KPMG

# Cyberodporność w erze zmian

## Barometr cyberbezpieczeństwa

Marzec 2026 | kpmg.pl

# Wstęp

**Szanowni Państwo,**

Z przyjemnością przedstawiam dziewiątą edycję raportu „Barometr cyberbezpieczeństwa". Od lat towarzyszy nam wspólny cel – budowanie świadomości i wspieranie organizacji działających w Polsce w skutecznym zarządzaniu bezpieczeństwem cyfrowym w obliczu nieustannie ewoluujących zagrożeń. Mam nadzieję, że wnioski z tegorocznego badania staną się cennym źródłem wiedzy i impulsem do dalszego wzmacniania cyberodporności Państwa firm.

Rok 2025 zapisał się jako przełomowy pod względem skali cyberzagrożeń. Po raz pierwszy w historii badania aż 96% organizacji odnotowało przynajmniej jeden incydent bezpieczeństwa, a w połowie firm wzrosła liczba prób ataków. Cyberzagrożenia przestały być problemem przyszłości – stały się codziennością wymagającą systemowego, strategicznego podejścia.

Jednocześnie obserwujemy pozytywne przemiany. Dwukrotnie wzrosła liczba firm z dedykowaną rolą CISO, co świadczy o rosnącej profesjonalizacji zarządzania bezpieczeństwem. Coraz więcej organizacji odchodzi od reaktywnego modelu obrony, budując kompleksową cyberodporność opartą na monitoringu, szybkim reagowaniu oraz planach ciągłości działania. Szczególnie istotne w obecnym kontekście geopolitycznym staje się zarządzanie bezpieczeństwem łańcuchów dostaw oraz przygotowanie na scenariusze zakłóceń infrastruktury krytycznej.

Wdrożenie dyrektywy NIS2 oraz postępująca implementacja Rozporządzenia AI Act stawiają przed firmami nowe wyzwania, ale także tworzą szansę na uporządkowanie i wzmocnienie fundamentów cyberbezpieczeństwa. Jak pokazują wyniki badania, największą barierą nie jest już brak budżetu czy technologii, lecz niewystarczające wsparcie najwyższego kierownictwa i zaangażowanie biznesu. To wyraźny sygnał, że cyberbezpieczeństwo musi przestać być domeną wyłącznie działów IT i stać się strategicznym priorytetem całej organizacji.

Życząc Państwu wartościowej lektury, zachęcam do wykorzystania przedstawionych wniosków jako punktu wyjścia do refleksji nad stanem cyberodporności Państwa organizacji. Szczególnie zależy mi na podkreśleniu potrzeby dialogu między liderami biznesu a specjalistami ds. cyberbezpieczeństwa – tylko taka współpraca zapewni skuteczną ochronę w dynamicznie zmieniającym się środowisku zagrożeń. Niech ten raport stanie się narzędziem wspierającym tę niezbędną rozmowę.

Z poważaniem


**Michał Kurek**

Partner, Advisory
Szef Zespołu Cyberbezpieczeństwa
w KPMG w Polsce i Europie
Środkowo-Wschodniej

# Najważniejsze spostrzeżenia z raportu

## Rośnie liczba i częstotliwość prób cyberataków i incydentów bezpieczeństwa

- W prawie połowie firm wzrosła lub znacząco **wzrosła liczba prób ataków** na bezpieczeństwo cyfrowe (2024 – 42%; **2025 – 49%**).
- W 2025 roku aż **96% firm doświadczyło** przynajmniej jednego **incydentu bezpieczeństwa** – jest to wzrost o 13 p.p. r/r i rekordowy odczyt w dziewięcioletniej historii „Barometru cyberbezpieczeństwa".
- Zwiększyła się też liczba firm doświadczających **wielokrotnych naruszeń bezpieczeństwa** – szczególnie tych, które odnotowały od czterech do dziewięciu incydentów (+20 p.p. r/r).

## Cyberzagrożenia z perspektywy firm

- Aż 46% badanych za największe zagrożenie dla firm uznało **hakerów działających w pojedynkę**, na drugiej pozycji znaleźli się **cyberterroryści** (35%).
- Rośnie znaczenie **haktywizmu** – blisko jedna czwarta respondentów postrzega ataki motywowane ideologicznie lub politycznie jako realne zagrożenie.
- Kradzież danych poprzez **phishing** zajęła pierwsze miejsce w katalogu ryzyk cyfrowych. Drugim najistotniejszym zagrożeniem są ataki wykorzystujące **błędy w aplikacjach**.

## Odpowiedzialność za cyberbezpieczeństwo jest coraz bardziej wyspecjalizowana

- W organizacjach coraz częściej funkcjonuje **rola CISO** (2024 – 13%; **2025 – 26**%).
- Choć za cyberbezpieczeństwo nadal najczęściej odpowiada CIO lub inny pracownik IT, odsetek takich wskazań z roku na rok spada (2023 – 47%; 2024 – 41%; **2025 – 36**%).
- Jedynie **2% firm** nie ma przypisanej odpowiedzialności za zarządzanie cyberbezpieczeństwem, a rola CEO w tym zakresie spada.

## Najbardziej dojrzałe obszary zabezpieczeń

1. Reagowanie na incydenty bezpieczeństwa
2. Bezpieczeństwo styku z siecią Internet
3. Monitorowanie bezpieczeństwa

Respondenci ocenili dojrzałość **niżej niż rok wcześniej w 11 z 14 analizowanych kategorii**. Jedynym obszarem, który uległ bezwzględnej poprawie, okazało się **zarządzanie tożsamością i dostępem**.

## Outsourcing jest stosowany szeroko, ale selektywnie

- Aż **94% organizacji** deleguje na zewnątrz co najmniej jedną funkcję cyberbezpieczeństwa (wzrost o 13 p.p. r/r).
- Większość firm (51%) zleca dostawcom wyłącznie jedną wybraną funkcję.
- Najczęściej realizowanym zewnętrznie procesem pozostaje **monitorowanie bezpieczeństwa** (41%).
- Niski poziom zlecania na zewnątrz testów podatności infrastruktury (13%) oraz działań o charakterze edukacyjnym (10%) sugeruje, że organizacje traktują je jako element budowy długofalowych kompetencji wewnętrznych.

## Najbardziej dofinansowane obszary cyberbezpieczeństwa w 2026 roku

1. Ochrona przed złośliwym oprogramowaniem
2. Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa
3. Bezpieczeństwo sieci wewnętrznej

W sześciu z 14 kategorii wartość inwestycji pozostanie na podobnym poziomie jak w ubiegłym roku, w pięciu – obniży się, a **jedynie w trzech wzrośnie**.

## Główne wyzwania w zakresie cyberbezpieczeństwa dotyczą talentów i współpracy z osobami decyzyjnymi

- Najważniejsze wyzwanie to **brak wsparcia ze strony najwyższego kierownictwa**, które przesunęło się z trzeciego miejsca w 2024 roku na pierwsze w 2025 (kluczowe dla **29% firm**).
- Następne w kolejności uplasowały się ex aequo: trudności w rekrutacji i retencji pracowników oraz brak zaangażowania biznesu (26% firm).
- Zarządzający cyberbezpieczeństwem wskazywali mniej istotnych barier niż w ubiegłej edycji.
- Wyniki sugerują przesunięcie postrzegania cyberbezpieczeństwa z obszaru techniczno-operacyjnego w stronę **zagadnienia o charakterze strategicznym i organizacyjnym**, wymagającego wkładu i współodpowiedzialności biznesu.

# Firmy kontrolują swoją cyberodporność

- Jedna trzecia firm ocenia swój poziom cyberodporności jako adekwatny do aktualnego przekroju cyberzagrożeń.
- 58% organizacji wskazuje na potrzebę usprawnień w wybranych obszarach zabezpieczeń cyfrowych, co świadczy o świadomości istniejących luk i zmiennego charakteru ryzyk.
- Co czwarta badana firma przeprowadziła audyt cyberodporności w ciągu ostatniego roku, a kolejne 23% deklaruje, że jest on w toku.
- Znacząca większość badanych firm (95%) stosuje mechanizmy monitorowania i testowania cyberodporności, a najczęściej wybieranym rozwiązaniem są regularne testy penetracyjne (36%).

# Najpopularniejsze formy zarządzania ciągłością działania w firmach

1. **Lista procesów krytycznych** aktualizowana na bieżąco – posiada ją 38% firm
2. **Rejestr zasobów** wspierających procesy krytyczne – prowadzi go 29% badanych organizacji
3. **Analiza ryzyka** obejmująca wszystkie zasoby istotne z perspektywy ciągłości działania – wykonuje ją 27% firm

# Mechanizmy zapewniania cyberodporności to przede wszystkim rozwiązania organizacyjne i procesowe

- Najpopularniejszym rozwiązaniem poprawiającym cyberodporność w firmach są programy zarządzania **bezpieczeństwem łańcucha dostaw** wraz z audytami dostawców (**46%**).
- 35% firm przygotowuje **kompleksowe plany zapewnienia ciągłości działania** – BCP, a 30% przeprowadza regularne **analizy ryzyka** w obszarze cyberbezpieczeństwa i ciągłości działania.

Jedynie co dziesiąta firma wdraża **systemy zarządzania kontami uprzywilejowanymi** (PAM), a zaledwie 9% badanych stosuje **mikrosegmentację sieci**, pełną architekturę **Zero Trust**, czy tzw. **cyberbunkier**.

# Najczęściej uwzględniane scenariusze w analizach ryzyka prowadzonych w ramach zarządzania ciągłością działania

1. Utrata kluczowego dostawcy **usług chmurowych** (37%)
2. Długotrwały brak **energii elektrycznej** (36%)
3. Długotrwały brak dostępu do **sieci Internet** (29%)

# 1 Przekrój cyberzagrożeń

Według danych Eurostatu w 2024 roku Polska znajdowała się na drugim miejscu w Unii Europejskiej pod względem liczby cyberataków na przedsiębiorstwa[1]. Jednocześnie nasila się zagrożenie w sektorze publicznym – dynamicznie wzrasta liczba ataków na instytucje rządowe, finansowe oraz sektor energetyczny i użyteczności publicznej, co wynika z geopolitycznego położenia Polski. Według raportu Check Point Research w pierwszym tygodniu 2026 roku odnotowano blisko 3,2 tys. prób ataków na krajowe instytucje rządowe, co stanowi najwyższy wynik wśród krajów europejskich[2]. W odpowiedzi na rosnące zagrożenia cyfrowe Polska wzmacnia mechanizmy ochrony. Sejm RP w styczniu 2026 roku uchwalił nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa, wdrażającą unijną dyrektywę NIS2, która ma zwiększyć poziom bezpieczeństwa usług i systemów wykorzystywanych publicznie, prywatnie i komercyjnie[3].

Nasilający się problem cyberataków potwierdzają wyniki badania KPMG – w 2025 roku prawie w połowie firm odnotowano wzrost ataków na bezpieczeństwo cyfrowe, a przynajmniej jednego incydentu doświadczyło rekordowe 96% organizacji. Jednocześnie wśród zagrożeń umacnia się pozycja hakerów działających w pojedynkę, a za największe ryzyko przedsiębiorcy uznają kradzież danych poprzez phishing. Cyberzagrożenia stały się trwałym elementem otoczenia biznesowego, a analiza najczęściej występujących typów zagrożeń oraz dynamiki incydentów stanowi istotne narzędzie prewencji i budowania cyberodporności.

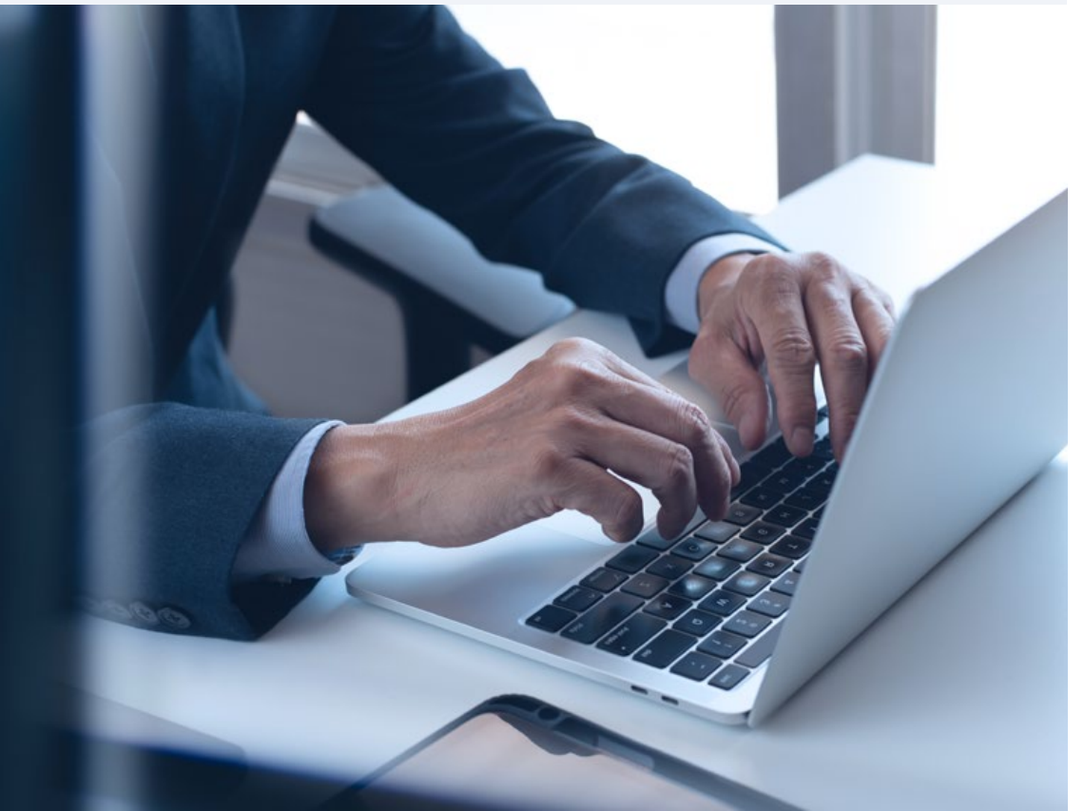
[1] Eurostat, "Security incidents and consequences by size class of enterprise", 2025, [data dostępu: 02.02.2026].

[2] Business Insider, „Cyberataki na polski rząd biją rekordy. Eksperci ostrzegają", 14.01.2026, [data dostępu: 02.02.2026].

[3] Serwis Rzeczpospolitej Polskiej, „Sejm uchwalił nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa", 26.01.2026, [data dostępu: 02.02.2026].

