KPMG

Barometr cyberbezpieczeństwa

Na fali, czy w labiryncie regulacji?

Luty 2024 | kpmg.pl

Wstęp

Szanowni Państwo,

Z przyjemnością prezentuję Państwu naszą najnowszą, siódmą już edycję raportu dotyczącego cyberbezpieczeństwa. Stworzyliśmy go z myślą o podniesieniu świadomości i rozwijaniu umiejętności skutecznego zarządzania bezpieczeństwem informatycznym w obliczu dynamicznie zmieniającej się scenerii zagrożeń w cyberprzestrzeni. Mam nadzieję, że zebrane wyniki ankiety staną się inspiracją do skutecznego wzmocnienia bezpieczeństwa Państwa organizacji stojących w obliczu współczesnych zagrożeń.

W badaniu uczestniczyło 100 polskich przedsiębiorstw, obejmujących zarówno duże, średnie, jak i małe firmy, reprezentowane przez osoby zajmujące się zagadnieniami bezpieczeństwa informacji. Ankieta została przeprowadzona na przełomie 2023 i 2024 roku. W bieżącej edycji badania położyliśmy szczególny nacisk na diagnozę wpływu pojawiających się regulacji na kierunki transformacji cyberbezpieczeństwa.

W Polsce nadal wyraźnie widać bardzo zróżnicowany stan przygotowania organizacji do stawienia czoła wirtualnym zagrożeniom, zwłaszcza w kontekście zmieniającego się otoczenia legislacyjnego. Około 45% firm wyraża przekonanie, że są bardzo dobrze lub dobrze przygotowane na te zmiany. Podobny odsetek respondentów czuje, że ich organizacje są przygotowane w umiarkowanym stopniu. Na przestrzeni tego roku wzrosła liczba przedsiębiorstw, które zarejestrowały przynajmniej jeden incydent w swojej organizacji. Pomimo tego, wszystkie badane przez nas grupy zagrożeń wywołują coraz mniejsze obawy wśród decydentów w zakresie cyberbezpieczeństwa w firmach. Być może wynika to z faktu, że w ciągu ostatnich kilku lat wszyscy obyliśmy się z tematem cyberprzestępczości, która jest już zjawiskiem powszechnym.

Wyłudzanie danych uwierzytelniających (phishing) pozostaje niezmiennie największym zagrożeniem dla firm w Polsce, a obszarami, w których firmy deklarują najwyższy poziom dojrzałości zabezpieczeń, są bezpieczeństwo styku z siecią Internet oraz ochrona przed złośliwym oprogramowaniem. Jak pokazuje nasze badanie, odsetek firm powierzających różnorodne kwestie bezpieczeństwa danych zewnętrznym dostawcom rośnie z każdym kolejnym rokiem i na koniec 2023 wyniósł 84%. W firmach biorących udział w badaniu już nie oograniczenia budżetowe, ale trudności związane z rekrutacją i utrzymaniem wykwalifikowanych pracowników były wymieniane jako największa przeszkoda w osiągnięciu odpowiedniego poziomu zabezpieczeń.

Nie od dziś wiadomo, że efektywna obrona przed cyberatakami to nie tylko wyzwanie, lecz także konieczna inwestycja w trwałość i sukces każdej organizacji. Aby przemiana była skuteczna, cyberbezpieczeństwo musi stać się integralnym elementem procesu transformacyjnego.

Życząc Państwu przyjemnej lektury, zapraszam do zapoznania się ze wszystkimi wnioskami płynącymi z naszego raportu. Zachęcam również do podejmowania działań na rzecz wzmocnienia bezpieczeństwa cyfrowego Państwa organizacji. Takie kroki wydają się konieczne w obliczu obecnych, znanych już zagrożeń i przyszłych potencjalnych wyzwań.

Z poważaniem,

Michał Kurek
Partner

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

Najważniejsze spostrzeżenia z raportu

W 2023 roku liczba firm, które zarejestrowały

przynajmniej jeden incydent

związany z cyberbezpieczeństwem, wzrosła o osiem punktów procentowych, do

66%

O 17 punktów procentowych spadły obawy związane z działaniami

zorganizowanych grup cyberprzestępczych,

które są uznawane za największe zagrożenie w sieci.

Niezmiennie **głównym zagrożeniem** w sieci jest kradzież danych poprzez

phishing.

W porównaniu z rokiem poprzednim firmy zgłaszają

wyższy poziom dojrzałości

obszarów takich jak bezpieczeństwo styku z siecią Internet, ochrona przed złośliwym oprogramowaniem czy bezpieczeństwo sieci wewnętrznej.

Najwyższy

wzrost inwestycji w zabezpieczenia,

aż o 12 punktów procentowych, zanotowano w obszarach zarządzania tożsamością i dostępem oraz bezpieczeństwa w procesach wytwarzania oprogramowania.

Połowa respondentów uważa, że

trudności związane z rekrutacją i utrzymaniem wykwalifikowanych pracowników

to największy problem w osiągnięciu odpowiedniego poziomu zabezpieczeń.

84%

firm korzysta z outsourcingu przynajmniej jednej funkcji cyberbezpieczeństwa.

45%

organizacji jest przekonanych, że są bardzo dobrze lub dobrze przygotowane do zmieniających się regulacji.

Główne

wyzwania stojące na drodze do skutecznej cybertransformacji

to szybko zmieniające się przepisy i normy prawne oraz brak świadomości zagrożeń wśród pracowników.

RODO dla

85%

przedsiębiorstw jest priorytetowym obszarem dla zapewniania zgodności IT i ochrony danych osobowych.

1 Krajobraz cyberzagrożeń

W obecnej dynamicznej rzeczywistości cyfrowej, w której innowacje napotykają wiele wyzwań, a technologia pełni rolę narzędzia zarówno dla kreatywnych twórców, jak i dla tych, którzy jej nadużywają wykorzystując niezgodnie z zasadami czy prawem, zagrożenia stają się integralnym elementem cyfrowego środowiska. Skala cyberataków nieustannie rośnie, a jedynym skutecznym podejściem wydaje się być podejmowanie proaktywnych działań, które pozwalają firmom antycypować działania atakujących, jednocześnie umożliwiając łagodzenie potencjalnych zakłóceń w przyszłości.

Przeformułowanie cyberbezpieczeństwa z reaktywnej strategii, opartej na incydentach, w integralną część działań transformacyjnych pozwala organizacjom nie tylko wzmocnić zabezpieczenia, ale także zredefiniować funkcjonowanie całego przedsiębiorstwa i zwiększyć jego efektywność. Kultura organizacyjna, która priorytetowo traktuje bezpieczeństwo i inspiruje pracowników do aktywnego zaangażowania się, odgrywa fundamentalną rolę. Takie środowisko, oprócz skutecznej ochrony przed zagrożeniami, korzystnie wpływa na innowacyjność, budowanie zaufania klientów oraz reputację firmy.

Mimo zauważalnego, choć nieuzasadnionego, spadku obaw związanych z różnymi grupami cyberprzestępców, można zaobserwować wzrost liczby firm, które doświadczyły przynajmniej jednego incydentu w sieci w ubiegłym roku. Trudno jednoznacznie określić czy mniejsze obawy wynikają z ewolucji świadomości czy też są rezultatem uśpionej czujności, co wpływa na percepcję ryzyka.

W miarę rozwoju wirtualnego świata, nowe trendy w zagrożeniach, takie jak włamania do urządzeń mobilnych czy ataki na sieci bezprzewodowe, zyskują na popularności. Jednocześnie jednak tradycyjne zagrożenia, typu wyłudzanie danych uwierzytelniających czy wykorzystywanie złośliwego oprogramowania, nadal utrzymują się w czołówce trzech głównych wyzwań dla organizacji.

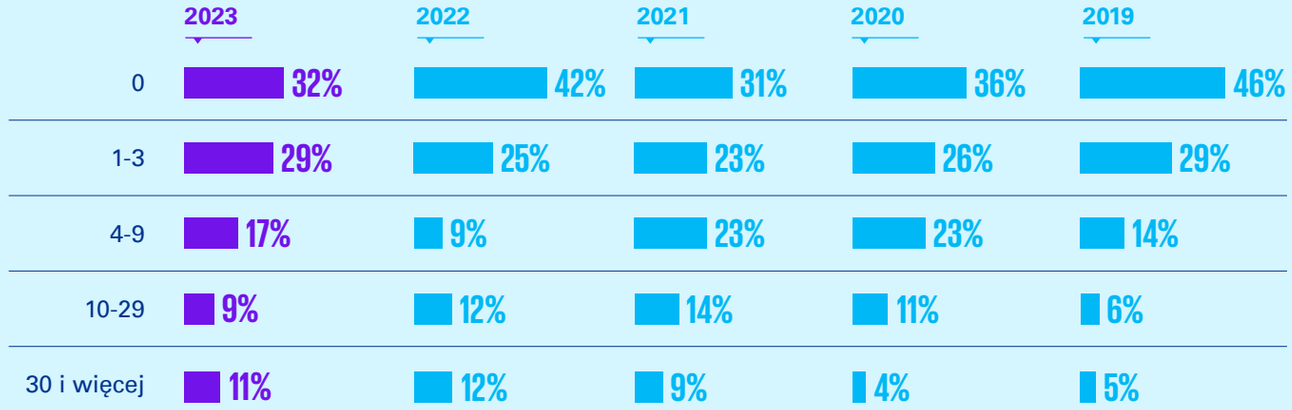
Cyberatak – powszechne ryzyko

W opinii większości ankietowanych, liczba zaobserwowanych prób cyberataków na systemy organizacji utrzymuje się na podobnym poziomie jak w poprzednim roku. Zauważalne są niewielkie wahania w liczbie incydentów, przy jednoczesnym wzroście świadomości i częstszym zgłaszaniu niefortunnych przypadków.

Chociaż firmy, które nie odnotowały żadnego incydentu, nadal stanowią największą grupę (jedna trzecia odpowiedzi), wartość ta obniżyła się o 10 punktów procentowych w porównaniu z rokiem ubiegłym. Liczba przedsiębiorstw, które zarejestrowały przynajmniej jeden incydent, wzrosła o osiem punktów procentowych, osiągając poziom 66%.

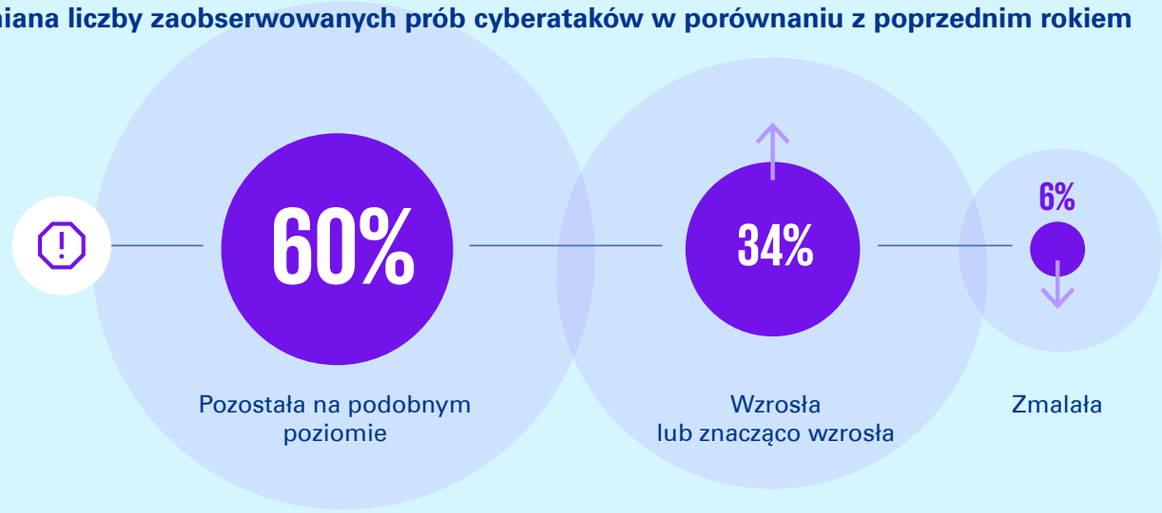
Odsetek firm notujących ponad 30 incydentów bezpieczeństwa w ciągu roku zmniejszył się o zaledwie jeden punkt procentowy w porównaniu z 2022 rokiem, który był rekordowy pod względem liczby ataków. W tej grupie duże firmy zatrudniające powyżej 250 pracowników stanowiły prawie jedną trzecią.

Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa



*Wartości na wykresie nie sumują się do 100% (2% stanowi odmowa odpowiedzi)

Zmiana liczby zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Śladami źródeł cyberzagrożeń

W najnowszej edycji badania zauważalny jest znaczny spadek obaw przedsiębiorstw związanych z zagrożeniami ze strony różnych grup cyberprzestępców. W porównaniu z wynikami sprzed roku, najbardziej widoczny jest spadek o 17 punktów procentowych jeżeli chodzi o obawy związane z działaniami zorganizowanych grup cyberprzestępczych, które jednocześnie są uznawane za najgroźniejsze w sieci. Odczuwalnie, o 14 punktów procentowych, zmniejszyło się także grono firm, które realnie dostrzegają zagrożenie ze strony cyberterrorystów. Pozostałe grupy, w tym hakerzy, dzieciarnia internetowa (Script kiddies) i aktywiści, również obecnie są postrzegane jako mniejsze zagrożenie niż rok wcześniej. Jedyną grupą, której istotność wzrosła w tegorocznym badaniu (o trzy punkty procentowe), są niezadowoleni lub podkupieni pracownicy.

W kontekście trwającej już dłuższy czas wojny w Ukrainie, odsetek firm wskazujących na zagrożenie ze strony grup wspieranych przez obce państwa zmniejszył się z 38% do 24%, co tym samym przywraca poziom tego wskaźnika do wartości sprzed czterech lat.

Należy jednak zauważyć, że obecnie prawdopodobnie postępuje zmniejszenie poziomu czujności firm, co może wpływać na percepcję postrzeganego ryzyka. Z tego powodu, w celu właściwej oceny sytuacji i dostosowania strategii bezpieczeństwa, ważne jest monitorowanie zarówno danych dotyczących cyberzagrożeń, jak i reakcji firm na nie.

Grupy stanowiące realne zagrożenie dla organizacji

Edycja raportu	2024	2023	2022	2021	2020
Cyberprzestępcy					
Zorganizowane grupy cyberprzestępcze	53%	70%	69%	54%	43%
Pojedynczy hakerzy	50%	59%	58%	57%	72%
Cyberterroryści	28%	42%	50%	18%	43%
Dzieciarnia internetowa (Script kiddies)	13%	22%	23%	19%	36%
Haktywiści	12%	18%	15%	12%	21%
Grupy wspierane przez obce państwa	24%	38%	27%	19%	24%
Niezadowoleni lub podkupieni pracownicy	24%	21%	42%	39%	58%

Źródło: KPMG w Polsce na podstawie badania ankietowego.

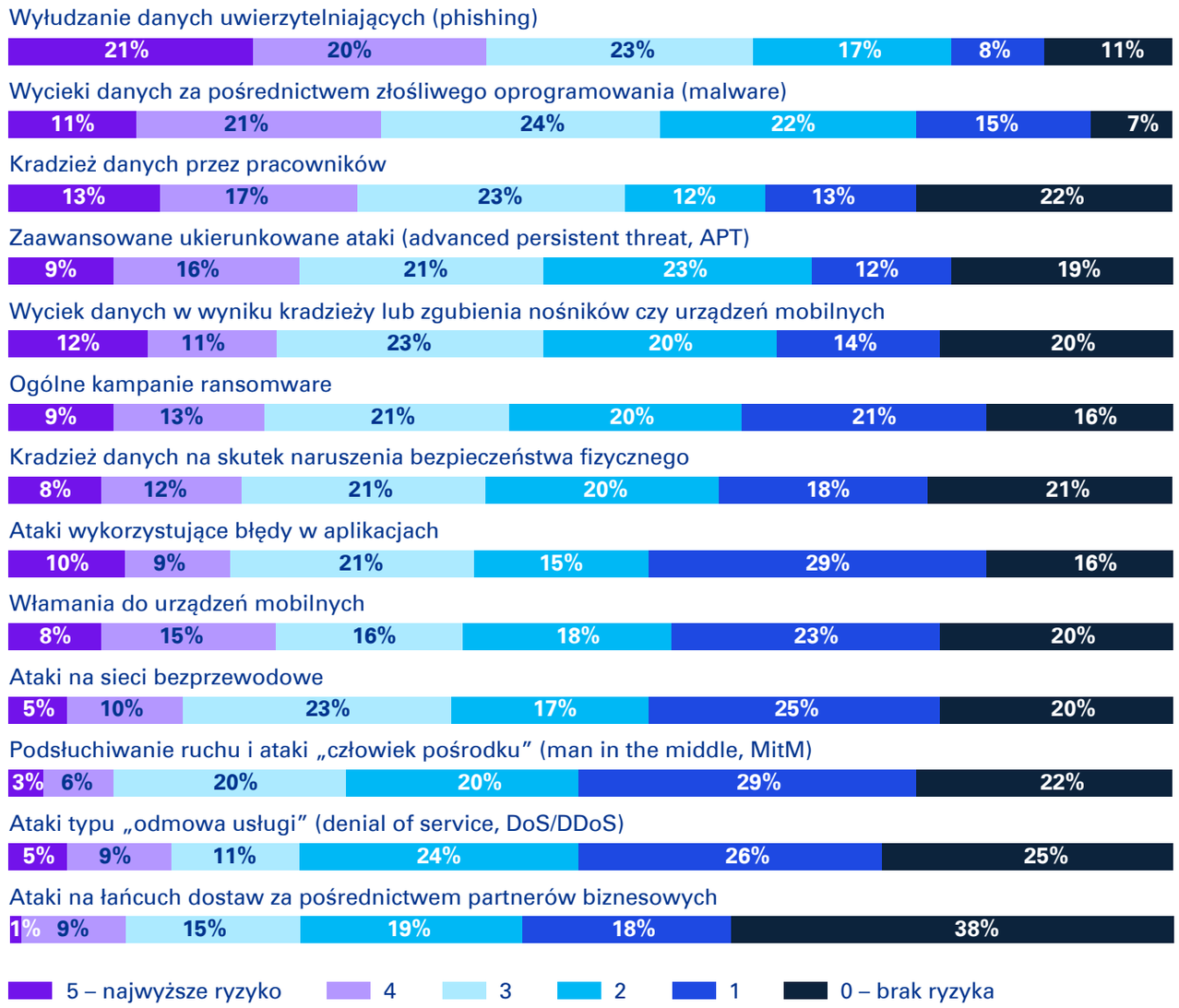
Arsenał cyberprzestępców

W cyfrowym środowisku kradzież danych poprzez phishing nadal stanowi główne zagrożenie, podobnie jak rok wcześniej. Jedna piąta firm, które wzięły udział w badaniu, wskazała to ryzyko jako najbardziej prominentne. W ciągu ostatniego roku szczególnie wzrosło znaczenie kradzieży danych związanej z naruszeniem bezpieczeństwa fizycznego oraz wycieków danych wynikających z kradzieży lub utraty nośników.

Kategorie, które zajmowały niższe pozycje w minionym roku, takie jak włamania do urządzeń mobilnych oraz ataki na sieci bezprzewodowe – w bieżącej edycji przesunęły się na wyższe miejsca. To wskazuje, że stały się one istotniejszym zagrożeniem z perspektywy polskich firm. Pomimo tych zmian, wycieki danych spowodowane przez złośliwe oprogramowanie, ukierunkowane ataki APT oraz kradzieże danych przez pracowników nadal pozostają głównymi wyzwaniami dla organizacji.

Ponad jedna trzecia firm biorących udział w tegorocznej edycji badania KPMG uznała za zupełnie nieistotne niebezpieczeństwa cyfrowe związane z atakami na łańcuch dostaw za pośrednictwem partnerów biznesowych. Natomiast co czwarty respondent barometru nie dostrzega zagrożenia dla swojej organizacji ze strony ataków typu „odmowa usługi".

Cyberzagrożenia stanowiące największe ryzyko dla organizacji



Źródło: KPMG w Polsce na podstawie badania ankietowego.

2

Transformacja cyberbezpieczeństwa

Bezpieczeństwo informacji staje się kluczowym elementem codziennego życia. W niniejszym raporcie przedstawione zostały wyniki ankiety, które rzucają światło na obszary odpowiedzialności, dojrzałości zabezpieczeń oraz planowanych inwestycji na przyszły rok. Zagadnienia dotyczące głównych ograniczeń w osiągnięciu pożądanego poziomu zabezpieczeń, a także funkcji i procesów bezpieczeństwa realizowanych przez dostawców (outsourcing), otwierają drzwi do lepszego zrozumienia wyzwań, z jakimi borykają się organizacje w obliczu ewoluujących zagrożeń.

Obszary zabezpieczeń w polskich firmach rozwijają się wprost proporcjonalnie do rosnących budżetów inwestycyjnych. Niemniej jednak, wiele z nich wciąż nie osiągnęło pełnej dojrzałości w zwalczaniu cyberprzestępczości, co widoczne jest w ostrożnej samoocenie zdolności obronnych. Pomimo tego, że wiele przedsiębiorstw nadal stosuje wewnętrzne rozwiązania w obszarze bezpieczeństwa danych, obserwuje się rosnący trend outsourcingu.

Obecnie największym wyzwaniem dla firm w osiągnięciu właściwego poziomu zabezpieczeń są trudności związane z rekrutacją i utrzymaniem wykwalifikowanych pracowników, a także ograniczone budżety. Analizując te wyzwania, przedsiębiorstwa zwracają uwagę na konieczność zwiększenia dostępności wysoko wykwalifikowanego personelu oraz odpowiedniego finansowania, aby skutecznie przeciwdziałać zagrożeniom.

Na straży informacji w erze cyberzagrożeń

Rola dyrektora IT (Chief Information Officer) w zakresie cyberbezpieczeństwa pozostaje stabilna, co potwierdza tegoroczna edycja badania. Najczęściej odpowiedzialność za procesy związane z cyberbezpieczeństwem przypisana jest w ramach struktur tego działu. Taka sytuacja ma miejsce niezmiennie w niemal połowie badanych firm na przestrzeni ostatnich lat.

Rola prezesa zarządu nieznacznie zmalała od ostatniego roku, co stanowi podtrzymanie obserwowanego od kilku lat trendu.

Przypisanie odpowiedzialności za cyberbezpieczeństwo występuje tak samo często w strukturach globalnych oraz w firmach, gdzie inne stanowiska niż dyrektor IT, CEO lub CSO (Chief Security Officer) / CISO (Chief Information Security Officer) pełnią tę funkcję.

Warto również zauważyć, że spadł odsetek firm, które formalnie nikomu nie przypisały odpowiedzialności za ten obszar (z 17% do 11%). Odsetek ten spada do 8% w przypadku dużych firm, zatrudniających powyżej 250 pracowników.

Osoby odpowiedzialne w organizacji za bezpieczeństwo informacji

Edycja raportu	2024	2023	2022	2021	2020
Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT	47%	45%	47%	48%	45%
Prezes zarządu (CEO)	16%	17%	15%	22%	23%
Niezależna dedykowana funkcja (CSO/CISO)	12%	8%	14%	11%	3%
Inne stanowisko w organizacji niż powyższe	8%	8%	5%	4%	12%
Odpowiedzialność przypisana w strukturach globalnych poza Polską	6%	5%	9%	2%	2%
Brak formalnego przypisania odpowiedzialności	11%	17%	10%	13%	15%

