KPMG

Barometr cyberbezpieczeństwa

Bezpieczeństwo AI – na progu rewolucji

Luty 2025 | kpmg.pl

Wstęp

Szanowni Państwo,

Z przyjemnością przedstawiam ósmą edycję raportu „Barometr Cyberbezpieczeństwa". Od początku celem tej publikacji jest zwiększanie świadomości i rozwijanie umiejętności skutecznego zarządzania bezpieczeństwem informatycznym w obliczu dynamicznie zmieniającego się krajobrazu zagrożeń w cyberprzestrzeni. Mam nadzieję, że zebrane wnioski będą dla Państwa inspiracją do efektywnego wzmacniania ochrony Państwa organizacji przed współczesnymi wyzwaniami.

W tegorocznym badaniu uczestniczyło 100 polskich przedsiębiorstw reprezentujących zarówno duże, średnie, jak i małe firmy. Ankietę wypełniły osoby odpowiedzialne za bezpieczeństwo informacji, a badanie zostało przeprowadzone w grudniu 2024 roku. W tej edycji raportu szczególną uwagę poświęciliśmy sztucznej inteligencji oraz jej wpływowi na cyfrowe bezpieczeństwo organizacji w kontekście intensywnego rozwoju tej technologii.

Skutki ekspansji AI w obszarze cyberbezpieczeństwa są trudne do przewidzenia, ponieważ obejmują szerokie spektrum potencjalnych scenariuszy. Sztuczna inteligencja może nie tylko generować nowe zagrożenia, takie jak zaawansowane oszustwa czy kradzież tożsamości, ale również oferować znaczące wsparcie w ochronie przed cyberatakami. Jej możliwości obejmują analizę danych, bardziej efektywne wykrywanie oszustw oraz przeprowadzanie zaawansowanych testów penetracyjnych, co czyni ją narzędziem o podwójnej roli – zarówno sprzymierzeńcem, jak i przeciwnikiem w walce z cyberzagrożeniami. Dodatkowo systemy biznesowe wykorzystujące modele sztucznej inteligencji stanowią ogromną wartość dla przedsiębiorstw i wymagają specjalnego podejścia do ich ochrony. Warto zauważyć, że ponad połowa badanych przewiduje wzrost zagrożeń związanych z nowymi typami ataków wynikającymi z szerokiego wdrożenia AI. Jednocześnie ponad jedna czwarta respondentów uważa, że AI nie wpłynie istotnie na poziom zagrożeń, a 16% liczy na spadek ryzyka dzięki jej zastosowaniom w ochronie cyfrowej.

Aż 83% badanych firm doświadczyło przynajmniej jednej próby cyberataku. Choć liczba takich incydentów stale rośnie, ich intensywność jest różna w zależności od wielkości organizacji – duże przedsiębiorstwa odczuwają je w większym stopniu niż średnie i małe. Podkreśla to potrzebę dostosowania strategii ochrony do specyfiki firmy oraz znaczenie odpowiednich działań prewencyjnych, które pozwolą skutecznie reagować na dynamicznie zmieniające się zagrożenia.

Efektywna obrona przed cyberatakami to nie tylko wyzwanie, ale przede wszystkim kluczowa inwestycja w stabilność i rozwój każdej organizacji. Aby transformacja była skuteczna, cyberbezpieczeństwo musi stanowić fundament całego procesu zmiany.

Życząc Państwu inspirującej lektury, zachęcam do pogłębienia refleksji nad poruszanymi zagadnieniami oraz podjęcia działań na rzecz wzmocnienia ochrony Państwa organizacji w obliczu obecnych i przyszłych zagrożeń w cyberprzestrzeni. W szczególności zależy nam na podjęciu dyskusji na temat bezpieczeństwa sztucznej inteligencji, tak aby nowa rewolucja cyfrowa, która dzieje się na naszych oczach, następowała w sposób kontrolowany, ale również pozbawiony nieuzasadnionych obaw.

Z poważaniem

Michał Kurek

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

Najważniejsze spostrzeżenia z raportu

W 2024 roku liczba firm, które zarejestrowały

przynajmniej jeden incydent

związany z cyberbezpieczeństwem, wzrosła o 16 p.p., do

83%.

Pojedynczy hakerzy i zorganizowane grupy przestępcze

stanowią największe realne zagrożenie dla cyfrowego bezpieczeństwa organizacji – tak uważa blisko połowa respondentów.

Wyciek danych za pośrednictwem złośliwego oprogramowania

wyprzedził kradzież danych poprzez phishing w rankingu największych cyberzagrożeń.

Ponad jedna trzecia respondentów wskazała

trudności z rekrutacją i utrzymaniem wykwalifikowanych pracowników

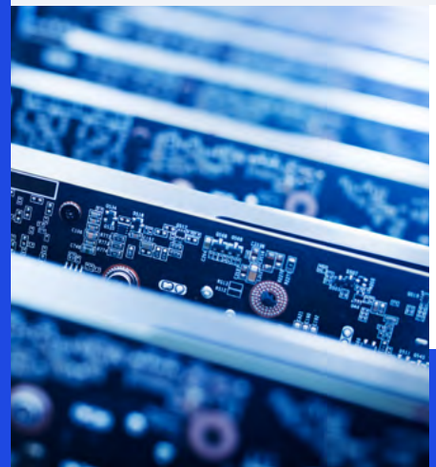
jako największy problem w osiągnięciu odpowiedniego poziomu cyberbezpieczeństwa.

W 41%

badanych firm

dyrektor IT

(Chief Information Officer) odpowiada za zapewnienie bezpieczeństwa informacji w organizacji.



Podobnie jak rok wcześniej, firmy zadeklarowały

najwyższy poziom dojrzałości

w obszarze bezpieczeństwa styku z siecią Internet oraz ochrony przed złośliwym oprogramowaniem.

Firmy planują

zwiększyć nakłady na inwestycje w cyberbezpieczeństwo

we wszystkich badanych obszarach w porównaniu z ubiegłym rokiem, a ich priorytety inwestycyjne pozostają niezmienione.

Aż 81%

firm korzystało z outsourcingu

przynajmniej jednej funkcji cyberbezpieczeństwa, przy czym wzrósł odsetek organizacji zlecających zewnętrznym usługodawcom tylko jedno takie zadanie.

Najbardziej popularnym modelem korzystania z AI są

usługi chmurowe.

68%

firm nie podjęło jeszcze działań

przygotowujących ich organizację do wdrożenia rozporządzenia

AI Act.

Ryzyko cyberataków jest największym wyzwaniem

dla polskich firm przy wdrożeniach systemów opartych na AI.

Kluczowym zagrożeniem są ataki typu jailbreak i prompt injection, które wskazało

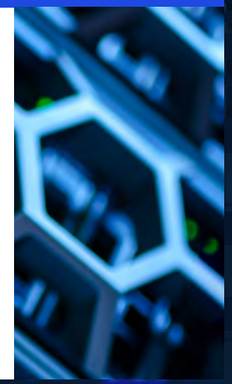
54%

respondentów.

Aż 56%

przedstawicieli badanych firm uważa, że

technologia AI spowoduje wzrost zagrożeń w cyberprzestrzeni.



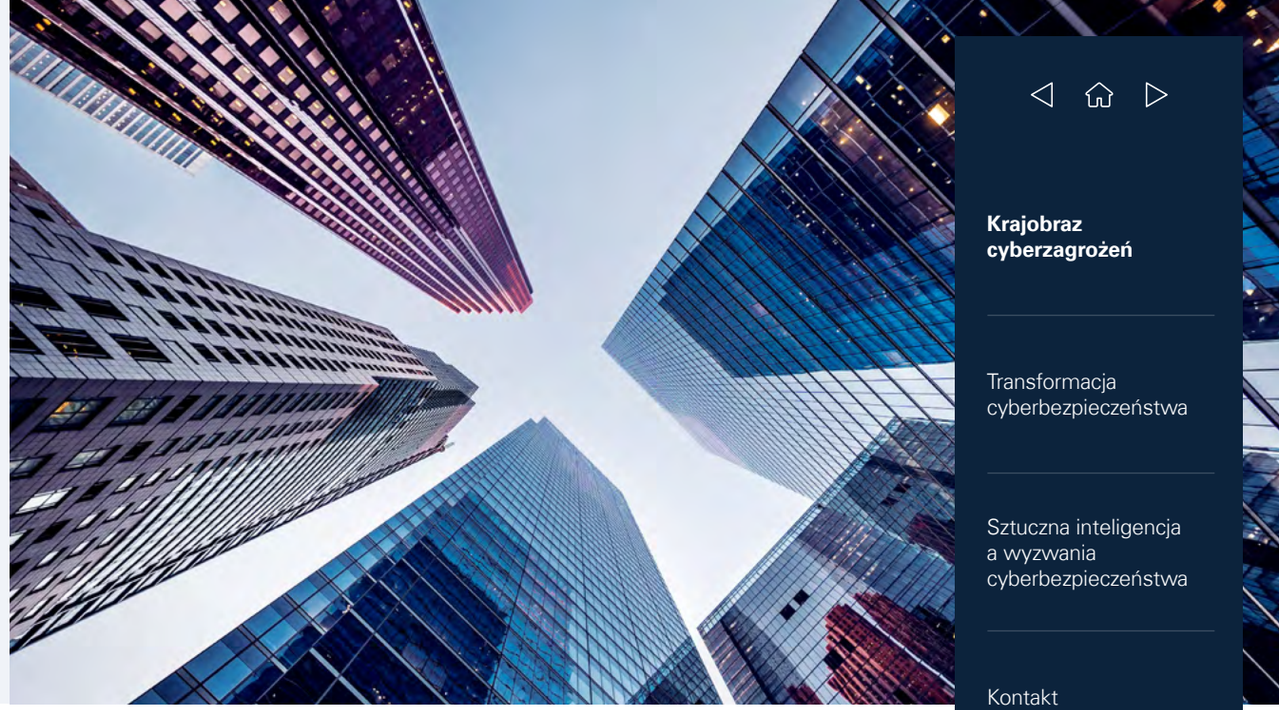
1 Krajobraz cyberzagrożeń

W dobie dynamicznego rozwoju technologii cyfrowych cyberzagrożenia uznawane są za jedno z kluczowych wyzwań współczesnego biznesu. Ich skala i złożoność wzrastają w miarę postępującej cyfryzacji przedsiębiorstw, administracji publicznej oraz codziennego życia. Cyberbezpieczeństwo, niezależnie od wielkości organizacji czy sektora działalności, traktowane jest jako fundament zapewniający stabilność operacyjną i ochronę danych, przyczyniając się tym samym do budowania zaufania klientów i partnerów biznesowych. W niniejszym rozdziale przeanalizowana została dynamika cyberzagrożeń oraz przedstawiono charakterystykę najczęściej występujących ataków i sylwetki ich sprawców.

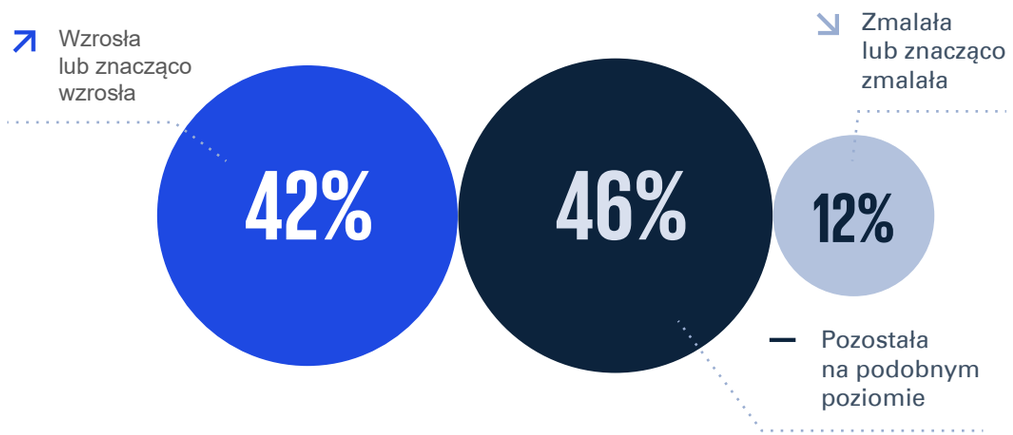
Tegoroczna edycja raportu wskazuje na istotny wzrost liczby prób cyberataków, które dotykają organizacje bez względu na ich jej wielkość. Największą intensywność incydentów odnotowuje się w dużych przedsiębiorstwach, ale problem obejmuje coraz szersze grono podmiotów. Potwierdzeniem tego jest znaczący spadek liczby organizacji, które nie doświadczyły żadnego ataku – w ciągu roku ich odsetek zmniejszył się dwukrotnie. Pomimo wzrostu skali zagrożeń poziom obaw wobec konkretnych osób i grup cyberprzestępczych utrzymuje się na stabilnym poziomie. Zjawisko to może wskazywać na rosnącą gotowość firm do radzenia sobie z incydentami oraz na większą profesjonalizację w obszarze cyberbezpieczeństwa. Zwiększa się również świadomość dotycząca typowych zagrożeń: phishing, choć wciąż postrzegany jako poważne ryzyko, po czterech latach ustąpił pierwszeństwa w rankingu największych ryzyk wyciekom danych spowodowanym działaniem złośliwego oprogramowania.