# Narastające zagrożenie cyberatakami

Zgodnie z wynikami tegorocznego badania w prawie połowie firm (49%) w 2025 roku wzrosła lub znacząco wzrosła liczba prób ataków na bezpieczeństwo cyfrowe – to o 7 p.p. więcej niż rok wcześniej. W 44% organizacji liczba prób pozostaje na zbliżonym poziomie (spadek o 2 p.p.), a tylko 7% odnotowało zmniejszenie aktywności atakujących (spadek o 5 p.p.). Co istotne, tendencja ta jest niezależna od wielkości przedsiębiorstwa – wyniki kształtują się podobnie w małych, średnich i dużych firmach.



**Zmiana liczby zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem**


Źródło: KPMG w Polsce na podstawie badania ankietowego.

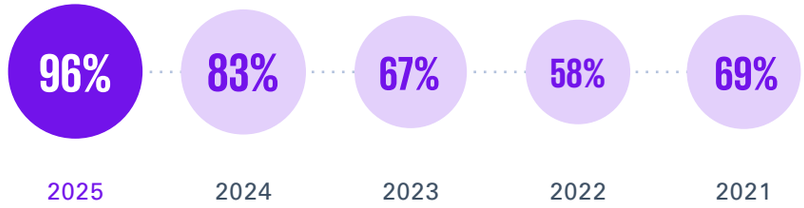
# W 2025 roku rekordowe 96% firm doświadczyło przynajmniej jednego incydentu bezpieczeństwa (wzrost o 13 p.p. r/r).

Od 2022 roku sukcesywnie rośnie liczba firm, które odnotowują co najmniej jeden incydent naruszający ich bezpieczeństwo cyfrowe. Uwzględniając wyniki wszystkich dziewięciu edycji „Barometru", w 2025 roku rekordowa liczba organizacji zarejestrowała co najmniej jedno niebezpieczne zdarzenie (96%). Oznacza to wzrost odsetka tej grupy o 13 p.p. względem zeszłorocznego badania.

Warto zwrócić uwagę na zwiększającą się częstotliwość cyberataków – zgodnie z deklaracjami respondentów w 2025 roku, w porównaniu z poprzednim, poszerzyło się grono firm, które doświadczyły co najmniej kilku naruszeń bezpieczeństwa cyfrowego w ciągu 12 miesięcy. Wyraźnie wzrósł odsetek organizacji, które odnotowały od czterech do dziewięciu incydentów (wzrost o 20 p.p. r/r). Wzrósł też odsetek firm najczęściej dotkniętych incydentami – od 10 do 29 razy oraz ponad 30 razy (wzrosty o odpowiednio 9 p.p. i 4 p.p.).

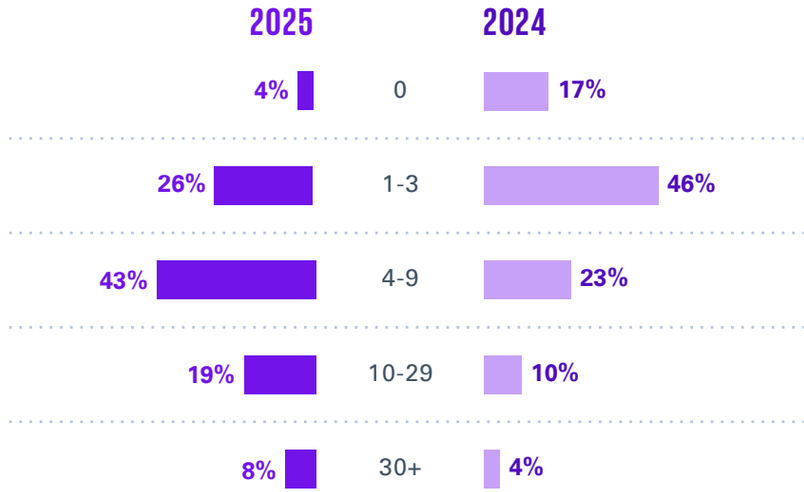
Im większe przedsiębiorstwo, tym większa częstotliwość niebezpiecznych zdarzeń. W 2025 roku 40% małych firm odnotowało maksymalnie trzy incydenty, podczas gdy 56% średnich i 35% dużych – od czterech do dziewięciu, a kolejne 35% dużych podmiotów – od 10 do 29. Wyniki badania wskazują więc na zwiększenie skali zagrożeń – zarówno pod względem zasięgu, jak i częstotliwości, która rośnie proporcjonalnie do wielkości organizacji.

**Odsetek przedsiębiorstw, które zarejestrowały co najmniej jeden incydent bezpieczeństwa**




Źródło: KPMG w Polsce na podstawie badania ankietowego.

**Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa**




Źródło: KPMG w Polsce na podstawie badania ankietowego.

*Rekordowy odsetek firm dotkniętych incydentami bezpieczeństwa nie jest przypadkowy. Wchodzimy w erę, w której sztuczna inteligencja fundamentalnie zmienia charakter cyberataków. Obserwujemy już kampanie phishingowe wykorzystujące modele językowe do generowania spersonalizowanych, bezbłędnych językowo wiadomości, które omijają tradycyjne filtry. Deepfake audio i wideo umożliwiają coraz bardziej przekonujące ataki socjotechniczne, a automatyzacja pozwala przestępcom przeprowadzać jednocześnie tysiące ukierunkowanych ataków.*

*W najbliższych latach złożoność ataków będzie rosła wykładniczo – AI nauczy się identyfikować podatności szybciej niż zespoły bezpieczeństwa zdążą je łatać, a ataki staną się bardziej adaptacyjne i inteligentne. Kluczowe pytanie brzmi: czy organizacje zdążą zbudować cyberodporność w tempie dorównującym ewolucji zagrożeń?"*


**Michał Kurek**

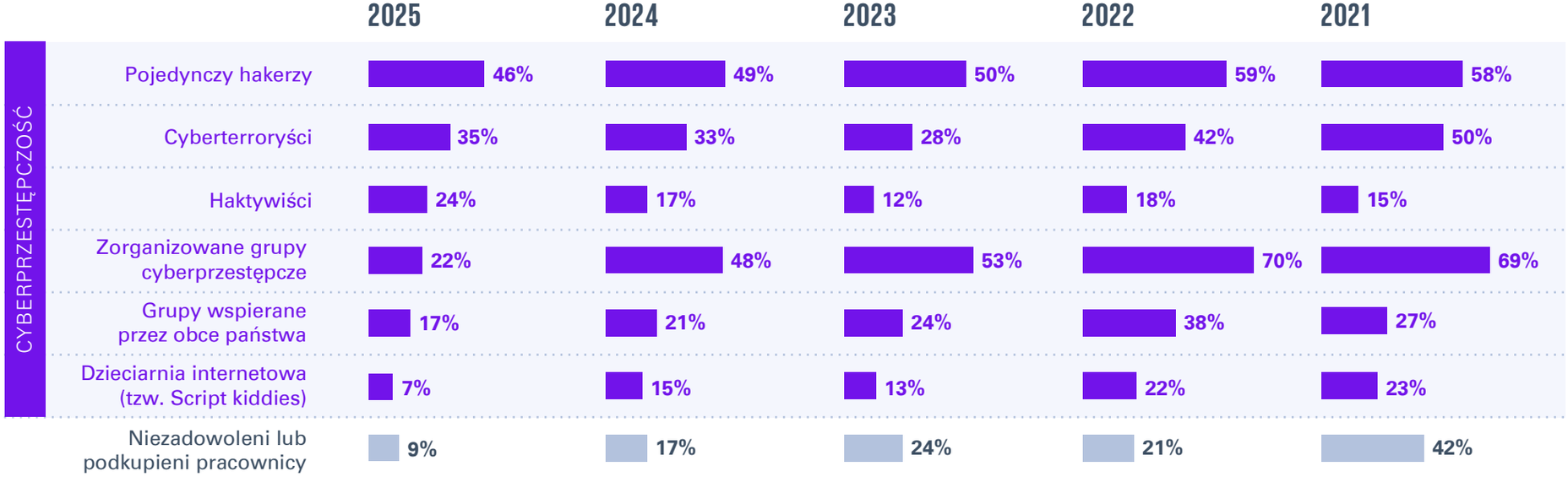
Partner, Advisory
Szef Zespołu
Cyberbezpieczeństwa
w KPMG w Polsce i Europie
Środkowo-Wschodniej

# Różne oblicza cyberprzestępczości

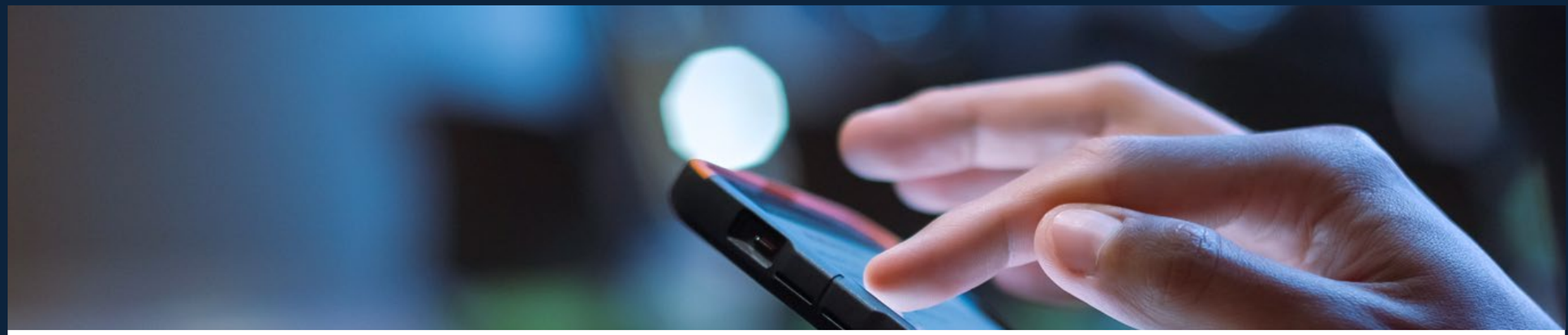
Z perspektywy przedsiębiorców w 2025 roku, spośród grup i osób mogących naruszyć bezpieczeństwo firm, największym zagrożeniem byli hakerzy działający w pojedynkę. Ich ataki wskazało aż 46% respondentów i choć oznacza to niewielki spadek – o 3 p.p. w stosunku do poprzedniego roku – przewaga tego typu zagrożeń nad innymi wyraźnie się umocniła. Drugim najważniejszym zagrożeniem z odsetkiem 35% odpowiedzi stały się działania cyberterrorystów. W konsekwencji nastąpiło przetasowanie i wyraźne zmniejszenie znaczenia zorganizowanych grup cyberprzestępczych, które jeszcze do 2023 roku były postrzegane jako najbardziej zagrażające, a w ubiegłorocznej edycji „Barometru" wskazywane przez prawie połowę badanych firm.

Nasilają się obawy przed atakami haktywistów, którzy jako realne zagrożenie są odbierani przez blisko jedną czwartą respondentów. Oznacza to, że aktywność cyberprzestępcza osób kierujących się ideami społecznymi czy politycznymi staje się coraz bardziej dotkliwa. Z drugiej strony poczucie zagrożenia ze strony grup wspieranych przez obce państwa – relatywnie wysokie tuż po wybuchu wojny w Ukrainie – ponownie zmalało; wskazało na nie jedynie 17% badanych. Najmniejszym zagrożeniem w opinii przedsiębiorców są sukcesywnie tracące na znaczeniu amatorskie działania tzw. dzieciarni internetowej. Choć cyberataki, za którymi stoją skonfliktowani z firmą lub podkupieni pracownicy, za realne zagrożenie uznało jedynie 9% badanych, to problem ten nie jest niezauważany – ci sami respondenci wskazali kradzież danych przez pracowników jako jedno z większych ryzyk dla swoich organizacji.

**Grupy stanowiące realne zagrożenie dla organizacji**




Źródło: KPMG w Polsce na podstawie badania ankietowego.



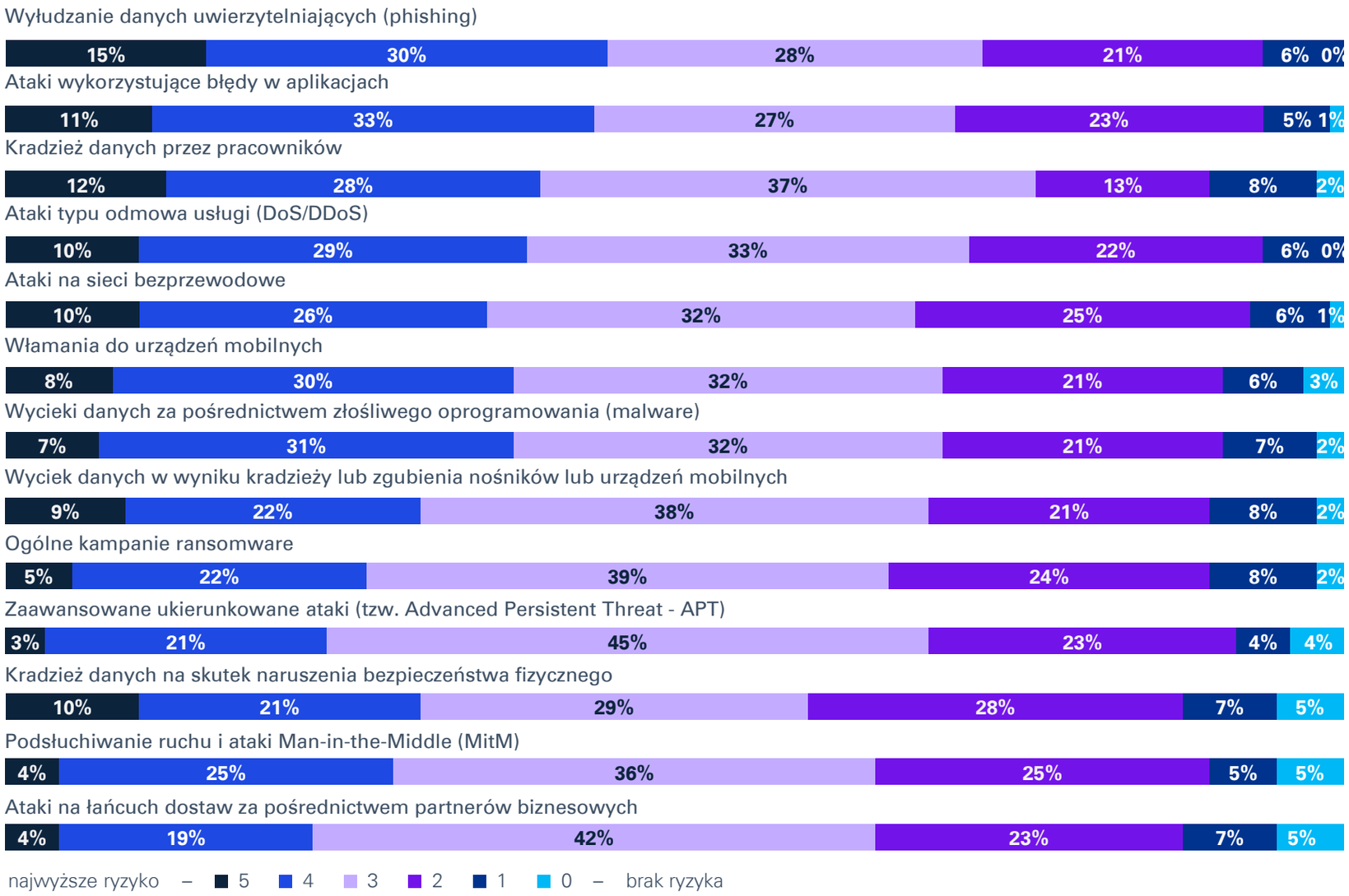
# Najbardziej dotkliwe cyberzagrożenia

Rokrocznie dochodzi do przetasowania w rankingu najważniejszych cyberzagrożeń identyfikowanych przez przedsiębiorców. W bieżącej edycji badania na pierwsze miejsce powrócił phishing – rok wcześniej jednorazowo wyprzedzony przez wycieki danych za pośrednictwem złośliwego oprogramowania, które obecnie zostały ocenione jako ryzyko o nieco mniejszym znaczeniu. Drugim najistotniejszym zagrożeniem są ataki wykorzystujące błędy w aplikacjach. W 2025 roku okazały się bardziej dotkliwe niż rok i dwa lata wcześniej, kiedy to zajmowały odpowiednio siódme i ósme miejsce w rankingu.