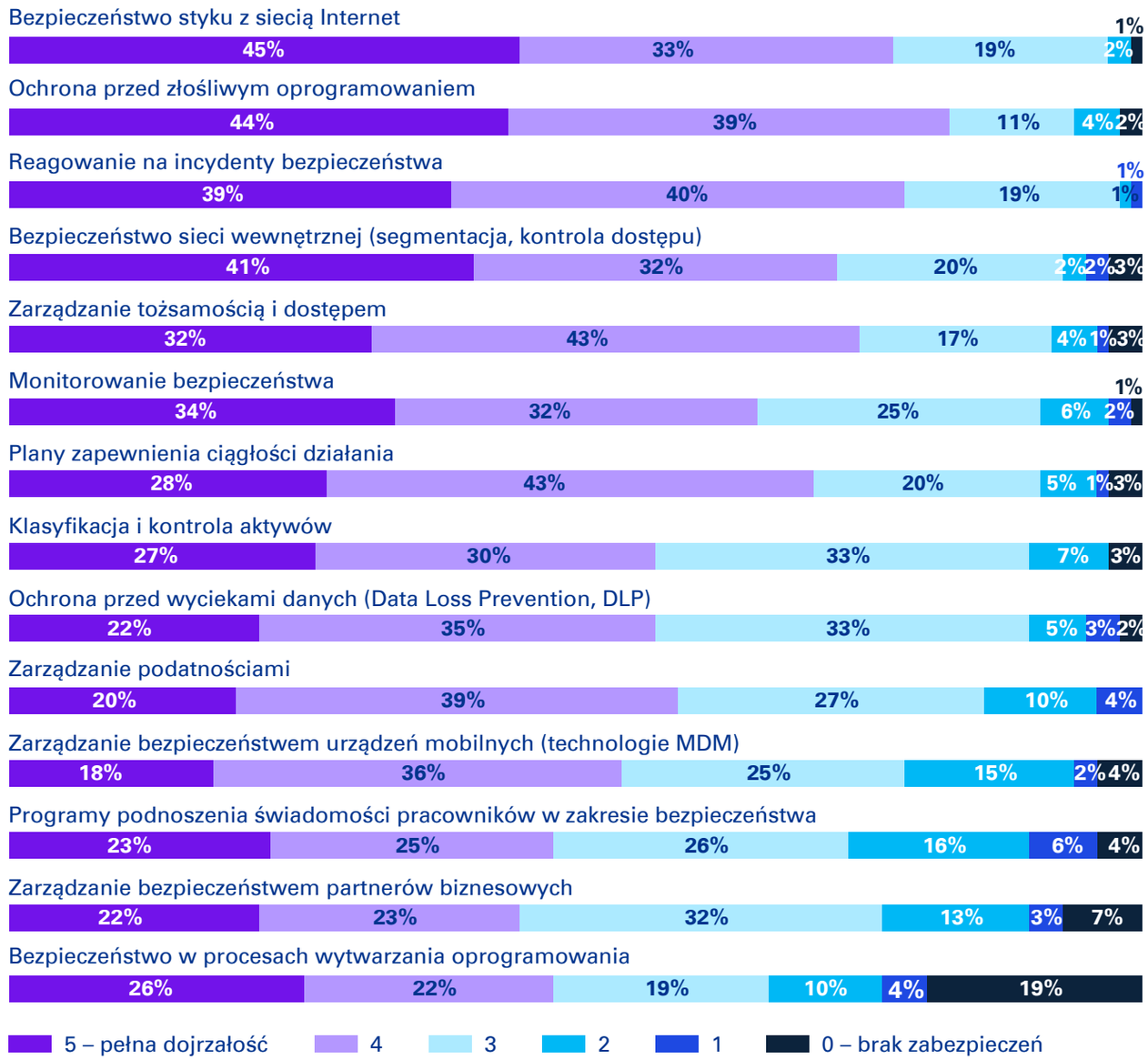
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Wyższy poziom dojrzałości

Optymizmem napawa fakt, że w obszarze bezpieczeństwa styku z siecią Internet oraz ochrony przed złośliwym oprogramowaniem, firmy w Polsce zgłaszają wyższy poziom dojrzałości w porównaniu do poprzedniego roku, co potwierdziło ponad 40% respondentów. Podobnie wysoko oceniane jest bezpieczeństwo sieci wewnętrznej, które również zostało uznane za obszar w pełni dojrzały przez ponad 40% ankietowanych.

Zarządzanie bezpieczeństwem urządzeń mobilnych, choć nadal pozostaje jednym z obszarów, które najmniej respondentów (18%) uważa za całkowicie wykształcony, zanotowało wzrost o pięć punktów procentowych w porównaniu do ubiegłego roku. Istotnym aspektem jest również fakt, że prawie co piąta firma nie kontroluje bezpieczeństwa w procesach wytwarzania oprogramowania, a to zjawisko jest szczególnie widoczne wśród dużych przedsiębiorstw, zatrudniających powyżej 250 pracowników.

Ocena dojrzałości poszczególnych obszarów zabezpieczeń w organizacji



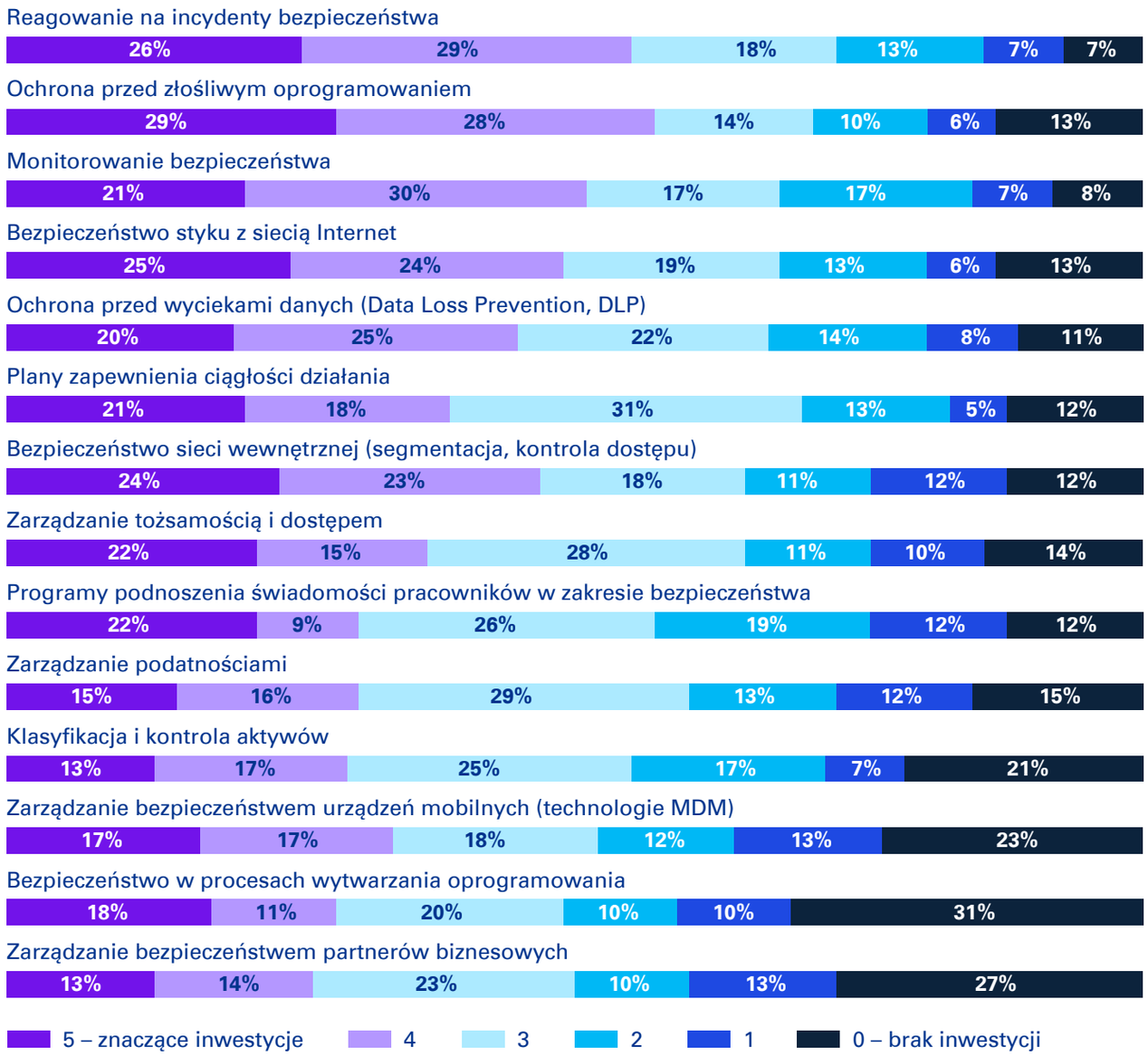
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Bezpieczne dziś, bezpieczne jutro

Nakłady inwestycyjne przedsiębiorstw w dziedzinie cyberbezpieczeństwa są zróżnicowane i uwzględniają charakterystykę branż, rozmiary firm oraz specyficzne potrzeby i zagrożenia. Planowane inwestycje w zabezpieczenia często wynikają z konieczności adaptacji do rozwijających się niebezpieczeństw oraz utrzymania konkurencyjności w dynamicznym środowisku online. Jednocześnie stanowią one skuteczną strategię minimalizowania ryzyka utraty danych i zakłóceń w działalności przedsiębiorstwa.

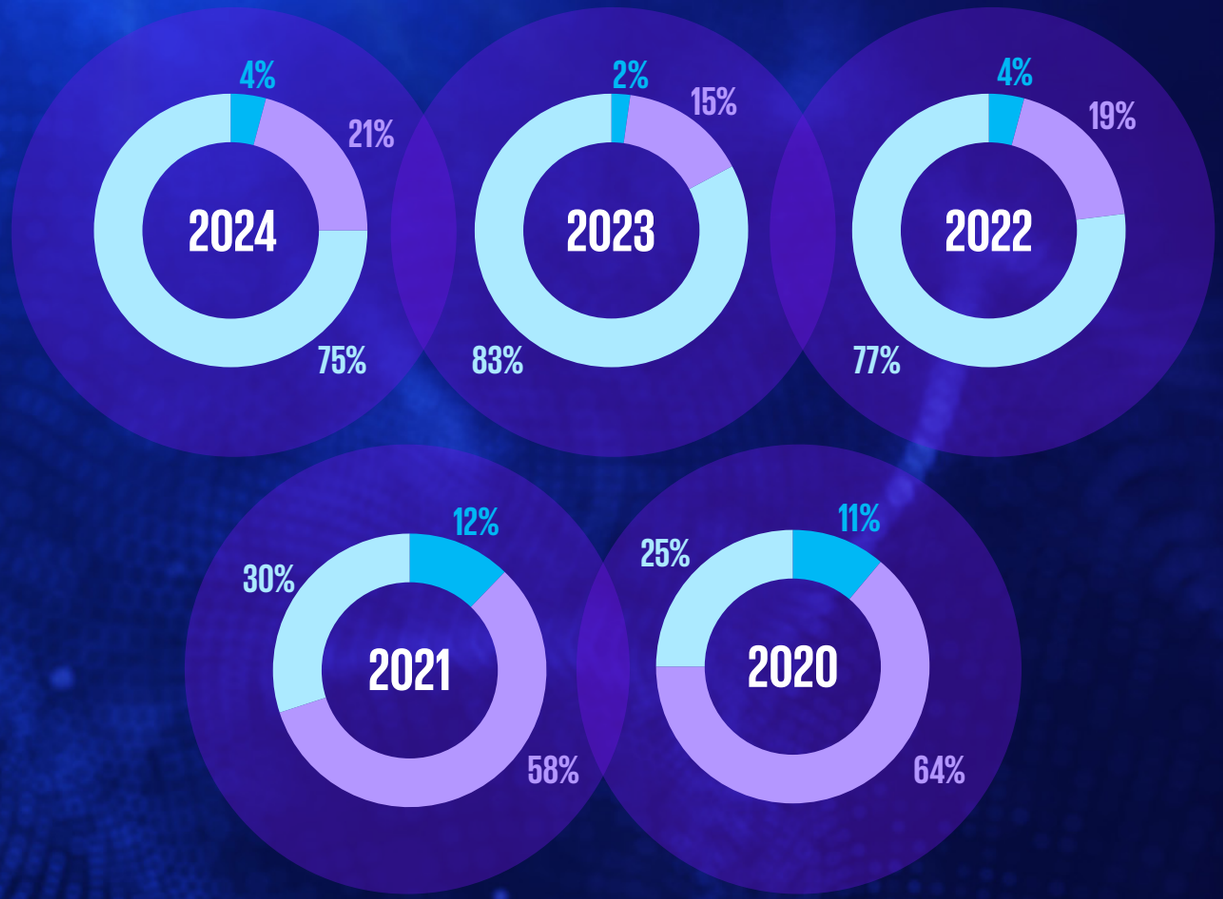
Globalnie zauważalny jest rosnący trend inwestycji w obszar cyberbezpieczeństwa, co wynika z rosnącego ryzyka cyberataków oraz coraz większej zależności firm od technologii. Tendencja ta jest również widoczna w Polsce, gdzie w ciągu ostatniego roku zaobserwowano znaczny wzrost budżetów przeznaczanych na ten cel. Szczególnie wyraźnie widać zwiększone zaangażowanie finansowe w obszary zarządzania tożsamością i dostępem oraz bezpieczeństwo w procesach wytwarzania oprogramowania, które zanotowały wzrost aż o 12 punktów procentowych w porównaniu z poprzednim rokiem. Niepokoi natomiast niska skłonność do inwestycji w procesy zarządzania bezpieczeństwem partnerów biznesowych, które stają się coraz bardziej istotne wraz ze wzrostem powiązań cyfrowego ekosystemu, w jakim funkcjonują dziś organizacje, a także w związku ze zmianami regulacyjnymi takimi jak NIS2, DORA, CRA, które nakładają na przedsiębiorstwa dodatkowe obowiązki w zakresie zapewnienia bezpieczeństwa łańcucha dostaw.

