Business Growth Review

RAPORT

NIS2 – Czy firmy w Polsce są gotowe na dyrektywę?

PARTNERZY RAPORTU:

Cloud by asseco

trecom

axians

OVHcloud

dhosting.pl

NIS2

Czy firmy w Polsce są gotowe na dyrektywę?

5 kluczowych wniosków

1. 27,4% dużych firm w Polsce nie podjęło praktycznych działań wdrożeniowych NIS2 – znajduje się na etapie analizy luk lub nie rozpoczęło przygotowań.
2. Bezpieczeństwo dostawców (3,0/5) i reagowanie na incydenty (3,21/5) to najsłabsze ogniwa – a zarazem obszary, na które NIS2 kładzie największy nacisk.
3. 37,4% firm nie informuje zarządu o ryzyku cyber, mimo że NIS2 nakłada osobistą odpowiedzialność na członków zarządu za cyberbezpieczeństwo.
4. Tylko 26,4% firm ma dedykowany budżet na NIS2, a 38,3% nie zdefiniowało progów poważnego incydentu – co grozi naruszeniem obowiązku zgłoszenia w 24 godz.
5. Efekt skali jest wyraźny: firmy 1000+ dwukrotnie częściej mają dedykowany budżet i o 11 pp. częściej są w zaawansowanej fazie wdrożeń niż firmy zatrudniające 300–499 pracowników.

Dyrektywa NIS2 (Network and Information Security Directive 2) to jedna z najważniejszych europejskich regulacji dotyczących cyberbezpieczeństwa, która fundamentalnie zmienia podejście do ochrony sieci i systemów informatycznych w państwach członkowskich Unii Europejskiej.

W Polsce jej wdrożenie dotyczy szerokiego spektrum podmiotów – od sektora energetycznego i transportowego, przez bankowość i zdrowie, po infrastrukturę cyfrową i administrację publiczną. Regulacja ta nakłada na organizacje szereg obowiązków: od formalnej oceny czy dyrektywa ich dotyczy, przez **wdrożenie zaawansowanych środków technicznych i organizacyjnych**, aż po raportowanie incydentów w ciągu 24 godzin i osobistą odpowiedzialność członków zarządu za stan cyberbezpieczeństwa.

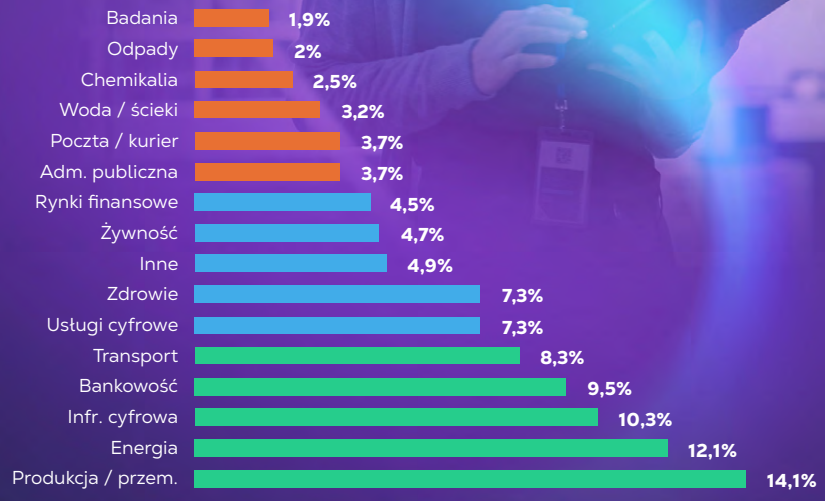
Niniejszy raport prezentuje wyniki kompleksowego badania przeprowadzonego na próbie **1018 firm zatrudniających co najmniej 300 pracowników i prowadzących działalność na terenie Polski.** Badanie objęło organizacje ze wszystkich kluczowych sektorów objętych dyrektywą NIS2, w tym energetykę (12,1%), produkcję i przemysł krytyczny (14,1%), infrastrukturę cyfrową (10,3%), bankowość (9,5%), transport (8,3%), zdrowie (7,3%) oraz dostawców usług cyfrowych (7,3%). Respondentami byli specjaliści i decydenci bezpośrednio zaangażowani w cyberbezpieczeństwo i compliance: CISO i specjaliści ds. bezpieczeństwa (24,8%), CIO i kadra IT (24,3%), osoby z obszaru ryzyka, compliance i audytu (21,6%), członkowie zarządów (14,2%) oraz specjaliści OT (6,7%).

Celem badania było dostarczenie rzetelnego i aktualnego obrazu gotowości dużych polskich firm na wdrożenie wymagań NIS2. Ankieta obejmowała 21 pytań dotyczących m.in. znajomości regulacji, statusu formalnej klasyfikacji, etapu przygotowań, poziomu dojrzałości w 10 kluczowych obszarach cyberbezpieczeństwa, zdolności reagowania na incydenty, zarządzania ryzykiem dostawców, budżetowania oraz identyfikacji największych barier i potrzeb w zakresie wsparcia zewnętrznego. Wyniki badania ukazują zarówno postępy, jak i istotne luki w przygotowaniach polskich organizacji, dostarczając cennych **wskazówek dla firm, doradców, dostawców technologii oraz regulatorów.**

Metodologia badania BGR: NIS2 – czy firmy w Polsce są gotowe na dyrektywę?

Badanie zostało zrealizowane metodą CAWI (Computer Assisted Web Interview) na próbie 1018 firm zatrudniających ponad 300 osób i prowadzących działalność w Polsce na przełomie stycznia-lutego 2026 r. Struktura próby obejmuje 16 sektorów objętych dyrektywą NIS2 oraz respondentów z kluczowych funkcji decyzyjnych w obszarze cyberbezpieczeństwa.

Business Growth Review



Typ badania i wielkość próby

Badanie przeprowadzono techniką CAWI – standaryzowanego wywiadu internetowego realizowanego za pośrednictwem kwestionariusza online. Metoda ta jest powszechnie stosowana w badaniach B2B i pozwala na dotarcie do respondentów pełniących wyspecjalizowane funkcje w organizacjach. Łączna próba wyniosła 1018 kompletnych wywiadów.

Kryterium kwalifikacyjne obejmowało dwa warunki: zatrudnienie powyżej 300 osób oraz prowadzenie działalności na terenie Polski. Oba warunki musiały być spełnione łącznie, co zapewniło jednorodność próby pod kątem wielkości i jurysdykcji regulacyjnej.

Profil respondentów – branże

Struktura sektorowa próby odzwierciedla zakres podmiotowy dyrektywy NIS2, obejmując **zarówno sektory kluczowe, jak i ważne**. Najliczniej reprezentowany jest sektor produkcji i przemysłu krytycznego (14,1%, n=144), infrastruktura cyfrowa – centra danych, chmura, DNS, IXP (10,3%, n=105) oraz energetyka (12,1%, n=123). Bankowość stanowi 9,5% próby (n=97), transport 8,3% (n=84), a zdrowie i dostawcy usług cyfrowych po 7,3%.

Obecne są również sektory o mniejszej reprezentacji: rynki finansowe (4,5%), żywność (4,7%), poczta i kurier (3,7%), administracja publiczna (3,7%), woda i ścieki (3,2%), chemikalia (2,5%), odpady (2%) oraz badania (1,9%). Pozostałe 4,9% to firmy z sektorów sklasyfikowanych jako inne.

Wielkość organizacji i struktura stanowisk

Próba jest **niemal równomiernie rozłożona między trzy segmenty wielkościowe**: firmy 300–499 pracowników (33,1%, n=337), 500–999 (35,4%, n=360) oraz 1000+ (31,5%, n=321). Taki rozkład umożliwia wiarygodne porównania między segmentami i analizę efektu skali.

Respondenci to **osoby bezpośrednio zaangażowane w cyberbezpieczeństwo**: CISO i specjaliści security (24,8%), CIO i kadra IT (24,3%), specjaliści ds. ryzyka, compliance i audytu (21,6%), członkowie zarządów (14,2%), specjaliści OT (6,7%) oraz inne role (8,4%).

Dominacja funkcji bezpieczeństwa i compliance w strukturze respondentów **zapewnia wysoką wiarygodność merytoryczną odpowiedzi**.

Struktura kwestionariusza

Kwestionariusz badawczy obejmował 21 pytań pogrupowanych w sześć bloków tematycznych: screening i klasyfikacja firmy (pytania 1–5), znajomość i status NIS2 (6–8), organizacja i governance (9–11), etap wdrożeń i dojrzałość cyberbezpieczeństwa (12–14), reagowanie na incydenty i dostawcy (15–18) oraz bariery i potrzeby (19–21). Pytanie 14 zawierało ocenę dojrzałości w 10 domenach cyberbezpieczeństwa w skali 1–5, co **pozwoliło na stworzenie szczegółowej mapy kompetencji**. Pytania wielokrotnego wyboru (łącznie cztery) umożliwiły identyfikację złożonych wzorców, a jednokrotne – precyzyjną segmentację odpowiedzi.

Co czwarta duża firma w Polsce nie podjęła odpowiednich działań wdrożeniowych NIS2

Badanie pokazuje, że 27,4% dużych organizacji wciąż znajduje się na wczesnym etapie przygotowań do dyrektywy NIS2 – nie rozpoczęło wdrożeń lub dopiero analizuje luki. To alarmujący sygnał w kontekście terminów implementacji krajowej.

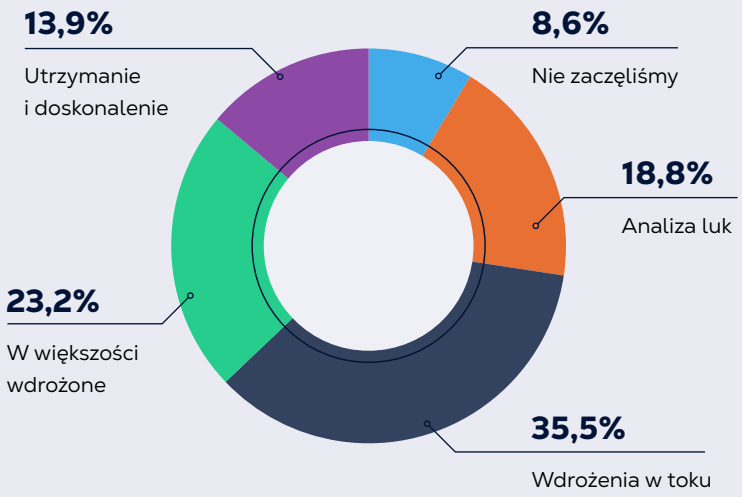
Dyrektywa NIS2, która rozszerza obowiązki dotyczące cyberbezpieczeństwa na znacznie większą liczbę podmiotów niż dotychczasowa NIS1, stawia przed polskimi firmami konkretne wymagania organizacyjne, techniczne i raportowe. Zgodnie z wynikami badania **ponad jedna czwarta z nich (27,4%) znajduje się dopiero na wczesnym etapie przygotowań.** W tej grupie 8,6% firm przyznaje, że nie rozpoczęło żadnych działań, a dalsze 18,8% jest na etapie analizy luk. To dane, które powinny budzić niepokój regulatorów i samych organizacji.

Wdrożenia w toku – ale tempo nie wystarcza

Największa grupa badanych (35,5%) deklaruje, że wdrożenia są w toku, co oznacza, że podjęto konkretne kroki, ale proces nie został ukończony. **Niemal co czwarta firma (23,2%) ocenia swoje przygotowania jako w większości wdrożone**, a jedynie 13,9% znajduje się w fazie utrzymania i doskonalenia. To sugeruje zaawansowany poziom gotowości. Oznacza to, że łącznie ponad 60% organizacji jest w trakcie aktywnych prac wdrożeniowych, ale jednocześnie znaczna część rynku pozostaje daleko od pełnej zgodności.

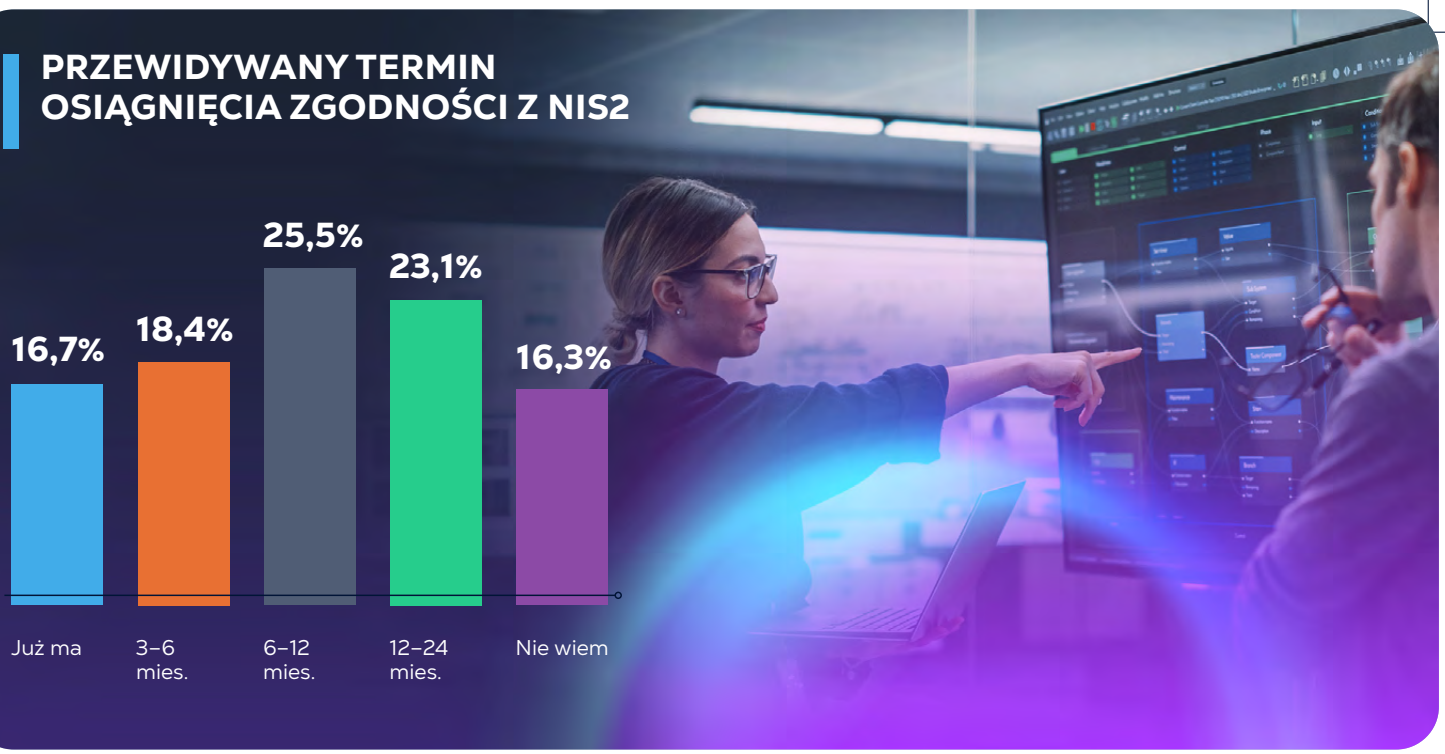
Dane dotyczące przewidywanego terminu osiągnięcia zgodności operacyjnej pogłębiają ten obraz. Zaledwie 16,7% firm deklaruje, że już spełnia wymagania NIS2. Kolejne 18,4% **przewiduje zgodność w ciągu 3–6 miesięcy**, a 25,5% w horyzoncie 6–12 miesięcy.