Respondenci przypisali nieco większą wagę niż rok wcześniej zagrożeniu w postaci kradzieży danych przez pracowników firmy – to obecnie trzecie najważniejsze ryzyko, które awansowało z zeszłorocznego piątego miejsca. Tuż za podium uplasowały się ataki typu odmowa usługi, które między siódmą i ósmą edycją badania znacząco zyskały na znaczeniu, zajmując przed rokiem trzecie miejsce. Chociaż ataki na łańcuch dostaw za pośrednictwem partnerów biznesowych, podsłuchiwanie ruchu czy kradzieże danych drogą naruszeń bezpieczeństwa fizycznego znajdują się na końcu zestawienia, to dla wielu firm nadal pozostają zagrożeniami najwyższego ryzyka – od 23% do 31% badanych przedsiębiorstw oceniło je jako zagrożenia jednego z dwóch najwyższych stopni. Warto podkreślić, że wszystkie analizowane kategorie cyberzagrożeń są dostrzegane przez przedsiębiorców, a przynajmniej minimalne ryzyko ich wystąpienia i dotkliwości potwierdza od 95% do 100% respondentów.

**Kradzież danych poprzez phishing jest największym ryzykiem dla cyberbezpieczeństwa firm.**

## Cyberzagrożenia stanowiące największe ryzyko dla organizacji




Źródło: KPMG w Polsce na podstawie badania ankietowego.

*Powrót phishingu na szczyt rankingu zagrożeń to nie nostalgia za klasycznymi metodami ataku, lecz wynik dynamicznej rewolucji technologicznej napędzanej przez AI. Współczesny phishing ma niewiele wspólnego z masowymi wiadomościami sprzed lat. Dziś atakujący wykorzystują modele językowe do analizy publicznych profili swoich ofiar, generowania wiadomości naśladujących styl komunikacji znanych im osób, czy syntezy głosu w czasie rzeczywistym. W efekcie phishing staje się bardziej przekonujący i trudniejszy do wykrycia. To właśnie synergia klasycznej metody ataku z możliwościami oferowanymi przez AI sprawia, że zagrożenie to zyskało nowy, bardziej niebezpieczny wymiar."*


**Łukasz Staniak**

Partner Associate, Advisory,
Szef Grupy Kompetencyjnej
Cyberbezpieczeństwa
Infrastruktury IT/OT,
KPMG w Polsce

# 2 Transformacja cyberbezpieczeństwa



Zgodnie z raportem Institute for Applied Network Security, ponad połowa CISO w Stanach Zjednoczonych zadeklarowała, że ich obowiązki zwiększyły się na przestrzeni ostatniego roku, a już jedna trzecia z nich raportuje bezpośrednio do kierownictwa C-level lub biznesowego zamiast do liderów IT[4]. Wyniki tegorocznej edycji „Barometru cyberbezpieczeństwa" pokazują, że również na polskim rynku rola CISO i innych wyspecjalizowanych liderów tego obszaru rośnie i uniezależnia się od funkcji czysto technologicznych. Jednak podczas gdy kompetencje menedżerów bezpieczeństwa cyfrowego i ich bezpośrednia odpowiedzialność za ryzyko biznesowe poszerzają się, wielu z nich pozostaje przeciążonych niedoborem zasobów i brakiem wsparcia zarządu.

Tymczasem firmy coraz krytyczniej oceniają swój poziom ochrony. W 2025 roku jedynie 3% organizacji w Polsce określiło swoje cyberzabezpieczenia jako w pełni dojrzałe w większości badanych obszarów. W tej sytuacji liderzy stawiają przede wszystkim na inwestycje w ochronę przed złośliwym oprogramowaniem oraz szkolenia podnoszące świadomość. W czasie gdy ataki malware i phishing stają się coraz bardziej złożone i trudne do wykrycia, czujność pracowników staje się istotnym elementem łańcucha obrony. Również trendy w outsourcingu pokazują, że organizacje skupiają się na budowie długofalowych kompetencji wewnętrznych – delegując na zewnątrz tylko pojedyncze, wysoko specjalistyczne zadania.

Funkcjonujące w złożonych ekosystemach informatycznych firmy muszą poszerzać granice zabezpieczeń, ale jednocześnie ściślej kontrolować dostęp do sieci wewnętrznej. Zgodnie z wynikami badania w 2026 roku będą realizować te zadania poprzez znaczny wzrost środków przeznaczanych na ochronę bezpieczeństwa partnerów biznesowych oraz priorytetyzację segmentacji sieci.

[4] IANS Research, „2025 State of the CISO Summary Report", 2025.

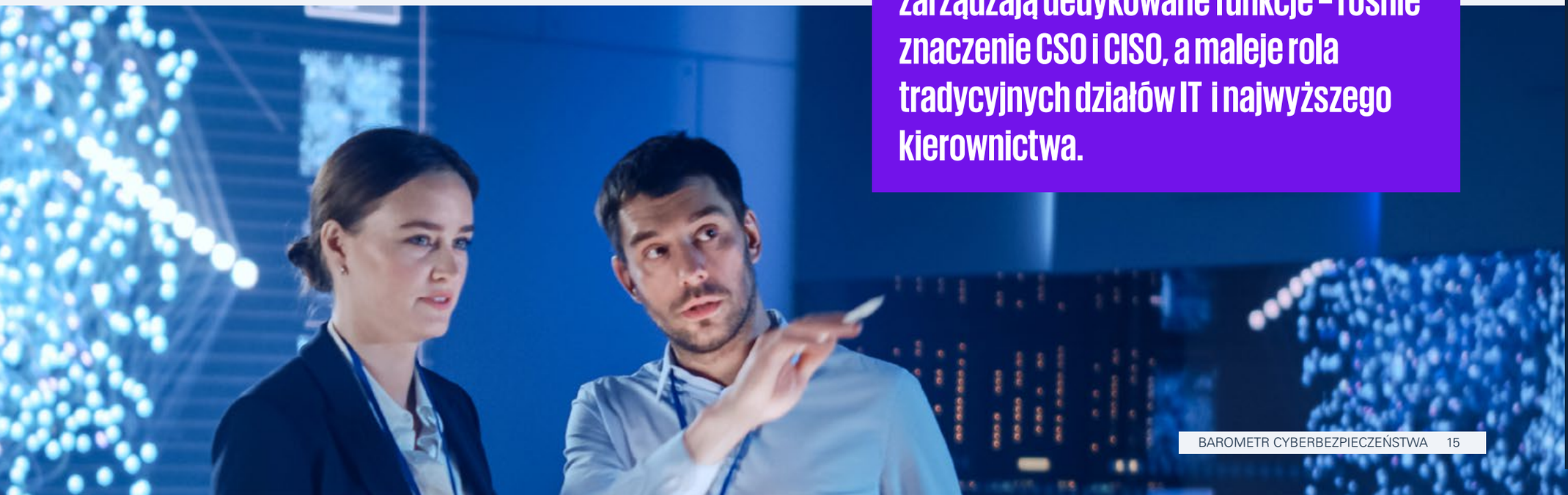
# Specjalizacja odpowiedzialności

W bieżącej edycji badania widoczna jest kontynuacja trendu polegającego na stopniowym ograniczaniu roli tradycyjnych działów IT w bezpośrednim zarządzaniu cyberbezpieczeństwem organizacji. Choć odpowiedzialność ta najczęściej nadal spoczywa na CIO (Chief Information Officer) lub innym wyznaczonym pracowniku w strukturach IT, to odsetek takich wskazań jest niższy o 5 p.p. w porównaniu z 2024 rokiem i o 11 p.p. względem 2023 roku. Jednocześnie dwukrotnie częściej niż w poprzedniej edycji badania respondenci deklarowali funkcjonowanie w organizacji niezależnej, dedykowanej roli CSO (Chief Security Officer) lub CISO (Chief Information Security Officer). Istotnie wzrosło również znaczenie innych, wyspecjalizowanych stanowisk odpowiedzialnych za obszar cyberbezpieczeństwa – odsetek takich wskazań zwiększył się o 10 p.p. Co ciekawe, obecność CISO była podobna niezależnie od wielkości organizacji.

Prezesi zarządu ponad dwukrotnie rzadziej niż w poprzednim roku obejmują odpowiedzialność za bezpieczeństwo informacji – odsetek takich wskazań spadł z 19% do 8%. Wyraźnie zmniejszyła się również liczba organizacji, które w ogóle nie przypisały odpowiedzialności za zarządzanie cyberbezpieczeństwem – z 11% do zaledwie 2% obecnie.

Uzyskane wyniki potwierdzają postępującą profesjonalizację i specjalizację zarządzania bezpieczeństwem informacji w polskich przedsiębiorstwach. Towarzyszy temu odchodzenie od modelu centralnego zarządzania bezpieczeństwem informacji przez osoby łączące tę odpowiedzialność z innymi kluczowymi rolami w firmie.

**Cyberbezpieczeństwem coraz częściej zarządzają dedykowane funkcje – rośnie znaczenie CSO i CISO, a maleje rola tradycyjnych działów IT i najwyższego kierownictwa.**



## Osoby odpowiedzialne za bezpieczeństwo informacji w organizacji

| | 2025 | 2024 | 2023 | 2022 | 2021 |
|---|---|---|---|---|---|
| Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT | 36% | 41% | 47% | 45% | 47% |
| Niezależna dedykowana funkcja (CSO/CISO) | 26% | 13% | 12% | 8% | 14% |
| Inne stanowisko w organizacji | 24% | 14% | 8% | 8% | 5% |
| Prezes zarządu (CEO) | 8% | 19% | 16% | 17% | 15% |
| Odpowiedzialność przypisana w strukturach globalnych poza Polską | 4% | 2% | 6% | 5% | 9% |
| Brak formalnego przypisania odpowiedzialności | 2% | 11% | 11% | 17% | 10% |

Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Stan zabezpieczeń – od prewencji do odporności

Postrzegana dojrzałość zabezpieczeń systematycznie spada – podobnie jak w ubiegłorocznej edycji „Barometru cyberbezpieczeństwa", respondenci ocenili ją gorzej niż rok wcześniej w 11 z 14 analizowanych kategorii. W dwóch kolejnych pozostała ona na tym samym poziomie, a jedynym obszarem, w którym nastąpiła bezwzględna poprawa, okazało się zarządzanie tożsamością i dostępem*.

W bieżącej edycji badania, w odróżnieniu od poprzedniej, która odnotowała pewną stabilizację, doszło do istotnego przetasowania w hierarchii obszarów uznawanych za najbardziej dojrzałe. Najwyżej uplasowało się reagowanie na incydenty bezpieczeństwa, które w poprzedniej edycji – mimo wyższej oceny dojrzałości – zajmowało dopiero trzecie miejsce. Drugą pozycję niezmiennie utrzymało bezpieczeństwo styku z siecią Internet, natomiast trzecią zajęło monitorowanie bezpieczeństwa. Warto odnotować, że obszary z pierwszego i trzeciego miejsca, które jednocześnie odnotowały wzrost pozycji w rankingu, w poprzednim roku były wskazywane jako dwa kluczowe priorytety inwestycyjne, co może świadczyć o skuteczności zaplanowanych działań.

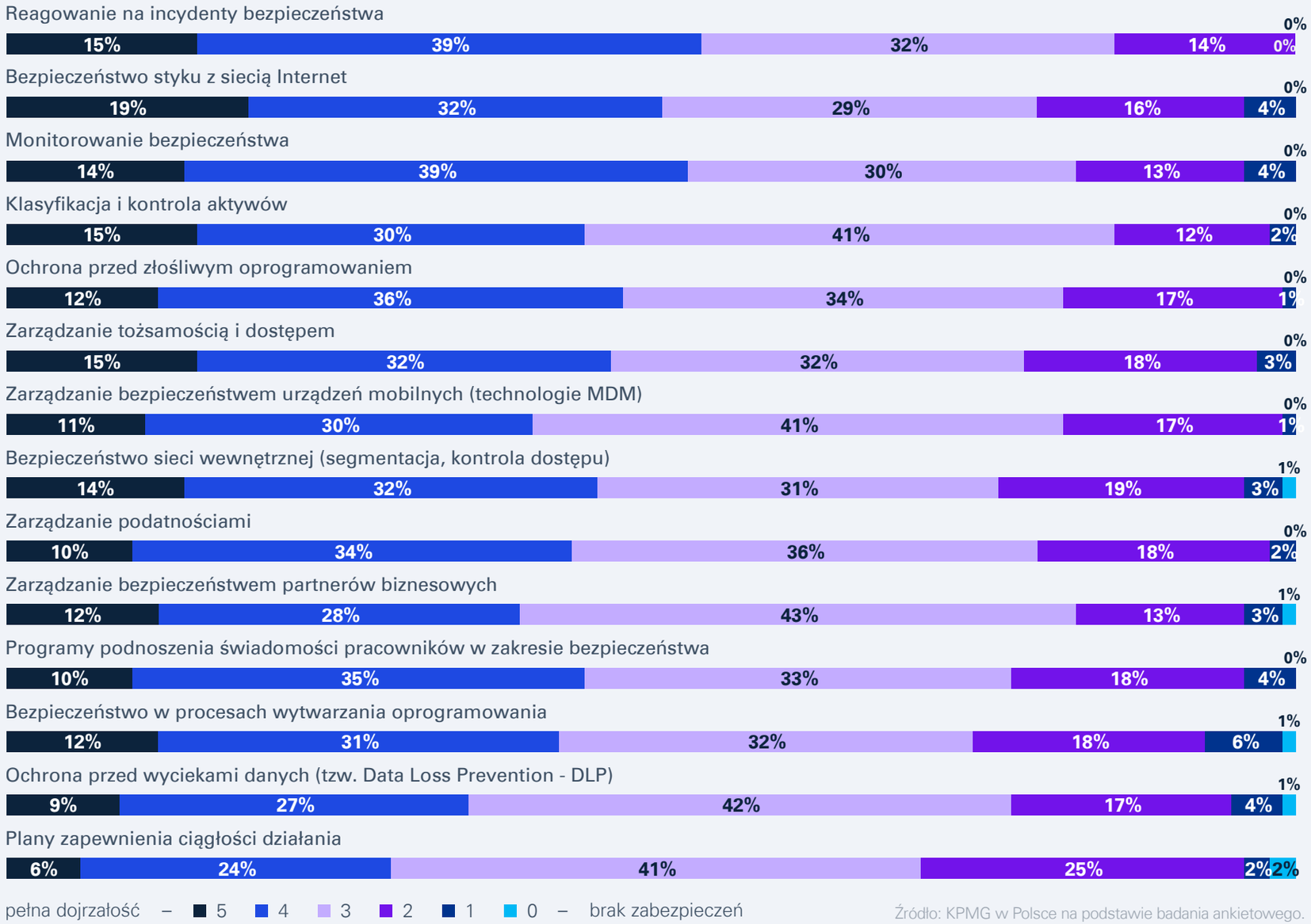
* Bezwzględna zmiana w dojrzałości zabezpieczeń została oszacowana na podstawie różnicy średniej ważonej liczby ocen od 1 do 5 w poszczególnych kategoriach między poprzednią a bieżącą edycją badania.

