KPMG

Barometr cyberbezpieczeństwa

Ochrona cyfrowej tożsamości

Wstęp

Szanowni Państwo,

Zachęcam do zapoznania się z wynikami piątej edycji badania KPMG „Barometr cyberbezpieczeństwa" diagnozującego bieżące trendy i podejście firm w Polsce w zakresie ochrony przed cyberprzestępczością. W badaniu wzięło udział 100 dużych, średnich i małych firm, reprezentowanych przez osoby odpowiedzialne za zapewnienie bezpieczeństwa informacji.

Tegoroczna edycja badania odbyła się w styczniu 2022 roku, czyli jeszcze przed wybuchem wojny w Ukrainie. Tragiczne wydarzenia za naszą wschodnią granicą oraz bezprecedensowe wzmożenie działań w cyberprzestrzeni z pewnością znacząco zmieniłyby postrzeganie cyberzagrożeń przez polskie przedsiębiorstwa. Niemniej jednak w wynikach ankiety już dało się odczuć rosnące napięcie związane z sytuacją międzynarodową, a w 2021 roku cyberincydentów doświadczyło 69% polskich organizacji. To o 5 p.p. więcej niż przed rokiem, co potwierdza, że zagrożenie staje się coraz bardziej powszechne.

Przedsiębiorstwa w Polsce nadal najbardziej obawiają się zorganizowanej cyberprzestępczości, a o 8 p.p. względem poprzedniego roku wzrosło – spadające do tej pory – poczucie zagrożenia działaniami w cyberprzestrzeni grup wspieranych przez obce państwa. Na liście trzech największych ryzyk pojawiły się zaawansowane, ukierunkowane ataki (Advanced Persistent Threat, APT) obok wyłudzenia danych uwierzytelniających (phishing) oraz wycieków danych przy użyciu złośliwego oprogramowania. Obserwowane obecnie ataki DoS/DDoS nie stanowiły natomiast dla polskich przedsiębiorstw istotnego zagrożenia przed wybuchem wojny.

W tegorocznym badaniu poświęciliśmy szczególną uwagę przybierającemu na znaczeniu obszarowi ochrony tożsamości cyfrowej. Co trzecia badana firma w Polsce wdrożyła rozwiązania automatyzujące procesy zarządzania uprawnieniami (Identity and Access Management, IAM), a niemal co druga posiada systemy chroniące dostęp do kont uprzywilejowanych (Privileged Access Management, PAM). Główną motywacją do inwestycji w te rozwiązania jest potrzeba podniesienia bezpieczeństwa, a w dalszej kolejności zapewnienie zgodności z regulacjami oraz odciążenie administratorów i funkcji wsparcia IT.

Największą barierą w budowaniu bezpieczeństwa są ponownie trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. Jest to zgodne z obserwowanym od kilku lat trendem. Organizacje w coraz większym stopniu zaczynają być również świadome krytycznej roli, jaką pełni biznes w zarządzaniu cyberbezpieczeństwem. Jego niewystarczające zaangażowanie zaczyna być jednym z najistotniejszych wyzwań obok braku środków na inwestycje w cyberbezpieczeństwo.

Pozostaje mi życzyć Państwu przyjemnej lektury oraz wielu przemyśleń i inspiracji, które przyczynią się do wzrostu bezpieczeństwa w Państwa organizacjach.

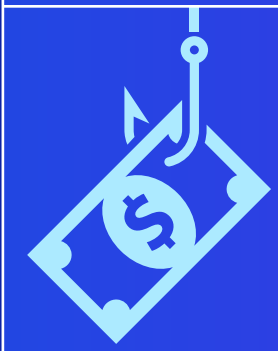
Michał Kurek

Partner, Dział Doradztwa Biznesowego, Szef Zespołu Cyberbezpieczeństwa w KPMG w Polsce i Europie Środkowo-Wschodniej

Najważniejsze wnioski

69% firm w Polsce przyznaje, że odnotowało w 2021 roku przynajmniej jeden incydent cyberbezpieczeństwa. To o 5 p.p. więcej niż przed rokiem.

Więcej niż 1/5 przedsiębiorstw zauważyła w 2021 roku wzrost liczby cyberataków, a tylko w 4% organizacji była ona mniejsza niż przed rokiem.



Zorganizowane grupy cyberprzestępcze pozostają grupą, której obawia się największy odsetek przedsiębiorstw w Polsce – 69%. Najpoważniejszym zagrożeniem zgodnie z deklaracjami przedstawicieli firm jest wyłudzanie danych poprzez phishing.

Wyraźnie wzrosło poczucie zagrożenia działaniami w cyberprzestrzeni grup wspieranych przez obce państwa. Na początku 2022 roku wykazywało je

27%

firm w Polsce – co oznacza odwrócenie malejącego trendu obserwowanego w poprzednich latach.

Spadł poziom postrzegania dojrzałości własnych zabezpieczeń w firmach. Na początku 2022 roku ponad trzy czwarte respondentów deklarowało pełną dojrzałość najwyżej w połowie analizowanych obszarów.

47%

firm w Polsce zadeklarowało posiadanie wdrożonego systemu PAM do zarządzania kontami uprzywilejowanymi. Spośród nich 79% wykorzystuje wymuszanie dodatkowej akceptacji w celu uzyskania dostępu, a 70% monitoruje i rejestruje sesje uprzywilejowane.

Inwestycje w zarządzanie tożsamością i dostępem są motywowane przez blisko

3/4

firm chęcią osiągnięcia większego poziomu bezpieczeństwa informacji, a dla 57% są ważne ze względu na obowiązki regulacyjne.

36% firm wdrożyło system IAM do zarządzania tożsamością i dostępem. Zgodnie z deklaracjami, ponad połowa z nich cieszy się pełną automatyzacją zarządzania uprawnieniami w kluczowych procesach.

Dynamika cyberataków na firmy działające w Polsce

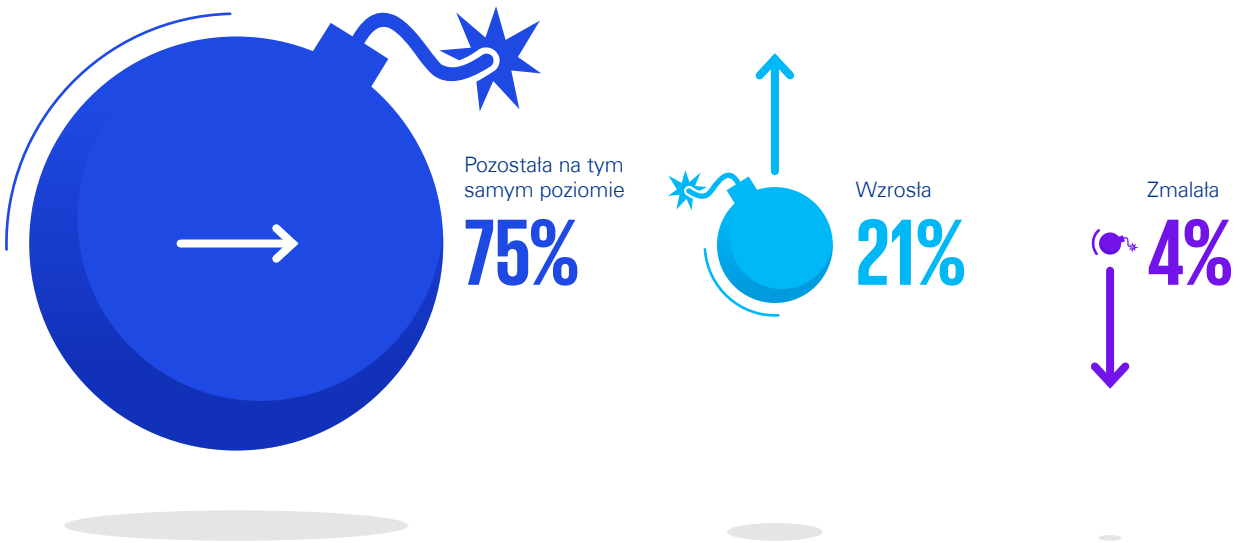
W 2021 roku zdecydowana większość (69%) firm działających w Polsce zarejestrowała przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa. W porównaniu z rokiem poprzednim, odsetek ten wzrósł o 5 p.p. Ponad dwukrotnie powiększył się natomiast w tym czasie odsetek firm, które zaobserwowały 30 i więcej incydentów bezpieczeństwa, co może świadczyć o wzroście aktywności cyberprzestępców. Tylko niecała jedna trzecia badanych przedsiębiorstw w ogóle nie doświadczyła w 2021 roku cyberataku.