ETAP PRZYGOTOWAŃ DO NIS2



Zobacz jeszcze: Etap przygotowań do NIS2 wg wielkości firmy (s. 31)

PRZEWIDYWANY TERMIN OSIĄGNIĘCIA ZGODNOŚCI Z NIS2



Niepokojące jest jednak to, że 23,1% organizacji szacuje czas do zgodności na 12–24 miesiące, a aż 16,3% nie potrafi w ogóle określić, kiedy osiągnie wymagany poziom gotowości.

Brak formalnej oceny i niejasny status

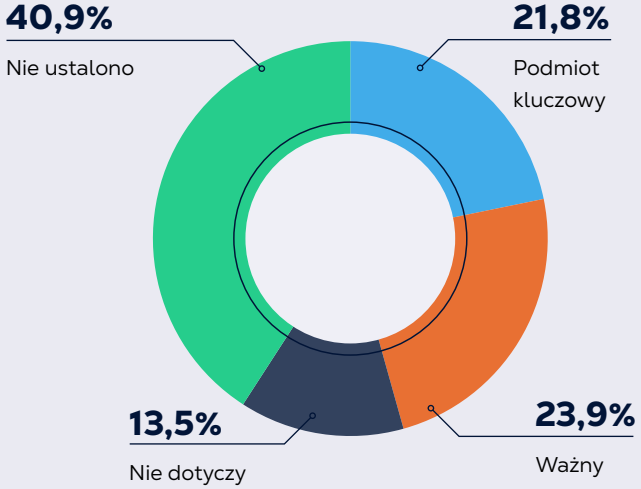
Dodatkowym czynnikiem ryzyka jest fakt, że 40,9% badanych firm nie ustaliło jeszcze swojego statusu w kontekście NIS2 – nie wie, czy jest podmiotem kluczowym, ważnym, czy dyrektywa ich w ogóle dotyczy. To poważna luka, ponieważ bez jasnej klasyfikacji nie sposób określić zakresu wymagań ani zaplanować odpowiednich działań.

Co więcej, **18,7% organizacji nie przeprowadziło formalnej oceny, czy NIS2 ma do nich zastosowanie,** a kolejne 14,1% nie potrafi odpowiedzieć na to pytanie. Tylko 34% firm potwierdziło, że taka ocena została przeprowadzona.

Wyniki badania wskazują, że polski rynek dużych przedsiębiorstw stoi przed poważnym wyzwaniem regulacyjnym. Choć większość firm podjęła jakieś działania, tempo przygotowań może okazać się niewystarczające. Organizacje, które wciąż nie rozpoczęły procesu wdrożeniowego, narażają się nie tylko na kary finansowe, ale przede wszystkim na realne ryzyko cybernetyczne, które dyrektywa NIS2 ma za zadanie minimalizować.

27,4% dużych organizacji wciąż znajduje się na wczesnym etapie przygotowań do dyrektywy NIS2

STATUS FIRMY W KONTEKŚCIE DYREKTYWY NIS2



Cloud by asseco

Zgodność z NIS2 bez chaosu. Dlaczego firmy nie powinny mierzyć się z regulacją w pojedynkę

Marcin Lebiecki
Wiceprezes Zarządu Asseco Cloud

Im wcześniej organizacja rozpocznie proces dostosowania do nowych wymogów, tym większa szansa na uporządkowane i efektywne wdrożenie zmian.

Implementacja NIS2 w postaci nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa znacząco przyczyni się do zwiększenia poziomu cyberochrony polskiego biznesu. Zmiany legislacyjne nie obejmą jedynie największych firm. Duże i średnie organizacje również staną przed licznymi wyzwaniami a zasoby, jakimi dysponują na bezpieczeństwo IT są często znacznie bardziej ograniczone. Według badania NIS2. Czy firmy w Polsce są gotowe na dyrektywę? jedynie nieco ponad 30% przedsiębiorstw zatrudniających od 300–499 pracowników ocenia, że jest w zaawansowanej fazie wdrożenia założeń nowej regulacji. Wśród firm zatrudniających ponad 1000 osób odsetek ten wynosi niemal 42%.

NIS2 nakłada na przedsiębiorstwa objęte ustawą obowiązek wdrożenia polityk i narzędzi umożliwiających zarządzanie ryzykiem cybernetycznym. Oznacza to potrzebę bieżącego monitoringu i reagowania na incydenty, zapewnienia planów ciągłości działania, tworzenia i przechowywania kopii zapasowych oraz wdrożenia rozwiązań umożliwiających przywrócenie działania systemów po awarii czy cyberataku.

Zapewnienie zgodności regulacyjnej, korzystając jedynie z wewnętrznych środków firmy, może być trudne, szczególnie mając na uwadze niedobór ekspertów z obszaru rozwiązań chmurowych oraz cyberbezpieczeństwa. Sporym wyzwaniem są również rosnące ceny i ograniczona dostępność infrastruktury IT. W wielu przypadkach decyzja o podjęciu

52%

badanych deklaruje potrzebę audytu i gap analysis, a 40% wsparcia w obszarze SOC i monitoringu

NIS2 nakłada na przedsiębiorstwa objęte ustawą obowiązek wdrożenia polityk i narzędzi umożliwiających zarządzanie ryzykiem cybernetycznym. Decyzja o podjęciu współpracy z partnerem technologicznym, który gwarantuje odpowiednie standardy bezpieczeństwa i profesjonalne doradztwo, jest najlepszą opcją.

współpracy z partnerem technologicznym, który gwarantuje odpowiednie standardy bezpieczeństwa i profesjonalne doradztwo, jest najlepszą opcją. Asseco Cloud pomaga w budowie efektywnego i dostosowanego do realnych potrzeb organizacji modelu bezpieczeństwa IT. Oferujemy outsourcing usług zarządzanych IT oraz rozwiązania z zakresu ciągłości działania biznesu – disaster recovery – zarówno w modelu dedykowanym, np. opartym na chmurze prywatnej, jak i w architekturze bazującej na chmurach publicznych.

Jak wynika z badania NIS2. Czy firmy w Polsce są gotowe na dyrektywę?, organizacje nie chcą zostać z NIS2 same. Prawie 52% badanych deklaruje potrzebę audytu i gap analysis, a 40% wsparcia w obszarze SOC i monitoringu. Firmy poszukują pomocy w przejściu całego procesu dostosowania do NIS2. Potwierdzają to dane z raportu Cyfrowe wyzwania polskiego biznesu opracowanego przez Asseco Cloud i PMR, w którym szkolenie pracowników IT i biznesu z nowych wymogów regulacyjnych wskazano jako kluczowy obszar przygotowań.

Mimo że wejście w życie NIS2 jest coraz bliżej, 24% firm, które wzięły udział w badaniu Business Growth Review nie ma pewności, czy dotyczą ich zmiany regulacyjne, a 45% ma wątpliwości odnośnie zakresu wymagań określonych w ustawie. Przygotowań nie warto zostawiać na ostatnią chwilę. Im wcześniej organizacja rozpocznie proces dostosowania do nowych wymogów, tym większa szansa na uporządkowane i efektywne wdrożenie zmian. Przy współpracy z doświadczonym partnerem zapewnienie zgodności regulacyjnej można przeprowadzić w sposób optymalny, właściwie wykorzystując dostępne zasoby i eliminując luki.

45%

firm, które wzięły udział w badaniu Business Growth Review, nie ma pewności, czy dotyczą ich zmiany regulacyjne

Bez względu na zakres wymagań, jaki nakłada NIS2, zmiany regulacyjne warto też potraktować jako impuls do weryfikacji gotowości firmy na aktualne wyzwania wynikające ze stale rosnącego zagrożenia cyberatakami. Wiele inicjatyw, takich jak opracowanie i wdrożenie planów ciągłości działania, może mieć istotne znaczenie w budowaniu przewagi konkurencyjnej np. dzięki minimalizowaniu strat wynikających z incydentów bezpieczeństwa. •

Marcin Lebiecki – absolwent wydziału Informatyki Politechniki Szczecińskiej. Z branżą IT związany jest od blisko 20 lat w obszarze kluczowych systemów informatycznych, centrów danych oraz usług cloud computing. Wcześniej odpowiedzialny za obszar biznesowy Centrum Danych w Unizeto Technologies, a następnie jako Dyrektor Zarządzający usługami Cloud & Data Center w Asseco Data Systems. Obecnie Wiceprezes Zarządu Asseco Cloud, w której odpowiada za Pion Usług Komercyjnych.

Braki kadrowe i budżetowe – dwie największe bariery wdrożenia NIS2 w polskich firmach

Implementacja dyrektywy NIS2 to nie tylko wyzwanie regulacyjne, ale przede wszystkim operacyjne. Badanie ujawnia skalę barier, z jakimi mierzą się organizacje próbujące dostosować swoje systemy i procesy do nowych wymogów. **Na czele listy przeszkód znajdują się braki kadrowe (57,3%) i ograniczenia budżetowe (55,3%)** – problemy, które dotykają nawet największe podmioty na rynku i sygnalizują głęboki deficyt kompetencji w obszarze cyberbezpieczeństwa.

37,9% firm realizuje wydatki związane z cyberbezpieczeństwem w ramach ogólnego budżetu IT, co często oznacza konkurowanie o środki z innymi projektami.

Dług technologiczny i brak kompetencji prawnych

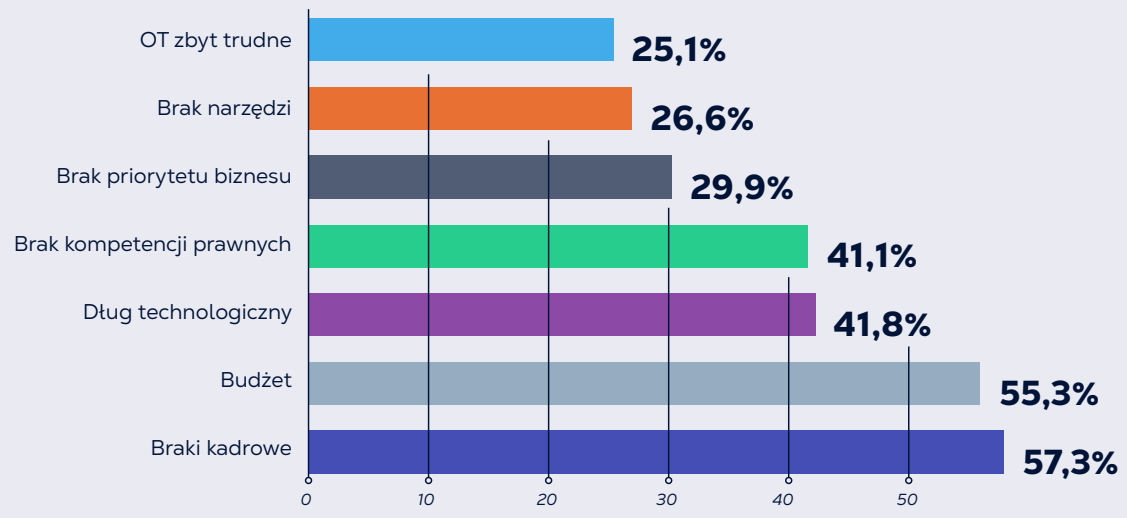
Poza brakami kadrowymi i budżetowymi firmy wskazują na dług technologiczny (41,8%) oraz brak kompetencji prawnych i compliance (41,1%) jako poważne bariery. **Dług technologiczny oznacza, że wiele organizacji operuje na przestarzałej infrastrukturze**, której modernizacja jest warunkiem wstępnym jakichkolwiek wdrożeń zgodnych z NIS2.

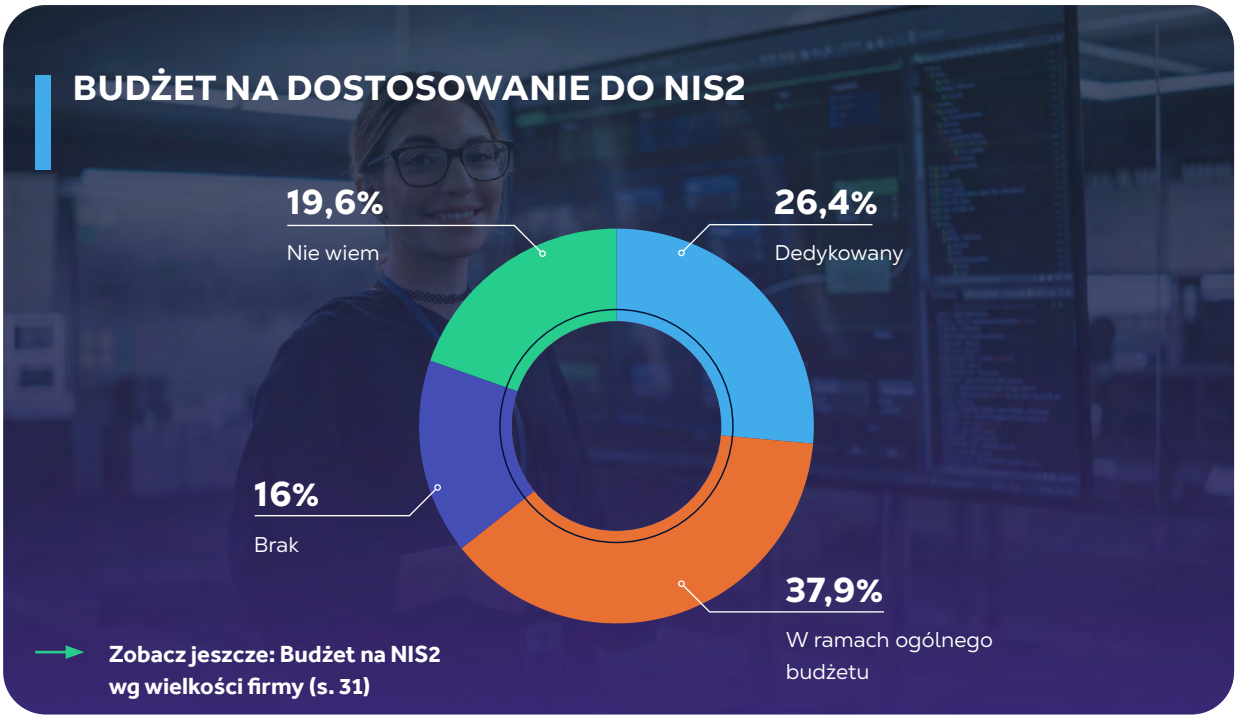
Z kolei brak wiedzy prawnej utrudnia interpretację wymagań dyrektywy i ich przełożenie na konkretne polityki i procedury wewnętrzne. Niemal co trzecia firma (29,9%) wskazuje też na brak priorytetu biznesowego – zarząd po prostu nie traktuje NIS2 jako pilnego zadania, co może skutkować opóźnieniami i karami.

Budżet – kluczowy, ale wciąż niedofinansowany

Struktura budżetowania potwierdza skalę problemu. **Zaledwie 26,4% firm dysponuje dedykowanym budżetem na dostosowanie do NIS2.**

NAJWIĘKSZE BARIERY WDROŻENIA NIS2





Największa grupa (37,9%) realizuje wydatki związane z cyberbezpieczeństwem w ramach ogólnego budżetu IT, co często oznacza konkurowanie o środki z innymi projektami.

