KPMG

Barometr cyberbezpieczeństwa

W kierunku rozwiązań chmurowych

Czerwiec 2020

KPMG.pl

Wstęp

Szanowni Państwo,

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

Tegoroczna edycja badania skupia się na analizie podejścia polskich przedsiębiorstw do przetwarzania w chmurze i jej implikacji dla bezpieczeństwa informacji. Badanie pokazuje, że ponad połowa firm nie korzysta aktualnie z chmury, choć 17% w najbliższym czasie planuje przenieść do niej część usług. Wydaje się, że przyczyną tej sytuacji jest wciąż niska wiedza na temat usług chmurowych – m.in. aż 62% organizacji nie potrafiła określić z jakiego typu chmury korzysta. Niska świadomość może być również przyczyną zaskakującej percepcji uczestników badania, że przetwarzanie danych w chmurze nie jest bardziej bezpieczne, niż wykorzystywanie do tego celu wyłącznie wewnętrznej infrastruktury. Choć z drugiej strony 43% firm jest zdania, że chmura publiczna pozwala na znaczące podniesienie poziomu bezpieczeństwa przetwarzanych danych. Natomiast jedynie 8% polskich przedsiębiorstw dostrzega dość powszechny problem, że działy biznesowe dokonują zakupów usług chmurowych z pominięciem działu IT i bez analizy ryzyka (tzw. zjawisko Shadow IT).

Obecna sytuacja zagrożenia epidemiologicznego oraz związane z nią upowszechnienie pracy zdalnej z pewnością zmienią tę percepcję. W najbliższej przyszłości można spodziewać się zwiększonego zainteresowania rozwiązaniami chmurowymi w polskich przedsiębiorstwach. Tym bardziej, że wiodący dostawcy infrastruktury chmurowej rozpoczęli pracę nad zbudowaniem regionalnych centrów przetwarzania danych zlokalizowanych w Polsce.

Choć odsetek polskich przedsiębiorstw dotkniętych cyberatakami zmniejszył się w porównaniu z poprzednimi latami, skutków cyberprzestępczości doświadczyła w 2019 roku większość polskich firm (54%). Co więcej, w minionym roku wzrost lub znaczący wzrost liczby prób cyberataków zanotowało 21% firm w Polsce, natomiast ich spadek odnotowało tylko 5% przedsiębiorców.

Polskie przedsiębiorstwa nadal najbardziej obawiają się zorganizowanej cyberprzestępczości. W szczególności trudnych do zidentyfikowania i odparcia ataków ukierunkowanych, cyberprzestępstw realizowanych za pośrednictwem złośliwego oprogramowania oraz wspieranych przez socjotechnikę. Firmy obawiają się również kradzieży danych przez ich pracowników, którzy pozostają istotnym, ale nie największym źródłem zagrożeń.

Ciekawym wynikiem badania jest wysoki optymizm polskich przedsiębiorstw w kwestii oceny dojrzałości wdrożonych zabezpieczeń. Z perspektywy doświadczeń KPMG z realizowanych audytów bezpieczeństwa, wydaje się, że tak wysoka samoocena, może niestety po części wynikać z wciąż niedostatecznej świadomości polskich firm w zakresie skali i złożoności dzisiejszych cyberzagrożeń.

W tym roku na znaczeniu stracił czynnik ludzki – mniej niż połowa przedsiębiorstw wskazuje, że ma trudność w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. Być może jest to związane z rosnącą skalą outsourcingu funkcji i procesów bezpieczeństwa, z którego korzysta obecnie 76% firm.

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
Szef zespołu ds. cyberbezpieczeństwa
KPMG w Polsce

Najważniejsze wnioski

43% firm w Polsce korzystało z rozwiązań chmurowych przed wybuchem pandemii COVID-19, z czego 5% tylko i wyłącznie z usług chmurowych. Najczęściej organizacje korzystają z witryn internetowych oraz poczty elektronicznej, które zlokalizowane są w chmurze.

Większość (62%) polskich firm nie wie w jakim modelu korzysta z chmury. Przeważa również pogląd, że wykorzystanie chmury nie przynosi korzyści z perspektywy bezpieczeństwa. Może to świadczyć o istotnej potrzebie edukacji polskich firm w tym zakresie.

Organizacje nie dostrzegają problemu tzw. shadow IT. Jedynie 8% przyznało, że biznes zamawia usługi chmurowe z pominięciem działów IT i bezpieczeństwa.

Główną **korzyść z zakresu bezpieczeństwa** w wykorzystaniu chmury polskie przedsiębiorstwa (6 na 10 firm) widzą w zapewnieniu **ciągłości procesów biznesowych**, które są kluczowym aspektem pozwalającym firmom minimalizować negatywne skutki przestoju spowodowanego pandemią COVID-19.

Maleje skala cyberataków wśród firm prowadzących działalność w Polsce. W 2019 roku przynamniej jeden cyberincydent odnotowało **54% organizacji**. Oznacza to **spadek o 14 p.p.** w stosunku do poprzedniej edycji badania.

