RAPORT

VIII EDYCJA
2025

Cyberbezpieczeństwo w polskich firmach

VECTO

SPIS treści

WSTĘP

Szanowni Państwo,

Oddajemy w Państwa ręce kolejną edycję Raportu „Cyberbezpieczeństwo w polskich firmach", przygotowanego przez VECTO cyklicznie i stanowiącego diagnozę dojrzałości polskiego rynku w obszarze ochrony danych oraz odporności na zagrożenia cyfrowe. Kluczową wartością raportu jest porównywalność danych: w każdej edycji wracamy do stałego rdzenia pytań, dzięki czemu możliwe jest obserwowanie trendów w świadomości ryzyka, gotowości organizacyjnej i realnych praktykach bezpieczeństwa. Jednocześnie raport musi nadążać za rzeczywistością - dlatego w 2025 roku rozszerzyliśmy badanie o obszary, które w ostatnich kilkunastu miesiącach stały się szczególnie istotne dla firm i instytucji w Polsce.

Niniejsza edycja Raportu powstaje w momencie szczególnym. Polska znajduje się w regionie, w którym cyberprzestrzeń stała się jednym z narzędzi oddziaływania geopolitycznego wrogich państw. Oprócz klasycznej cyberprzestępczości nastawionej na zysk obserwujemy incydenty o charakterze zakłócającym i destrukcyjnym, wymierzone w instytucje, sektory strategiczne oraz elementy infrastruktury krytycznej. Dla biznesu oznacza to wzrost ryzyka bezpośredniego oraz pośredniego - poprzez łańcuchy dostaw i zależności od dostawców usług cyfrowych.

W tym samym czasie, polskie przedsiębiorstwa transformują się cyfrowo. Firmy przenoszą dane i procesy do chmury, rozwijają modele pracy zdalnej, integrują systemy z partnerami, automatyzują finanse i obsługę klienta, a coraz częściej wdrażają narzędzia oparte o sztuczną inteligencję. Te zmiany zwiększają produktywność, ale poszerzają też „powierzchnię ataku" poprzez zwiększoną liczbę kont, urządzeń, dostępów i uprawnień. W takim środowisku cyberbezpieczeństwo przestaje być kwestią wyłącznie technologiczną i staje się elementem zarządzania ryzykiem biznesowym oraz wskaźnikiem odporności operacyjnej.
Ważnym kontekstem dla niniejszego Raportu są również zmiany regulacyjne. Oprócz utrwalonych już obowiązków związanych z RODO, na znaczeniu zyskują wymagania wynikające z NIS_2 oraz krajowych przepisów dotyczących Krajowego Systemu Cyberbezpieczeństwa. Dodatkowo upowszechnienie narzędzi AI wymusza nowe zasady zarządzania informacją, szczególnie w kontekście ochrony danych, ograniczenia „shadow IT", weryfikacji ryzyk i edukacji pracowników. Właśnie dlatego w 2025 roku wprowadziliśmy pytania, które pozwalają zobaczyć, na jakim etapie jest polski rynek w tych dwóch obszarach.

Celem naszego Raportu - niezmiennie od 2017 roku - jest dostarczenie możliwie pełnego obrazu rynku i weryfikacja tego, co polskie firmy deklarują, a co realnie wdrażają, gdzie widać postęp, a gdzie kumulują się słabe punkty. Wierzymy, że opracowanie będzie użyteczne dla zarządów, menedżerów IT, osób odpowiedzialnych za finanse, a także dla wszystkich, którzy współtworzą cyberbezpieczeństwo w organizacji.

Serdecznie zapraszam do lektury.
Jakub Wychowański
Prezes Zarządu VECTO

KONTEKST 2025:

zagrożenia, praktyka cyfrowa i regulacje

Zanim przejdziemy do wyników ankiety, warto osadzić je w realnym pejzażu 2025 roku - zarówno w Polsce, jak i globalnie. Ten kontekst wyjaśnia, dlaczego niektóre wyniki rosną szybciej niż inne i dlaczego część obszarów, jak tożsamość, procedury finansowe czy dostawcy, staje się dziś kluczowa.

Rok 2025 był kolejnym, w którym cyberbezpieczeństwo w Polsce pozostawało silnie związane z sytuacją geopolityczną. W praktyce oznacza to większą liczbę działań zakłócających i presji operacyjnej, szczególnie wobec instytucji publicznych oraz sektorów strategicznych. Utrzymuje się też wysoka aktywność cyberprzestępcza o motywacji finansowej - ransomware, kradzież danych, spoofing oraz kampanie phishingowe.

W ubiegłym roku uwagę opinii publicznej zwróciły m.in. incydenty dotyczące instytucji państwowych i sektorów wrażliwych. W marcu 2025 r. wykryto cyberatak na infrastrukturę IT Polskiej Agencji Kosmicznej[1] (POLSA), a instytucja czasowo odłączyła swoją sieć od Internetu w celu zabezpieczenia systemów. W tym samym miesiącu media informowały o cyberataku na Szpital MSWiA w Krakowie[2],

w którym wdrożono procedury awaryjne, a działania wspierały krajowe zespoły reagowania. Incydenty tego typu pokazują, że ryzyko dotyczy zarówno sfery publicznej, jak i sektorów, od których zależy zdrowie oraz bezpieczeństwo wszystkich obywateli.

Na przełomie 2025/2026 roku CERT Polska opublikował szczegółowy raport[3] z cyberincydentu w sektorze energii, który wymierzony był m.in. w farmy wiatrowe i fotowoltaiczne oraz jedną z dużych elektrociepłownię. W opisie incydentu pojawia się m.in. wykorzystanie złośliwego oprogramowania typu wiper oraz rola rozwiązań EDR w blokowaniu destrukcyjnych działań. Ten przykład pokazuje, że obok ransomware rośnie znaczenie ataków nastawionych na zakłócenie działania i sabotaż, a jednocześnie potwierdza, jak ważne staje się wczesne wykrywanie i efektywna odpowiedź na wystąpienie tego typu incydentów.

W 2025 roku w Europie obserwowano również wzrost aktywności grup realizujących ataki DDoS, które motywowane były ideologicznie. W lipcu 2025 r. media opisywały międzynarodową operację służb, koordynowaną przez Europol, wymierzoną w infrastrukturę związaną z prorosyjską siecią NoName057(16)[4]. Choć skala działań różni się między krajami i sektorami, trend jest czytelny: zakłócanie dostępności usług staje się narzędziem presji i elementem krajobrazu zagrożeń w naszym regionie.

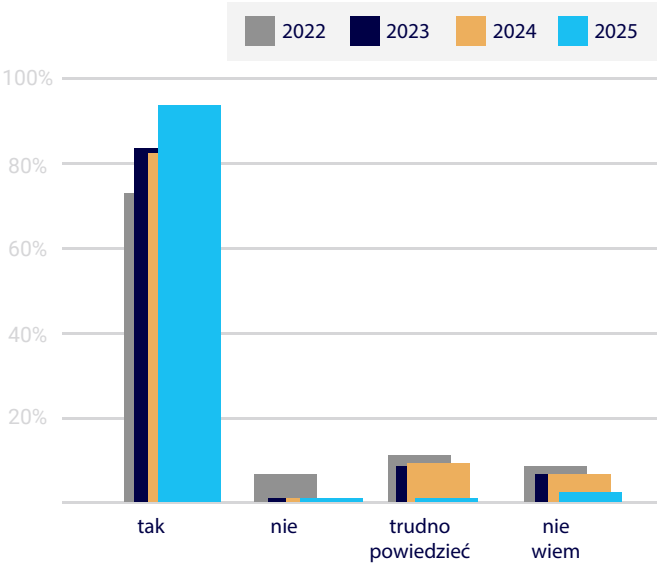
Równolegle globalne raporty wskazują na kilka stałych zjawisk, które mocno wpływają również na polskie organizacje. Po pierwsze, rośnie znaczenie ataków opartych o tożsamość - skradzione dane uwierzytelniające, przejęte konta i nadużycia zaufanych kanałów. Po drugie, silnie rośnie skala socjotechniki wspieranej sztuczną inteligencją. Raport CrowdStrike[5] za 2025 r. wskazuje m.in. na wielokrotny wzrost vishingu (socjotechnika głosowa), co wprost przekłada się na ryzyko oszustw BEC i prób wyłudzania przelewów czy zmian danych kontrahentów. Po trzecie, rośnie ryzyko „trzeciej strony": Verizon Data Breach Investigations Report 2025[6] zwraca uwagę, że udział naruszeń z udziałem dostawców/partnerów rośnie, a ransomware pozostaje istotnym składnikiem wielu incydentów.

Istotnym tłem 2025 roku są także regulacje. NIS_2[7] wzmacnia podejście oparte o zarządzanie ryzykiem, odpowiedzialność oraz raportowanie incydentów w określonych ramach czasowych. Dla wielu organizacji oznacza to konieczność formalizacji: analizy luk, planu wdrożenia, polityk i procesów, a także oceny bezpieczeństwa dostawców. Z kolei AI Act wprowadza wymagania stosowane stopniowo - m.in. obowiązki związane z AI literacy, governance dla modeli ogólnego przeznaczenia oraz szersze stosowanie zasad w kolejnych latach. W praktyce oznacza to, że zasady korzystania z rozwiązań AI w firmach stają się elementem zarządzania informacją i zgodności, a nie wyłącznie kwestią „dobrych praktyk".

NAJWAŻNIEJSZE

wnioski z badania 2025

Zacznijmy od kluczowych obserwacji, które następnie rozwinięte zostaną w analizie poszczególnych obszarów.