Co szesnasta firma (16%) nie ma żadnego budżetu na ten cel, a niemal co piąta (19,6%) nie potrafi określić swojej sytuacji budżetowej. **Bez wydzielonych środków organizacje nie będą w stanie sfinansować niezbędnych wdrożeń** – od narzędzi technicznych, przez szkolenia, po usługi doradcze.

Potrzeby wsparcia – audyt, prawo, monitoring

Dane dotyczące zapotrzebowania na wsparcie zewnętrzne **rysują obraz rynku, który pilnie potrzebuje specjalistycznej pomocy**. Ponad połowa firm (51,9%) wskazuje na potrzebę przeprowadzenia audytu lub analizy luk, co oznacza, że organizacje zdają sobie sprawę ze swoich braków, ale nie mają wewnętrznych kompetencji, by je samodzielnie zdiagnozować.

Na drugim miejscu plasuje się zapotrzebowanie na programy i procedury (45,9%) oraz wsparcie prawne i compliance (45,3%). Istotna część firm potrzebuje też pomocy w zakresie SOC i monitoringu (40%), reagowania na incydenty (39,6%) oraz zarządzania bezpieczeństwem dostawców (32,7%).

Na czele listy przeszkód wdrożenia NIS2 znajdują się braki kadrowe

57,3%

oraz ograniczenia budżetowe

55,3%

Wyniki badania pokazują, że polskie firmy stoją przed podwójnym wyzwaniem: muszą jednocześnie budować kompetencje kadrowe i pozyskiwać środki finansowe na wdrożenia NIS2. Bez systemowego podejścia do rozwiązania tych barier – zarówno na poziomie organizacji, jak i całego rynku – tempo wdrożeń będzie daleko odbiegać od oczekiwań regulatorów. Dla firm doradczych, kancelarii prawnych i dostawców rozwiązań cyberbezpieczeństwa jest to jednocześnie niemała szansa rynkowa.

trecom

Braki kadrowe i nieświadome zarządy. Duże wyzwania przed polskimi firmami

Mirosław Maj
Współzałożyciel Open CSIRT Foundation i audytor SIM3, w Trecom wspiera rozwój zaawansowanych usług bezpieczeństwa

Stały program ćwiczeń to najbardziej praktyczny test bezpieczeństwa, który najszybciej pokazuje, co poprawić.

Raport daje obraz mocno spolaryzowany. Z jednej strony widać organizacje, które realnie wdrażają wymagania i budują procesy – z drugiej takie, które są na początku drogi albo jej jeszcze nie zaczęły. Uśredniony wynik bywa więc mylący: średnia nie oznacza, że większość jest w podobnym miejscu, tylko że mamy dwie grupy o bardzo różnej dojrzałości. To ważna wskazówka dla regulatora i rynku: jedni potrzebują doprecyzowania i narzędzi do domknięcia wdrożeń, inni – podstawowej mapy drogowej i impulsu do startu.

Szczególnie niepokojące są braki kadrowe. Tego deficytu nie da się uzupełnić w krótkim czasie, a w ujęciu globalnym – przy skali potrzeb – prawdopodobnie w ogóle. Dlatego kluczowe będzie skalowanie istniejących kompetencji i rozwiązań: usługi typu CISO-as-a-Service, wspólne SOC/SIEM, automatyzacja, a także wsparcie w korzystaniu z informacji, które już dziś oferują CSIRT-y krajowe (ostrzeżenia, podatności, rekomendacje). Bez tego łatwo wpaść w wirtualne i papierkowe bezpieczeństwo: polityki, procedury i raporty bez realnej zdolności detekcji i reakcji.

Słusznie ankietowani wskazują bezpieczeństwo łańcucha dostaw jako najsłabsze ogniwo. To jeden z najtrudniejszych elementów do zaplanowania, bo w sektorach NIS2 mamy dziesiątki, jeśli nie setki tysięcy poddostawców. Ich poziom cyberbezpieczeństwa jest często niski i – bez wsparcia, presji kontraktowej oraz prostych standardów minimalnych

Ankietowani wskazują bezpieczeństwo łańcucha dostaw jako najsłabsze ogniwo. To jeden z najtrudniejszych elementów do zaplanowania.

Absolutnym must na już jest włączenie w te procesy zarządów. NIS2 nie zadziała, jeśli pozostanie projektem IT. Musi być świadomość, decyzje budżetowe i operacyjne wsparcie.

– jeszcze długo taki pozostanie. Tu potrzebne są praktyczne mechanizmy: segmentacja dostawców, wymagania bazowe, audyty risk-based, i gotowe klauzule oraz wzorce oceny.

Absolutnym must na już jest włączenie w te procesy zarządów. NIS2 nie zadziała, jeśli pozostanie projektem IT. Musi być świadomość, decyzje budżetowe i operacyjne wsparcie. Ułatwieniem może okazać się osobista odpowiedzialność członków zarządu oraz wymóg przechodzenia przez nich specjalistycznych szkoleń – to w praktyce wymusza język ryzyka, priorytety i mierzalność.

Nisko ocenione procedury reagowania na incydenty to sygnał, że jest tu szczególnie źle – i doświadczenia praktyczne to potwierdzają. W czasie cyberataków firmy szybko wpadają w kryzys i nie potrafią z niego wyjść: brakuje ról, decyzji, komunikacji i zasad zarządzania kryzysowego pod cyber. To skomplikowana materia, a jedynym skutecznym sposobem jest stały program ćwiczeń (table-top, techniczne, międzydziałowe). To najbardziej praktyczny test bezpieczeństwa, który najszybciej pokazuje, co poprawić. Kluczowe jest budowanie odporności własnie w ten sposób.

Na koniec: fakt, że blisko 20% uważa, iż NIS2 ich nie dotyczy, z dużym prawdopodobieństwem wynika z błędnej oceny. Nie było dotąd regulacji, która tak szeroko obejmowałaby podmioty gospodarcze. Zachęcam do ponownej weryfikacji zakresu – warto uniknąć myślenia życzeniowego. •

20%

ankietowanych uważa, iż NIS2 ich nie dotyczy - to z dużym prawdopodobieństwem wynika z błędnej oceny.

Jedne organizacje potrzebują doprecyzowania i narzędzi do domknięcia wdrożeń, inne – podstawowej mapy drogowej i impulsu do startu.

Mirosław Maj – ekspert cyberbezpieczeństwa, prezes Fundacji Bezpieczna Cyberprzestrzeń. Współpracował z Radą ds. Cyfryzacji V kadencji oraz był doradcą Ministra Obrony Narodowej w obszarze cyberbezpieczeństwa. Współzałożyciel Open CSIRT Foundation i audytor SIM3. W Trecom wspiera rozwój zaawansowanych usług bezpieczeństwa.

Bezpieczeństwo łańcucha dostaw – najsłabsze ogniwo polskich firm w kontekście NIS2

Dyrektywa NIS2 kładzie bezprecedensowy nacisk na zarządzanie ryzykiem w łańcuchu dostaw. Wymaga od organizacji nie tylko identyfikacji i oceny ryzyk związanych z dostawcami, ale również **wdrożenia konkretnych mechanizmów kontroli**: wymagań umownych, audytów, monitoringu ciągłego i procedur zgłaszania incydentów po stronie partnerów. Tymczasem dane z badania wskazują, że właśnie ten obszar stanowi najsłabszy punkt ekosystemu cyberbezpieczeństwa polskich przedsiębiorstw.

W porównaniu z pozostałymi dziewięcioma domenami objętymi badaniem, bezpieczeństwo dostawców uzyskało najniższą średnią ocenę dojrzałości – zaledwie 3,0 na 5-stopniowej skali. Dla kontekstu, najwyżej oceniono polityki i procedury (3,63) oraz kopie zapasowe i testy odtwarzania (3,57). **Nawet reagowanie na incydenty, tradycyjnie uznawane za obszar niedoinwestowany, osiągnęło wyższą średnią (3,21).**

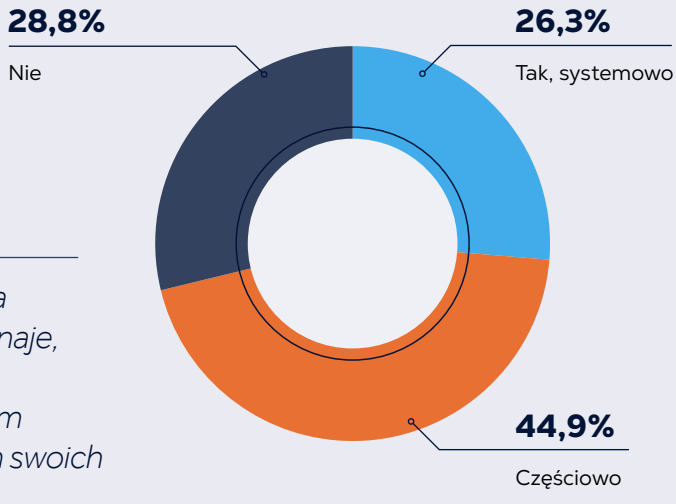
Bezpieczeństwo łańcucha dostaw wypada więc istotnie poniżej przeciętnej dojrzałości organizacji, co w świetle wymagań NIS2 stanowi poważne ryzyko regulacyjne i operacyjne.

Trzy poziomy zaangażowania – i aż 29% poza kontrolą

Struktura odpowiedzi na pytanie o zarządzanie ryzykiem cyber dostawców ujawnia trójdzielny rynek. **Największa grupa firm (44,9%) deklaruje częściowe zarządzanie tym ryzykiem** – podejmuje pewne działania, ale nie w sposób systemowy ani kompleksowy.

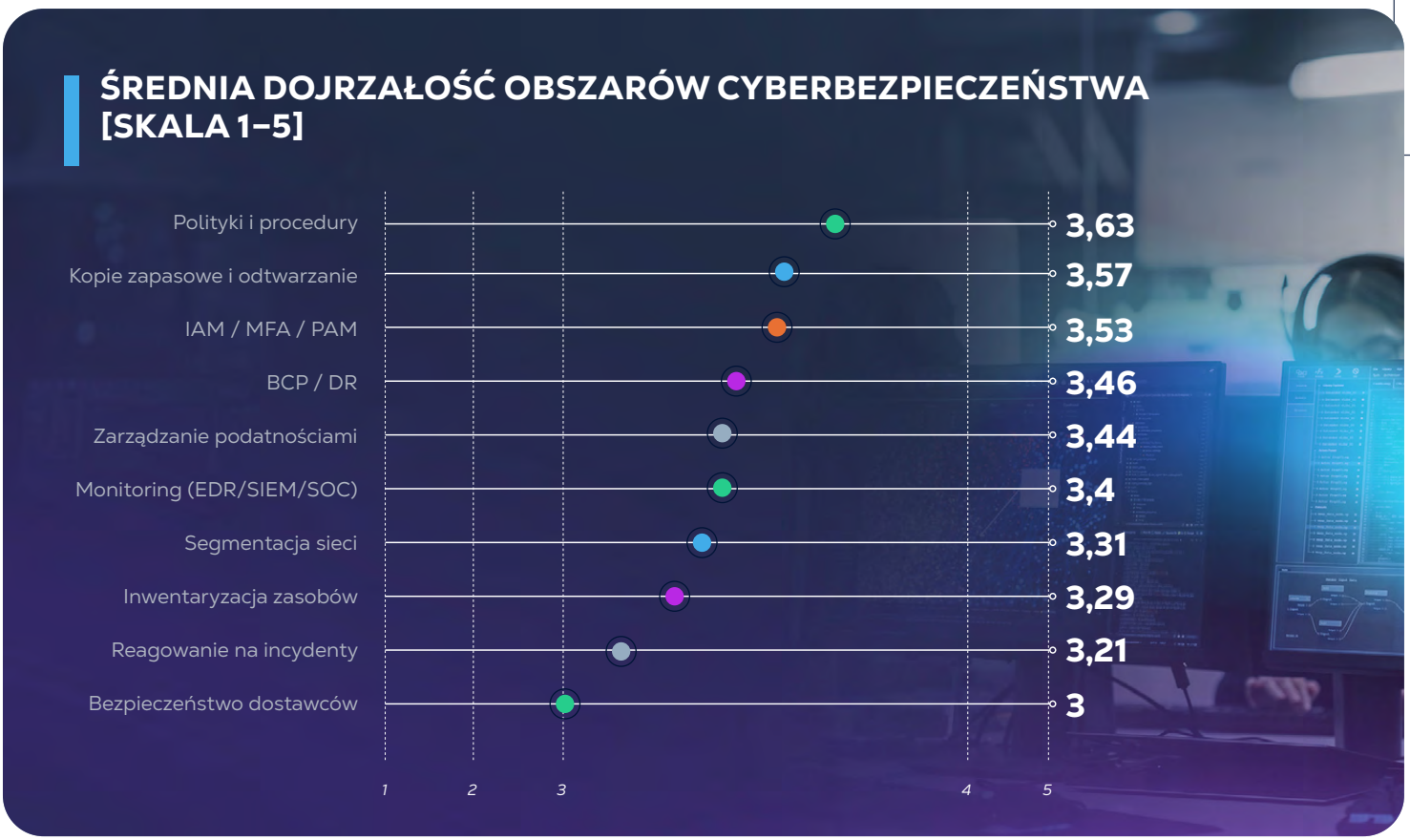
Nieco ponad jedna czwarta (26,3%) ma wdrożone, systematyczne podejście obejmujące wymagania umowne, cykliczne oceny i bieżący monitoring. Pozostałe 28,8% – czyli niemal co trzecia duża firma – **przyznaje, że w ogóle nie zarządza ryzykiem cybernetycznym swoich dostawców**. To blisko 300

ZARZĄDZANIE RYZYKIEM CYBER DOSTAWCÓW



Niemal co trzecia duża firma przyznaje, że w ogóle nie zarządza ryzykiem cybernetycznym swoich dostawców.

ŚREDNIA DOJRZAŁOŚĆ OBSZARÓW CYBERBEZPIECZEŃSTWA [SKALA 1–5]



organizacji z próby badawczej, które funkcjonują bez formalnej kontroli nad bezpieczeństwem swoich partnerów biznesowych.

Łańcuch dostaw jako źródło niepewności regulacyjnej

Wyniki badania wpisują się w szerszy obraz trudności interpretacyjnych. Łańcuch dostaw wskazywany jest przez 39,2% respondentów jako jeden z głównych obszarów niejasności związanych z NIS2, ustępując jedynie zakresowi wymagań (44,9%). **Firmy nie są pewne, jakie dokładnie obowiązki spoczywają na nich w zakresie weryfikacji i nadzoru nad dostawcami** – czy wystarczą klauzule umowne, czy konieczne są regularne audyty, a jeśli tak, to o jakim zakresie i częstotliwości.

Problem dostawców ma też wymiar sektorowy. Zarządzanie bezpieczeństwem dostawców w firmach z sektora zdrowia (7,3% próby) oraz transportu (8,3%) jest szczególnie złożone ze względu na rozbudowane łańcuchy podwykonawców i specyfikę regulacyjną tych branż. Jednocześnie to sektory, które NIS2 obejmuje jako kluczowe lub ważne, co oznacza **podwyższone oczekiwania regulatorów wobec ich programów zarządzania ryzykiem dostawców.**

W porównaniu z pozostałymi dziewięcioma domenami objętymi badaniem, bezpieczeństwo dostawców uzyskało najniższą średnią ocenę dojrzałości – zaledwie 3,0 na 5-stopniowej skali.

