICS CO LTD		3 024
6	ALIBABA GROUP HOLDING LTD		2 523
7	STATE GRID CORP CHINA		2 383
8	CHINA MOBILE COMMUNICATIONS GROUP CO LTD		2 311
9	INTEL CORP		2 267
10	AMAZON TECH INC		2 085
11	BANK OF AMERICA		1 818
12	INDUSTRIAL & COMMERCIAL BANK OF CHINA CO LTD		1 731
13	CISCO TECH INC		1 725
14	DELL PRODUCTS LP		1 634
15	CHINA TELECOM CO LTD		1 515

Źródło: Opracowanie własne na podstawie EPO (espacenet) • Narzędzie: Datawrapper

NCBR
Narodowe Centrum Badań i Rozwoju

Cyberbezpieczeństwo – priorytety Polski

Krajowe dokumenty, polityki i strategie dotyczące cyberbezpieczeństwa

Cyberbezpieczeństwo zostało uznane za jeden z filarów bezpieczeństwa narodowego, a rozwój Krajowego Systemu Cyberbezpieczeństwa (KSC) traktowany jest jako kluczowy element wzmacniania suwerenności cyfrowej państwa.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 pozostaje spójna z działaniami dotyczącymi ochrony systemów teleinformatycznych operatorów infrastruktury krytycznej; uwzględnia również potrzeby Sił Zbrojnych RP w zakresie zdolności do prowadzenia operacji w cyberprzestrzeni — zarówno na poziomie krajowym, jak i w ramach struktur sojuszniczych i koalicyjnych.

Strategia państwa w zakresie cyberbezpieczeństwa opiera się na integracji działań legislacyjnych, organizacyjnych i technologicznych. Centralnym elementem cyberbezpieczeństwa jest **Krajowy System Cyberbezpieczeństwa (KSC)** – systemowy mechanizm stworzony. który integruje działania administracji publicznej, podmiotów prywatnych, służb specjalnych oraz wyspecjalizowanych zespołów reagowania (CSIRT) w celu wykrywania, analizowania i przeciwdziałania zagrożeniom w przestrzeni cyfrowej jego rozwój ukierunkowany jest zarówno na zgodność z europejskim prawodawstwem, jak i na budowę realnej odporności państwa na zagrożenia cyfrowe poprzez inwestycje w ludzi, systemy i międzynarodowe partnerstwa.

W 2025 r., Krajowy System Cyberbezpieczeństwa będzie podlegał istotnym zmianom, wynikającym z konieczności wdrożenia do polskiego porządku prawnego dyrektywy NIS2 oraz innego prawodawstwa Unii Europejskiej (m.in. Toolbox 5g). Powyższe zostanie zrealizowane poprzez uchwalenie procedowanej nowelizacji UKSC. Ponadto w planach jest uchwalenie **nowej Strategi Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029**, zawierającej wnioski i doświadczenia z dotychczasowego funkcjonowania KSC oraz która zaadoptuje wyzwania związane z postępem technologicznym, zmianami społecznymi i prawnymi.

Ważnym źródłem wiedzy o bieżącej kondycji krajowego systemu cyberbezpieczeństwa jest **Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa**. W sprawozdaniu za 2024 rok wyraźnie zarysowano strategiczne kierunki rozwoju polityki państwa w zakresie ochrony cyberprzestrzeni.. Jednym z nadrzędnych celów raportu na rok 2024 było przygotowanie KSC do implementacji dwóch fundamentalnych regulacji Unii Europejskiej: **dyrektywy NIS2 oraz rozporządzenia DORA**. Obie regulacje mają wspólny mianownik – budowę systemowej odporności kluczowych usług i sektorów na rosnącą skalę zagrożeń cyfrowych.

Kluczowe krajowe dokumenty strategiczne, legislacyjne i sprawozdawcze:

2013	**Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej**
2017	**Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022**
2018	**Ustawa o krajowym systemie cyberbezpieczeństwa**
2019	**Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024**
2020	**Strategia Bezpieczeństwa Narodowego RP**
2024	**Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok**
2025?	**Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 *(trwają prace)***

Wsparcie publiczne w Polsce w dużej mierze nakierowane jest na wzmocnienie i rozbudowę Krajowego Sytemu Cyberbezpieczeństwa – stanowiącego podwaliny dla implementacji sprawnych i nowoczesnych rozwiązań technologicznych

Krajowy System Cyberbezpieczeństwa (KSC)- system, którego celem jest zapewnienie cyberbezpieczeństwa usług mających kluczowe znaczenie dla działania państwa polskiego, świadczonych przez podmioty publiczne i wybrane przedsiębiorstwa (operatorów usług kluczowych i dostawców usług cyfrowych).

Został utworzony na mocy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w spójności do dyrektywy NIS z 2016 r. nakładającej na państwa członkowskie Unii Europejskiej wspólne, minimalne wymagania dot. cyberbezpieczeństwa

Usługi kluczowe wg KSC to te, których zakłócenie miałoby istotny wpływ na funkcjonowanie państwa, gospodarkę, zdrowie i bezpieczeństwo obywateli: m.in.:

- Zaopatrzenie w energię, surowce energetyczne i paliwa
- Łączność
- Systemy finansowe i infrastruktura rynków finansowych
- Zaopatrzenie w żywność
- Zaopatrzenie w wodę pitną
- Ochrona zdrowia
- Transport
- Produkcja, składowanie i stosowanie substancji chemicznych i promieniotwórczych
- Poczta
- Infrastruktura cyfrowa

Do **kluczowych sektorów KSC** zalicza się:

- Sektor energetyczny
- Sektor transportowy
- Sektor bankowy i infrastruktury rynków finansowych
- Sektor ochrony zdrowia
- Sektor zaopatrzenia w wodę pitną i jej dystrybucji
- Sektor infrastruktury cyfrowej
- Sektor administracji publicznej
- Ponadto, do kluczowych sektorów mogą być zaliczane także inne obszary

Kluczowe podmioty objęte KSC to:

1. **Operatorzy usług kluczowych**
2. **Dostawcy usług cyfrowych** –
3. **Zespoły CSIRT (Computer Security Incident Response Team**) poziomu krajowego
   - **CSIRT GOV – prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego**, odpowiedzialny za koordynację obsługi incydentów zgłaszanych przez administrację publiczną, operatorów infrastruktury krytycznej oraz właścicieli i posiadaczy obiektów infrastruktury krytycznej.
   - **CSIRT NASK – prowadzony przez Naukową i Akademicką Sieć Komputerową (NASK)**, odpowiedzialny za obsługę incydentów zgłaszanych przez pozostałe podmioty, w tym operatorów usług kluczowych, dostawców usług cyfrowych, małe i średnie przedsiębiorstwa oraz osoby fizyczne.
   - **CSIRT MON – prowadzony przez Ministra Obrony Narodowej**, odpowiedzialny za obsługę incydentów zgłaszanych przez podmioty podległe MON lub przez niego nadzorowane.
4. **Podmioty świadczące usługi z zakresu cyberbezpieczeństwa**
5. **Sektorowe zespoły cyberbezpieczeństwa**
6. **Organy właściwe do spraw cyberbezpieczeństwa** – organy administracji publicznej odpowiedzialne za różne aspekty cyberbezpieczeństwa,
7. **Pojedynczy Punkt Kontaktowy (PPK)**

Priorytety dla Polski wynikające z dokumentów strategicznych

Budowa odpornego systemu narodowego cyberbezpieczeństwa

Rozwój KSC jako kluczowy filarem bezpieczeństwa państwa.
System ten musi obejmować zarówno sektor publiczny, prywatny, jak i komponent wojskowy, tworząc **spójną strukturę odporną na incydenty** o charakterze technicznym, organizacyjnym i geopolitycznym.
Niezbędne jest dalsze wzmacnianie: integracja krajowych i sektorowych zespołów CSIRT, wdrażanie jednolitych metodyk oceny i zarządzania ryzykiem oraz rozwój kanałów wymiany informacji o zagrożeniach, podatnościach i incydentach. **Systemowe podejście do reagowania – z wykorzystaniem nowoczesnych narzędzi i procedur.**

I

Ochrona usług kluczowych i infrastruktury krytycznej

. Obszary takie jak **energetyka, transport, finanse, zdrowie, telekomunikacja i administracja publiczna** tworzą kręgosłup państwa, a ich odporność na cyberzagrożenia jest warunkiem ciągłości działania państwa i bezpieczeństwa obywateli.
Kluczowe jest zatem wdrażanie zharmonizowanych standardów bezpieczeństwa, testów penetracyjnych, kontroli zgodności z wymaganiami ustawy o KSC oraz systematyczne zarządzanie podatnościami w środowisku OUK i operatorów infrastruktury krytycznej.
Strategia jednoznacznie wskazuje na Warunkiem skuteczności tego priorytetu jest również włączenie sektora prywatnego w model zarządzania odpornością usług kluczowych.

II

Inwestycje w krajowe technologie i kompetencje

Budowanie suwerennego potencjału technologicznego w obszarze cyberbezpieczeństwa **wymaga inwestycji w rozwój krajowych rozwiązań, zdolności badawczo-rozwojowych oraz kompetencji specjalistów.**
Polska powinna wspierać innowacyjne MŚP, startupy i krajowych integratorów technologii w tworzeniu rozwiązań zgodnych z europejskimi standardami, jednocześnie rozwijając krajowy system certyfikacji. Równolegle niezbędne jest wzmacnianie kapitału ludzkiego – zarówno poprzez specjalistyczne programy edukacyjne, jak i kampanie społeczne podnoszące świadomość zagrożeń cyfrowych.
W dokumentach przedstawiono szereg inicjatyw : program PWCyber, granty dla MŚP, szkolenia z zakresu AI, ćwiczenia z cyberhigieny i ochrony danych.

III

Integracja obrony cywilnej i militarnej oraz współpraca międzynarodowa

Polska, jako państwo frontowe i członek NATO i UE, musi **rozwijać zdolność Sił Zbrojnych do prowadzenia działań defensywnych i ofensywnych w cyberprzestrzeni oraz utrzymywać gotowość do reagowania na działania o charakterze hybrydowym i** informacyjnym.
Wskazano potrzebę scalenia systemów obronnych i cywilnych oraz aktywnej obecności w strukturach międzynarodowych.
Dokumenty wskazują na **potrzebę synergii między instytucjami administracji rządowej, podmiotami prywatnymi i służbami odpowiedzialnymi za bezpieczeństwo** narodowe – jako warunek efektywnego funkcjonowania i dalszego rozwoju KSC.

IV

Systemowe podejście do wdrażania i regulacji

Polityka cyberbezpieczeństwa musi być zarządzana w sposób systemowy, **zgodny z długofalową wizją i strategiczną architekturą państwa**. Kluczowe jest, aby wszystkie inicjatywy – legislacyjne, organizacyjne, edukacyjne czy technologiczne – były spójne, powiązane logicznie i podporządkowane wspólnym celom operacyjnym oraz mierzalnym wskaźnikom. Dokumenty wyraźnie wskazują na konieczność planowego wdrażania **Narodowych Standardów Cyberbezpieczeństwa** (NSC), krajowego systemu certyfikacji, rejestrów incydentów i podatności, a także wdrażania i monitorowania przepisów wykonawczych do aktów jak **NIS2 i DORA**.
Zintegrowane podejście wymaga jasnego przypisania odpowiedzialności instytucjonalne oraz wdrożenia mechanizmów analizy skuteczności i elastycznego dostosowania
do nowych zagrożeń.

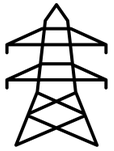
V

Obszary priorytetowe* dla Polski

*Na podstawie *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* i *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok*

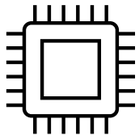
Edukacja

Rozwój kompetencji w zakresie cyberbezpieczeństwa. Kluczowe jest kształtowanie świadomości zagrożeń i umiejętności cyfrowych już na etapie edukacji ogólnej oraz rozwój kadr technicznych i specjalistycznych. Rekomenduje się włączenie tematyki „cyber" do podstaw programowych, rozwój kierunków studiów i certyfikację specjalistów.



Infrastruktura krytyczna

Za infrastrukturę krytyczną uznajemy systemy, których zakłócenie może zagrozić bezpieczeństwu państwa, zdrowiu obywateli lub funkcjonowaniu gospodarki – w szczególności w sektorach energii, finansów, transportu i zdrowia. W 2024 r. realizowano testy penetracyjne, analizy podatności oraz współpracę CSIRT-ów sektorowych z operatorami. Postuluje się standaryzację zabezpieczeń, rozwój wymiany informacji i wdrażanie audytów bezpieczeństwa. Dokumenty podkreślają konieczność stałego nadzoru i budowania odporności systemowej.



Sektor prywatny

Pełni kluczową rolę w budowie odporności cyfrowej kraju, jako dostawca technologii, usług oraz innowacyjnych rozwiązań. Wsparcie powinno koncentrować się na uproszczeniu dostępu do narzędzi ochronnych, zwiększeniu skali doradztwa oraz promowaniu rozwiązań open source. W 2024 r. prowadzono analizy potrzeb MŚP, udostępniono usługi ochronne (AntyDDoS, Zastrzeż PESEL) i realizowano działania edukacyjne. Rekomenduje się rozwój certyfikacji branżowej, ściślejszą współpracę z administracją oraz wspieranie działalności B+R w obszarze technologii bezpieczeństwa i systemów zgodnych z krajowymi standardami.