Brak wystarczającego budżetu na zabezpieczenia jest największym ograniczeniem wskazywanym przez 64% firm w osiągnięciu oczekiwanego poziomu bezpieczeństwa. W bieżącym roku na znaczeniu stracił czynnik ludzki – mniej niż połowa przedsiębiorstw wskazuje, że ma trudność w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników.

Wzrost liczby cyberataków w 2019 roku zauważyła co piąta firma, ich spadek zaledwie 5% organizacji.

72% firm najbardziej obawia się pojedynczych hakerów. Na kolejnych miejscach znaleźli się niezadowoleni lub podkupieni pracownicy na których wskazało 58% organizacji oraz cyberterroryści i zorganizowane grupy cyberprzestępcze, których obawia się 43% respondentów.

76% firm korzysta z outsourcingu funkcji i procesów bezpieczeństwa u zewnętrznych dostawców. Wśród nich, 6 na 10 organizacji outsourcuje więcej niż jedną funkcję lub proces bezpieczeństwa. Najczęściej zlecana na zewnątrz jest usługa analizy złośliwego oprogramowania.

Za bezpieczeństwo informacji w przedsiębiorstwach bez zmian najczęściej odpowiedzialny jest **pracownik działu IT** (dyrektor lub dedykowany pracownik).

Największym ryzykiem dla firm są wycieki danych za pośrednictwem **złośliwego oprogramowania, phishing** – czyli wyłudzanie danych uwierzytelniających oraz ogólne kampanie ransomware.

Przedsiębiorstwa **najlepiej oceniają swoją ochronę przed złośliwym oprogramowaniem** oraz zabezpieczenia styku z siecią Internet. W dużym stopniu osiągnęły dojrzałość w kwestii bezpieczeństwa w procesach wytwarzania oprogramowania i sieci wewnętrznej oraz kwestii planowania zapewnienia ciągłości działania.

Korzystanie z technologii chmurowych przez firmy w Polsce

Ponad połowa badanych firm nie korzystała z chmury na początku 2020 roku przed wybuchem pandemii COVID-19. 17% ankietowanych firm zadeklarowało chęć przeniesienia do chmury części swoich usług. W związku z aktualną sytuacją należy się spodziewać, że odsetek firm, które zdecydowały się na ten krok może być zdecydowanie większy. Warto zwrócić uwagę na potencjalnie trudne położenie w jakim znalazło się 40% ankietowanych przedsiębiorstw, które zadeklarowały, że nie planowały przeniesienia usług do chmury. Wśród organizacji, które korzystają z rozwiązań chmurowych, większość przyznała, że przetwarza dane dwutorowo, działając również w lokalnym centrum przetwarzania danych.

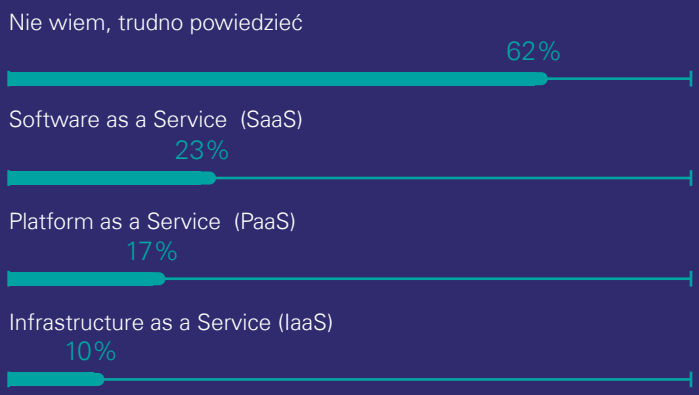
Aktualnie nie wykorzystujemy chmury 57%

Korzystamy z usług chmurowych 43%

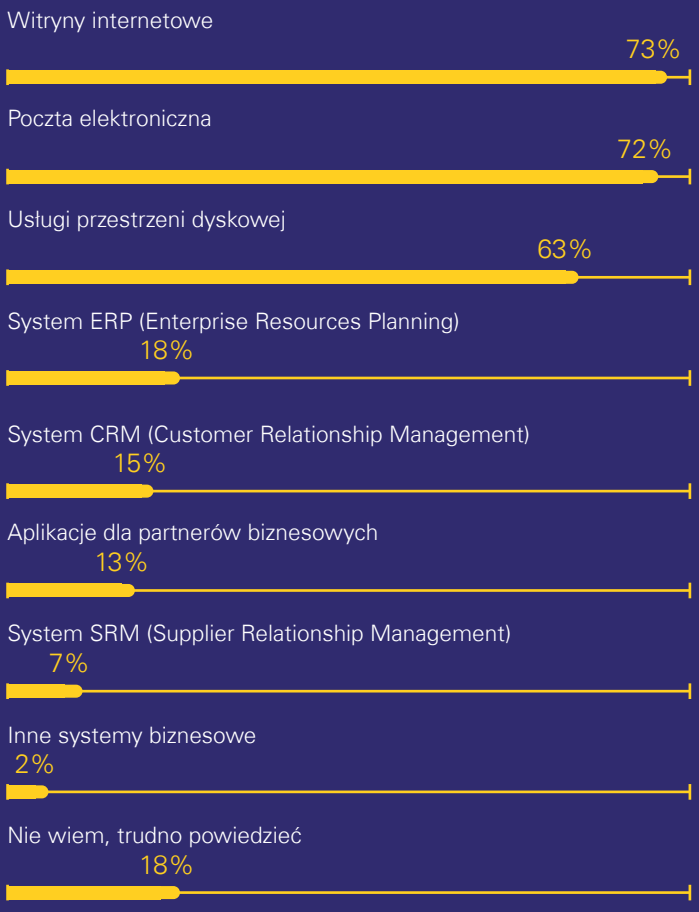
Wykorzystywane przez firmy usługi chmurowe