Dane z badania sugerują, że bez znaczącego przyspieszenia działań w obszarze bezpieczeństwa łańcucha dostaw, polskie firmy mogą stanąć przed podwójnym problemem. Z jednej strony ryzykiem cybernetycznym wynikającym z niekontrolowanych zależności od zewnętrznych partnerów, z drugiej – ryzykiem niezgodności regulacyjnej i potencjalnych sankcji ze strony organów nadzorczych. Warto zauważyć, że 32,7% firm deklaruje potrzebę wsparcia zewnętrznego właśnie w zakresie zarządzania dostawcami, co wskazuje na rosnącą świadomość problemu – choć niekoniecznie na gotowość do jego rozwiązania.

axians

Od narzędzi IT do systemu bezpieczeństwa – prawdziwa zmiana NIS2

Wojciech Gliniecki
Infrastructure Director, Axians

Nowa dyrektywa NIS2 przesuwa punkt ciężkości z wdrażania pojedynczych rozwiązań na budowę spójnego modelu bezpieczeństwa, w którym kluczowa staje się integracja widoczności zagrożeń, mechanizmów reagowania na incydenty i kontroli dostępu.

Wyniki badania pokazują, że znaczna część polskich przedsiębiorstw znajduje się nadal na wczesnym lub bardzo wczesnym etapie wdrażania wymogów NIS2. Respondenci najczęściej wskazują na trzy bariery: wysokie koszty, niedobór specjalistów cyberbezpieczeństwa oraz brak kompetencji prawnych i compliance potrzebnych do właściwej interpretacji regulacji. Warto również pamiętać, że badanie było realizowane jeszcze przed wejściem w życie krajowych przepisów implementujących NIS2 w ramach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Oznacza to, że część organizacji mogła nie mieć wówczas pełnej świadomości zakresu obowiązków ani skali odpowiedzialności spoczywającej na kadrze zarządzającej. W praktyce dopiero teraz — wraz z doprecyzowaniem wymagań — można spodziewać się wyraźnego wzrostu świadomości regulacyjnej i większej aktywności firm w obszarze przygotowań.

NIS2

promuje podejście systemowe — zdolność do ciągłej widoczności zagrożeń, szybkiego wykrywania incydentów, automatycznej reakcji oraz odtwarzania działania usług krytycznych.

Analiza poziomu dojrzałości technologicznej płynąca z wniosków raportu pokazuje, że organizacje wciąż mają trudności z zapewnieniem pełnego pokrycia procesowego wymogów NIS2. Najsłabiej wypadają obszary bezpieczeństwa dostawców oraz reagowania na incydenty — kluczowe z perspektywy

Firmy, które potraktują dyrektywę wyłącznie jako projekt regulacyjny, będą raczej reagować na kolejne braki, zamiast budować trwałą zdolność operacyjną.

nowej dyrektywy. Nieco lepiej oceniane są monitoring i detekcja, jednak wyniki wskazują raczej na istnienie narzędzi niż ich skuteczną integrację. Organizacje stosunkowo dobrze rozwijają podstawowe zabezpieczenia, ale wyraźnie odstają w monitoringu, reagowaniu, zarządzaniu ryzykiem dostawców czy raportowaniu. W mojej opinii, to właśnie warstwa operacyjna bezpieczeństwa pozostaje dziś największym wyzwaniem dla firm działających na rynku polskim.

Z naszych obserwacji wynika, że w wielu organizacjach funkcjonują rozwiązania do monitorowania zdarzeń, ochrony stacji roboczych czy kontroli dostępu, jednak działają one w rozproszeniu, bez wspólnej architektury. Tymczasem NIS2 promuje podejście systemowe — zdolność do ciągłej widoczności zagrożeń, szybkiego wykrywania incydentów, automatycznej reakcji oraz odtwarzania działania usług krytycznych.

Z perspektywy Axians dyrektywa NIS2 zmienia punkt ciężkości rozmowy — z pytania jakie narzędzie wdrożyć na jak zbudować spójny model odporności cyfrowej. Oznacza to konieczność uporządkowania środowiska bezpieczeństwa i połączenia rozwiązań z różnych obszarów, często też od różnych producentów w jeden model działania. W praktyce przekłada się to na integrację zarządzania tożsamością i uprawnieniami, bezpieczeństwa sieci, analizy zdarzeń oraz zarządzania podatnościami w jedną architekturę bezpieczeństwa.

Organizacje, które wykorzystają NIS2 jako impuls do uporządkowania architektury bezpieczeństwa, jednocześnie ograniczą dług technologiczny i wytworzą zdolność do ciągłego doskonalenia. Firmy, które potraktują dyrektywę wyłącznie jako projekt regulacyjny, będą raczej reagować na kolejne braki, zamiast budować trwałą zdolność operacyjną. W najbliższych latach kluczowa będzie integracja procesów, narzędzi i odpowiedzialności — obszar, w którym Axians od lat wspiera organizacje jako partner w projektowaniu, wdrażaniu i utrzymaniu rozwiązań cyberbezpieczeństwa. •

Z perspektywy Axians dyrektywa NIS2 zmienia punkt ciężkości rozmowy — z pytania jakie narzędzie wdrożyć na jak zbudować spójny model odporności cyfrowej.

Wojciech Gliniecki – dyrektor w Axians odpowiedzialny za pion infrastruktury. Zarządza zespołami Network & Security, Data Center oraz serwisem, odpowiadając za rozwój biznesu, utrzymanie relacji z klientami i partnerami technologicznymi oraz realizację złożonych projektów infrastrukturalnych. Wspiera organizacje w projektowaniu i wdrażaniu rozwiązań dopasowanych do potrzeb środowisk IT, współpracując z zespołami sprzedaży, presales i wsparcia technicznego. Angażuje się w przygotowanie koncepcji architektonicznych, spotkania z klientami oraz wkład techniczny do kluczowych postępowań ofertowych.

Zarząd w ciemno – 37% firm nie informuje kierownictwa o ryzyku cyber

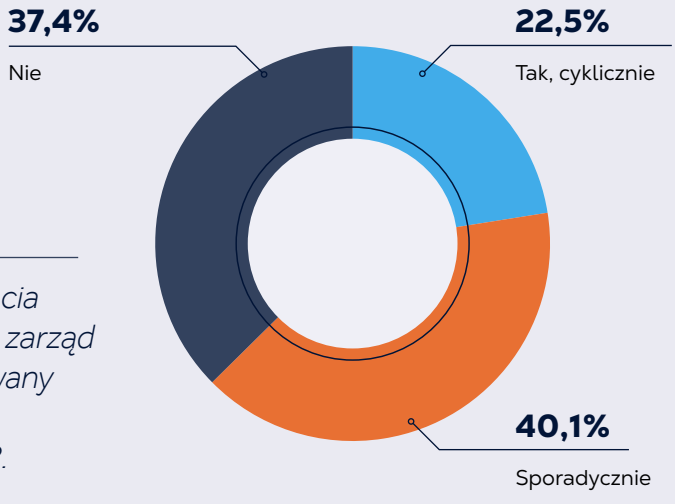
Jednym z fundamentalnych założeń dyrektywy NIS2 jest przeniesienie odpowiedzialności za cyberbezpieczeństwo na najwyższy szczebel zarządzania. Artykuł 20 dyrektywy stanowi, że organy zarządzające podmiotów kluczowych i ważnych **muszą zatwierdzać środki zarządzania ryzykiem, nadzorować ich wdrażanie i mogą ponosić osobistą odpowiedzialność za naruszenia**. W praktyce oznacza to, że członek zarządu nie może zasłonić się niewiedzą – regulacja wymaga aktywnego zaangażowania kierownictwa w kwestie cyberbezpieczeństwa.

Tymczasem wyniki badania dają obraz daleki od tych oczekiwań. **Zaledwie 22,5% organizacji deklaruje, że zarząd jest informowany o ryzyku cyber i postępach NIS2 w sposób cykliczny** – a więc zgodny z duchem dyrektywy. Największą grupę (40,1%) stanowią firmy, w których takie informowanie odbywa się jedynie sporadycznie, bez regularnego harmonogramu.

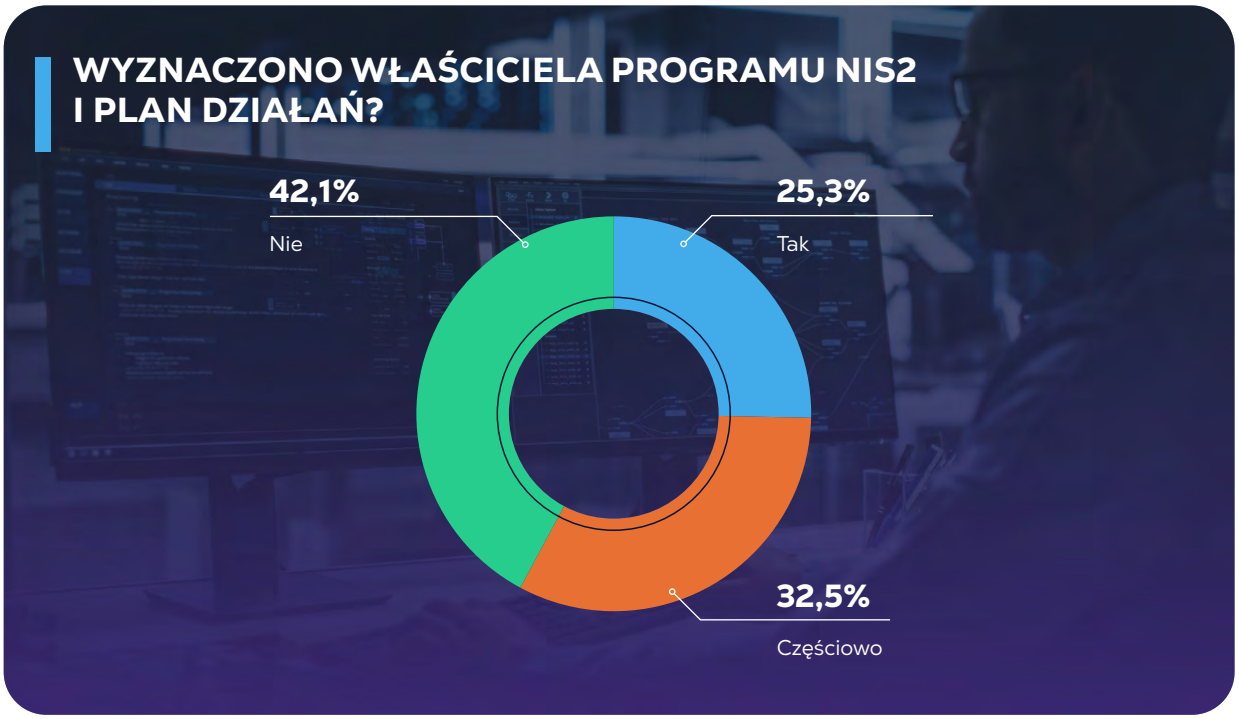
Najbardziej niepokojące jest jednak to, że 37,4% badanych firm – ponad jedna trzecia – przyznaje, iż zarząd nie jest informowany w ogóle. To 381 dużych organizacji z próby badawczej, w których najwyższe kierownictwo podejmuje decyzje biznesowe bez świadomości poziomu ryzyka cybernetycznego.

W prawie połowie dużych polskich firm nie istnieje formalna struktura zarządcza odpowiedzialna za wdrożenie dyrektywy.

CZY ZARZĄD JEST INFORMOWANY O RYZYKU CYBER I POSTĘPACH NIS2?



Ponad jedna trzecia firm przyznaje, iż zarząd nie jest informowany o ryzyku cyber i postępach NIS2.



Brak właściciela, brak struktury

Problem braku zaangażowania zarządu koresponduje z danymi dotyczącymi formalnego przypisania odpowiedzialności za program NIS2. Na pytanie o wyznaczenie właściciela programu NIS2 i planu działań z horyzontem czasowym oraz kamieniami milowymi, aż 42,1% firm odpowiedziało przecząco. **Jedynie co czwarta organizacja (25,3%) potwierdziła pełne przypisanie odpowiedzialności**, a 32,5% zadeklarowało częściowe rozwiązanie tego zagadnienia.

Oznacza to, że w prawie połowie dużych polskich firm nie istnieje formalna struktura zarządcza odpowiedzialna za wdrożenie dyrektywy – nie ma wyznaczonej osoby, nie ma harmonogramu i brakuje zdefiniowanych kamieni milowych.

Odpowiedzialność zarządu jako źródło niejasności

Co znamienne, odpowiedzialność zarządu pojawia się też jako istotny obszar niejasności regulacyjnych. Spośród ośmiu kategorii wątpliwości dotyczących NIS2 badanych w ankiecie, odpowiedzialność zarządu wskazało 33,4% firm. **Organizacje nie są pewne, jakie konkretnie obowiązki spoczywają na kierownictwie**, w jakim zakresie zarząd może delegować odpowiedzialność i jakie konsekwencje grożą za niedopełnienie wymogów. Te wątpliwości interpretacyjne częściowo tłumaczą bierność wielu zarządów, ale nie usprawiedliwiają braku jakiegokolwiek zaangażowania.

40,9%

firm nie ustaliło swojego statusu regulacyjnego – nie wie, czy jest podmiotem kluczowym czy ważnym.

Skala problemu staje się jeszcze wyraźniejsza w zestawieniu z danymi o formalnej ocenie stosowania NIS2. Aż 40,9% firm nie ustaliło nawet swojego statusu regulacyjnego – nie wie, czy jest podmiotem kluczowym czy ważnym. W połączeniu z brakiem informowania zarządu i niewyznaczeniem właściciela programu, rysuje się obraz **organizacji, które wchodzą w erę NIS2 bez kompasu**. Nie wiedzą, co im grozi, kto za to odpowiada i jak zmierzyć postępy. To sytuacja, w której ryzyko regulacyjne nakłada się na ryzyko operacyjne, a członkowie zarządów mogą nieświadomie narażać się na osobiste konsekwencje prawne i finansowe wynikające z nowej dyrektywy.

OVHcloud

NIS2 katalizatorem zmiany strategii chmurowych

Grzegorz Soczewka
VP Sales Eastern Europe w OVHcloud

Dyrektywa NIS2 nie jest kolejną regulacją, którą organizacje mogą sprowadzić do formalnego odhaczenia w ramach procesów *compliance*. Stanowi ona istotny punkt zwrotny w podejściu do zarządzania ryzykiem technologicznym – skłaniając zarządy i kadrę menadżerską do ponownej oceny architektury IT, modelu odpowiedzialności za dane oraz stopnia kontroli nad infrastrukturą cyfrową. W tym sensie NIS2 wykracza poza wymogi formalne i realnie wpływa na strategiczne decyzje dotyczące bezpieczeństwa, odporności operacyjnej i wyboru modelu chmurowego.

NIS2 wykracza poza wymogi formalne i realnie wpływa na strategiczne decyzje dotyczące bezpieczeństwa, odporności operacyjnej i wyboru modelu chmurowego.