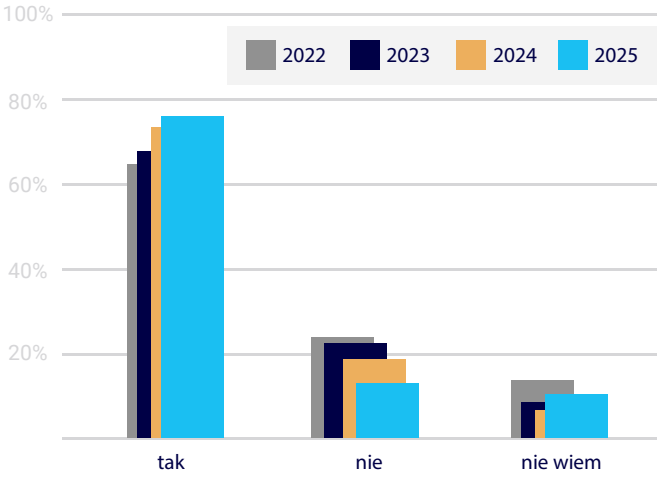
Czy uważasz, że zabezpieczanie danych informatycznych w firmie jest ważne?

Po pierwsze, świadomość konieczności ochrony danych IT osiągnęła rekordowy poziom: 91,4 proc. respondentów uznaje, że zabezpieczanie danych informatycznych w firmie jest ważne. Jest to wyraźny skok względem poprzedniego roku (2024: 81,3 proc.), co sugeruje, że rynek coraz częściej traktuje cyberbezpieczeństwo jako element ciągłości działania, a nie jako temat incydentalny.

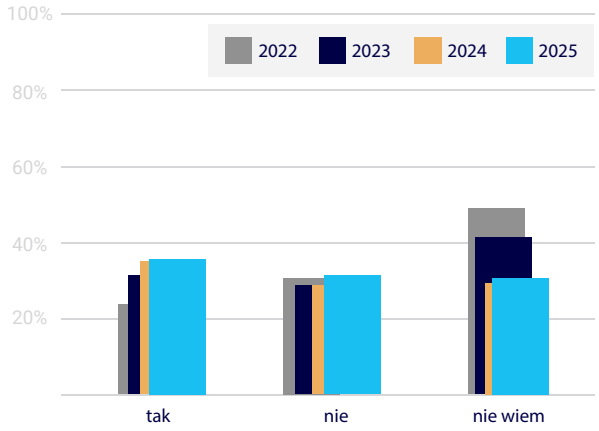
Po drugie, doświadczenie incydentów jest powszechne: 76,2 proc. badanych deklaruje,

76 proc. ankietowanych deklaruje, że ich firma zetknęła się z cyberatakiem.

że ich firma zetknęła się z cyberatakiem. Oznacza to, że dla dużej części organizacji cyberzagrożenia przestały być hipotezą i stały się realnym czynnikiem ryzyka, z którym trzeba żyć i zarządzać nim długofalowo.

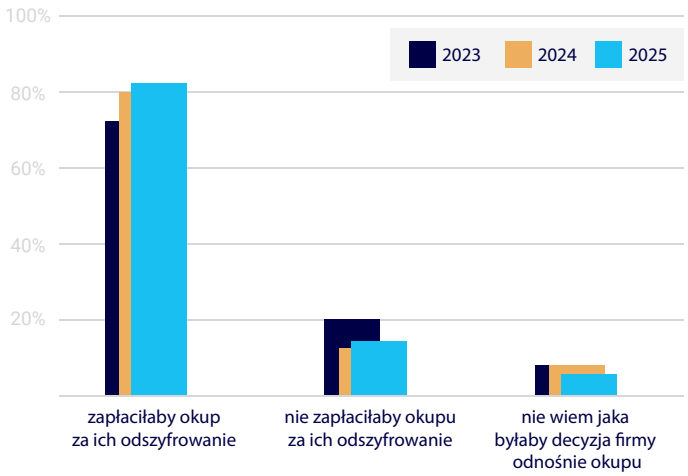


Czy Twoja firma zetknęła się kiedykolwiek z cyberatakiem?



Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

Po trzecie, utrzymuje się luka między świadomością a praktyką. Tylko 35,4 proc. firm monitoruje zagrożenia, a 30,8 proc. posiada przygotowany scenariusz postępowania na wypadek incydentu. To oznacza, że wiele organizacji wciąż funkcjonuje w trybie reaktywnym: dowiaduje się o incydencie późno, a decyzje podejmowane są pod presją czasu i skutków biznesowych.



Co zrobiłaby Twoja firma po skutecznie przeprowadzonym ataku typu ransomware, skutkującym zaszyfrowaniem wszystkich danych?

Po czwarte, ransomware pozostaje scenariuszem, który rynek postrzega jako szczególnie groźny. Aż 81,5 proc. respondentów uważa, że po zaszyfrowaniu wszystkich danych firma zapłaciłaby okup, co może być sygnałem ograniczonej pewności co do skuteczności kopii zapasowych, testów odtworzeniowych i planów ciągłości działania. Ten wątek powraca w dalszej części raportu w kontekście odporności i testów backupów.

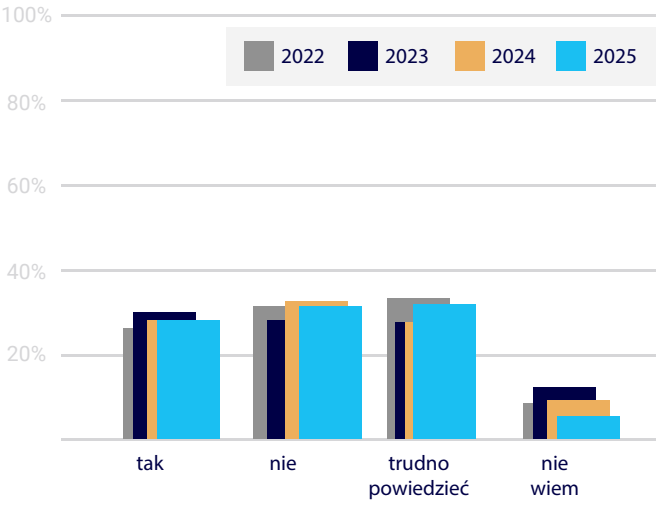
Wreszcie, rok 2025 przyniósł dwa nowe obszary, które będą w coraz większym stopniu determinować ryzyko w 2026 roku: **bezpieczeństwo tożsamości (wdrożenia uwierzytelniania wieloskładnikowego) oraz nadzór nad narzędziami GenAI.** To właśnie w tych tematach polskie firmy mają dziś największą przestrzeń do szybkiej poprawy przy relatywnie wysokim zwrocie z inwestycji.

Przejdźmy do

KONKRETÓW!

1. Świadomość i percepcja ryzyka

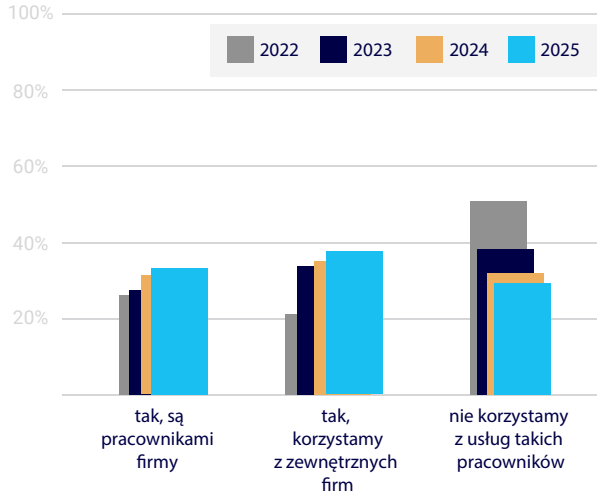
Z perspektywy wielu lat prowadzenia badań widać, że 2025 rok jest momentem, w którym świadomość cyberbezpieczeństwa została w dużej mierze „zinternalizowana" przez pracowników. 91,4 proc. odpowiedzi „tak" na pytanie o wagę zabezpieczenia danych to nie tylko deklaracja, ale też efekt rosnącej liczby incydentów, większej obecności tematu w mediach oraz wzrostu zależności biznesu od usług cyfrowych. Jednocześnie ocena własnego bezpieczeństwa pozostaje niska. Na pytanie, czy sieć w firmie jest prawidłowo zabezpieczona, tylko 27,6 proc. respondentów odpowiada „tak", a 32,8 proc. mówi wprost „nie". Wysoki pozostaje też udział odpowiedzi „trudno powiedzieć" (34,5 proc.). Ten wynik warto czytać jako sygnał braku mierzalności: w wielu organizacjach bezpieczeństwo nie jest opisane wskaźnikami, nie jest okresowo audytowane lub nie ma jednoznacznego właściciela procesu, który potrafiłby ocenić sytuację bez intuicyjnych założeń.W pytaniach o źródła zagrożeń i podatności widoczna jest rosnąca świadomość, że atak nie zawsze pochodzi „z zewnątrz". Chociaż wciąż dominuje obraz „nieznanych grup hakerów", respondenci coraz częściej wskazują na rolę czynnika ludzkiego i procesów: błędy użytkowników, nieostrożność, brak procedur oraz presję czasu. To ważny trend, bo nowoczesne ataki - szczególnie oparte na technice przejmowania kont i socjotechnice - wykorzystują przede wszystkim luki organizacyjne, a nie wyłącznie techniczne.



Czy uważasz, że sieć w Twojej firmie jest prawidłowo zabezpieczona?

2. Kompetencje i odpowiedzialność za bezpieczeństwo

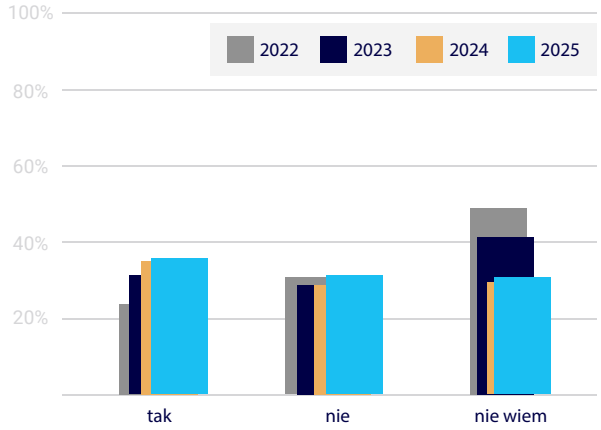
Na tle wcześniejszych lat pozytywnie wygląda profesjonalizacja obszaru bezpieczeństwa. W 2025 roku 34,1 proc. firm deklaruje, że specjalista ds. bezpieczeństwa jest pracownikiem organizacji, a 38,4 proc. korzysta z kompetencji zewnętrznych. Model usługowy (outsourcing) rośnie szybciej niż budowa kompetencji wewnątrz firmy, co jest zrozumiałe w segmencie MŚP: zapewnia dostęp do kompetencji i narzędzi bez konieczności budowania pełnego zespołu. Jednocześnie outsourcing nie zastąpi odpowiedzialności: organizacja musi rozumieć, za co płaci, jak wygląda zakres monitoringu i reakcji oraz jakie są czasy obsługi incydentu.