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



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Obszary zabezpieczeń ocenione jako w pełni dojrzałe



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Pełne obroty – podnoszenie poprzeczki

Ocena dojrzałości analizowanych obszarów bezpieczeństwa uległa zmianom na przestrzeni lat, szczególnie w kontekście wpływu pandemii Covid-19 oraz trwającej wojny w Ukrainie. Od 2022 roku zauważalny jest wzrost sceptycyzmu firm wobec własnej dojrzałości. Respondenci coraz rzadziej wybierają odpowiedzi typu „w większości analizowanych obszarów", na rzecz częściej wskazywanych w ankiecie „najwyżej w połowie."

W tegorocznej edycji badania jedna piąta firm zadeklarowała dojrzałość w większości analizowanych kategorii. Choć jest to wynik o sześć punktów procentowych wyższy niż w poprzednim roku, to jednak w porównaniu do okresu sprzed pandemii (2019) stanowi spadek o ponad 60 punktów procentowych.

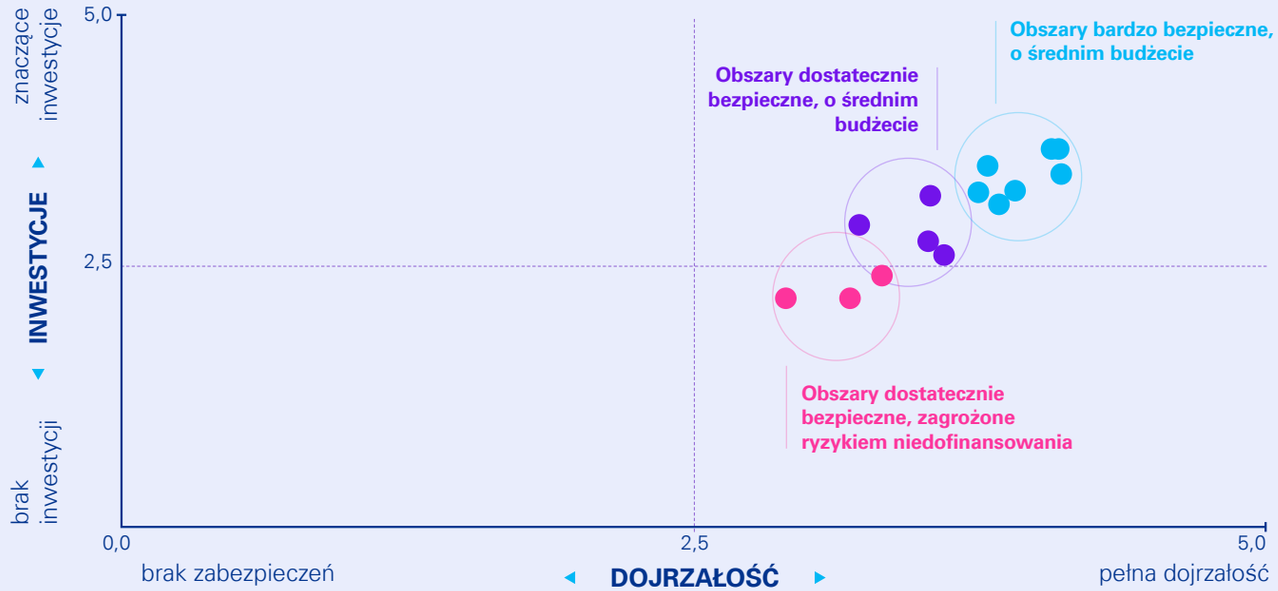
Rok 2024 przyniósł również ponowny wzrost deklarowanej dojrzałości we wszystkich obszarach zabezpieczeń, jednakże całościowo jest to niewielki odsetek firm. Wyraźnie widać, że teraźniejsze wyzwania globalne i zmienne czynniki zewnętrzne mają istotny wpływ na postrzeganie i samoocenę firm w kwestiach związanych z bezpieczeństwem.

Ochrona w kadrze – dojrzałość kontra inwestycje

Analiza matrycy poziomu dojrzałości skuteczności zabezpieczeń oraz prognozowanych inwestycji wskazuje, że z ogólnej perspektywy wszystkie obszary charakteryzują się wysokim stopniem dojrzałości, przy jednoczesnym utrzymaniu niskich lub średnich planów inwestycyjnych. Tegoroczne badanie pokazuje, że planowane jest zwiększenie nakładów inwestycyjnych we wszystkich analizowanych obszarach.

Firmy biorące udział w badaniu KPMG wykazują najmniejszą dojrzałość w zakresie bezpieczeństwa w procesach tworzenia oprogramowania oraz zarządzania bezpieczeństwem partnerów biznesowych i urządzeń mobilnych. Paradoksalnie, budżet na bezpieczeństwo w procesach tworzenia oprogramowania zwiększył się najbardziej w ciągu roku, ex aequo z inwestycjami w zarządzanie tożsamością i dostępem (+12 punktów procentowych). Najmniej środków zarezerwowano na plany dotyczące zapewnienia ciągłości działania, z prognozowanym wzrostem o trzy punkty procentowe.

Obecna dojrzałość firm a planowane inwestycje



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Obszary bezpieczne, o średnim budżecie:

- bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu),
- reagowanie na incydenty bezpieczeństwa,
- ochrona przed złośliwym oprogramowaniem,
- bezpieczeństwo styku z siecią Internet,
- zarządzanie tożsamością i dostępem,
- monitorowanie bezpieczeństwa,
- plany zapewnienia ciągłości działania.

Obszary dostatecznie bezpieczne, o średnim budżecie:

- zarządzanie podatnościami,
- programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa,
- klasyfikacja i kontrola aktywów,
- ochrona przed wyciekami danych tzw. DLP.

Obszary dostatecznie bezpieczne, zagrożone ryzykiem niedofinansowania:

- zarządzanie bezpieczeństwem partnerów biznesowych,
- bezpieczeństwo w procesach wytwarzania oprogramowania,
- zarządzanie bezpieczeństwem urządzeń mobilnych – technologie MDM.

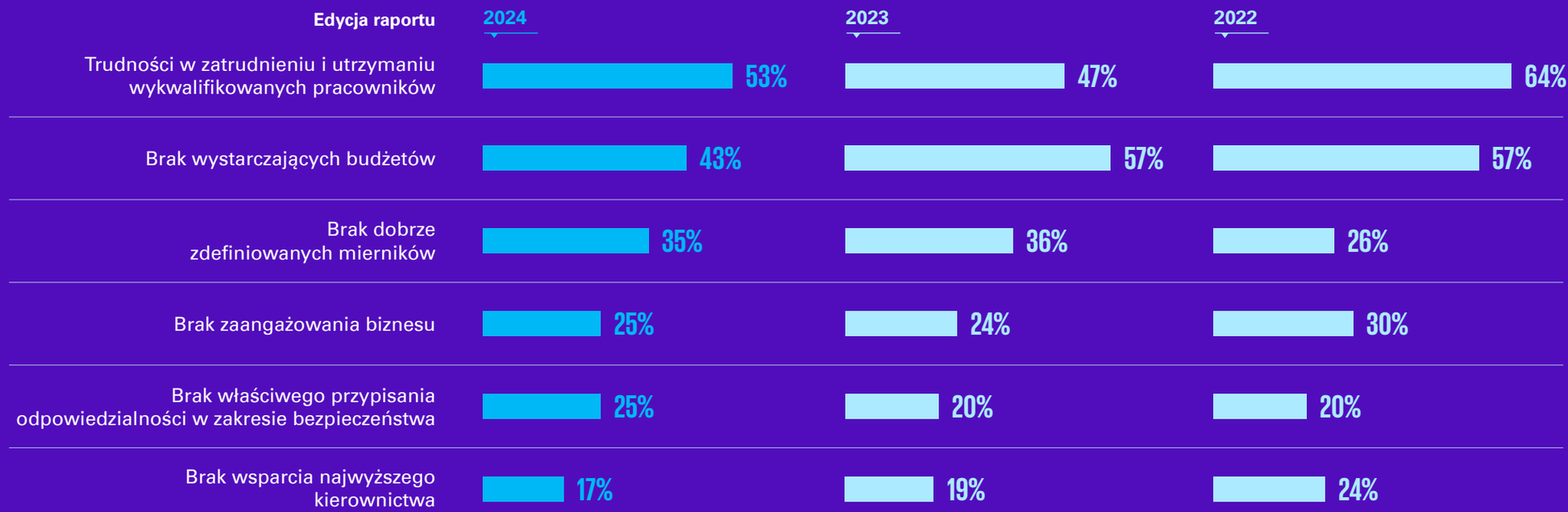
Wyboista droga do cyberbezpieczeństwa

Przez ostatnie pięć lat zauważalnie dwie najczęściej wskazywane przeszkody w dziedzinie zabezpieczeń przed cyberatakami to właśnie trudności kadrowe oraz ograniczone finansowe.

Obecnie największym wyzwaniem dla firm w osiągnięciu odpowiedniego poziomu zabezpieczeń są trudności związane z rekrutacją i utrzymaniem wykwalifikowanych pracowników, co zostało wskazane przez ponad połowę respondentów. Natomiast brak wystarczających budżetów, choć wciąż istotny, spadł na drugie miejsce.

Dodatkowo, zgodnie z odpowiedziami respondentów, na zbliżonym poziomie pozostają inne wyzwania, takie jak brak klarownie zdefiniowanych wskaźników oraz brak pełnego zaangażowania biznesu i najwyższego kierownictwa. Jedna czwarta badanych wskazała również brak odpowiedniego przypisania odpowiedzialności w zakresie bezpieczeństwa, co stanowi wzrost o pięć punktów procentowych w porównaniu do zeszłego roku.

Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji



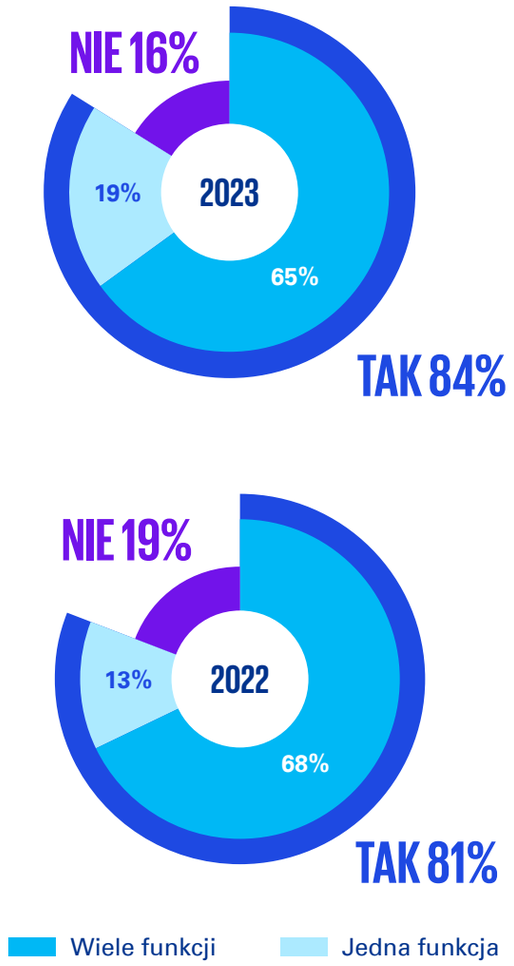
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Bezpieczeństwo w cudzych rękach

Zdecydowana większość badanych firm zleca różnorodne aspekty zarządzania bezpieczeństwem zewnętrznym dostawcom. Na zakończenie 2023 roku już 84% ankietowanych korzystało z usług outsourcingu, a jak pokazują wyniki poprzednich badań KPMG, odsetek ten stale rośnie. Chociaż większość przedsiębiorstw przekazuje więcej niż jedną funkcję bezpieczeństwa zewnętrznym dostawcom, w 2023 roku odnotowano o trzy punkty procentowe mniej takich organizacji niż w poprzednim. Ten spadek wskazuje na rosnącą świadomość potrzeby skorzystania z ekspertyzy zewnętrznych dostawców, a jednocześnie promuje bardziej zrównoważone podejście, łączące zarówno zewnętrzne, jak i wewnętrzne rozwiązania.