Siły zbrojne RP

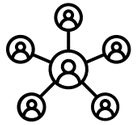
Wojska Obrony Cyberprzestrzeni zyskały istotne zdolności operacyjne i technologiczne. Rozwijano infrastrukturę, prowadzono ciągły monitoring i testy odporności systemów wojskowych. MON zintensyfikował współpracę międzynarodową oraz szkolił kadry specjalistyczne. W 2024 r. wdrażano Narodowe Standardy Cyberbezpieczeństwa dla resortu obrony, tworzono zaplecze techniczne do analizy zagrożeń, a także przygotowywano procedury reagowania na poziomie strategicznym i taktycznym. Rozbudowywano także zdolności ofensywne i prowadzono szkolenia w ramach ćwiczeń zintegrowanych, m.in. w zakresie cyberobrony infrastruktury wojskowej i wspólnego reagowania z partnerami sojuszniczymi. Rekomenduje się kontynuację programów CYBER.MIL i Akademia_CYBER.MIL, rozwój zaplecza kadrowego oraz większe zaangażowanie w działania unijne, m.in. w ENISA i ćwiczenia UE.

Obszary priorytetowe* dla Polski

*Na podstawie *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* i *Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok*

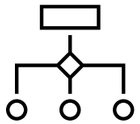
Społeczeństwo

Budowa świadomego i odpornego społeczeństwa traktowana jest jako jeden z filarów systemu bezpieczeństwa państwa. Wskazuje się na konieczność kontynuacji wielokanałowych kampanii informacyjnych, dalszego rozwoju usług samoobrony cyfrowej i silniejszego zaangażowania NGO w działania profilaktyczne.



Operatorzy usług cyfrowych

Stanowią strategiczne ogniwo krajowego systemu cyberbezpieczeństwa. W 2024 r. prowadzono kontrole zgodności z ustawą o KSC, wspierano ich poprzez narzędzia samooceny i komunikaty ostrzegawcze publikowane przez Pełnomocnika. CSIRT-y sektorowe zapewniały wsparcie operacyjne i analityczne. Wskazuje się na potrzebę ujednolicenia standardów zabezpieczeń, zwiększenia odporności na incydenty ransomware oraz włączenia operatorów w systemową wymianę informacji i reagowanie na incydenty.



JST

JST są wskazywane jako najsłabsze ogniwo krajowego systemu cyberbezpieczeństwa, ze względu na niską dojrzałość organizacyjną i technologiczny deficyt zabezpieczeń. W 2024 r. uruchomiono program „Cyberbezpieczny Samorząd”, oferujący finansowanie, szkolenia oraz audyty. Do najczęstszych problemów należą brak zespołów reagowania, niespójne procedury oraz niska świadomość wśród decydentów lokalnych. Rekomenduje się powoływanie lokalnych SOC-ów, integrację z CSIRT NASK i włączenie JST w krajowy obieg informacji o zagrożeniach. Zalecane jest także wdrożenie planów ciągłości działania oraz szkolenia dedykowane pracownikom JST w ramach systemów zarządzania kompetencjami.

Administracja publiczna

Objęta procesem wdrażania Narodowych Standardów Cyberbezpieczeństwa, rozbudowy SOC-ów oraz bezpiecznej komunikacji międzyresortowej. W 2024 r. uruchomiono Centrum Operacji Bezpieczeństwa Państwa (COBP), realizowano testy podatności i wdrożono systemy wymiany informacji. Rekomenduje się konsolidację usług bezpieczeństwa, rozwój kompetencji kadry zarządzającej, włączenie cyberbezpieczeństwa w procesy decyzyjne oraz ścisłej koordynacji między urzędami. Zaleca się rozwój kompetencji, certyfikację pracowników, budowę systemów zarządzania ciągłością działania oraz wyrównanie różnic płacowych względem sektora prywatnego.

Korzyści z rozwijania krajowego sektora cyberbezpieczeństwa są wielowymiarowe i obejmują zarówno sferę bezpieczeństwa, jak i gospodarki, społeczeństwa, edukacji oraz pozycji międzynarodowej.

Wymiar ekonomiczny

- Wzmocnienie zaufanie inwestorów do prowadzenia działalności w Polsce.
- Przyciągnięcie kapitał, lokowanie centrów operacyjnych i technologicznych
- Rozwój rodzimego sektora high-tech.
- Oszczędności - zapobieżenie przestojom, wyciekom danych i szkodom wizerunkowym.

Wymiar społeczny

- Budowa dojrzałości cyfrowej obywateli.
- Bezpieczeństwo korzystania z technologii.
- Wzrost zaufania obywateli do usług cyfrowych,

Wymiar edukacyjny i badawczo -rozwojowy

- Zwiększone zapotrzebowanie na specjalistów w dziedzinach związanych z bezpieczeństwem cyfrowym
- Uruchamianie kierunków studiów oraz szkoleń
- Wzrost znaczenie praktycznej współpracy między środowiskiem naukowym a sektorem publicznym i prywatnym
- Specjalizacja ośrodków badawczych i centrów kompetencji,
- Tworzenie sieci współpracy krajowej i międzynarodowej.

Znaczenie krajowych rozwiązań i sposoby wdrożenia

Realizacja celów Strategii Cyberbezpieczeństwa RP oraz działań opisanych w sprawozdaniu Pełnomocnika Rządu wymaga zastosowania szerokiego wachlarza konkretnych narzędzi. Poniżej przedstawiono **główne mechanizmy wdrażania polityki cyberbezpieczeństwa:**

1. Narzędzia legislacyjne i regulacyjne
- Nowelizacje ustaw – np. ustawy o KSC, przygotowanie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)
- Strategie i plany działań – przyjmowanie dokumentów takich jak: Strategia Cyberbezpieczeństwa, Plan działań wykonawczych

2. Finansowanie i instrumenty wsparcia
- Dotacje
- Fundusz Cyberbezpieczeństwa – świadczenia teleinformatyczne i inwestycje
- Konkursy grantowe
- Krajowy Plan Odbudowy (KPO) – finansowanie projektów zwiększających odporność cyfrową państwa

3. Mechanizmy organizacyjne
- CSIRT-y (Gov, MON, NASK, sektorowe) – zespoły reagowania na incydenty, analizy zagrożeń, komunikacja z interesariuszami
- Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC)

4. Mechanizmy edukacyjne i kompetencyjne
- Programy szkoleniowe i certyfikacja
- Portal edukacyjny

5. Narzędzia operacyjne i technologiczne
- Systemy bezpieczeństwa
- Platformy technologiczne .
- Testy i audyty cyberbezpieczeństwa.

6. Współpraca międzynarodowa
- Zaangażowanie w ENISA, NATO, UE, współpraca z Ukrainą

NCBR
Narodowe Centrum Badań i Rozwoju

Wyzwania dla rozwoju technologii na rzecz cyberbezpieczeństwa

Stały wysoki wzrost rynku cyberbezpieczeństwa w Polsce

Zgodnie z raportami PMR, **wartość rynku cyberbezpieczeństwa w Polsce w 2024 roku wyniosła 2,8 mld zł**, osiągając wzrost o 11% rok do roku. Prognozy wskazują, że **w 2025 roku rynek ten osiągnie wartość około 3,5 mld.**

Rynek cyberbezpieczeństwa **zdefiniowano wąsko jako urządzenia zabezpieczające firmową sieć** (głównie UTM i NGFW), **rozwiązania aplikacyjne** (od podstawowych antywirusów po m.in. firewalle, rozwiązania anty spam/spyware, systemy IDS/IPS, DLP, anty-ATP, anty-DDoS, do kompleksowych systemów SIEM) **oraz usługi** (audyt, pentesty, doradztwo, usługi zarządzane, SOC)

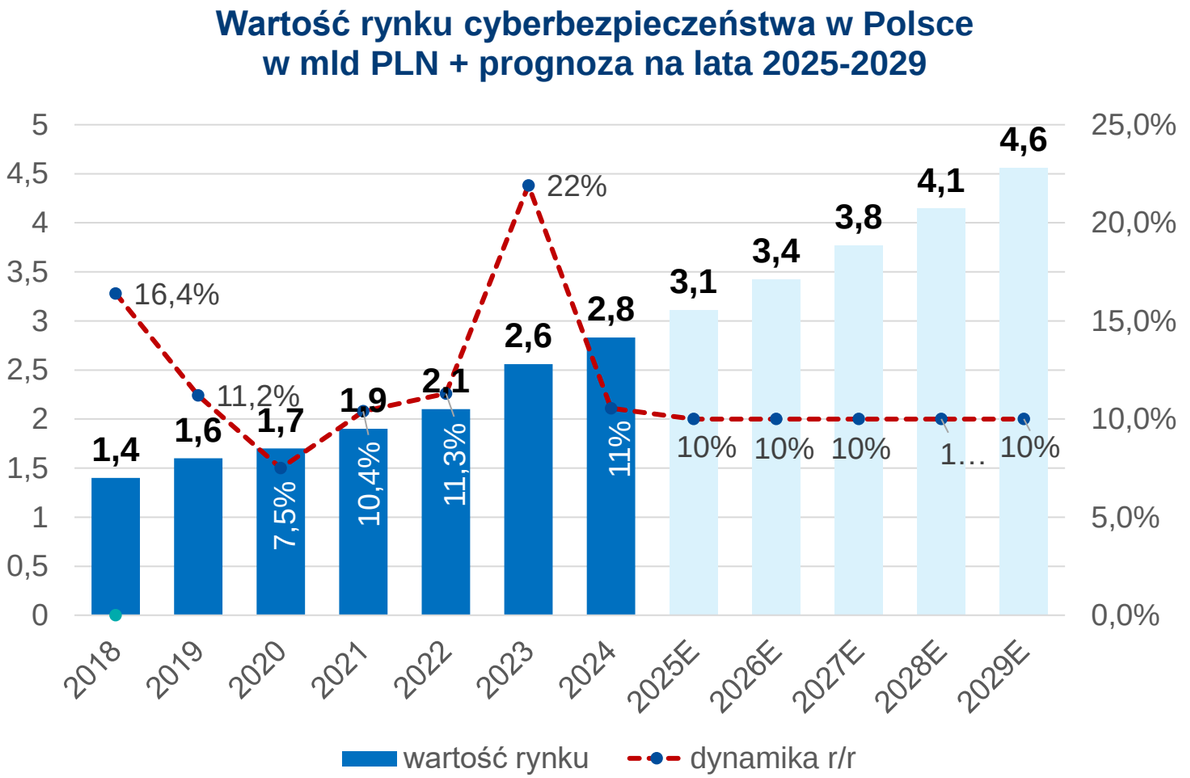
Szerokie podejście do zdefiniowania rynku cyberbezpieczeństwa rozszerzone **o chmurę obliczeniową, rynek usług data centrowych, backup, hosting** oraz inne obszary, takie jak zapewnienie bezpieczeństwa fizycznego, zasilanie awaryjne i informatykę śledczą, **zwiększa jego wartość do ok 12 mld zł.**

Na lata 2025–2029 przewiduje się dalszy wzrost rynku, z dynamiką na poziomie 10% rocznie, co wynika z:

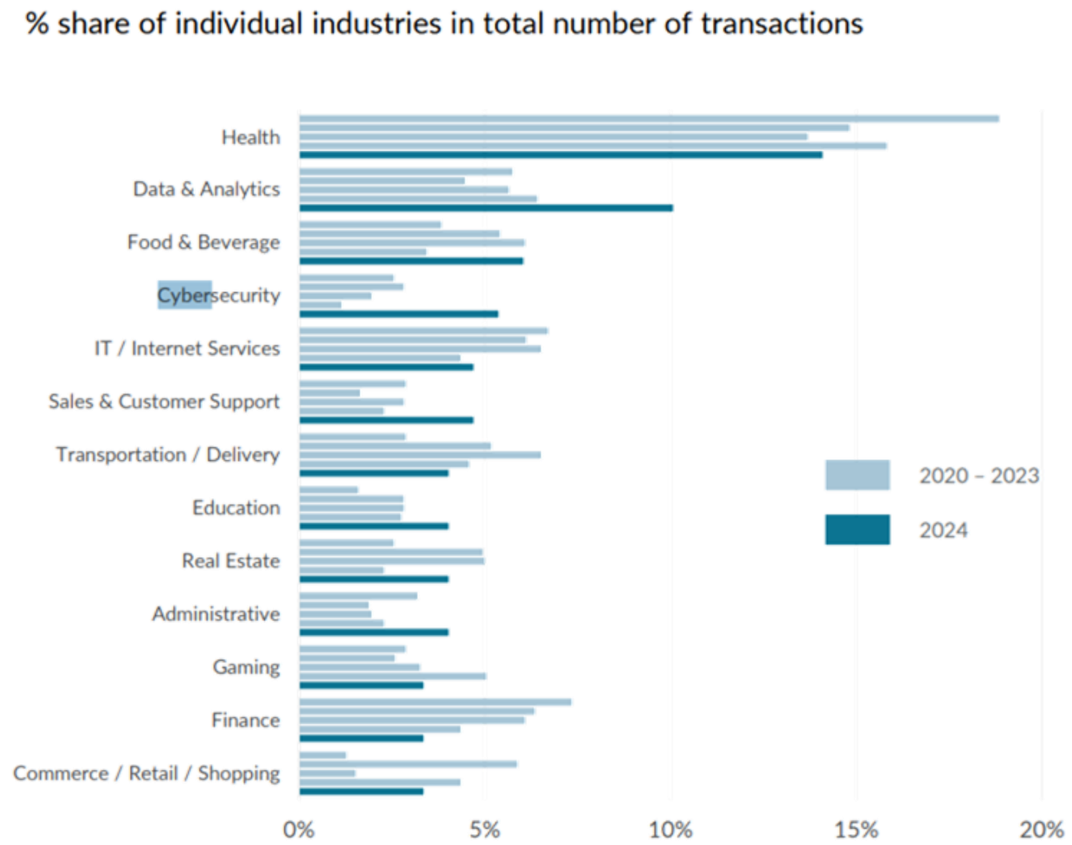
- **rosnącej liczby cyberataków** (np. 83% firm w Polsce odnotowało incydent w 2024 roku, wzrost o 16 p.p. względem 2023)

- **wdrożenia regulacji takich jak unijna dyrektywa NIS2**, która zaostrza wymogi dla kluczowych sektorów

- **zwiększonego zapotrzebowania na rozwiązania oparte na chmurze i sztucznej inteligencji** (AI).