Czy Twoja firma zatrudnia specjalistę od bezpieczeństwa danych w firmie?

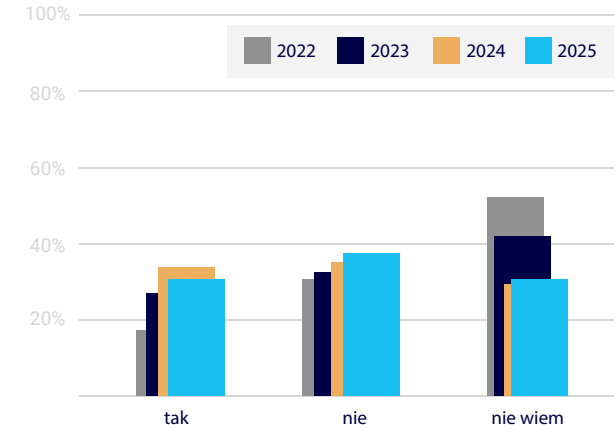
3. Monitoring zagrożeń i gotowość na incydent

Monitoring zagrożeń zadeklarowało w 2025 roku 35,4 proc. firm. W porównaniu z 2022 rokiem (22 proc.) widać poprawę, jednak przy skali codziennego doświadczania cyberataków jest to, w opinii twórców Raportu, wciąż poziom niski. W praktyce oznacza to, że wiele organizacji niezmiennie dowiaduje się o incydencie dopiero wtedy, gdy jest on widoczny biznesowo - gdy systemy przestają działać, użytkownicy tracą dostęp albo pojawia się wymuszenie okupu. Tymczasem skuteczna odpowiedź na incydent zależy od wczesnego wykrycia i szybkiej deeskalacji.

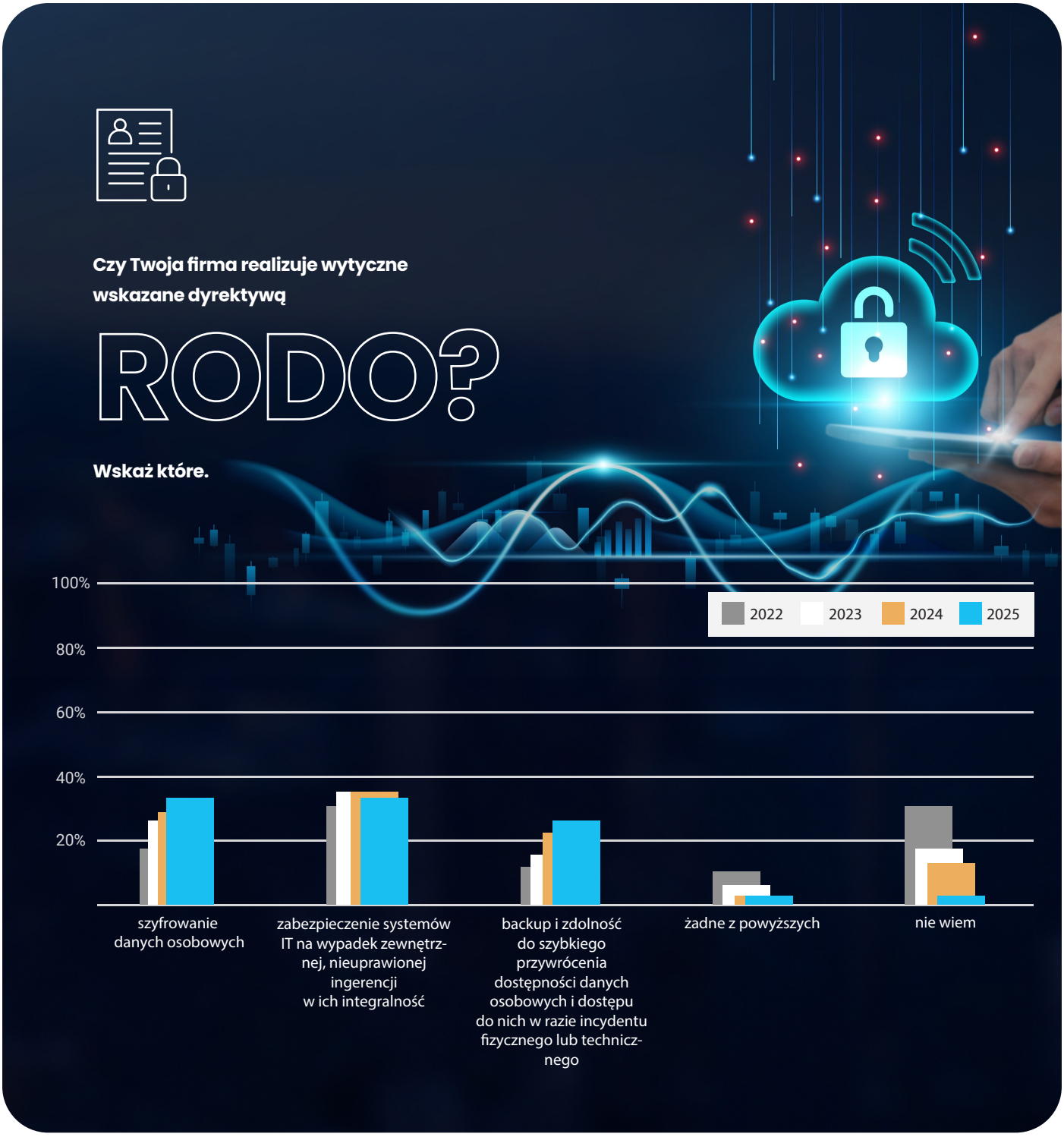


Czy Twoja firma monitoruje zagrożenia wynikające z cyberprzestępczości?

Podobnie wygląda gotowość proceduralna. Scenariusz postępowania w przypadku incydentu deklaruje 30,8 proc. firm, a 38,9 proc. odpowiada „nie". Co istotne, w 2025 roku ten wskaźnik jest nieco niższy niż w 2024 (34,9 proc.). Można to interpretować na dwa sposoby: część organizacji mogła „przeszacować" swoją gotowość w 2024 r., a w 2025 r. odpowiedzi stały się bardziej ostrożne; albo rzeczywiście w praktyce procedury nie stały się standardem. W obu przypadkach wniosek jest podobny: firmy potrzebują prostych, testowanych planów - kto podejmuje decyzje, jak wygląda komunikacja, jak uruchamia się odtworzenia systemów, kiedy wchodzi w grę zgłoszenie do organów i klientów.



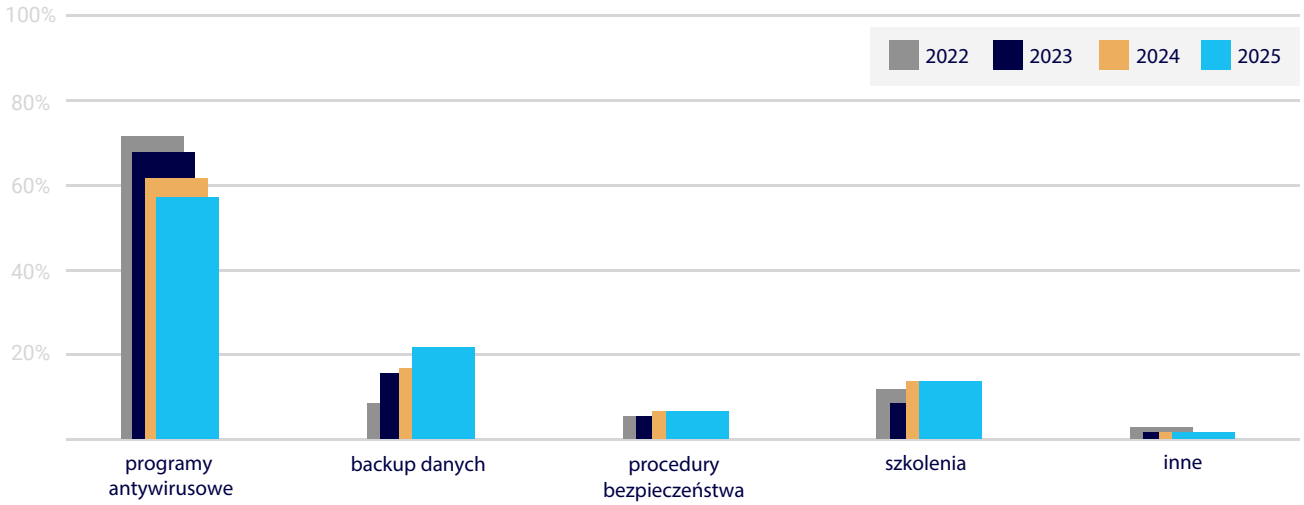
Czy Twoja firma ma przygotowany scenariusz postępowania w przypadku wystąpienia incydentu naruszającego bezpieczeństwo danych w firmie?



4. Zabezpieczenia w świetle RODO - praktyka i luki

RODO jest obecne w polskich organizacjach od lat, ale w praktyce poziom wdrożenia środków technicznych i organizacyjnych pozostaje zróżnicowany. Pytanie o realizację wytycznych dyrektywy (w raporcie: szyfrowanie, zabezpieczenie systemów, backup i zdolność do szybkiego przywrócenia dostępności) pokazuje, które elementy są w firmach najczęściej rozumiane jako „RODO w IT", a które pozostają najsłabsze. Warto podkreślić, że w wielu organizacjach RODO bywa kojarzone głównie z dokumentacją i zgodami, podczas gdy kluczowe są właśnie praktyki bezpieczeństwa: kontrola dostępu, szyfrowanie, czy kopie zapasowe.