Wzrost liczby cyberataków zauważyło 21% przedsiębiorców, natomiast spadek odnotowało jedynie 4% respondentów badania. Trzy czwarte firm twierdzi z kolei, że względem 2020 roku liczba incydentów nie zmieniła się znacząco.

Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa

	2021	2020	2019	2018	2017
0	31%	36%	46%	32%	19%
1-3	23%	26%	29%	33%	29%
4-9	23%	23%	14%	21%	28%
10-29	14%	11%	6%	8%	13%
30 i więcej	9%	4%	5%	6%	11%

Zmiana liczby zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem



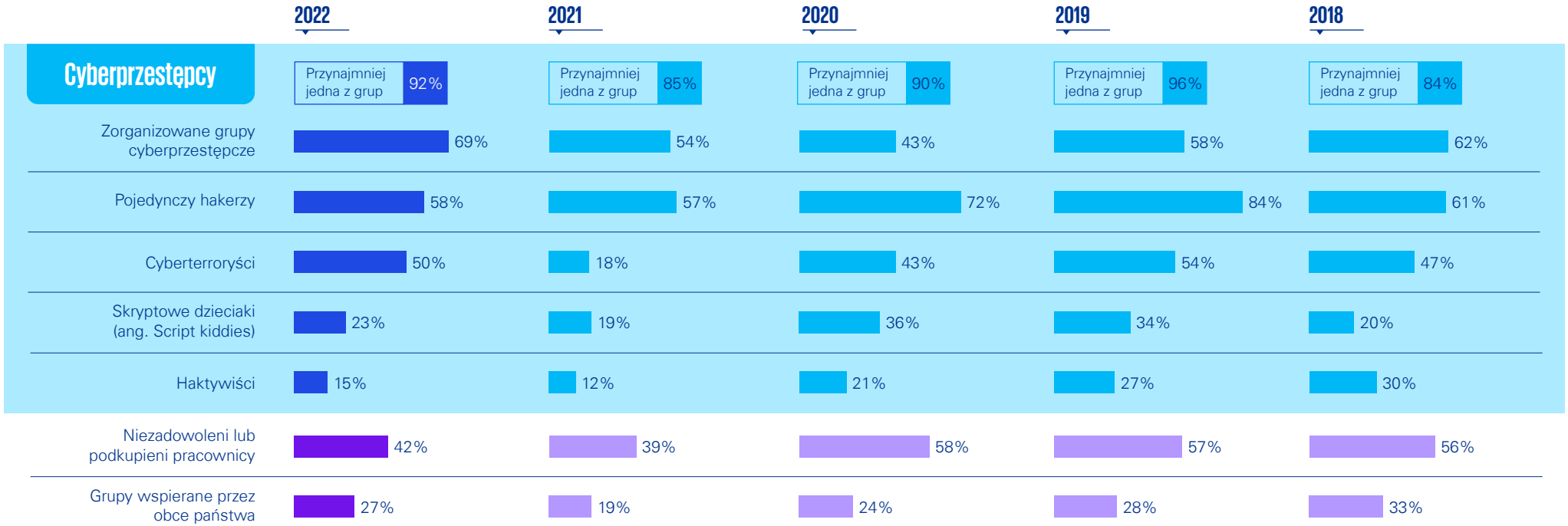
Źródła cyberzagrożeń

W 2022 roku wzrosły obawy przedsiębiorstw wobec wszystkich grup stanowiących zagrożenie dla cyberbezpieczeństwa. Przedsiębiorstwa w Polsce niezmiennie od kilku lat najczęściej wskazują, że realne zagrożenie dla ich funkcjonowania stanowią różnego rodzaju cyberprzestępcy. Na zagrożenie płynące z tej strony od przynajmniej jednej z kategorii cyberprzestępców na początku 2022 roku zwracało uwagę 92% respondentów.

Największym zagrożeniem (po 3 latach) przestają już być jednak pojedynczy hakerzy. Obecnie najwięcej respondentów (69%) źródła realnego zagrożenia dla organizacji upatruje w zorganizowanych grupach cyberprzestępczych. Pokaźny wzrost nastąpił na trzecim miejscu – cyberterrorystów obawia się już połowa badanych firm.

W badaniu przeprowadzanym na przełomie stycznia i lutego 2022 roku odnotowano już zwiększony odsetek przedsiębiorstw wskazujących na zagrożenia ze strony grup wspieranych przez obce państwa. Pełnoskalowa agresja Rosji na Ukrainę nastąpiła dopiero w kolejnych tygodniach, natomiast wojna w cyberprzestrzeni już wtedy miała miejsce. Od 2018 roku sukcesywnie malał udział procentowy takich firm – z 33% do 19% w roku 2021, by w 2022 roku wzrosnąć do 27%.

Grupy stanowiące realne zagrożenie dla organizacji:

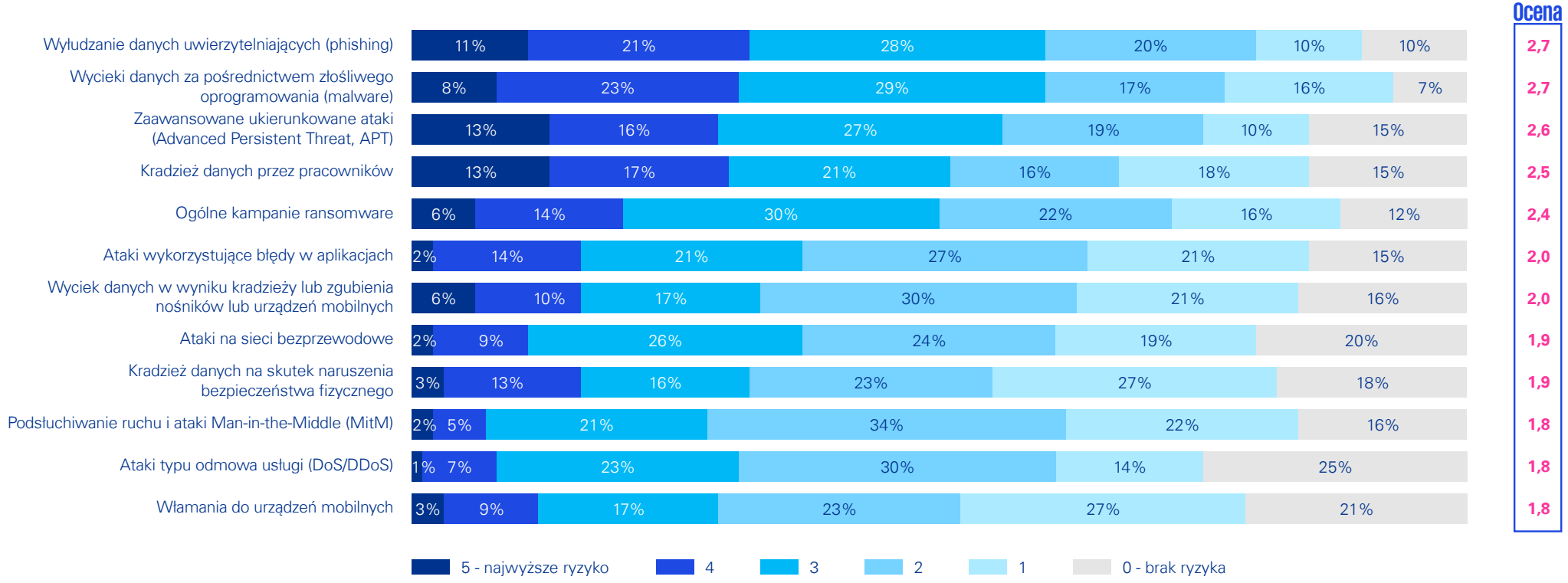


Największe cyberzagrożenia

Kradzież danych poprzez phishing (wyłudzanie danych uwierzytelniających) lub malware (wyciek danych w wyniku złośliwego oprogramowania) jest przez firmy działające w Polsce uznawana za kluczowe zagrożenie w świecie cyfrowym. Ponadto przedsiębiorstwa wyraźnie obawiają się zaawansowanych ataków ze strony profesjonalistów (Advanced Persistent Threat, APT), jak również kradzieży danych przez pracowników. Te stojące na dwóch biegunach różnorodności cyberzagrożenia zostały wskazane ex aequo przez najwyższy odsetek (13%) respondentów jako największe ryzyko dla organizacji.