Niebezpieczna cyfrowa codzienność

Blisko połowa respondentów (46%) zadeklarowała, że liczba prób ataków na bezpieczeństwo cyfrowe pozostała na poziomie porównywalnym z poprzednim rokiem. Jest to jednak istotny spadek w porównaniu do wyników ubiegłorocznej edycji badania, w którym aż 60% wskazywało na brak zmiany w liczbie incydentów na przestrzeni dwóch lat. W bieżącej edycji odpowiedzi na ten temat straciły na znaczeniu na rzecz zarówno zaobserwowanego spadku, jak i wzrostu liczby ataków. Coraz więcej firm zauważa nasilenie cyberataków (wzrost o 8 p.p.), ale aż dwukrotnie więcej niż rok temu odnotowało zmniejszenie aktywności cyberprzestępców (wzrost z 6% na 12%).



Zmiana liczby zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Całkowita liczba prób ataków rośnie niezależnie od wielkości firmy, choć największą intensyfikację odnotowują duże przedsiębiorstwa (55% z nich zauważyło wzrost lub znaczny wzrost w porównaniu do 38% średnich firm i 40% małych firm). O zwiększeniu intensywności ataków świadczy również niemal dwukrotny spadek liczby organizacji, które nie odnotowały żadnego ataku – z 33% do 17%, co jest najniższym wynikiem w historii ośmiu edycji Barometru. Wzrost liczby cyberataków tłumaczy także gwałtowny wzrost odsetka przedsiębiorstw, które zarejestrowały od jednej do trzech prób prób (z 30% do 46%). Jednocześnie po osiągnięciu szczytu w 2022 roku odsetek organizacji, które zmierzyły się z 30 lub więcej cyberatakami, niezmiennie spada, osiągając obecnie jedynie 4% (niemal trzykrotnie mniej niż w poprzedniej edycji badania). To wszystko pozwala sądzić, że liczba cyberataków rośnie, choć strategia działania cyberprzestępców nieustannie się zmienia.

W 2024 roku 83% firm doświadczyło przynajmniej jednej próby cyberataku

Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa

	2024	2023	2022	2021	2020	2019
0	17%	33%	42%	31%	36%	46%
1-3	46%	30%	25%	23%	26%	29%
4-9	23%	17%	9%	23%	23%	14%
10-29	10%	9%	12%	14%	11%	6%
30+	4%	11%	12%	9%	4%	5%

Źródło: KPMG w Polsce na podstawie badania ankietowego.

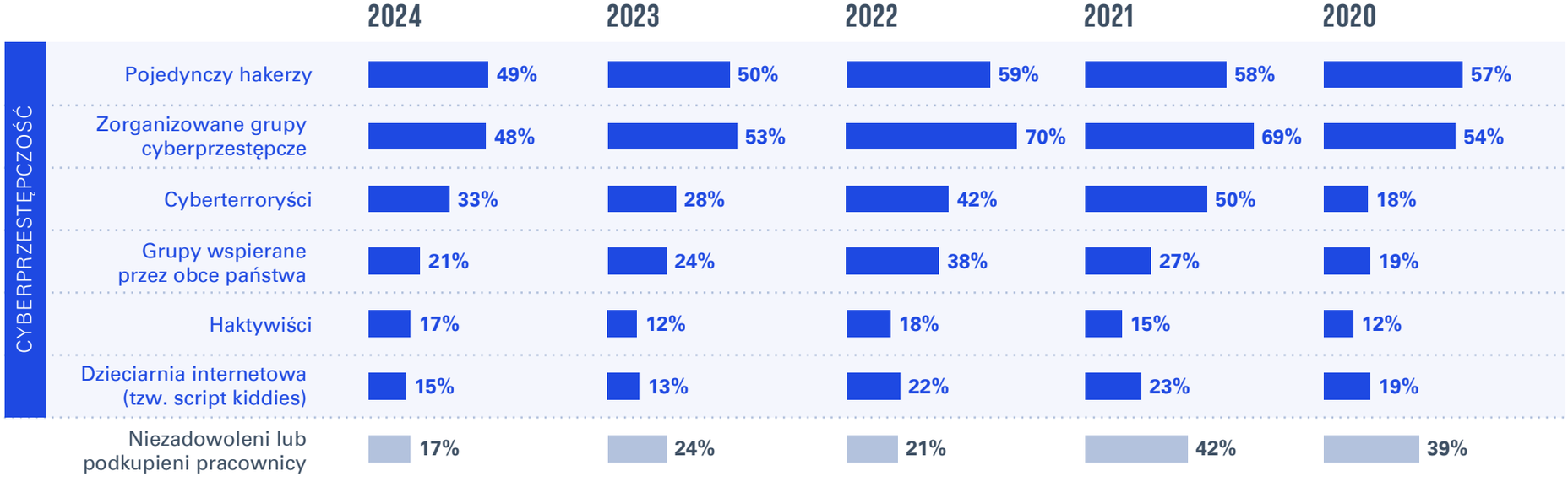
Cyberprzestępca, czyli kto?

Po znacznym spadku poczucia zagrożenia przedsiębiorców ze strony cyberprzestępców w okresie 2022-2023, bieżąca edycja przynosi stabilizację tego trendu. Poczucie ryzyka pozostaje stosunkowo niskie w porównaniu do lat ubiegłych, ale w ciągu ostatniego roku nie uległo znaczącym zmianom. Obserwacja tych tendencji w kolejnych latach pozwoli odpowiedzieć na pytanie, czy wynika to z osłabienia czujności firm, czy też ze wzrostu świadomości i wdrażania bardziej zaawansowanych zabezpieczeń.

Wciąż na najwyższym poziomie, podobnie jak w zeszłym roku, utrzymują się obawy dotyczące ataków hakerów działających indywidualnie oraz zorganizowanych grup cyberprzestępczych, które stanowią realne zagrożenie według około połowy przedsiębiorstw. Niewielki wzrost obaw wiąże się natomiast z działaniami cyberterrorystów, haktywistów kierujących się w swoich działaniach ideami społecznymi i politycznymi, a także amatorów, tzw. dzieciarni internetowej, nieposiadających zaawansowanej wiedzy programistycznej. Grupy te zajmują odpowiednio trzecie, czwarte i piąte miejsce w rankingu zagrożeń.

Poczucie zagrożenia ze strony grup wspieranych przez obce państwa stopniowo maleje po osiągnięciu szczytu w 2022 roku, spowodowanego wzrostem aktywności rosyjskich hakerów w związku z wojną w Ukrainie. Największy, choć wciąż stosunkowo niski spadek obaw (o 7 p.p.) odnotowano w odniesieniu do niezadowolonych lub podkupionych pracowników.

Grupy stanowiące realne zagrożenie dla organizacji



Źródło: KPMG w Polsce na podstawie badania ankietowego.

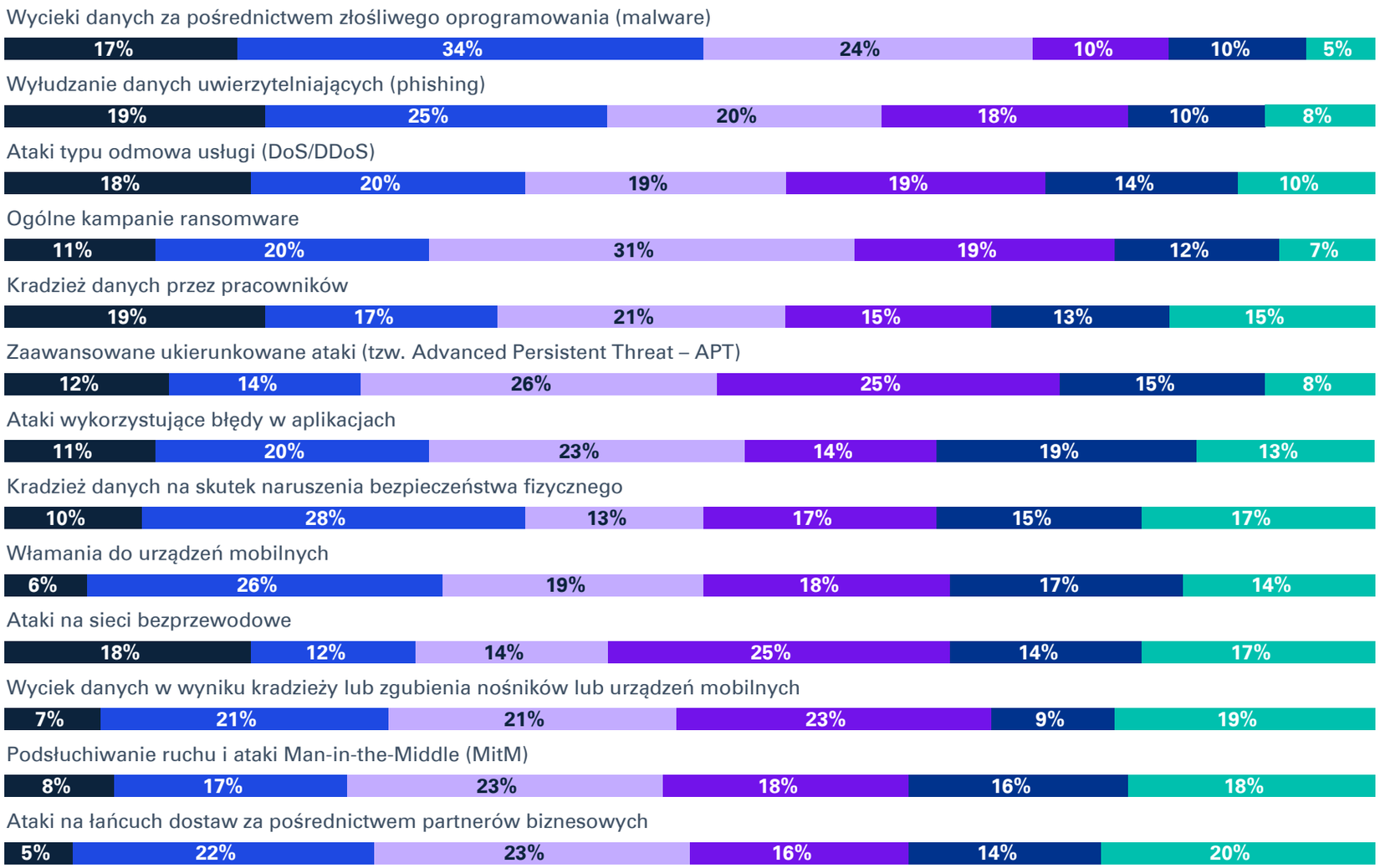
Mapa ryzyk

W edycji 2025 ranking najpoważniejszych cyberzagrożeń ukształtował się inaczej niż w poprzednich czterech edycjach, w których phishing zdeklasował inne rodzaje ataków. W tegorocznym badaniu nadal wiele firm uznało go za główne ryzyko, jednak ostatecznie najwyższą rangę uzyskały wycieki danych za pośrednictwem złośliwego oprogramowania. Wskazuje to na potencjalny wzrost tego typu incydentów w ciągu ostatniego roku oraz na skuteczność kampanii informacyjnych dotyczących phishingu i jego identyfikacji.