Wybierz metodę, która Twoim zdaniem jest najskuteczniejszą w ochronie przed cyberzagrożeniami:



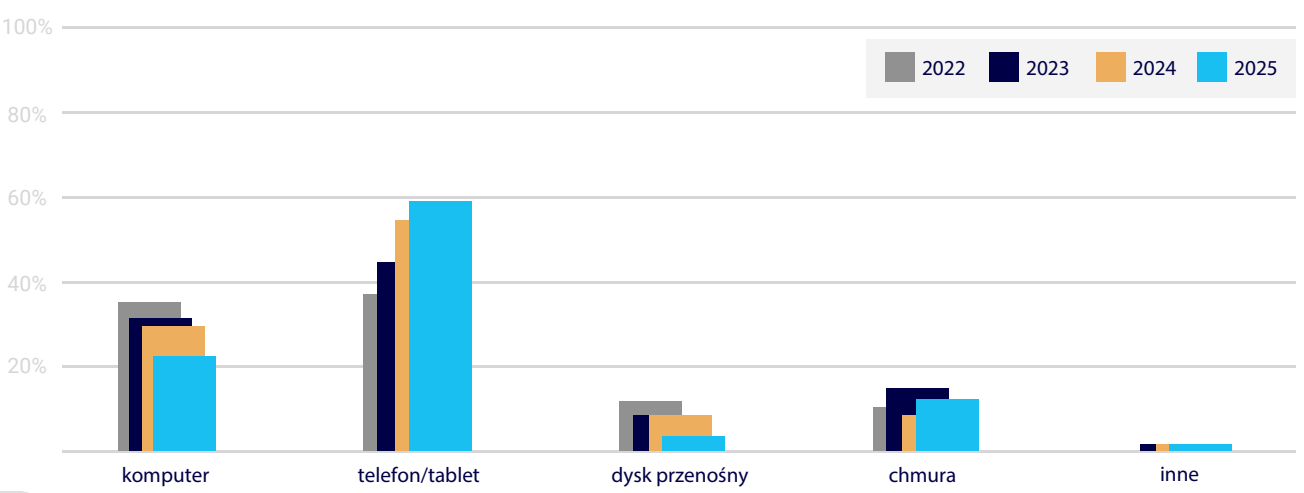
5. Narzędzia i podejście do ochrony - co rynek uznaje za najskuteczniejsze

Interesujące wnioski przynosi pytanie o to, co respondenci uznają za najskuteczniejszą metodę ochrony przed cyberzagrożeniami. Odpowiedzi zwykle rozkładają się między „narzędzia" (np. antywirus), „backup" oraz „procedury i szkolenia". W 2025 roku warto zwrócić uwagę na rosnącą rolę podejścia procesowego: w świecie ataków opartych o tożsamość i socjotechnikę sama technologia nie wystarczy, jeśli organizacja nie ma procedur weryfikacji dyspozycji finansowych, zasad klasyfikacji informacji czy procesu nadawania i odbierania uprawnień.

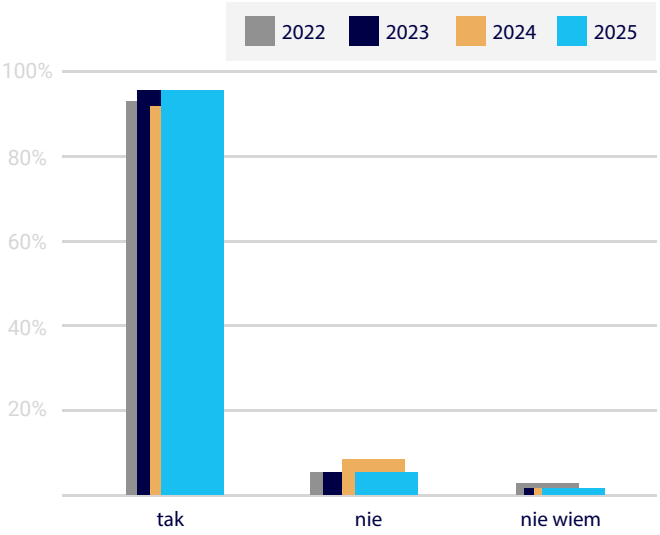
6 Dane, urządzenia i praktyka użytkowników

Transformacja cyfrowa powoduje, że bezpieczeństwo przenosi się na poziom codziennych praktyk użytkowników: gdzie są dane, jak chronione są urządzenia, czy mieszają się zastosowania prywatne i służbowe oraz jak organizacja zabezpiecza pracę zdalną. Wyniki dotyczące miejsc przechowywania danych pokazują zmianę modelu pracy: coraz większy udział chmury i urządzeń mobilnych, mniejsza rola nośników przenośnych. To trend korzystny z perspektywy centralizacji i możliwości zarządzania, ale tylko pod warunkiem, że organizacja potrafi kontrolować dostęp, stosuje uwierzytelnianie MFA, zarządza uprawnieniami i ma zasady przechowywania danych.

Gdzie przechowujesz najcenniejsze dla siebie dane?



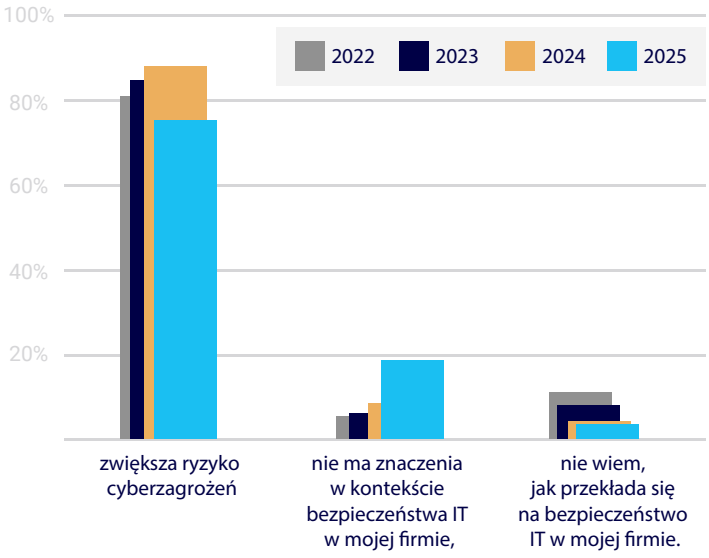
Jednocześnie w 2025 roku 94,2 proc. respondentów deklaruje wykorzystywanie firmowego komputera lub telefonu do celów prywatnych. Takie zachowanie samo w sobie nie jest zaskoczeniem - w modelu pracy hybrydowej granice się zacierają - ale ma konsekwencje: większa ekspozycja na aplikacje i usługi poza kontrolą firmy, większe ryzyko phishingu, a także większa rola rozwiązań zarządzania urządzeniami mobilnymi (MDM) i separacji danych służbowych.



Czy używasz firmowego komputera/ telefonu do celów prywatnych?

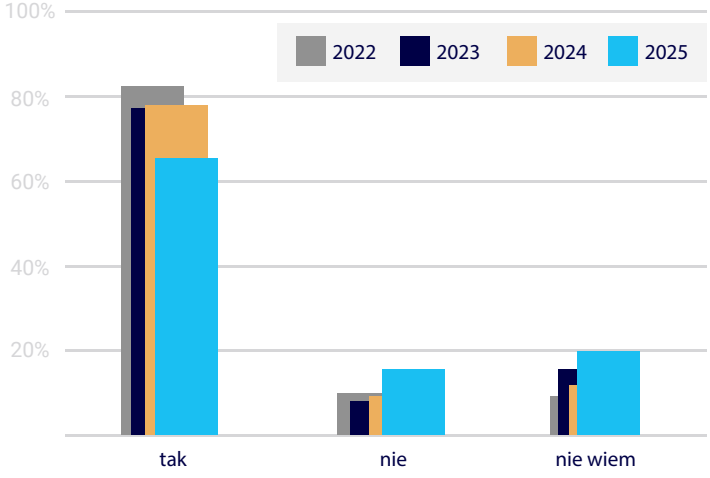
Percepcja ryzyka pracy zdalnej zmieniła się w porównaniu z 2024 rokiem. W 2025 roku zmniejszył się odsetek respondentów, którzy uważają, że praca zdalna zwiększa ryzyko cyberzagrożeń (76,6 proc.vs 87,2 proc.). Spadek względem poprzedniego roku może oznaczać oswojenie modelu hybrydowego lub przekonanie, że wdrożone zabezpieczenia są już wystarczające. Jednak dane o praktyce sugerują ostrożność: dodatkowe zabezpieczenia dla pracowników zdalnych wdrożyło 39,4 proc. firm. Ten wynik jest ważny, bo w wielu współczesnych atakach kanałem wejścia są konta pocztowe i narzędzia współpracy używane właśnie poza biurem.

Praca zdalna, Twoim zdaniem:



39 proc. firm wdrożyło dodatkowe zabezpieczenia dla pracowników zdalnych

Czy praca zdalna, Twoim zdaniem, wpłynęła bezpośrednio na konieczność inwestowania w rozwiązania IT w Twojej firmie?