Źródło: PMR, obliczenia własne



Źródło: PFR Polish VC market Outlook 2024

Dane PFR pokazują **zwiększenie udziału inwestycji związanych z cyberbezpieczeństwem przez polskie fundusze Venture Capital w** 2024 roku (ok. 5%). **W 2024 był to czwarty pod względem znaczenia obszar inwestycyjny**. Niestety ze względu na brak dokładnych danych o transakcjach nie da się określić na ile wzrost ten spowodowany jest spadkiem w pozostałych kategoriach, a na ile wzrostem znaczenia AI.

Zgodnie z danymi Fundacji Startup Poland **w Polsce działa 14 funduszy** (spośród 165 dla których dostępne są dane), **których strategia inwestycyjna obejmuje cyberbezpieczeństwo**. Są to: Aria Fund, BitSpiration Booster Fund, Eastshield, EEC Magenta, ffVC Tech&Gaming, Grupa Assay, LT Capital, OTB, PKO VC, Polski Instytut Badań i Rozwoju, Quality Business Network QBN Seed Fund, Satus Starter, Tradecim Innovation Fund, Warsaw Equity Group.

Wzrost udziału inwestycji polskich funduszy VC w cyberbezpieczeństwo w 2024 roku

Co najmniej połowa tych funduszy finansuje wczesną fazę wzrostu spółek (*seed, proof-of principle/proof of concept*), ale cześć finansuje także fazy późniejsze (*post-seed, early growth stage)* oraz fazę wzrostu (*growth stage*). Powoduje to, że to **tzw. ticket inwestycyjny jest dość zróżnicowany w zależności od fazy i funduszu. Według dostępnych danych waha się od 200 tys. do 15 mln EUR**. Tym samym można założyć, że pod tym względem teoretycznie nie występuje luka w finansowaniu dla spółek z sektora CyberSec.

Przykłady spółek portfelowych związanych z sektorem to:

SECFENSE

Założona w 2018 roku spółka, oferująca min. metody uwierzytelniania. Swoje rozwiązania wdraża w polskich przedsiębiorstwach, bankach, administracji publicznej.

CYBERPREVENT

Spółka, oferująca m.in. infrastrukturę oraz narzędzia do utrzymania bezpieczeństwa wraz z ich wdrożeniem, konfiguracją i obsługą.

NaviRisk

Jest siecią firm konsultingowych zajmujących się ryzykiem biznesowym, wywiadem, cyberbezpieczeń-stwem i bezpieczeństwem

FUDO SECURITY

Oferuje oprogramowanie do zarządzania dostępem uprzywilejowanym (PAM). Spółka obsługuje ok. 500 klientów w 35 krajach. Fudo Security jest beneficjentem NCBR

W strukturze rynku dominują duże przedsiębiorstwa, ale największa dynamika prognozowana jest w sektorze MŚP

Prognoza wzrostu rynku cyberbezpieczeństwa w Polsce na lata 2025–2030

Ogólna dynamika rynku: rynek cyberbezpieczeństwa w Polsce będzie rósł w tempie 10% rocznie, osiągając wartość blisko 5 mld zł w wąskiej definicji do 2029 roku. W szerszej definicji (z uwzględnieniem chmury, data center itp wartość może przekroczyć 15 mld zł.

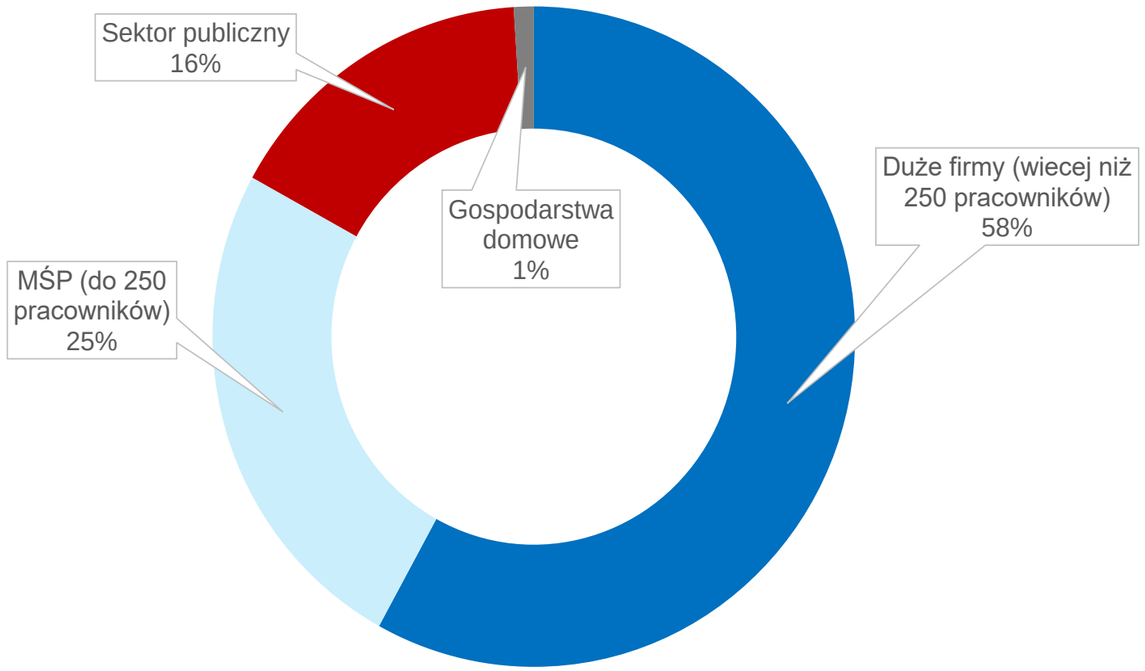
Kluczowe czynniki wzrostu:

- **Rosnące zagrożenia**: wzrost liczby ataków (np. +126% ataków ransomware w I kw. 2025) i ich złożoność (wykorzystanie AI) wymuszają inwestycje w zaawansowane technologie.
- **Regulacje**: wdrożenie NIS2 i zmiany w ustawie KSC zwiększają presję na zgodność z wymogami, szczególnie w sektorach krytycznych.
- **Sztuczna inteligencja**: AI staje się kluczowym narzędziem w walce z cyberprzestępczością (95% CISO uważa, że AI poprawia efektywność działań prewencyjnych), ale wymaga też nowych zabezpieczeń.
- **Chmura i praca zdalna**: migracja do chmury (np. RChO, IaaS) i hybrydow modele pracy zwiększają popyt na rozwiązania bezpieczeństwa aplikacji i danych

Zmiany wg segmentów rynku:

- **Duże przedsiębiorstwa i sektor publiczny**: największy wzrost dzięki regulacjom i inwestycjom w infrastrukturę krytyczną.
- **MŚP**: szybki wzrost dzięki cyfryzacji i dostępności chmurowych rozwiązań.
- **Konsumenci indywidualni**: wzrost umiarkowany, ale napędzany e-commerce i m-commerce.

Struktura rynku cyberbezpieczeństwa według wydatków grup odbiorców w Polsce (2021)



Źródło: PMR

Duże przedsiębiorstwa

- **Udział w rynku**:

duże przedsiębiorstwa (**ok. 5000 największych firm w Polsce) odpowiadają za około 58% wartości rynku** cyberbezpieczeństwa

- **Charakterystyka**:

liderami wydatków są **sektory bankowy, finansowy i telekomunikacyjny**, gdzie bezpieczeństwo danych jest kluczowe ze względu na charakter działalności i regulacje. W 2021 roku widoczne były także inwestycje dostawców VOD i treści multimedialnych, co wskazuje na rosnącą rolę sektora mediów. Duże firmy inwestują w zaawansowane rozwiązania, takie jak systemy SIEM, firewalle nowej generacji (NGFW), DLP, IDS/IPS oraz usługi zarządzane (SOC).

- **Potencjał wzrostu**:

wzrost wydatków napędzany jest przez transformację cyfrową, migrację do chmury oraz konieczność dostosowania do regulacji (np. NIS2, AI Act). **Przewiduje się stabilny wzrost na poziomie 10–12% rocznie**, wynikający z większej liczby incydentów (np. 2300 ataków ransomware w I kw. 2025, +126% r/r) i rosnącej świadomości zagrożeń.

- **Kluczowe trendy**:

zwiększone **wykorzystanie AI w zabezpieczeniach** (34% firm używa AI do wsparcia IT, ale tylko 13% w cyberbezpieczeństwie) oraz inwestycje w ochronę infrastruktury krytycznej (energetyka, finanse, zdrowie).

Małe i średnie przedsiębiorstwa (MŚP)

- **Udział w rynku**:

MŚP mają mniejszy **udział w rynku (25%),** ale ich znaczenie rośnie dzięki cyfryzacji i pracy zdalnej.

- **Charakterystyka**

Są bardziej narażone na ataki ransomware i phishing, co zwiększa **popyt na podstawowe rozwiązania, takie jak antywirusy, firewalle i szkolenia**. Ograniczony budżet i brak specjalistów IT sprawiają, że MŚP coraz **częściej sięgają po usługi zarządzane i rozwiązania chmurowe.**

- **Potencjał wzrostu**:

segment ten ma **wysoki potencjał wzrostu (ok. 15–20% rocznie**), ponieważ cyfryzacja i regulacje wymuszają inwestycje w zabezpieczenia.

- **Kluczowe trendy**

Popularność chmurowych rozwiązań bezpieczeństwa (np. IaaS od dużych dostawców) rośnie, co obniża bariery wejścia dla MŚP.

Wzrost popytu na usługi outsourcingu IT i szkolenia z cyberbezpieczeństwa, szczególnie w kontekście pracy zdalnej i hybrydowej.

Sektor publiczny

- **Udział w rynku**:

16% (w tym administracja centralna, samorządy, instytucje militarne) stanowi istotną część rynku, szczególnie w kontekście regulacji KSC i NIS2.

- **Charakterystyka**:

w 2024 roku odnotowano 627 339 zgłoszeń incydentów; **inwestuje w rozwiązania chmurowe** (np. Rządowa Chmura Obliczeniowa, Krajowe Centrum Przetwarzania Danych) **oraz w szkolenia** podnoszące cyberświadomość.

Kluczowe obszary: ochrona infrastruktury krytycznej (energetyka, zdrowie, transport) oraz przeciwdziałanie dezinformacji, szczególnie w kontekście wyborów prezydenckich 2025.

- **Potencjał wzrostu**:

wzrost **o 12–15% rocznie,** napędzany przez regulacje (NIS2, KSC) i konieczność modernizacji systemów IT w administracji.

- **Kluczowe trendy**:

wymagają szczególnego wsparcia **ze względu na ograniczone budżety i brak specjalistów, co zwiększa popyt na usługi zewnętrzne i rozwiązania chmurowe**.

Konsumenci indywidualni

- **Udział w rynku**:

najmniejszy segment, **szacowany na 1% rynku**, głównie ze względu na ograniczoną świadomość i niskie budżety.

- **Charakterystyka**:

obejmuje **podstawowe oprogramowanie antywirusowe, VPN-y i rozwiązania do ochrony danych osobowych**. Wzrost zainteresowania wynika z rosnącej liczby ataków phishingowych i kradzieży danych w e-commerce (np. 38% badanych chce aktywnych informacji o zagrożeniach od e-sklepów).

- **Potencjał wzrostu**:

wzrost na poziomie 5–10% rocznie, napędzany rosnącą świadomością cyberzagrożeń i popularyzacją zakupów online (m-commerce ma wzrosnąć do ponad 50% sprzedaży e-commerce do 2028).

- **Kluczowe trendy**:

Zwiększone zapotrzebowanie na proste, przystępne cenowo rozwiązania, szczególnie w segmencie e-grocery i m-commerce.

Narodowe Centrum Badań i Rozwoju

Stan cyberbezpieczeństwa przedsiębiorstw w Polsce

Rosnąca liczba cyberzagrożeń i ich negatywnych konsekwencji dla firm

Na podstawie danych z raportu KPMG „Barometr cyberbezpieczeństwa z 2025 r

83% firm w Polsce doświadczyło cyberataków w 2024 r.

42% firm w Polsce odczuwa wzrost liczby zaobserwowanych prób cyberataków w 2024 r.

Wg cyklicznego badania prowadzonego przez KPMG pt Barometr cyberbezpieczeństwa , w edycji z 2025 roku **blisko połowa firm (46%) odnotowuje stabilną liczbę ataków , na bezpieczeństwo cyfrowe w porównaniu do lat wcześniejszych. Coraz więcej firm - w sumie 42%** (o 8 pp. w stosunku do uprzedniego roku) **zauważyło nasilenie cyberataków**

O zwiększeniu intensywności ataków świadczy również niemal **dwukrotny spadek liczby organizacji, które nie odnotowały żadnego ataku – z 33% do 17%** w analogicznym okresie.

Całkowita liczba prób ataków rośnie niezależnie od wielkości firmy - największą intensyfikację odnotowują duże przedsiębiorstwa (55% z nich zauważyło wzrost lub znaczny wzrost).W grupie średnich znaczny wzrost odnotowało 38% firm, a w grupie małych 40% .