Na trzecim miejscu znalazły się ataki typu odmowa usługi, co stanowi najbardziej zauważalną zmianę w polskim krajobrazie cyberzagrożeń w porównaniu z historycznymi wynikami, gdzie ataki te były jednymi z ostatnich na liście obaw. Na kolejnych miejscach znalazły się ogólne kampanie ransomware i kradzież danych przez pracowników. Spadek tej ostatniej pozycji (z trzeciego na piąte miejsce) jest zgodny z wynikami dotyczącymi poczucia zagrożenia ze strony konkretnych grup, które pokazują, że pracodawcy mniej obawiają się cyberprzestępczości ze strony własnych pracowników. Wciąż jednak istnieje liczna grupa firm, która nadała temu zagrożeniu najwyższą wagę (19%). Mimo niższego miejsca w rankingu ataki na sieci bezprzewodowe są również uznawane za duże zagrożenie przez znaczną część firm (18%). Choć zajmują czwarte miejsce od końca, wzrost liczby najwyższych ocen na skali określającej siłę zagrożenia jest znaczny (o 13 p.p.).

Za najmniej zagrażające uznawane są ataki na łańcuch dostaw za pośrednictwem partnerów biznesowych, jednak warto zauważyć, że 5% wskazań dla najwyższej oceny ryzyka to pięciokrotny wzrost w porównaniu z poprzednim rokiem. Z kolei 20% firm, które oceniły, że takie ryzyko nie istnieje, to spadek aż o 18 p.p. w porównaniu z wcześniejszą edycją badania. Być może nowe regulacje (jak NIS2 czy DORA) kładące nacisk na ochronę przed tymi zagrożeniami podniosły poziom świadomości polskich przedsiębiorstw w tym zakresie.

Cyberzagrożenia stanowiące największe ryzyko dla organizacji



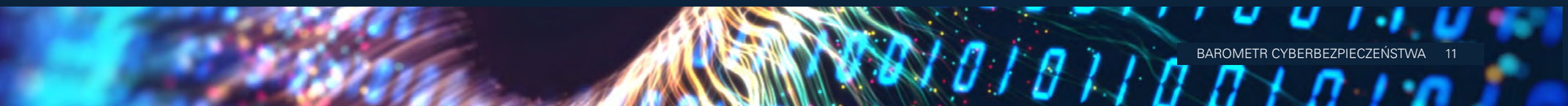
Źródło: KPMG w Polsce na podstawie badania ankietowego.

2 Transformacja cyberbezpieczeństwa

Wraz z rozwojem technologii katalog zagrożeń cyfrowych zmienia się w sposób dynamiczny, co wymaga nieustannego doskonalenia rozwiązań zapewniających cyberbezpieczeństwo. Analiza wyników badania przeprowadzonego na potrzeby tegorocznej edycji raportu pozwala przyjrzeć się trendom i zmianom, które zachodzą w obszarze odpowiedzialności, dojrzałości zabezpieczeń oraz planowanych inwestycji w cyberbezpieczeństwo. Identyfikacja głównych ograniczeń na drodze do osiągnięcia pożądanego poziomu bezpieczeństwa oraz znajomość funkcji i procesów realizowanych przez dostawców zewnętrznych (outsourcing) otwierają drzwi do lepszego zrozumienia wyzwań, przed którymi stoją organizacje w zmieniającym się środowisku cyfrowym.

Zabezpieczenia chroniące firmy przed cyberzagrożeniami są rozwijane, co znajduje potwierdzenie w planach inwestycyjnych oraz umiarkowanie pozytywnej ocenie dojrzałości tych rozwiązań na obecnym etapie. Zmienia się także podejście do planowania i realizacji rozwiązań w organizacjach. Choć outsourcing cyberbezpieczeństwa wciąż pozostaje popularny, rośnie odsetek firm, które kupują z zewnątrz jedynie pojedyncze usługi.

Podobnie jak w ubiegłym roku, największym wyzwaniem w zapewnianiu odpowiedniego poziomu zabezpieczeń pozostaje dla badanych firm problem z zatrudnianiem i utrzymaniem wykwalifikowanych specjalistów. Optymistycznym sygnałem jest jednak fakt, że taką trudność wskazało mniej firm niż w poprzedniej edycji badania.



Odpowiedzialni za cyberbezpieczeństwo

Z najnowszej edycji badania wynika, że niezmiennie kluczową rolę w zakresie cyberbezpieczeństwa pełnią dyrektorzy IT lub CIO (Chief Information Officer). W porównaniu do poprzedniego roku odnotowano jednak spadek o 6 p.p. liczby organizacji wskazujących na takie rozwiązanie organizacyjne. Można wnioskować, że stało się to na rzecz wzmocnienia roli CEO oraz rozszerzenia zakresu kompetencji stanowisk, które standardowo nie zajmowały się cyberbezpieczeństwem.

W porównaniu do poprzedniej edycji badania nie zmienił się odsetek firm, które nie przypisały formalnie odpowiedzialności za cyberbezpieczeństwo żadnej z funkcji w organizacji – nadal wynosi 11%.

Osoby odpowiedzialne za bezpieczeństwo informacji w organizacji

	2024	2023	2022	2021	2020
Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT	41%	47%	45%	47%	48%
Prezes zarządu (CEO)	19%	16%	17%	15%	22%
Inne stanowisko w organizacji niż powyższe	14%	8%	8%	5%	4%
Niezależna dedykowana funkcja (CSO/CISO)	13%	12%	8%	14%	11%
Odpowiedzialność przypisana w strukturach globalnych poza Polską	2%	6%	5%	9%	2%
Brak formalnego przypisania odpowiedzialności	11%	11%	17%	10%	13%

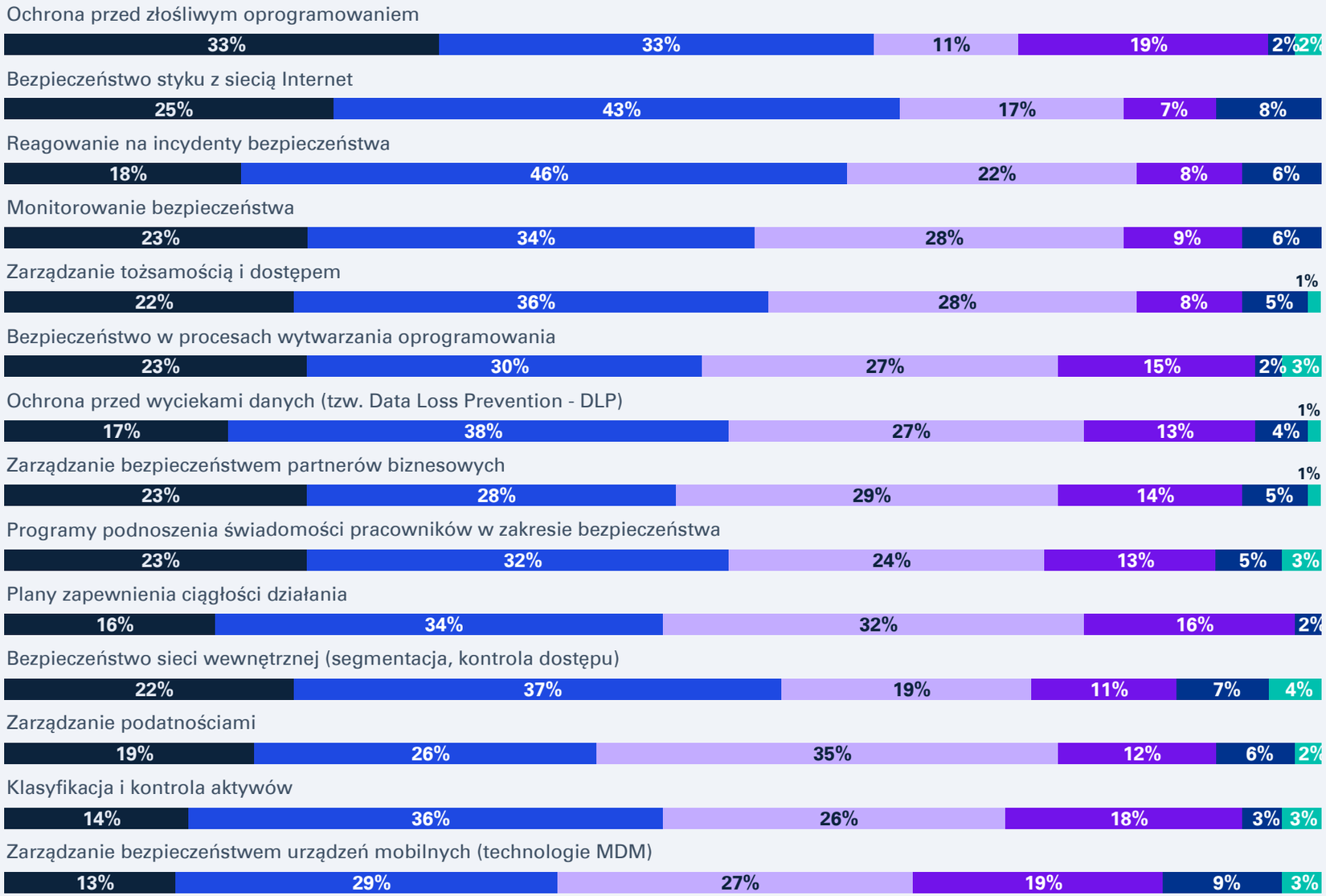
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Nieustanna wędrówka ku dojrzałości cyfrowej

W 11 na 14 obszarów zarządzania cyberbezpieczeństwem dojrzałość jest oceniana niżej niż w poprzednim roku. Zakładając, że firmy rozwijają swoje zabezpieczenia, taki stan rzeczy może wynikać ze wzrostu świadomości w zakresie cyberbezpieczeństwa oraz dynamicznego rozwoju nowych rodzajów cyberzagrożeń. Mimo to najbardziej dojrzałe obszary są podobne jak w poprzedniej edycji badania – najwyższą średnią ocenę w kategorii dojrzałości rozwiązań z zakresu cyberbezpieczeństwa uzyskała ochrona przed złośliwym oprogramowaniem oraz bezpieczeństwo styku z siecią Internet. Co istotne, mimo wysokiej średniej, obie te grupy rozwiązań zostały ocenione jako w pełni dojrzałe w mniejszym stopniu – spadek wynosi odpowiednio 11 p.p. i 20 p.p. w porównaniu z rokiem poprzednim. Kolejnymi obszarami w rankingu oceny dojrzałości zabezpieczeń są te dotyczące reagowania na incydenty bezpieczeństwa, monitorowania bezpieczeństwa oraz zarządzania tożsamością i dostępem, które uzyskały bardzo podobne średnie oceny.

Zarządzanie bezpieczeństwem urządzeń mobilnych pozostaje obszarem ocenianym najniżej – zarówno na poziomie średnim, jak i pełnym (jedynie 13% organizacji osiągnęło pełną dojrzałość). Warto zauważyć, że odsetek pełnej dojrzałości firm w tym zakresie spadł o 5 p.p. w porównaniu do ubiegłego roku. Niewiele wyższe średnie oceny przyznano klasyfikacji i kontroli aktywów oraz zarządzaniu podatnościami, co może wskazywać na wzrost wyzwań w tych kategoriach, które rok wcześniej były oceniane jako lepiej zabezpieczone.