Wśród firm, które posiadają rozwiązania chmurowe, aż 62% ich przedstawicieli nie jest w stanie określić typu wykorzystywanej infrastruktury. Może to świadczyć o wciąż niewystarczającej wiedzy w polskich firmach na temat rozwiązań chmurowych. Najpopularniejszym modelem jest Software as a Service (SaaS), z którego korzysta 23% respondentów. Zdecydowanie lepszą znajomość respondenci wykazują w przypadku typów usług, z których korzystają w chmurze. Najczęściej są to witryny internetowe i poczta elektroniczna z których korzysta ponad 70% organizacji.

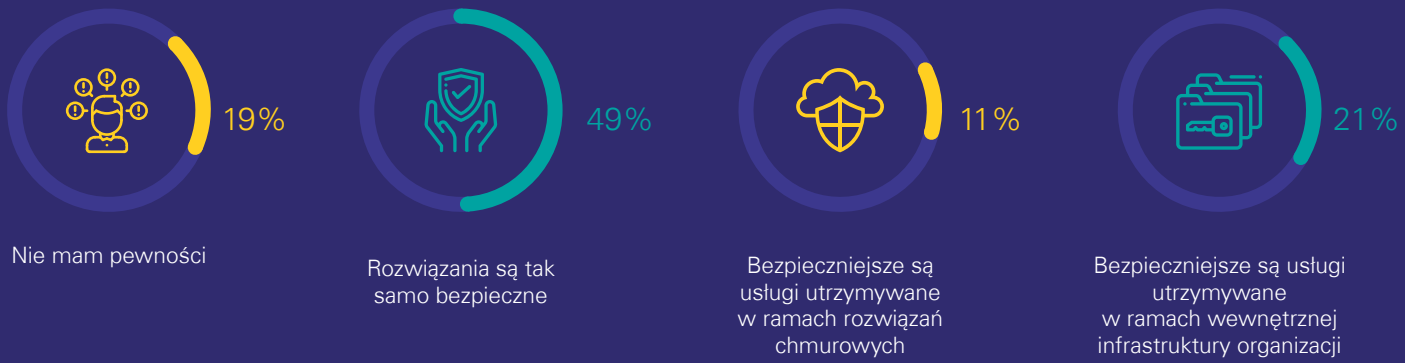
Wykorzystywana infrastruktura chmurowa



Wykorzystywane usługi



Opinie o bezpieczeństwie usług



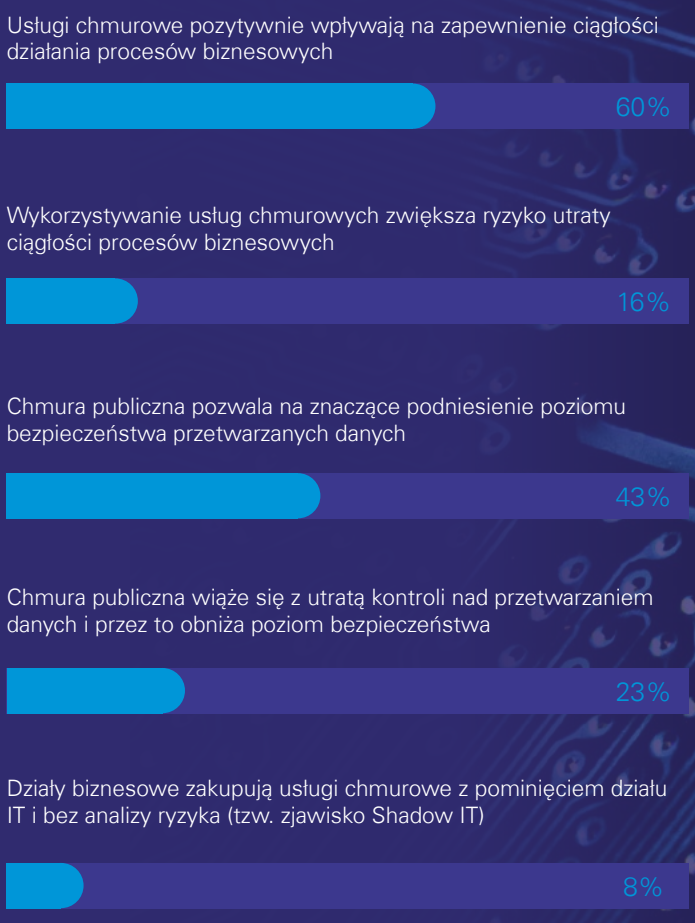
Zaskakujące jest, że wśród uczestników badania przeważa pogląd, że przeniesienie danych do chmury nie zwiększy poziomu ich bezpieczeństwa. Można również interpretować ten wynik jako wskaźnik potrzeby edukacji polskich przedsiębiorstw w zakresie korzyści płynących z wykorzystania chmury.