33% firm Polsce w 2023 roku doświadczyło kłopotów związanych z utratą bezpieczeństwa cyfrowego. W największym stopniu problemy ten dotykał podmiotów dużych, z których aż 44% miał tego typu problemy, 40% podmiotów średnich i około 30% małych**.**

Rodzaje incydentów w przedsiębiorstwach:

29,7% - brak możliwości korzystania z zasobów ICT przedsiębiorstwa z powodu **awarii sprzętu lub oprogramowania**

7,7% - zniszczenie lub uszkodzenie danych z powodu **awarii oprogramowania** lub sprzętu

3,0% - niemożność korzystania z zasobów ICT przedsiębiorstwa z powodu **ataku hackerskiego np. typu DoS, ransomware**

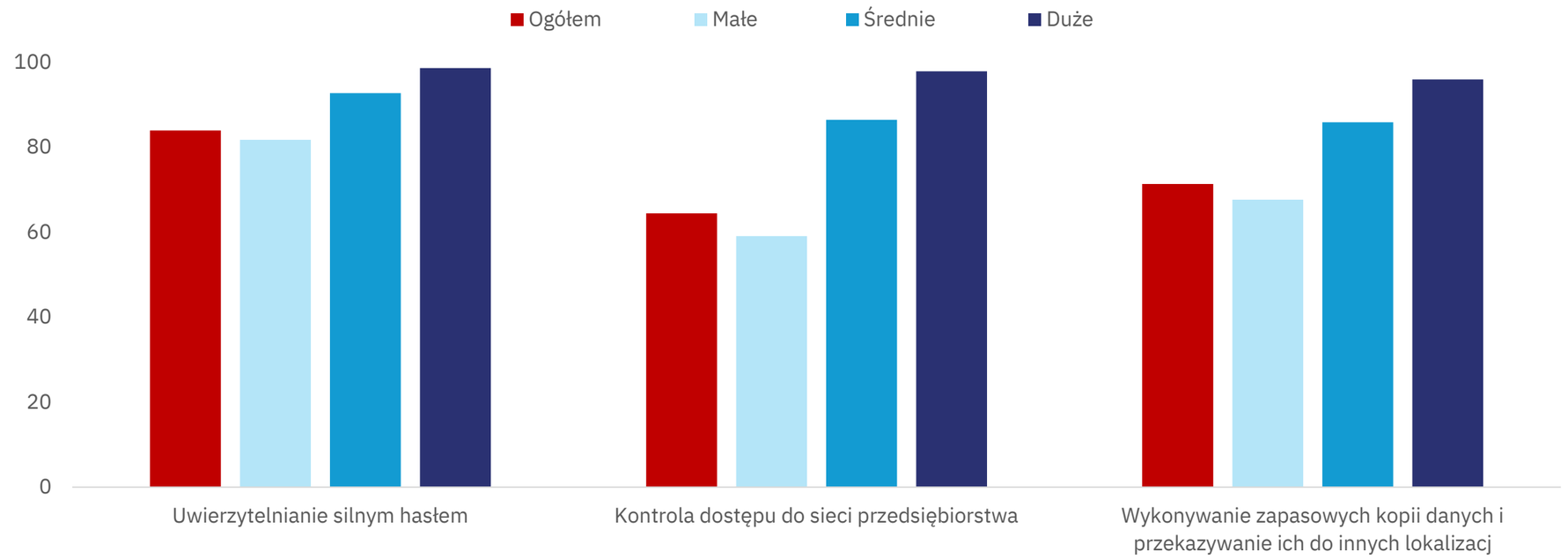
2,6% - zniszczenie lub uszkodzenie danych z powodu **zainfekowania złośliwym oprogramowaniem lub włamania**

1,1% - ujawnienie poufnych danych z powodu **włamania, ataku typu pharming, phishing** , celowego działania pracowników

1.0% - ujawnienie poufnych danych w wyniku niedopatrzenia ze strony pracowników

Polskie firmy w umiarkowany sposób zabezpieczają się przed cyberzagrożeniami

Udział przedsiębiorstw stosujących wybrane środki bezpieczeństwa ICT w 2024 r



Źródło: Społeczeństwo informacyjne w Polsce w 2024 r. GUS

Wg danych GUS - w 2024 r. **odsetek przedsiębiorstw stosujących przynajmniej jeden z trzech podstawowych środków bezpieczeństwa ICT wyniósł 94,1%.** Wszystkie z badanych środków wykorzystywano **najczęściej w dużych przedsiębiorstwach - 99,6%.** Sytuacja wygląda diametralnie odmiennie **w przypadki sektora małych przedsiębiorstw**, wśród których około 80% zabezpiecza swoje zasoby ICT przez uwierzytelnienie hasła dostępowego, a **jedynie około 60% kontroluje w ogóle dostęp do sieci przedsiębiorstwa.**

Tendencja ta choć niepokojąca jest zgodna z analogicznymi wynikami dla przedsiębiorstw w całej UE. Poziom zabezpieczeń w firmach Polskich jest nawet na wyższym niż średnio w UE poziomie. **Zgodnie z wynikami *European Union survey on ICT zrealizowanej w 2023 w całej UE* 83% dużych przedsiębiorstw stosuje co najmniej jeden środek bezpieczeństwa ICT, ale w przypadku MŚ jest to tylko 49%.**

Najniższy poziom zabezpieczeń stosują formy z branży turystycznej oraz budownictwa

W ujęciu branżowym najbardziej zabezpieczone są przedsiębiorstwa z sektora ICT – **ponad 90% podmiotów korzysta ze wszystkich trzech sposobów ochrony.**

W najmniejszym stopniu natomiast budownictwo oraz podmioty świadczące usługi turystyczne oraz budownistwo – nieco ponad połowa chroni dostęp do swoich sieci

Niepokojący jest stosunkowo wysoki odsetek – **ok 20% podmiotów zajmujących się dostawą kluczowych usług dla społeczeństwa** – dostawa energii i dostawa wody, w których nie stosuje się ani zabezpieczeń kontroli dostępu do sieci, ani kopii zapasowych dla danych systemowych.

sektor	Uwierzytelnianie silnym hasłem	Kontrola dostępu do sieci przedsiębiorstwa	Wykonywanie zapasowych kopii danych i przekazywanie ich do innych lokalizacji
Przetwórstwo przemysłowe	**83,7**	**62,8**	**71**
Wytwarzanie i zaopatrywanie w energię elektryczną, gaz, parę wodną i gorącą wodę	**94,8**	**81,8**	**80,7**
Dostawa wody, gospodarowanie ściekami i odpadami; rekultywacja	**90,6**	**79,1**	**77,8**
Budownictwo	**76,1**	**51,9**	**61,4**
Handel; naprawa pojazdów samochodowych	**86**	**67,4**	**73,9**
Transport i gospodarka magazynowa	**82,8**	**57,6**	**69,9**
Zakwaterowanie i gastronomia	**77,3**	**53,9**	**56,4**
Informacja i komunikacja	**96**	**92,1**	**91,2**
Obsługa rynku nieruchomości	**92**	**80,6**	**78,1**
Działalność profesjonalna, naukowa i techniczna	**93,6**	**83,2**	**86,3**
Administrowanie i działalność wspierająca	**81,2**	**64,5**	**69,9**
Naprawa i konserwacja komputerów i sprzętu komunikacyjnego	**96,4**	**91,7**	**93,5**

Źródło: Społeczeństwo informacyjne w Polsce w 2024 r. GUS

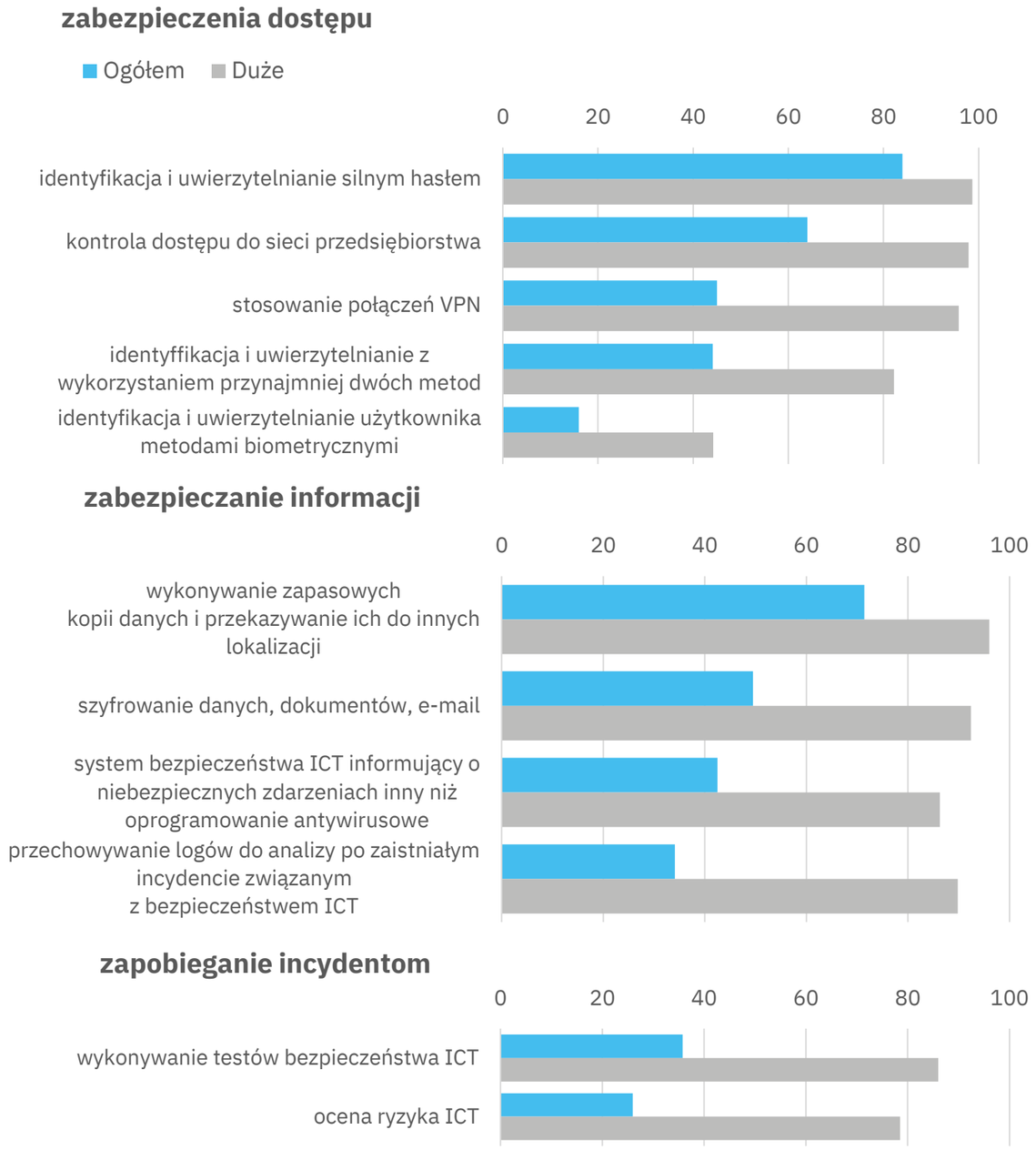
Ogromna dysproporcja w stosowaniu zabezpieczeń między przedsiębiorstwami dużymi a MŚP

Dane GUS* wskazują na **ogromne dysproporcje w poziomie zabezpieczeń przed cyberzagrożeniami w przedsiębiorstwach w Polsce w zależności od wielkości firm.**
Przedsiębiorstw duże stosują najczęściej kilkustopniowe zabezpieczenia w większości kluczowych obszarów potencjalnego ataku (dostęp do wewnętrznych systemów, zagrożenia dla danych wewnętrznych) , a także stosują (choć rzadziej) działania służące zapobieganiu incydentom w ogóle – takie ja testy bezpieczeństwa, ocena ryzyka ICT.

W przypadku **MŚP najczęściej stosowane zabezpieczenia do w przypadku dostępu do systemów wewnętrznych to identyfikacja silnym hasłem (ponad 80%),** VPN lub uwierzytelnienie dwustopniowe stosuje około 45%.
Rzadziej chronione są w MŚP dane wewnętrzne – ok 70% MŚP wykonuje kopie zapasowe, a ok. 45% szyfruje dane i dokumenty. **Jedynie ¼ tego typu firm dokonuje ocen ryzyka ICT.**

Wniosek ten i podobna tendencję w innych krajach UE potwierdzają ustalania *EUROPEAN UNION AGENCY FOR CYBERSECURITY* zamieszczone w raporcie: *„2024 report on the state of cybersecurity in the union”,* gdzie również wskazano na wyraźne – analogiczne do tych w firmach w Polsce - równice zależne od wielkości firmy i dojrzałości sektora w zakresie wdrażania różnorodnych form zapobiegania ryzykom w obszarze cyberbezpieczeństwa oraz dysproporcję miedzy świadomością zagrożeń a realnymi działaniami zaradczymi.