NIS2 w ekosystemie regulacyjnym UE: od interpretacji do egzekwowania

Dyrektywa funkcjonuje w szerszym ekosystemie regulacyjnym UE. Łącznie z DORA, RODO, AI Act i Data Act tworzy spójny zestaw wymagań dotyczących kontroli nad przepływem danych, audytowalności infrastruktury oraz ograniczania zależności od podmiotów działających w systemach prawnych spoza UE. Dodatkowym wzmocnieniem tego kierunku jest rezolucja Parlamentu Europejskiego z 22 stycznia 2026 r. dotycząca europejskiej suwerenności technologicznej i infrastruktury cyfrowej, która wprost wskazuje na konieczność redukcji strategicznych zależności oraz budowy europejskich zdolności w obszarze chmury, danych i AI. W praktyce oznacza to, że suwerenność przestaje być wyłącznie interpretacją regulacyjną, a staje się elementem oficjalnego kierunku polityki UE, istotnie wpływającym na decyzje rynkowe.

Natomiast w Polsce obserwujemy wyraźne przejście od etapu interpretacji regulacji do ich egzekwowania przez organy nadzorcze, takie jak KNF czy UODO. W tym kontekście strategie IT oparte wyłącznie na globalnych hiperskalerach – bez jasno zdefiniowanych mechanizmów kontroli prawnej, operacyjnej i kontraktowej – stają się coraz trudniejsze do obrony w procesach audytu i nadzoru.

Od eksperckiej debaty do realnego kryterium biznesowego

Równolegle zmienia się charakter decyzji technologicznych podejmowanych przez organizacje. O ile jeszcze w 2024 r. suwerenność cyfrowa była tematem debat eksperckich, o tyle od 2025 r. stała się realnym kryterium przetargowym, elementem strategii cyberbezpieczeństwa oraz istotnym składnikiem oceny ryzyka operacyjnego. Potwierdzają to dane rynkowe – według raportu IDC z 2025 r. pt. *Choosing a Sovereign Cloud Solution*, 44% organizacji aktywnie rozważa wdrożenie suwerennych rozwiązań chmurowych, a 48% spodziewa się wzrostu wykorzysta-

nia suwerennej chmury w obszarach AI w ciągu dwóch kolejnych lat. W praktyce oznacza to, że w 2026 roku suwerenna chmura przestaje być alternatywą, a zaczyna pełnić rolę architektury referencyjnej dla sektorów regulowanych.

Compliance jako czynnik redefiniujący architektury chmurowe

Jednym z kluczowych czynników przyspieszających tę transformację jest presja związana z *compliance*. Audytorzy coraz częściej wymagają szczegółowych informacji dotyczących fizycznej lokalizacji danych, podstaw prawnych dostępu do nich, obowiązujących jurysdykcji oraz całego łańcucha podwykonawców. Równie istotne stają się realistyczne i możliwe do wdrożenia scenariusze wyjścia (*exit plans*) z danej infrastruktury chmurowej.

Co znamienne, w modelach *multicloud* brak komponentu suwerennościowego coraz częściej nie jest uznawany za akceptowalne ryzyko. W efekcie podejście *sovereign by design* staje się jednym z najskuteczniejszych sposobów ograniczania ryzyka regulacyjnego już na etapie projektowania systemów.

Rola administracji publicznej w rozwoju suwerennej chmury

Szczególną rolę w tym procesie odgrywa administracja publiczna. Ze względu na charakter przetwarzanych danych – obejmujących systemy krytyczne i dane obywateli – sektor instytucjonalny nie może pozwolić sobie na uzależnienie od jednego dostawcy ani na funkcjonowanie w ramach systemów prawnych pozostających poza jego kontrolą. Projekty e administracji w sposób naturalny wymuszają model suwerenny, zapewniający pełną kontrolę nad lokalizacją danych, dostępem do nich oraz ciągłością działania. W rezultacie administracja publiczna staje się jednym z głównych motorów rozwoju lokalnej i europejskiej infrastruktury chmurowej - nie tylko na poziomie legislacyjnym, ale przede wszystkim operacyjnym.

44%

organizacji aktywnie rozważa wdrożenie suwerennych rozwiązań chmurowych

Suwerenność przestaje być wyłącznie interpretacją regulacyjną, a staje się elementem oficjalnego kierunku polityki UE.

48%

organizacji spodziewa się wzrostu wykorzystania suwerennej chmury w obszarach AI w ciągu dwóch kolejnych lat

Dojrzałość rynku i dostępność suwerennych modeli chmurowych w Polsce

Wbrew obawom, polski rynek technologiczny jest przygotowany na ten kierunek zmian. Suwerenna chmura przestała być rozwiązaniem niszowym – organizacje mogą dziś korzystać zarówno z oferty lokalnych, jak i europejskich operatorów, wdrażać zaawansowane modele hybrydowe oraz projektować architektury *sovereign by design* jako standard dla sektorów regulowanych. Co istotne, koszt wdrożenia przestaje być barierą – znacznie większe ryzyka wiążą się obecnie z potencjalnym niespełnieniem wymogów regulacyjnych niż z inwestycją w odpowiednią infrastrukturę.

NIS2 jako impuls do strategicznego przeglądu strategii chmurowej

Obowiązki wynikające z NIS2 powinny stać się impulsem do całościowego przeglądu strategii chmurowej, a nie jedynie realizacją listy kontrolnej wymogów. Organizacje, które już dziś traktują suwerenność jako fundament projektowania architektury IT, zyskują przewagę nie tylko regulacyjną, lecz także operacyjną i reputacyjną – budując zaufanie klientów, partnerów oraz instytucji nadzorczych. W świecie, w którym ryzyko technologiczne coraz częściej wynika z zależności prawnych i strukturalnych, a nie wyłącznie z luk w zabezpieczeniach, odpowiednio dobrana i zaprojektowana chmura staje się kluczowym elementem zgodności z NIS2 i długoterminowej odporności organizacji. •

Grzegorz Soczewka – VP Sales na region Europy Środkowo Wschodniej w OVHcloud, globalnym dostawcy chmury i europejskim liderze w tym obszarze. Odpowiada za realizację strategii Go To Market, Be Ahead, rozwój programu partnerskiego oraz ekspansję w segmentach AI, fintech, administracji publicznej i Przemysłu 4.0. Koncentruje się na wzmacnianiu pozycji OVHcloud jako europejskiego dostawcy łączącego suwerenność danych z rozwojem rozwiązań AI. Posiada ponad 20 lat doświadczenia w sprzedaży, IT i rozwoju biznesu, specjalizując się w budowie struktur sprzedażowych, ekspansji międzynarodowej oraz komercjalizacji rozwiązań opartych na AI.

Tylko co czwarta firma ma dedykowany budżet na NIS2

Wdrożenie dyrektywy NIS2 wiąże się z konkretnymi kosztami: od audytów i analiz luk, przez modernizację infrastruktury technicznej, wdrożenie nowych narzędzi bezpieczeństwa, po szkolenia pracowników i usługi doradztwa prawnego. Każdy z tych elementów wymaga zaplanowanych, wyodrębnionych środków finansowych.

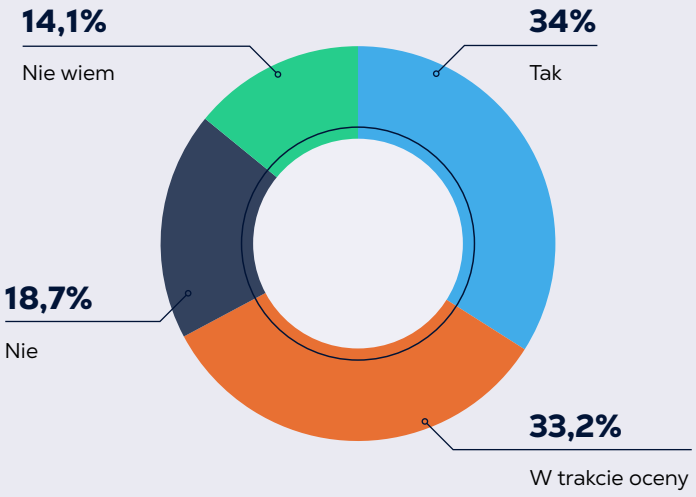
Tymczasem badanie pokazuje, że **zdecydowana większość polskich organizacji nie ma dedykowanego budżetu na ten cel**. Zaledwie 26,4% badanych firm dysponuje wydzielonymi środkami na dostosowanie do NIS2, co oznacza, że trzy czwarte rynku dużych przedsiębiorstw finansuje cyberbezpieczeństwo w sposób doraźny lub nie finansuje go wcale.

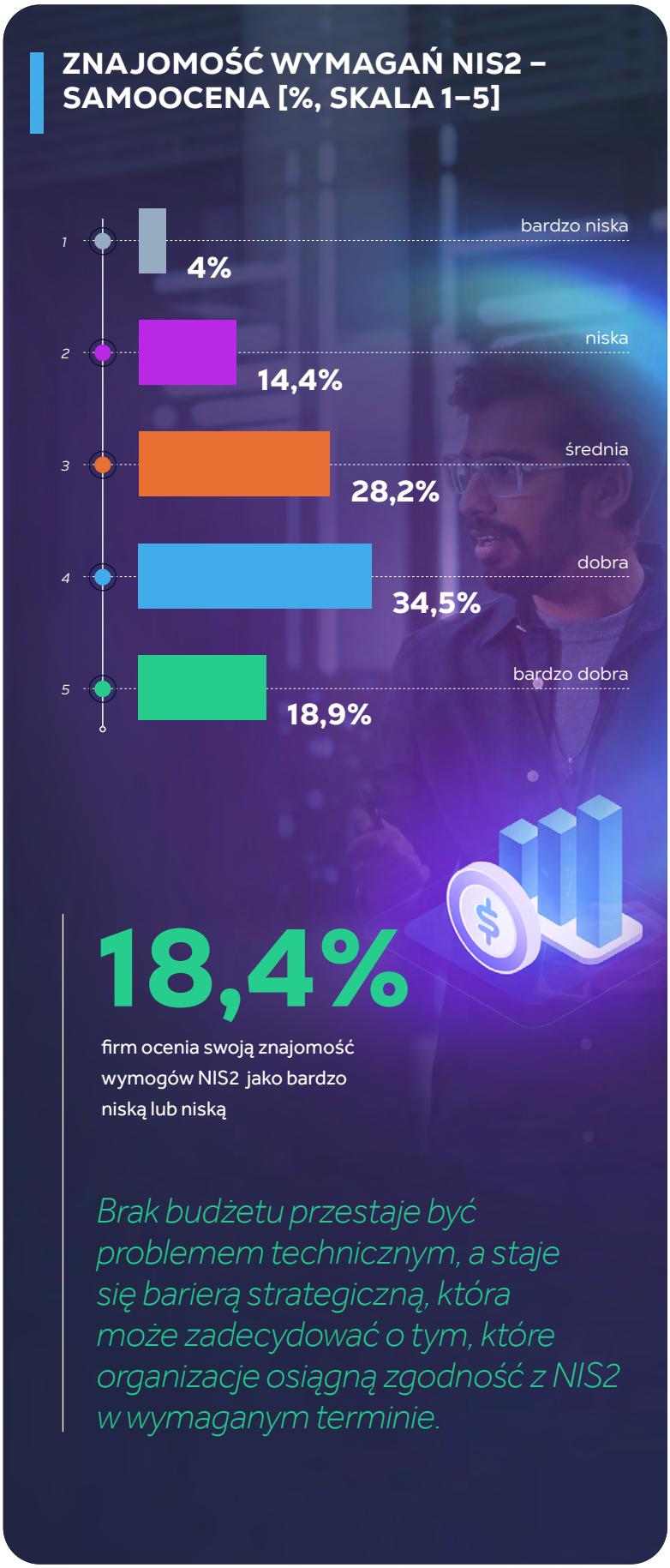
Największą grupę (37,9%) stanowią organizacje, które **realizują wydatki związane z NIS2 w ramach ogólnego budżetu IT lub cyberbezpieczeństwa**. W praktyce oznacza to konieczność rywalizacji o środki z innymi priorytetami technologicznymi – od transformacji cyfrowej, przez utrzymanie systemów, po projekty rozwojowe. W takim modelu wdrożenie NIS2 staje się jednym z wielu zadań, często bez gwarancji wystarczającego finansowania.

Trzy czwarte rynku dużych przedsiębiorstw finansuje cyberbezpieczeństwo w sposób doraźny lub nie finansuje go wcale.

Sytuacja jest jeszcze poważniejsza w przypadku 16% firm, które deklarują brak jakiegokolwiek budżetu na dostosowanie do dyrektywy, oraz 19,6%, które nie potrafią określić swojej sytuacji budżetowej.

CZY FIRMA FORMALNIE OCENIŁA, CZY NIS2 JĄ DOTYCZY?





Sugeruje to brak nawet podstawowej dyskusji na ten temat w strukturach organizacyjnych.

Znajomość wymogów a alokacja środków

Problem budżetowy nie istnieje w próżni – koreluje z poziomem znajomości wymogów NIS2 w organizacjach. Badanie wykazało, że **średnia samoocena znajomości dyrektywy wynosi 3,5 na 5-stopniowej skali**. Rozkład odpowiedzi wskazuje, że 18,4% firm ocenia swoją wiedzę jako bardzo niską lub niską (oceny 1–2), a najliczniejszą grupę (34,5%) stanowią organizacje ze średnio-zaawansowaną znajomością (ocena 4).

Jedynie 18,9% badanych przyznaje sobie najwyższą ocenę. Niepełna wiedza o wymogach utrudnia uzasadnienie potrzeby budżetowej przed zarządem – trudno wnioskować o środki na działania, których zakresu organizacja nie rozumie w pełni.

Konsekwencje finansowej bierności

Brak wyodrębnionych środków na NIS2 ma bezpośrednie przełożenie na zdolność firm do realizacji wdrożeń. Badanie pokazuje, że **ograniczenia budżetowe stanowią drugą najczęściej wskazywaną barierę wdrożenia** – na ten problem wskazuje 55,3% respondentów. Jednocześnie ponad połowa firm (51,9%) deklaruje potrzebę zewnętrznego audytu lub analizy luk, a 45,3% potrzebuje wsparcia prawnego – to usługi, które bez odpowiedniego finansowania pozostaną w sferze deklaracji. W sytuacji, gdy 27,4% firm nie podjęło jeszcze odpowiednich działań wdrożeniowych, brak budżetu przestaje być problemem technicznym, a staje się barierą strategiczną, która może zadecydować o tym, które organizacje osiągną zgodność z NIS2 w wymaganym terminie, a które narażą się na konsekwencje regulacyjne.

dhosting.pl

Bezpieczna infrastruktura w dobie NIS2

Rafał Kuśmider
CEO dhosting.pl

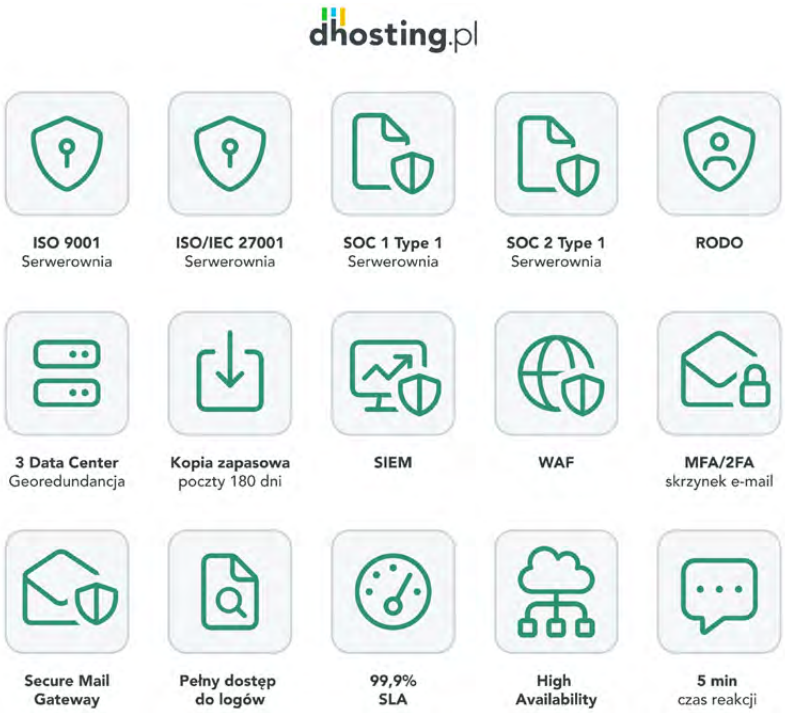
Wraz z wejściem w życie dyrektywy NIS2 wybór infrastruktury przestaje być wyłącznie decyzją biznesową - staje się elementem strategii zarządzania ryzykiem i ciągłości działania. W dhosting.pl od blisko 20 lat wspieramy organizacje w budowie zaawansowanych środowisk hostingowych i IaaS, m.in. dla sektora publicznego, medycznego oraz podmiotów przetwarzających dane wrażliwe. Projektujemy dedykowane, odseparowane środowiska zapewniające wysoką dostępność i zgodność regulacyjną.