# Firmy najczęściej deklarują „pełną dojrzałość” w obszarze bezpieczeństwa styku z siecią Internet.

Czwarta w kolejności uplasowała się klasyfikacja i ochrona aktywów – jest to wyraźny awans z przedostatniego miejsca w ubiegłorocznym rankingu dojrzałości. Z kolei dopiero na piątej pozycji znalazła się ochrona przed złośliwym oprogramowaniem, która rok wcześniej uzyskała najwyższą ocenę. Wszystkie obszary plasujące się na miejscach od pierwszego do piątego, pomimo istotnych zmian kolejności w rankingu, uzyskały w bieżącej edycji niższe średnie oceny dojrzałości niż rok wcześniej.

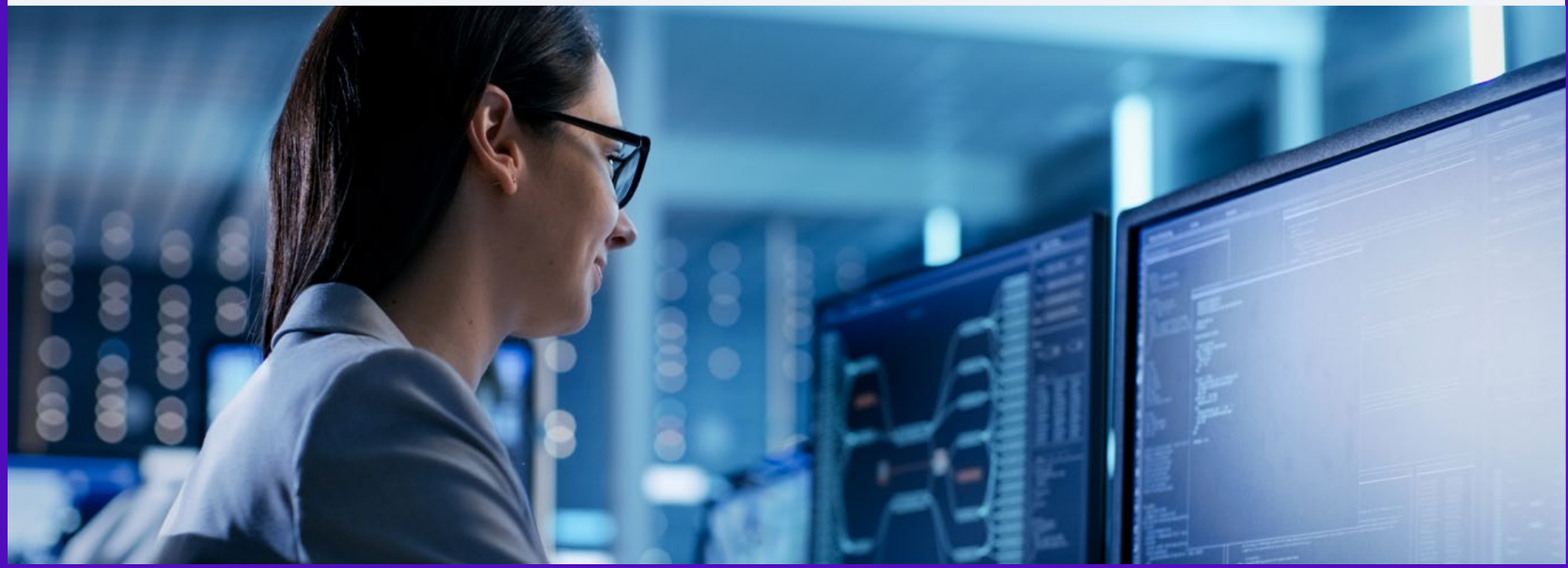
Do kategorii, które w 2025 roku poprawiły swoją pozycję względem pozostałych, należą również bezpieczeństwo sieci wewnętrznej, zarządzanie podatnościami oraz bezpieczeństwo urządzeń mobilnych – ten ostatni obszar zanotował szczególnie wyraźny awans, przesuwając się z ostatniego na siódme miejsce. Pozostałe funkcje, takie jak zarządzanie bezpieczeństwem partnerów biznesowych, programy podnoszenia świadomości pracowników czy bezpieczeństwo w procesach wytwarzania oprogramowania, znalazły się na niższych pozycjach rankingu niż rok wcześniej.

## Ocena dojrzałości poszczególnych obszarów zabezpieczeń w organizacji




Źródło: KPMG w Polsce na podstawie badania ankietowego.

Wyniki wskazują na delikatne przesunięcie z podejścia wyłącznie prewencyjnego w stronę skupienia na cyberodporności organizacji. Firmy coraz częściej zakładają nieuchronność incydentów i koncentrują się na wykrywaniu, reagowaniu oraz ograniczaniu skutków ataków, co znajduje odzwierciedlenie w relatywnie większej dojrzałości monitoringu i reagowania na incydenty. Również rosnąca pozycja klasyfikacji i kontroli aktywów świadczy o bardziej świadomym, uwzględniającym specyfikę zasobów podejściu do ochrony krytycznych systemów i danych. Zmiany te wpisują się w szerszy trend dojrzewania rynku i pokazują, że elastyczne dostosowywanie strategii cyberbezpieczeństwa staje się koniecznością w obliczu rosnącej skali zagrożeń i nowych wymogów regulacyjnych. Jednocześnie spadające średnie oceny dojrzałości sugerują coraz większą świadomość tempa tego procesu, podkreślając konieczność nieustannego wzmacniania poziomu ochrony.



# Inwestycje w odpowiedzi na ryzyka

W 2025 roku organizacje planowały zrealizować większe niż rok wcześniej inwestycje we wszystkich badanych obszarach. Rok 2026 przynosi jednak powściągliwość przedsiębiorców w tym zakresie. W sześciu kategoriach wartość inwestycji pozostanie na podobnym poziomie jak w ubiegłym roku, w pięciu – obniży się, a jedynie w trzech wzrośnie. Firmy najwięcej inwestować będą w ochronę przed złośliwym oprogramowaniem, programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa, a także bezpieczeństwo sieci wewnętrznej w zakresie segmentacji i kontroli dostępu. Mimo awansu względem innych obszarów, średni poziom tych inwestycji pozostaje podobny do ubiegłorocznego*.

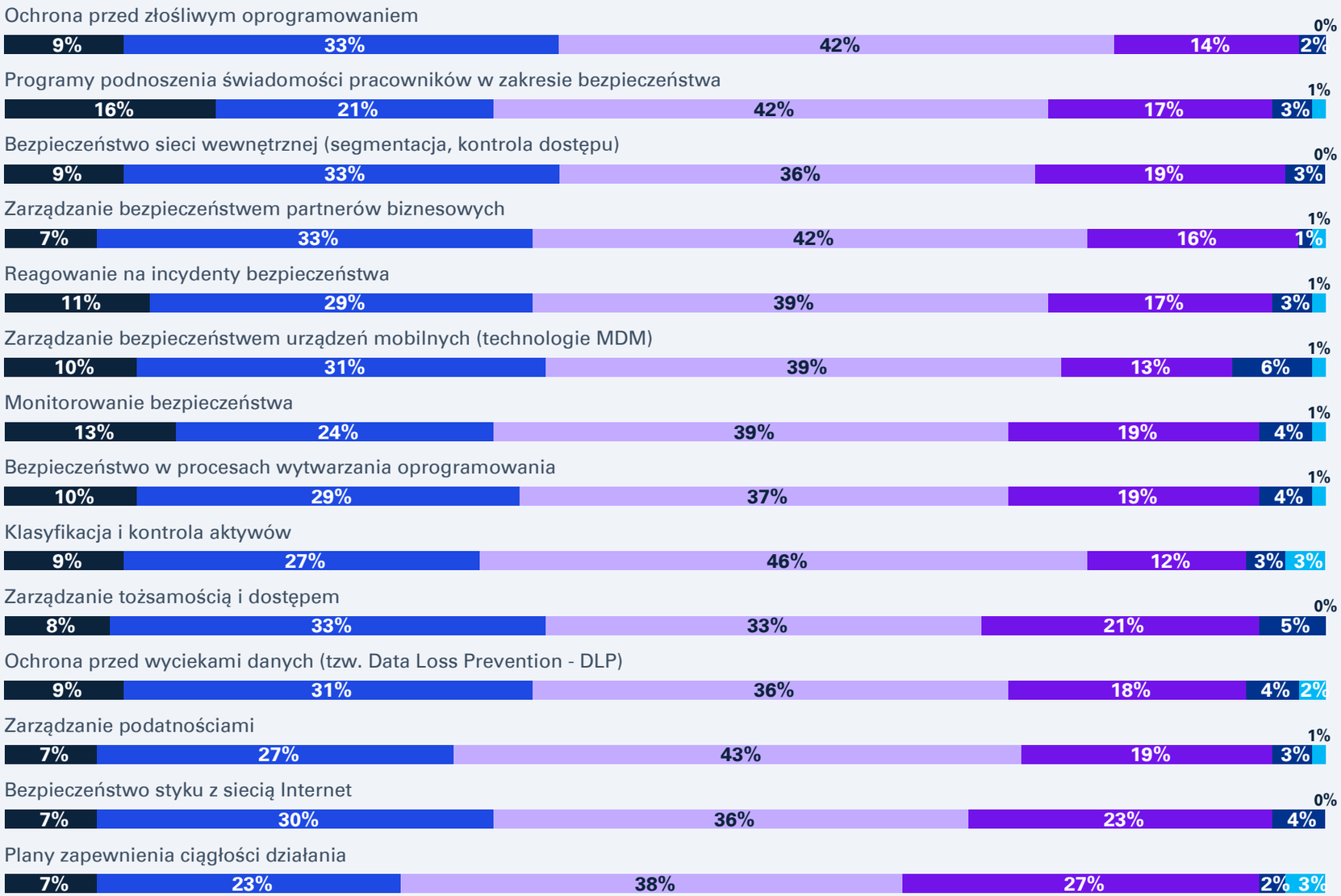
Najwyższa pozycja inwestycji w ochronę przed złośliwym oprogramowaniem wskazuje na jej szczególną istotność dla firm, które w bieżącej edycji badania oceniły ten obszar jako mniej dojrzały na tle pozostałych niż w roku poprzednim. Choć spadł on z pierwszego na, wciąż względnie wysokie, piąte miejsce w rankingu dojrzałości, firmy zadecydowały, że to ten zakres najbardziej wymaga kolejnych inwestycji.

Będące drugim w kolejności priorytetem inwestycyjnym programy zwiększające świadomość pracowników, a także zajmujące trzecią pozycję bezpieczeństwo sieci wewnętrznej oraz czwartą – zarządzanie bezpieczeństwem partnerów biznesowych, znajdują się w drugiej połowie rankingu dojrzałości. Oznacza to, że są to obszary postrzegane jako istotne z punktu widzenia poprawy poziomu cyberbezpieczeństwa organizacji, jednak nie są one jeszcze dostatecznie rozwinięte. Wysoka potrzeba szkolenia pracowników podkreśla, że firmy identyfikują nieświadomość oraz nieostrożność jako jedne z głównych źródeł incydentów, co jest spójne z rosnącymi obawami dotyczącymi coraz bardziej zaawansowanego technologicznie phishingu. Z kolei wzrost znaczenia inwestycji w bezpieczeństwo relacji zewnętrznych odzwierciedla presję regulacyjną i audytową, w tym wymagania dyrektywy NIS2, które obligują do aktywnego zarządzania ryzykiem w całym łańcuchu dostaw ICT. Szczególną uwagę przyciąga również reagowanie na incydenty bezpieczeństwa, które, pomimo najwyżej ocenianej dojrzałości, jest stosunkowo wysokim, bo piątym priorytetem inwestycyjnym, co wskazuje na dążenie firm do podnoszenia skuteczności doraźnych reakcji.

**Firmy najczęściej planują „znaczące inwestycje" w obszarze programów edukacyjnych dla pracowników.**

* Bezwzględna zmiana wartości inwestycji została oszacowana na podstawie różnicy średniej ważonej liczby ocen od 1 do 5 w poszczególnych kategoriach między poprzednią a bieżącą edycją badania.

## Obszary zabezpieczeń, w które firmy planują inwestować w ciągu najbliższych 12 miesięcy




Źródło: KPMG w Polsce na podstawie badania ankietowego.

Główne priorytety inwestycyjne kształtują się inaczej niż w poprzednim roku. Największe względne spadki priorytetu inwestycji – o sześć miejsc – odnotowały bezpieczeństwo styku z siecią Internet (z siódmego na 13. miejsce), a także monitorowanie bezpieczeństwa (z pierwszego na siódme). W połączeniu z wysokimi miejscami (drugim i trzecim) tych obszarów w rankingu dojrzałości, spadki te należy interpretować jako stabilizację, spowodowaną osiągnięciem adekwatnej na ten moment dojrzałości. Z kolei największy wzrost, z 12. na czwarte miejsce, wystąpił w zakresie inwestycji w zarządzanie bezpieczeństwem partnerów biznesowych.