Za całkowicie nieistotne cyberzagrożenie najwięcej firm (25%) uznało ataki typu DoS/DDoS, czyli zmasowane przesyłanie zapytań, pochłaniające zasoby, aż atakowana infrastruktura lub usługa ulegnie przeciążeniu i przestanie działać. Takie ataki są uciążliwe dla ofiar, jednak poza możliwością szantażu nie dają wymiernych korzyści napastnikom. Często wykorzystywane są jako forma sprzeciwu społeczności internetowej lub grup wspieranych przez państwa wobec firm i instytucji publicznych. Na początku 2022 roku ze wzmożonymi atakami DDoS zmagała się zarówno Ukraina, jak i Rosja.

Które z poniższych cyberzagrożeń stanowią największe ryzyko dla organizacji?



Przypisanie odpowiedzialności za bezpieczeństwo informacji

W przedsiębiorstwach w Polsce odpowiedzialność za bezpieczeństwo informacji wciąż spoczywa głównie na dyrektorze IT (CIO) lub innym pracowniku w strukturach IT. Taka sytuacja od 2019 roku ma miejsce niezmiennie w blisko połowie badanych firm.

Na przestrzeni lat widać jednak znaczny wzrost nacisku na utrzymywanie niezależnego stanowiska Chief Security Officer lub Chief Information Security Officer. W 2022 roku dbali oni o bezpieczeństwo informacji w 14% firm w Polsce, podczas gdy jeszcze dwa-trzy lata temu odsetek ten był znikomy. Coraz rzadziej to prezes zarządu odpowiada za ten obszar lub bezpieczeństwo informacji nie jest w ogóle formalnie przypisane.

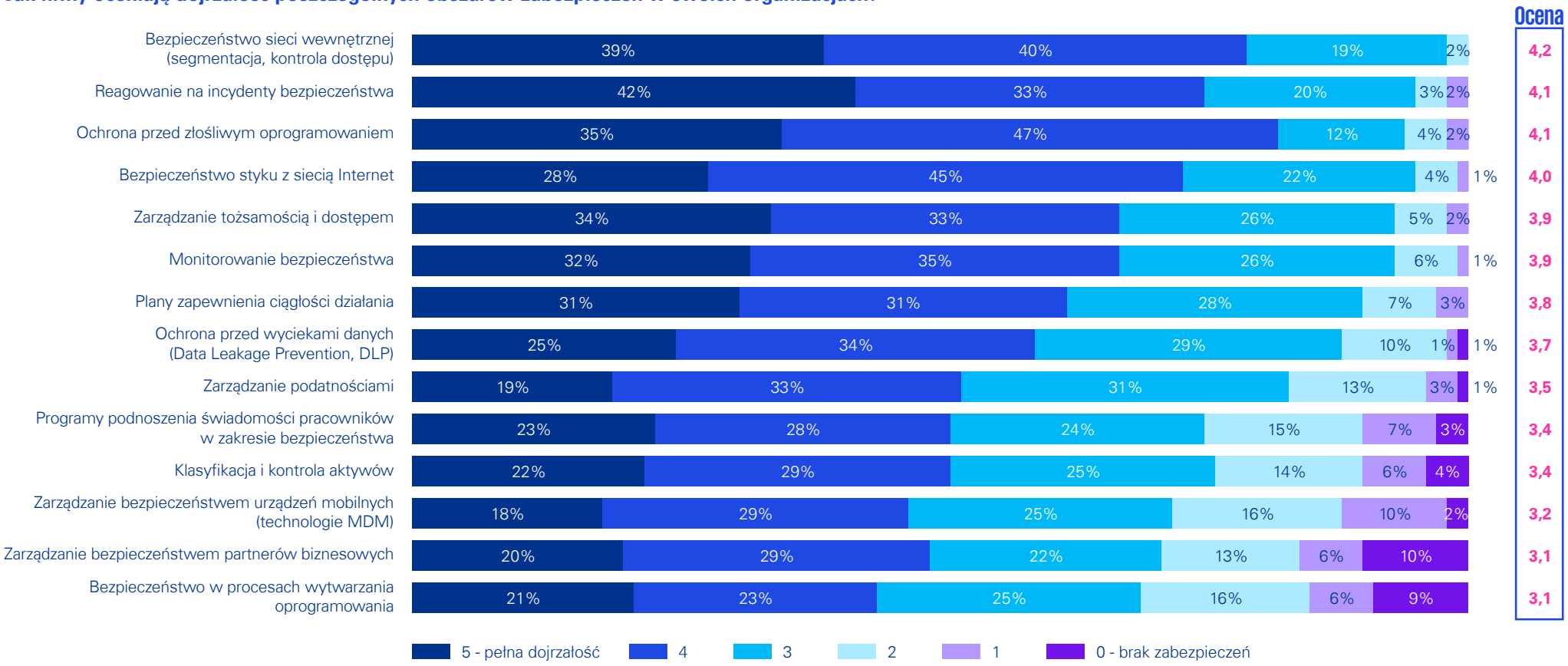
Osoby odpowiedzialne w organizacji za bezpieczeństwo informacji

	2022	2021	2020	2019
Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT	47%	48%	45%	44%
Prezes zarządu (CEO)	15%	22%	23%	30%
Niezależna dedykowana funkcja (CSO/CISO)	14%	11%	3%	2%
Odpowiedzialność przypisana w strukturach globalnych poza Polską	9%	2%	2%	5%
Inne stanowisko w organizacji niż powyższe	5%	4%	12%	13%
Brak formalnego przypisania odpowiedzialności	10%	13%	15%	6%

Stopień dojrzałości obszarów zabezpieczeń w firmach w Polsce

Najwięcej badanych (42%) oceniło, że ich firmy doskonale potrafią na bieżąco reagować na incydenty bezpieczeństwa. Niewiele mniejszy odsetek przedsiębiorstw (39%) wzorowo dba o bezpieczeństwo swojej sieci wewnętrznej. Obszarem zabezpieczeń, który najmniej respondentów (18%) uznało za w pełni dojrzały, jest zarządzanie bezpieczeństwem urządzeń mobilnych. Warto również zwrócić uwagę na obszar, który wybija się pod względem odsetka wskazań braku jakichkolwiek zabezpieczeń. Aż 1 na 10 firm w ogóle nie kontroluje bezpieczeństwa swoich partnerów biznesowych.

Jak firmy oceniają dojrzałość poszczególnych obszarów zabezpieczeń w swoich organizacjach?