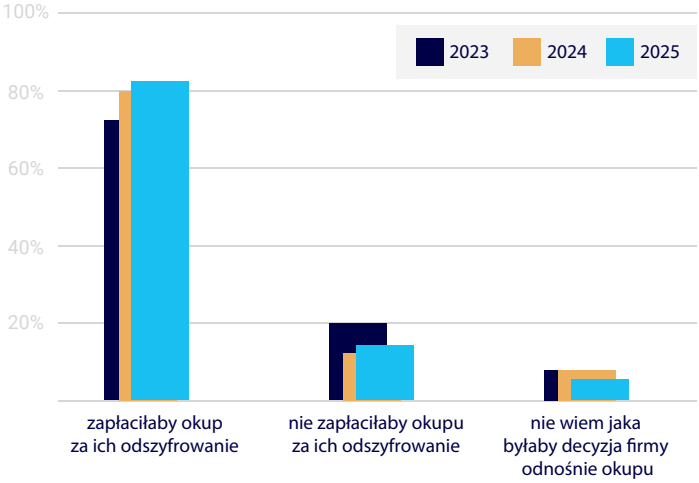


7. Ransomware i odporność organizacji

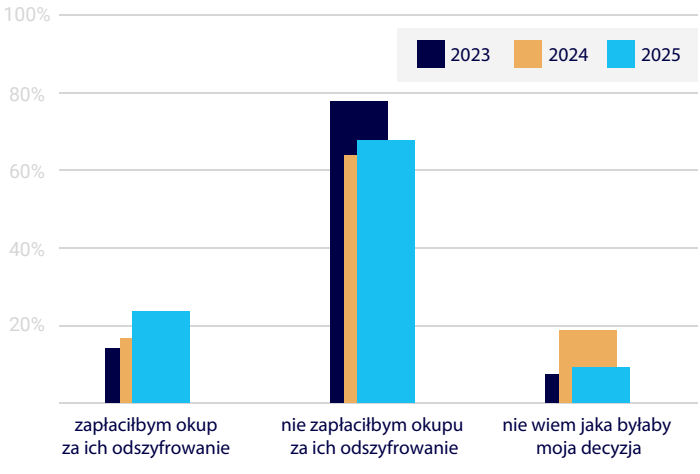
Ransomware pozostaje jednym z najpoważniejszych scenariuszy ryzyka. Wymusza decyzje pod presją czasu i bezlitośnie uderza w zdolność firmy do działania. W 2025 roku 81,5 proc. respondentów uważa, że po zaszyfrowaniu wszystkich danych firma zapłaciłaby okup. Tak wysoki odsetek jest czytelnym sygnałem: wiele organizacji nie ma pewności, że jest w stanie szybko odtworzyć krytyczne systemy bez współpracy z przestępcami. Jednocześnie globalne badania pokazują, że w praktyce część firm płaci, ale część unika płatności dzięki odporności i przygotowaniu. Raport Sophos[8] z 2025 r. wskazuje, że „niemal połowa" firm dotkniętych ransomware decyduje się zapłacić, przy czym wiele organizacji negocjuje kwoty. Z perspektywy zarządczej wniosek jest prosty: przygotowanie (backup, testy, plan reakcji) przesuwa firmę z pozycji „musimy zapłacić" do pozycji „mamy opcje".

Odpowiedzi dotyczące analogicznej sytuacji, ale w kontekście danych prywatnych są znacząco inne. Gdy pytamy respondentów o to, czy zapłaciliby okup za odszyfrowanie wyłącznie ich prywatnych danych, „tak" deklaruje 22,8 proc., a „nie" 67,9 proc.. Ta różnica między perspektywą osobistą a firmową dobrze pokazuje mechanizm presji: w firmie stawką jest ciągłość działania, zobowiązania wobec klientów i koszty przestoju, które potrafią być wyższe niż okup. Tym bardziej rośnie znaczenie odporności technicznej i procesowej.

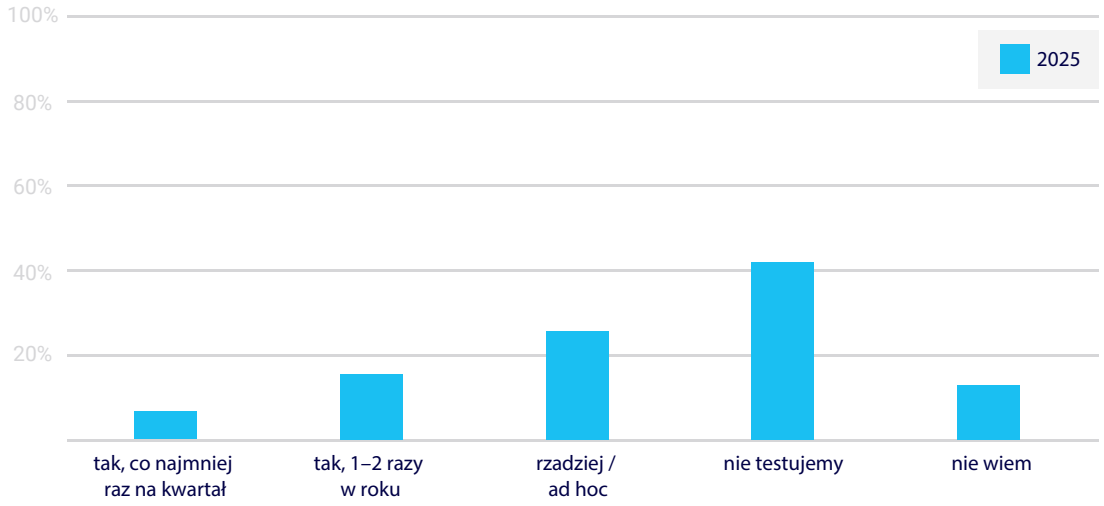
Po skutecznie przeprowadzonym ataku typu ransomware, skutkującym zaszyfrowaniem wszystkich danych, Twoja firma?



Czy gdyby atak ransomware dotyczyłby wyłącznie Twoich danych prywatnych:



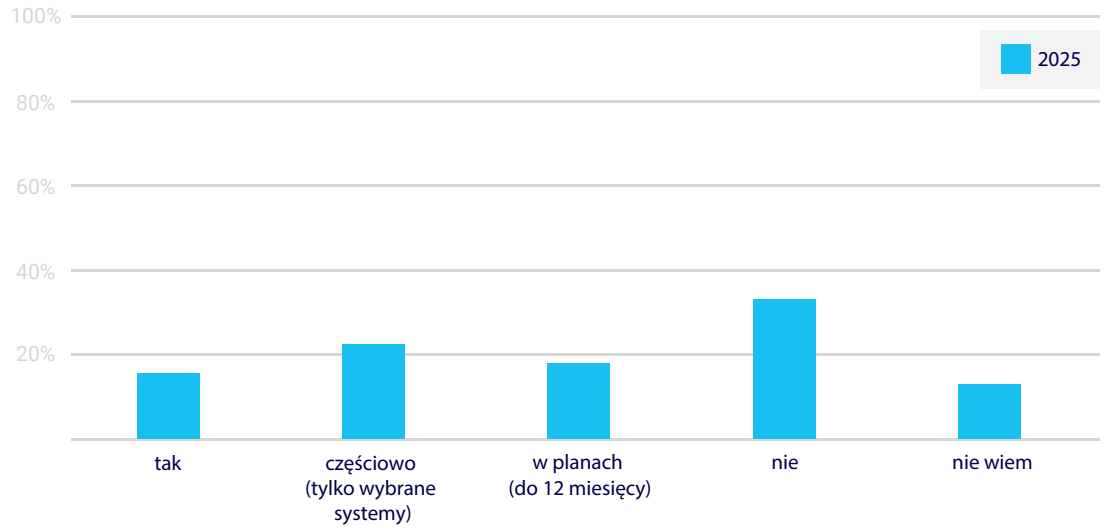
Czy testujecie odtwarzanie danych z backupu (restore test)?



Posiadanie kopii zapasowej nie jest równoznaczne z odpornością na ransomware. Współczesne grupy atakujące coraz częściej próbują najpierw przejąć środowisko backupowe, a dopiero potem szyfrują dane produkcyjne lub doprowadzają do wycieku informacji. Z tego powodu kluczowe są dwa elementy: regularne testy odtwarzania oraz kopie odporne na modyfikację. W 2025 roku testowanie odtwarzania danych deklaruje zróżnicowany odsetek firm - część wykonuje je kwartalnie, część raz-dwa razy w roku, a część w ogóle. Z perspektywy odporności liczy się nie tylko częstotliwość, ale też zakres: czy test dotyczy systemów krytycznych, czy obejmuje pełny łańcuch (backup-restore-walidacja) i czy wyniki testów są raportowane do osób decyzyjnych.

Podobnie jest z kopiami odpornymi na ransomware. Sama deklaracja posiadania backupu to za mało, jeśli w tym samym czasie zostaną zaszyfrowane również kopie zapasowe. Rozwiązania niezmienialne oraz pozostające offline zmieniają kalkulację ryzyka, ponieważ utrudniają atakującym „zabranie" firmie jedynej drogi powrotu do działania.

Czy posiadacie kopie zapasowe odporne na ransomware?



8. Nowe wyzwania wymagają świeższej analizy.

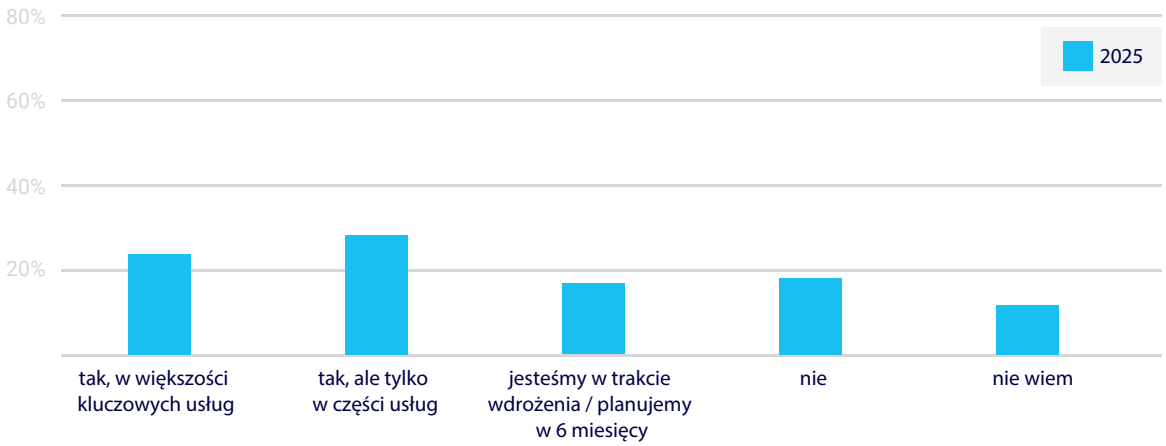
Premierowe pytania w Raporcie

W 2025 roku do raportu dodano blok pytań odpowiadających na najważniejsze trendy w cyberbezpieczeństwie: ochronę tożsamości, detekcję i reakcję, odporność na ransomware, bezpieczeństwo łańcucha dostaw oraz przygotowanie regulacyjne. Część tych pytań, które pojawiają się w raporcie po raz pierwszy, otwierają możliwość obserwowania kolejnych trendów w nadchodzących latach.