Ocena dojrzałości poszczególnych obszarów zabezpieczeń w organizacji



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Inwestycje w bezpieczną przyszłość

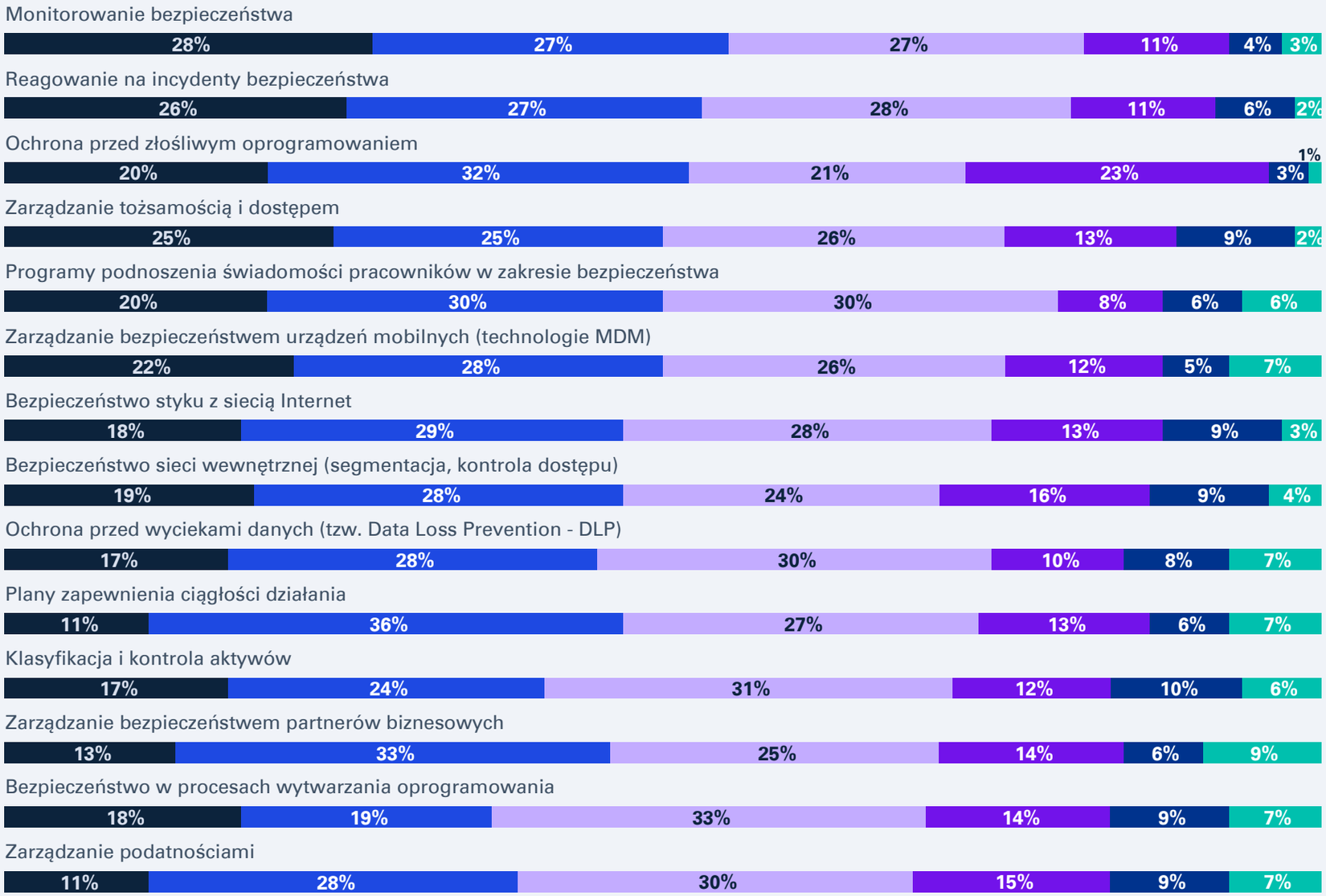
Inwestycje w cyberbezpieczeństwo obejmują zarówno wdrażanie nowoczesnych technologii i strategii ochrony, jak i rozwijanie kompetencji zespołów IT, aby sprostać dynamicznym zmianom i minimalizować ryzyko zakłóceń w działalności firmy. Zabezpieczenia te chronią przed utratą danych i minimalizują zaburzenia operacyjne, co z kolei pomaga budować zaufanie klientów i partnerów biznesowych, a w dzisiejszych realiach stanowi istotną przewagę konkurencyjną. W badaniu przeprowadzonym na potrzeby raportu „KPMG 2024 CEO Outlook”[1] 48% polskich liderów największych firm zadeklarowało zwiększenie inwestycji w cyberbezpieczeństwo, koncentrując się szczególnie na ochronie przed zagrożeniami związanymi ze sztuczną inteligencją.

Firmy planują większe inwestycje w cyberbezpieczeństwo niż w ubiegłym roku – wszystkie analizowane obszary uzyskały wyższą średnią rangę w porównaniu do poprzedniej edycji badania. Jest to spójne z wynikami dotyczącymi dojrzałości zabezpieczeń, której spadek najwyraźniej skłania organizacje do nowych planów inwestycyjnych. W 2025 roku firmy będą przede wszystkim koncentrować się na monitorowaniu bezpieczeństwa oraz reagowaniu na incydenty. Ważnym obszarem będzie także rozwój ochrony przed złośliwym oprogramowaniem oraz zarządzanie tożsamością i dostępem, co wskazuje na rosnącą świadomość zagrożeń i potrzebę szybkiej reakcji na ataki. W porównaniu do poprzedniego badania trzy główne priorytety inwestycyjne pozostały bez zmian. Na podstawie średniej ważonej oceny respondentów obszar zarządzania tożsamością i dostępem awansował o cztery miejsca w rankingu, co podkreśla znaczenie ochrony danych użytkowników oraz precyzyjnego nadzoru nad dostępem do zasobów.

Najmniejsze nakłady inwestycyjne planowane są w zakresie zarządzania podatnościami, co jest bardzo alarmującym wnioskiem w zestawieniu z niską oceną dojrzałości tego krytycznego dziś obszaru cyberbezpieczeństwa. Nieco wyższe inwestycje planowane są w obszarze bezpieczeństwa wytwarzania oprogramowania oraz zarządzania bezpieczeństwem partnerów biznesowych. Nie oznacza to jednak, że firmy zaniedbują te dziedziny – to właśnie w przypadku drugiego i trzeciego z najniżej ocenianych obszarów nastąpił największy przyrost inwestycji w porównaniu do poprzedniego badania. Większy wzrost planowanych nakładów finansowych odnotowano jedynie w przypadku programów podnoszenia świadomości pracowników w zakresie cyberbezpieczeństwa, co pokazuje, że firmy różnicują swoją strategię ochrony, planując działania prewencyjne.

1 „KPMG 2024 CEO Outlook. Adaptacja do zmian to kształtowanie przyszłości”, KPMG w Polsce, 2024.

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



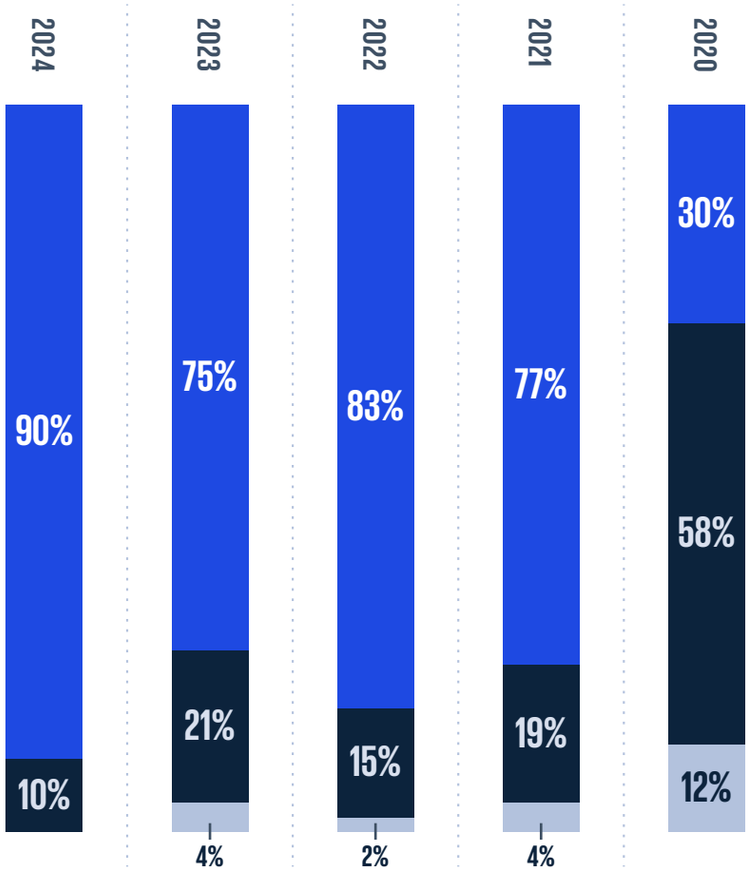
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Jeden krok w przód, dwa kroki w tył

Ocena dojrzałości zabezpieczeń przed incydentami cyfrowymi zmieniła się na przestrzeni ostatnich pięciu lat. Na tę sytuację bez wątpienia wpływ miały nie tylko dynamiczny rozwój technologii, ale również zawirowania geopolityczne i gospodarcze. Jeszcze na początku tej dekady przeważała opinia o pełnej dojrzałości zabezpieczeń w „większości analizowanych obszarów". Obecnie ten pogląd reprezentantów badanych firm ustąpił miejsca opinii, że są one dojrzałe „najwyżej w połowie".

W tegorocznej edycji badania tylko jedna na dziesięć firm zadeklarowała pełną dojrzałość w większości obszarów zabezpieczeń. Jest to wynik o 11 p.p. niższy niż w poprzednim roku. Dodatkowo, po raz pierwszy od 2020 roku, żadna z badanych firm nie stwierdziła pełnej dojrzałości we wszystkich analizowanych obszarach. Jest to wyraźny sygnał narastającego tempa rozwoju nowych wyzwań w zakresie cyberbezpieczeństwa oraz rosnącej świadomości konieczności dalszego rozwoju zabezpieczeń.

Dojrzałość firm w zakresie zabezpieczeń



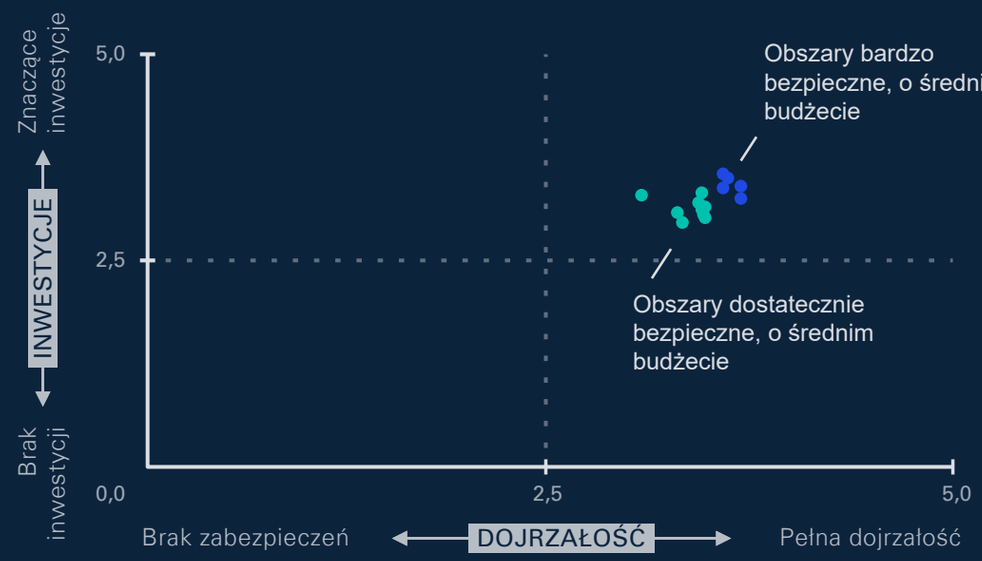
- Pełna dojrzałość najwyżej w połowie analizowanych obszarów
- Pełna dojrzałość w większości analizowanych obszarów
- Pełna dojrzałość w każdym z analizowanych obszarów

Źródło: KPMG w Polsce na podstawie badania ankietowego.

Trafnie określone priorytety

Matryca obrazująca poziom dojrzałości rozwiązań oraz planowanych inwestycji w cyberbezpieczeństwo wskazuje, że wszystkie typy zabezpieczeń objęte analizą w badanych firmach są uznawane za dostatecznie lub bardzo bezpieczne (dojrzałe). Poziom deklarowanych inwestycji w ich rozwój pozostaje dostateczny – w przeciwieństwie do ubiegłego roku nie zidentyfikowano zagrożenia ryzykiem niedofinansowania. Oznacza to, że firmy, zgodnie z deklaracjami z poprzedniej edycji badania, zrealizowały w ciągu ostatniego roku zwiększone inwestycje na cyberbezpieczeństwo.