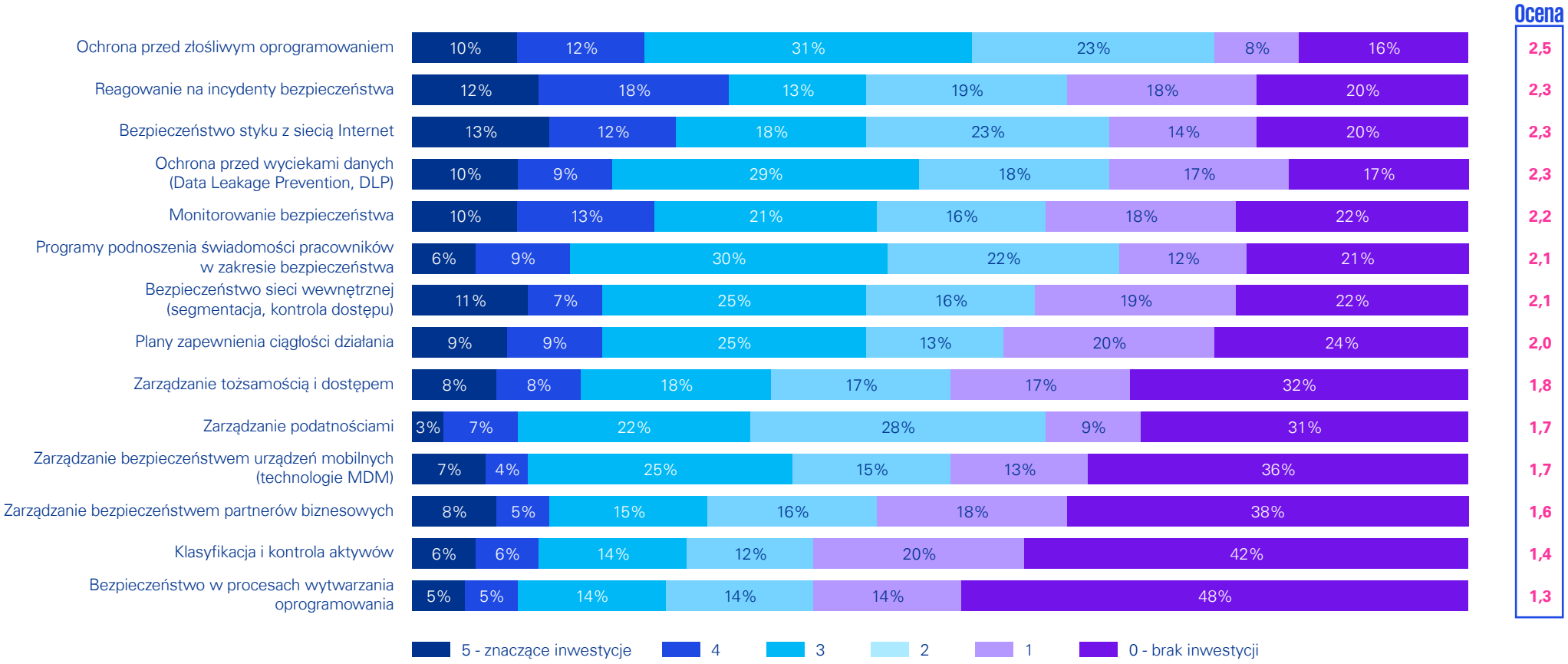


Planowane przez firmy inwestycje w zabezpieczenia

Podobnie jak przed rokiem, firmy w Polsce planują największe nakłady przeznaczać na ochronę przed złośliwym oprogramowaniem. Największy odsetek firm planuje dokonywać w przyszłości znaczących inwestycji na poprawę reagowania na incydenty bezpieczeństwa (13%) i bezpieczeństwo styku z siecią Internet (12%).

Prawie połowa firm (48%) wcale nie planuje inwestować w bezpieczeństwo w procesach wytwarzania oprogramowania, a 42% nie zamierza ponosić nakładów na klasyfikację i kontrolę aktywów. Względem badania przeprowadzonego przed rokiem, na początku 2022 roku we wszystkich obszarach zabezpieczeń odnotowano zwiększony odsetek przedsiębiorstw nie zamierzających przeznaczać na nie nakładów inwestycyjnych.

W jakie obszary zabezpieczeń planują inwestować firmy?



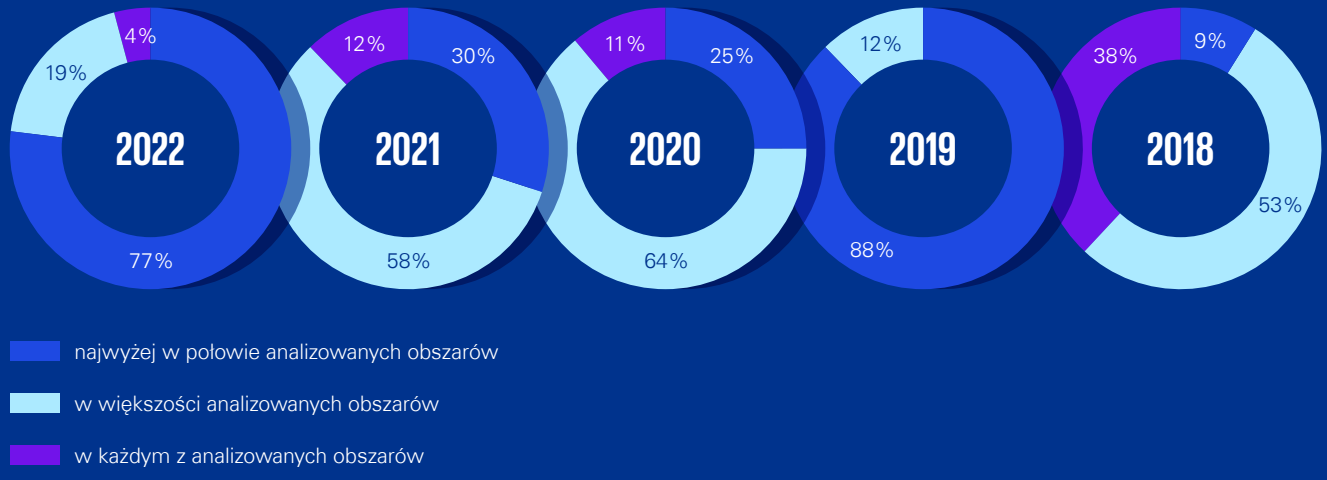
W pełni dojrzałe obszary zabezpieczeń

Okazuje się, że poziom postrzegania dojrzałości własnych zabezpieczeń w badanych organizacjach diametralnie spadł względem poprzedniego roku. Ponad trzy czwarte respondentów na początku 2022 roku zadeklarowało pełną dojrzałość zabezpieczeń najwyżej w połowie analizowanych obszarów.

Wyniki mogą być odzwierciedleniem świadomego podejścia firm do kwestii związanych z rosnącym zapotrzebowaniem na odpowiednie zabezpieczenia względem obecnego stanu. Nowa rzeczywistość biznesowa w ostatnim roku i międzynarodowe cyberataki obserwowane w styczniu i lutym 2022 roku wymusiły dodatkowe zweryfikowanie dojrzałości zabezpieczeń. Wpłynęły tym samym na bardziej racjonalne podejście do planowania i zwiększania nacisku na działania zapewniające ciągłość w tym zakresie.

Tylko 19% firm może pochwalić się dojrzałością zabezpieczeń w większości analizowanych obszarów, a jedynie 4% we wszystkich.

Obszary zabezpieczeń ocenione jako w pełni dojrzałe



Obszary zabezpieczeń – obecna dojrzałość a planowane inwestycje

Matryca poziomu dojrzałości wdrożonych zabezpieczeń oraz planowanych inwestycji wskazuje, że na ogólnym poziomie wszystkie obszary cechują się wysoką dojrzałością, natomiast niskimi planami inwestycji. Relatywnie najsłabszym obszarem jest bezpieczeństwo w procesach wytwarzania oprogramowania, które jest oceniane jako najmniej dojrzałe, a jednocześnie w niższym stopniu niż w innych obszarach planowane są nakłady inwestycyjne.