Połowa organizacji niezależnie od tego, czy już korzystają czy dopiero planują, w dużej mierze uważa rozwiązania chmurowe za porównywalnie bezpieczne z rozwiązaniami opartymi na wewnętrznej infrastrukturze.

Opinie o usługach chmurowych

Niemal 2/3 firm jest przekonanych o pozytywnym wpływie usług chmurowych na zapewnienie ciągłości działania procesów biznesowych w organizacji. Dodatkowo blisko połowa uważa, że dzięki chmurze publicznej podnosi się bezpieczeństwo przetwarzania danych. Przeciwnego zdania, które wyraża się przekonaniem, że korzystanie z chmury publicznej obniża bezpieczeństwo poprzez utratę kontroli nad przetwarzanymi danymi jest 23% firm biorących udział w badaniu. Jednocześnie 16% organizacji uważa, że korzystanie z chmury może zwiększać ryzyko utraty ciągłości procesów biznesowych.

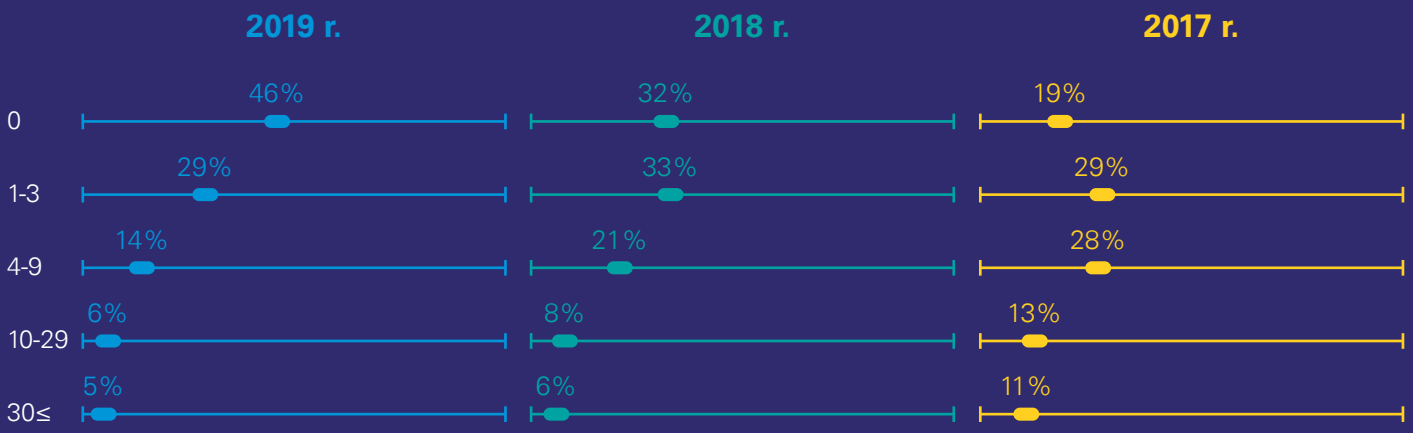