Jednym z nich jest pytanie o wdrożenia uwierzytelniania wieloskładnikowego (MFA) w kluczowych systemach (poczta, VPN, ERP/CRM, chmura). Wyniki z 2025 roku pokazują rynek w fazie wdrożeń, ale bez pełnej standaryzacji. 23 proc. firm deklaruje MFA w większości kluczowych usług, 27 proc. stosuje je tylko częściowo, a 18 proc. jest w trakcie wdrożenia lub planuje je w najbliższych miesiącach. Jednocześnie istotny jest udział odpowiedzi „nie" oraz „nie wiem", co wskazuje, że w części technologie MFA wciąż nie są traktowane jako standard.

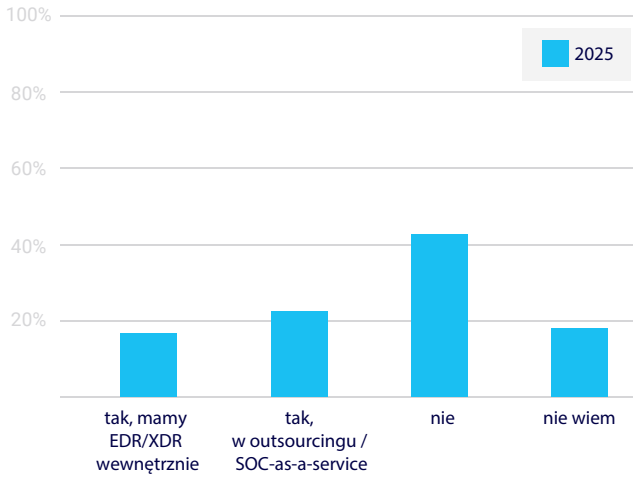
Tymczasem w kontekście trendów globalnych MFA zyskuje rolę „pierwszej linii obrony" w atakach opartych o przejęcie kont. Tam, gdzie przestępcy wykorzystują skradzione hasła, jednorazowe kody, aplikacje uwierzytelniające lub klucze sprzętowe potrafią znacząco ograniczyć skuteczność ataków. Jednocześnie MFA samo w sobie nie rozwiązuje problemu, jeśli organizacja nie uzupełnia go o procesy: bezpieczne odzyskiwanie kont, kontrolę uprawnień administracyjnych i monitoring anomalii logowań.

Czy w kluczowych systemach/usługach (poczta, VPN, ERP/CRM, chmura) Twoja firma wdrożyła (uwierzytelnianie wieloskładnikowe)?

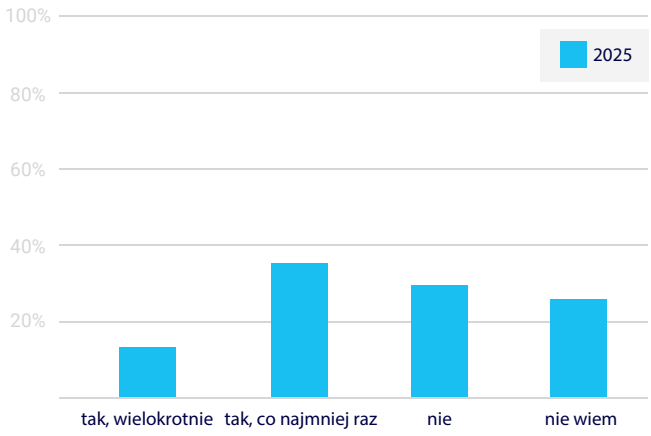


9. EDR/XDR oraz wykrywanie incydentów

Kolejnym elementem dojrzałości jest zdolność do wykrywania i reagowania na incydenty na stacjach roboczych i serwerach. W 2025 roku część organizacji posiada EDR/XDR wewnętrznie, część korzysta z usług zewnętrznych (SOC-as-a-service), a część nie ma takich rozwiązań. Ten obszar jest szczególnie ważny, co dowodzi przywołany na początku niniejszego Raportu cyberincydent w sektorze z końca 2025 roku. CERT Polska wyraźniej wskazał, że rozwiązanie klasy EDR odegrało kluczową rolę w blokowaniu destrukcyjnych działań.



Czy stosujecie rozwiązania EDR/XDR lub macie taką usługę w outsourcingu?



Czy w ostatnich 12 miesiącach odnotowaliście próby oszustwa typu BEC, w tym z użyciem AI?

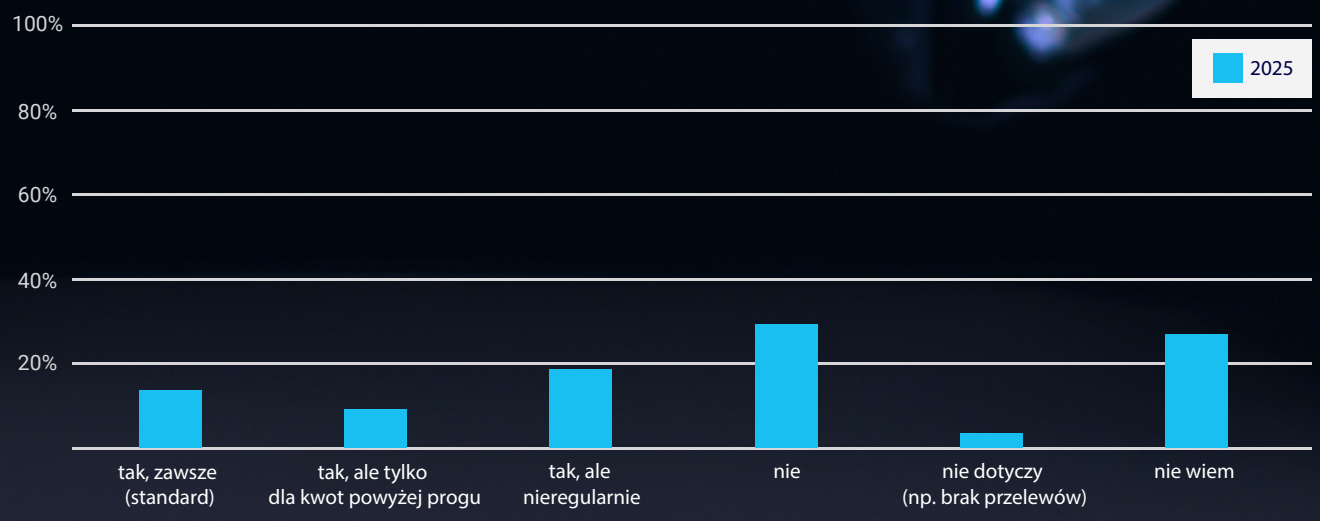
10. BEC i procedury finansowe

Oszustwa typu BEC (Business Email Compromise), polegające na podszyciu się pod przełożonego lub kontrahenta są jednym z najgroźniejszych scenariuszy strat finansowych. Co prawda, respondenci nie wykazują dużej wiedzy na temat tego typu ataków, ale upowszechnienie GenAI drastycznie zwiększa ich wiarygodność i z pewnością skala tego typu zagrożeń będzie rosła. Zresztą potwierdzają to dane globalne - Raport CrowdStrike wskazuje na dynamiczny wzrost socjotechniki głosowej (vishing), co wprost przekłada się na ryzyko podszywania się pod osoby decyzyjne.

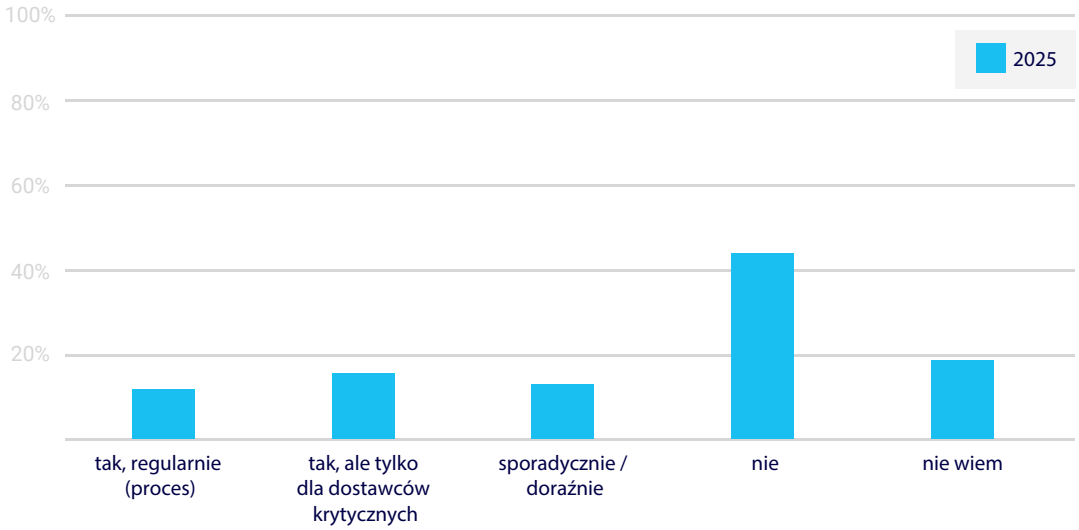
Czy macie obowiązkową

PROCEDURĘ WERYFIKACJI

„wrażliwych dyspozycji" (np. zmiana numeru konta dostawcy, pilny przelew) niezależnym kanałem (np. call-back / 2-osobowa autoryzacja)?