Obszarem o relatywnie najniższej dojrzałości na tle pozostałych grup rozwiązań, podobnie jak rok wcześniej, pozostaje zarządzanie bezpieczeństwem urządzeń mobilnych. Jednak widoczny jest trend rozwojowy – w badanych firmach deklarowany poziom inwestycji w ten obszar spowodował, że nie jest on już zagrożony niedofinansowaniem.



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Obszary bardzo bezpieczne, o średnim budżecie:

- ochrona przed złośliwym oprogramowaniem,
- bezpieczeństwo styku z siecią Internet,
- reagowanie na incydenty bezpieczeństwa,
- monitorowanie bezpieczeństwa,
- zarządzanie tożsamością i dostępem.

Obszary dostatecznie bezpieczne, o średnim budżecie:

- bezpieczeństwo w procesach wytwarzania oprogramowania,
- ochrona przed wyciekami danych (tzw. Data Loss Prevention – DLP),
- zarządzanie bezpieczeństwem partnerów biznesowych,
- programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa,
- bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu),
- plany zapewnienia ciągłości działania,
- zarządzanie podatnościami,
- klasyfikacja i kontrola aktywów,
- zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM).

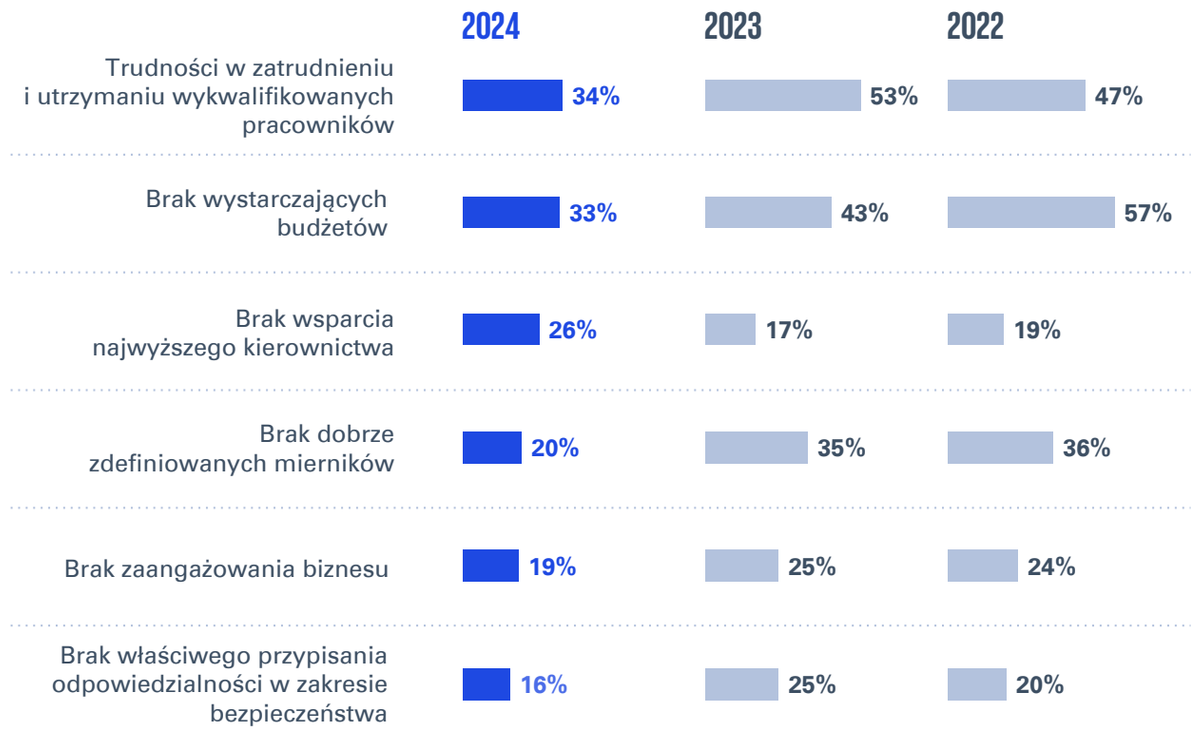
Bezpieczeństwo cyfrowe pod presją wyzwań

W 2024 roku największym wyzwaniem wskazywanym przez respondentów były trudności w zatrudnieniu i utrzymaniu wykwalifikowanych specjalistów, co potwierdziło 34% badanych. W porównaniu do 2023 roku odsetek ten zmniejszył się znacząco, o 19 p.p. Można przypuszczać, firmy zaczynają lepiej zarządzać tym obszarem, choć nadal stanowi on kluczowe ograniczenie w osiąganiu odpowiedniego poziomu cyberbezpieczeństwa.

Drugim najczęściej wymienianym wyzwaniem w 2024 roku był brak wystarczających budżetów, który dotyczył 33% respondentów. Również ten problem stracił na znaczeniu w porównaniu do poprzednich lat – w 2023 roku wskazywało go 43% badanych, a w 2022 roku 57%. Prawdopodobnie wynika to ze wzrostu świadomości i traktowania cyberbezpieczeństwa jako priorytetu w firmowych budżetach.

Warto również zwrócić uwagę na wzrost znaczenia bariery w postaci braku wsparcia najwyższego kierownictwa (26% w 2024 roku w porównaniu do 17% w 2023 roku). Pozostałe ograniczenia były wskazywane przez mniejszą liczbę respondentów niż w dwóch poprzednich edycjach, co może sugerować, że organizacje stopniowo usprawniają swoje strategie zarządzania bezpieczeństwem.

Główne ograniczenia dla uzyskania oczekiwanego poziomu zabezpieczeń w organizacji



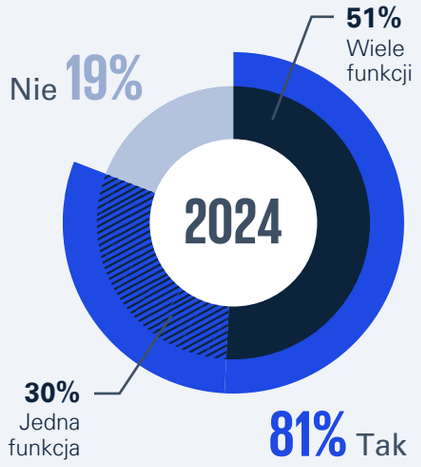
Źródło: KPMG w Polsce na podstawie badania ankietowego.

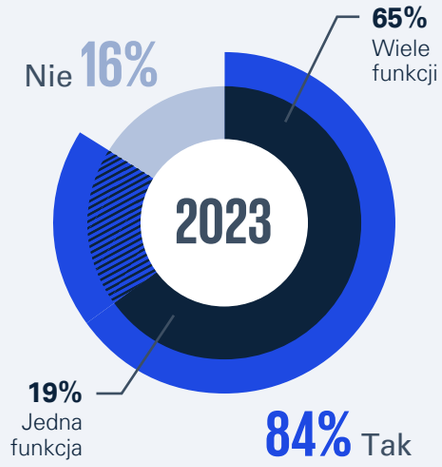
Zewnętrzni sojusznicy w drodze do bezpieczeństwa cyfrowego

Trend zlecania zadań związanych z cyberbezpieczeństwem zewnętrznym dostawcom usług jest nadal powszechny – w 2024 roku dotyczył on 81% badanych organizacji. Przedsiębiorstwa najczęściej stosują outsourcing dla więcej niż jednej funkcji bezpieczeństwa, jednak w porównaniu do poprzedniego roku wzrosła liczba firm zlecających tylko jedno zadanie. Odsetek ten zwiększył się o 11 p.p. Taki trend może wynikać zarówno z rosnącej świadomości cyberzagrożeń, jak i z poprawy wewnętrznych kompetencji zespołów IT, które pozwalają firmom przejąć odpowiedzialność za szerszy zakres działań związanych z bezpieczeństwem.

Najczęściej zlecanym zewnętrznym usługodawcom zadaniem jest monitorowanie bezpieczeństwa, które zadeklarowało 40% organizacji, co stanowi wzrost o 5 p.p. w porównaniu do poprzedniej edycji badania. Prawie jedna trzecia firm korzysta z outsourcingu w zakresie analizy złośliwego oprogramowania oraz przeglądów kodu źródłowego. Wśród outsourcingowanych kompetencji dominują techniczne, które trudniej jest budować wewnętrznie, m.in. dlatego, że bardzo często jest to nieopłacalne.

Korzystanie z outsourcingu





Źródło: KPMG w Polsce na podstawie badania ankietowego.

Funkcje lub procesy bezpieczeństwa realizowane przez zewnętrznych dostawców

6 Sztuczna inteligencja a wyzwania cyberbezpieczeństwa

Sztuczna inteligencja odgrywa coraz większą rolę w codziennym życiu, co dla biznesu oznacza rewolucyjne zmiany. Jej zdolność do przetwarzania ogromnych ilości danych, automatyzacji procesów i przewidywania złożonych zjawisk stwarza ogromne możliwości, ale także rodzi nowe zagrożenia, takie jak manipulacja danymi, automatycznie generowane ataki czy ułatwione przełamywanie zabezpieczeń. Te nowe ryzyka stają się realnym wyzwaniem dla zachowania płynności operacyjnej organizacji.

Jednak, tak jak w przypadku innych dynamicznie upowszechniających się nowych technologii, szanse związane z wykorzystaniem AI przewyższają zagrożenia. Sztuczna inteligencja znajduje szerokie zastosowanie w firmach, szczególnie w rozwiązaniach chmurowych i tych dostarczanych przez zewnętrznych dostawców. Jednym z obszarów o największym potencjale rozwoju jest obsługa klienta, w którym technologia ta umożliwia poprawę jakości interakcji oraz optymalizację kosztów.

Jednocześnie sztuczna inteligencja budzi liczne obawy, szczególnie w kontekście cyberataków, które okazują się największym wyzwaniem. Dla wielu firm stanowią one poważniejszy problem niż koszty wdrożenia czy brak kontroli nad wykorzystaniem AI przez pracowników. Obawy podkreślane przez przedsiębiorstwa pozwalają wnioskować, że kluczowym czynnikiem wpływającym na decyzję o wykorzystaniu konkretnego rozwiązania AI jest poziom zabezpieczeń oraz transparentność w wykorzystaniu danych przez wybrany model.

Warto zauważyć, że w badaniu jedynie 14% przedsiębiorstw zadeklarowało, że obecnie spełnia wymogi rozporządzenia AI Act. Dodatkowo co czwarta badana firma nie podjęła jeszcze żadnych działań w tym zakresie ani nie określiła planów działania związanych z rozporządzeniem. Tymczasem zapoznanie się z dobrymi praktykami i wdrożenie odpowiednich procedur jest kluczowe dla zmniejszenia liczby cyberzagrożeń związanych z użytkowaniem AI, które – zdaniem większości respondentów – wzrosną wraz z upowszechnieniem i rozwojem opartych na niej rozwiązań.

Rozpoczęła się kolejna rewolucja technologiczna, która będzie miała dalej idące konsekwencje dla świata niż rozwój sieci Internet. ChatGPT spopularyzował się w rekordowym tempie – milion użytkowników w zaledwie 5 dni. Dziś wszyscy zastanawiają się, jak będzie wyglądała nasza przyszłość w dobie AI. Jak w przypadku każdej nowej technologii, pojawiają się również obawy na temat ryzyk – w szczególności w zakresie cyberbezpieczeństwa.

Na tematykę bezpieczeństwa AI warto spojrzeć z czterech perspektyw:

- *Jak sztuczna inteligencja może pomóc w zapewnieniu bezpieczeństwa w firmach?*
- *Jakie zagrożenia wiążą się z wykorzystywaniem przez firmy systemów AI?*
- *Jakie zagrożenia wiążą się z korzystaniem przez pracowników z zewnętrznych usług AI?*
- *Jakie nowe zagrożenia generuje AI w rękach cyberprzestępców?*

Tak jak w zastosowaniach biznesowych, również w cyberbezpieczeństwie szybkie wnioskowanie na podstawie dostępu do dużych zbiorów danych może przynieść ogromne korzyści. Identyfikacja podejrzanych działań użytkowników w sieci i systemach informatycznych przez dostosowane do specyfiki firmy modele AI może wyrównać siły w nierównej dotychczas walce z cyberprzestępcami. AI trwale zmieni oblicze cyberbezpieczeństwa w najbliższych latach.

