KPMG

Barometr cyberbezpieczeństwa

Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu

Luty 2023 | kpmg.pl

Wstęp

Szanowni Państwo,

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

Tegoroczna edycja badania odbyła się na koniec 2022 roku, czyli w trakcie trwania wojny w Ukrainie oraz związanego z nią podwyższonego stopnia alarmowego CHARLIE-CRP w naszej cyberprzestrzeni. Tragiczne wydarzenia za naszą wschodnią granicą oraz bezprecedensowe wzmożenie działań w cyberprzestrzeni niewątpliwie wpłynęło na postrzeganie cyberzagrożeń przez polskie przedsiębiorstwa. Co trzecia polska firma odczuła wzrost intensywności cyberataków, a jedna na pięć organizacji bezpośrednio wiąże ten fakt z trwającą cyberwojną. Najbardziej niepokojącym źródłem zagrożeń cyfrowych pozostają zorganizowane grupy cyberprzestępcze, dodatkowo największy odsetek firm w historii badania obawia się grup wspieranych przez obce państwa. Nie dziwi w związku z tym znaczący wzrost obaw przed zaawansowanymi, ukierunkowanymi atakami APT (tzw. *Advanced Persistent Threat*).

W związku z cyberwojną w tegorocznej edycji Barometru Cyberbezpieczeństwa skupiliśmy się w szczególności na analizie sposobu, w jaki polskie firmy podchodzą do monitorowania bezpieczeństwa i reagowania na cyberataki. Niestety pomimo wskazania tych obszarów przez ankietowane organizacje jako kluczowych kierunków inwestycji, wciąż aż 57% polskich firm przyznaje, że bezpieczeństwo nie jest regularnie monitorowane. Co trzecia firma zadeklarowała powołanie zespołów SOC (*Security Operations Center*), jednak w większości przypadków zespoły te nie pracują w trybie całodobowym. Jedynie co piąta firma zbudowała wewnętrzny zespół reagowania na cyberataki. Natomiast jest to jedna z najchętniej outsourcowanych funkcji bezpieczeństwa.

Outsourcing cyberbezpieczeństwa nie był w historii badania tak powszechny jak obecnie. Korzysta z niego 81% polskich firm. Być może tłumaczy to zaobserwowaną w badaniu zmianę postrzegania głównych barier w budowaniu bezpieczeństwa. W bieżącym roku problem z pozyskaniem i utrzymaniem pracowników ustąpił kwestiom finansowym. Być może ma na to również wpływ niepewność związana z nadchodzącym kryzysem finansowym.

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

Z poważaniem,

Michał Kurek

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

Najważniejsze wnioski

1/3 firm działających w Polsce odnotowała wzrost intensywności cyberataków na swoje systemy w 2022 roku

Przedsiębiorstwa najczęściej wskazują jako realne zagrożenie

zorganizowane grupy cyberprzestępcze (70%)

oraz **pojedynczych hakerów** (59%)

20%

badanych organizacji odnotowało wzmożoną intensywność ataków w związku z trwającą agresją Rosji na Ukrainę

31% firm zetknęło się z atakiem *ransomware*, ale **wszystkie** deklarują, że zdołały sobie z nim poradzić **bez płacenia okupu**

Odsetek przedsiębiorstw obawiających się ataków ze strony **grup wspieranych przez obce państwa** wzrósł o ponad 10 p.p., do 38%

Pełną dojrzałość firmy działające w Polsce deklarują najczęściej w obszarze **bezpieczeństwa sieci wewnętrznej** oraz **ochrony przez złośliwym oprogramowaniem**

Braki w budżecie (57%) i trudności w zatrudnieniu oraz utrzymaniu **wykwalifikowanych pracowników** (47%) są wskazywane jako najpoważniejsze przeszkody utrudniające poprawę cyberzabezpieczeń

81% firm korzysta z outsourcingu przynajmniej jednej z funkcji cyberbezpieczeństwa

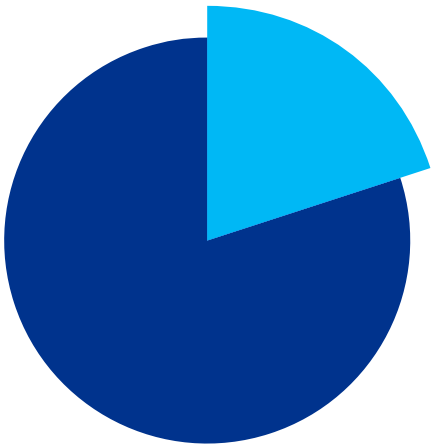
Ponad 2/3 firm wykorzystuje zewnętrzne źródła informacji o zagrożeniach (*Threat Intelligence*) jako element detekcji ataków

36% firm w Polsce wydzieliło w swoich strukturach komórkę SOC do monitorowania cyberzagrożeń

Agresja Rosji na Ukrainę w kontekście cyberbezpieczeństwa

Już w czasie poprzedniej edycji badania, na początku 2022 roku, dało się zaobserwować wzmożone obawy przed zagrożeniem cyberatakami ze strony grup inspirowanych przez obce państwa. Od tego czasu wprowadzano na terenie Polski kolejne stopnie alarmowe w związku z zagrożeniem bezpieczeństwa cyfrowego. Co piąta firma biorąca udział w badaniu KPMG w Polsce przeprowadzonym w grudniu 2022 roku wskazała, że w związku z trwającą wojną w Ukrainie odnotowała wzmożoną aktywność hakerską skierowaną przeciwko niej. Pozostałe takich zmian nie zaobserwowały, co może jednak w niektórych przypadkach oznaczać, że atak nie został jeszcze wykryty.

Wpływ wojny w Ukrainie na cyberbezpieczeństwo w Polsce



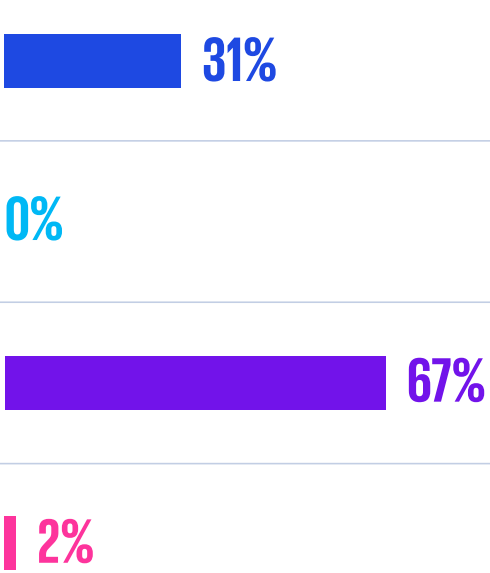
20%
Odnotowano wzmożoną aktywność przeciwko firmie

80%
Nie odnotowano istotnych zmian

Ataki typu *ransomware*

W ostatnich latach na świecie nasileniu uległy ataki typu *ransomware*. To rodzaj złośliwego oprogramowania szyfrującego dane, które znajdują się na dysku lub blokującego system. Hakerzy żądają zapłacenia okupu w zamian za przywrócenie dostępu. Większość tego typu ataków zaczyna się od napisania wiadomości email, która zawiera link do strony kontrolowanej przez atakującego lub załącznik ze złośliwym kodem. Blisko jedna trzecia respondentów wskazała, że padła w przeszłości ofiarą tego typu ataku. Żadna z badanych firm nie przyznała się jednak do zapłacenia okupu, twierdząc, że udało im się obronić przed atakiem i odtworzyć ciągłość działania.

Czy organizacja padła ofiarą znaczącego ataku typu *ransomware*?