Wybór infrastruktury staje się elementem strategii zarządzania ryzykiem i ciągłości działania.

Jak dhosting.pl wspiera zgodność z NIS2?

Nasze podejście koncentruje się na technologiach, które bezpośrednio adresują wymagania dyrektywy w obszarze środków technicznych i organizacyjnych.

- **Bezpieczeństwo fizyczne i lokalizacja danych:** Centra danych zapewniają pełną zgodność prawną oraz georedundancję (3 niezależne lokalizacje). Bezpieczeństwo potwierdzają **certyfikaty ISO 9001, ISO/IEC 27001 oraz SOC 1 i SOC 2 Type 1.**
- **Ochrona sieci i systemów:** Zaawansowane mechanizmy **antyDDoS** (do 100 Gbps) i **WAF** skutecznie neutralizują ataki i chronią aplikacje.
- **Zarządzanie incydentami i logowanie:** **System klasy SIEM** umożliwia monitoring zdarzeń w czasie rzeczywistym i szybką reakcję - kluczową przy obowiązku raportowania incydentów w ciągu 24 godzin.
- **Ciągłość działania i backup:** Poczta Biznesowa zapewnia **retencję danych przez 180 dni** (do 360 dni w osobnej lokalizacji dla projektów indywidualnych), **SLA 99,9%** oraz czas reakcji na zgłoszenia do **5 minut.**



Komentarz

NIS2 zmienia postrzeganie poczty i hostingu – z prostego zakupu w strategiczne partnerstwo technologiczne. Z badań wynika, że 38% firm nie ma zdefiniowanych progów poważnego incydentu, a bezpieczeństwo dostawców pozostaje najsłabszym ogniwem. W dhosting.pl budujemy środowiska oparte na pełnej kontroli, odseparowanej infrastrukturze i monitoringu w czasie rzeczywistym, wspierając zarządzanie podatnościami i szybką reakcję wymaganą przez nowe regulacje. W praktyce oznacza to bezpieczną przystań dla organizacji, które oczekują wydajności znanej z usług Google czy Microsoft Exchange, ale jednocześnie potrzebują suwerenności danych, w tym pewności, że są one hostowane i przetwarzane w Polsce.

Rafał Kuśmider
CEO dhosting.pl

Na co zwrócić uwagę, wybierając partnera pod NIS2?

Raporty wskazują, że najsłabszym ogniwem firm jest bezpieczeństwo łańcucha dostaw, dlatego kluczowa jest weryfikacja dostawcy.

1. Prawo do weryfikacji: Jako polski podmiot umożliwiamy weryfikację procesów bezpieczeństwa oraz fizyczną kontrolę lokalizacji przetwarzania danych w kraju.

2. Pełna kontrola i elastyczność: Oferujemy wydzieloną fizycznie infrastrukturę z dedykowaną adresacją i routingiem dla projektów wymagających pełnej izolacji, zarówno w warstwie pocztowej, jak i hostingowej.

38%

firm nie ma zdefiniowanych progów poważnego incydentu, a bezpieczeństwo dostawców pozostaje najsłabszym ogniwem.

3. Zaawansowane uwierzytelnianie: Systemy wspierają MFA/2FA (np. dla Webmaila) oraz umożliwiają wymuszanie polityk haseł.

4. Ochrona poczty: E-mail pozostaje głównym wektorem ataków, dlatego wykorzystujemy autorski system CleanBox AI oparty na AI, uczeniu maszynowym i analizie heurystycznej. Dla wymagających środowisk dostępny jest Secure Mail Gateway klasy Enterprise z zaawansowanymi politykami filtrowania, ochroną przed wyciekiem danych oraz opcjonalnym lokalnym Sandboxem do izolowanego testowania załączników. •

Rafał Kuśmider – Prezes Zarządu dhosting.pl, od 19 lat rozwija usługi hostingowe w Polsce, koncentrując się na automatyzacji, bezpieczeństwie i wydajności – także w kontekście wymagań regulacyjnych, w tym NIS2. W 2016 roku stworzył Elastyczny Web Hosting, projektowany pod realne obciążenia i potrzeby wymagających organizacji. W dhosting.pl odpowiada za rozwój rozwiązań wdrażanych u klientów o podwyższonych wymaganiach w obszarze bezpieczeństwa i zgodności z politykami. Jest również ekspertem w zakresie bezpieczeństwa poczty elektronicznej i współpracuje przy rozwiązaniach wykorzystywanych przez globalne marki. W 2026 roku rozpoczyna ekspansję zagraniczną pod marką mybox.com.

38% firm nie wie, co to poważny incydent – a NIS2 wymaga zgłoszenia w 24 godziny

Dyrektywa NIS2 wprowadza rygorystyczny reżim raportowania incydentów. Podmioty kluczowe i ważne zobowiązane są do przekazania wstępnego ostrzeżenia w ciągu 24 godzin od powzięcia informacji o poważnym incydencie, a pełnego zgłoszenia w ciągu 72 godzin.

Aby ten mechanizm mógł działać, **organizacja musi dysponować jasno zdefiniowanymi progami klasyfikacji** – wiedzieć, które zdarzenia kwalifikują się jako poważne i uruchamiają procedurę raportowania. Dane z badania wskazują, że znaczna część rynku nie jest przygotowana do spełnienia tego wymogu.

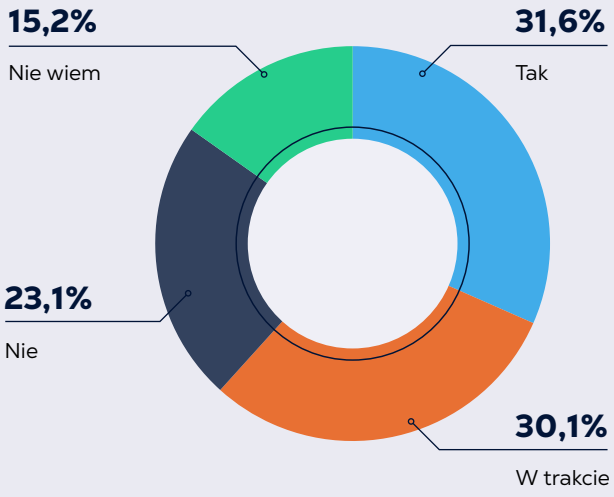
Blisko cztery na dziesięć dużych firm nie dysponuje operacyjnymi kryteriami klasyfikacji incydentów lub nie ma wiedzy o ich istnieniu w swojej organizacji.

Zgodnie z wynikami, zaledwie 31,6% firm potwierdziło, że ma zdefiniowane progi poważnego incydentu i wewnętrzną klasyfikację zdarzeń. Kolejne 30,1% jest w trakcie opracowywania tych definicji. Niepokojące jest jednak to, że 23,1% organizacji deklaruje brak takich progów, a dalsze 15,2% nie potrafi odpowiedzieć na to pytanie. Łącznie 38,3% dużych firm – blisko cztery na dziesięć – nie dysponuje operacyjnymi kryteriami klasyfikacji incydentów lub **nie ma wiedzy o ich istnieniu w swojej organizacji**.

Procedury raportowania – lepiej, ale wciąż niewystarczająco

Nieco lepiej, choć wciąż daleko od ideału, przedstawia się sytuacja w zakresie samych procedur raportowania incydentów.

ZDEFINIOWANE PROGI POWAŻNEGO INCYDENTU



Konswwencje niezgłoszenia zdarzenia to ryzyko nałożenia sankcji regulacyjnych oraz zwiększone szkody operacyjne i finansowe.

24h
na wstępne przekazanie ostrzeżenia

72h
na przekazanie pełnego zgłoszenia

Na pytanie o posiadanie procedury raportowania (zarówno wewnętrznego, jak i zewnętrznego) twierdząco odpowiedziało 35,1% firm. Kolejne 30,3% jest w trakcie tworzenia takich procedur. Pozostałe 34,6% organizacji albo nie ma procedur raportowania (20,2%), albo nie ma wiedzy na ten temat (14,4%). Oznacza to, że nawet wśród firm, które zidentyfikowały progi incydentów, **nie wszystkie dysponują formalnym mechanizmem przekazywania informacji** – zarówno wewnątrz organizacji, jak i do właściwych organów nadzorczych.

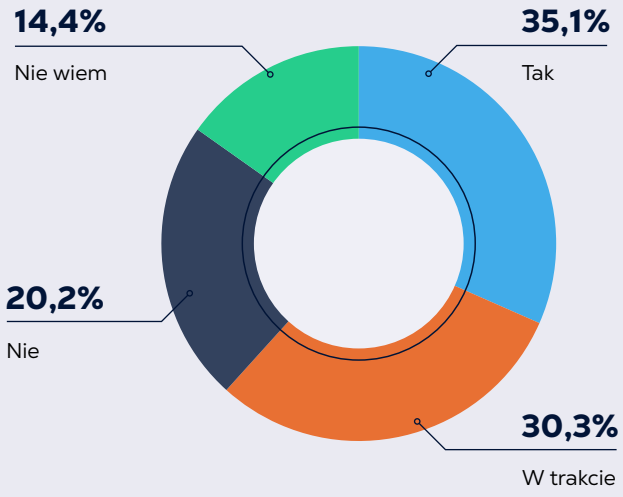
Incydenty się zdarzają – pytanie, czy firmy je raportują

Kontekst operacyjny nadaje tym danym dodatkowej wagi. **Badanie wykazało, że incydenty cyberbezpieczeństwa nie są zjawiskiem marginalnym w polskich firmach.** Zaledwie 16,1% organizacji zadeklarowało zero istotnych incydentów w ciągu ostatnich 12 miesięcy. Największa grupa (32%) doświadczyła 1–2 incydentów, 24,4% odnotowało 3–5 zdarzeń, a 11,4% zmierzyło się z sześcioma lub więcej incydentami. Kolejne 16,1% nie potrafiło określić liczby incydentów, co samo w sobie może świadczyć o brakach w monitoringu i dokumentowaniu zdarzeń.

Incydenty występują regularnie w zdecydowanej większości organizacji, ale niemal cztery na dziesięć firm nie dysponują kryteriami pozwalającymi ocenić, **które z tych zdarzeń kwalifikują się jako poważne w rozumieniu NIS2**. Jednocześnie ponad jedna trzecia nie ma formalnych procedur raportowania. W praktyce oznacza to, że znaczna część rynku może nie tylko nie zgłosić incydentu w wymaganym terminie 24 godzin, ale w ogóle nie rozpoznać, że doszło do zdarzenia wymagającego zgłoszenia.

To luka, która niesie ze sobą podwójne ryzyko. Z jednej strony sankcje regulacyjne za brak notyfikacji, z drugiej – wydłużony czas reakcji na konkretne zagrożenie, co zwiększa potencjalne szkody operacyjne i finansowe.

PROCEDURA RAPORTOWANIA INCYDENTÓW



Reagowanie na incydenty: polskie firmy nie ćwiczą procedur, których wymaga NIS2

Dyrektywa NIS2 stawia reagowanie na incydenty w centrum wymagań operacyjnych. Organizacje objęte regulacją **muszą nie tylko posiadać sformalizowane procedury reagowania, ale również regularnie je testować poprzez ćwiczenia symulacyjne**. Celem jest zapewnienie, że w momencie ataku firma potrafi szybko wykryć zagrożenie, ograniczyć jego skutki i przywrócić ciągłość działania.

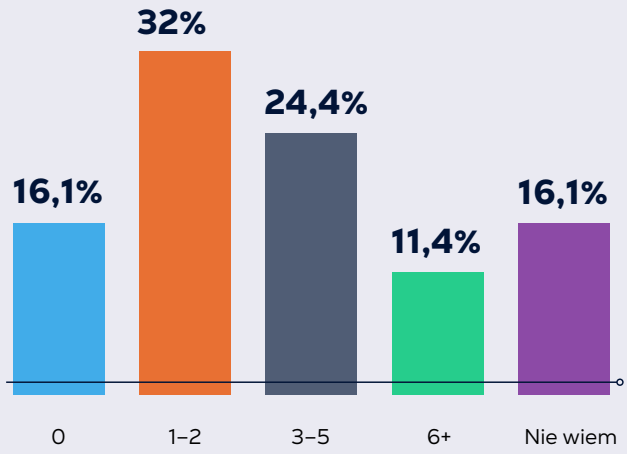
Wyniki badania wskazują, że ten obszar pozostaje jednym z najsłabiej rozwiniętych w krajowym ekosystemie cyberbezpieczeństwa.

Ze średnią oceną dojrzałości na poziomie 3,21 na 5-stopniowej skali, reagowanie na incydenty i ćwiczenia plasuje się na przedostatnim miejscu wśród dziesięciu badanych domen. Niżej wypadło jedynie bezpieczeństwo dostawców (3,0). Dla porównania: polityki i procedury – obszar o najwyższej dojrzałości – osiągnęły średnią 3,63, a kopie zapasowe i testy odtwarzania 3,57. Różnica między szczytem a dołem rankingu wynosi 0,63 punktu, co na 5-stopniowej skali jest wartością istotną i sygnalizuje wyraźną **nierównowagę w podejściu organizacji do poszczególnych aspektów cyberbezpieczeństwa**.

Incydenty się zdarzają – gotowość pozostaje niska

Niska dojrzałość w zakresie reagowania nabiera szczególnego znaczenia w konfrontacji z rzeczywistością operacyjną. **Badanie wykazało, że incydenty cyberbezpieczeństwa dotykają zdecydowanej większości organizacji.** Jedynie 16,1% firm zadeklarowało, że w ciągu ostatnich 12 miesięcy nie doświadczyło żadnego istotnego incydentu. Największa grupa respondentów (32%) odnotowała 1–2 incydenty, niemal co czwarta firma (24,4%) zmierzyła się z 3–5 zdarzeniami, a 11,4% raportowało sześć lub więcej incydentów w ciągu roku.

ISTOTNE INCYDENTY CYBER W OSTATNICH 12 MIESIĄCACH



Organizacje nie są pewne, jakie zdarzenia podlegają obowiązkowi notyfikacji, w jakim formacie należy przygotować zgłoszenie i do jakich organów je kierować.