**Źródło: Społeczeństwo informacyjne w Polsce w 2024 r. GUS*



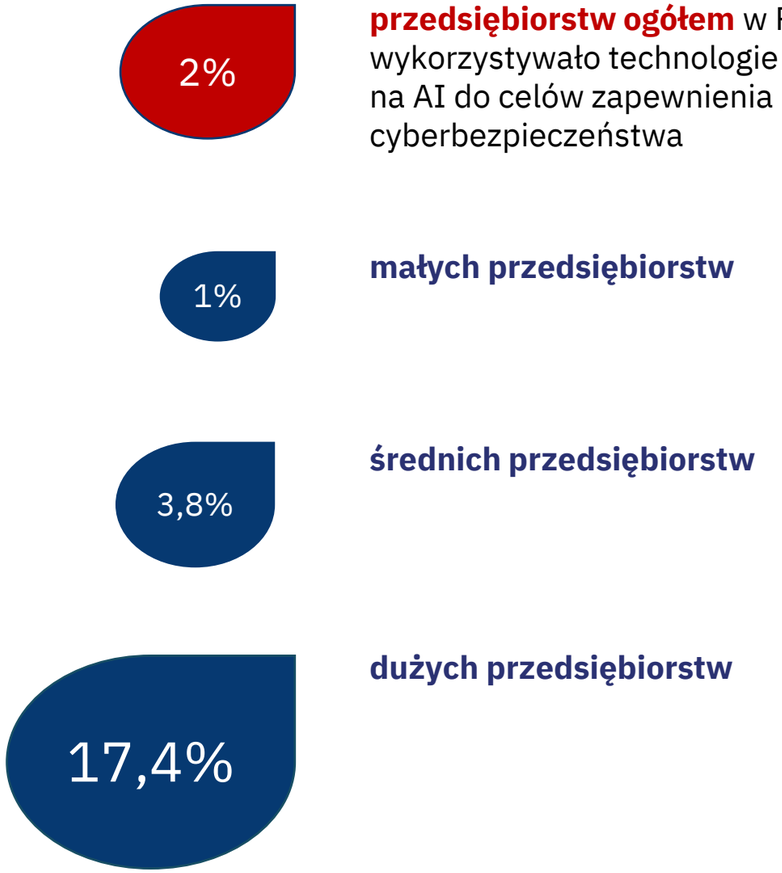
Tylko 2% przedsiębiorstw wykorzystuje nowoczesne technologie AI do wzmocnienia swojego cyberbezpieczeństwa

Wykorzystanie AI do celów cyberbezpieczeństwa w przedsiębiorstwach w Polsce wg struktury własności

własność krajowa 1,4% ⟷ **6,2% własność zagraniczna**

Zgodnie z wynikami raportu przygotowanego przez EY z 2024 *r pt: Jak polskie firmy wdrażają AI? Analiza zmian rok do roku Edycja 2”,* zdecydowana większość firm deklaruje działania na rzecz zwiększania cyberbezpieczeństwa w procesie wdrażania nowych technologii, w szczególności AI, ale ich rzeczywiste zaangażowanie w ten obszar jest znacznie niższe. Wg autorów raportu **92% firm zadeklarowało, że wdrożyło dodatkowe zabezpieczenia z zakresu cyberbezpieczeństwa przed rozpoczęciem korzystania z narzędzi AI, ale tylko 32 % zadeklarowała rzeczywiste inwestycje finansowe** w tego typu zabezpieczeń.

Również dane gromadzone przez GUS dotyczące **wykorzystania technologii AI do zapewnienia cyberbezpieczeństwa przedsiębiorstw wskazują, że dzieje się tak jedynie w 2% firm w ogóle,** a w 17,5% dużych



przedsiębiorstw ogółem w Polsce wykorzystywało technologie oparte na AI do celów zapewnienia cyberbezpieczeństwa

małych przedsiębiorstw

średnich przedsiębiorstw

dużych przedsiębiorstw

Rosnąca świadomość cyberzagrożeń - firmy planują zwiększenie nakładów na nowoczesne technologie i strategie ochrony

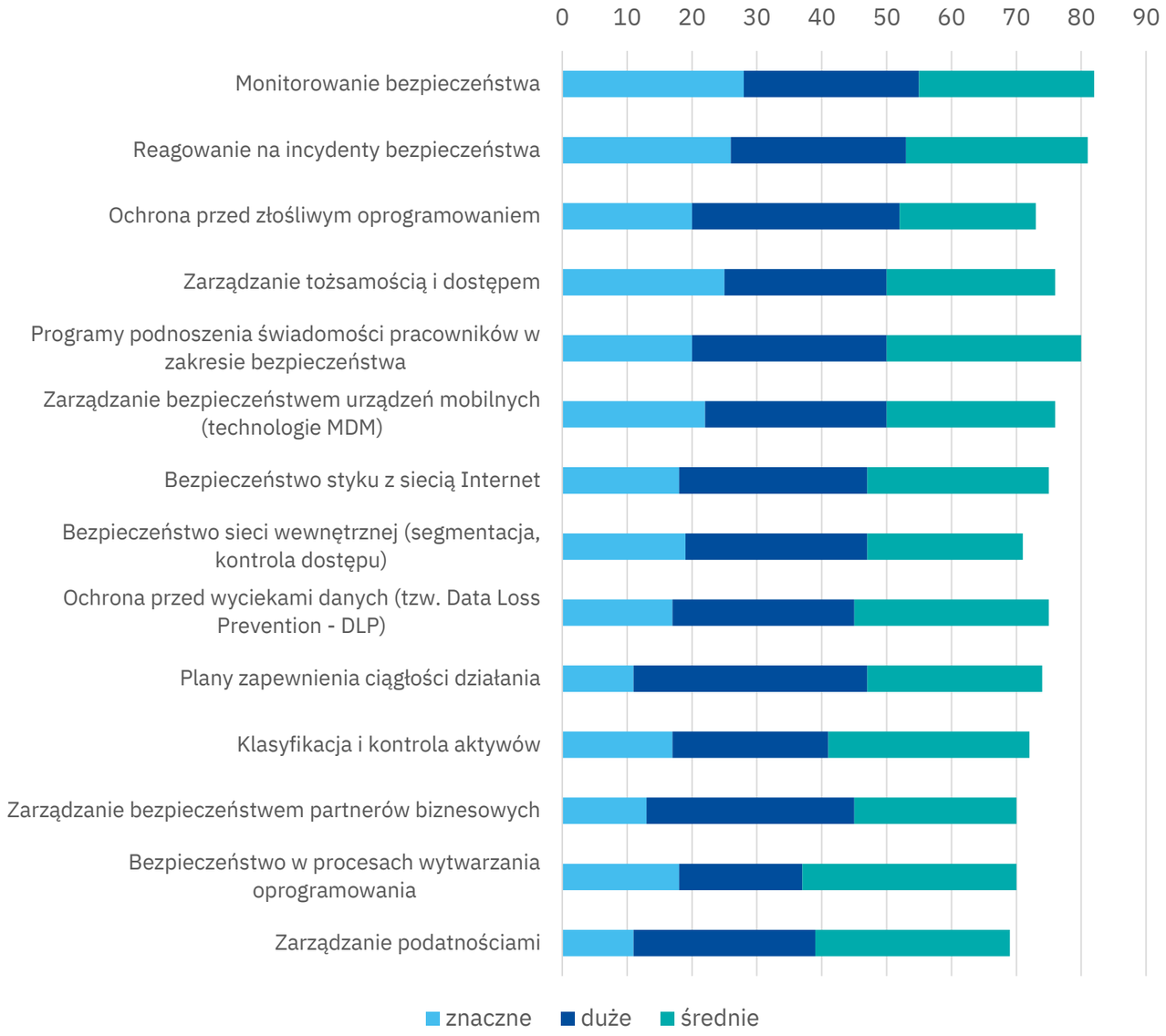
Na podstawie danych z raportu KPMG „Barometr cyberbezpieczeństwa z 2025r

Ocena dojrzałości zabezpieczeń przed incydentami, prezentowana w raporcie KPMG zmieniła się na przestrzeni ostatnich pięciu lat. **W 2020 roku** wśród badanych firm **przeważała opinia o pełnej dojrzałości zabezpieczeń w „większości analizowanych obszarów przesądzających o zabezpieczeniu cyfrowym**. **W 2024 już tylko jedna na dziesięć firm zadeklarowała pełną dojrzałość w większości obszarów** zabezpieczeń, pozostałe 90% dojrzałość w mniej niż połowie obszarów.

Jest to **wyraźny sygnał narastającego tempa rozwoju nowych wyzwań w zakresie cyberbezpieczeństwa oraz rosnącej świadomości konieczności dalszego rozwoju zabezpieczeń.**

Firmy planują **większe inwestycje w cyberbezpieczeństwo niż w poprzednich latach– przede wszystkim na monitorowanie bezpieczeństwa oraz reagowanie na incydenty, rozwój ochrony przed złośliwym oprogramowaniem oraz zarządzanie tożsamością i dostępem**. Ten ostatni obszar awansował o cztery miejsca w rankingu w stosunku do poprzedniej edycji badania, co podkreśla znaczenie ochrony danych użytkowników oraz precyzyjnego nadzoru nad dostępem do zasobów.

Poziom inwestycji w obszary cyberbezpieczeństwa



Dwucyfrowy wzrost rynku cyberbezpieczeństwa w Polsce, chociaż plany firm w ograniczonym stopniu dotyczą najbardziej nowoczesnych rozwiązań technologicznych

Na podstawie danych z raportu: PMR Market Eksperts, Rynek cyberbezpieczeństwa w Polsce 2023. Analiza rynku i prognozy rozwoju na lata 2023-2028

Plany firm w Polsce dotyczące rozwiązań z zakresu cyberbezpieczeństwa w obszarze technologii chmury obliczeniowej, analizy zachowań użytkowników oraz AI & Deep learning

	Chmura obliczeniowa	Analiza zachowań użytkownika (UBA)	AI & Deep learning
Planujemy rozszerzenie	44%	17%	13%
Planujemy wdrożenie	18%	14%	22%
Nie zamierzamy ani rozszerzyć, ani wdrożyć	30%	52%	48%
Nie wiem/trudno powiedzieć	8%	17%	17%

Źródło: PMR, 2023 r.

W ciągu kolejnych 2 lat **40% średnich i dużych firm w Polsce planuje rozbudowę rozwiązań związanych z obszarem cyberbezpieczeństwa i chmurą obliczeniową, a kolejne 18 % wdrożenie** tego typu rozwiązań.

Około **13% planuje inwestować w rozszerzenie** rozwiązań na rzecz cyberbezpieczeństwa wykorzystujących **AI i deep learning, a około 1/5 planuje w ogóle ich wdrożenie.**

W najmniejszym stopniu firmy są gotowe do wdrożenia nowoczesnych technologii UBA/UEBA wykorzystujących m.in. analizy behawioralne i uczenie maszynowe **do detekcji nietypowych zachowani użytkowników,** w tym innych niż ludzie**.**

Narodowe Centrum Badań i Rozwoju

Wsparcie publiczne

Ponad 1 mld EUR na włączenie kolejnych podmiotów do KSC oraz podniesienie kompetencji specjalistów – działania te mają głównie charakter inwestycyjny, w marginalnym stopniu badawczo-rozwojowy

FERC – Fundusze Europejskie na Rozwój Cyfrowy

Działanie 02.02 Wzmocnienie krajowego systemu cyberbezpieczeństwa – 378 mln EUR

Przewidziane działania

- Projekty na rzecz wzmocnienia krajowego systemu cyberbezpieczeństwa.
- Wdrażanie rozwiązań łączących różne zakresy interwencji zaplanowanej w II Priorytecie FERC

Działanie 02.05 Wsparcie umiejętności cyfrowych – 62,7 mln EUR

Przewidziane działania (jedno z wielu)

- Podnoszenie kompetencji kadr zaangażowanych w świadczenie usług, produktów lub procesów cyfrowych, w tym m.in. wsparcie zaawansowanych kompetencji specjalistycznych z zakresu cyberbezpieczeństwa i gospodarki danych, jak również dostępności cyfrowej

Fundusz Cyberbezpieczeństwa

uchwalony przez Radę Ministrów w 2022 r- **ok 250 mln zł rocznie (ok 59 mln EUR – rocznie)**Państwowy fundusz celowy, którym zarządza minister cyfryzacji. Świadczenia dla osób realizujących zadania w podmiotach KSC służące m.in. analizie złośliwego oprogramowania, analizie powłamaniowej (forensic), wykrywaniu zagrożeń lub incydentów (cyber threat intelligence), tworzeniu rekomendacji technicznych.

Program Współpracy w Cyberbezpieczeństwie (PWCyber)

Współpraca partnerska pomiędzy sektorem publicznym i prywatnym na rzecz krajowego systemu cyberbezpieczeństwa. Jest to przedsięwzięcie niekomercyjne o charakterze partnerstwa publiczno-prywatnego, służące pogłębieniu współpracy, wymianie informacji, wspólnych rekomendacjach.

KPO – Krajowy Plan Odbudowy

Przewidziane działania

Inwestycja C3.1.1. KPO - Cyberbezpieczeństwo -CyberPL - infrastruktura przetwarzania danych i dostarczania usług cyfrowych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – ok. 2,4 mld złotych (ok 560 mln EUR)

Przewidziane 4 działania w obszarze cyberbezpieczeństwa

- Ustanowienie sieci obejmującej co najmniej 5 sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w sektorach: energetyki, transportu, służby zdrowia, bankowości, infrastruktury rynków finansowych, infrastruktury cyfrowej, zaopatrzenia w wodę i przedsiębiorstwach łączności elektronicznej;
- podłączenie 385 podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem;
- udzielenie 500 podmiotom wsparcia na rzecz modernizacji i rozbudowania infrastruktur cyberbezpieczeństwa,
- utworzenie sieci specjalistów w dziedzinie cyberbezpieczeństwa na szczeblu wojewódzkim,

CYBER.MIL.PL - program Ministerstwa Obrony Narodowej, którego celem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni

- Powołanie 8.02.2022 - Wojska Obrony Cyberprzestrzeni
- konsolidacji posiadanych zasobów naukowych i intensyfikacji badań naukowych w obszarze cyberbezpieczeństwa
- Prowadzenie prac B+R m.in. przez Wojskowy Instytut Łączności PIB
- Rozbudowa oferty edukacyjnej

Rozbudowa ponadnarodowych sieci współpracy oraz wzmocnienie B+R w zakresie wykorzystanie AI i technologii postkwantowych jako priorytety wsparcia obszaru cyberbezpieczeństwa w UE

Komisja Europejska

Digital Europ Programme (DEP), w ramach którego jeden z priorytetów zoperacjonalizowany został jako programu dot. cyberbeziepczeństwa: Cybersecurity Work Programme 2025–2027 - 357 mln EUR

Przewidziane działania:

- Europejski system ostrzegania o cyberbezpieczeństwie: rozmieszczenie centrów operacyjnych ds. bezpieczeństwa
- Działania w zakresie gotowości, takich jak skoordynowane testy gotowości podmiotów działających w sektorach wysokim poziomie krytyczności.
- Sztuczna inteligencja na rzecz cyberbezpieczeństwa
- Szyfrowanie postkwantowe: przejście na technologie szyfrowania postkwantowego dla przemysłu i administracji publicznej

Horyzont Europa

Klaster III - bezpieczeństwo cywilne społeczeństwa, sekcja 3.1.3. Bezpieczeństwo cybernetyczne.