Dynamika cyberataków na firmy działające w Polsce

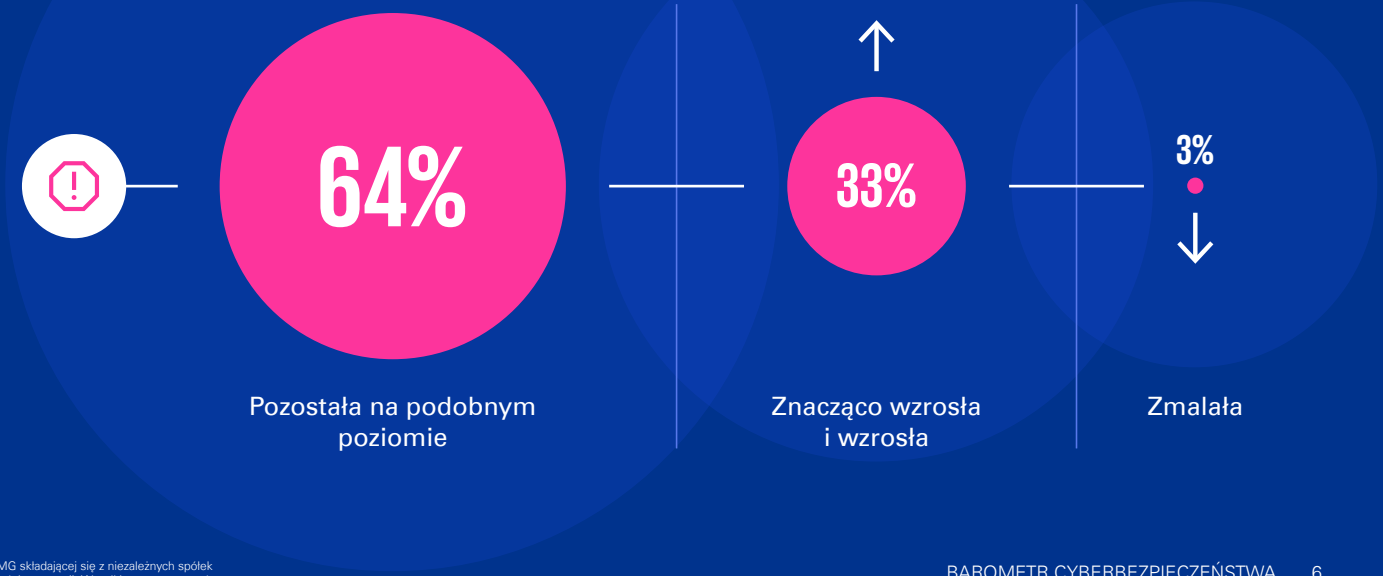
W ciągu 2022 roku ponad połowa badanych firm w Polsce (58%) zarejestrowała przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa. Wzrósł odsetek firm, które nie przyznają się do odnotowania jakiegokolwiek ataku na swoje systemy. Studzi jednak fakt, że aż u jednej trzeciej badanych podmiotów, intensywność prób naruszeń wzrosła. To najwyższy od pięciu lat odsetek firm, które przyznają, że notują coraz więcej ataków. Firmy, które odpowiedziały, że nie zetknęły się z tego typu incydentami, mogły jedynie jeszcze tego nie wykryć.

Jeszcze nigdy w historii badania KPMG w Polsce odsetek firm, które odnotowały więcej niż 30 cyberincydentów, nie był tak wysoki. W 2022 roku taką statystykę zaraportowało 12% ankietowanych.

Liczba zarejestrowanych przez firmy incydentów zagrażających cyberbezpieczeństwu firmy

	2022	2021	2020	2019	2018
0	42%	31%	36%	46%	32%
1-3	25%	23%	26%	29%	33%
4-9	9%	23%	23%	14%	21%
10-29	12%	14%	11%	6%	8%
30 i więcej	12%	9%	4%	5%	6%

Zmiana liczby zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem

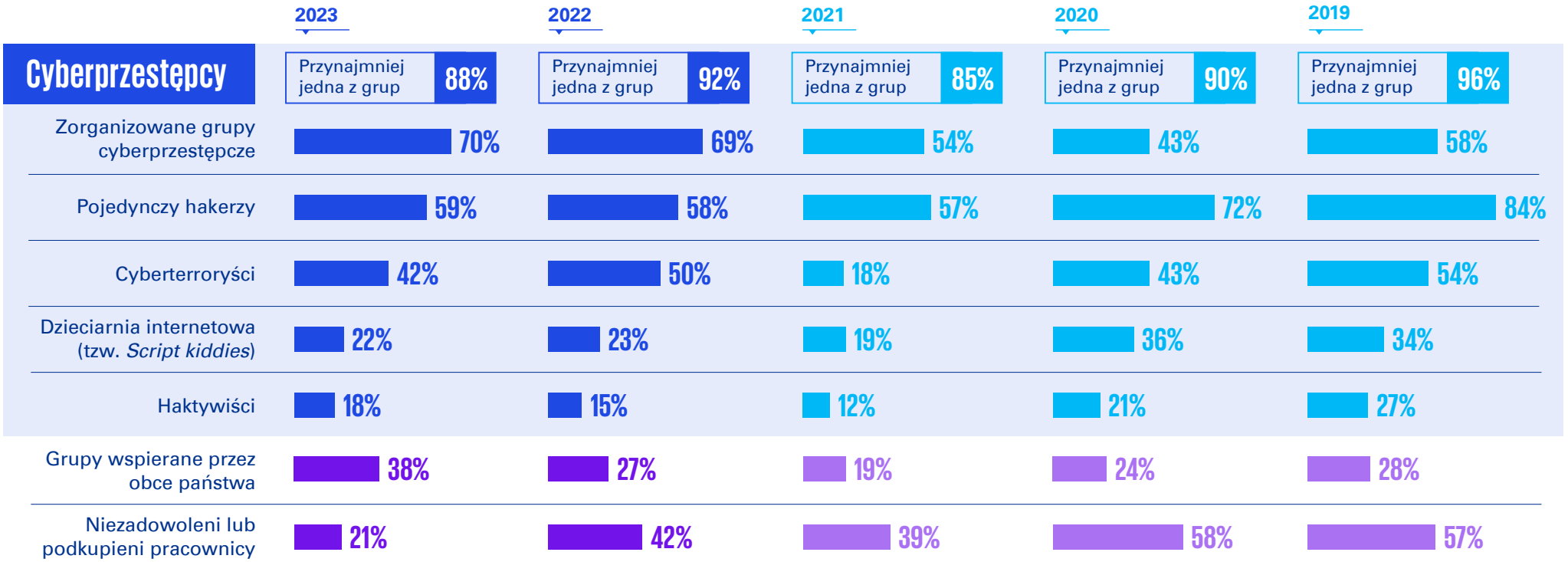


Źródła cyberzagrożeń

W najnowszej edycji badania nieznacznie spadł odsetek przedsiębiorstw obawiających się zagrożeń ze strony którejś z grup cyberprzestępców. Porównując z wynikami sprzed roku, nie zmieniła się pozycja najpoważniejszych z nich. Na koniec 2022 roku z 50% do 42% zmniejszyło się grono odczuwające realne zagrożenie ze strony cyberterrorystów. Do 21%, czyli dokładnie o połowę, zmniejszył się odsetek osób odpowiedzialnych za cyberbezpieczeństwo, które boją się jego naruszenia ze strony niezadowolonych lub podkupionych pracowników.

Poprzednie badanie zrealizowane na krótko przed rosyjską inwazją na Ukrainę już pokazało odczuwalny wzrost napięć między grupami z różnych krajów w cyberprzestrzeni. W czasie toczącej się pełnoskalowej wojny obawy wzrosły tak, że w grudniu 2022 już 38% ankietowanych firm wskazywało na zagrożenie płynące ze strony grup wspieranych przez obce państwa.

Grupy stanowiące realne zagrożenie dla organizacji



Łukasz Staniak

Dyrektor,
Dział Doradztwa Biznesowego, Zespół Cyberbezpieczeństwa, KPMG w Polsce

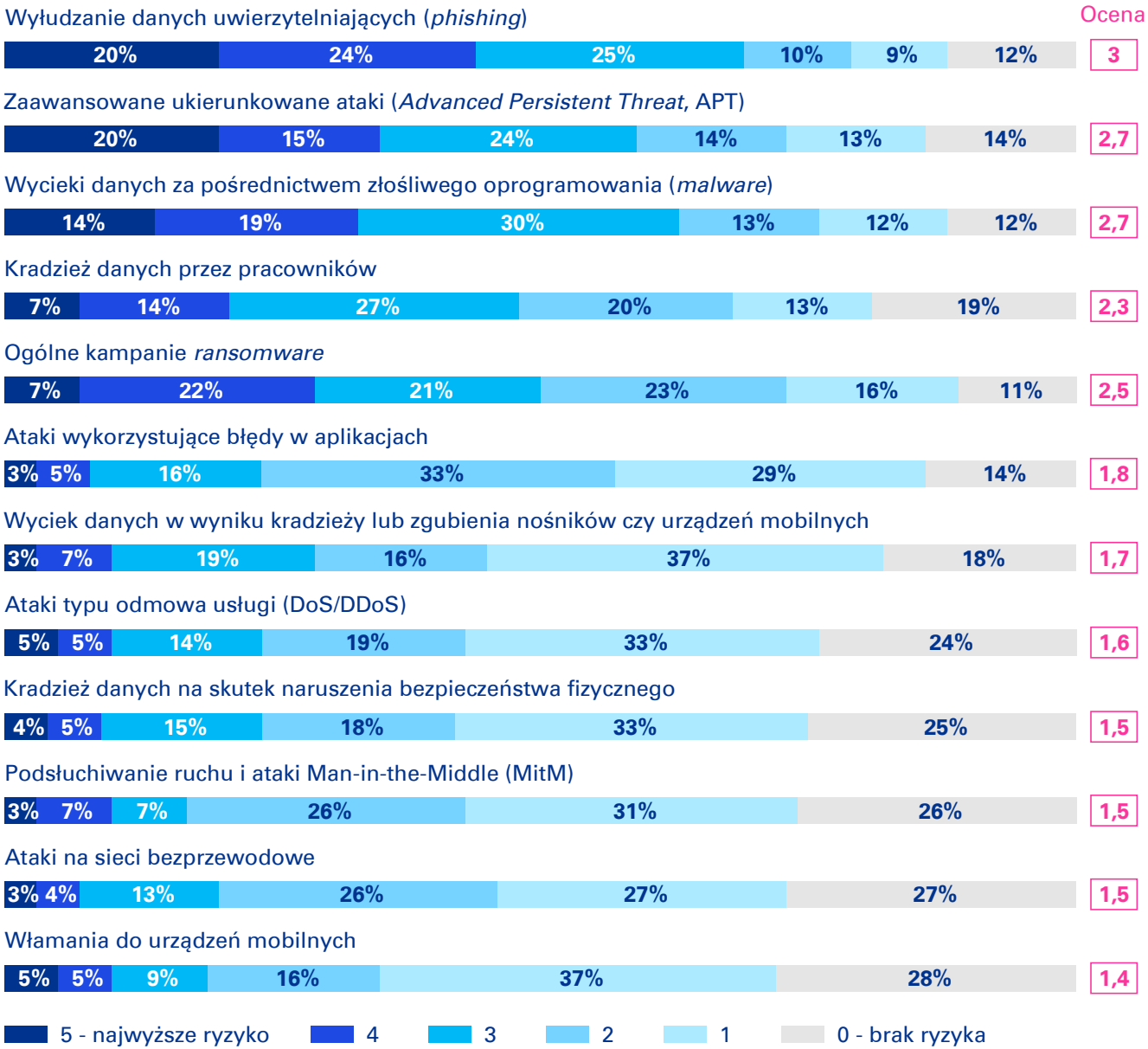
Cyberzagrożenia wywołane trwającą wojną w Ukrainie nawet jeśli nie bezpośrednio, to w pośredni sposób pojawiają się w odpowiedziach ankietowanych. Firmy szukają pomocy w zidentyfikowaniu i zaadresowaniu wszelkich słabości w infrastrukturze teleinformatycznej, które mogłyby zostać wykorzystane przez zorganizowane grupy cyberprzestępcze. Świadomość swoich słabości oraz odpowiednie podejście do zminimalizowania ryzyka, które z nich wynika, jest kluczowa w obecnej sytuacji.