3,21/5

W ocenie dojrzałośc na 5-stopniowej skali, reagowanie na incydenty i ćwiczenia plasuje się na przedostatnim miejscu wśród dziesięciu badanych domen.

→ **Zobacz ocenę wszystkich badanych domen (s. 13)**

Warto zwrócić uwagę, że kolejne 16,1% nie potrafiło określić liczby incydentów – to może świadczyć nie tyle o ich braku, ile o deficytach w monitoringu i dokumentowaniu zdarzeń bezpieczeństwa.

Raportowanie incydentów jako źródło niejasności

Obraz dopełnia analiza obszarów niejasności regulacyjnych zgłaszanych przez firmy. Raportowanie incydentów wskazało jako źródło wątpliwości aż 38,7% respondentów, co czyni ten temat trzecim najczęściej wymienianym obszarem niejasności – po zakresie wymagań (44,9%) i łańcuchu dostaw (39,2%). **Organizacje nie są pewne, jakie zdarzenia podlegają obowiązkowi notyfikacji**, w jakim formacie należy przygotować zgłoszenie i do jakich organów je kierować. Ta niepewność proceduralna, w połączeniu z niską dojrzałością operacyjną, tworzy lukę, która w przypadku rzeczywistego incydentu może skutkować zarówno przekroczeniem terminu 24-godzinnego zgłoszenia, jak i chaosem komunikacyjnym wewnątrz organizacji.

Wyniki badania wskazują na strukturalny problem polskiego rynku cyberbezpieczeństwa. **Firmy inwestują przede wszystkim w dokumentację i polityki – elementy stosunkowo łatwe do wdrożenia i wykazania w ramach audytu** – jednocześnie zaniedbując zdolności operacyjne, które decydują o skuteczności obrony w momencie kryzysu. Tymczasem NIS2 kładzie wyraźny nacisk nie na posiadanie dokumentów, lecz na faktyczną zdolność organizacji do szybkiego i skoordynowanego reagowania. Bez regularnych ćwiczeń i testów procedur nawet najlepsza dokumentacja pozostaje teorią, która nie przełoży się na skuteczne działanie w obliczu zagrożenia.

Dojrzałość cyberbezpieczeństwa w polskich firmach – gdzie są największe luki?

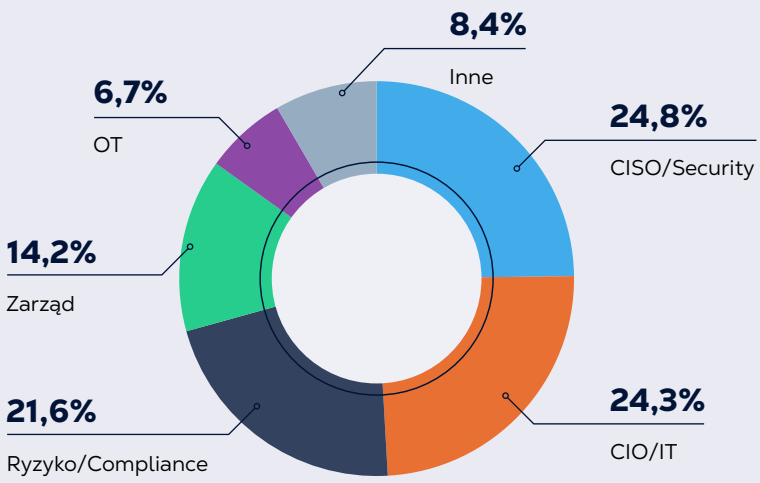
Badanie objęło ocenę dojrzałości firm w dziesięciu kluczowych domenach cyberbezpieczeństwa, bezpośrednio powiązanych z wymaganiami dyrektywy NIS2. Respondenci – przedstawiciele 1018 organizacji zatrudniających ponad 300 osób – oceniali poziom zaawansowania swojej firmy w każdym obszarze w skali od 1 (bardzo niski) do 5 (bardzo wysoki). **Wyniki tworzą mapę kompetencji, która pozwala zidentyfikować zarówno mocne strony polskich przedsiębiorstw, jak i obszary wymagające pilnej interwencji.**

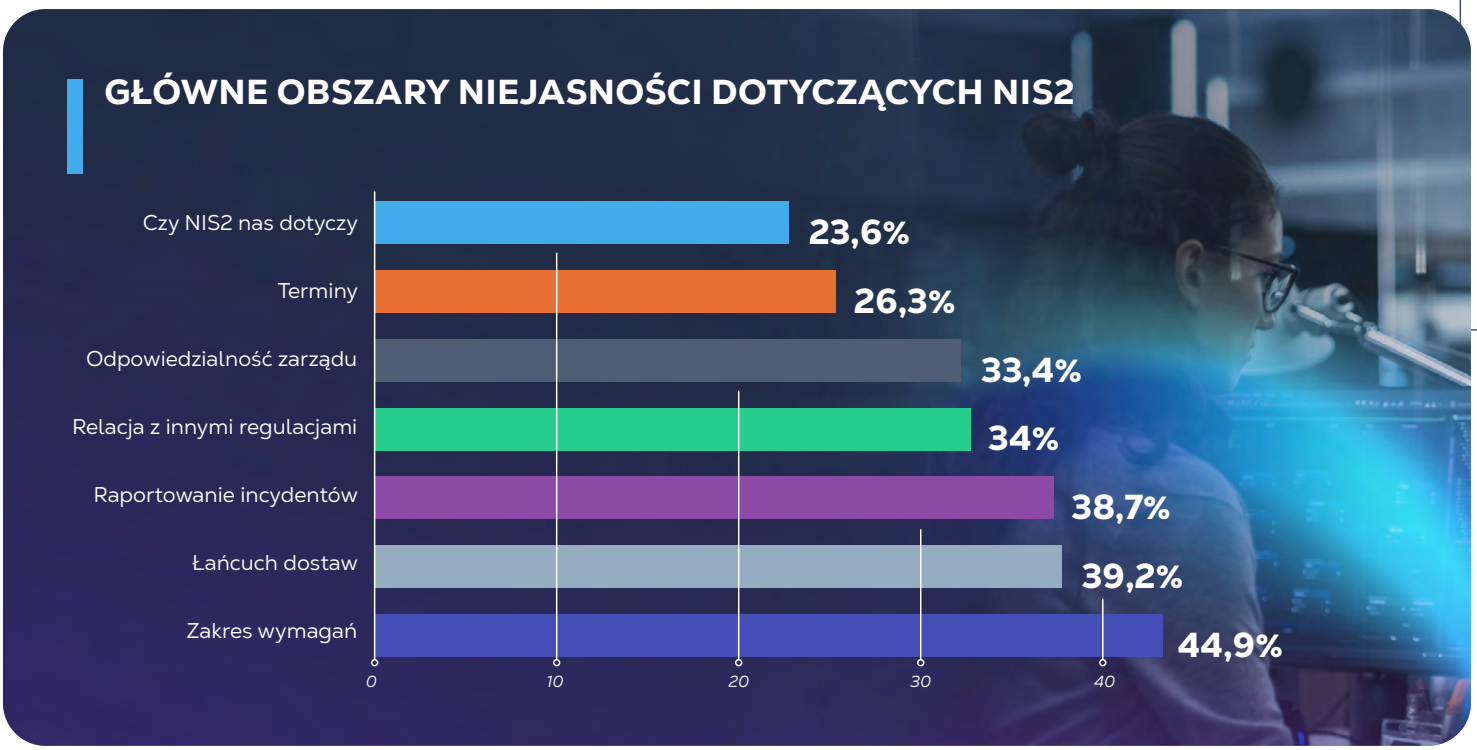
Na szczycie rankingu dojrzałości znajdują się trzy domeny: polityki i procedury (3,63), kopie zapasowe i testy odtwarzania (3,57) oraz wdrożenie IAM/MFA/PAM (3,53). Są to obszary o relatywnie wysokim stopniu formalizacji – łatwiejsze do zdefiniowania, wdrożenia i wykazania w ramach kontroli. Ich wyższe oceny odzwierciedlają wieloletnie inwestycje firm w systemy zarządzania tożsamością i dostępem oraz backupy, często motywowane nie tylko regulacjami, ale także doświadczeniami z ataków ransomware i awarii infrastruktury.

Środek stawki – solidna baza z rezerwami

W środkowej części rankingu plasują się domeny o średniej dojrzałości w przedziale 3,29–3,46. Zarządzanie podatnościami i patching (3,44), wdrożone BCP/DR (3,46) oraz monitoring i detekcja EDR/SIEM/SOC (3,40) osiągają oceny zbliżone do mediany. To obszary, w których **firmy poczyniły postępy, ale wciąż istnieją rezerwy** – szczególnie w zakresie automatyzacji procesów wykrywania zagrożeń i testowania planów ciągłości działania. Segmentacja i bezpieczeństwo sieci (3,31) oraz inwentaryzacja zasobów i krytyczność (3,29) zamykają tę grupę, sygnalizując, że nawet podstawowe działania porządkowe – wiedza o tym, jakie zasoby firma posiada i jak są chronione – pozostają niedokończone.

ROLA RESPONDENTÓW W ORGANIZACJI





Dół rankingu – ryzyko regulacyjne i operacyjne

Dwa najsłabiej ocenione obszary to reagowanie na incydenty i ćwiczenia (3,21) oraz bezpieczeństwo dostawców (3,0). **To domeny o wyraźnie operacyjnym charakterze, wymagające nie tyle dokumentacji, ile zdolności wykonawczych**: sprawdzonych procedur, przećwiczonych scenariuszy, umów z dostawcami i mechanizmów bieżącego nadzoru. Ich niskie oceny wskazują na systemowy wzorzec. Jaki to wzorzec? Polskie firmy są lepsze w definiowaniu zasad niż w ich egzekwowaniu. Różnica między najwyższą a najniższą średnią (0,63 punktu) jest znacząca. Sygnalizuje, że compliance formalny znacząco wyprzedza gotowość operacyjną.

Kto odpowiadał na pytania o dojrzałość?

Wiarygodność ocen dojrzałości wzmacnia profil respondentów. Badanie objęło osoby bezpośrednio zaangażowane w cyberbezpieczeństwo i compliance: CISO i specjaliści security stanowili 24,8% próby, CIO i kadra IT – 24,3%, a specjaliści ds. ryzyka, compliance i audytu – 21,6%. Dodatkowo 14,2% respondentów to członkowie zarządów, 6,7% specjaliści OT, a 8,4% pełniło inne role związane z bezpieczeństwem. Struktura ta oznacza, że **oceny dojrzałości pochodzą od osób posiadających bezpośrednią wiedzę o stanie cyberbezpieczeństwa w swoich organizacjach**, co nadaje wynikom wysoką wartość diagnostyczną.

> *Fundamenty formalne NIS2 zostały położone, ale zdolności operacyjne – te, które decydują o skuteczności obrony w momencie kryzysu – pozostają w tyle.*

Mapa dojrzałości wyłaniająca się z badania rysuje **obraz polskiego rynku jako znajdującego się w fazie przejściowej**. Fundamenty formalne zostały położone, ale zdolności operacyjne – te, które decydują o skuteczności obrony w momencie kryzysu – pozostają w tyle. Dyrektywa NIS2 weryfikuje właśnie te zdolności, a to oznacza, że firmy koncentrujące się dotychczas na dokumentacji mogą odkryć, że ich pozornie wysoka dojrzałość nie przekłada się na rzeczywistą zgodność z nowymi wymogami.

Efekt skali: firmy 1000+ znacznie dalej w przygotowaniach do NIS2 niż mniejsze podmioty

Badanie objęło trzy segmenty wielkościowe: firmy zatrudniające 300–499 osób (33,1% próby, n=337), 500–999 osób (35,4%, n=360) oraz ponad 1000 osób (31,5%, n=321). Analiza etapu przygotowań do NIS2 w podziale na te segmenty ujawnia **wyraźną korelację między wielkością organizacji a stopniem zaawansowania procesów wdrożeniowych**. Zależność ta przejawia się na obu krańcach spektrum: większe firmy częściej osiągają zaawansowane etapy, a mniejsze częściej pozostają na etapach początkowych.

W segmencie firm 1000+ aż 41,7% deklaruje, że wdrożenie NIS2 jest w większości zakończone lub organizacja znajduje się w fazie utrzymania i doskonalenia. W segmencie 500–999 pracowników ten odsetek spada do 39,2%, a wśród firm 300–499 wynosi 30,6%. Na drugim biegunie – wśród organizacji, które nie rozpoczęły wdrożeń lub dopiero analizują luki – proporcje się odwracają: 36,2% w segmencie 300–499 wobec 25,3% w segmencie 500–999 i zaledwie 20,6% w segmencie 1000+. Różnica między najmniejszymi a największymi firmami na wczesnym etapie sięga niemal 16 punktów procentowych.

Budżet jako mechanizm napędowy

Jednym z kluczowych czynników stojących za efektem skali jest **dostępność dedykowanego budżetu**. W segmencie 1000+ aż 38,6% firm dysponuje wydzielonymi środkami na NIS2, wobec 23,1% w segmencie 500–999 i tylko 18,4% w segmencie 300–499. Różnica jest ponad dwukrotna.

Jednocześnie brak jakiegokolwiek budżetu deklaruje zaledwie 9,7% firm 1000+ w porównaniu z 22,8% firm 300–499. Większe organizacje nie tylko dysponują większymi zasobami finansowymi, ale **znacznie częściej wyodrębniają je celowo na potrzeby compliance regulacyjnego**, co przekłada się bezpośrednio na tempo wdrożeń.

W segmencie firm 1000+ aż 41,7% deklaruje, że wdrożenie NIS2 jest w większości zakończone lub organizacja znajduje się w fazie utrzymania i doskonalenia.

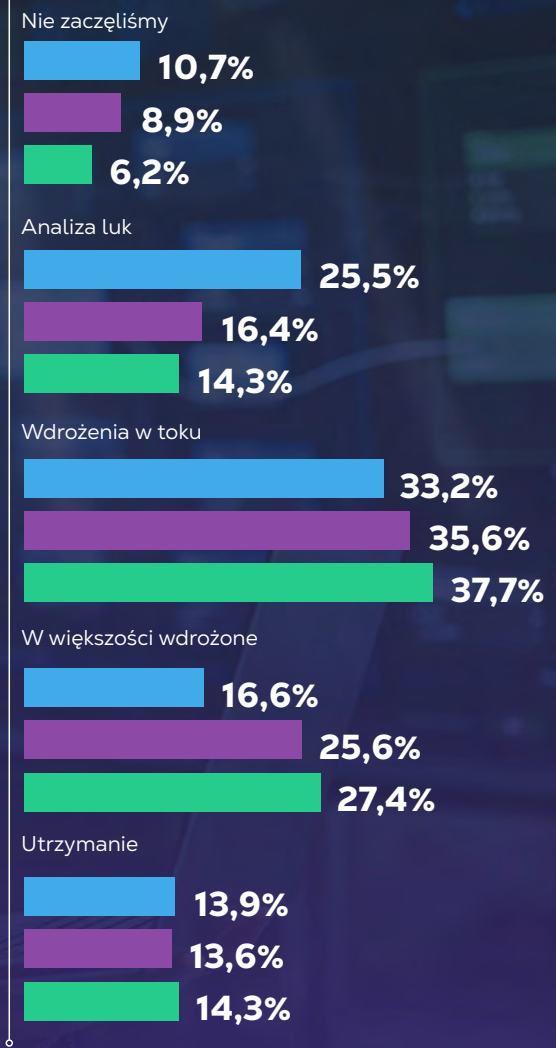
Skala nie gwarantuje pełnej gotowości

Mimo wyraźnej przewagi, nawet segment 1000+ wykazuje deficyty. Ponad jedna piąta największych firm (20,6%) wciąż znajduje się na wczesnym etapie przygotowań, a cykliczne informowanie zarządu o ryzyku cyber deklaruje jedynie 25,5% – niewiele więcej niż w mniejszych segmentach. **Efekt skali działa wyraźnie na poziomie finansowania i formalizacji procesów**, ale nie rozwiązuje problemów strukturalnych: braku specjalistów (57,3% wskazań niezależnie od wielkości firmy), luk kompetencyjnych w zakresie compliance ani niejasności regulacyjnych.