**W 2026 roku inwestycje w zarządzanie bezpieczeństwem partnerów biznesowych wyraźnie zyskają na znaczeniu.**

Organizacje będą najmniej inwestować w plany zapewnienia ciągłości działania, które jednocześnie znalazły się na ostatniej pozycji pod względem dojrzałości. W kontekście faktu, że ponad jedna trzecia badanych przedsiębiorstw deklaruje posiadanie takich planów, stanowi to niepokojący sygnał świadczący o braku wizji rozwoju tego kluczowego dla utrzymania odporności operacyjnej obszaru. W obliczu eskalacji ataków ransomware, częstszych zakłóceń łańcuchów dostaw ICT oraz obowiązków wynikających między innymi z dyrektywy NIS2 i rozporządzenia DORA, marginalizacja inwestycji w plany ciągłości może prowadzić do sytuacji, w której nawet skuteczne mechanizmy prewencyjne nie przełożą się na realną zdolność organizacji do utrzymania kluczowych usług w warunkach kryzysowych, ponieważ brakować będzie przetestowanych scenariuszy działania.
Układ priorytetów ukazuje silną koncentrację na mierzalnych, a także łatwych do komunikacji zarządom obszarach cyberbezpieczeństwa – takich jak monitoring czy reagowanie na incydenty, a nie zarządzanie podatnościami, plany ciągłości czy bezpieczeństwo wytwarzania oprogramowania. Choć znaczenie tych ostatnich zakresów dla odporności organizacji jest fundamentalne, to ich wartość ujawnia się dopiero w sytuacjach kryzysowych. W organizacjach często myślenie operacyjne i reaktywne dominuje nad systemowym, kładącym nacisk na kompleksowe zapewnienie cyberodporności.

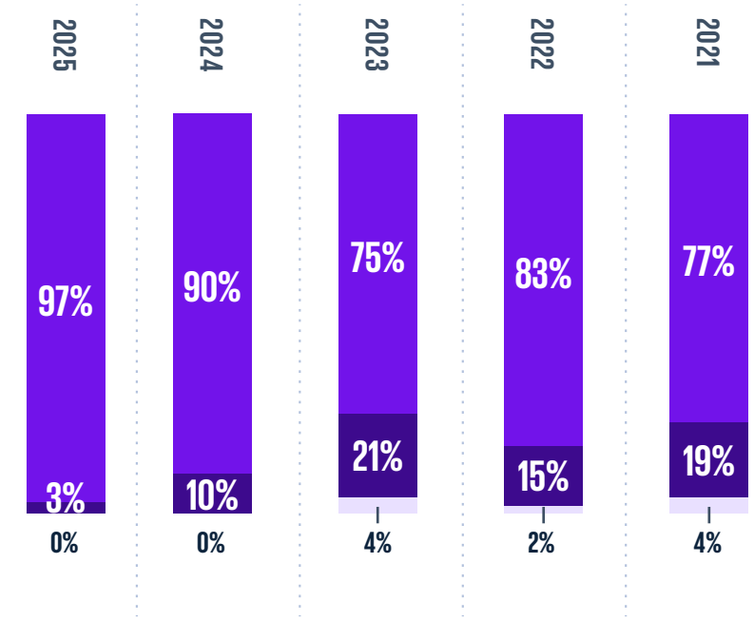
# Dojrzałość ochrony – wyścig bez mety

Z roku na rok organizacje coraz bardziej krytycznie oceniają swoją dojrzałość w zakresie cyberbezpieczeństwa. Już drugi rok z rzędu żadna z badanych firm nie zadeklarowała pełnej dojrzałości we wszystkich analizowanych wymiarach. Co więcej, odsetek organizacji osiągających wysoki poziom dojrzałości w większości obszarów systematycznie maleje od 2023 roku, a w obecnej edycji badania spadł do zaledwie 3%. Pozostałe 97% firm wskazało pełną dojrzałość w maksymalnie siedmiu z 14 ocenianych kategorii.

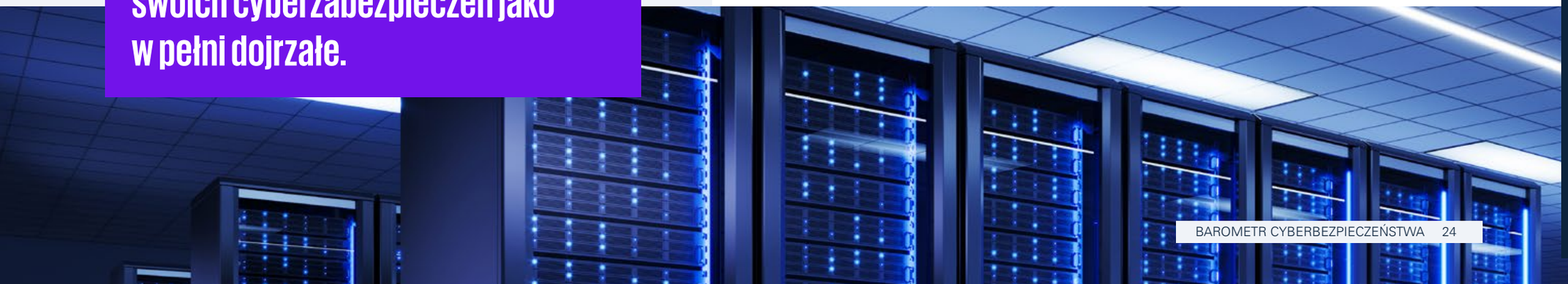
Wyraźny spadek ocen respondentów odzwierciedla tempo zmian oraz rosnącą złożoność incydentów cyberbezpieczeństwa, ich powiązanie z niestabilną sytuacją geopolityczną, a także ewolucję technologii stosowanej zarówno w atakach, jak i w narzędziach ochrony. Specjaliści coraz częściej identyfikują nieadekwatność dotychczasowych rozwiązań, które jeszcze kilka miesięcy wcześniej mogły być wystarczające. Cyberbezpieczeństwo to obszar, który wymaga nieustannej aktualizacji, a organizacje, które nie wprowadzają ulepszeń na bieżąco, szybko pozostają w tyle.

**Jedynie 3% firm oceniło większość swoich cyberzabezpieczeń jako w pełni dojrzałe.**

**Dojrzałość firm w zakresie zabezpieczeń**




Źródło: KPMG w Polsce na podstawie badania ankietowego.



# Mapa dojrzałości i priorytetów inwestycyjnych

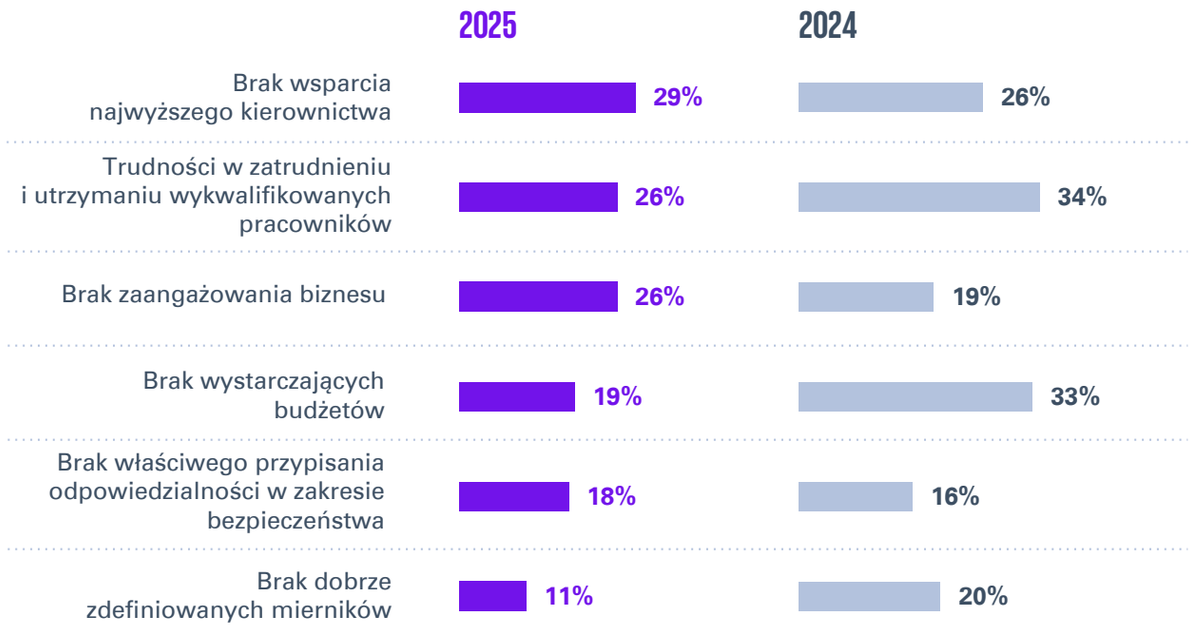
| | | Ranga dojrzałości | | Ranga inwestycji | |
|---|---|---|---|---|---|
| | | 2025 | 2024 | 2025 | 2024 |
| **Obszary względnie dojrzałe, o niskim priorytecie inwestycji** | Bezpieczeństwo styku z siecią Internet | 2 | 2 | 13 ↓ | 7 |
| | Monitorowanie bezpieczeństwa | 3 | 4 | 7 ↓ | 1 |
| | Klasyfikacja i ochrona aktywów | 4 ↑ | 13 | 9 | 11 |
| **Obszary niewystarczająco dojrzałe, wymagające priorytetowych inwestycji** | Bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu) | 8 | 11 | 3 ↑ | 8 |
| | Zarządzanie bezpieczeństwem partnerów biznesowych | 10 | 8 | 4 ↑ | 12 |
| | Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa | 11 | 9 | 2 ↑ | 5 |
| | Bezpieczeństwo w procesach wytwarzania oprogramowania | 12 ↓ | 6 | 8 ↑ | 13 |
| **Obszar kluczowy, wymagający stałych inwestycji** | Ochrona przed złośliwym oprogramowaniem | 5 ↓ | 1 | 1 | 3 |
| **Obszar najmniej dojrzały, zagrożony niedoinwestowaniem** | Plany zapewnienia ciągłości działania | 14 ↓ | 10 | 14 ↓ | 10 |
| **Obszar o rosnącej dojrzałości przy stabilnych inwestycjach** | Zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM) | 7 ↑ | 14 | 6 | 6 |

Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Współpraca w centrum wyzwań

W 2025 roku zmieniła się hierarchia głównych wyzwań w osiąganiu odpowiedniego poziomu cyberbezpieczeństwa organizacji. Na pierwsze miejsce, z wynikiem 29%, wysunął się brak wsparcia ze strony najwyższego kierownictwa – wcześniej zajmujący dopiero trzecią pozycję. Wyprzedził główną barierę poprzedniej edycji, czyli trudności w pozyskaniu i utrzymaniu wykwalifikowanych specjalistów, wskazywane obecnie przez nieco ponad jedną czwartą respondentów. Podobnie istotne okazało się niskie zaangażowanie biznesu w zagadnienia cyberbezpieczeństwa. Układ wyzwań pokazuje, że większym problemem niż budżet czy kwestie operacyjne – takie jak definiowanie mierników czy przypisanie odpowiedzialności – jest brak aktywnego udziału i współpracy osób decyzyjnych na wszystkich szczeblach organizacji.

**Główne ograniczenia dla uzyskania oczekiwanego poziomu zabezpieczeń**




Źródło: KPMG w Polsce na podstawie badania ankietowego.

Co istotne, zarządzający cyberbezpieczeństwem wskazywali mniej trudności niż w ubiegłej edycji, a odsetek odpowiedzi spadł w trzech z sześciu analizowanych kategorii. Sugeruje to, że niektóre wyzwania wyróżniają się wyraźnie znaczeniem i dominują nad innymi, mimo ich równoczesnego występowania. Barierami, których znaczenie wzrosło, są te związane ze wsparciem kierownictwa, zaangażowaniem biznesu i odpowiedzialnością. Taki wynik sygnalizuje przesunięcie postrzegania cyberbezpieczeństwa z obszaru techniczno-operacyjnego w stronę zagadnienia o charakterze strategicznym i organizacyjnym, wymagającego aktywnego wkładu najwyższego kierownictwa oraz realnej współodpowiedzialności biznesu. Jednocześnie wskazuje on na rosnącą świadomość, że dalsza poprawa poziomu cyberbezpieczeństwa zależy nie tylko od narzędzi i kompetencji zespołów technicznych, ale w coraz większym stopniu także od odpowiedniej klasyfikacji i priorytetyzacji ryzyk oraz integracji cyberbezpieczeństwa ze strategią biznesową.

*Fakt, że brak wsparcia ze strony najwyższego kierownictwa stał się główną barierą, to sygnał alarmowy, ale jednocześnie oznaka dojrzewania rynku. Cyberbezpieczeństwo przestaje być problemem technicznym, który można w pełni oddelegować do IT. W erze AI staje się fundamentalnym elementem strategii biznesowej.*

*Dlaczego wsparcie zarządu jest teraz krytyczne? Wdrażanie AI w organizacji tworzy nowe powierzchnie ataku i wymaga decyzji na najwyższym szczeblu. Kto ponosi odpowiedzialność za dane treningowe? Jak zarządzać ryzykiem związanym z modelami AI dostawców zewnętrznych? Jak zachować zgodność z AI Act?*

*To pytania, na które CISO nie odpowie samodzielnie. Wymagają one zaangażowania całego zarządu. Organizacje, które to rozumieją, zyskują przewagę konkurencyjną."*