Największe cyberzagrożenia

Kradzież danych poprzez phishing oraz zaawansowane i ukierunkowane ataki (tzw. *Advanced Persistent Threat*) są uznawane za kluczowe zagrożenia w cyfrowym świecie. Jedna piąta badanych firm wskazała te cyberzagrożenia jako ryzyka o najwyższym priorytecie. Ich znaczenie wzrosło na przestrzeni ostatniego roku – w poprzedniej edycji badania nie były one tak często wskazywane jako kluczowe. Jednym z głównych cyberzagrożeń są również wycieki danych za pośrednictwem *malware*. Kradzież danych przez pracowników oraz ogólne kampanie *ransomware* zostały ex aequo wskazane przez 7% respondentów jako jedne z największych ryzyk dla organizacji.

Ponad jedna czwarta firm uznała włamania do urządzeń mobilnych oraz ataki na sieci bezprzewodowe za całkowicie nieistotne cyberzagrożenie (odpowiednio 28% i 27%).

Cyberzagrożenia stanowiące największe ryzyko dla organizacji



Osoby odpowiedzialne w organizacji za bezpieczeństwo informacji

	2023	2022	2021	2020	2019
Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT	45%	47%	48%	45%	44%
Prezes zarządu (CEO)	17%	15%	22%	23%	30%
Niezależna dedykowana funkcja (CSO/CISO)	8%	14%	11%	3%	2%
Odpowiedzialność przypisana w strukturach globalnych poza Polską	5%	9%	2%	2%	5%
Inne stanowisko w organizacji niż powyższe	8%	5%	4%	12%	13%
Brak formalnego przypisania odpowiedzialności	17%	10%	13%	15%	6%

Przypisanie odpowiedzialności za bezpieczeństwo informacji

W przedsiębiorstwach w Polsce odpowiedzialność za cyberbezpieczeństwo spoczywa najczęściej na dyrektorze IT (CIO) lub innym pracowniku w strukturach tego działu. Taka sytuacja ma miejsce niezmiennie w niemal połowie badanych firm na przestrzeni ostatnich lat.

Jeszcze do zeszłego roku kurczył się odsetek firm, w których to CEO okazywał się osobą odpowiedzialną za bezpieczeństwo informacji. Najnowsza edycja badania pokazała po raz pierwszy od kilku lat zmianę tej spadkowej tendencji i wzrost o 2 p.p. do 17%. O prawie połowę (z 14% do 8%) spadła natomiast odpowiedzialność za bezpieczeństwo informacji przypisana do niezależnej funkcji CSO/CISCO.

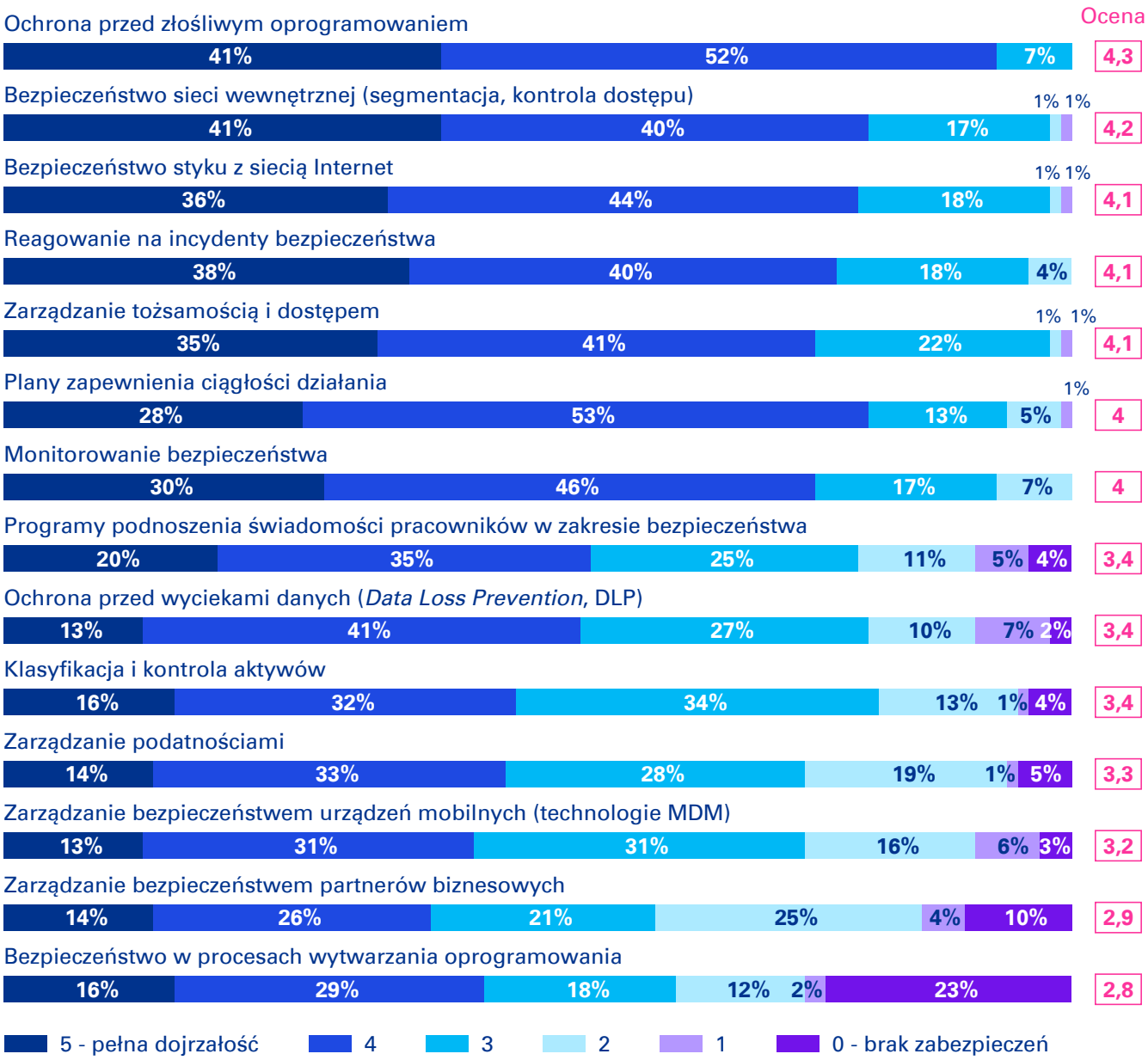
Aż 17% badanych firm w grudniu 2022 wskazało, że formalnie nie przypisano w nich nikomu odpowiedzialności za omawiany obszar. Odsetek ten spada jednak do 4% w przypadku dużych firm, zatrudniających przynajmniej 250 pracowników.