Obszary bezpieczne, o średnim budżecie

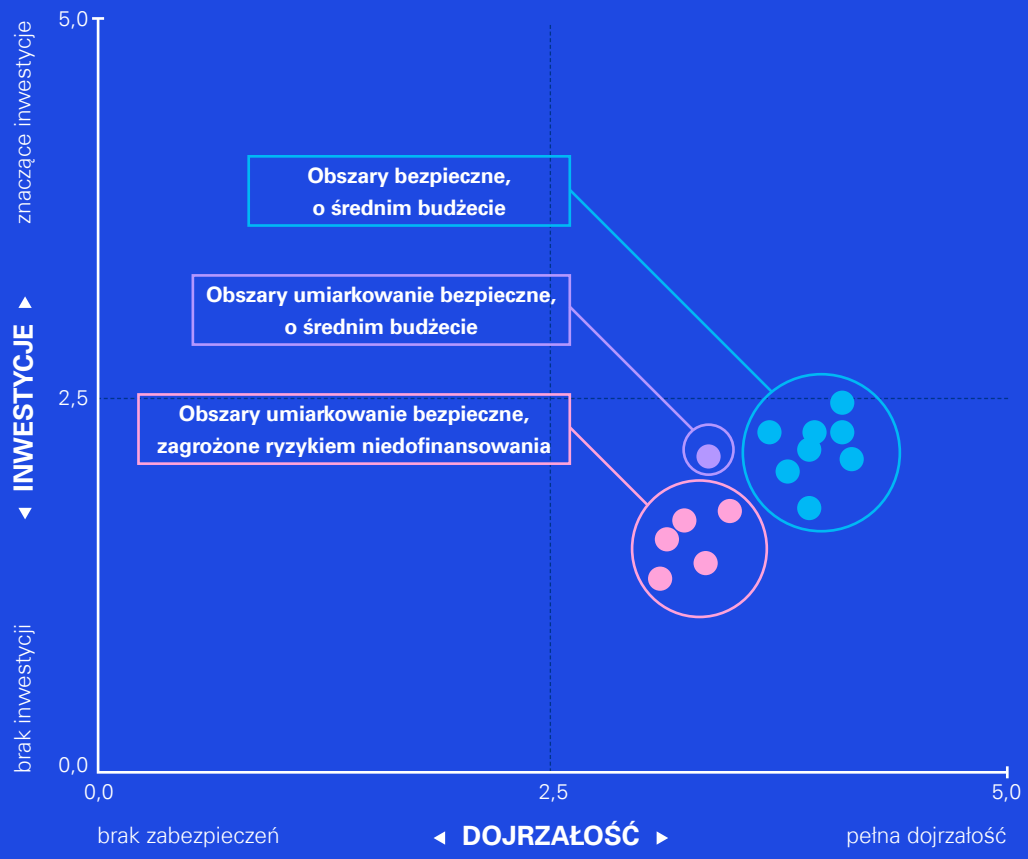
- Bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu)
- Reagowanie na incydenty bezpieczeństwa
- Ochrona przed złośliwym oprogramowaniem
- Bezpieczeństwo styku z siecią Internet
- Zarządzanie tożsamością i dostępem
- Monitorowanie bezpieczeństwa
- Plany zapewnienia ciągłości działania
- Ochrona przed wyciekami danych (Data Leakage Prevention, DLP)

Obszary umiarkowanie bezpieczne, o średnim budżecie

- Zarządzanie podatnościami

Obszary umiarkowanie bezpieczne, zagrożone ryzykiem niedofinansowania

- Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa
- Klasyfikacja i kontrola aktywów
- Zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM)
- Zarządzanie bezpieczeństwem partnerów biznesowych
- Bezpieczeństwo w procesach wytwarzania oprogramowania



Ograniczenia w budowaniu cyberbezpieczeństwa w firmach

Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji

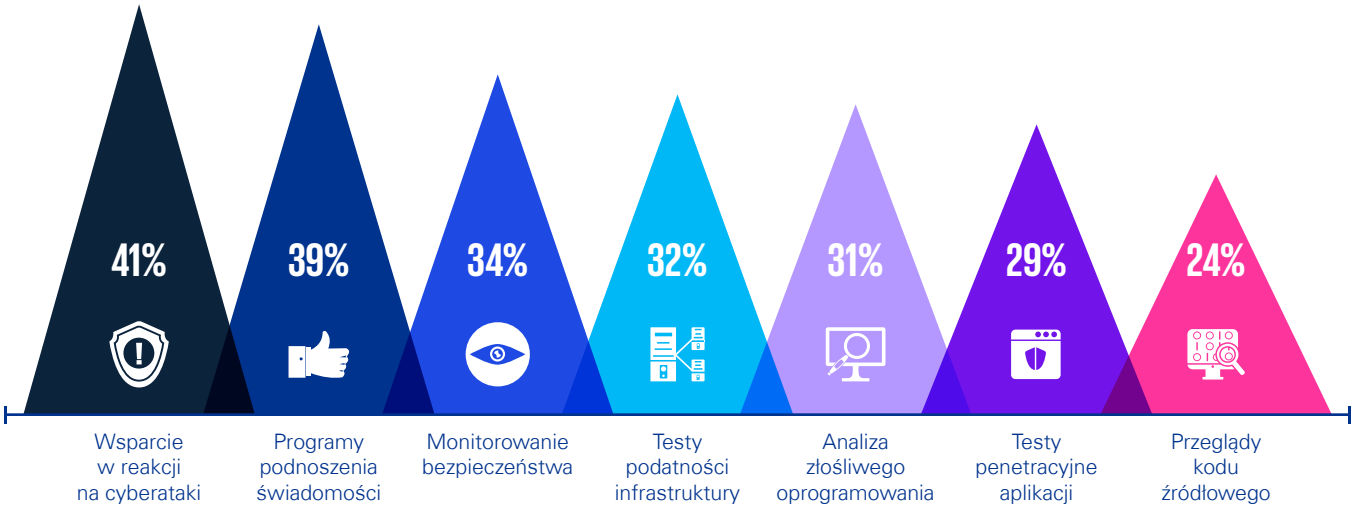
Największym ograniczeniem firm w zakresie uzyskania odpowiedniego poziomu zabezpieczeń niezmiennie są trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. Kwestia ta jest problematyczna dla 64% respondentów. Drugą istotną barierą jest brak wystarczających budżetów, na które wskazuje ponad połowa badanych przedsiębiorstw. Znaczenie obu tych problemów istotnie wzrosło względem badania przeprowadzonego rok wcześniej – odpowiednio o 14 i 15 p.p. Pozostałe ograniczenia są znacznie mniej powszechne i to niezależnie od wielkości firm.

Outsourcing funkcji i procesów bezpieczeństwa

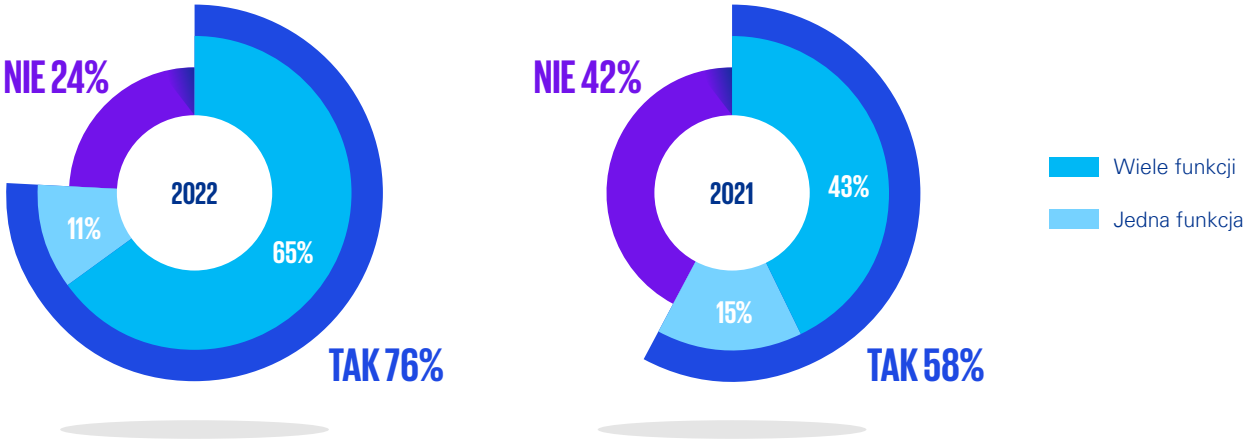
W trzech czwartych badanych firm kwestie bezpieczeństwa danych w organizacji są realizowane przez zewnętrznych dostawców. Jest to istotny wzrost względem ubiegłego roku, kiedy to nieco ponad połowa firm deklarowała zlecanie na zewnątrz funkcji lub procesów bezpieczeństwa. W większości przypadków kwestie bezpieczeństwa firm powierzane są dostawcom zewnętrznym w sposób całościowy (więcej niż jedna funkcja bądź proces) i tendencja ta wzrasta.

Zaskakujący jest fakt, że wsparcie w reakcji na cyberataki, które według wyników ubiegłorocznego badania było najrzadziej outsourcowanym procesem, aktualnie przenoszone jest na dostawców zewnętrznych aż przez 41% badanych firm. Nadal w czołówce funkcji i procesów najczęściej powierzanych zewnętrznym dostawcom są programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa, a także monitorowanie bezpieczeństwa.