**Marcin Kieszkowski**

Dyrektor, Advisory,
Zespół Cyberbezpieczeństwa,
KPMG w Polsce

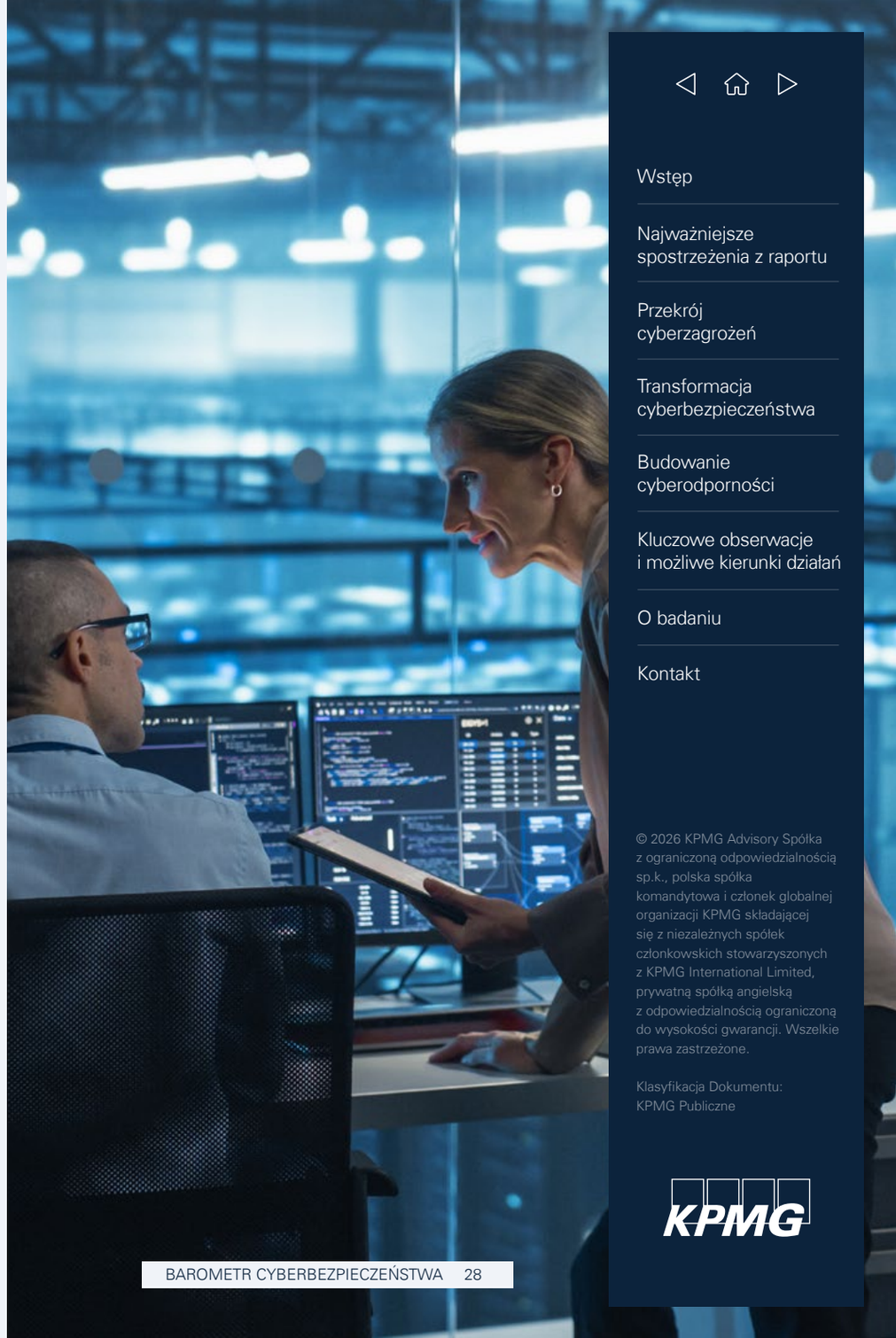
# Strategiczny podział zadań

Liczba firm korzystających z outsourcingu zadań związanych z cyberbezpieczeństwem zdecydowanie się zwiększyła – obecnie aż 94% z nich deleguje co najmniej jedną funkcję z tego zakresu (wzrost o 13 p.p. r/r). Nastąpiło jednak przesunięcie preferencji w kierunku zlecania zewnętrznym firmom wyłącznie jednej funkcji zamiast kilku – wspomniany wzrost liczby firm korzystających z outsourcingu wystąpił jedynie w tym zakresie. Wskazuje to na coraz bardziej selektywne podejście organizacji do outsourcingu cyberbezpieczeństwa – zamiast szerokiego przekazywania odpowiedzialności podmiotom zewnętrznym, koncentrują się one na wydzielaniu wyspecjalizowanych obszarów, w których braki kompetencyjne lub kosztowe są największe, przy jednoczesnym zachowaniu kontroli nad kluczowymi funkcjami bezpieczeństwa wewnątrz organizacji. Taka zmiana może świadczyć o stopniowym dojrzewaniu rynku.

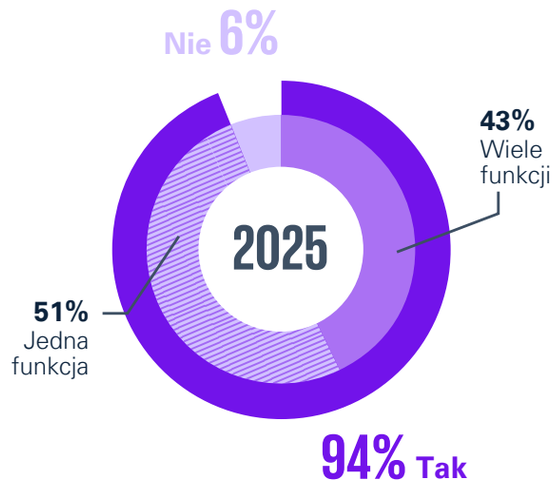
**Aż 94% firm korzysta z outsourcingu w realizacji co najmniej jednego zadania związanego z cyberbezpieczeństwem.**

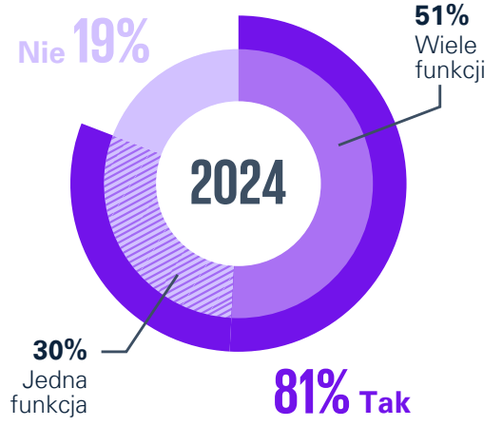
Outsourcing jest wykorzystywany przede wszystkim w obszarach wymagających wysokospecjalistycznych kompetencji oraz zaawansowanych narzędzi. Zewnętrzni dostawcy, tak jak w poprzednim roku, najczęściej realizują zadania z zakresu monitorowania bezpieczeństwa – odsetek firm delegujących tę funkcję wynosi 41% i jest podobny do ubiegłorocznego. Co czwarta firma zleca zewnętrznie przeglądy kodu źródłowego, analizę złośliwego oprogramowania i wsparcie w reakcji na cyberataki. Niewiele mniej organizacji korzysta z takiej pomocy w przypadku testów penetracyjnych aplikacji (23%). Jednocześnie niski poziom zlecania na zewnątrz testów podatności infrastruktury (13%) oraz działań o charakterze edukacyjnym (10%) sugeruje, że organizacje traktują je jako element budowy długofalowych kompetencji wewnętrznych.

Z powodu większego stosunku liczby firm delegujących wyłącznie jedną kategorię zadań do tych delegujących kilka, odsetki odpowiedzi w poszczególnych kategoriach outsourcingu zmniejszyły się w porównaniu do poprzedniej edycji pomimo ogólnego wzrostu popularności samego rozwiązania. Największy spadek – aż o 10 p.p. – wystąpił w przypadku testów podatności infrastruktury. Ewentualne wzrosty zmieściły się w zakresie 1-3 p.p. i dotyczyły monitorowania bezpieczeństwa, wsparcia w reakcji na cyberataki oraz testów penetracyjnych aplikacji.



## Korzystanie z outsourcingu




Źródło: KPMG w Polsce na podstawie badania ankietowego.

## Funkcje lub procesy bezpieczeństwa realizowane przez zewnętrznych dostawców


Źródło: KPMG w Polsce na podstawie badania ankietowego.

# 3 Budowanie cyberodporności

Cyberodporność coraz wyraźniej wykracza poza obszar czysto technicznego zabezpieczania systemów, obejmując konieczność stałej aktualizacji wiedzy, monitorowania zmieniającego się katalogu zagrożeń oraz utrzymywania wysokiego poziomu gotowości organizacyjnej i operacyjnej. Wyniki badania pokazują, że cyberodporność w wielu organizacjach jest obszarem aktywnie rozwijanym, ale rzadziej postrzeganym jako dojrzały. Zdecydowana większość firm identyfikuje potrzebę usprawnień, a jednocześnie regularnie podejmuje działania mające na celu ocenę i wzmocnienie swojej odporności na zagrożenia cyfrowe. Jest to podejście ewolucyjne.

Analiza wyników badania ujawnia wyraźną przewagę działań proceduralnych i organizacyjnych nad wdrożeniami zaawansowanych mechanizmów technicznych. Audyty, analizy ryzyka, plany ciągłości działania oraz zarządzanie zależnościami zewnętrznymi stanowią fundament deklarowanych praktyk. Jednocześnie badanie wskazuje na ograniczony zakres systemowego testowania zdolności reagowania w warunkach skrajnych zakłóceń, co może ograniczać rzeczywistą skuteczność nawet formalnie wdrożonych rozwiązań.

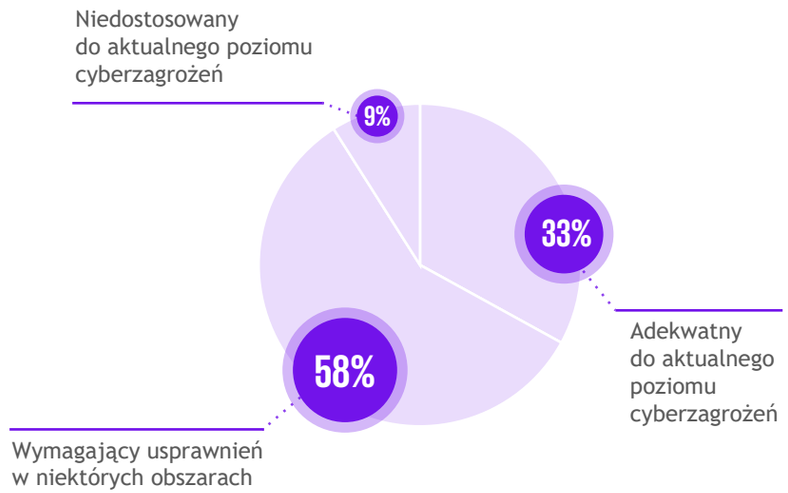
Istotnym kontekstem dla oceny cyberodporności staje się również rosnąca rola sztucznej inteligencji oraz wynikające z niej obowiązki regulacyjne. Wejście w życie Rozporządzenia AI Act przesuwa punkt ciężkości z samego wdrażania rozwiązań opartych na AI na ich bezpieczne, kontrolowane i zgodne z prawem wykorzystanie. Natomiast tempo i jakość projektów wdrażanych w odpowiedzi na nowe regulacje mają bezpośredni wpływ na długoterminową cyberodporność.

# Cyberodporność pod lupą

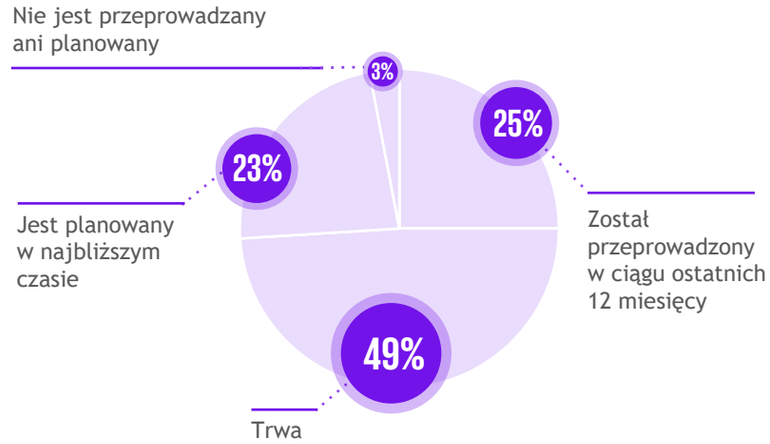
Wyniki oceny własnej cyberodporności przez organizacje pozwalają lepiej zrozumieć, na ile nadążają one za szybko zmieniającym się krajobrazem zagrożeń cyfrowych. Jedna trzecia respondentów deklaruje, że poziom cyberodporności ich firmy jest adekwatny do aktualnego przekroju cyberzagrożeń, a 58% wskazuje na potrzebę usprawnień w wybranych obszarach zabezpieczeń cyfrowych. Taki rozkład odpowiedzi sugeruje, że większość przedsiębiorstw ma świadomość zmiennego charakteru ryzyk i na bieżąco wzmacnia swoją cyberodporność lub przynajmniej potrafi trafnie identyfikować istniejące luki. Pozytywnym sygnałem jest fakt, że jedynie 9% badanych organizacji ocenia swoje przygotowanie jako wyraźnie niedostosowane do obecnego poziomu cyberzagrożeń.

Regularna, formalna ocena cyberodporności jest podstawą skutecznego zarządzania bezpieczeństwem informacji. Co czwarta organizacja przeprowadziła audyt cyberodporności w ciągu ostatnich 12 miesięcy, a w prawie połowie firm (49%) proces audytowy jest obecnie w toku. Kolejne 23% respondentów deklaruje, że taki audyt jest planowany w najbliższym czasie. Oznacza to, że zdecydowana większość organizacji albo już weryfikuje poziom swojej cyberodporności, albo przygotowuje się do takiej oceny. Jedynie 3% badanych wskazuje, że zewnętrzna kontrola cyberodporności nie jest ani realizowana, ani planowana, co potwierdza rosnącą dojrzałość podejścia do systemowego zarządzania cyberbezpieczeństwem.