Opinia o usługach chmurowych



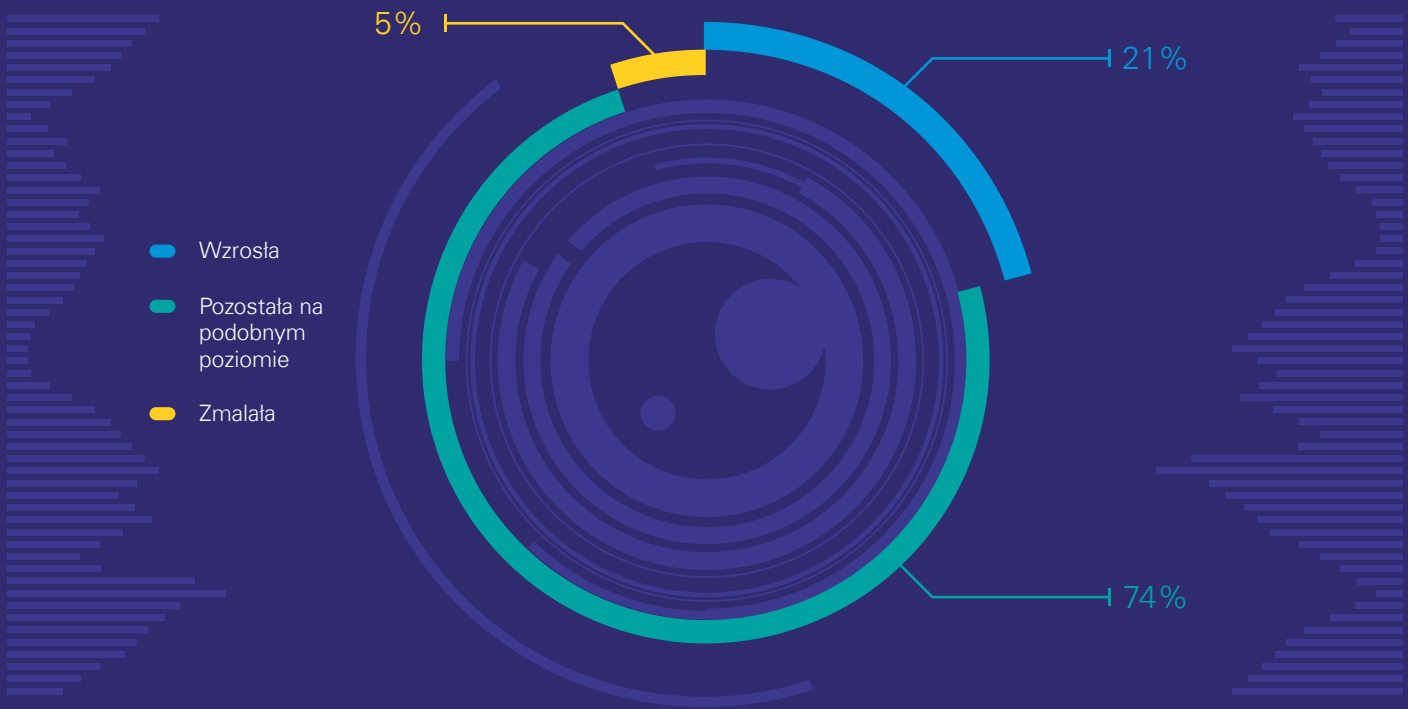
Dynamika cyberataków na firmy działające w Polsce

Niemal połowa badanych firm w 2019 roku nie zarejestrowała żadnych incydentów związanych z naruszeniem bezpieczeństwa. Z odpowiedzi ankietowanych organizacji wynika, że poprzedni rok był najbezpieczniejszy od 3 lat. W 2019 roku wzrost liczby prób cyberataków zauważyło natomiast 21% przedsiębiorców, ich spadek z kolei zadeklarowało 5% respondentów. Ponad 7 na 10 organizacji uważa, że liczba zaobserwowanych prób cyberataków pozostała na niezmienionym poziomie w stosunku do 2018 roku. Warto zaznaczyć, że największe firmy, zatrudniające powyżej 250 pracowników częściej od pozostałych deklarują wzrost zaobserwowanych prób cyberataków.

Liczba zarejestrowanych incydentów bezpieczeństwa przez firmy:



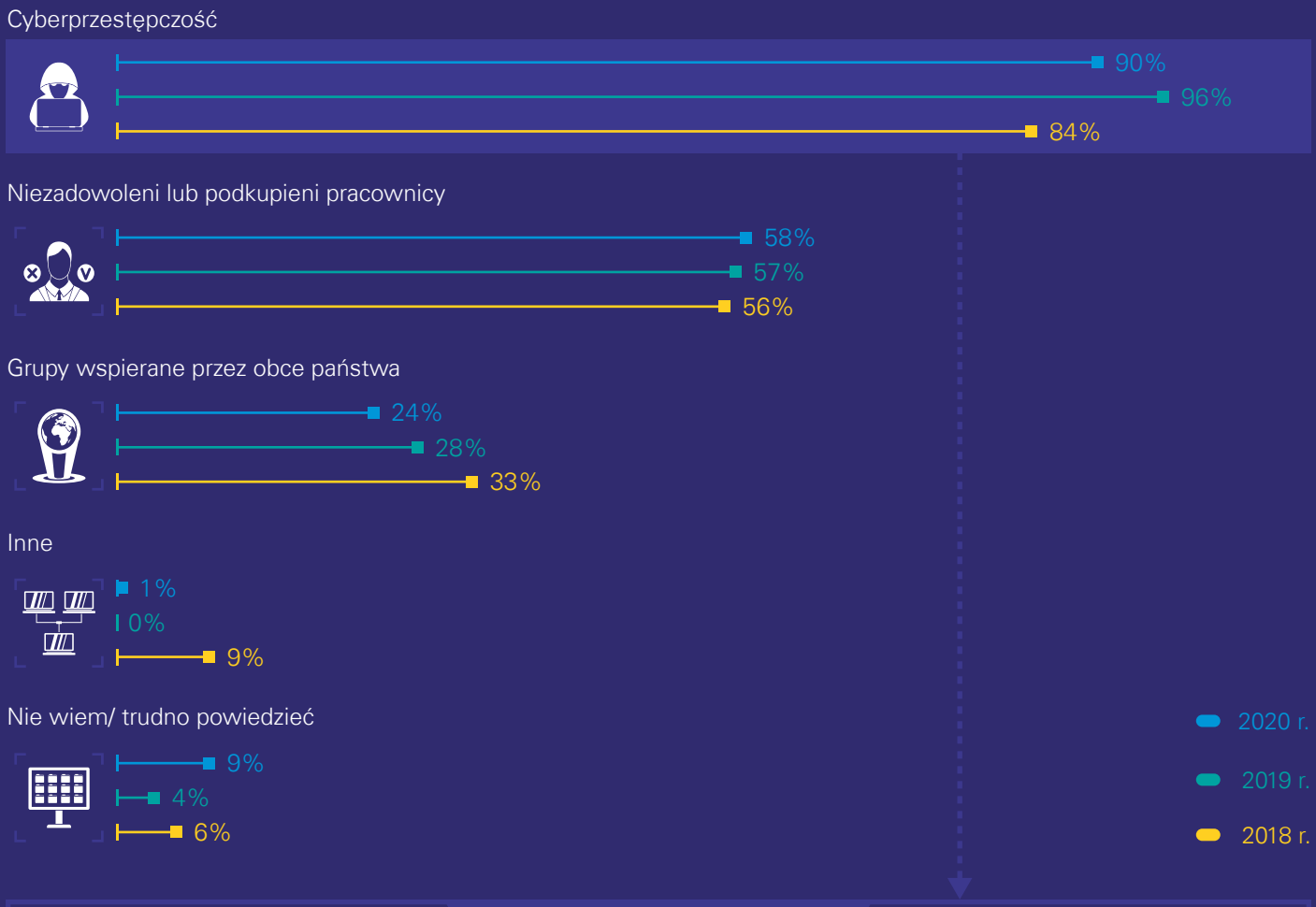
W ciągu ostatniego roku liczba zaobserwowanych prób cyberataków w porównaniu z poprzednim rokiem

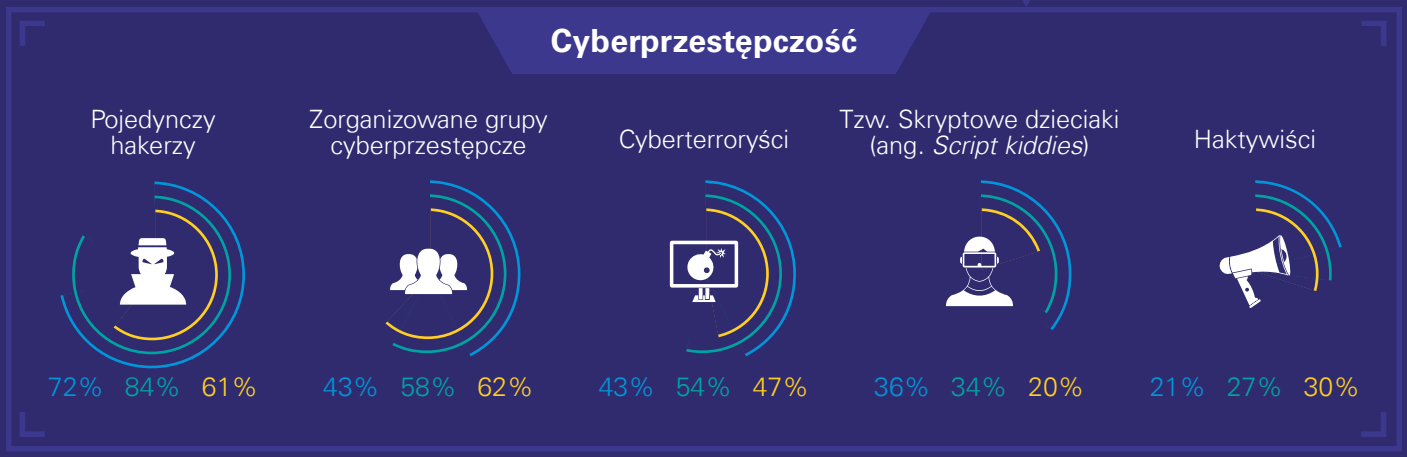


Źródła cyberzagrożeń

Szeroko rozumiana cyberprzestępczość od lat jest największym zagrożeniem dla organizacji. 72% firm uważa, że najgroźniejsi są pojedynczy hakerzy. Oznacza to spadek o 12 p.p. w stosunku do poprzedniej edycji badania. Z roku na rok można zaobserwować rosnące zagrożenie, które organizacje dostrzegają w niezadowolonych lub podkupionych pracownikach. Blisko połowa firm obawia się również zorganizowanych grup cyberprzestępczych oraz cyberterrostów. Warto również zauważyć, że w tym roku blisko co dziesiąta osoba miała trudności ze wskazaniem grup, które stanowią realne zagrożenie dla firmy.