Tak jak i modeli biznesowych… Wdrażanie systemów AI wiąże się jednak z koniecznością przedefiniowania podejścia do zapewnienia bezpieczeństwa tych aplikacji. Oczywiście zostaje cały wachlarz cyberzagrożeń specyficznych dla systemów informatycznych. Natomiast dochodzi jeszcze m.in. konieczność zabezpieczenia procesu trenowania modeli AI, który jest niezwykle wrażliwy, a mimo to najczęściej realizowany w rozluźniony pod względem bezpieczeństwa sposób, charakterystyczny dla środowisk rozwojowych.

Sztuczna inteligencja zwiększa również zagrożenie ze strony pracowników naruszających poufność danych wysyłanych do zewnętrznych systemów AI, łamiących prawa autorskie lub powielających nieprawdziwe informacje w bezkrytyczny sposób, ufając odpowiedziom uzyskanym od modeli LLM. Są oni również w jeszcze większym stopniu podatni na zaawansowane (wykorzystujące materiały deep fake) i automatycznie sprofilowane cyberataki wspierane przez AI. Bardziej niż kiedykolwiek, firmy muszą dbać o świadomość pracowników na temat nowych zagrożeń.

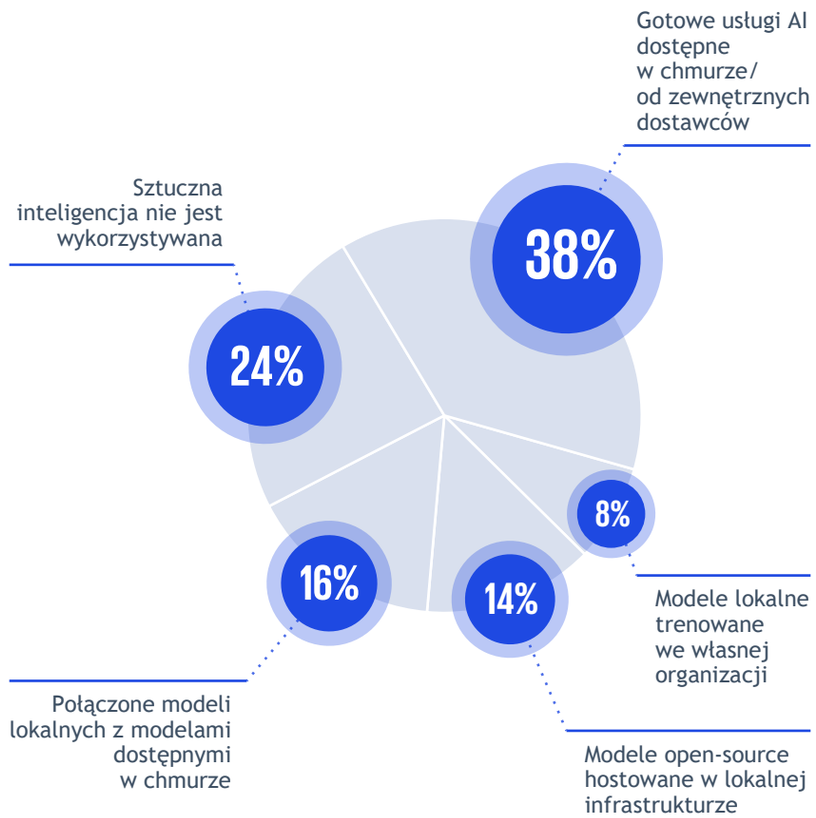
Michał Kurek

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

Arsenał rozwiązań sztucznej inteligencji

Sztuczna inteligencja znajduje szerokie zastosowanie w firmach, choć preferencje w wyborze rozwiązań są wyraźnie zróżnicowane. Najwięcej organizacji (38%) korzysta z gotowych usług AI dostępnych w chmurze lub od zewnętrznych dostawców, co wskazuje na popularność łatwych do wdrożenia i skalowalnych rozwiązań. Podejście hybrydowe, łączące modele lokalne z chmurowymi, zostało wskazane przez 16% firm, co podkreśla ich chęć wykorzystania elastyczności obu rozwiązań. Mniej popularne są modele open-source hostowane lokalnie (14%) oraz modele trenowane wewnętrznie przez organizacje (8%), które wymagają większych zasobów technicznych i finansowych. Prawie jedna czwarta badanych firm przyznała, że nie wykorzystuje w ogóle sztucznej inteligencji, co może wynikać z ograniczeń technologicznych, kosztowych lub braku świadomości korzyści, jakie mogą płynąć z wdrożenia takich rozwiązań.

Rodzaje rozwiązań AI wykorzystywane w firmach



Źródło: KPMG w Polsce na podstawie badania ankietowego.

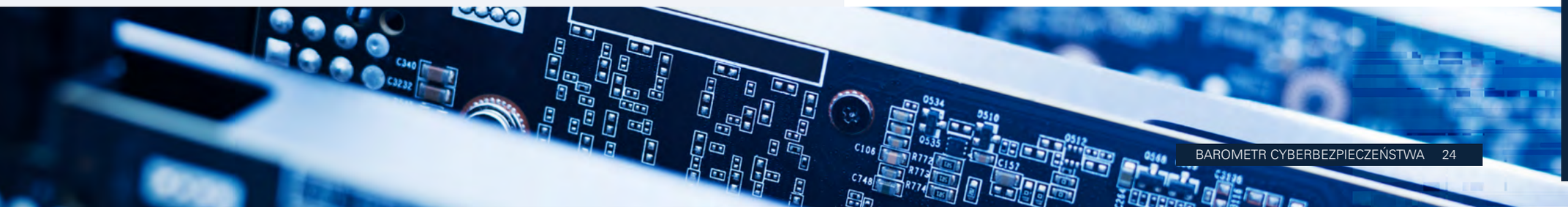
Sztuczna inteligencja jest wykorzystywana w różnych obszarach działalności organizacji. Wśród firm, które wdrożyły technologię AI, największy potencjał dostrzegany jest w obszarze wsparcia procesów związanych z obsługą klienta – wskazało tak 37% respondentów. Jest to zgodne z globalnymi trendami, które pokazują, że chatboty, wirtualni asystenci i systemy analizy opinii klientów są szeroko stosowane w celu poprawy jakości obsługi i redukcji kosztów operacyjnych.

Automatyzacja zadań, takich jak generowanie kodu źródłowego, analiza logów systemowych czy wczesne wykrywanie problemów technicznych, to przykłady zastosowań, które pomagają zwiększyć efektywność działów IT. To w tym obszarze często integruje się rozwiązania AI z mechanizmami cyberbezpieczeństwa, na przykład w zakresie wykrywania anomalii w ruchu sieciowym czy automatycznego reagowania na incydenty. Wykorzystywanie sztucznej inteligencji do wsparcia działów IT wskazało 34% ankietowanych.

Stosowanie sztucznej inteligencji bezpośrednio w obszarze cyberbezpieczeństwa zadeklarowało jedynie 13% respondentów. Może to wynikać z faktu, że wdrożenie systemów AI w tym zakresie wymaga nakładów finansowych, dostępu do zaawansowanych danych oraz wyspecjalizowanego personelu, co wciąż stanowi barierę dla wielu organizacji. Można jednak zakładać, że dynamiczny rozwój narzędzi opartych na AI oraz rosnąca liczba incydentów spowodują, że w najbliższych latach technologia ta będzie coraz częściej wykorzystywana jako kluczowe wsparcie w ochronie przed zagrożeniami cyfrowymi.

Obszary działalności firm wspierane przez sztuczną inteligencję

Źródło: KPMG w Polsce na podstawie badania ankietowego.



Najistotniejsze wyzwania dla wdrożenia rozwiązań opartych na AI

Źródło: KPMG w Polsce na podstawie badania ankietowego.

Bezpieczeństwo przede wszystkim

Wyniki badania potwierdzają, że sztuczna inteligencja wzbudza wiele obaw, szczególnie w obszarach etyki i bezpieczeństwa. Wyzwania te okazały się ważniejsze niż kwestie związane z wydajnością modeli czy kosztami implementacji. Przedstawiciele firm, proszeni o wskazanie maksymalnie trzech najistotniejszych wyzwań, równie często podkreślali ryzyko cyberataków na systemy AI, możliwość naruszania praw autorskich, brak odpowiedniego nadzoru nad wykorzystaniem sztucznej inteligencji w organizacji oraz niski poziom świadomości pracowników dotyczący bezpiecznego korzystania z AI.

Możliwe problemy dotyczą więc zarówno obszarów zależnych od wybranego systemu AI, jak i tych spoza samego narzędzia. Obejmują zagadnienia od braku odpowiednich zabezpieczeń oprogramowania, przez nieprawidłowe wytrenowanie modeli skutkujące niewłaściwym wykorzystaniem przekazanych danych, po nieodpowiednie procedury organizacyjne w firmie. Choć kwestie organizacyjne można rozwiązać poprzez szkolenia i wdrożenie odpowiednich funkcji nadzorczych, obawy związane z postrzeganiem AI jako „czarnej skrzynki" pozostają istotnym wyzwaniem. Brak przejrzystości modeli w zakresie wykorzystania danych podkreśla, jak kluczowym kryterium przy wyborze rozwiązań AI jest ich transparentność.

Zawodność systemów AI oraz trudności w ich implementacji i konfiguracji były istotne dla jedynie 10% dużych firm, w porównaniu z 20% małych i 26% średnich przedsiębiorstw. Wynik ten wskazuje, że największe organizacje dostrzegają większe korzyści wynikające z integracji AI z codzienną działalnością biznesową. Zaskakujące jest jednak stosunkowo niskie miejsce wyzwań związanych z wymogami rozporządzenia AI Act. Mimo to niemal co piąta firma uznaje je za istotne, przy czym trzy czwarte tych organizacji to małe i średnie przedsiębiorstwa.

Systemy sztucznej inteligencji otwierają przed biznesem nowe perspektywy rozwoju, umożliwiając automatyzację procesów, zwiększenie efektywności operacyjnej oraz tworzenie innowacyjnych rozwiązań dostosowanych do specyficznych potrzeb organizacji.

Przedsiębiorstwa mogą korzystać z gotowych, wytrenowanych modeli, takich jak LLM, opracowywać własne modele na bazie wewnętrznych danych lub dostosowywać istniejące modele poprzez fine-tuning. Każde z tych podejść ma swoje zalety – gotowe modele pozwalają na szybkie wdrożenie rozwiązań, własne modele zapewniają pełną kontrolę nad działaniem systemu, natomiast fine-tuning umożliwia precyzyjne dopasowanie modelu do specyficznych potrzeb firmy, jednocześnie optymalizując koszty szkolenia.

Wykorzystanie własnych danych do personalizacji AI, mimo wyzwań związanych z kosztami i infrastrukturą, jest inwestycją, która może znacząco zwiększyć skuteczność modeli, i poprzez to jakość usług i produktów. Odpowiednio wytrenowany model może stać się kluczowym zasobem organizacji, zapewniając jej trwałą przewagę konkurencyjną.

Jednocześnie model AI wymaga odpowiedniej ochrony – zarówno przed nieautoryzowanym dostępem, jak i manipulacjami, które mogą wpłynąć na jego skuteczność i wiarygodność. Proces trenowania modeli jest szczególnie wrażliwy na ingerencję, która może prowadzić do obniżenia jakości wyników, a w skrajnych przypadkach nawet do błędnych decyzji biznesowych. Z tego względu kluczowe jest wdrożenie odpowiednich mechanizmów zabezpieczeń na każdym etapie – od przygotowania danych, przez trenowanie modelu, aż po jego wdrożenie i monitorowanie w środowisku produkcyjnym.