Funkcje lub procesy bezpieczeństwa realizowane przez zewnętrznych dostawców



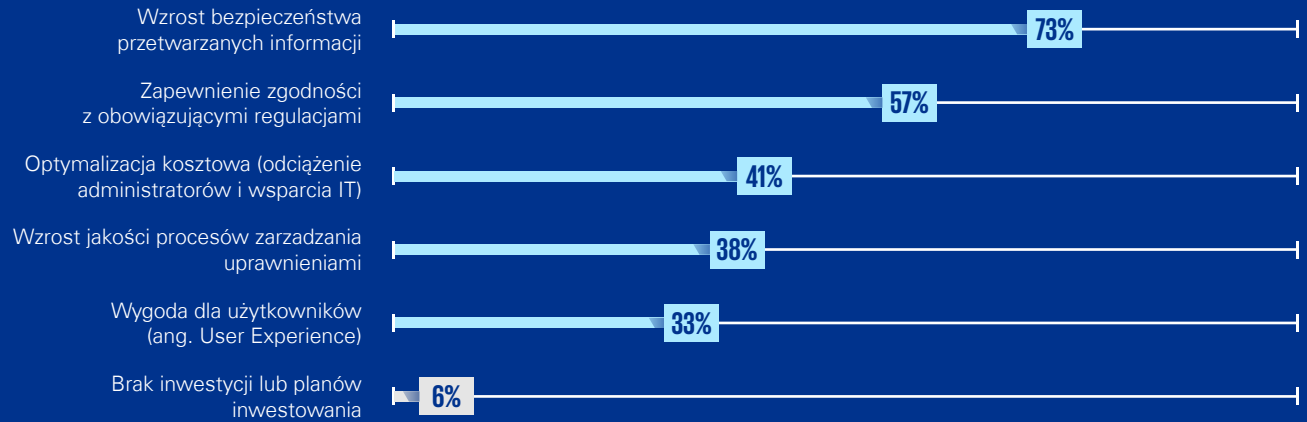
Korzystanie z outsourcingu



Korzyści z systemowego zarządzania tożsamością i dostępem

Dla specjalistów odpowiedzialnych w firmach za bezpieczeństwo informacji najważniejszym czynnikiem wpływającym na decyzję rozpoczęcia inwestycji w procesy zarządzania tożsamością i dostępem jest osiągnięcie wzrostu bezpieczeństwa przetwarzanych informacji – na które wskazało 73% respondentów. Dla 57% jedną z głównych motywacji okazała się potrzeba zapewnienia zgodności z regulacjami, a kolejne 41% widzi w takich inwestycjach szansę na optymalizację kosztową w efekcie odciążenia personelu. Mniej więcej co trzecia firma wśród najważniejszych potencjalnych korzyści wymienia zwiększenie jakości zarządzania uprawnieniami lub wygodę użytkowników. Wśród ankietowanych znalazło się 6% firm, które nie planują inwestować w procesy zarządzania tożsamością i dostępem.

Główne motywacje do inwestycji w procesy zarządzania tożsamością i dostępem



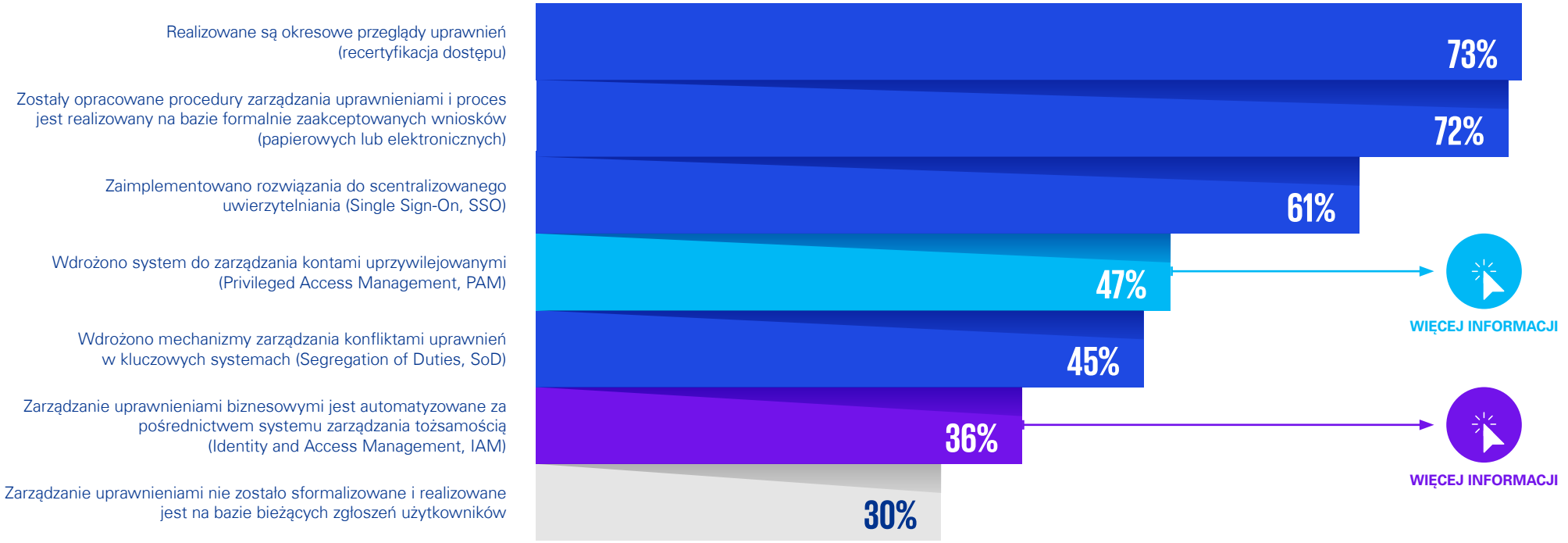
Podejście do zarządzania uprawnieniami

Mniej niż jedna na trzy badane firmy przyznała, że nie posiada sformalizowanego procesu zarządzania uprawnieniami użytkowników. W 72% przedsiębiorstw opracowano w tym zakresie odpowiednie procedury i proces jest realizowany na bazie formalnie zaakceptowanych wniosków. Jeszcze większy odsetek (73%) dokonuje okresowych przeglądów uprawnień. W obu przypadkach odsetek odpowiedzi twierdzących rośnie w dużych firmach, zatrudniających przynajmniej 250 pracowników – odpowiednio do 80% i 76%.

Proces zarządzania uprawnieniami mogą wspomagać określone systemy. Bardzo popularne w organizacjach prowadzących działalność w Polsce okazały się tzw. rozwiązania SSO, służące do scentralizowanego uwierzytelniania, integrujące rozproszone oprogramowanie. Na ich wdrożenie zdecydowało się 61% respondentów.

Systemy wspierające zarządzanie kontami uprzywilejowanymi (Privileged Access Management, PAM) są bardziej popularne niż systemy do zarządzania tożsamością i dostępem (Identity and Access Management, IAM) i wspierają niemal co drugą firmę (47%) w Polsce. Tylko 36% organizacji zautomatyzowało procesy zarządzania uprawnieniami.