Stopień dojrzałości obszarów zabezpieczeń w firmach w Polsce

Ochrona przed złośliwym oprogramowaniem oraz bezpieczeństwo sieci wewnętrznej są obszarami, w których firmy w Polsce deklarują najwyższy poziom dojrzałości. 41% respondentów wskazało je jako w pełni dojrzałe sektory w swoich organizacjach. Wysoko oceniane jest także własne bezpieczeństwo styku z siecią Internet, procesy reagowania na incydenty oraz zarządzanie tożsamością i dostępem.

Obszarami zabezpieczeń, które przez najmniejszy odsetek respondentów (13%) zostały uznane za w pełni dojrzałe, są zarządzanie bezpieczeństwem urządzeń mobilnych oraz ochrona przed wyciekami danych – DLP. Warto również zwrócić uwagę na dwa obszary, które wybijają się pod względem odsetka wskazań braku jakichkolwiek zabezpieczeń. Prawie co czwarta firma w ogóle nie kontroluje bezpieczeństwa w procesach wytwarzania oprogramowania, a co dziesiąta nie dba o bezpieczeństwo swoich partnerów biznesowych.

Ocena dojrzałości poszczególnych obszarów zabezpieczeń w organizacji



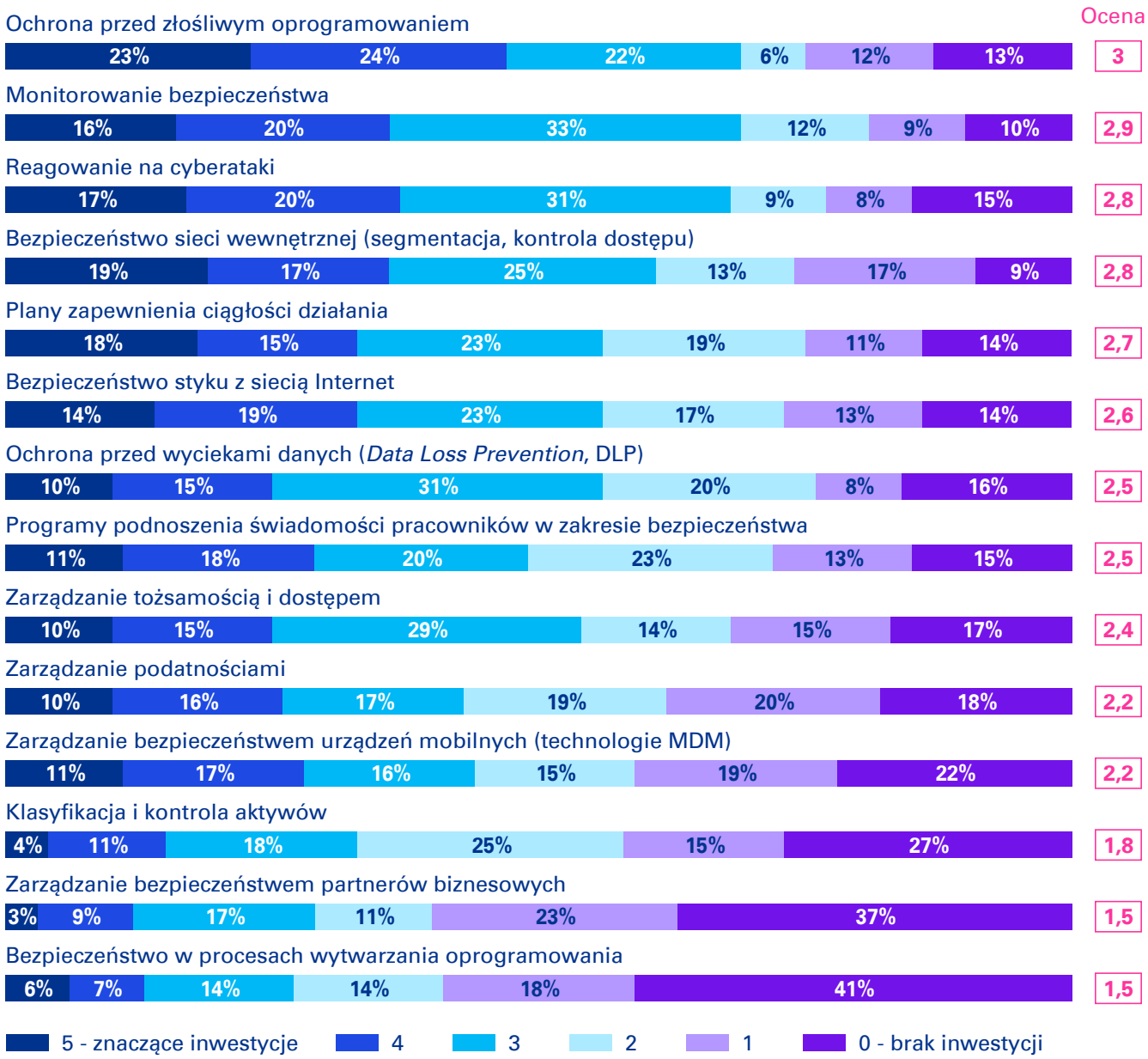
Planowane przez firmy inwestycje w zabezpieczenia

Porównując wyniki badania przeprowadzonego na koniec 2022 roku z poprzednią edycją raportu KPMG można zauważyć, że organizacje w Polsce planują zwiększać inwestycje we wszystkich obszarach zabezpieczeń przed cyberzagrożeniami.

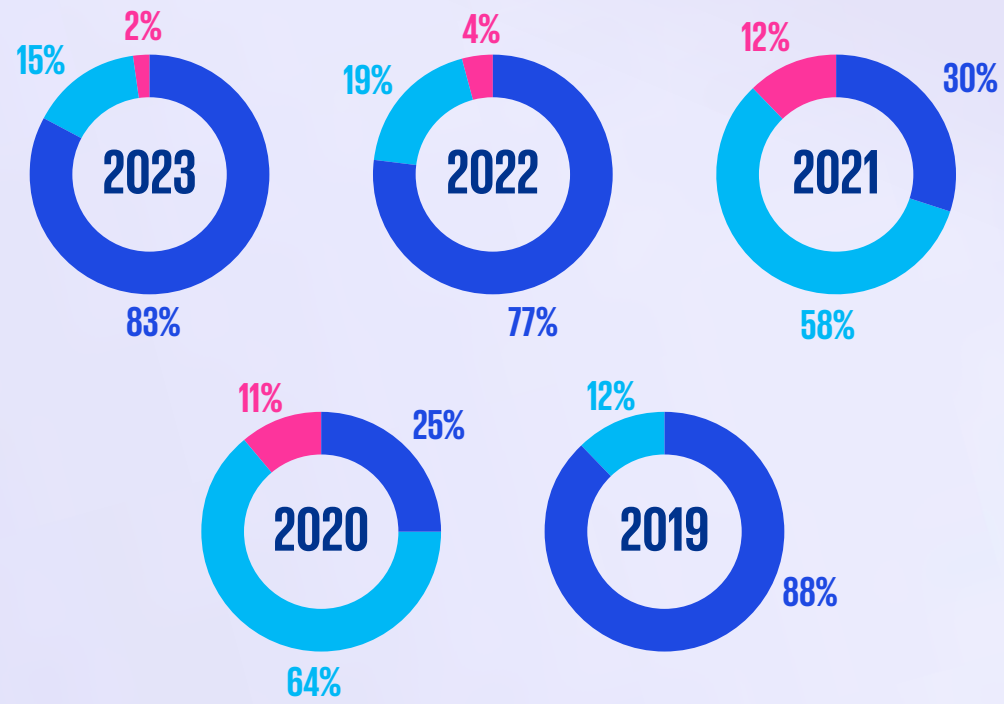
Największe nakłady w ciągu najbliższego roku zostaną przeznaczone na obszar związany z ochroną przed złośliwym oprogramowaniem (23%), monitorowanie bezpieczeństwa i reakcję na cyberataki (16% i 17% odpowiednio).

Najmniejsze środki firmy zamierzają zainwestować w bezpieczeństwo w procesach wytwarzania oprogramowania oraz zarządzanie bezpieczeństwem partnerów biznesowych.