Mniejsze firmy stoją przed tym samym zestawem wyzwań, tyle że z ograniczonym budżetem i mniejszym zespołem. To czyni lukę w gotowości szczególnie trudną do nadrobienia w krótkim czasie.

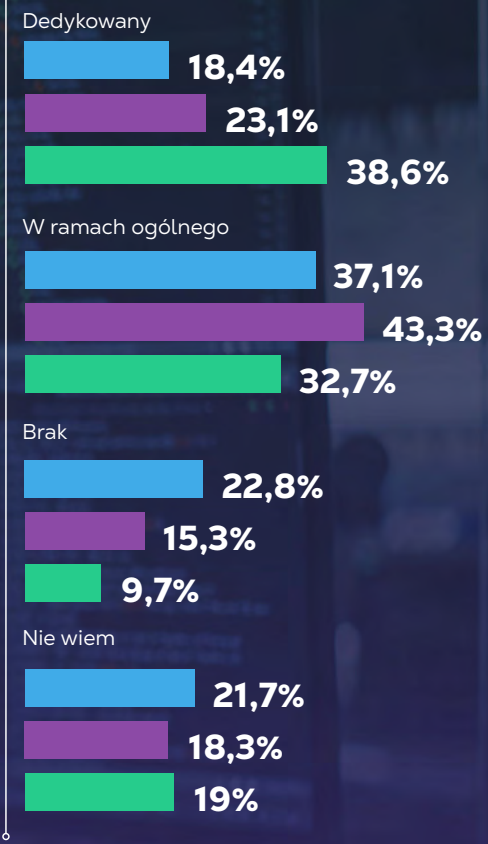
Efekt skali działa wyraźnie na poziomie finansowania i formalizacji procesów, ale nie rozwiązuje problemów strukturalnych.

ETAP PRZYGOTOWAŃ DO NIS2 WG WIELKOŚCI FIRMY



Liczba osób zatrudnionych w firmach:
- 300–499
- 500–999
- 1000+

BUDŻET NA NIS2 WG WIELKOŚCI FIRMY



Liczba osób zatrudnionych w firmach:
- 300–499
- 500–999
- 1000+

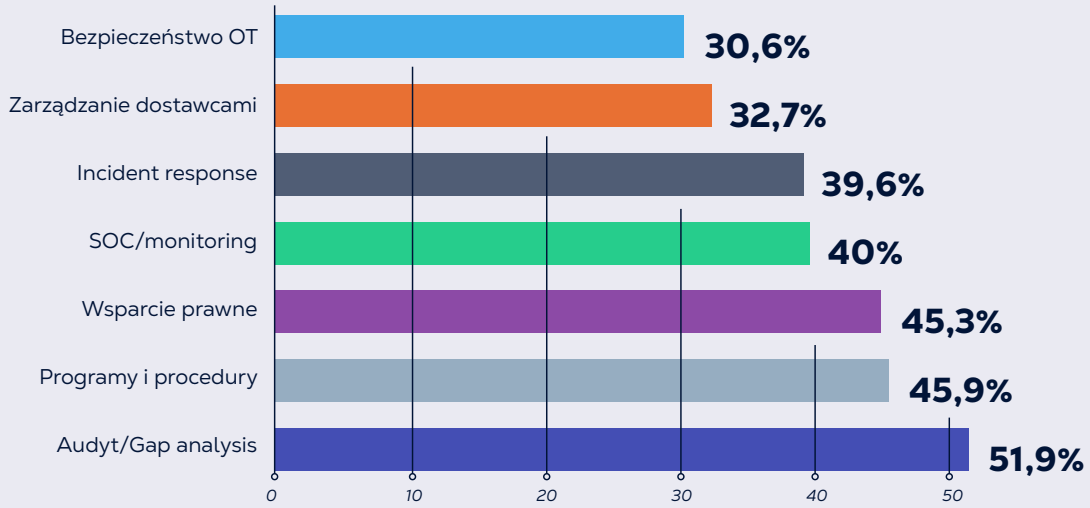
Czego potrzebują polskie firmy? Audyt, prawo i monitoring na szczycie listy

W badaniu zapytaliśmy respondentów o rodzaje wsparcia zewnętrznego, jakiego ich organizacja potrzebuje w związku z dyrektywą NIS2. Pytanie miało charakter wielokrotnego wyboru, a wyniki pokazują, że polskie firmy zgłaszają zapotrzebowanie jednocześnie w wielu obszarach. Sugeruje to, że potrzeby mają charakter systemowy, a nie punktowy. Średnia liczba wskazanych kategorii na respondenta wynosi blisko trzy, co oznacza, że **organizacje poszukują kompleksowego wsparcia łączącego doradztwo, technologię i prawo**.

Na szczycie listy znalazł się audyt i gap analysis, wskazany przez 51,9% firm. To wynik spójny z faktem, że 27,4% organizacji wciąż znajduje się na wczesnym etapie przygotowań – audyt stanowi naturalny punkt startowy procesu wdrożeniowego. Niewiele niżej plasują się opracowanie programów i procedur bezpieczeństwa (45,9%) oraz wsparcie prawne i compliance (45,3%). Te trzy kategorie tworzą spójny klaster potrzeb fundamentalnych – dotyczących podstaw organizacyjnych i regulacyjnych, **bez których dalsze wdrożenia nie mogą się rozpocząć**.

Bezpieczeństwo technologii operacyjnych jest potrzebą niemal co trzeciej dużej firmy, a specyfika tych systemów wymaga wyspecjalizowanej wiedzy, której wiele organizacji nie ma wewnętrznie.

ZAPOTRZEBOWANIE NA WSPARCIE ZEWNĘTRZNE



40,9%

firm nie ustaliło swojego statusu regulacyjnego – nie wie, czy jest podmiotem kluczowym czy ważnym.

Potrzeby technologiczne – SOC i incident response

Druga grupa potrzeb ma charakter technologiczno-operacyjny. Usługi SOC i monitoringu wskazało 40% respondentów, a incident response i ćwiczenia – 39,6%. Oba wyniki korespondują z niską dojrzałością tych obszarów: monitoring i detekcja osiągnęły średnią 3,40/5, a reagowanie na incydenty zaledwie 3,21/5. **Firmy rozpoznają swoje słabości operacyjne i sygnalizują gotowość do szukania wsparcia zewnętrznego.** Otwiera to istotną przestrzeń rynkową dla dostawców usług takich jak MSSP czy SOC-as-a-Service.

Nieco niżej, choć wciąż na znaczącym poziomie, plasują się zarządzanie dostawcami (32,7%) i bezpieczeństwo OT (30,6%). Ten ostatni wynik jest szczególnie istotny w kontekście struktury próby: 38,5% badanych firm ma środowiska OT/ICS/SCADA, a 56% świadczy usługi w trybie 24/7. Bezpieczeństwo technologii operacyjnych jest więc potrzebą niemal co trzeciej dużej firmy, a specyfika tych systemów wymaga wyspecjalizowanej wiedzy, której wiele organizacji nie ma wewnętrznie.

Potrzeby zależą od etapu – ale nie znikają

Analiza potrzeb w podziale na etap przygotowań ujawnia interesujący wzorzec. Firmy na wczesnym etapie (nie zaczęły lub analizują luki, n=279) najczęściej wskazują audyt (60,2%) i programy/procedury (52,7%) – potrzeby typowe dla fazy początkowej. Firmy zaawansowane (wdrożone lub w fazie utrzymania, n=378) zgłaszają nieco niższe, ale wciąż wysokie zapotrzebowanie: audyt 49,2%, wsparcie prawne 46,3%, SOC/monitoring 41,8%. Oznacza to, **że potrzeba wsparcia zewnętrznego nie znika wraz z postępem wdrożeń – zmienia jedynie swój profil**, przesuwając się od fundamentów regulacyjnych w stronę optymalizacji operacyjnej i ciągłego doskonalenia. Dla dostawców usług cyberbezpieczeństwa rynek NIS2 nie jest więc jednorazowym projektem, lecz źródłem długoterminowego popytu.

Wnioski końcowe: polskie firmy wobec NIS2 – między ambicją a gotowością

Analiza wyników badania pozwala na sformułowanie kilku kluczowych obserwacji dotyczących stanu gotowości polskich przedsiębiorstw na dyrektywę NIS2. Każda z nich ma bezpośrednie implikacje zarówno dla samych organizacji, jak i dla szerszego ekosystemu rynkowego: dostawców usług cyberbezpieczeństwa, regulatorów i decydentów kształtujących politykę wsparcia dla sektora prywatnego.

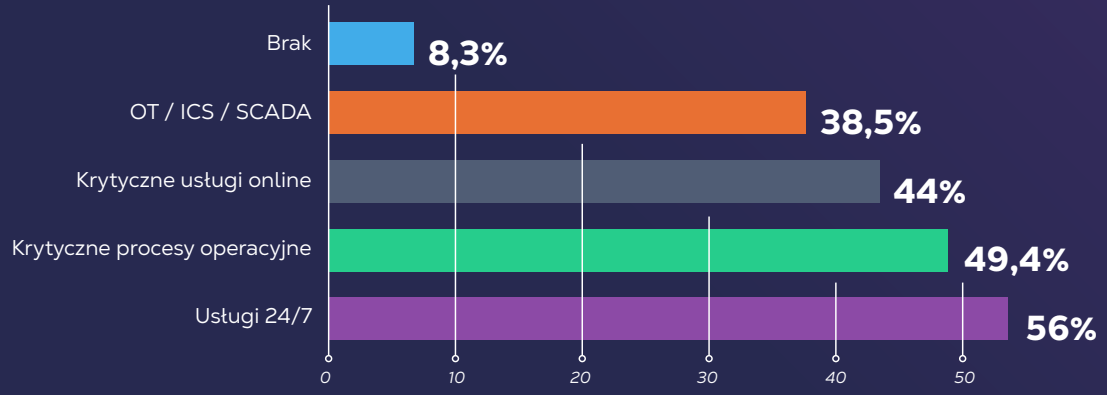
1 Rynek jest wyraźnie podzielony. Nieco ponad jedna trzecia firm (37,1%) znajduje się w zaawansowanej fazie wdrożeń, kolejne 35,5% prowadzi aktywne prace wdrożeniowe, ale 27,4% wciąż pozostaje na etapie początkowym. Ta trójdzielna struktura oznacza, że NIS2 nie jest problemem marginalnym – dotyczy zdecydowanej większości dużych organizacji, a tempo dostosowania jest nierównomierne.

2 Dojrzałość cyberbezpieczeństwa wykazuje wyraźną asymetrię między wymiarem formalnym a operacyjnym. Polityki i procedury (3,63/5) oraz kopie zapasowe (3,57) plasują się znacząco wyżej niż bezpieczeństwo dostawców (3,0) i reagowanie na incydenty (3,21). NIS2 weryfikuje przede wszystkim zdolności operacyjne, co oznacza, że firmy o pozornie wysokiej dojrzałości formalnej mogą okazać się nieprzygotowane na wymogi dyrektywy.

3 Bariery mają charakter systemowy. Braki kadrowe (57,3%) i budżetowe (55,3%) dotykają rynku niezależnie od wielkości firmy, choć efekt skali jest wyraźny: firmy 1000+ dwukrotnie częściej dysponują dedykowanym budżetem (38,6% vs 18,4% w segmencie 300–499). Jednocześnie 37,4% firm nie informuje zarządu o ryzyku cyber, a 42,1% nie wyznaczyło właściciela programu NIS2 – to sygnalizuje deficyt governance, którego żadne nakłady finansowe nie rozwiążą bez zmiany podejścia organizacyjnego.

4 Rynek usług cyberbezpieczeństwa stoi przed wyraźną falą popytu. Ponad połowa firm (51,9%) deklaruje potrzebę zewnętrznego audytu, 45,3% wsparcia prawnego, a 40% usług SOC. Zapotrzebowanie nie maleje wraz z postępem wdrożeń – zmienia jedynie profil, co oznacza długoterminowy, powtarzalny popyt na usługi doradcze i zarządzane.

ŚRODOWISKA KRYTYCZNE I OT W BADANYCH FIRMACH



Jako specjalistyczna firma badawcza z doświadczeniem w badaniach CAWI i analizie polskiego rynku B2B, a także rozwojem mediów z niemal 20-letnim doświadczeniem, oferujemy rzetelną metodologię, dostęp do sieci respondentów biznesowych oraz profesjonalne opracowanie wyników – od surowych danych po gotowe raporty i artykuły analityczne. Współpraca z BGR to gwarancja wiarygodnych danych, które wzmacniają pozycję ekspercką partnera i skutecznie wspierają działania marketingowe oraz sprzedażowe.

Redaktor prowadzący: Grzegorz Kubera
Treści, opracowanie: Sebastian Zbywarski, Przemysław Sobieraj, Daria Szewczyk
Kontakt: redakcja@bgreview.pl

O Business Growth Review (BGR)

Business Growth Review to polski serwis biznesowo-technologiczny oraz kwartalnik skierowany do menedżerów, przedsiębiorców i entuzjastów nowoczesnych technologii. Dostarcza rzetelnych analiz, raportów rynkowych i materiałów eksperckich, które pomagają podejmować trafniejsze decyzje biznesowe. BGR łączy świat biznesu z technologią – śledzi trendy, omawia strategie wzrostu i prezentuje dane z polskiego rynku B2B. Kwartalnik BGR to pogłębione opracowania dla firm chcących rozumieć zmieniające się otoczenie rynkowe. Serwis online uzupełnia go o bieżące treści, które inspirują i edukują liderów biznesu każdego dnia.

Business Growth Review

O BGR Quantic

BGR Quantic to agencja badawcza realizująca projekty badań rynku w Polsce i na terenie Unii Europejskiej. Działamy zgodnie z normami UE, zapewniając najwyższe standardy metodologiczne, rzetelność danych oraz pełną zgodność z wymogami RODO. Specjalizujemy się w badaniach CAWI, analizach B2B i dostarczaniu wiarygodnych danych wspierających strategiczne decyzje biznesowe. BGR Quantic to gwarancja profesjonalizmu, transparentności i jakości na każdym etapie projektu badawczego.

BGR Quantic

Marzec 2026 r. Chociaż dołożono wszelkich starań w celu weryfikacji dokładności tych informacji, Business Growth Review nie ponosi żadnej odpowiedzialności za jakiejkolwiek komentarze ani informacje, opinie lub wnioski zawarte w niniejszym raporcie. Aby zacytować dane z raportu, prosimy o użycie tytułu: NIS2 – Czy firmy w Polsce są gotowe na dyrektywę? i pełnej nazwy wydawcy, tj. Business Growth Review.

© 2026 Business Growth Review. Wszelkie prawa zastrzeżone.

Business Growth Review

bgrev.pl