### Ocena poziomu cyberodporności własnej organizacji




### Audyt cyberodporności

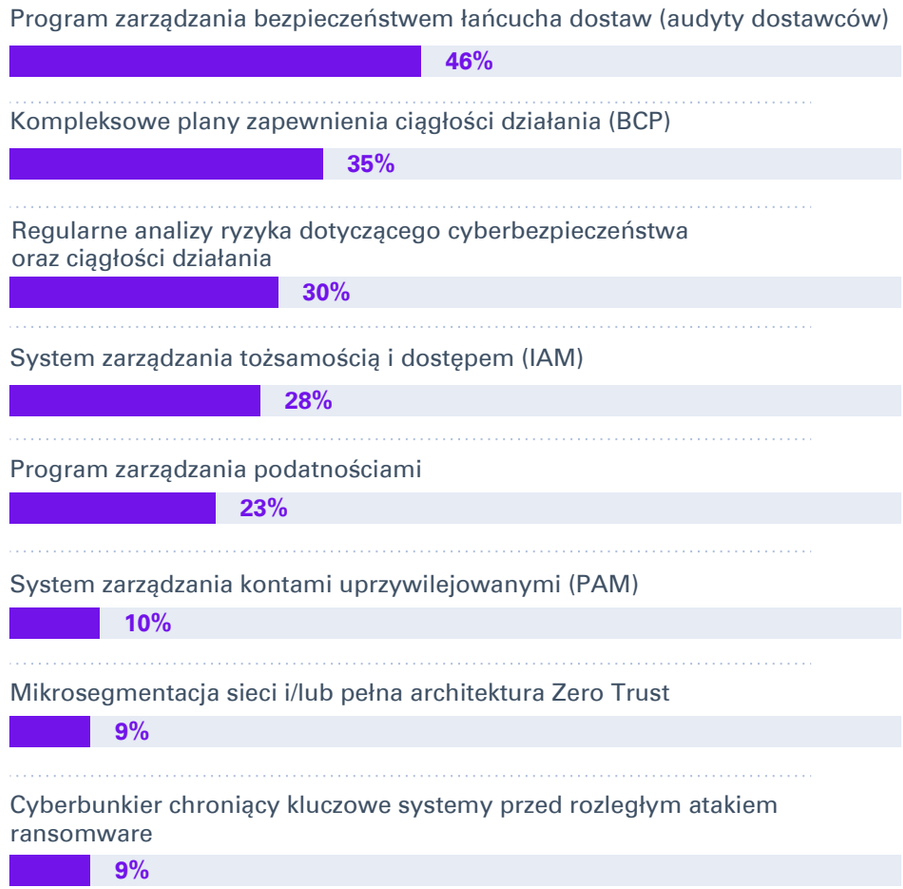



Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Fundamenty bezpieczeństwa oparte na procedurach

Deklarowane przez firmy mechanizmy zapewnienia cyberodporności koncentrują się przede wszystkim na rozwiązaniach o charakterze organizacyjnym i procesowym. Najczęściej wykorzystywany jest program zarządzania bezpieczeństwem łańcucha dostaw, w tym audyty dostawców, który wdrożyło 46% badanych organizacji. Relatywnie często organizacje przygotowują również kompleksowe plany zapewnienia ciągłości działania – BCP (35%) oraz przeprowadzają regularne analizy ryzyka w obszarze cyberbezpieczeństwa i ciągłości działania (30%). Wysoki wynik w obszarze ciągłości działania zaskakuje w obliczu nisko ocenianej dojrzałości, a także niskiego priorytetu inwestycyjnego dla tego obszaru, które kwestionują skuteczność obecnie realizowanych działań. W wielu przypadkach zadania z zakresu ciągłości mogą być przygotowywane jedynie dla spełnienia wymogów regulacyjnych – a zatem posiadać charakter formalny, a nie operacyjny, obejmujący regularne testy. W konsekwencji systemy mogą nie przetrwać próby realnego incydentu.

**Wdrożone mechanizmy bezpieczeństwa zapewniające cyberodporność firm**




Źródło: KPMG w Polsce na podstawie badania ankietowego.

Wśród mechanizmów wspierających cyberodporność często implementowane są również systemy zarządzania tożsamością i dostępem (IAM), wdrożone w 28% organizacji, oraz programy zarządzania podatnościami, wskazywane przez 23% respondentów. Znacznie rzadziej deklarowane są rozwiązania stricte techniczne, takie jak systemy zarządzania kontami uprzywilejowanymi (PAM) – 10%, mikrosegmentacja sieci lub pełna architektura Zero Trust – 9%, czy tzw. cyberbunkier chroniący kluczowe systemy przed rozległym atakiem ransomware – również 9%.

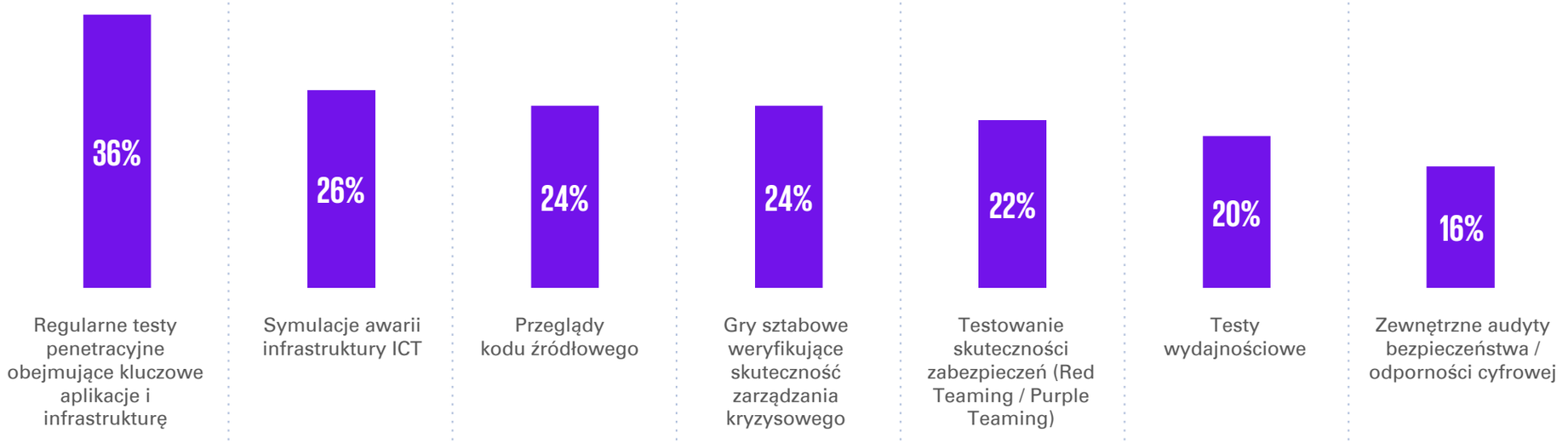
Taki rozkład odpowiedzi sygnalizuje dwa główne trendy – po pierwsze, sugeruje, że organizacje częściej budują cyberodporność poprzez procedury i zarządzanie ryzykiem niż poprzez zaawansowane narzędzia techniczne.

Po drugie, znacząca rola ochrony łańcucha dostaw i planów ciągłości jest związana z coraz bardziej rozmywającymi się granicami infrastruktury ICT, które coraz częściej obejmują środowiska chmurowe, usługi SaaS, pracę zdalną oraz rozbudowane ekosystemy partnerów i dostawców, pozostające poza bezpośrednią kontrolą organizacji. Rośnie znaczenie zarządzania zależnościami zewnętrznymi i odporności procesowej, ponieważ istotna część ryzyk materializuje się obecnie poza tradycyjnym perymetrem sieciowym. Trend ten jest dodatkowo wzmacniany przez zagrożenia o charakterze geopolitycznym, w tym nasilające się ataki na łańcuchy dostaw, które powodują, że cyberodporność staje się zagadnieniem systemowym, obejmującym całe otoczenie biznesowe organizacji.

Zdecydowana większość, bo 95% badanych firm stosuje mechanizmy monitorowania i testowania cyberodporności. Wyniki badania pokazują zróżnicowany poziom zaawansowania działań podejmowanych przez organizacje w tym zakresie. Najczęściej wskazywanym rozwiązaniem są regularne testy penetracyjne obejmujące kluczowe aplikacje i infrastrukturę, na które decyduje się 36% organizacji. Istotną rolę odgrywają również symulacje awarii infrastruktury ICT (26%), przeglądy kodu źródłowego oraz gry sztabowe weryfikujące skuteczność zarządzania kryzysowego (po 24%). Bardziej zaawansowane formy sprawdzania, takie jak testowanie skuteczności zabezpieczeń w modelu Red Teaming lub Purple Teaming, realizuje 22% organizacji, natomiast testy wydajnościowe prowadzi jedna piąta badanych. Zewnętrzne audyty bezpieczeństwa i weryfikację odporności cyfrowej przez podmioty trzecie deklaruje 16% respondentów. Istnieje więc niewielka grupa firm, które nie podejmują się żadnej z form monitorowania i testowania cyberodporności, ale te, które to robią, sięgają po zróżnicowane rozwiązania.

Zestawienie tych wyników wskazuje, że monitorowanie i testowanie cyberodporności stało się rynkowym standardem, jednak w większości organizacji ma ono charakter punktowy i selektywny, a nie ciągły i systemowy. Dominacja testów penetracyjnych oraz symulacji awarii sugeruje koncentrację na weryfikacji pojedynczych elementów infrastruktury przy relatywnie rzadszym stosowaniu testów odzwierciedlających kompletne scenariusze zagrożeń i zdolności reagowania całej organizacji.

## Mechanizmy bezpieczeństwa monitorujące i testujące cyberodporność w firmach




Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Cyberodporność w warunkach zakłóceń

Istotą zarządzania ciągłością działania jest utrzymanie najważniejszych procesów biznesowych na założonym poziomie, nawet w warunkach wystąpienia zakłóceń lub incydentów. W kontekście cyberbezpieczeństwa oznacza to przede wszystkim zapewnienie dostępności zasobów informatycznych wspierających realizację procesów krytycznych, takich jak infrastruktura ICT, sieć, sprzęt, systemy, aplikacje oraz dane. Układanie planu ciągłości działania polega na analizie wpływu potencjalnych zagrożeń na działalność organizacji, a następnie na definiowaniu i wdrażaniu adekwatnych zabezpieczeń – zarówno prewencyjnych, jak i reakcyjnych. Istotnym elementem są również testy zdefiniowanych scenariuszy oraz jasno określone procedury działania i komunikacji na wypadek sytuacji kryzysowej. Tak ułożony schemat postępowania pozwala skutecznie ograniczać i łagodzić konsekwencje incydentów, minimalizując ich wpływ na ciągłość funkcjonowania organizacji.

Zarządzanie ciągłością działania w badanych firmach koncentruje się przede wszystkim na identyfikacji i porządkowaniu kluczowych elementów działalności. Najczęściej deklarowanym rozwiązaniem jest aktualizowana na bieżąco lista procesów krytycznych, którą posiada 38% respondentów. Relatywnie wysokie odsetki dotyczą również prowadzenia rejestru zasobów wspierających procesy krytyczne (29%) oraz analiz ryzyka obejmujących wszystkie zasoby istotne z perspektywy ciągłości działania (27%). Uzupełnieniem tych kroków jest mapowanie zależności pomiędzy systemami krytycznymi, realizowane w 24% organizacji, oraz regularna analiza wpływu na biznes (BIA), obejmująca wszystkie procesy biznesowe – obecna w 21% firm.

Nieco rzadziej organizacje deklarują wdrożenie rozwiązań związanych z operacyjnym testowaniem zdolności odtworzeniowych. Regularne testy możliwości przywrócenia działania systemów po awarii prowadzi jedna piąta, a testy weryfikujące ciągłość działania przy całkowitej utracie głównego centrum przetwarzania danych – 15% firm. Jeszcze niższy poziom wdrożeń dotyczy formalnych odniesień do normy ISO 22301 – zgodność deklaruje 9% organizacji, a formalną certyfikację posiada jedynie 5% badanych.

## Rozwiązania obecne w procesach zarządzania ciągłością w firmach


Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Scenariusze cyberzagrożeń

Zakres scenariuszy zagrożeń uwzględnianych w analizach ryzyka w ramach zarządzania ciągłością działania pokazuje, na ile organizacje przygotowują się na zdarzenia o charakterze systemowym i długotrwałym. Wyniki wskazują, że firmy coraz częściej uwzględniają w analizach ryzyka scenariusze o charakterze infrastrukturalnym i geopolitycznym. Najczęściej analizowana w tym kontekście jest utrata kluczowego dostawcy usług chmurowych, którą uwzględnia 37% respondentów. Niewiele rzadziej organizacje przygotowują się na długotrwały brak energii elektrycznej (36%) oraz dostępu do sieci Internet (29%), co potwierdza rosnącą świadomość zależności biznesu od infrastruktury technicznej i zewnętrznych usługodawców.

Istotne miejsce w analizach ryzyka zajmują również scenariusze związane z celowymi działaniami o wrogim charakterze. Wojna hybrydowa i sabotaż są uwzględniane przez 26% organizacji, a awaria technologicznego łańcucha dostaw, mogąca powstać w wyniku zainfekowanych aktualizacji, przez 23%. Rozległy atak ransomware analizuje 21% respondentów, natomiast pełnoskalowy konflikt zbrojny – 16%. Znacznie rzadziej brane pod uwagę są scenariusze pandemii oraz katastrof naturalnych, które wskazało po 11% badanych. W połączeniu z często włączanymi w analizę ryzyka scenariuszami takie odsetki sugerują, że pomimo rosnącej świadomości związanej z zależnością od kluczowych usług i dostawców, nadal często pomijane są scenariusze skrajne – w których wypadku zerwana współzależność okazałaby się szczególnie dotkliwa.

Na tle tych wyników warto zwrócić uwagę, że 5% organizacji w ogóle nie przeprowadza analizy ryzyka w ramach procesu zarządzania ciągłością działania, a dodatkowe 2% deklaruje prowadzenie takiej analizy bez uwzględnienia któregokolwiek z wymienionych scenariuszy, co może ograniczać jej praktyczną użyteczność.

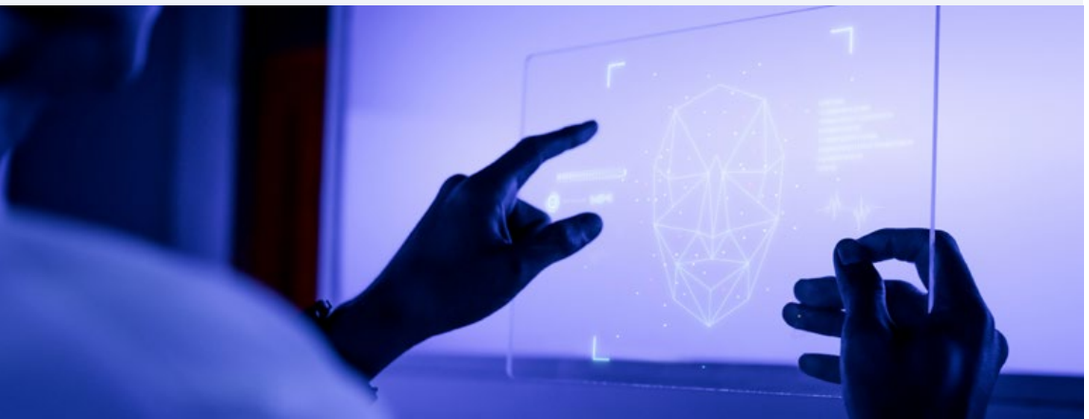
**Scenariusze zagrożeń uwzględniane w analizie ryzyka w ramach procesu zarządzania ciągłością działania**

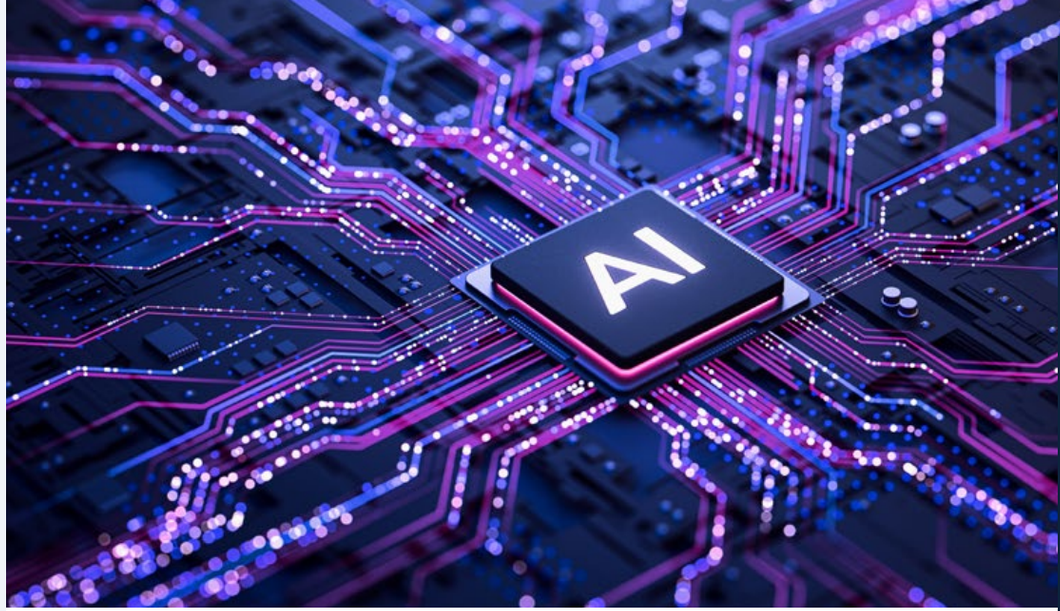

Źródło: KPMG w Polsce na podstawie badania ankietowego.