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



Obszary zabezpieczeń ocenione jako w pełni dojrzałe



w większości analizowanych obszarów

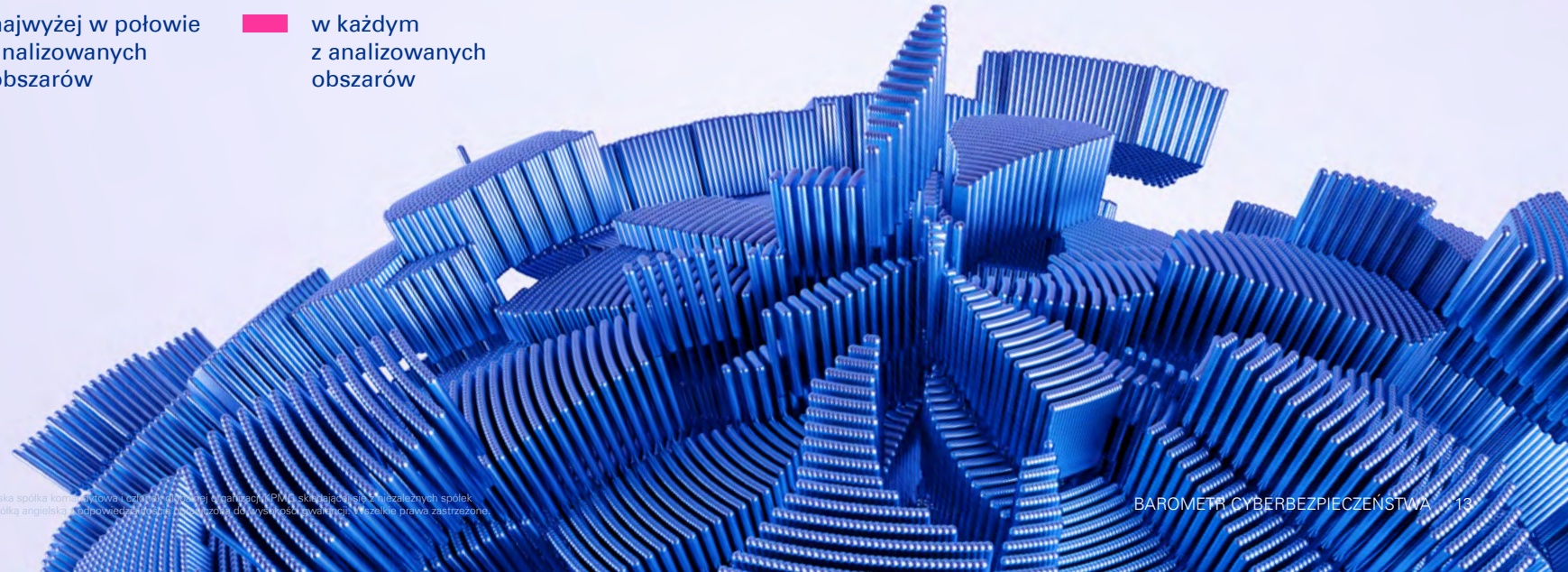
najwyżej w połowie analizowanych obszarów

w każdym z analizowanych obszarów

W pełni dojrzałe obszary zabezpieczeń

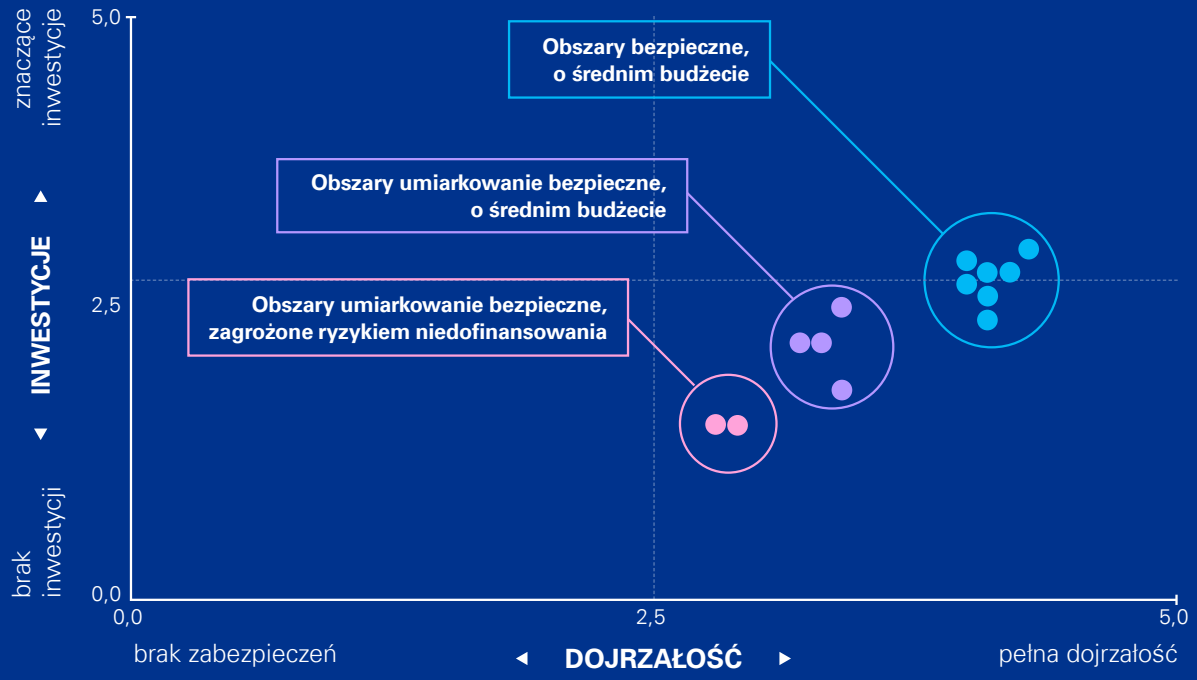
Na przestrzeni ostatnich lat obniża się poziom samooceny dojrzałości analizowanych obszarów bezpieczeństwa. W najnowszej edycji badania tylko 2% organizacji zadeklarowało pełną dojrzałość wszystkich obszarów cyberzabezpieczeń, a kolejne 15% jedynie połowiczną gotowość.

W czasie przeprowadzania badania na terenie całego kraju obowiązywał podwyższony stopień alarmowy CHARLIE-CRP w związku ze zwiększonym ryzykiem wystąpienia ataków w cyberprzestrzeni. Niepewność może skłaniać firmy do przykładania większej wagi do zabezpieczeń, a zarazem uznawania za bardziej istotne zagrożeń dotąd ignorowanych.



Obszary zabezpieczeń – obecna dojrzałość a planowane inwestycje

Matryca poziomu dojrzałości wdrożonych zabezpieczeń oraz planowanych inwestycji wskazuje, że na ogólnym poziomie wszystkie obszary cechują się z jednej strony wysoką dojrzałością, jednak z drugiej niskimi lub średnimi planami inwestycyjnymi. Relatywnie najsłabszymi obszarami są bezpieczeństwo w procesach wytwarzania oprogramowania i zarządzanie bezpieczeństwem partnerów biznesowych, które są oceniane jako najmniej dojrzałe, a jednocześnie w niższym stopniu niż w innych obszarach planowane są nakłady inwestycyjne. Kategorie brane pod uwagę w badaniu, których budżet zwiększył się na przestrzeni roku to programy podnoszenia świadomości pracowników, kontrola aktywów oraz zarządzanie bezpieczeństwem urządzeń mobilnych. Poziom bezpieczeństwa spadł natomiast w zakresie DLP.



Obszary bezpieczne, o średnim budżecie:

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

Obszary umiarkowanie bezpieczne, o średnim budżecie:

- Zarządzanie podatnościami
- Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa
- Klasyfikacja i kontrola aktywów
- Zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM)
- Ochrona przed wyciekami danych (tzw. DLP)

Obszary umiarkowanie bezpieczne, zagrożone ryzykiem niedofinansowania:

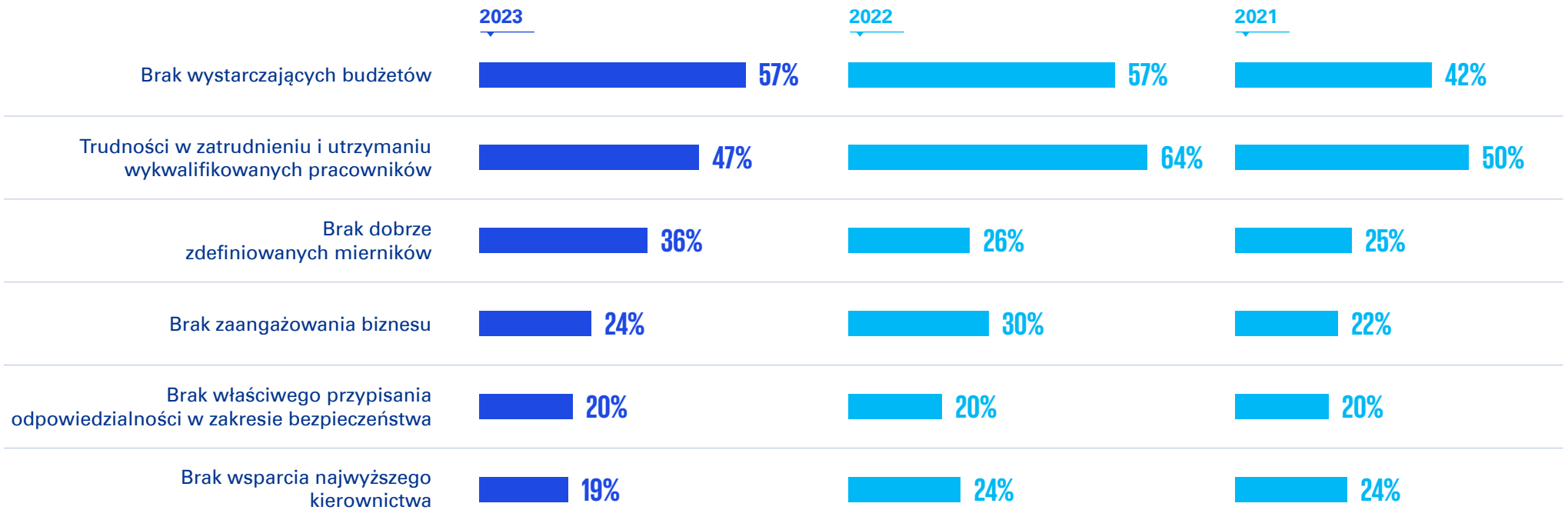
- Zarządzanie bezpieczeństwem partnerów biznesowych
- Bezpieczeństwo w procesach wytwarzania oprogramowania

Ograniczenia w budowaniu cyberbezpieczeństwa w firmach

Największym ograniczeniem firm w zakresie uzyskania odpowiedniego poziomu zabezpieczeń jest brak wystarczających budżetów. Odsetek ten nie zmienił się i pozostaje na poziomie 57%. Również dużym ograniczeniem dla blisko połowy organizacji są trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników, jednak w porównaniu z poprzednim rokiem odsetek firm wskazujących na to ograniczenie zmalał o 17 p.p.