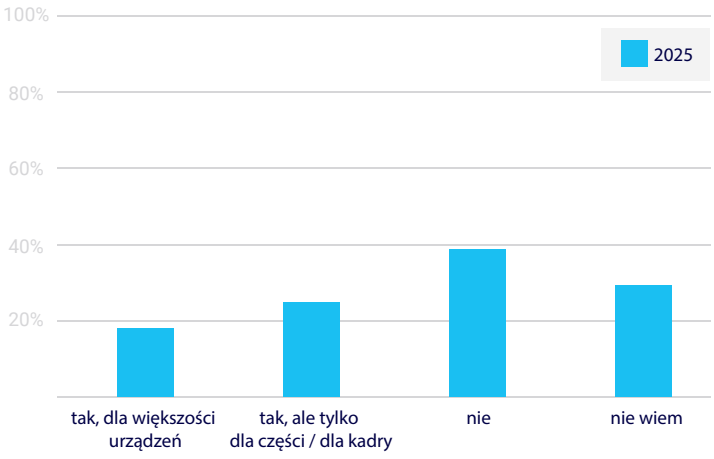


Równolegle autorzy Raportu zadali pytanie o to, czy organizacje mają obowiązkową procedurę weryfikacji „wrażliwych dyspozycji" niezależnym kanałem - typu call-back, dwuosobowa autoryzacja czy potwierdzenie przez drugi lub niezależny kanał komunikacji. To obszar, w którym stosunkowo proste procedury potrafią dać bardzo wysoki zwrot: wiele incydentów BEC jest skutecznych właśnie dlatego, że organizacja nie ma ustalonego standardu i działa pod presją czasu. W tym kontekście dane z ankiet świadczą o konieczności skuteczniejszego zagospodarowania tego typu ryzyk - 56 proc. respondentów wskazało tu odpowiedź „nie" lub „nie wiem", jako standard zaś procedurę weryfikacji wskazuje wyłącznie 12 proc. badanych firm.



11. MDM i porządkowanie mobilności

Centralne zarządzanie urządzeniami mobilnymi (MDM) jest coraz ważniejsze, bo smartfony i tablety stały się kluczowym narzędziem pracy. MDM pozwala wymuszać minimalny standard bezpieczeństwa: PIN, szyfrowanie, zdalne wymazanie, separację danych służbowych. Wyniki analizy odpowiedzi na pytanie o dostępność tego typu rozwiązań wskazują, że ponownie ponad połowa firm nie stosuje narzędzi MDM. Zwiększa to drastycznie potencjalne zagrożenia, szczególnie w sytuacji, gdy respondenci badania deklarują - w zasadzie powszechne - używanie służbowych urządzeń do celów prywatnych.



Czy firmowe urządzenia mobilne są zarządzane centralnie (MDM) — np. wymuszanie PIN, zdalne wymazanie, separacja danych służbowych?

Czy oceniacie cyberbezpieczeństwo dostawców/ partnerów (np. ankieta, wymagania w umowie, audyt, obowiązek zgłaszania incydentów)?

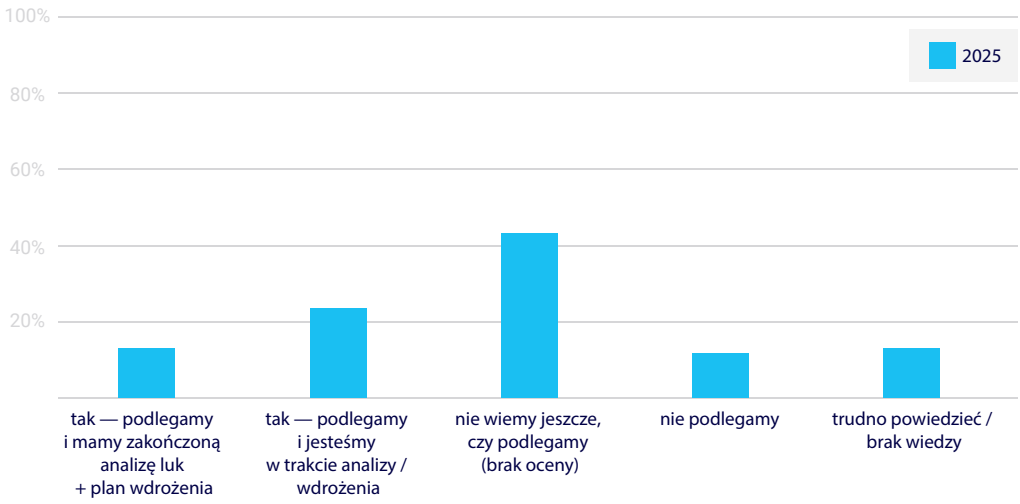
12. Bezpieczeństwo dostawców i łańcuch dostaw

Wyniki pytania o weryfikację stosowania rozwiązań z zakresu cyberbezpieczeństwa przez dostawców i uczestników łańcucha dostaw pokazują wyraźną lukę: do regularnego analizowania tego typu danych lub procesów przyznaje się wyłącznie 11 proc. respondentów, część (16 proc.) ogranicza się do dostawców krytycznych, a duża grupa nie ma tego typu procedur w ogóle lub nie potrafi tego ocenić. W świetle trendów globalnych jest to obszar, który będzie w 2026 roku rosnąć na znaczeniu - nie tylko z powodu incydentów u dostawców, ale też przez wymagania regulacyjne i oczekiwania dużych klientów.

13. NIS2/KSC i gotowość regulacyjna

Autorzy Raportu zapytali również respondentów o to, czy ich organizacja podlega wymaganiom NIS_2/znowelizowanemu Krajowemu Systemowi Cyberbezpieczeństwa[9] oraz na jakim etapie są te przygotowania. Wyniki wyraźnie wskazują, że w tym aspekcie największą barierą może być nie wdrożenie, ale sam etap rozpoznania czy organizacja podlega regułom NIS2/nowelizacji KSC. Duży udział odpowiedzi „nie wiemy jeszcze,

Czy organizacja zidentyfikowała, czy podlega wymaganiom NIS2 / noweli-zacji KSC i na jakim etapie jest przygotowanie?

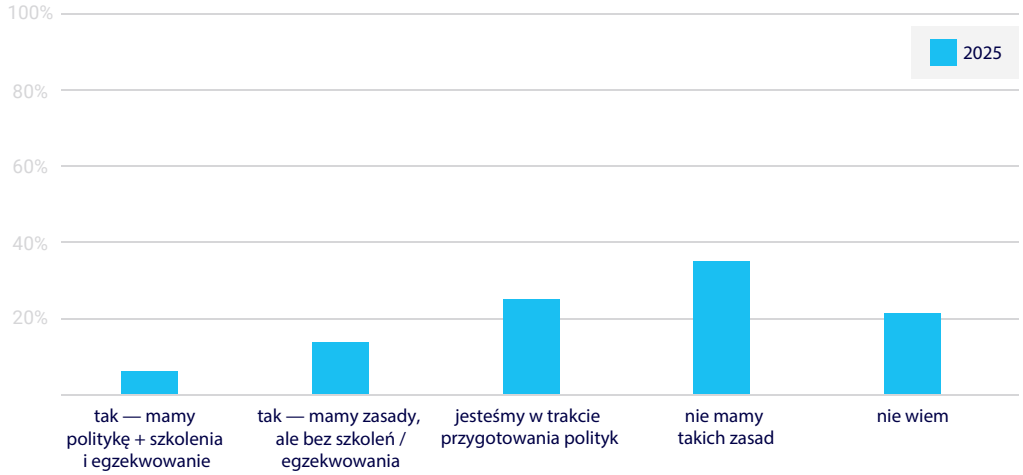


czy podlegamy" (42 proc.) i „Trudno powiedzieć/brak wiedzy" (12 proc.) oznacza ryzyko opóźnienia całego procesu: analizy luk, planu wdrożenia, budżetu i przypisania ról. Tymczasem NIS2 wzmacnia podejście procesowe: zarządzanie ryzykiem, raportowanie incydentów, kontrola dostawców i utrzymywanie zdolności reagowania.

14. Zasady korzystania z GenAI (AI Act)[10]

Edycja 2025 niniejszego badania po raz pierwszy prezentuje odpowiedzi na pytanie o zasady korzystania z narzędzi AI/GenAI (np. ChatGPT, Copilot) w kontekście ochrony danych i oceny ryzyk. To jeden z najszybciej rosnących obszarów ryzyka „miękkiego": wycieki informacji do narzędzi zewnętrznych, przetwarzanie danych wrażliwych poza kontrolą organizacji, a także powstawanie shadow IT. Wyniki z 2025 roku dowodzą, że rynek jest w fazie przejściowej: część organizacji buduje polityki, część nie ma zasad, a niewielka część ma pełny model obejmujący szkolenia i egzekwowanie. W 2025 roku zaledwie 5 proc. firm deklaruje posiadanie polityki wraz ze szkoleniami i egzekwowaniem, 14 proc. ma zasady bez szkoleń/egzekwowania, a 24 proc. jest w trakcie przygotowania polityk. Jednocześnie 36 proc. wyraźnie wskazuje na brak zasad, a 21 proc. nie potrafi tego ocenić. W praktyce oznacza to, że w wielu organizacjach użycie GenAI może odbywać się poza kontrolą i bez jasnych granic dotyczących bezpieczeństwa czy poufności danych.

Warto dodać, że AI Act wprowadza wymagania stopniowo, a jednym z najwcześniejszych elementów jest nacisk na AI literacy oraz governance. Oznacza to, że organizacje powinny już teraz inwestować w podstawowe zasady i edukację: co wolno wprowadzać do narzędzi, jak klasyfikować informacje, jak korzystać z wersji firmowych narzędzi, jakie są ryzyka prompt injection oraz w jaki sposób weryfikować wyniki generowane przez AI.



Czy firma ma zasady korzystania z narzędzi AI/GenAI (np. ChatGPT/copilot), obejmujące ochronę danych i ocenę ryzyk (zgodnie z AI Act)?