– działania w ramanmach HE w zakresie cyberbezpieczeństwa powierzone przez KE do zarządzane przez ECCCC – European Cybersecurity Competencje Center; a na poziomie krajowym **Krajowe Centrum Kompetencji Cyberbezpieczeństwa - 90,55 mln EUR w 2025 r**

Przewidziane działania:

- Generatywna sztuczna inteligencja dla aplikacji cyberbezpieczeństwa (40 mln EUR)
- Nowe zaawansowane narzędzia i procesy dla Cyberbezpieczeństwa (23,5 mln EUR)
- Technologie zwiększające ochronę prywatności (11 mln EUR)
- Analiza algorytmów pod kątem potencjalnych zagrożeń ze strony komputerów kwantowych (4 mln EUR)
- 2 konkursy dotyczące bezpieczeństwa algorytmów kwantowych i ich integracji (12 mln EUR)

NCBR
Narodowe Centrum Badań i Rozwoju

Wsparcie NCBR obszaru cyberbezpieczeństwa

NCBR sfinansował rozwiązania z zakresu cyberbezpieczeństwa na kwotę ponad 1 mld zł

Od 2007 roku NCBR dofinansowało ponad 130 projektów mających związek z cyberbezpieczeństwem

Na podstawie predefiniowanej listy słów kluczowych występujących w tytułach projektów znajdujących się w bazie NCBR zidentyfikowano 135 dotyczących szeroko rozumianego cyberbezpieczeństwa.

Wg stanu na koniec 2024 roku, trwających lub zakończonych było 91% z nich, rozwiązano lub zawieszono pozostałe 9%.

Rysunek (...) częstotliwość występowania słów kluczowych w tytułach projektów dot. cyberbezpieczenstwa

1,08 mld zł - łączna wartość projektów

82% - udział dofinansowania NCBR

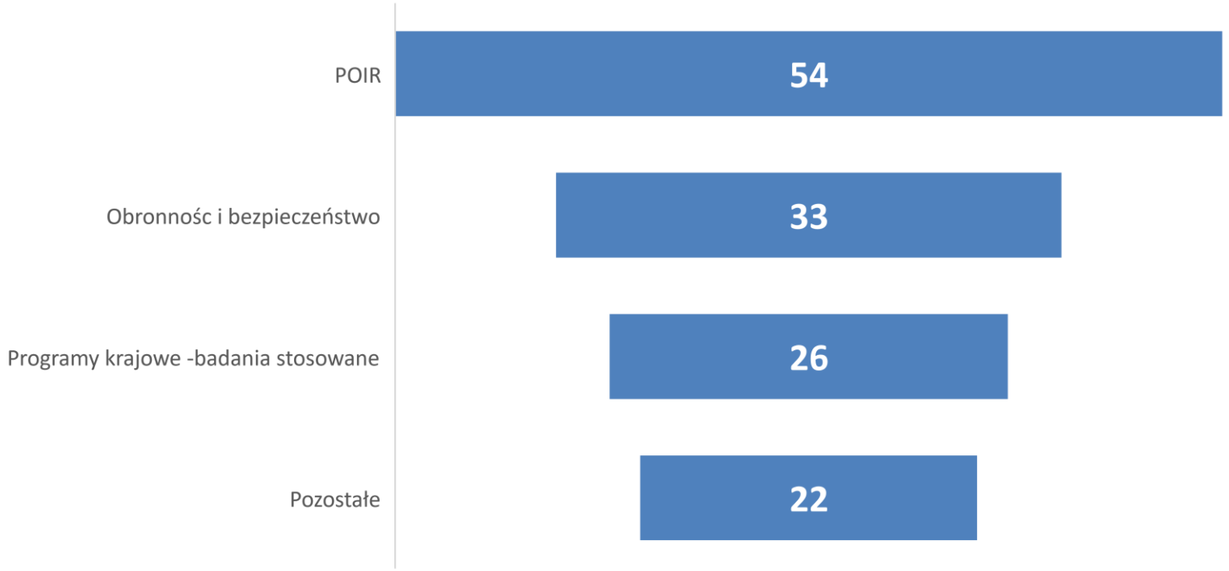
8,01 mln zł – średnia wartość projektu

11 – liczba rozwiązanych umów

83 mln zł – wartość umów rozwiązanych

5 – liczba nadal realizowanych projektów

Programy w których realizowano projekty dot. cyberbezpieczeństwa

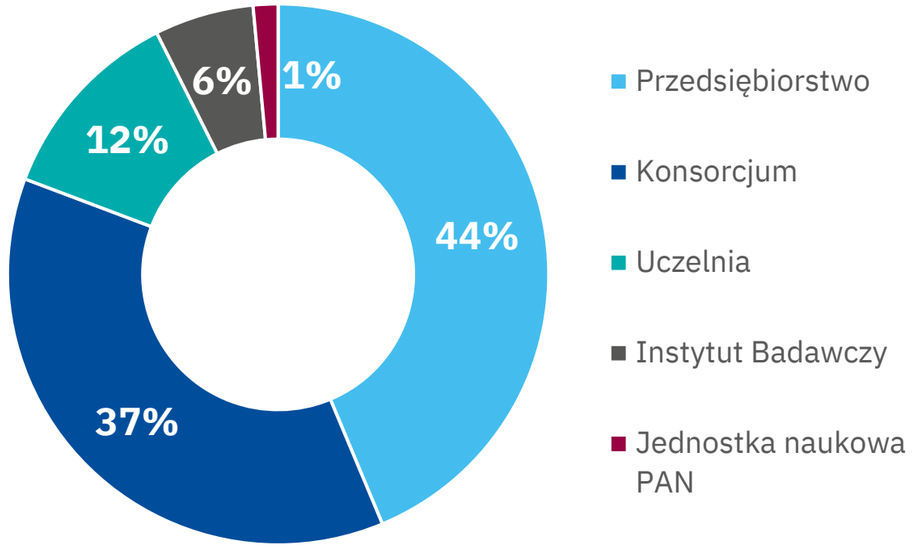


Najwięcej projektów było realizowanych w Programie Operacyjnym Inteligentny Rozwój, w ramach konkursu **„Szybka ścieżka - Innowacje cyfrowe”.**

W programach obronnościowych dominowały projekty realizowane w ramach serii konkursów **„Projekty rozwojowe”.**

W tzw. „krajówce” niemal wszystkie projekty realizowano w (specjalnie dedykowanym tej tematyce) konkursie **„CyberSecident I-IV”**

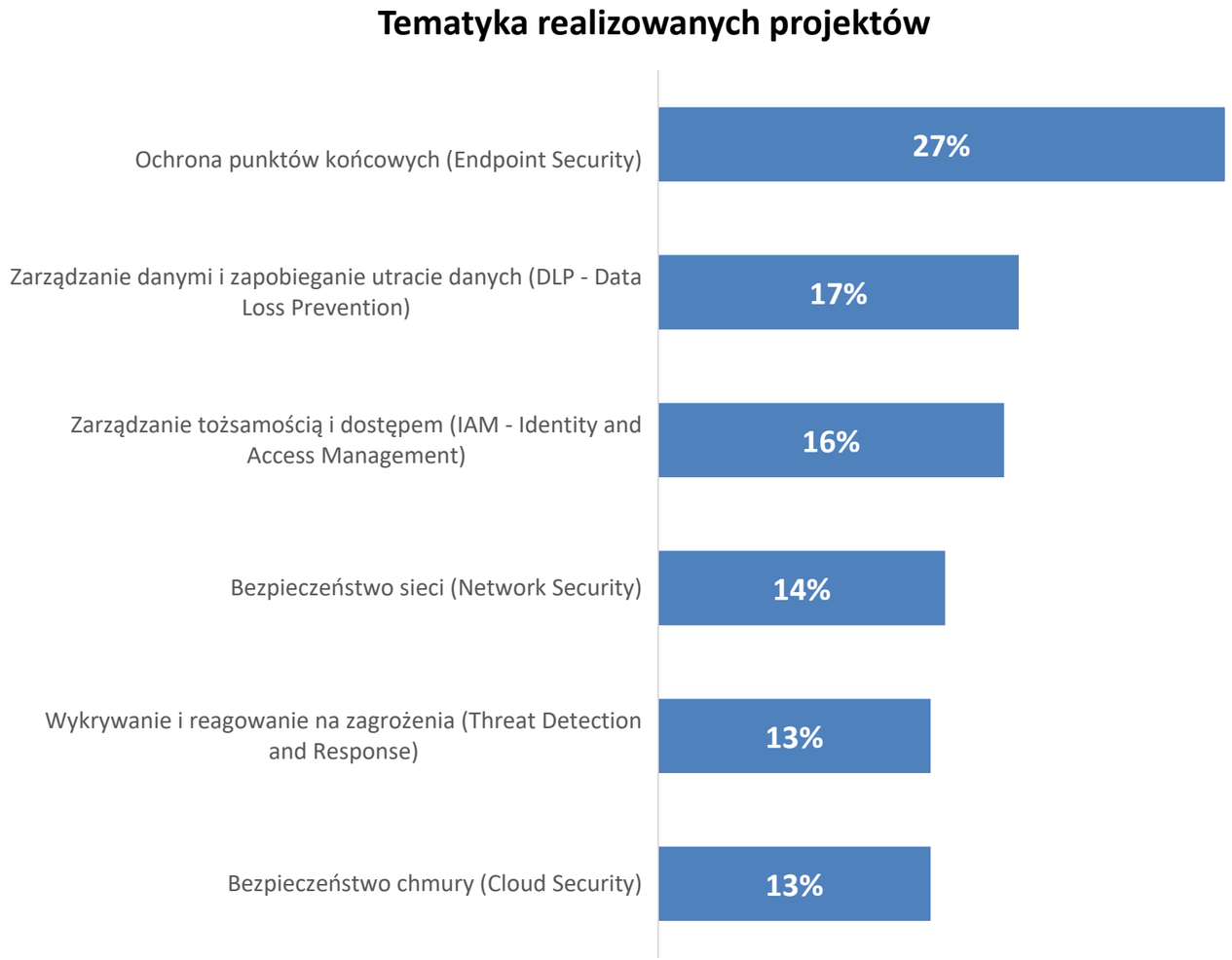
Forma prawna beneficjentów



Wśród beneficjentów **dominowały przedsiębiorstwa**, działające samodzielnie lub w konsorcjach z jednostkami naukowymi. Łącznie ich udział przekraczał 80% wszystkich projektów.

Najmniej licznie były reprezentowane instytuty badawcze wraz z jednostkami Polskiej Akademii Nauk

Ochrona punktów końcowych sieci jako dominująca tematyka projektów w NCBR



Najwięcej projektów było skierowanych na ochronę końcowych użytkowników urządzeń narażonych na cyberataki np.:

SendGuard - zwiększające bezpieczeństwo odbiorców innowacyjne narzędzie oparte o technologię Machine Learning oraz Artificial Intelligence do walki z problemem spamu i phishingu w wiadomościach e-mail marketingowych oraz transakcyjnych

Środowisko budowy i eksploatacji bezpiecznych aplikacji działających w chmurze w oparciu o inteligentne wykrywanie anomalii w klastrach obliczeniowych oraz techniki kryptograficzne blockchain/DLT

TAMAbox – wirtualne i fizyczne urządzenia chroniące przed atakami typu DDoS (Distributed Denial of Service).

CyberSecIdent - Specjalny program poświęcony cyberbezpieczeństwa finansowany w NCBR

W 2017 roku NCBR ogłosiło pierwszy z czterech konkursów „CyberSecident”

Cel główny
Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2028.

Cele szczegółowe
wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości
wdrożenie metod i technik identyfikacji i uwierzytelniania.

Działanie	liczba projektów	wartość ogółem
CyberSecident I	4	48 080 542,75 zł
CyberSecident II	6	63 840 227,02 zł
CyberSecident III	3	39 831 081,75 zł
CyberSecIdent IV	9	88 619 939,25 zł

Liderem ponad połowy projektów była Wojskowa Akademia Techniczna w Warszawie

Wojskowa Akademia Techniczna

- **W konkursach dofinansowano 22 projekty na łączna kwotę 240 mln zł**
- **Rozwiązano 1 umowę o wartości 8,9 mln zł**
- **Łączne dofinasowanie NCBR wyniosło 224 mln zł**

NCBR
Narodowe Centrum Badań i Rozwoju

Obszary wymagające wsparcia: desk reserch na potrzeby ewaluacji cybersecident

Wnioski płynące z badania ewaluacyjnego CyberSecIdent

REKOMENDOWANE OBSZARY WSPARCIA

Dostępne wsparcie w przyszłości powinno w większym stopniu adresować cyberzagrożenia dotykające obywateli, przedsiębiorców – umożliwiać opracowanie narzędzi i zasad współpracy służb składających się na systemowe wsparcie obywatela w przypadku incydentu.