Natomiast w porównaniu z badaniem przeprowadzonym rok wcześniej z 26% do 36% wzrosła grupa firm wskazujących na ograniczenie związane z brakiem dobrze zdefiniowanych mierników.

Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji

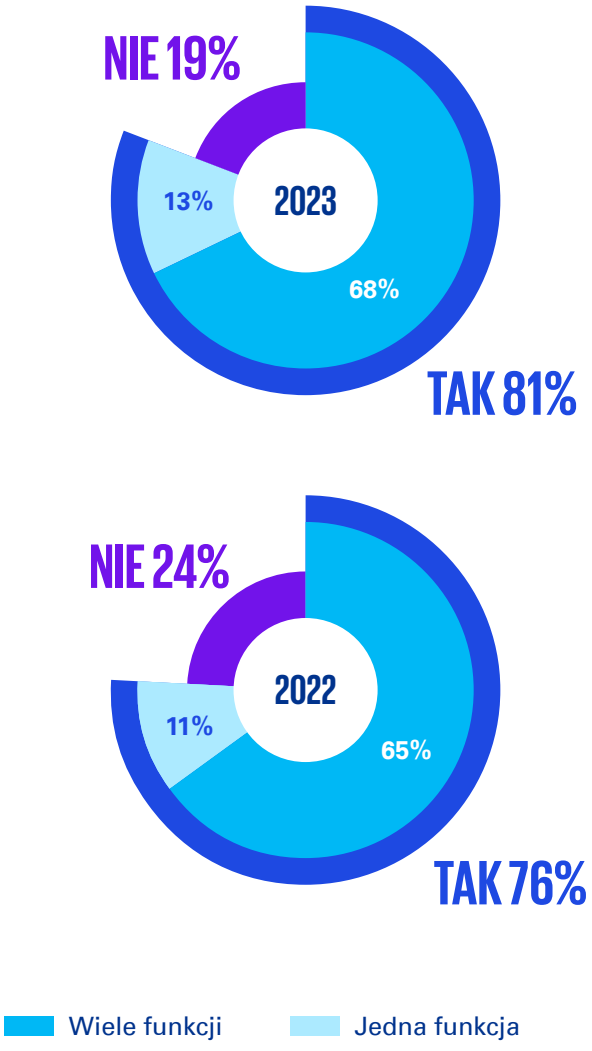


Outsourcing funkcji i procesów bezpieczeństwa

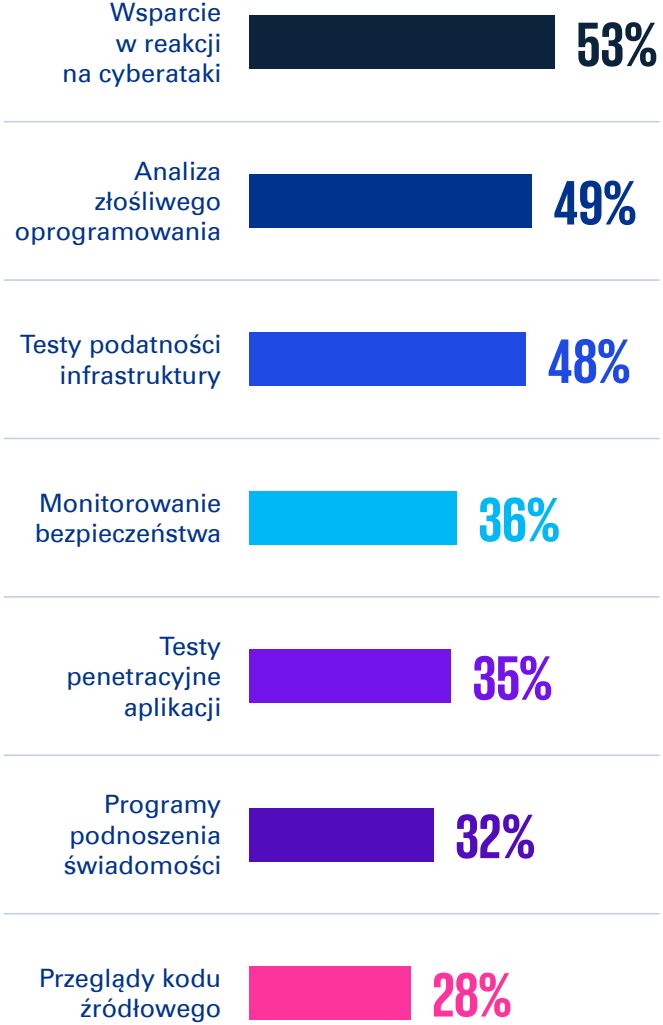
Zdecydowana większość badanych firm powierza kwestie bezpieczeństwa danych w organizacji zewnętrznym dostawcom. Na koniec 2022 roku z outsourcingu korzystało już 81% ankietowanych, a jak pokazują badania KPMG, odsetek ten rośnie z każdym kolejnym rokiem. Podobnie zwiększa się grupa firm, które realizują więcej niż jedną funkcję bezpieczeństwa w sieci za pośrednictwem zewnętrznych dostawców.

Wsparcie w reakcji na cyberataki, analiza złośliwego oprogramowania oraz testy podatności infrastruktury to trzy najczęściej outsourcowane procesy bezpieczeństwa. Z usług zewnętrznych firm do ich realizacji korzysta około połowa respondentów.

Korzystanie z outsourcingu



Funkcje lub procesy bezpieczeństwa realizowane przez zewnętrznych dostawców

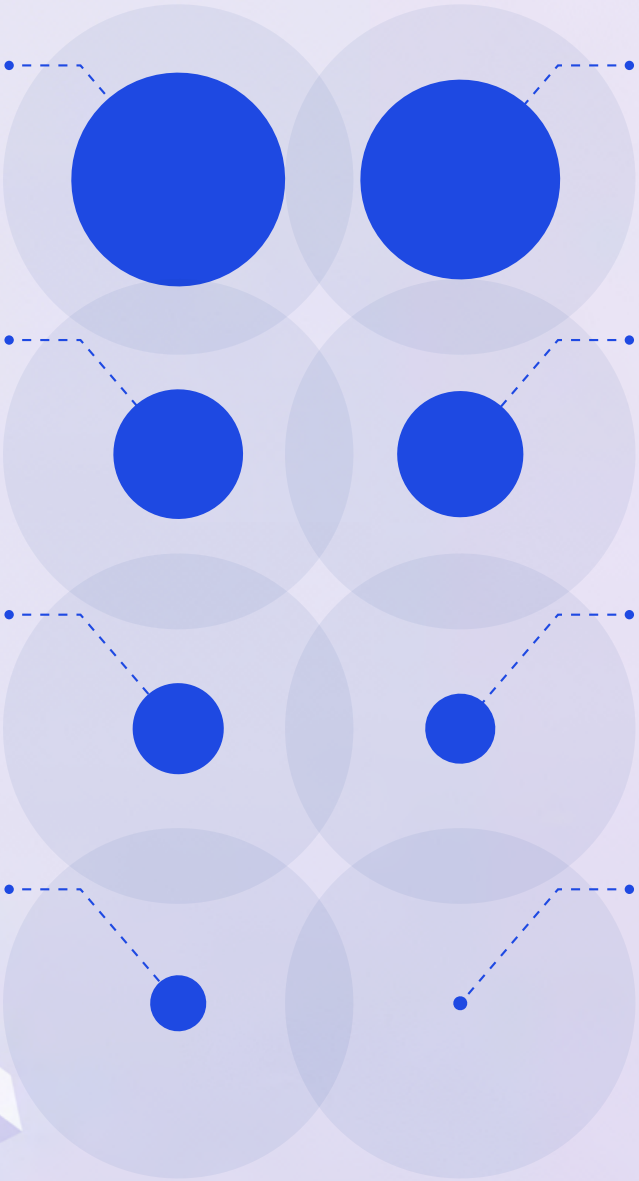


Monitorowanie bezpieczeństwa

Bieżące badanie zagrożeń cyberbezpieczeństwa może występować w różnej formie. Regularne monitorowanie bezpieczeństwa zostało już formalnie wpisane w obowiązki pracowników w 61% badanych organizacji, a w 36% powierzono je zewnętrznej firmie. Również 36% firm powołało w swoich strukturach komórkę *Security Operations Center* do monitorowania zagrożeń. W większości przypadków nie działa ona jednak całodobowo.