REKOMENDACJE

i perspektywa na 2026 rok

Jak wynika z analizy odpowiedzi respondentów, **priorytetem na 2026 rok dla polskich firm i instytucji powinno być uporządkowanie fundamentów bezpieczeństwa:** tożsamości i dostępu, kopii zapasowych oraz procedur reagowania. W praktyce oznacza to upowszechnienie MFA w kluczowych usługach, wprowadzenie standardów dla kont uprzywilejowanych oraz uzupełnienie technologii o procesy odzyskiwania kont i reagowania na anomalie logowań.

Drugim filarem jest odporność na ransomware. Wysoka deklarowana skłonność do zapłaty okupu sugeruje, że część organizacji wciąż nie ma pewności co do zdolności odzyskania kontroli nad zaszyfrowanymi danymi. Tymczasem kopie odporne na modyfikację oraz regularne testy odtwarzania powinny być dziś powszechnym standardem, a nie działaniem „od święta". Równolegle organizacje powinny posiadać uzgodniony na poziomie zarządczym scenariusz decyzyjny, w tym kryteria komunikacji, zgłoszeń, współpracy z dostawcami i ocenę ryzyk, również wizerunkowych, wynikających z płacenia okupu.

Trzecim priorytetem jest bezpieczeństwo procesów finansowych i ochrona przed BEC. W świecie rosnącej wiarygodności socjotechniki procedury weryfikacji dyspozycji (call-back, zasada dwóch par oczu, progi kwotowe, weryfikacja zmiany danych kontrahenta) są jednymi z najbardziej efektywnych kosztowo mechanizmów ograniczania strat.

Czwartym obszarem jest ryzyko łańcucha dostaw. Organizacje powinny - co najmniej dla dostawców krytycznych - wdrożyć podstawowy proces: wymagania bezpieczeństwa w umowach, obowiązek zgłaszania incydentów, minimalne standardy (MFA, backup, monitoring), a w wybranych przypadkach audyt lub ankietę oceny. Trend wzrostu naruszeń z udziałem podmiotów trzecich sprawia, że brak takiego procesu będzie coraz bardziej kosztowny.

Wreszcie, 2026 rok będzie czasem porządkowania użycia narzędzi AI. Wysoki odsetek polskich firm, które nie mają uregulowanych zasad wykorzystania tego typu technologii pokazuje, że rynek potrzebuje prostych, praktycznych polityk: klasyfikacji danych, listy dozwolonych narzędzi, zasad przechowywania promptów i wyników oraz szkoleń z ryzyk (wycieki, halucynacje, prompt injection, socjotechnika). Wprowadzenie tych elementów zmniejsza bowiem ryzyko operacyjne i ułatwi osiąganie zgodności z nadchodzącymi aktualnymi i nadchodzącymi wymaganiami, wynikającymi z regulacji prawnych.

PODSUMOWANIE

Raport „Cyberbezpieczeństwo w polskich firmach 2025" pokazuje rynek w fazie wysokiej świadomości zagrożeń i rosnącej zależności od usług cyfrowych. Jednocześnie utrzymują się wyraźne różnice między deklarowaną troską o bezpieczeństwo a dojrzałością procesów. Monitoring zagrożeń i scenariusze postępowania po incydencie wciąż nie są standardem, a postrzeganie ransomware jako sytuacji, w której „trzeba będzie zapłacić", sugeruje potrzebę wzmocnienia odporności backupu i zdolności odzyskiwania ciągłości procesów.

Raport za rok 2025 wprowadza do badania obszary, których analiza w kolejnych latach będzie kluczowa dla wiedzy o cyberodporności: ochronę tożsamości (MFA) oraz zasady korzystania z GenAI w kontekście ochrony danych i zarządzania ryzykiem. Włączenie tych pytań tworzy podstawę do obserwowania trendów i oceny czy rynek nadąża za zmianami w sposobie pracy i w poddanym bezustannym zmianom krajobrazie współczesnych cyberzagrożeń.

Perspektywa na 2026 rok obejmuje jednocześnie wzrost presji regulacyjnej (NIS2/KSC, AI Act), dalszą digitalizację procesów oraz rozwój ataków opartych o tożsamość i socjotechnikę wspieraną AI. W takim środowisku przewagę zyskają organizacje, które zbudują spójny system ochrony: połączą technologię z procesami, zapewnią widoczność (monitoring), przygotują efektywne scenariusze reakcji oraz uporządkują zarządzanie dostawcami i użyciem GenAI.

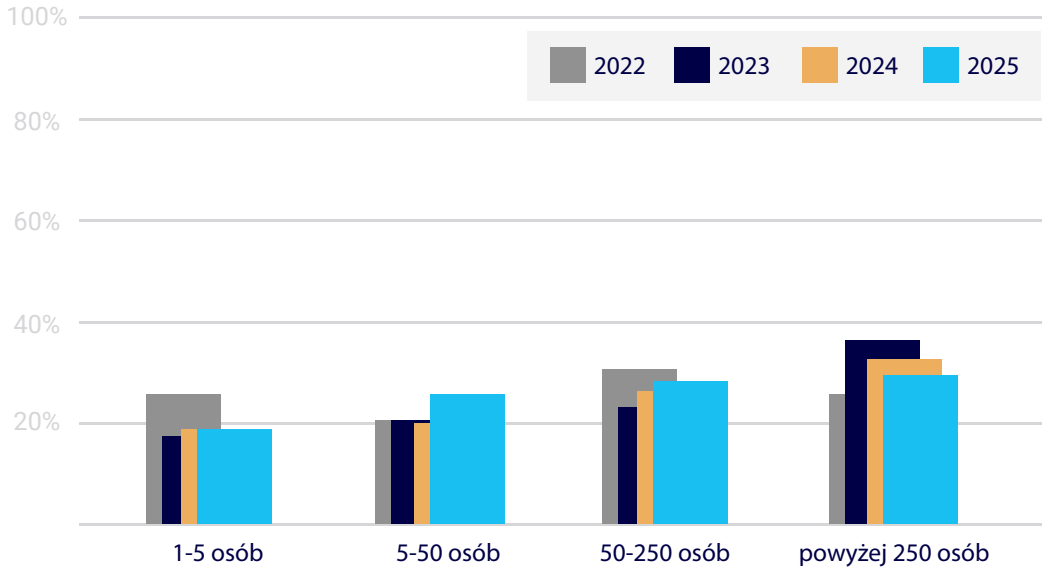
O RAPORCIE

i metodologii

Raport powstał w oparciu o badanie ankietowe realizowane cyklicznie przez VECTO. Rdzeń pytań, powtarzany w kolejnych edycjach, pozwala obserwować trendy w świadomości ryzyka, ocenie własnej gotowości oraz w podejmowanych działaniach. W edycji 2025 zachowano zestaw pytań trendowych, a jednocześnie rozszerzono ankietę o pytania odpowiadające na nowe zjawiska: ochronę tożsamości (MFA), zaawansowaną detekcję i reagowanie (EDR/XDR), oszustwa BEC wspierane AI, odporność kopii zapasowych, zarządzanie urządzeniami mobilnymi (MDM), bezpieczeństwo łańcucha dostaw oraz gotowość regulacyjną (NIS2/KSC, AI Act).

Struktura respondentów w edycji 2025 pokazuje istotny udział sektorów szczególnie wrażliwych na incydenty: finanse i bankowość, administracja publiczna oraz ochrona zdrowia. Wśród respondentów dominowali przedstawiciele dużych firm (powyżej 250 osób) - 29,3 proc., firmy średniej wielkości (50-250 osób) - 27,4 proc. oraz małych firm (5-50 osób) - 24,1. 19,2 proc. odpowiedzi pochodziło od przedstawicieli mikroprzedsiębiorstw, zatrudniających do 5 osób.

Firma, w której pracuję zatrudnia:



Reprezentuję branżę: (metryczka)

budownictwo / architektura / wykończenie wnętrz	1,8 proc.
edukacja / badania naukowe	1,7 proc.
finanse / bankowość	16,3 proc.
gastronomia / hotelarstwo / turystyka / rekreacja / sport	3,3 proc.
handel hurtowy i detaliczny	4,9 proc.
instytucje rządowe i samorządowe	15,7 proc.
łączność / telekomunikacja	7,4 proc.
media / kultura i sztuka / rozrywka	2,9 proc.
medycyna / ochrona zdrowia	13,6 proc.
produkcja / dystrybucja / logistyka	4,1 proc.
przemysł komputerowy / oprogramowanie	9,7 proc.
przemysł komputerowy / sprzęt	5,1 proc.
usługi dla firm / usługi dla ludności	7,2 proc.
usługi internetowe	2,4 proc.
inna	3,9 proc.

PRZYPISY

1. https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowano-polska-agencje-kosmiczna-zadzialaly-sluzby
2. https://www.medonet.pl/zdrowie/wiadomosci,cyberatak-na-szpital-mswia-w-krakowie--moglo-dojsc-do-wycieku-danych,artykul,80167350.html
3. https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/ (30.01.2026).
4. https://www.europol.europa.eu/cms/sites/default/files/documents/Internetowa-przestepczosc-zorganizowana-jak-Europol-zwalcza-cyberprzestepczosc-PL.pdf
5. https://www.crowdstrike.com/en-us/global-threat-report/
6. https://www.verizon.com/business/resources/reports/dbir/
7. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=pl
8. https://www.sophos.com/en-us/content/state-of-ransomware
9. https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1955
10. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689

ORGANIZATOR

badania

VECTO sp. z o.o.

Spółka działa od 2008 roku. Firma łączy kilkudziesięcioletnie doświadczenie kadry kierowniczej z potencjałem młodego zespołu, który rozumie realia rynku IT i wyzwania stojące przed firmami i instytucjami wobec dynamicznie zmieniającej się technologii. Spółka dostarcza i wdraża systemy informatyczne oraz świadczy usługi outsourcingu IT dla firm. Oferuje kompleksowe rozwiązania IT w tym w szczególności zabezpieczania danych oraz backupu w oparciu o produkty renomowanych firm jak również monitoringu infrastruktury i badania jej podatności na incydenty na bazie rozwiązań Open Source. Wszystkie prace wdrożeniowe wykonuje zespół certyfikowanych, doświadczonych inżynierów.

VECTO

www.vecto.pl