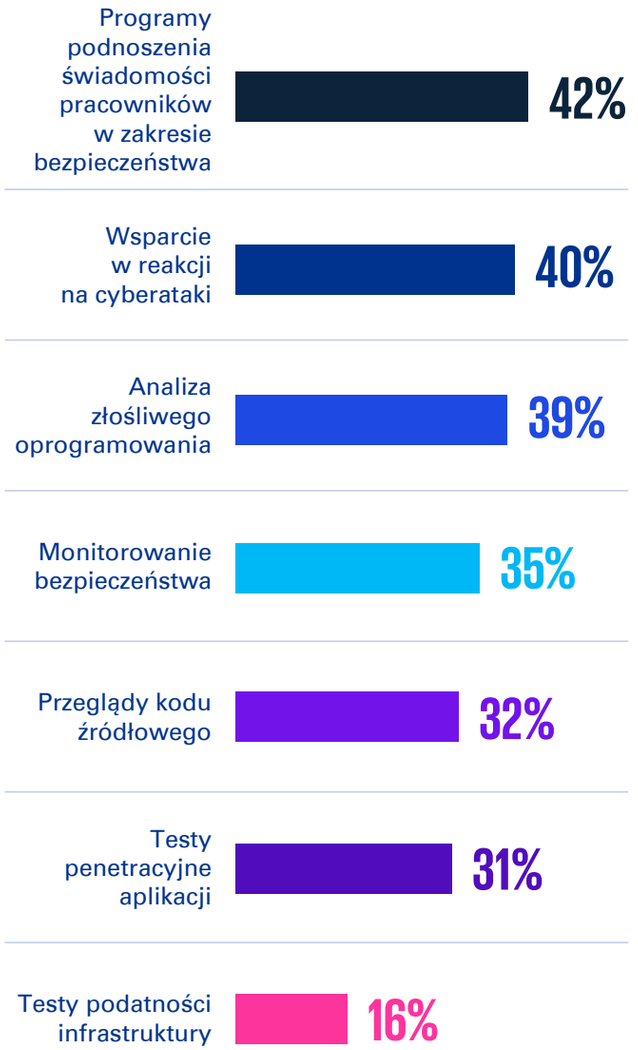
Programy podnoszenia świadomości pracowników, wsparcie w reakcji na cyberataki oraz analiza złośliwego oprogramowania to trzy najczęściej zlecane firmom zewnętrznym procesy bezpieczeństwa. Około 40% respondentów korzysta z outsourcingu w ich realizacji.

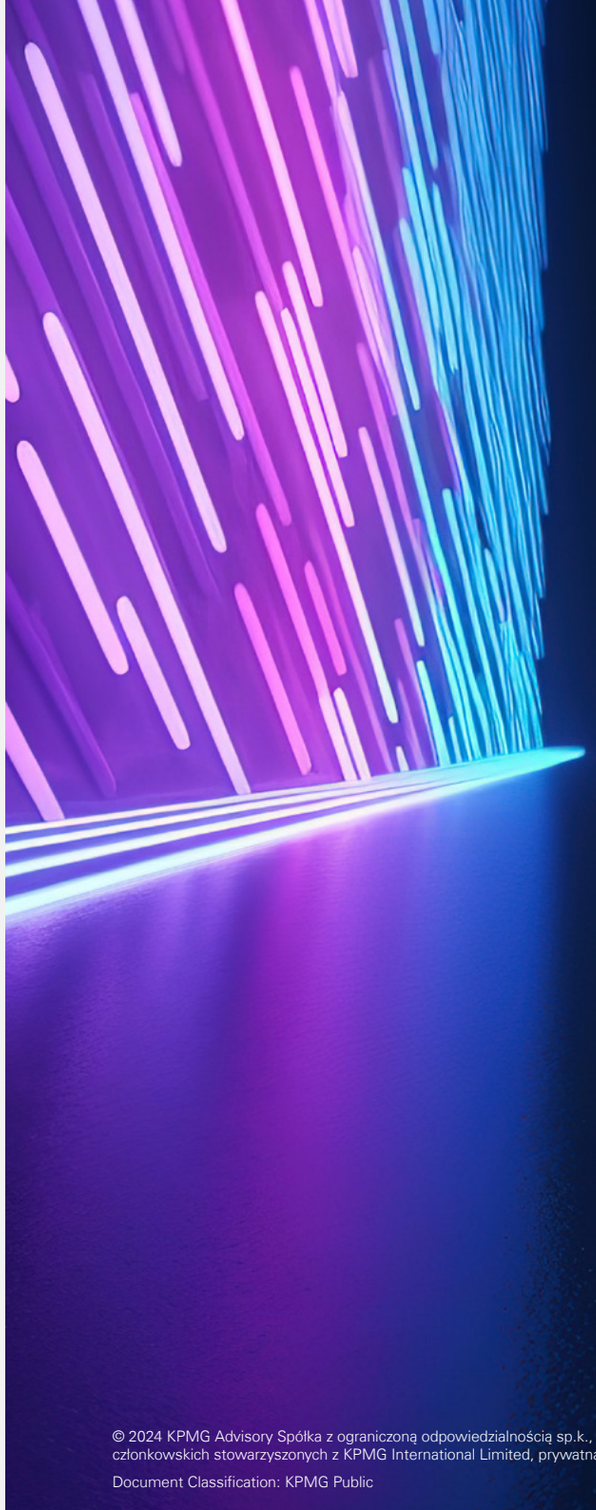
Korzystanie z outsourcingu



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Funkcje lub procesy bezpieczeństwa realizowane przez zewnętrznych dostawców





3

Regulacje w służbie bezpieczeństwa

Ciągły nadzór i precyzyjne dostosowywanie się do polityk bezpieczeństwa IT oraz ochrony danych stanowią fundamenty efektywnej strategii cyberbezpieczeństwa. W obliczu dynamicznej ewolucji zagrożeń w cyberprzestrzeni, organizacje powinny przejąć inicjatywę i proaktywnie podchodzić do ochrony swoich systemów informatycznych. Ważne, żeby skuteczna ochrona bazowała na ciągłej analizie ryzyka, obejmującej zarówno ocenę zewnętrznych cyberzagrożeń, jak również weryfikację sposobu realizacji procesów biznesowych. Istotnym elementem transformacji cyberbezpieczeństwa jest również zapewnienie zgodności z regulacjami.

Wyniki badania pokazują, że firmy coraz bardziej doceniają znaczenie przestrzegania przepisów, zwłaszcza w kontekście ogólnego rozporządzenia o ochronie danych. Niemniej jednak, mimo że większość organizacji deklaruje zaangażowanie w dostosowywanie się do przepisów, istnieje nadal pewne wyzwanie związane z dynamicznym charakterem regulacji oraz potrzebą ciągłej edukacji pracowników.

Analiza składu zespołów odpowiedzialnych za zapewnienie zgodności z regulacjami IT w organizacjach wykazuje, że większość firm posiada dedykowany zespół lub osobę odpowiedzialną za tę dziedzinę. Większość organizacji korzysta jednak z zewnętrznych audytów w celu uzyskania niezależnej oceny w tym zakresie. Wsparcie z zewnątrz jest również pomocne w pozyskaniu wiedzy na temat dynamicznie zmieniającego się otoczenia regulacyjnego. Nie tak dawno mieliśmy rewolucję związaną z RODO, a później pojawiła się Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Za chwilę wejdą w życie unijne regulacje, takie jak NIS2, DORA czy AI Act.

Michał Kurek

Partner

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

Cyberbezpieczeństwo stało się w ostatnich latach kluczowym wyzwaniem dla firm na całym świecie. W nowoczesnych, cyfrowych organizacjach stanowi ono stały punkt na agendach zarządów. Niestety, w wielu polskich przedsiębiorstwach nadal brakuje świadomości kluczowej roli, jaką w zarządzaniu cyberbezpieczeństwem odgrywają kierownicy jednostek biznesowych. W wielu organizacjach odpowiedzialność ta przypisywana jest działowi IT, a kierownictwo uważa temat za odpowiednio zarządzony. Powszechnie brakuje właściwego dialogu pomiędzy ekspertami, którzy rozumieją cyberzagrożenia, a biznesem, posiadającym wiedzę na temat wartości chronionych aktywów oraz wrażliwości nadzorowanych procesów biznesowych. Szczególnie dzisiaj, wobec ograniczeń budżetowych oraz braku wykwalifikowanych specjalistów, istotne jest podejmowanie decyzji na bazie analizy ryzyka uwzględniającej wymagania biznesowe, aby chronić to, co istotne.

W tym duchu powstaje wiele nowych regulacji dotyczących cyberbezpieczeństwa w reakcji na rosnące wyzwania w tej dziedzinie w ostatnich latach. Wykonywanie analizy ryzyka i zapewnienie proporcjonalności są ich kluczowymi założeniami. Regulacje, obok rzeczywistych cyberataków, które corocznie dotykają już większość rodzimych firm, są też dziś najczęstszym motywatorem do inwestowania w cyberbezpieczeństwo. Głównie dlatego, że w przypadku wykrycia niezgodności, regulatorzy mają możliwość wymierzania dotkliwych kar finansowych. Wskazując kierunki inwestycji w obszarze cyberbezpieczeństwa, regulacje jednocześnie podnoszą ogólny poziom bezpieczeństwa oraz uspójniają i harmonizują sposób jego budowania. Krytyczne jest, aby cel zapewnienia zgodności z regulacjami nie przykrywał nadrzędnego celu, jakim powinna być skuteczna ochrona firmy. Samo zapewnienie zgodności nie jest niestety równoznaczne z zapewnieniem bezpieczeństwa.

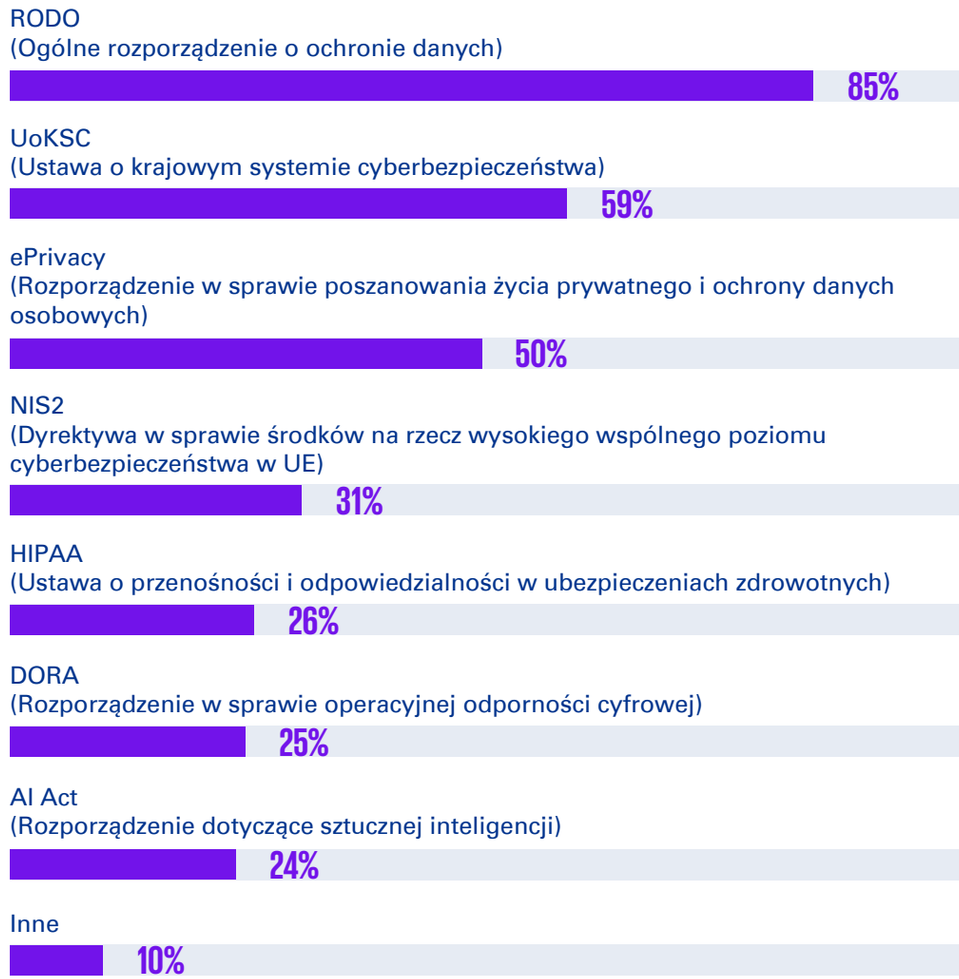
W tegorocznej edycji badania postanowiliśmy przeanalizować w jaki sposób polskie przedsiębiorstwa podchodzą do tematu zapewnienia zgodności z regulacjami dotyczącymi cyberbezpieczeństwa.