Potrzebne jest też stworzenie portalu, systemu, narzędzi, które będą **skupiały w jednym miejscu wszystkie najważniejsze dla obywatela informacje z zakresu cyberbezpieczeństwa –** w tym przedstawiały scenariusze/ścieżki pomocy dla osoby/podmiotu, która jej potrzebuje w związku z wystąpieniem cyberincydentu. Taki system jednocześnie może agregować i dostarczać zbiorczych statystyk decydentom.

Obecne wyzwania w obszarze cyberbezpieczeństwa mocno wiążą się z technikami dezinformacji. Działania wspierające rozwiązania z zakresu cyberbezpieczeństwa powinny być też nakierowane na opracowanie procedur i narzędzi dla obywateli do zgłaszania przypadków dezinformacji służbom.

Sygnalizuje się też potrzebę wsparcia dla rozwiązań pomagających pozyskiwać i motywować kandydatów na specjalistów z zakresu cyberbezpieczeństwa.

Zdecydowanie też powinno utrzymać się zakres zagadnień związanych z **koordynacją działań między różnymi domenami bezpieczeństwa cyberprzestrzeni** oraz z wdrażaniem metod i technik identyfikacji i uwierzytelniania.

KLUCZOWE WNIOSKI Z BADANIA

Poza Programem CyberSecIdent, identyfikuje się inne inicjatywy o zasięgu ogólnopolskim, realizowane przez NCBR oraz poza Centrum, które w różnym stopniu dotyczą obszaru cyberbezpieczeństwa. **Żaden z nich nie miał jednak takiego istotnego znaczenia jak CyberSecIdent,** wynikającego z umocowania , w zapisach Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

Rezultaty Programu wspierały wdrażanie nowych regulacji unijnych i krajowych związanych z cyberbezpieczeństwem. Co ważne, **Program dał możliwości tworzenia rodzimych rozwiązań z obszaru cyberbezpieczeństwa**, co wpływa na budowanie polskiej niezależności w tym zakresie.

Konstrukcja Programu w zakresie określonych obszarów tematycznych dla realizowanych projektów była trafna, nakreślona z zachowaniem odpowiedniej swobody poruszania się między różnymi zagadnieniami w ramach wskazanych dziedzin. Pozwalała na uwzględnienie szerokiego zakresu projektów, w ramach których pracowano nad różnymi rozwiązaniami branżowymi.

Skutecznej realizacji Programu sprzyjały elastyczne założenia dotyczące jego wdrażania, doświadczenie realizatorów projektów, dobra komunikacja między Beneficjentami a NCBR oraz świadomość o istotnej roli Programu w ramach poprawy cyberbezpieczeństwa kraju.

Do barier ewaluatorzy zaliczyli: dynamicznie przebiegające zmiany w branży informatycznej, negatywny wpływ pandemii COVID-19, **trudności w dotarciu do specjalistów z obszaru cyberbezpieczeństwa, niejasne zasady dotyczące praw autorskich do wypracowanych rozwiązań i problemy z ich komercjalizacją**

Obszary wymagające wsparcia – wnioski płynące z badania ewaluacyjnego

Obszar tematyczny	Dlaczego wymaga wsparcia? (uzasadnienie z raportu)
Wsparcie obywatela w sytuacji incydentu	Program CyberSecIdent (SCI) nie uwzględnia incydentów dotykających obywateli i przedsiębiorców. Obywatele są oszukiwani (phishing, ransomware), a nie wiedzą, gdzie zgłosić problem. Brakuje zintegrowanego systemu umożliwiającego szybkie i intuicyjne zgłoszenie cyberoszustwa oraz otrzymanie pomocy.
Portal/system informacji i pomocy dla obywateli (CyberSpace)	Brak zintegrowanego punktu dostępu do informacji o cyberbezpieczeństwie. Taki portal powinien pełnić funkcję centrum kompetencji oraz zawierać scenariusze postępowania w przypadku incydentów.
Dezinformacja, manipulacja, farmy trolli	Obszar niedostatecznie uwzględniony przez CSI, mimo że rośnie jego wpływ na destabilizację społeczną. Brakuje narzędzi do zgłaszania dezinformacji i jej analizy.
Kadry i kompetencje	Niedostateczne rozwiązani systemowe na rzecz pozyskiwania, motywowania i utrzymywania ekspertów. Należy opracować długofalową strategię rozwoju kadr, wspieraną przez mechanizmy kształcenia, stypendialne, certyfikacyjne i partnerskie.
Uwierzytelnianie i identyfikacja	Konieczne jest rozwijanie bezpiecznych, ale jednocześnie przyjaznych dla użytkownika metod uwierzytelniania, w tym mechanizmów wieloskładnikowych, biometrycznych oraz rozwiązań zgodnych z europejskim portfelem cyfrowym.
Nowe cyberzagrożenia (AI, LLM, DeepFake, spear phishing)	Spektrum zagrożeń się zmienia – aktualne technologie (np. WormGPT, vishing na deepfake głosowy) znacznie zwiększają efektywność ataków.

Obszary wymagające wsparcia – wnioski płynące z badania ewaluacyjnego

Obszar tematyczny	Dlaczego wymaga wsparcia? (uzasadnienie z raportu)
Big Data i automatyzacja cyberdetekcji	CSI nie wspierał rozwoju systemów automatyzujących wykrywanie i analizę zagrożeń (brak AI/ML/Big Data).
Wizja cyber-ekosystemu – narodowa odporność cyfrowa	Wskazana potrzeba podejścia systemowego – na wzór Izraela. Wymaga to rozwiązań wspierających kompetencje i innowacje, np. Hackathony, BugBounty.
Zgłaszanie incydentów (technicznie i instytucjonalnie)	Choć istnieje incydent.cert.pl, obywatele i MŚP nie wiedzą, jak zgłaszać incydenty. Brakuje „pierwszej linii wsparcia" techniczno-organizacyjnego.
Cyberbezpieczeństwo sektora usług publicznych i lokalnych JST	Niedostateczne przygotowanie gmin, urzędów i instytucji publicznych niższego szczebla do reagowania na cyberzagrożenia (np. brak zespołów IT, brak przeszkolenia pracowników, brak polityk bezpieczeństwa).
Dostępność i UX systemów cyberbezpieczeństwa	Podkreślono, że wiele narzędzi (w tym portale informacyjne) jest trudna w obsłudze, nieczytelna, a nawet niedostosowana do potrzeb osób starszych lub z niepełnosprawnościami.
Edukacja i włączenie cyfrowe obywateli	Niewystarczające działania adresowane do obywateli – szczególnie tych z grup wykluczonych cyfrowo. Obywatele nie mają świadomości, jak zgłaszać incydenty ani jak interpretować zagrożenia. Wspomniane są też bariery językowe i technologiczne (np. wiek, niepełnosprawność, brak kompetencji cyfrowych)
Koordynacja domen i tożsamość cyfrowa	Obszar nadal aktualny i zgodny z NIS2 i KSC. Istniejące rozwiązania należy utrzymać i synchronizować z aktualnymi zmianami regulacyjnymi.

Narodowe Centrum Badań i Rozwoju

Podsumowanie i rekomendacje dla NCBR

Podsumowanie

Wzmocnienie systemu funkcjonalnego dla krajowej polityki cyberbezpieczeństwa, które nastąpiło w ostatnich latach w Polsce – m.in. dzięki **wdrożeniu Krajowego Systemu Cyberbezpieczeństwa, stanowi solidną bazę dla wzmocnienia zdolności w zakresie cyberbezpieczeństwa Polski**, zwiększenia odporności i poprawy strategicznej współpracy między międzynarodowej w tym obszarze. **Kluczowe znaczenie ma jednak także zapewnienie dostępności finansowania badań, rozwoju innowacji dla krytycznych technologii i zastosowań** w celu dalszego wzmocnienia zdolności w zakresie cyberbezpieczeństwa kraju i obszaru Europy.

Jak wskazujemy w raporcie gros środków i wysiłku publicznego w ostatnich latach został położony na ten pierwszy aspekt – budowę stabilnego, skutecznego systemu bezpieczeństwa,. Ma to przełożenie w wysokiej ocenie Polski pod względem cyberbezpieczeństwa. **Brakuje jednak programów wsparcia publicznego ukierunkowanego na rozwój rozwiązań technologicznych i wykorzystanie najnowszych technologii, w tym AI i algorytmów post kwantowych**, co umożliwiłoby w większym stopniu możliwości tworzenia rodzimych rozwiązań z obszaru cyberbezpieczeństwa i budowanie polskiej niezależności w tym zakresie. Kluczowe jest łączenie zaawansowanych technologii (AI, ML, automatyzacja) z wykwalifikowaną kadrą i strategiami proaktywnymi, aby sprostać dynamicznie zmieniającym się zagrożeniom.

Równie ważne dla minimalizowania ryzyka jest **podnoszenie świadomości i wiedzy praktycznej na temat cyberbezpieczeństwa** i unikania zagrożeń wśród społeczeństwa, a w przypadku pracodawców wśród pracowników. Dotyczy to kwestii wydawałoby się dosyć oczywistych jak np. stosowania silnych haseł, aktualizowania oprogramowanie czy uwierzytelnia niania dwuskładnikowe. Są to działania służące budowie kultury odpowiedzialnego korzystania z zasobów cyfrowych.

Polskie przedsiębiorstwa **zaczynają zdawać sobie sprawę z zagrożeń** jakie niesie nieodpowiednie przechowywanie danych, implementowanie procesów czy projektowanie infrastruktury. W odpowiedzi na rosnące wyzwania z zakresu bezpieczeństwa cyfrowego **wzmacniają swoje podejście do ochrony systemów informatycznych, koncentrując się na budowie dedykowanych zespołów, wdrażaniu zaawansowanych narzędzi monitorowania zabezpieczeń** oraz formalizowaniu procedur reagowania na incydenty. Zdecydowanie częściej szkolą też swoich pracowników w tym zakresie.

Dodatkowym impulsem jest także **presja regulacyjna** wymuszająca na firmach dostosowanie się do coraz bardziej rygorystycznych przepisów dotyczących ochrony informacji – m.in. Dyrektywa NIS2, która rozszerza katalog branż uznanych za krytyczne dla funkcjonowania państwa i tym samym rozszerza liczbę podmiotów włączonych do KSC. NIS2 nakłada na przedsiębiorstwa szereg obowiązków, obejmujących m. zgłaszanie incydentów w odpowiednim czasie, przeprowadzanie oceny ryzyka cybernetycznego i wdrożenie zabezpieczeń czy szkolenie pracowników. Wszystko to sprawia, że w **ujęciu globalnym w Polsce poziom zaawansowania cyberbezpieczeństwa firm podnosi się, a tempo zmian i inwestycji będzie jedynie przyspieszać** , Tworzy to zatem rynek na produkty oraz usługi w zakresie a cyberbezpieczeństwa, które są w stanie wesprzeć bezpieczną transformację firm.

Zauważalne są jednak ogromne dysproporcje w poziomie zabezpieczeń przed cyberzagrożeniami w przedsiębiorstwach w Polsce w zależności od wielkości firm. Wynika to oczywiście z potencjału technologicznego podmiotów, ale także świadomości i posiadanych zasobów, w tym kadrowych**.** Jak wskazują prognozy, które przytaczamy w raporcie wszystkie sektory będą jednak wzmacniać swoje zdolności do zabezpieczenia.

Rekomendacje

Lp	OBSZAR	WNIOSEK	REKOMENDACJA
1	**zakres wsparcia publicznego**	Strategia Cyberbezpieczeństwa RP na lata 2019-2024 podkreśla konieczność zwiększenia nakładów na badania i rozwój w celu zwiększenia odporności na zagrożenia cybernetyczne oraz ochrony informacji w sektorach publicznym, wojskowym i prywatnym. W Polsce pomimo, że stan cyberbezpieczeństwa jest oceniany jako wysoce skuteczny, nadal niedostatecznie oceniany jest poziom nakładów na działalność B+R na wypracowanie krajowych rozwiązań. W obecnej perspektywie większość środków publicznych skierowana będzie na wzmocnienie systemu KSC, w mniejszym stopniu na samą technologię. Potwierdzeniem jest także ewaluacja programu NCBR CyberSecIdnt, w której podkreślono, że konstrukcja programu była unikalna i wypełniała lukę finasowania B+R w zakresie cyberbezpieczeństwa.	Kontynuacja programu ukierunkowanego na wzmacnianie cyberbezpieczeństwa. Kluczowe jest włączenie, na etapie definiowana do przyszłego zakresu programu instytucji istotnych z punktu widzenia KSC, m.in. takich jak: Minister ds. cyfryzacji, Minister ds. obrony, Minister ds. spraw wewnętrznych, tak aby zachować spójność i komplementarność z działaniami nadzorowanymi i koordynowanymi w tych instytucjach.
2	**zakres wsparcia publicznego**	Wyniki badań w Polsce i Europie (m.in. Agencji ENISA) wskazują na niedostateczny poziom zabezpieczeń obszarów krytycznych dla sprawnego funkcjonowania Państwa związanych z funkcjonowaniem infrastruktury sieciowej i transportowej (sektor morski, przestrzeń kosmiczna, sektor kolejowy) i sieciowo - przesyłowej (gaz) oraz opieki zdrowotnej.	Włączenie tematyki cyberzabepieczenia infrastruktury sieciowej i transportowej w zakres programów wsparcia NCBR w porozumieniu z operatorami i instytucjami zarządzającymi danym typem infrastruktury w państwie, jako: a. element zdefiniowania agendy badawczej w programie ukierunkowanym na wzmocnienie cyberbezpieczeństwa b. temat zamawiany w programach realizowanych obecnie przez NCBR –m.in. Gospostrateg, Infostrateg
3	**zakres wsparcia publicznego**	Dotychczasowe wsparcie w przeważającej mierze koncentrowało się na kwestii rozwoju systemu cyberbezpieczeństwa, co oczywiście stanowi niezbędną podstawę dla skutecznej ochrony państwa i jego obywateli. Potrzebne jest też wzmocnienie działań nakierowanych bezpośrednio na zachowania obywateli w obliczu zagrożeń lub zachowania w sytuacji obcowania ze skutkami przestępstw (dezinformacja, fałszerstwa, etc.). Taki system jednocześnie może agregować i dostarczać zbiorczych statystyk decydentom.	Dostępne wsparcie w przyszłości powinno w większym stopniu adresować cyberzagrożenia dotykające obywateli, przedsiębiorców – przede wszystkim skupienie w jednym miejscu najważniejszych informacji i procedur oraz narzędzi dla obywatela m.in. scenariusze/ścieżki pomocy dla osoby/podmiotu, która jej potrzebuje w związku z wystąpieniem cyberincydentu