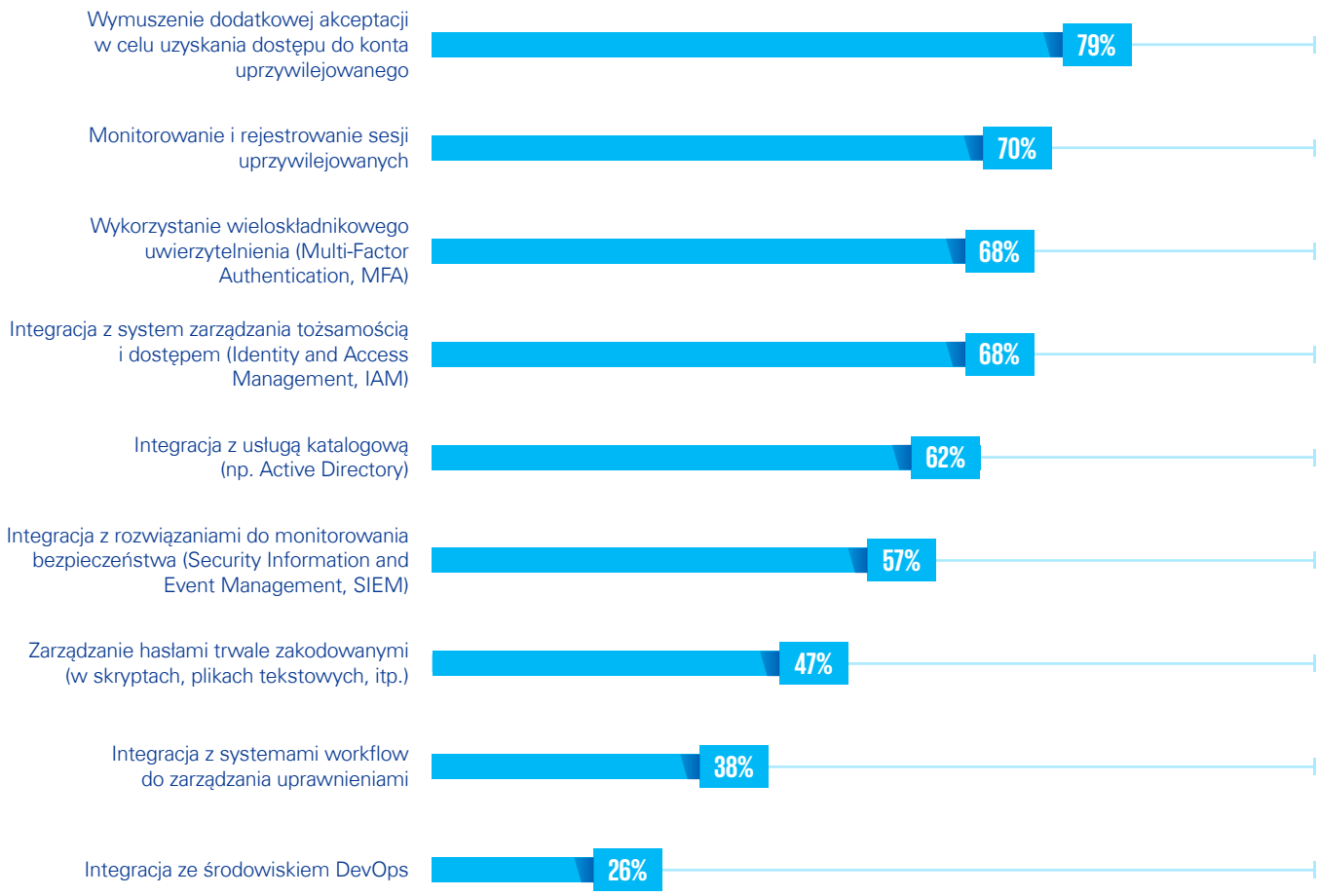
Stwierdzenia opisujące dojrzałość procesów zarządzania uprawnieniami w firmach



Zarządzanie kontami uprzywilejowanymi

Wśród 47% badanych firm, które wdrożyły rozwiązania do zarządzania kontami z wysokimi poziomami uprawnień, stopień ich wykorzystania jest różnorodny. Większość firm (79%) posiadających system typu PAM wymusza dodatkową akceptację w celu uzyskania dostępu do konta uprzywilejowanego, a 70% monitoruje i rejestruje sesje uprzywilejowane. Więcej niż co trzecia firma korzystająca z systemu PAM stosuje wieloetapowe uwierzytelnianie (MFA). W tak samo wielu firmach PAM jest zintegrowany z systemem zarządzania tożsamością i dostępem (IAM). Rzadziej stosowana jest integracja z usługą katalogową (62%), rozwiązaniami do monitorowania bezpieczeństwa (57%), systemami workflow do zarządzania uprawnieniami (38%) lub środowiskiem DevOps (26%). Ponadto niemal połowa respondentów korzystających z PAM zarządza hasłami trwale zakodowanymi.

Deklarowane zakresy wdrożenia systemu zarządzania dostępem uprzywilejowanym (PAM)*



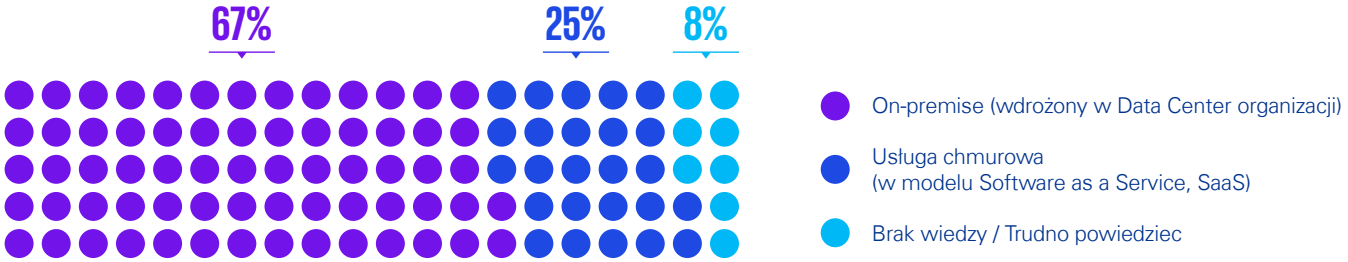
* Wartości procentowe dotyczą odsetka wskazań wśród firm deklarujących posiadanie wdrożonego systemu PAM.

Zarządzanie tożsamością i dostępem

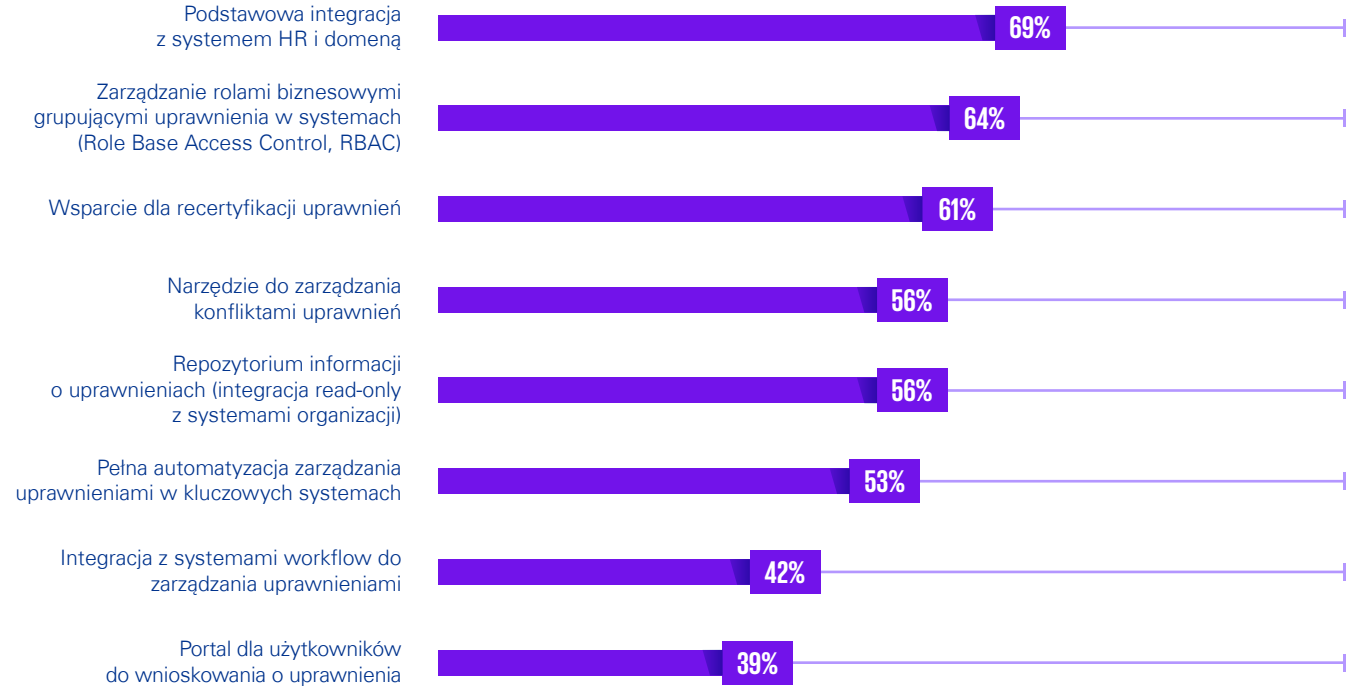
Przeszło jedna trzecia (36%) badanych firm zadeklarowała, że zarządzanie uprawnieniami biznesowymi jest w nich automatyzowane za pośrednictwem systemu zarządzania tożsamością i dostępem (IAM). Okazuje się, że najczęściej jest on wdrażany w data center organizacji (67% przypadków), a tylko co czwarta firma z wdrożonym IAM korzysta z usługi chmurowej dostarczanej w modelu SaaS.