W kierunku doskonałości

W dzisiejszym świecie cyfrowym, standardy zgodności IT i ochrony prywatności danych odgrywają kluczową rolę, zapewniając ramy dla efektywnej ochrony informacji oraz przestrzegania przepisów dotyczących prywatności.

Aż 85% firm zadeklarowało, że RODO stanowi najważniejszy aspekt zewnętrznych wymagań (95% w przypadku dużych firm). Na kolejnych miejscach znalazły się ustawa o krajowym systemie cyberbezpieczeństwa (UoKSC) – 59% odpowiedzi oraz rozporządzenie w sprawie poszanowania życia prywatnego i ochrony danych osobowych (ePrivacy), zdobywając ponad połowę wskazań. Z kolei mniej znaczące dla respondentów wydają się regulacje dotyczące klasyfikowania systemów sztucznej inteligencji według ryzyka i wprowadzania zróżnicowanych wymagań dotyczących ich rozwoju i użytkowania (AI Act), a także regulacja Parlamentu i Rady Europejskiej dotycząca operacyjnej odporności cyfrowej sektora finansowego (DORA). Prawdopodobnie wiele organizacji nie zdaje sobie sprawy, że mogą być objęte wymogami tej regulacji, zakładając błędnie, że dotyczy ona wyłącznie firm z branży finansowej.

Priorytetowe standardy zgodności IT i ochrony prywatności danych



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Marcin Kieszkowski

Starszy Menedżer

Consulting, Zespół Cyberbezpieczeństwa

KPMG w Polsce

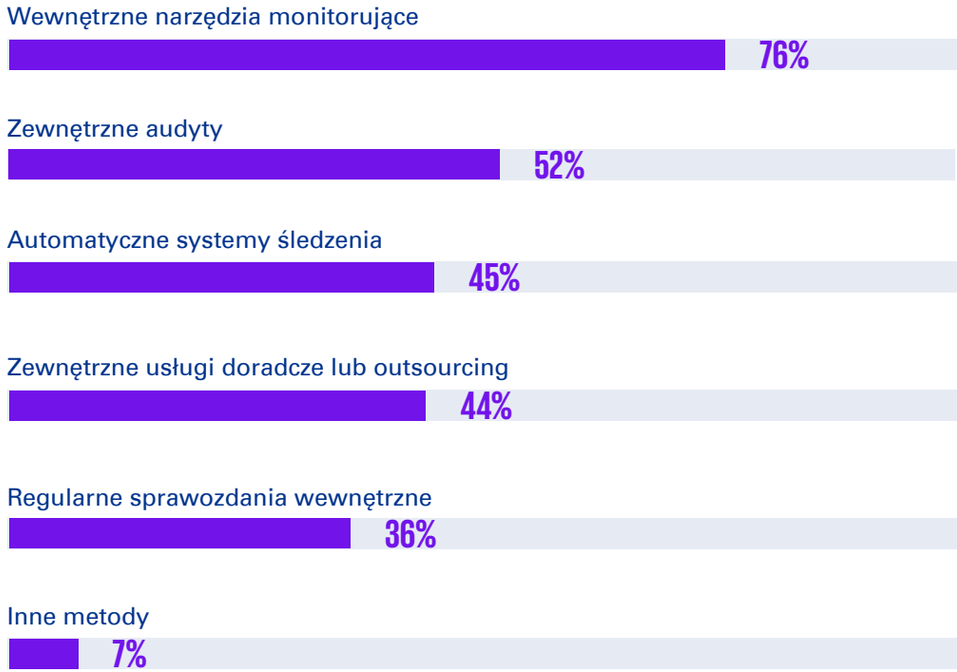
W obliczu rosnących zagrożeń i przestępczości w cyberprzestrzeni, podejmowane są inicjatywy regulacyjne mające na celu dostosowanie się do dynamicznego świata technologii. Na szczególną uwagę zasługują tutaj dyrektywa NIS2 oraz rozporządzenie DORA, czyli unijne regulacje mające na celu podniesienie poziomu cyberbezpieczeństwa w całej UE. Każda z tych regulacji stawia przed organizacjami unikalne wyzwania.

NIS2, jako aktualizacja pierwotnej dyrektywy NIS, nakłada zaostrzone wymagania na różne sektory, kategoryzując podległe przedsiębiorstwa jako kluczowe lub ważne. Regulacja kładzie nacisk na zwiększenie odporności sieci i systemów informatycznych, co często wymaga dodatkowych inwestycji finansowych oraz pozyskania unikalnych kompetencji technicznych. Warto również zauważyć, że dyrektywa wymaga od firm raportowania o incydentach bezpieczeństwa oraz współpracy z krajowymi organami ds. cyberbezpieczeństwa.

Z kolei DORA skupia się na sektorze finansowym, wymagając od instytucji finansowych i ich dostawców usług ICT adekwatnych do prowadzonej działalności ram zarządzania ryzykiem ICT oraz zapewnienia operacyjnej odporności. Wyzwaniem dla organizacji z tego sektora może być opracowanie i wdrożenie strategii zarządzania ciągłością działania, a także wdrożenie skutecznych mechanizmów monitorowania zewnętrznych dostawców usług ICT, co jest istotne w kontekście rosnącej zależności od usług w chmurze i innych technologii zewnętrznych.

Obie regulacje charakteryzują się tym, że w wielu przypadkach trudno jednoznacznie stwierdzić, czy dana organizacja będzie podlegać wytycznym oraz w jakim zakresie. Dodatkowo, w kontekście NIS2 oczekujemy jeszcze na implementację unijnej dyrektywy do krajowego porządku prawnego, co może przynieść dalsze zmiany regulacyjne.

Sposoby monitorowania i raportowania zgodności z wymogami IT



Sztuka skutecznej harmonii

Monitorowanie i raportowanie zgodności z wymogami IT są kluczowymi elementami wspierającymi organizację w utrzymaniu wysokiego poziomu bezpieczeństwa informatycznego oraz spełnianiu obowiązujących norm i przepisów. Te działania stanowią integralną część efektywnej strategii zarządzania ryzykiem.

Ponad trzy czwarte respondentów wskazało wewnętrzne narzędzia, a 52% uznało zewnętrzne audyty za najskuteczniejsze metody oceny zgodności. Warto zauważyć, że ten odsetek wzrasta, zwłaszcza wśród dużych firm. Natomiast na drugim końcu skali znalazły się regularne sprawozdania wewnętrzne oraz inne metody, takie jak ręczne przeglądanie, zbieranie informacji od pracowników czy nawet brak raportowania.

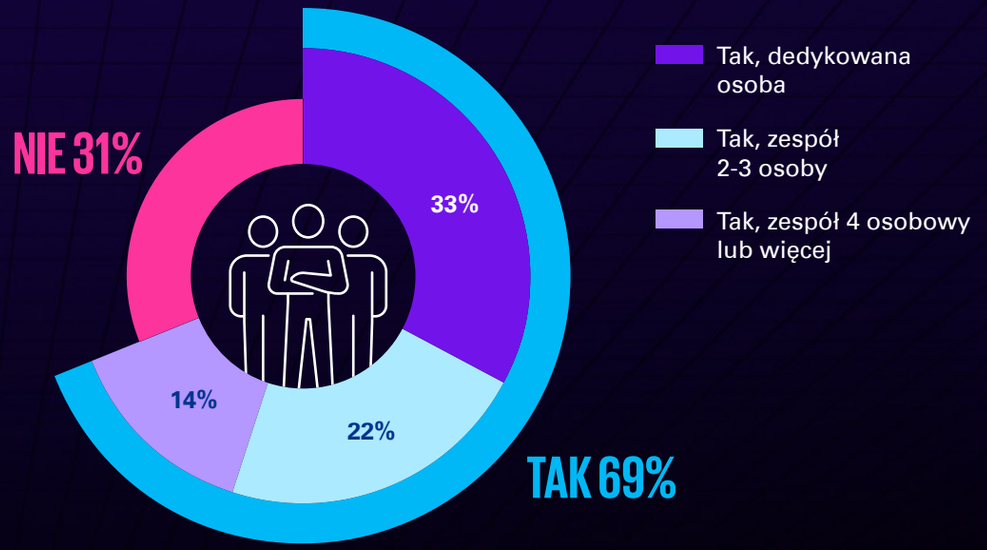
Źródło: KPMG w Polsce na podstawie badania ankietowego.

Nowe horyzonty odpowiedzialności

Schemat odpowiedzialności w organizacji określają jasne role i obowiązki pracowników na różnych szczeblach hierarchii. Właściwie zaplanowana struktura pomaga zwiększyć efektywność organizacji, uniknąć zamieszania w przypisywaniu obowiązków i tworzyć klarowne ścieżki komunikacji.

Prawie 70% respondentów odpowiedziało twierdząco na pytanie, czy w ich organizacji istnieje dedykowany zespół lub osoba odpowiedzialna za zapewnienie zgodności z regulacjami IT. Respondenci, którzy potwierdzili funkcjonowanie takiej dedykowanej jednostki w swojej organizacji podzielili się mniej więcej po połowie na tych, którzy posiadają zespół (36%) i tych z przypisaną jedną osobą (33%).

Występowanie dedykowanego zespołu lub osoby odpowiedzialnej za zapewnienie zgodności z regulacjami IT

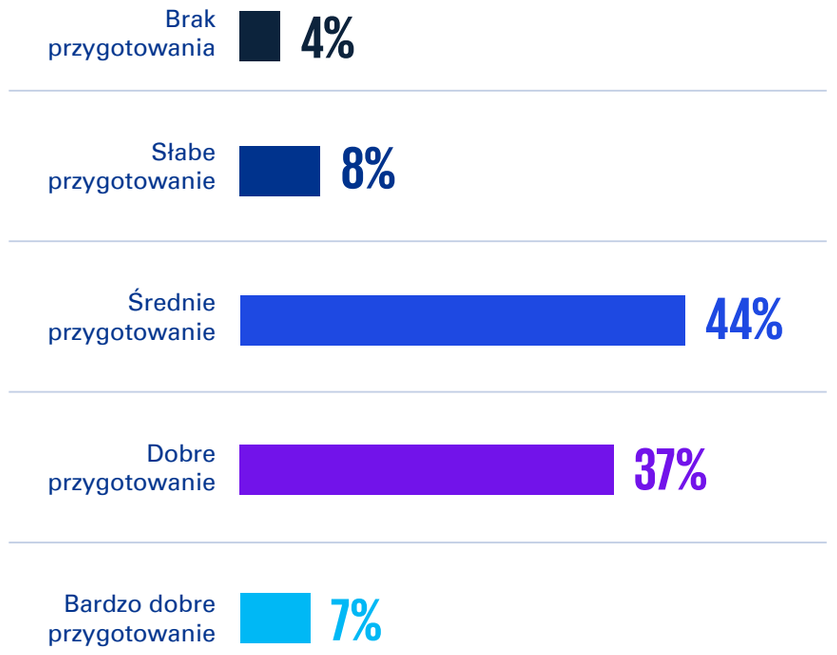


Źródło: KPMG w Polsce na podstawie badania ankietowego.