Rekomendacje

Lp	OBSZAR	WNIOSEK	REKOMENDACJA
4	**technologie**	Cyberbezpieczeństwo w dobie szybko rozwijającej i zmieniającej się technologii- szczególnie sztucznej inteligencji - wymaga stałego inwestowania i nowych narzędzi. Ciągły wyścig między zabezpieczeniami a zagrożeniami przejawia się we wzrastających budżetach na obszar cyberbezpieczeństwa w firmach. Tendencja ta na pewno będzie w kolejnych latach utrzymywać się, a rozwój AI i technologii kwantowych tylko wymusi proces ciągłego dostosowywanie zabezpieczeń do zagrożeń wywołanych nowymi technologiami. Kluczowe jest zatem proaktywne podejście do tematu cyberbezpieczeństwa i finasowanie innowacyjnych rozwiązań przyszłości w celu zapewnienia bezpieczeństwa użytkowania nowoczesnych technologii. Współcześnie strach przed zagrożeniami hamuje wdrażanie rozwiązań AI w firmach	Na obecnym etapie rozwoju technologii jako dwa kluczowe wyzwania wymagające ciągłego doskonalenia nowych rozwiązań technologicznych mających zapewnić cyberbezpieczeństwa w szeroko rozumianej strefie publicznej i prywatnej definiowane są a. rozwiązania AI , Big data na rzecz cyberbezpieczeństwa b. rozwiązania kryptograficzne zapewniające kwantoodporne algorytmy szyfrowania danych
5	**mechanizm wsparcia/ programowanie**	Podniesienie poziomu cyberbezpieczeństwa jest zadaniem złożonym i wymagającym odpowiedniej strategii już na etapie formowania nowego rozwiązania lub produktu. Często dla opracowania nowej technologii, lub późniejszego jej pełnego wykorzystania niezbędne są zadania w zakresie pozyskiwania i przetwarzana różnego rodzaju danych. Umożliwione finasowania technologii cyberzabezpieczających w takim przypadku- na etapie opracowania rozwiązania - zwiększałoby użyteczność i bezpieczeństwo rezultatów projektów wspieranych przez NCBR	1. Powiązanie (włączenie do kosztów kwalifikowanych) - w programach NCBR - budżetów projektów z wymogami dotyczącymi zapewnienia cyberzabezpieczeń nowych technologii. W szczególności, gdy w toku realizacji projektu i użytkowania wypracowanych rozwiązań (technologii/produktów) konieczne będzie gromadzenie i przetwarzanie danych.
6	**mechanizm wsparcia/ programowanie**	j.w.	2. Wprowadzenie, w dokumentacji konkursowej, wymogu przygotowania kompleksowych rozwiązań łączących procedury, analizę ryzyka i narzędzia zapewniające cyberbezpieczeństwa dla wypracowanych rozwiązań
7	**kadry B+R**	W wyniku coraz bardziej skomplikowanych ataków, skuteczna ochrona działania organizacji wymaga coraz większych nakładów i specjalistów. Wyzwaniem dla skutecznej ochrony przez cyberzagrozeniami pozostaje fakt niedoborów specjalistów ds. cyberbezpieczeństwa w firmach. Na ten problem wskazuje około 80% firm w Polsce w badaniu zrealizowanym w 2025 -Cisco Cybersecurity Readiness Index 2025) https://mikrokontroler.pl/wp-content/uploads/2025/05/2025_Cisco_Cybersecurity_Readiness_Index_PL.pdf	Włączenie do kluczowych kierunków wsparcia szkolnictwa wyższego na poziomie II i III obszaru cyberbezpieczeństwa - przede wszystkim tworzenia nowych / modyfikowania programów studiów doktoranckich, co zapewniłoby ustrukturyzowane i trwałe warunki dla rozwijania kadry naukowców pracujących na rzecz sektora.

NCBR
Narodowe Centrum Badań i Rozwoju

ANEKS 1: Źródła danych

Bibliografia

Bazy danych

Dealroom.co: https://dealroom.co/guides/space-tech-europe

ESA BIC: https://esabic.pl/

Espacenet: https://worldwide.espacenet.com/

Eurostat: https://ec.europa.eu/eurostat

OECD: https://data-explorer.oecd.org/

Space Capital: https://www.spacecapital.com/

Web of Science: https://www.webofscience.com/

Dokumenty

Polska

NIK (2019) Kontrola Najwyższej Izby Kontroli „Rozwój sektora kosmicznego”, KGP.430.017.2019 Nr ewid. 44/2020/P/19/021/KGP

NIK (2024) Kontrola Najwyższej Izby Kontroli „Sektor kosmiczny i jego rozwój”, KGP.430.10.2023 Nr ewid. 120/2023/P/23/012/KGP

Ustawa z dnia 26 września 2014 r. o Polskiej Agencji Kosmicznej (Dz.U. 2014 poz. 1533)

SOR (2017) Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) (Uchwała nr 8 Rady Ministrów z dnia 14 lutego 2017 r. w sprawie przyjęcia SOR, M.P. 2017 poz. 260)

SP2030 (2022) Strategia Produktywności 2030 (Uchwała nr 154 Rady Ministrów z dnia 12 lipca 2022 r., M.P. 2022 poz. 926, przygotowana przez Ministerstwo Rozwoju i Technologii)

PSK (2017) Polska Strategia Kosmiczna (Uchwała nr 6 Rady Ministrów z dnia 26 stycznia 2017 r., M.P. 2017 poz. 203, przygotowana przez ówczesne Ministerstwo Rozwoju (dziś Rozwoju i Technologii))

POLSA (2024) Ewaluacja Polskiej Strategii Kosmicznej, Warszawa, luty 2024

Projekt Ustawy o działalności kosmicznej (Projekt z dnia 12 maja 2025 r., przygotowany przez Ministerstwo Finansów i Gospodarki - https://www.gov.pl/web/premier/projekt-ustawy-o-dzialalnosci-kosmicznej [data dostępu: 1.12.2025])

Zarządzenie Ministra Rozwoju nr 9 z dnia 29 czerwca 2020 r. w sprawie powołania Zespołu do spraw Polityki Kosmicznej (Dz. Urz. Min. Roz. poz. 13)

Unia Europejska

Konkluzje Rady UE dot. szeroko pojętej tematyki technologii kosmicznych:

- konkluzje o roli usług kosmicznych w zapewnianiu zrównoważonego charakteru regionowi Arktyki (2019)
- konkluzje wskazujące rolę polityki kosmicznej w zrównoważonym rozwoju (2020) – szczególny nacisk położono na wkład przestrzeni kosmicznej w długoterminowy zrównoważony wzrost oraz kształcenie i umiejętności odnoszące się do przestrzeni kosmicznej
- konkluzje dotyczące europejskiego wkładu w ustanawianie głównych zasad globalnej gospodarki kosmicznej (w ramach przygotowań do 10. posiedzenia Rady ds. Przestrzeni Kosmicznej z udziałem ESA) (2020)
- konkluzje dotyczące wspierania ludności zamieszkującej obszary przybrzeżne za pomocą technologii kosmicznych (2021)
- konkluzje, w których mowa o potrzebie europejskiego podejścia do New Space (2021)
- konkluzje pt. „Przestrzeń kosmiczna dla wszystkich” (2021)
- konkluzje w sprawie zarządzania ruchem w przestrzeni kosmicznej i programu Copernicus (2022)
- konkluzje w sprawie sprawiedliwego i zrównoważonego wykorzystywania przestrzeni kosmicznej (2023)
- konkluzje w sprawie pierwszej strategii kosmicznej UE na rzecz bezpieczeństwa i obrony (2023)

Unijny Program bezpiecznej łączności na lata 2023–2027 (Rozporządzenie (UE) 2023/588)

Strategia kosmiczna UE na rzecz bezpieczeństwa i obrony (JOIN(2023)9)

Źródła danych

2024 Report on the State of the Cybersecurity in the Union; ENISA ; 2024 - https://enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf

Barometr cyberbezpieczeństwa z 2025r; KPMG, 2025 - https://kpmg.com/pl/pl/home/insights/2025/02/barometr-cyberbezpieczenstwa-2025.html

Cisco Cybersecurity Readiness Index 2025; CISCO - https://mikrokontroler.pl/wpcontent/uploads/2025/05/2025_Cisco_Cybersecurity_Readiness_Index_PL.pdf

https://brandsit.pl/cyberparadoks-dlaczego-mimo-miliardow-na-cyberbezpieczenstwo-firmy-sa-coraz-bardziej-narazone; 25_05_2025

ENISA NIS360 2024 Cybersecurity Maturity & Criticality Assessment of NIS2 sectors, ENISA; 2025 - https://enisa.europa.eu/news/enisa-nis360-2024-report

Ewaluacja on going programu CyberSecident “Cyberbezpieczeństwo i e-Tożsamość” ; 2023; NCBR - https://www.gov.pl/web/ncbr/zrealizowane

Fundusze.gov.pl

Jak polskie firmy wdrażają AI? Analiza zmian rok do roku Edycja 2”, EY, 2024

Mordor Intelligence, Statista, Fortune Business Insights, Netscout, Gartner, MarketsandMarkets, IDC, PwC, Global Cyber Insurance Market Report, MarketsandMarkets 2023

Narodowy Indeks Bezpieczeństwa Cybernetycznego; Eestońska Akademię e-Governance ; 2024- https://ncsi.ega.ee/ncsi-index/

PFR Polish VC market Outlook 2024; PFR - https://pfrventures.pl/en/artykul/polish-vc-market-outlook-2024

Rynek cyberbezpieczeństwa w Polsce; PMR Market Experts, 2025 - https://mypmr.pro/products/rynek-cyberbezpieczenstwa-w-polsce?gad_source=1&gad_campaignid=22374640981&gbraid=0AAAAAotP9yKtHNcOue8ZLMOLJEf95bt&gclid=EAIaIQobChMI8NrFyJKZjgMV7hiiAx0lzS0_EAAYASAAEgJcRvD_BwE

Społeczeństwo informacyjne w Polsce w 2024 r. GUS - https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2024-roku,1,18.html

Sprawozdanie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa za 2023 rok - https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie

Strategia Bezpieczeństwa Narodowego RP - https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 - https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024

Transakcje na polskim rynku VC 2024; Transakcje na polskim rynku VC 2024 Ventures; 2025 - https://pfrventures.pl/document/2210

NCBR
Narodowe Centrum Badań i Rozwoju

Aneks 2: Metodologia

Dane patentowe

Do analizy wykorzystano bazę Escpacenet Europejskiego Urzędu Patentowego (EPO). Wykorzystano w niej klaryfikację patentową CPC (Cooprative Patent Classification), wspólna system klasyfikacji EPO i Urzędu Patentowego Stanów Zjednoczonych (USPTO).

- korzystano z następujących kodów klasyfikacji: grupa G06F21 - Układy zabezpieczające do ochrony komputerów lub systemów komputerowych przed działaniami nieupoważnionymi, H04L63 - architektura sieci lub protokoły komunikacji sieciowej dla bezpieczeństwa sieci.

- Przy wyszukiwaniu cyberzagrożeń korzystano z wyszukiwania we wszystkich polach tekstowych po następujących frazach: DDoS (Distributed-Denial-of-Service), DoS (Denial of Service), Phishing, Malware, Ransomware, Social engineering, IP spoofing, eavesdropping-attack, replay-attack, cross-site-scripting, deepfake, critical infrastructure, SQL-injection, insider-threat, password attack, DNS-attack, session-hijacking, advanced-persistent-threat, rootkit, drive-by download, spyware, cryptojacking, trojan, Privilege escalation

Analiza bibliometryczna

W analizie prac naukowych korzystano z jednej z dwóch największych baz tekstów naukowych Web of Science.

- Prace naukowe wyszukiwano w kategorii tematycznej "4.187 Security Systems„, uwzględniaono następujące rodzaje prac naukowych: proceeding paper, artykuł naukowy, rozdział w książce, early access.

- Przy wyszukiwaniu cyberzagrożeń korzystano z wyszukiwania po słowach kluczowych wraz z frazami powiązanymi: DDoS (Distributed-Denial-of-Service), DoS (Denial of Service), Phishing, Malware, Ransomware, Social engineering, IP spoofing, eavesdropping-attack, replay-attack, cross-site-scripting, deepfake, critical infrastructure, SQL-injection, insider-threat, password attack, DNS-attack, session-hijacking, advanced-persistent-threat, rootkit, drive-by download, spyware, cryptojacking, trojan, Privilege escalation

Analiza danych NCBR

Wewnętrzne bazy projektowe NCBR, m.in. Superbaza NCBR