Grupy stanowiące realne zagrożenie dla organizacji:

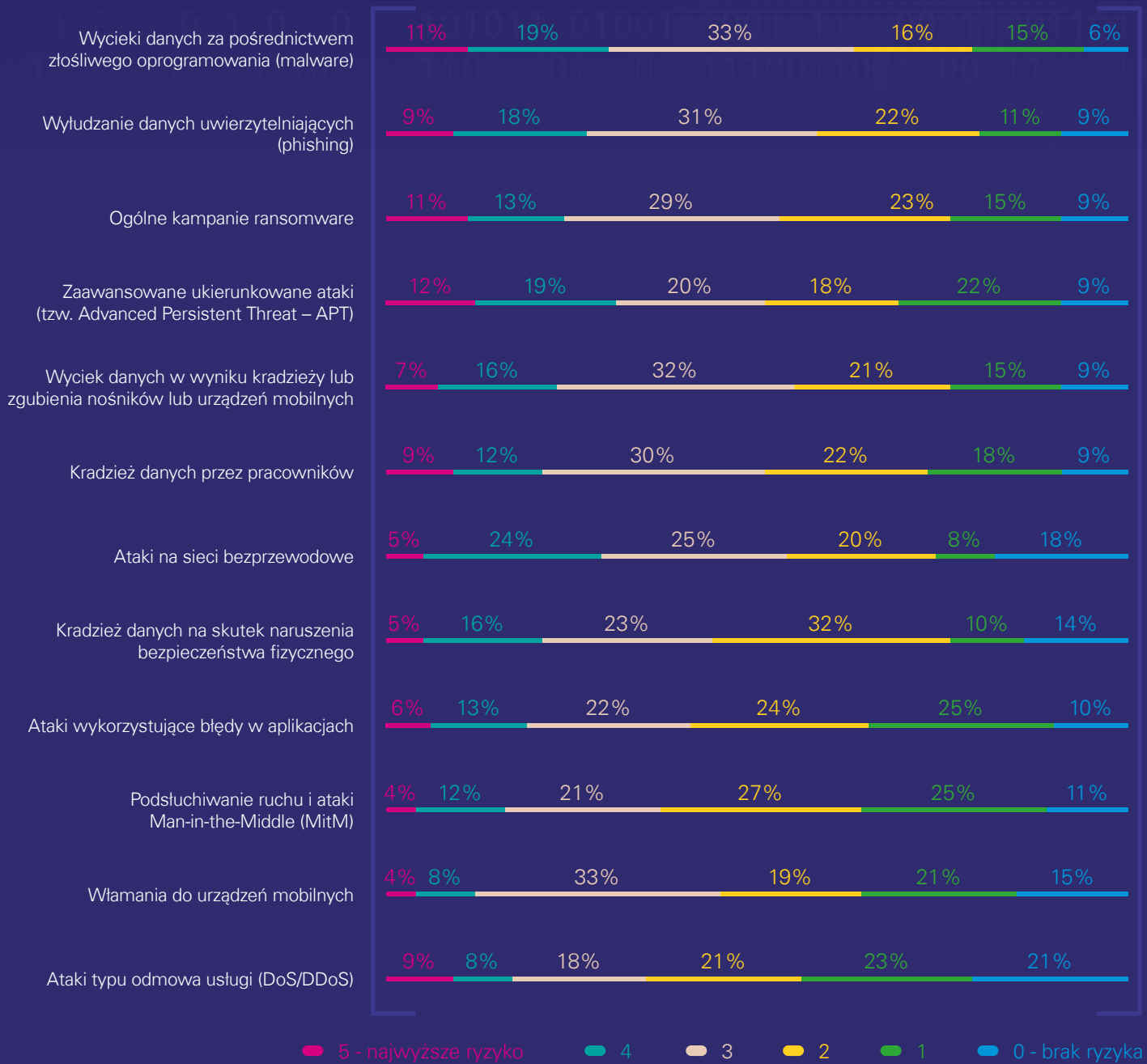




Największe cyberzagrożenia

Zdaniem ankietowanych przedsiębiorstw największe ryzyko stanowią dla nich wycieki danych za pośrednictwem złośliwego oprogramowania (malware), phishing – czyli wyłudzanie danych uwierzytelniających oraz ogólne kampanie ransomware. Kradzież danych przez pracowników lub ataki na sieci bezprzewodowe są postrzegane przez firmy jako obarczone średnim ryzykiem. Organizacje z kolei najmniej obawiają się włamań do urządzeń mobilnych oraz ataków typu odmowa usługi (DoS/DDoS).