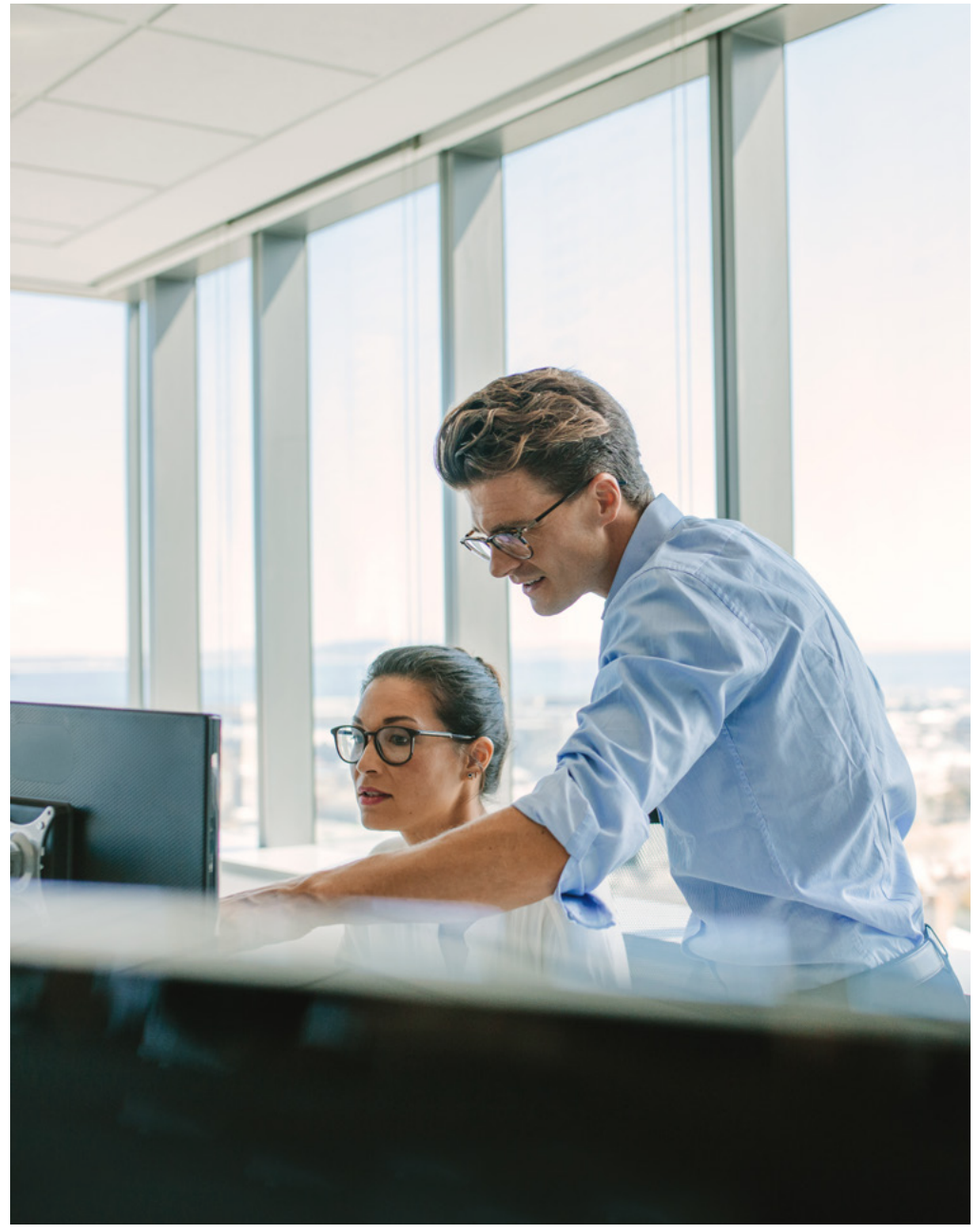
Gotowi na wyzwania

Pomimo dynamicznych zmian w regulacjach prawnych, 44% organizacji wyraziło przekonanie, że były dobrze przygotowane. Ten sam odsetek respondentów ocenił swoją gotowość jako średnią wobec ewoluujących przepisów. Jedynie zaledwie 12% uczestników badania stwierdziło, że nie czuło się gotowymi na nadchodzące zmiany lub oceniło swoje przygotowanie jako słabe.

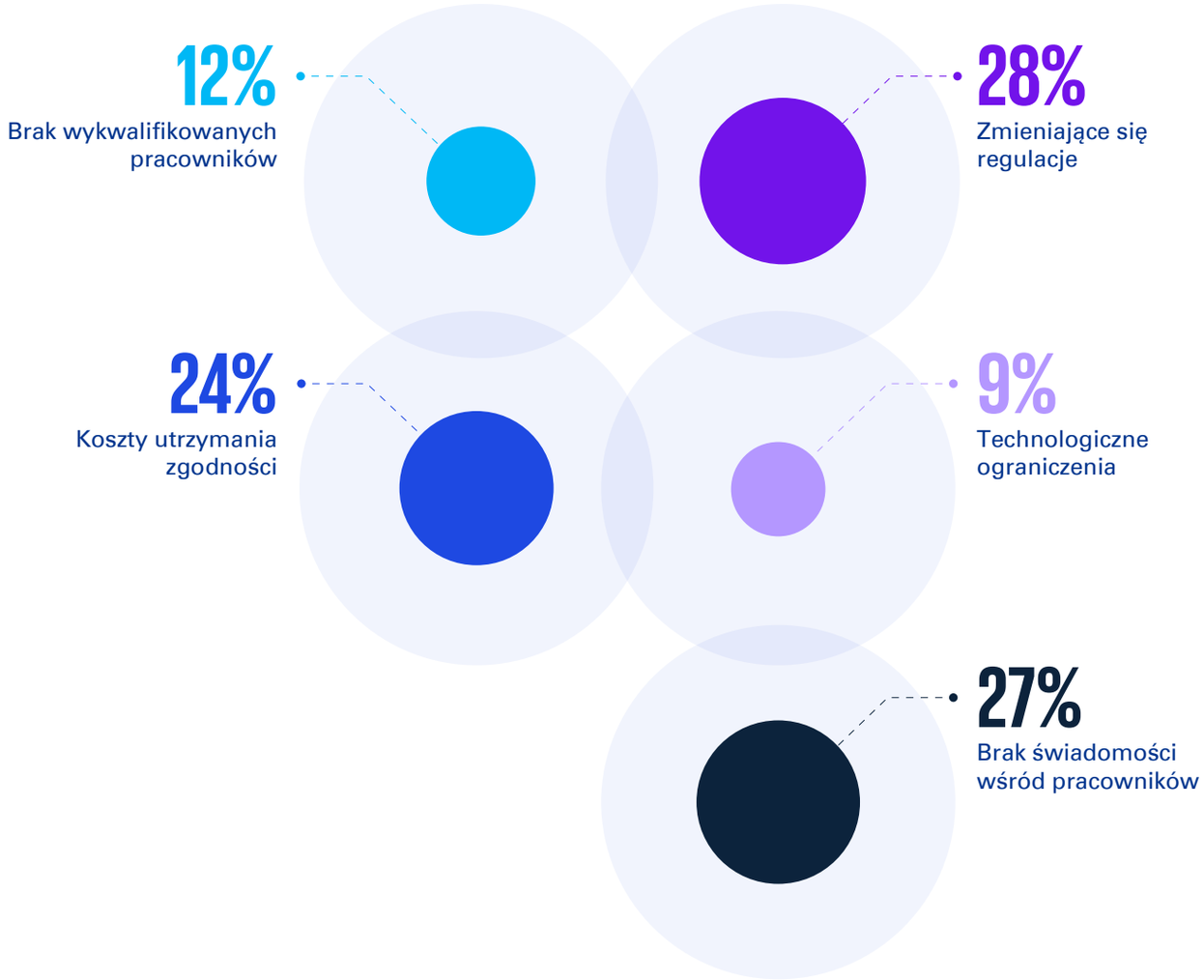
Przygotowanie firm w obliczu zmieniających się regulacji



Źródło: KPMG w Polsce na podstawie badania ankietowego.



Główne wyzwania stojące na drodze do zgodności



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Kłody pod nogi

Główne wyzwania w zarządzaniu zgodnością IT i ochroną prywatności danych w organizacji mogą wynikać z różnych czynników. Konieczne jest bieżące dostosowywanie polityk i procedur do aktualnych przepisów prawnych, co może wymagać znacznych nakładów czasowych i finansowych. Jak wskazali respondenci, najczęściej te wyzwania mają związek z szybko zmieniającymi się regulacjami i normami prawnymi oraz brakiem świadomości zagrożeń wśród pracowników.

Jedna na cztery osoby zaznaczyła również, że trudność stanowią koszty utrzymania zgodności, będące jednym z głównych wyzwań stojących na drodze do skutecznego zarządzania zgodnością IT i ochroną danych.

Najmniej istotne z perspektywy respondentów są ograniczenia technologiczne, wskazane przez 9% firm, głównie małych przedsiębiorstw.

Incydenty naruszenia ochrony danych osobowych

Właściwie zaprojektowany proces postępowania z incydentami związanymi z ochroną danych osobowych jest jednym z kluczowych warunków zgodności.

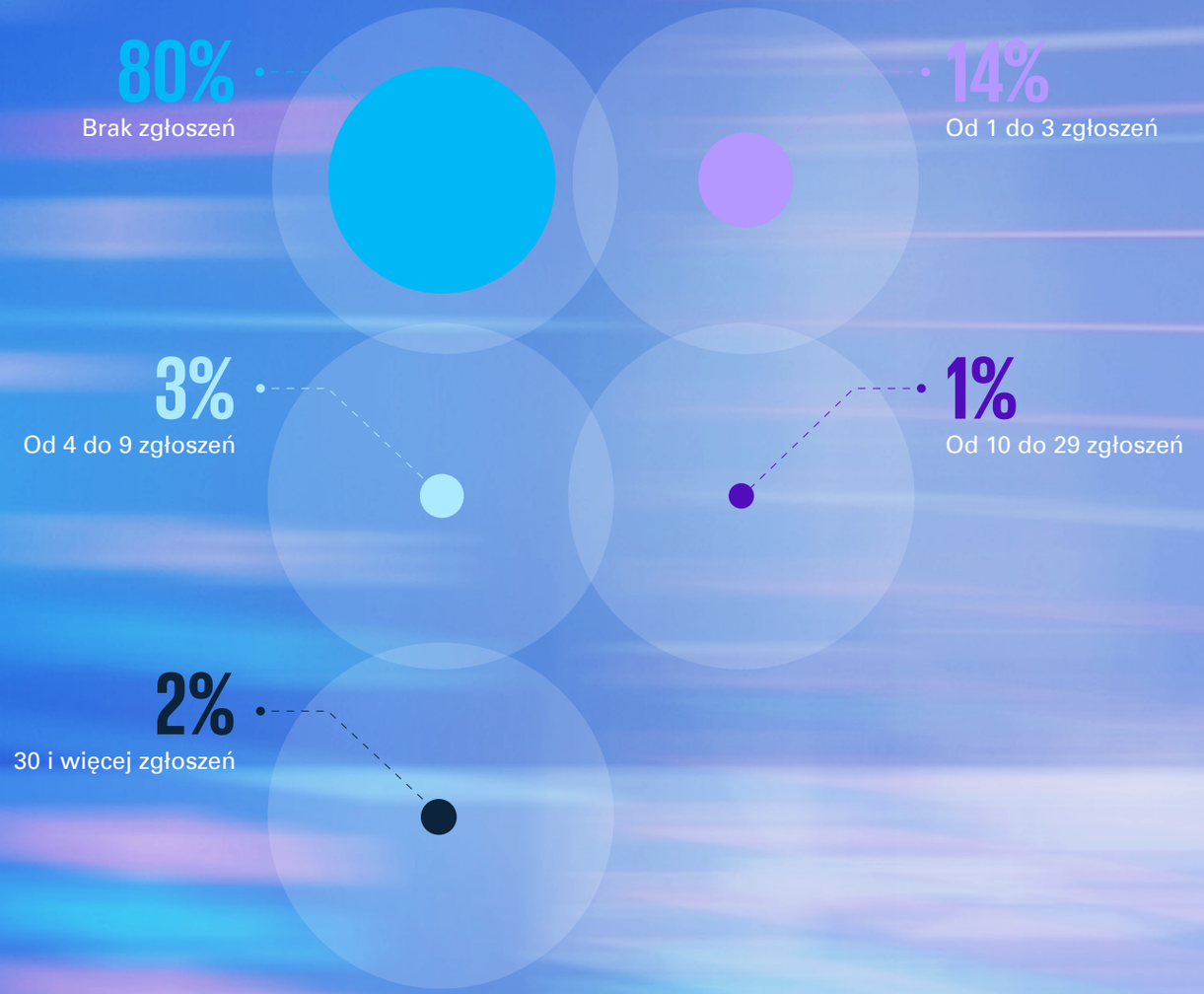
Jeżeli analiza zdarzenia wykaże istotne ryzyko naruszenia praw lub wolności osób fizycznych, konieczne może być powiadomienie organu nadzoru, a niejednokrotnie również osób, których te dane dotyczą. Odnosi się to do sytuacji, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą w stosunku do osób, których dane naruszono.

Podjęcie szybkich i skutecznych działań pozwala zminimalizować potencjalne szkody wobec osób dotkniętych naruszeniem oraz pokazuje zaangażowanie organizacji w przestrzeganie przepisów dotyczących ochrony danych, budując zaufanie klientów i interesariuszy.

Brak właściwej reakcji administratora danych na incydent i niezgłoszenie go do organu nadzoru może skutkować sankcjami przewidzianymi w RODO.

Tegoroczne badanie ujawnia, że w 2023 roku aż 80% firm zadeklarowało, że nie wystąpiły żadne naruszenia ochrony danych, podczas gdy jedynie 2% zgłosiło więcej niż 30 takich przypadków.

Analiza liczby zgłoszeń do Prezesa UODO



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Ocena kroków po ostatnim naruszeniu zgodności IT

Źródło: KPMG w Polsce na podstawie badania ankietowego.