Cyberbezpieczeństwo odgrywa fundamentalną rolę w skutecznym wdrażaniu systemów AI. Ochrona zarówno danych treningowych, jak i samego modelu przed nieuprawnionym dostępem czy atakami ma kluczowe znaczenie dla zapewnienia jego niezawodności i bezpieczeństwa. Świadome zarządzanie ryzykiem oraz wdrażanie odpowiednich mechanizmów ograniczających ryzyka związane cyberbezpieczeństwem stanowią nieodłączny element nowoczesnych wdrożeń sztucznej inteligencji, pozwalając firmom bezpiecznie w pełni wykorzystać potencjał tej technologii.

Leszek Ortyński

Dyrektor, Lider ds. AI i Data Science, KPMG w Polsce

Nowa technologia – nowe zagrożenia

W przeciwieństwie do rankingu wyzwań związanych z wdrażaniem sztucznej inteligencji, hierarchia największych cyberzagrożeń dla systemów AI jest wyraźna. Niezależnie od wielkości firmy respondenci dość jednomyślnie ocenili kluczowe zagrożenia.

Za najpoważniejsze uznano obejścia zabezpieczeń AI, takie jak ataki typu jailbreak i prompt injections. Niewiele mniej wskazań dotyczyło obaw związanych z utratą poufności danych przesyłanych do systemów AI przez użytkowników. Oba te rodzaje zagrożeń zostały wskazane przez ponad połowę badanych jako kluczowe.

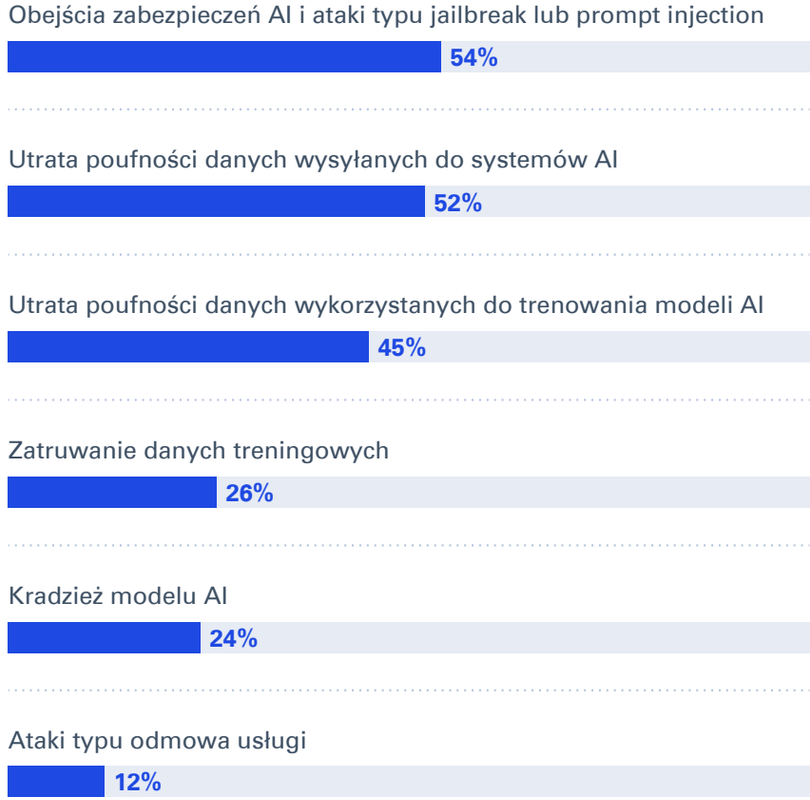
Niewiele mniej firm obawia się utraty poufności danych wykorzystywanych podczas trenowania modeli AI. Może to wskazywać na świadomość polskich przedsiębiorstw, że proces trenowania modeli AI jest bardzo wrażliwy i powinien być odpowiednio kontrolowany. Jednocześnie ingerencja w ten proces i zatruwanie danych treningowych budzą już znacznie mniejsze obawy.

Podobnie jedynie co czwarta firma obawia się kradzieży modelu AI. Może to wynikać z braku pełnego zrozumienia wartości właściwie wytrenowanych modeli AI, które mogą stanowić o przewadze konkurencyjnej organizacji. Jeszcze mniej, bo jedynie 12% respondentów, wskazało na ryzyko ataków typu odmowa usługi (denial of service). Wyniki te ponownie podkreślają, że dla biznesu bezpieczeństwo systemów AI ma wyższy priorytet niż ich wydajność.

Jednocześnie raport „KPMG 2024 CEO Outlook”[2] wskazuje, że firmy wciąż mają trudności z oceną skali zagrożeń związanych z AI oraz ich konsekwencji. Aż 40% polskich liderów przyznało, że nie potrafi ocenić poziomu przygotowania swojej organizacji w tym zakresie.

2 „KPMG 2024 CEO Outlook. Adaptacja do zmian to kształtowanie przyszłości”, KPMG w Polsce, 2024.

Największe cyberzagrożenia dla systemów AI



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Zarządy firm na całym świecie dostrzegają w sztucznej inteligencji szansę na rozwój i coraz lepiej rozumieją, że opóźnienia w jej wdrażaniu mogą prowadzić do utraty przewagi rynkowej.

Równocześnie liderzy biznesu są świadomi, że nieprzemyślane decyzje mogą narazić organizację na trudne do przewidzenia zagrożenia.

Aby skutecznie zmierzyć się z tym wyzwaniem, konieczne jest odpowiedzialne podejście – dostosowanie rozwiązań do realnych potrzeb, właściwa ocena ryzyka oraz mechanizmy ograniczające jego skutki.

Brak przygotowania i zbyt pochopne działania mogą zwiększać podatność na zagrożenia związane z cyberbezpieczeństwem.

Nie należy jednak traktować tych kwestii jako bariery dla rozwoju. Korzyści biznesowe wynikające z AI znacząco przewyższają potencjalne ryzyka, o ile odpowiednie zabezpieczenia zostaną uwzględnione na każdym etapie wdrożenia. Kluczowe jest zaangażowanie doświadczonego, interdyscyplinarnego zespołu.

Andrzej Gałkowski

Partner, Lider doradztwa dla sektora bankowego, Head of AI w KPMG w Polsce i Europie Środkowo-Wschodniej

Przedsiębiorstwa planujące wdrożenie rozwiązań opartych na sztucznej inteligencji powinny przygotować się do tego procesu we właściwy sposób. Dostępnych jest wiele zestawów najlepszych praktyk w zakresie bezpieczeństwa AI (np. NIST, MITRE, OWASP), których kompilacja i dostosowanie do specyfiki firmy pozwala na przygotowanie właściwego środowiska do wdrożeń i późniejszej bezpiecznej eksploatacji tego rodzaju systemów.

Konieczne jest również upewnienie się, że wdrażana technologia spełnia wymagania regulacyjne. W szczególności należy zwrócić uwagę na uchwalone w ubiegłym roku rozporządzenie AI Act, które wymaga kompleksowego, opartego na analizie ryzyka podejścia do zaadresowania szerokiego wachlarza zagrożeń dla systemów sztucznej inteligencji. Bardzo ważną regulacją jest również Rozporządzenie o Ochronie Danych Osobowych. Trzeba bardzo uważać, by do trenowania modeli AI nie użyć danych osobowych, dla których nie zostały zgromadzone stosowne pozwolenia.

Marcin Kieszkowski

Assiociate Director, Advisory, Zespół Cyberbezpieczeństwa, KPMG w Polsce

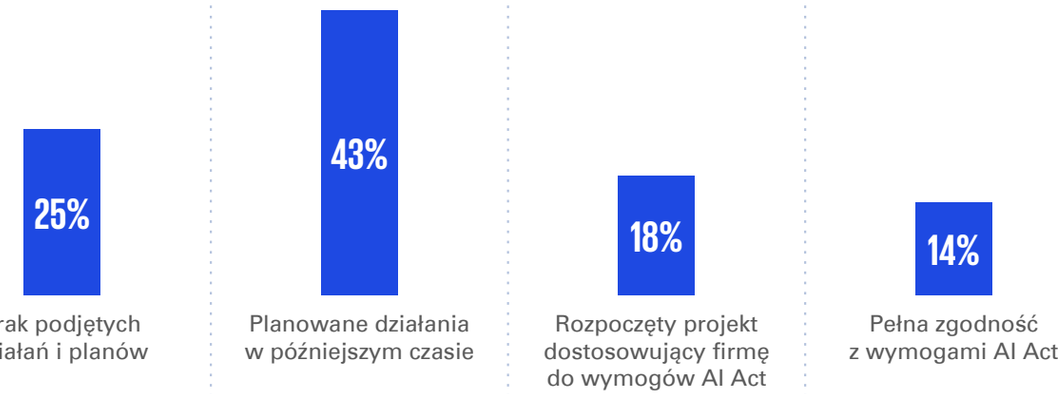
Pierwsze kroki z AI Act

Rewolucja związana ze sztuczną inteligencją oraz obawy związane m.in. z cyberbezpieczeństwem znajdują swoje odzwierciedlenie w unijnym rozporządzeniu AI Act (Rozporządzenie o sztucznej inteligencji), opublikowanym w Dzienniku Urzędowym Unii Europejskiej 12 lipca 2024 roku. Choć w pełnej formie zacznie obowiązywać dopiero w 2027 roku, jego kolejne etapy są rozłożone w czasie, a już teraz obowiązują ograniczenia dotyczące systemów AI o wysokim ryzyku. Kolejna faza zaplanowana jest na lipiec 2025 roku, kiedy to wejdą w życie przepisy dotyczące systemów AI ogólnego przeznaczenia. Kluczowym celem dokumentu jest stworzenie stabilnych ram prawnych, które umożliwią bezpieczne i etyczne korzystanie z systemów AI, ochronią użytkowników przed nadużyciami oraz w dłuższej perspektywie zbudują społeczne zaufanie do tej technologii.

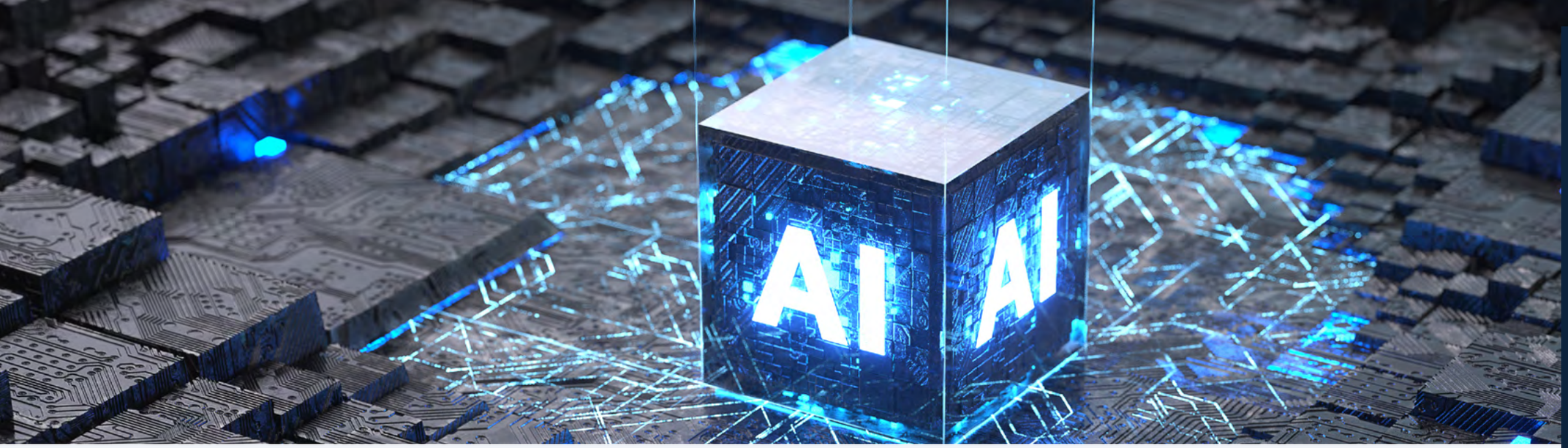
Niemniej jednak firmy odkładają przygotowania do uzyskania zgodności z nowymi przepisami. Prawie połowa z nich zaplanowała działania na później, bliżej terminu obowiązywania regulacji, a jedynie 18% firm już rozpoczęło projekt dostosowujący organizację do wymagań AI Act. Zaledwie 14% przedsiębiorstw jest w pełni zgodnych z wymogami, a co czwarta organizacja nie podjęła jeszcze żadnych działań przygotowawczych. Nie ma bezpośredniej zależności między wielkością firmy a zaawansowaniem w implementacji rozporządzenia, chociaż pełną zgodność na ten moment osiągnęły głównie duże firmy (20% z nich).