W ponad jednej trzeciej firm monitoruje się bezpieczeństwo kontrahentów (37%), a 26% prowadzi tzw. *Threat Hunting*, poszukując cyberprzestępców, którzy mogą być już w chronionej infrastrukturze. Jednak aż 57% respondentów przyznaje, że logi bezpieczeństwa nie są w ich organizacjach przeglądane regularnie.

Podejście organizacji do monitorowania bezpieczeństwa



61%
Regularne monitorowanie bezpieczeństwa zostało formalnie wpisane w obowiązki pracowników

57%
Logi bezpieczeństwa przeglądane są nieregularnie

37%
Monitorowane jest bezpieczeństwo dostawców i partnerów biznesowych

36%
Monitorowanie bezpieczeństwa zostało powierzone zewnętrznej firmie (*outsourcing*)

26%
Realizowane są proaktywne poszukiwania śladów cyberprzestępców w sieci (*Threat Hunting*)

20%
Powołany został zespół SOC (*Security Operations Center*) monitorujący bezpieczeństwo w trybie 8 godzin / 5 dni w tygodniu

16%
Powołany został zespół SOC (*Security Operations Center*) monitorujący bezpieczeństwo w trybie 24 godzin / 7 dni w tygodniu

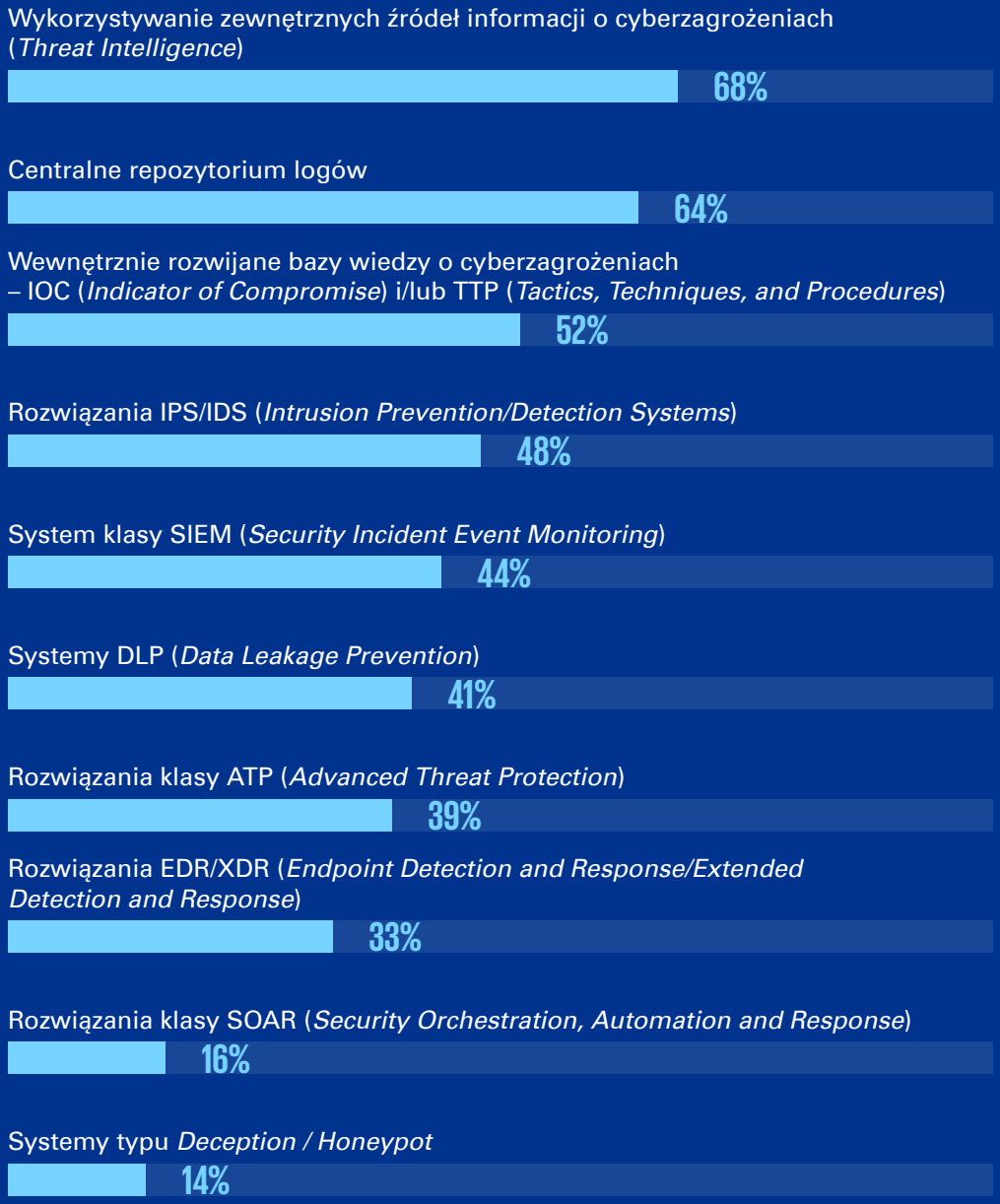
4%
Monitorowanie bezpieczeństwa nie jest w ogóle realizowane

Sposoby wykrywania ataków

W celu wykrycia cyberataków przedsiębiorstwa stosują szeroki wachlarz rozwiązań, wśród których najwięcej, bo aż dwie trzecie firm (68%) wykorzystuje zewnętrzne źródła informacji o zagrożeniach, czyli tzw. *Threat Intelligence*. Popularne są także centralne repozytoria logów (64%) oraz bazy wiedzy o zagrożeniach atakami typu IOC lub TTP (52%). Nie należy zapominać o rozwiązaniach IPS/IDS oraz systemach klasy SIEM stanowiących rozwiązania detekcji cyberataków w blisko połowie firm.

Najrzadziej spotykanym rozwiązaniem są systemy typu *Deception* stanowiące swego rodzaju pułapki zastawiane na cyberprzestępców (14%) oraz rozwiązania klasy SOAR (*Security Orchestration, Automation and Response*) usprawniające monitorowanie bezpieczeństwa i reakcję (16%).

Wdrożone rozwiązania w celu detekcji cyberataków



Reakcja na cyberataki

Podejście organizacji do cyberataków jest bardzo zróżnicowane. Blisko trzy czwarte respondentów przyznaje, że w ich przedsiębiorstwach zostały opracowane ogólnofirmowe procedury reagowania na wypadek ataku (73%). Chcąc zapobiegać cyberatakom organizacje w Polsce często decydują się na korzystanie ze wsparcia zewnętrznych firm. 42% spośród ankietowanych w badaniu KPMG przedsiębiorstw podpisało umowy z dostawcami usług w tym zakresie. O ile testy symulacyjne procedur reagowania są rzadko spotykane (13% wskazań), to już co trzecia badana organizacja korzysta z testów penetracyjnych typu *Red Teaming* do weryfikowania własnej skuteczności w obronie przed cyberatakami.

21% firm powołało wewnętrzny zespół do reagowania na incydenty – CSIRT (*Computer Security Incident Response Team*).