Pełną automatyzację zarządzania uprawnieniami w kluczowych systemach deklaruje 53% firm. Na przynajmniej podstawową integrację IAM ze swoim systemem HR i domeną wskazuje 69% organizacji. Kolejne 64% zarządza rolami biznesowymi grupującymi uprawnienia w systemach, a w 61% firm wdrożony system IAM pomaga w recertyfikacji uprawnień. Tylko 39% przedsiębiorstw korzystających z rozwiązań do zarządzania tożsamością i dostępem posiada portal dla użytkowników umożliwiający wnioskowanie o nadawanie lub modyfikowanie uprawnień.

W jakim modelu został wdrożony system zarządzania tożsamością i dostępem (IAM)?*



Deklarowane zakresy wdrożenia systemu zarządzania tożsamością i dostępem (IAM)*

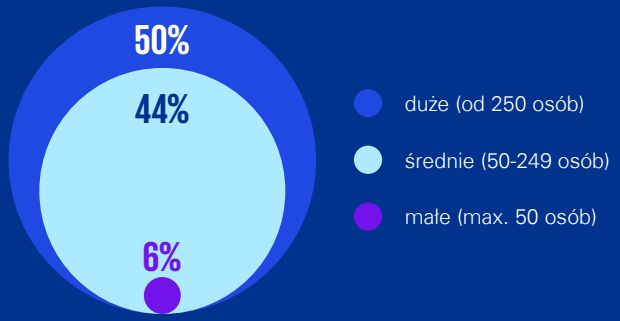


* Wartości procentowe dotyczą odsetka wskazań wśród firm deklarujących posiadanie wdrożonego systemu IAM.

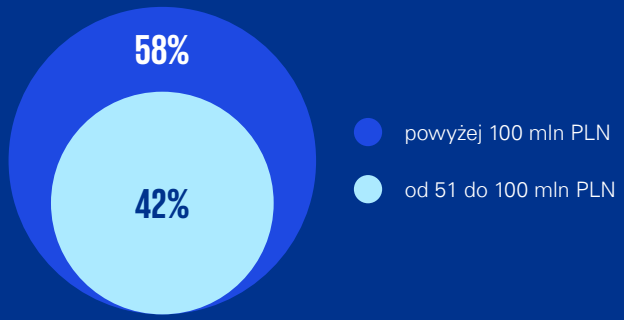
Informacje o badaniu

Badanie zostało zrealizowane metodą wywiadów telefonicznych CATI wśród osób odpowiedzialnych za bezpieczeństwo IT w firmach (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar). Badanie zostało zrealizowane na próbie 100 organizacji o przychodach minimum 51 mln zł na przełomie stycznia i lutego 2022 roku przez firmę Norstat Polska.

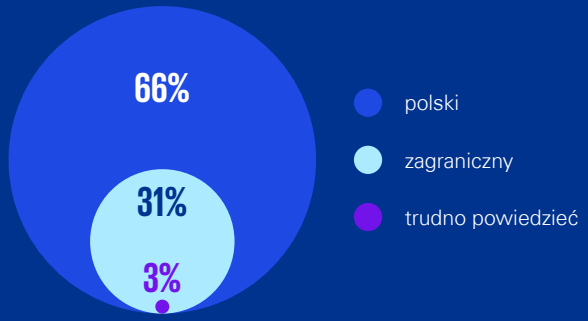
Wielkość badanych firm



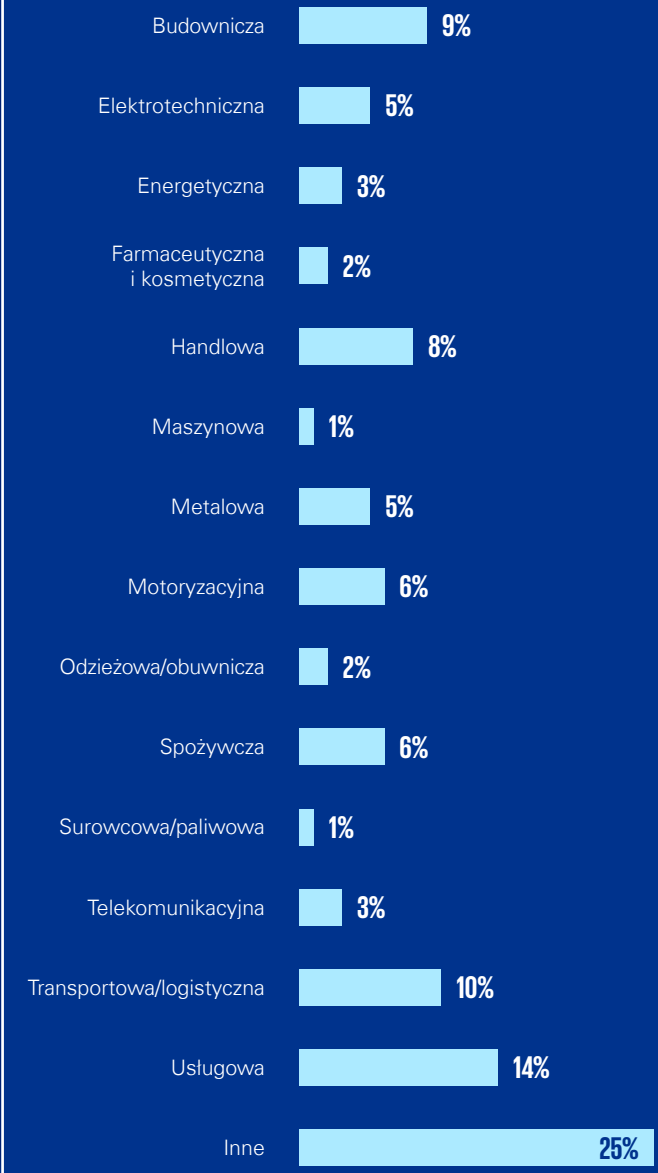
Przychody badanych firm



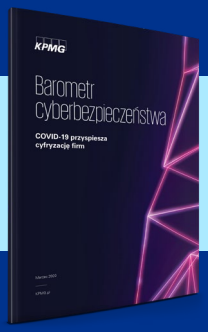
Typ kapitału



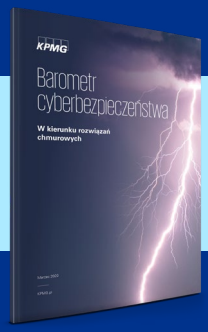
Branża



Wybrane publikacje KPMG w Polsce i na świecie



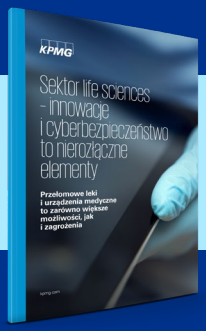
Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm (2021)



Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych (2020)

Barometr cyberbezpieczeństwa. W obronie przed cyberatakami (2019)

Cyberbezpieczeństwo – wyzwanie współczesnego prezesa



Sektor life sciences – innowacje i cyberbezpieczeństwo to nierozłączne elementy

Bezpieczeństwo technologii mobilnych

Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym (2018)

Securing the cloud – the next chapter

Control System Cyber Security Annual Report 2020

Kontakt

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

Michał Kurek

Partner, Dział Doradztwa Biznesowego,
Szef Zespołu Cyberbezpieczeństwa
w KPMG w Polsce i Europie
Środkowo-Wschodniej

E: michalkurek@kpmg.pl

Łukasz Staniak

Starszy Menedżer,
Dział Doradztwa Biznesowego,
Zespół Cyberbezpieczeństwa,
KPMG w Polsce

E: lstaniak@kpmg.pl

Biura KPMG w Polsce

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

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

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

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

Gdańsk
al. Zwycięstwa 13a
80-219 Gdańsk
T: +48 58 772 95 00
E: gdansk@kpmg.pl

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

Łódź
ul. Składowa 35
90-127 Łódź
T: +48 42 232 77 00
E: lodz@kpmg.pl

KPMG Poland

kpmg.pl