# (Nie)gotowi na AI Act

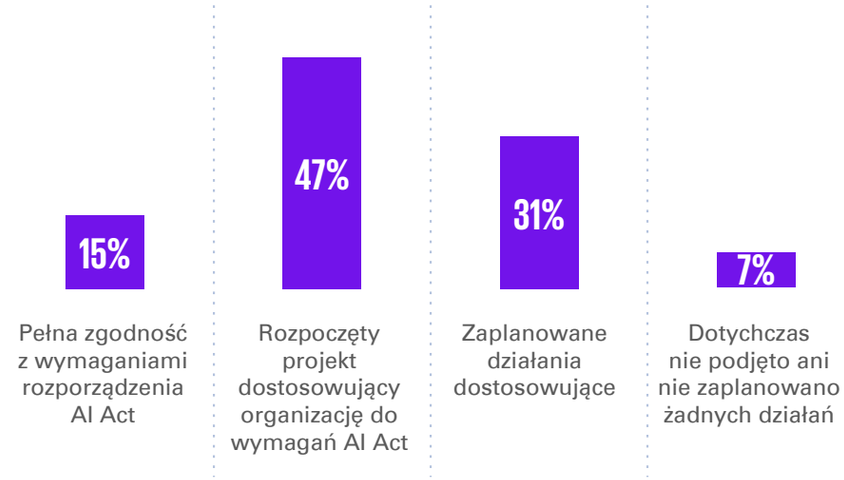
Od 1 sierpnia 2024 roku obowiązuje Rozporządzenie AI Act. Ma ono chronić użytkowników sztucznej inteligencji poprzez wsparcie świadomego wdrażania rozwiązań opartych na tej technologii i zapobieganie praktykom zagrażającym bezpieczeństwu cyfrowemu. Co istotne, rozporządzenie wchodzi w życie etapami, a u progu 2026 roku obowiązują dwie pierwsze grupy przepisów – dotyczące zakazanych praktyk oraz nakładające obowiązki na dostawców modeli AI ogólnego przeznaczenia oraz określające kary za naruszanie przepisów rozporządzenia. Proces dostosowywania trwa, a te firmy, które sprawnie reagują na zmiany regulacyjne w obszarze AI, zyskują przewagę konkurencyjną i wzmocnienie cyberodporności.

Przedsiębiorcy zapytani o przygotowanie ich organizacji do zgodności z Rozporządzeniem AI Act w większości deklarują rozpoczęcie realizacji projektów dostosowujących (47%) lub ich planowanie (31%). Proporcja pomiędzy tymi dwoma podejściami odwróciła się w porównaniu do zeszłorocznej edycji badania – znacznie przybyło organizacji, które przeszły od planów do prac przygotowawczych (wzrost o 29 p.p.). Jednak pełną zgodność z wymogami rozporządzenia w 2025 roku osiągnęło jedynie 15% badanych firm, czyli tylko o 1 p.p. więcej niż rok wcześniej. Warto pamiętać, że proces dostosowywania, jego tempo i jakość wykonanych w tym celu projektów, będzie w najbliższych miesiącach i latach jednym z fundamentów budowania trwałej odporności na cyberzagrożenia związane ze sztuczną inteligencją.






**Przygotowanie organizacji do zgodności z Rozporządzeniem AI Act**




Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Kluczowe obserwacje i możliwe kierunki działań

## Rosnąca skala i intensywność cyberataków

W połowie firm odnotowano wzrost liczby prób ataków, a 96% organizacji doświadczyło w 2025 roku co najmniej jednego incydentu bezpieczeństwa – to najwyższy wynik w historii badania. Coraz częstsze wielokrotne naruszenia wskazują, że incydenty przestają mieć charakter jednostkowy, co wzmacnia potrzebę przejścia z reaktywnego na ciągły, systemowy model zarządzania cyberbezpieczeństwem.

## Profesjonalizacja i specjalizacja zarządzania cyberbezpieczeństwem

Dwukrotnie częściej niż w 2024 roku firmy deklarują istnienie niezależnej roli CSO lub CISO, a prezesi zarządu ponad dwukrotnie rzadziej obejmują bezpośrednią odpowiedzialność za bezpieczeństwo informacji (spadek z 19% do 8%). Znacząco wzrosło też znaczenie innych wyspecjalizowanych stanowisk (wzrost o 10 p.p.). Dedykowana rola CISO/CSO zapewnia niezależność, właściwe ukierunkowanie strategiczne oraz bezpośredni dostęp do najwyższego kierownictwa.

## Dominacja ryzyk związanych z danymi i aplikacjami

Kradzież danych poprzez phishing oraz ataki wykorzystujące podatności aplikacyjne znajdują się na czele katalogu zagrożeń, co potwierdza, że słabym ogniwem pozostają zarówno użytkownicy, jak i jakość zabezpieczeń warstwy aplikacyjnej. W dłuższej perspektywie oznacza to konieczność łączenia inwestycji w technologie ochronne z systematycznym podnoszeniem dojrzałości procesów wytwórczych i zarządzania dostępem.

## Niskie zaangażowanie kierownictwa i biznesu

Brak wsparcia ze strony najwyższego kierownictwa stał się głównym wyzwaniem, wyprzedzając problemy kadrowe i budżetowe. Niskie zaangażowanie biznesu w kwestie cyberbezpieczeństwa (problem dla 29% firm) sygnalizuje, że bez aktywnego udziału decydentów na wszystkich szczeblach strategia cyberbezpieczeństwa nie będzie kompletna.

## Plany ciągłości działania – zaniedbany fundament odporności operacyjnej

Plany zapewnienia ciągłości działania znalazły się na ostatnim miejscu zarówno w rankingu dojrzałości, jak i priorytetów inwestycyjnych na 2026 rok. Ponad jedna trzecia firm deklaruje posiadanie takich planów, ale brak inwestycji w ich rozwój oznacza, że mogą być one nieaktualne lub nietestowane. To niepokojący sygnał w obliczu eskalacji ataków ransomware, zakłóceń łańcuchów dostaw ICT oraz wymogów regulacyjnych.

## Cyberodporność jako proces, nie stan docelowy

Tylko jedna trzecia organizacji ocenia swój poziom cyberodporności jako w pełni adekwatny do obecnych zagrożeń, podczas gdy większość wskazuje na potrzebę dalszych usprawnień. Wysoki poziom aktywności audytowej oraz powszechne stosowanie mechanizmów monitorowania i testowania sugerują rosnącą świadomość luk, ale także konieczność przejścia od działań punktowych do bardziej spójnych, długofalowych programów wzmacniania odporności.

## Inwestycje na wielu poziomach – stosunkowo wysokie nakłady na świadomość i zarządzanie ryzykiem w całym łańcuchu dostaw ICT

Zaraz za ochroną przed złośliwym oprogramowaniem, programy podnoszenia świadomości pracowników to drugi najważniejszy priorytet inwestycyjny na 2026 rok, a zarządzanie bezpieczeństwem partnerów biznesowych zanotowało największy wzrost znaczenia – z 12. na czwarte miejsce.

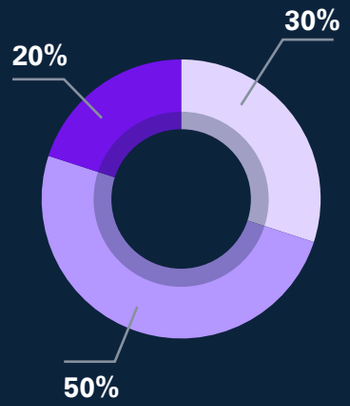
## Ciągłość działania oparta na identyfikacji, nie na testach skrajnych scenariuszy

Najczęściej stosowane formy zarządzania ciągłością działania koncentrują się na porządkowaniu procesów i zasobów krytycznych. Choć stanowi to istotny fundament, relatywnie niższy poziom wdrożeń testów odtworzeniowych może ograniczać zdolność organizacji do realnego sprawdzenia przygotowania na długotrwałe lub kumulujące się zakłócenia.

# O badaniu

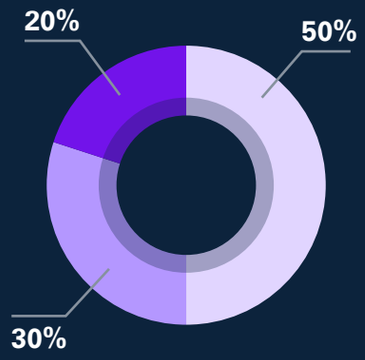
Raport „Barometr cyberbezpieczeństwa. Cyberodporność w erze zmian" został opracowany przez KPMG w Polsce na podstawie wyników ankiety przeprowadzonej metodą CATI w grudniu 2025 roku. W badaniu uczestniczyło 100 respondentów z organizacji działających w Polsce, którzy w swoich firmach odpowiadają za bezpieczeństwo IT – takich jak członkowie zarządu, dyrektorzy ds. bezpieczeństwa, dyrektorzy IT i inne osoby odpowiedzialne. Próba badawcza objęła organizacje o przychodach przekraczających 51 mln złotych z 16 głównych branż.

### Wielkość badanych firm



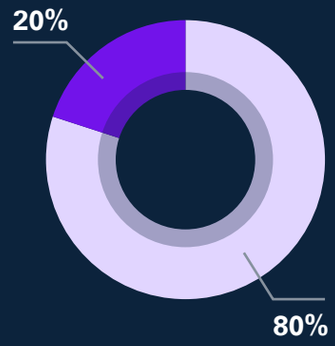

- Małe (max. 50 osób)
- Średnie (50-249 osób)
- Duże (od 250 osób)

### Przychody badanych firm



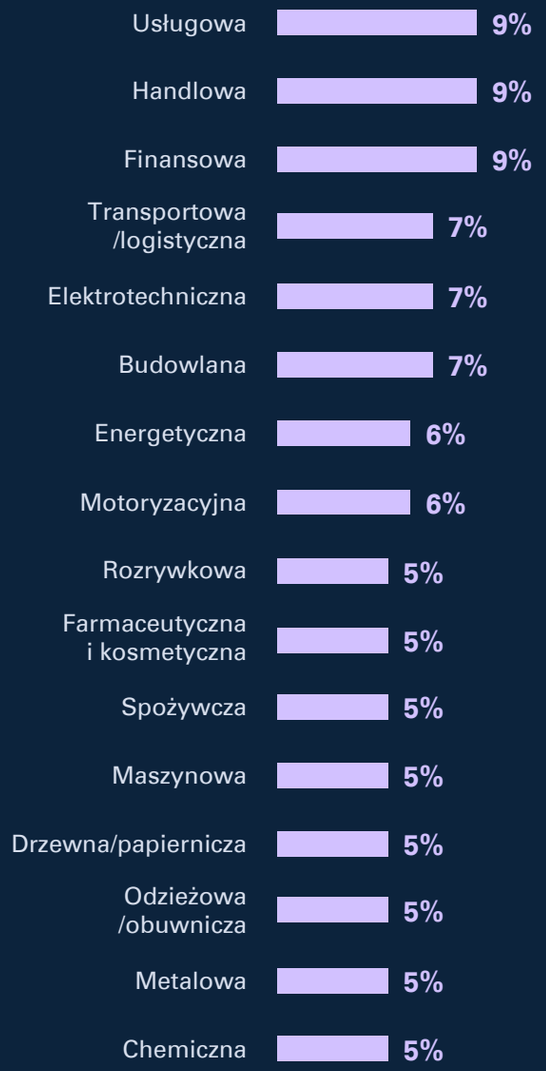

- 51-100 mln zł
- 101-200 mln zł
- Powyżej 200 mln zł

### Typ kapitału




- Polski
- Zagraniczny

### Branże badanych firm




Źródło: KPMG w Polsce na podstawie badania ankietowego.

# Wybrane publikacje KPMG w Polsce i na świecie


**Barometr cyberbezpieczeństwa 2025. Bezpieczeństwo AI – na progu rewolucji**


**Sztuczna inteligencja w Polsce. Krajobraz pełen paradoksów**


**Dylematy cyberbezpieczeństwa 2025**


**Globalne trendy technologiczne KPMG 2026**

# Kontakt

**KPMG w Polsce**
ul. Inflancka 4A
00-189 Warszawa
**T:** +48 22 528 11 00
**E:** kpmg@kpmg.pl

**Michał Kurek**
Partner

Advisory, Szef Zespołu
Cyberbezpieczeństwa
w KPMG w Polsce i Europie
Środkowo-Wschodniej

**E:** michalkurek@kpmg.pl

**Biura KPMG w Polsce**

**Warszawa**
ul. Inflancka 4a
00-189 Warszawa
**T:** +48 22 528 11 00
**E:** kpmg@kpmg.pl

**Kraków**
ul. Opolska 114
31-323 Kraków
**T:** +48 12 424 94 00
**E:** krakow@kpmg.pl

**Poznań**
ul. Roosevelta 22
60-829 Poznań
**T:** +48 61 845 46 00
**E:** poznan@kpmg.pl

**Wrocław**
ul. Szczytnicka 11
50-382 Wrocław
**T:** +48 71 370 49 00
**E:** wroclaw@kpmg.pl

**Gdańsk**
ul. Marynarki Polskiej 197
80-868 Gdańsk
**T:** +48 58 772 95 00
**E:** gdansk@kpmg.pl

**Katowice**
ul. Francuska 36
40-028 Katowice
**T:** +48 32 778 88 00
**E:** katowice@kpmg.pl

**Łódź**
ul. Kopcińskiego 62d
90-032 Łódź
**T:** +48 42 232 77 00
**E:** lodz@kpmg.pl

KPMG Poland

**kpmg.pl**