Podejście do reakcji na cyberataki

Opracowano ogólnofirmowe procedury reagowania / plany zarządzania kryzysowego na wypadek cyberataku

73%

Podpisano umowy ramowe z zewnętrznymi firmami na wypadek konieczności wsparcia przy ewentualnych cyberatakach

42%

Skuteczność operacyjna procedur detekcji i reakcji na cyberataki jest weryfikowana poprzez testy penetracyjne przy podejściu *Red Team*

33%

Wykupiona została polisa ubezpieczeniowa od skutków cyberataku

24%

Zorganizowany został wewnętrzny zespół CSIRT (*Computer Security Incident Response Team*)

21%

Procedury reakcji na cyberataki są testowane poprzez gry symulacyjne

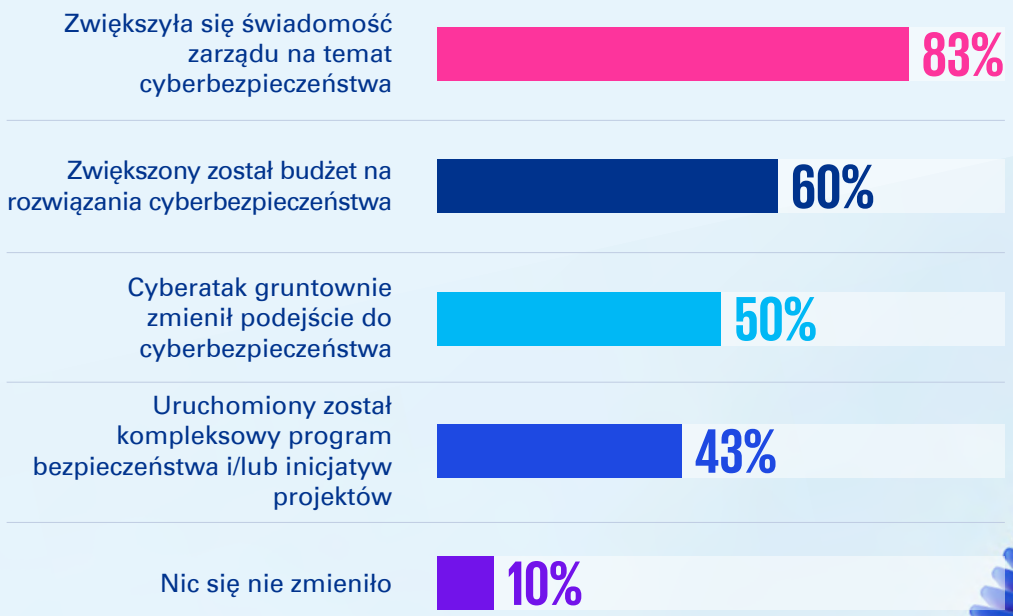
13%

Wnioski wynikające z doświadczenia cyberataku

Doświadczenie zetknięcia się z cyberatakiem w organizacji w znaczący sposób wpływa na działanie przedsiębiorstw w tym obszarze. Aż 83% respondentów deklaruje, że po takim incydencie zwiększyła się świadomość zarządu w temacie bezpieczeństwa, a w połowie firm gruntownie zmieniono podejście do cyberbezpieczeństwa. Doświadczenie incydentu sprawiło, że w 60% przedsiębiorstw zwiększono budżet na zabezpieczenia. Częściej dodatkowe nakłady są skłonne ponosić duże firmy (68% wskazań wśród organizacji zatrudniających przynamniej 250 osób). Kompleksowy program bezpieczeństwa wdrożono po zidentyfikowaniu cyberataku w 43% ogranizacji.

Dla 10% firm, w których incydent miał miejsce, nic się nie zmieniło w podejściu do kwestii związanych z bezpieczeństwem. Takie bagatelizowanie zagrożeń może niestety prowadzić do dużych strat zarówno finansowych, jak i wizerunkowych.

Zmiany, jakie zaszły w organizacji po zetknięciu z cyberatakiem*



*Próba obejmuje wyłącznie firmy, które doświadczyły w przeszłości przynajmniej jednego cyberataku

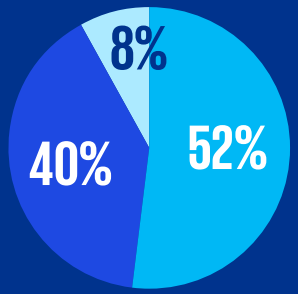
Piotr Smulikowski
Starszy Menadżer, Dział Doradztwa Biznesowego, Zespół Cyberbezpieczeństwa, KPMG w Polsce

Bezpieczeństwo w świecie cyfrowym wymaga proaktywnych działań, nieustannej edukacji oraz codziennych praktyk związanych z tzw. cyberhigieną. Nie chcąc ryzykować utraty danych czy naruszenia reputacji firmy powinniśmy się na to odpowiednio przygotować m.in. posiadać i regularnie testować scenariusze postępowania na wypadek ewentualnych cyberataków. Działania wyłącznie 'post factum' nie są w stanie zapewnić nam bezpieczeństwa, a straty związane ze skutkami ataków w konsekwencji mogą prowadzić do utraty zaufania klientów i ograniczenia zysków.

Informacje o badaniu

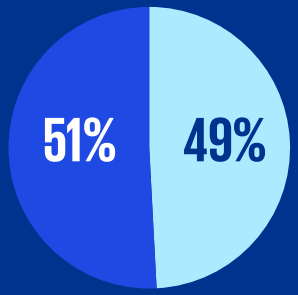
Badanie zostało zrealizowane metodą wywiadów telefonicznych CATI wśród osób odpowiedzialnych za bezpieczeństwo IT w firmach (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar). Badanie zostało zrealizowane na próbie 100 organizacji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

Liczba pracowników



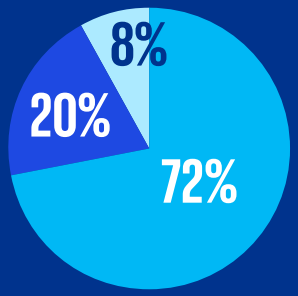
- duże (od 250 osób)
- średnie (50-249 osób)
- małe (max. 50 osób)

Przychody badanych firm



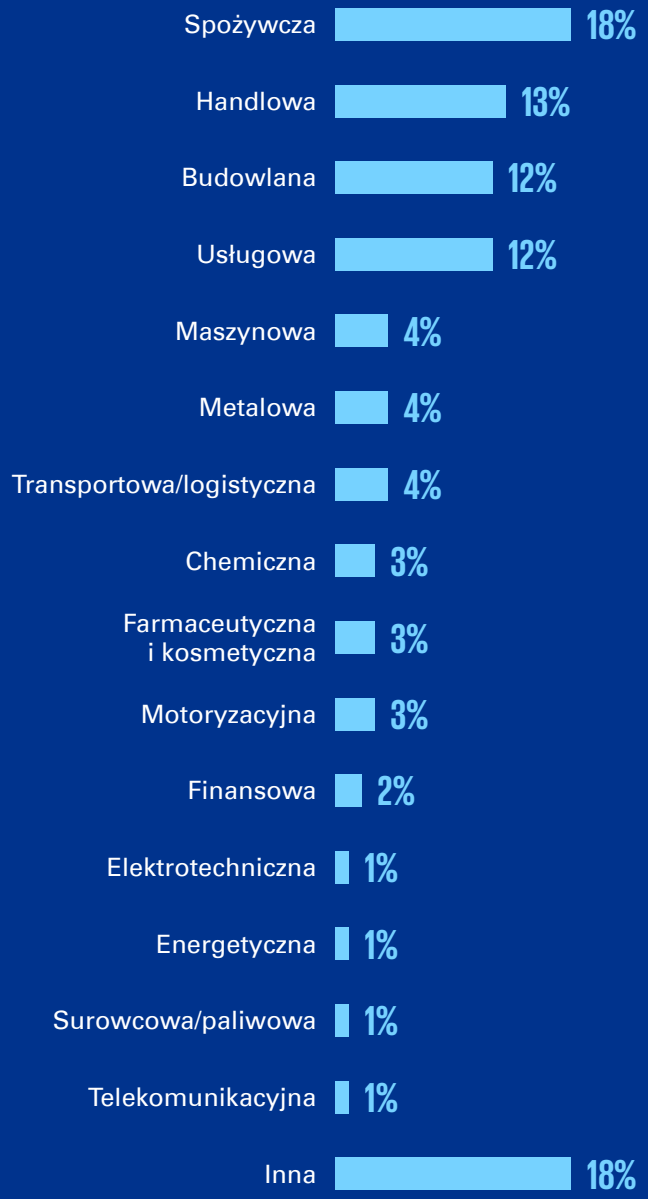
- powyżej 100 mln PLN
- od 51 do 100 mln PLN

Typ kapitału



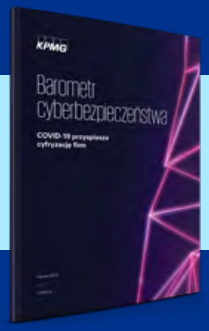
- polski
- zagraniczny
- trudno powiedzieć

Branża firmy

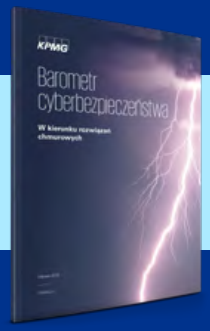


Wybrane publikacje KPMG w Polsce i na świecie

Barometr cyberbezpieczeństwa. Ochrona cyfrowej tożsamości (2022)



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



Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych (2020)

Bezpieczeństwo technologii mobilnych (2018)

Cyber considerations from the conflict in Ukraine (2022)

Cyber security considerations (2022)

KPMG Cyber trust insights (2022)

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
Dyrektor

Dział Doradztwa Biznesowego,
Zespół Cyberbezpieczeństwa,
KPMG w Polsce

E: lstaniak@kpmg.pl

Piotr Smulikowski
Starszy Menadżer

Dział Doradztwa Biznesowego,
Zespół Cyberbezpieczeństwa,
KPMG w Polsce

E: piotrsmulikowski@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