Nauka na własnych błędach

Ocena kroków po ostatnim naruszeniu zgodności IT jest niezwykle istotnym elementem procesu zapewnienia bezpieczeństwa. Po wykryciu naruszenia, niezbędne jest przeprowadzenie kompleksowej oceny, aby zidentyfikować istniejące luki w systemie zgodności oraz podjąć odpowiednie kroki naprawcze. 44% respondentów w odpowiedzi na takie zdarzenie zapewnia szkolenia swoim pracownikom, a 39% wzmacnia zabezpieczenia IT.

Ponad jedna trzecia wprowadza nowe procedury bezpieczeństwa lub przeprowadza aktualizację. Co ciekawe, taki sam odsetek respondentów niestety nie podejmuje żadnych dodatkowych działań.

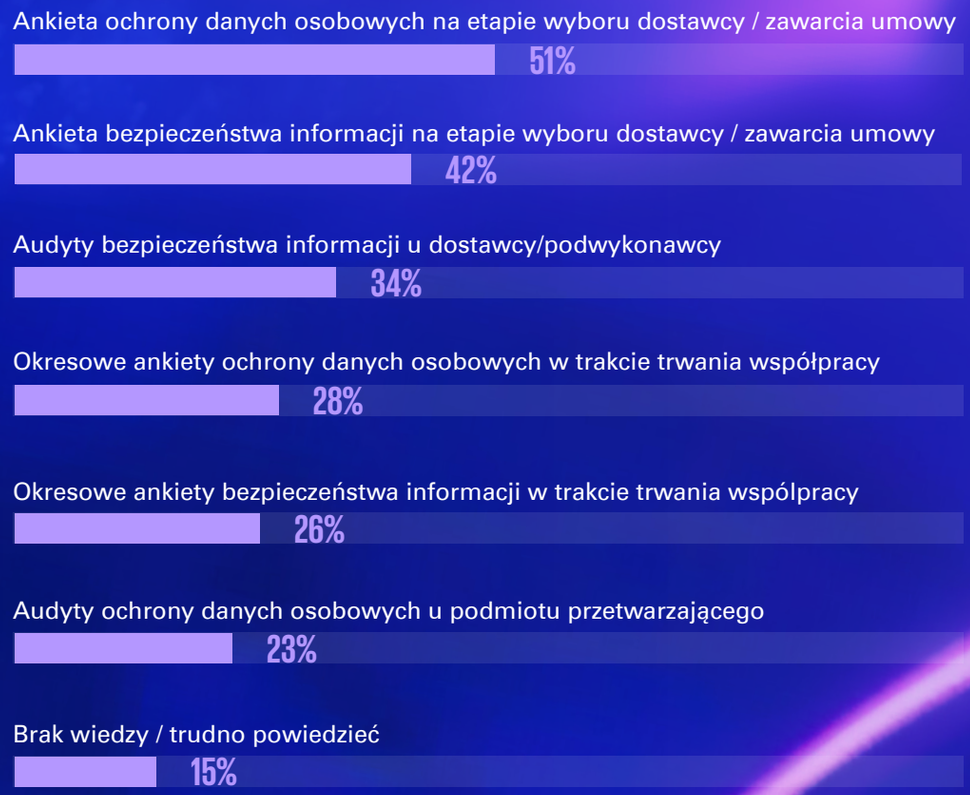
Głównym celem tych przedsięwzięć poza przywróceniem zgodności IT jest wzmocnienie systemu zabezpieczeń oraz prewencja przyszłych incydentów związanych z naruszeniem zgodności.

Bezpieczeństwo partnerów biznesowych

Przedsiębiorstwa funkcjonują dziś w złożonym ekosystemie, składającym się z szeregu współzależnych partnerstw biznesowych. Nie zmniejsza to jednak odpowiedzialności organizacji za zapewnienie bezpieczeństwa przetwarzanych danych.

Organizacje stosują różnorodne strategie i procedury w celu skutecznej weryfikacji oraz nadzoru nad swoimi podwykonawcami. Najczęściej wskazywanym przez respondentów sposobem była ankieta ochrony danych wypełniana na wczesnym etapie umowy, który wskazany został przez ponad połowę biorących udział w badaniu KPMG firm. Inne popularne strategie to ankieta bezpieczeństwa (42%) oraz audyt bezpieczeństwa informacji u podwykonawcy (34%).

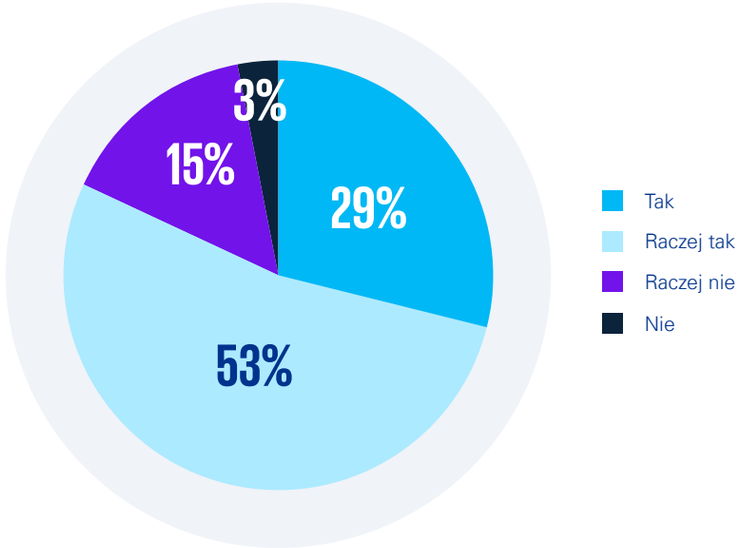
Sposoby weryfikacji i nadzoru podwykonawców



Źródło: KPMG w Polsce na podstawie badania ankietowego.

W poszukiwaniu standardów – RODO w działaniu

Potencjalne zaangażowanie w nowy kodeks postępowania branżowego dotyczącego RODO



Źródło: KPMG w Polsce na podstawie badania ankietowego.

Ogólne rozporządzenie o ochronie danych RODO wprowadziło możliwość opracowywania kodeksów postępowania przez zrzeszenia czy inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających.

Stosowanie kodeksu, potwierdzone przez akredytowany podmiot monitorujący, przynosi szereg korzyści, minimalizując ryzyko prawne. Kodeks branżowy wspiera realizację zasady rozliczalności, a zgodność z jego postanowieniami stanowi dodatkowe potwierdzenie zasady należytej staranności w stosowaniu odpowiednich środków technicznych i organizacyjnych. Takie podejście zapewnia pewnego rodzaju ochronę również w kontekście ewentualnych kar pieniężnych, ponieważ organ nadzorczy, nakładając sankcje, bierze pod uwagę właściwe stosowanie kodeksu postępowania. Nic więc dziwnego, że aż 82% organizacji zadeklarowało swoje zaangażowanie w kodeks właściwy dla swojej branży.

Piotr Burzyk

Starszy Menedżer

Consulting, Zespół Cyberbezpieczeństwa

KPMG w Polsce

Niemal sześć lat obowiązywania ogólnego rozporządzenia o ochronie danych pozwoliło firmom oswoić się z obowiązkami wynikającymi z tej regulacji. Dla zdecydowanej większości organizacji, RODO jest najważniejszym standardem zgodności w obszarze IT i prywatności.

Zauważalne jest ogromne zainteresowanie badanych firm stosowaniem kodeksów postępowania. W Polsce ten instrument zaczyna być coraz bardziej popularny, zwłaszcza po zatwierdzeniu przez Prezesa Urzędu Ochrony Danych Osobowych dwóch kodeksów oraz w wyniku intensywnych prac nad kolejnymi inicjatywami kodeksowymi z różnych branż.

Stosowanie standardów, w tym samoregulacyjnych, ma ułatwiać nie tylko zapewnienie bezpieczeństwa danych przez samych administratorów, ale także wspomóc w nadzorze nad podmiotami przetwarzającymi dane na ich zlecenie. Jak pokazują wyniki badania, ocena ryzyka prywatności stron trzecich (Third Party Privacy Risk Assessment) w trakcie trwania kontraktu nie jest jeszcze powszechną praktyką, pomimo że odpowiedzialność administratora nie kończy się na etapie wyboru procesora.

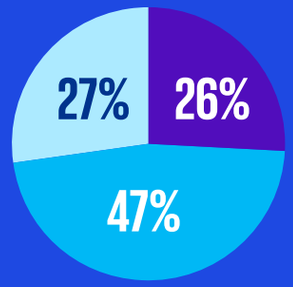
Ponieważ RODO jest neutralne technologicznie, co oznacza, że nie zabrania żadnej formy technologii ani nie zmusza do korzystania z którejkolwiek z nich, coraz większe znaczenie nabierają regulacje o charakterze technicznym, nakierowane na poprawę cyberbezpieczeństwa, takie jak NIS2 czy DORA, zwłaszcza w kontekście ochrony danych osobowych.

Tymczasem dynamiczny rozwój technologiczny stawia przed firmami przetwarzającymi dane osobowe kolejne wyzwania, związane z wykorzystywaniem technologii opartych na rozwiązaniach chmurowych oraz mechanizmów sztucznej inteligencji.

Informacje o badaniu

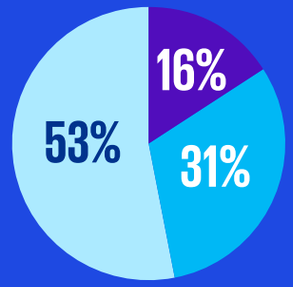
Badanie przeprowadzono za pomocą wywiadów telefonicznych CATI wśród osób zajmujących się bezpieczeństwem IT w firmach, takich jak członkowie zarządu, dyrektorzy ds. bezpieczeństwa, dyrektorzy IT i inne osoby odpowiedzialne za ten obszar. Próba badawcza obejmowała 100 organizacji o przychodach przekraczających 51 milionów złotych, reprezentujących różnorodne branże. Badanie zostało zrealizowane przez firmę Norstat Polska na przełomie 2023 i 2024 roku.

Wielkość badanych firm



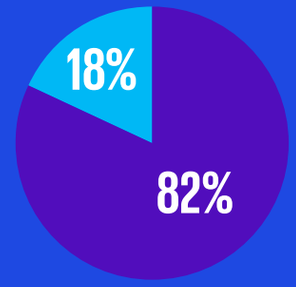
- duże (od 250 osób)
- średnie (50-249 osób)
- małe (max. 50 osób)

Przychody badanych firm



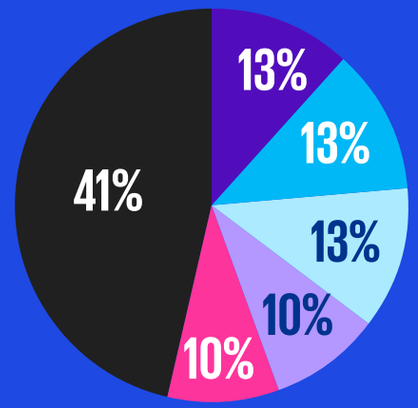
- powyżej 200 mln PLN
- od 101 do 200 mln PLN
- od 51 do 100 mln PLN

Typ kapitału



- polski
- zagraniczny

Branża firmy

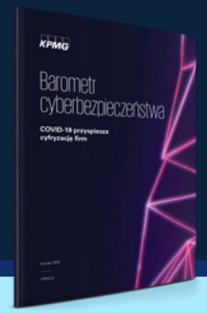


- usługowa
- motoryzacyjna
- budowlana
- transportowa/logistyczna
- handlowa
- pozostałe

Wybrane publikacje KPMG w Polsce i na świecie

Barometr Cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu (2023)

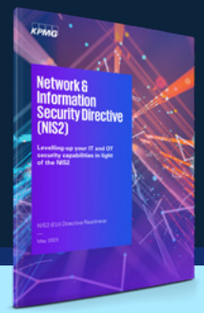
Barometr Cyberbezpieczeństwa. Ochrona cyfrowej tożsamości (2022)



Barometr Cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm (2021)

Cyberbezpieczeństwo w ESG

Dylematy Cyberbezpieczeństwa



Dyrektywa NIS2

Prywatność w czasach AI

Maintaining cyber vigilance and staying resilient

Cybersecurity considerations 2024

Digital Operational Resilience Act

Kontakt

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

Michał Kurek
Partner

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

E: michalkurek@kpmg.pl

Piotr Burzyk
Starszy Menadżer

Consulting, Zespół Cyberbezpieczeństwa

KPMG w Polsce

E: pburzyk@kpmg.pl

Marcin Kieszkowski
Starszy Menadżer

Consulting, Zespół Cyberbezpieczeństwa

KPMG w Polsce

E: mkieszkowski@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