Pomimo widocznego zainteresowania tematem 25% firm, które nie podjęły żadnych działań, to zdecydowanie za dużo. Niezbędne jest, aby wszystkie organizacje zapoznały się z zakresem obowiązywania aktu, chociażby po to, by upewnić się, czy korzystają z rozwiązań sztucznej inteligencji zgodnie z wytycznymi i jakie zmiany będą musiały wprowadzić. Zapoznanie się ze standardami zawartymi w rozporządzeniu może stanowić odpowiedź na wiele z cytowanych obaw i wyzwań związanych z wdrożeniem tej technologii. Liczby mówią same za siebie: 26% firm zadeklarowało, że nie wie, czy podlega rozporządzeniu i czy jest zgodna z jego wymogami.

Stan przygotowania firm do zgodności z AI Act



Źródło: KPMG w Polsce na podstawie badania ankietowego.



Coraz więcej firm wdraża rozwiązania oparte na sztucznej inteligencji, a wraz z tym pojawiają się zarówno wyzwania technologiczne, jak i regulacyjne. Unijny AI Act określa akceptowalny poziom ryzyka i redukuje niepewność co do przyszłych regulacji, dzięki czemu organizacje mogą rozwijać swoje inicjatywy AI w przewidywalnych ramach prawnych. Jednak samo dostosowanie się do wymogów to dopiero pierwszy krok – pozostają ryzyka związane z samą technologią, na które firmy muszą odpowiedzieć.

W zależności od etapu przygotowań organizacje różnie postrzegają te wyzwania. Firmy, które dopiero pracują nad zgodnością z regulacjami, za największy problem uznają brak nadzoru nad wykorzystaniem AI w organizacji (56%). Natomiast te, które przeszły już przez ten proces, wskazują na to zagadnienie znacznie rzadziej (14%), co pokazuje, że skuteczna implementacja regulacji prowadzi do uporządkowania wewnętrznych struktur zarządzania AI.

Firmy, które dostosowały się do AI Act, koncentrują się na kwestiach cyberbezpieczeństwa – aż 64% z nich uznaje ryzyko cyberataków na systemy AI za jedno z trzech najpoważniejszych zagrożeń. To niemal dwukrotnie więcej niż wśród organizacji na wcześniejszych etapach dostosowania. Oznacza to, że po wdrożeniu regulacji kluczowe stają się wyzwania związane z ochroną modeli i systemów AI przed atakami zewnętrznymi.

Co ciekawe, im dalej firma jest w procesie dostosowania, tym częściej postrzega samo spełnienie wymogów AI Act jako istotne wyzwanie. Może to sugerować, że organizacje na początkowym etapie wdrożenia nie doszacowują skali koniecznych zmian. To dodatkowy argument przemawiający za tym, aby nie odkładać działań na później.

Porównanie priorytetów firm na różnych etapach wdrażania regulacji pokazuje, że AI Act sprzyja zwiększaniu świadomości w zakresie cyberbezpieczeństwa. Organizacje, które już dostosowały się do przepisów, dostrzegają szeroki wachlarz zagrożeń, w tym rosnące ryzyko kradzieży modeli AI. Wśród firm mniej zaawansowanych w tym procesie świadomość tego zagrożenia jest niższa, co może wynikać z niedoceniania wartości własnych modeli.

Niezależnie od etapu wdrożenia regulacji, firmy wskazują na obejścia zabezpieczeń AI, ataki typu jailbreak i prompt injection jako jedne z najistotniejszych zagrożeń. Są to również najbardziej medialne ryzyka związane z rozwojem sztucznej inteligencji, wymagające stałego monitorowania i adaptacji strategii cyberbezpieczeństwa.

Dwa oblicza sztucznej inteligencji w cyberbezpieczeństwie

Szybki rozwój sztucznej inteligencji stał się kolejną przyczyną obaw o bezpieczeństwo cyfrowe. Ponad połowa (56%) respondentów uważa, że poziom zagrożeń wzrośnie lub znacząco wzrośnie w związku z nowymi rodzajami ryzyka, które pojawią się w wyniku szerokiego wprowadzenia tej technologii na rynek. Z kolei jedynie 16% przewiduje, że zagrożenia zmaleją dzięki usprawnieniom w metodach zabezpieczeń, możliwym dzięki AI. Jednocześnie 28% badanych sądzi, że sztuczna inteligencja nie wpłynie znacząco na ich poziom w tej dziedzinie. Warto dodać, że badanie nie wykazało większej liczby cyberincydentów w firmach korzystających z AI w porównaniu do tych, które jeszcze jej nie wdrożyły. Oznacza to, że obawy firm wynikają raczej z niepewności co do przyszłego rozwoju zagrożeń niż z konkretnych doświadczeń związanych z wdrożeniem tej technologii.

Dokładne skutki stosowania AI w cyberbezpieczeństwie są trudne do przewidzenia, nie tyle z powodu niepewności co do możliwych scenariuszy, ile z dużej liczby konkurencyjnych dróg rozwoju. Choć AI otwiera drzwi do nowych rodzajów oszustw, takich jak kradzież tożsamości za pomocą materiałów typu deepfake, umożliwia także bardziej efektywną ochronę przed różnorodnymi zagrożeniami.

Warto zauważyć, że wartość światowego rynku AI w cyberbezpieczeństwie w 2023 roku wyniosła 19,5 mld dolarów amerykańskich, a prognozy na 2028 rok szacują ją na 77,7 mld dolarów amerykańskich, z czego 30,2% przypadnie na sektor bankowości, usług finansowych i ubezpieczeń[3]. Potencjał jest ogromny – algorytmy sztucznej inteligencji w połączeniu z istniejącymi systemami ochrony, takimi jak oprogramowanie antywirusowe czy systemy wykrywania oszustw, zwiększają ich efektywność dzięki szybkiemu analizowaniu ogromnych zbiorów danych. AI umożliwia również przeprowadzanie zaawansowanych testów penetracyjnych dostosowanych do indywidualnych potrzeb.

Wszystko to sprawia, że sztuczna inteligencja staje się mieczem obosiecznym w cyberbezpieczeństwie – narzędziem, które skutecznie rozwiązuje problemy, do których rozwoju sama się przyczynia.

3 „Global Artificial Intelligence-Based Cybersecurity Market 2024-2028", Technavio, 2024.

Wpływ rozwoju sztucznej inteligencji na poziom cyberzagrożeń w opinii respondentów

Źródło: KPMG w Polsce na podstawie badania ankietowego.

Systemy AI są łakomym kąskiem dla cyberprzestępców. Wynika to faktu, że poza słabościami związanymi z wykorzystaniem standardowych elementów środowiska teleinformatycznego, pojawiają się dodatkowe słabości bezpośrednio związane z nową technologią i chęcią jej jak najszybszego wdrożenia. W oczach cyberprzestępcy zwiększona „powierzchnia ataku" w połączeniu z dużą ilością wrażliwych danych, jakie systemy AI przetwarzają, stanowi idealny cel ataku. Innym poważnym zagrożeniem związanym z systemami AI jest również zatruwanie danych wejściowych (data poisoning), które może prowadzić do manipulacji wynikami działania modelu. Warto zapoznać się z opisami jak wiele nowych zagrożeń wnosi sztuczna inteligencja w dziedzinie bezpieczeństwa, sięgając do repozytoriów takich jak MITRE ATLAS, czy opracowania OWASP (np. Top 10 for LLM Applications).

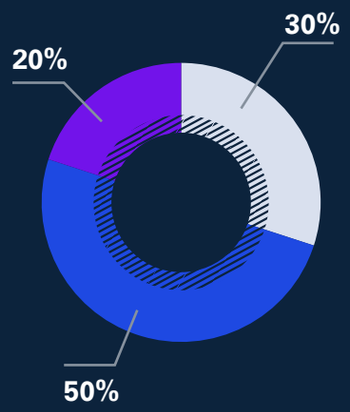
Łukasz Staniak

Dyrektor, Advisory,
Lider Red Team w Zespole Cyberbezpieczeństwa,
KPMG w Polsce

Informacje o badaniu

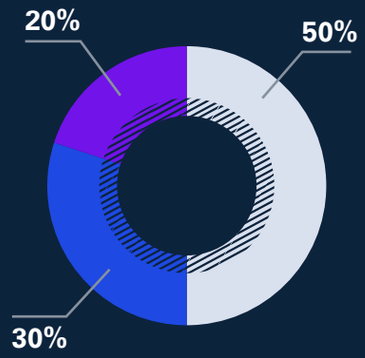
Badanie przeprowadzono za pomocą wywiadów telefonicznych CATI wśród osób zajmujących się bezpieczeństwem IT w firmach, takich jak członkowie zarządu, dyrektorzy ds. bezpieczeństwa, dyrektorzy IT i inne osoby odpowiedzialne za ten obszar. Próba badawcza obejmowała 100 organizacji o przychodach przekraczających 51 mln złotych. Badanie zostało zrealizowane w grudniu 2024 roku.

Wielkość badanych firm



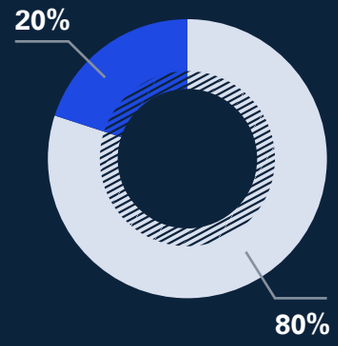
- Małe (max. 50 osób)
- Średnie (50-249 osób)
- Duże (od 250 osób)

Przychody badanych firm



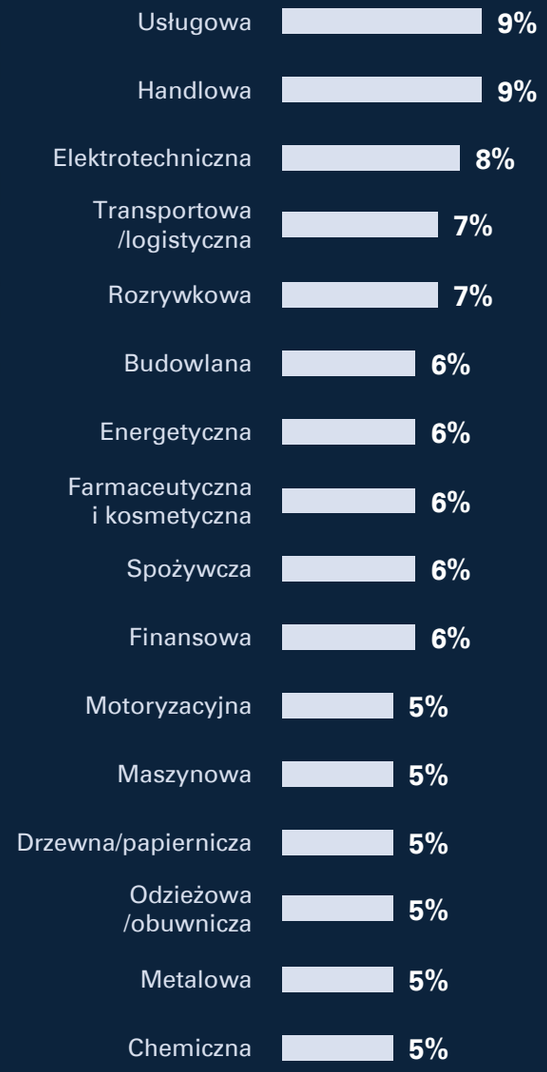
- 51-100 mln zł
- 101-200 mln zł
- Powyżej 200 mln zł

Typ kapitału



- Polski
- Zagraniczny

Branże badanych firm



Źródło: KPMG w Polsce na podstawie badania ankietowego.

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