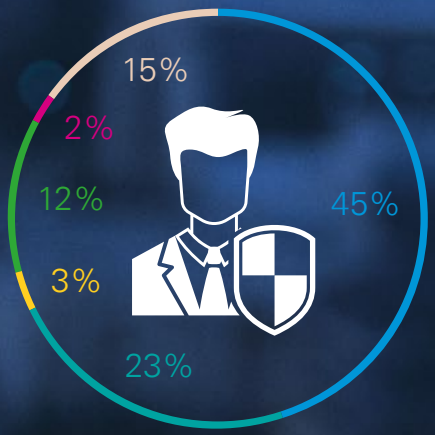
Które z poniższych cyberzagrożeń stanowią największe ryzyko dla organizacji?



Przypisanie odpowiedzialności za bezpieczeństwo informacji

Firmy w Polsce w dalszym ciągu mają wiele do zrobienia w kwestii organizacji zarządzania bezpieczeństwem. W zaledwie 3% firm za obszar bezpieczeństwa odpowiada dedykowana do tego celu jednostka organizacyjna. W blisko połowie organizacji za bezpieczeństwo informacji odpowiedzialny jest pracownik działu IT – dyrektor lub dedykowany pracownik. Natomiast w niemal co czwartej firmie bezpieczeństwem zajmuje się prezes zarządu.

Osoby odpowiedzialne w organizacji za bezpieczeństwo informacji

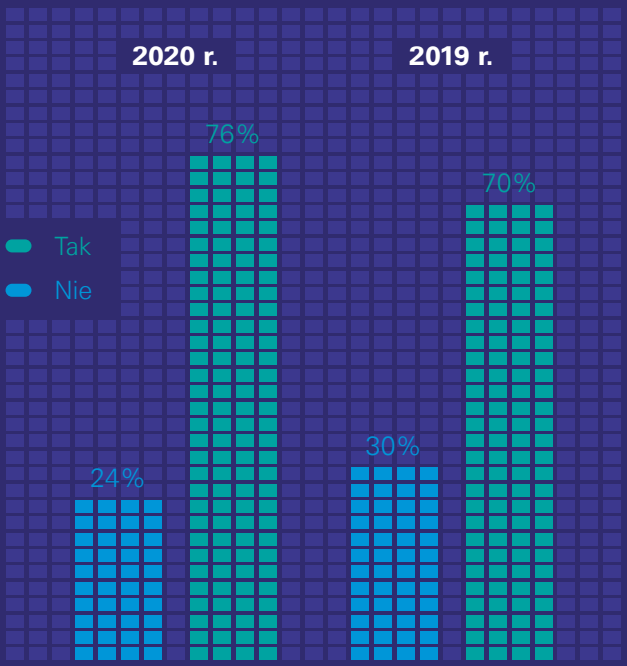


- Dyrektor IT (CIO) lub dedykowany pracownik w strukturach IT
- Prezes zarządu (CEO)
- Niezależna dedykowana funkcja (CSO/CISO)
- Inne stanowisko w organizacji niż powyższe
- Odpowiedzialność przypisana w strukturach globalnych poza Polską
- Brak formalnego przypisania odpowiedzialności

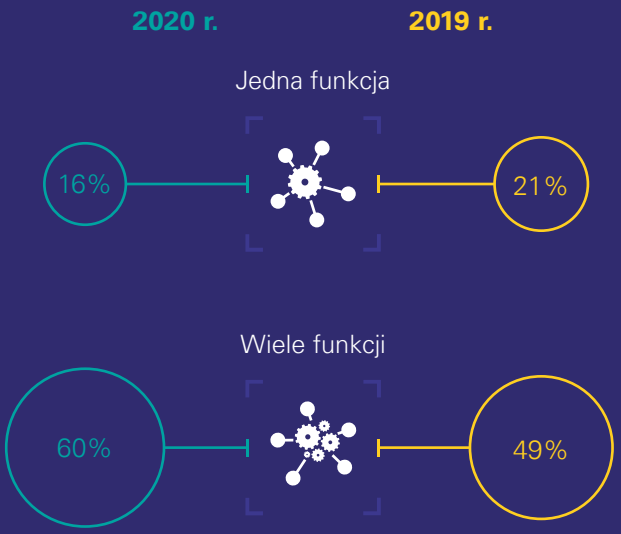
Outsourcing funkcji i procesów bezpieczeństwa

Blisko 8 na 10 firm biorących udział w badaniu zleca kwestie bezpieczeństwa informacji zewnętrznym dostawcom, z czego 60% powierza zewnętrznej firmie więcej niż jedną funkcję lub proces bezpieczeństwa. Najczęściej firmy zewnętrzne zajmują się analizą złośliwego oprogramowania, monitorowaniem bezpieczeństwa i wsparciem w reakcji na cyberataki.

Korzystanie z outsourcingu



Liczba funkcji lub procesów bezpieczeństwa w organizacji realizowana przez dostawców

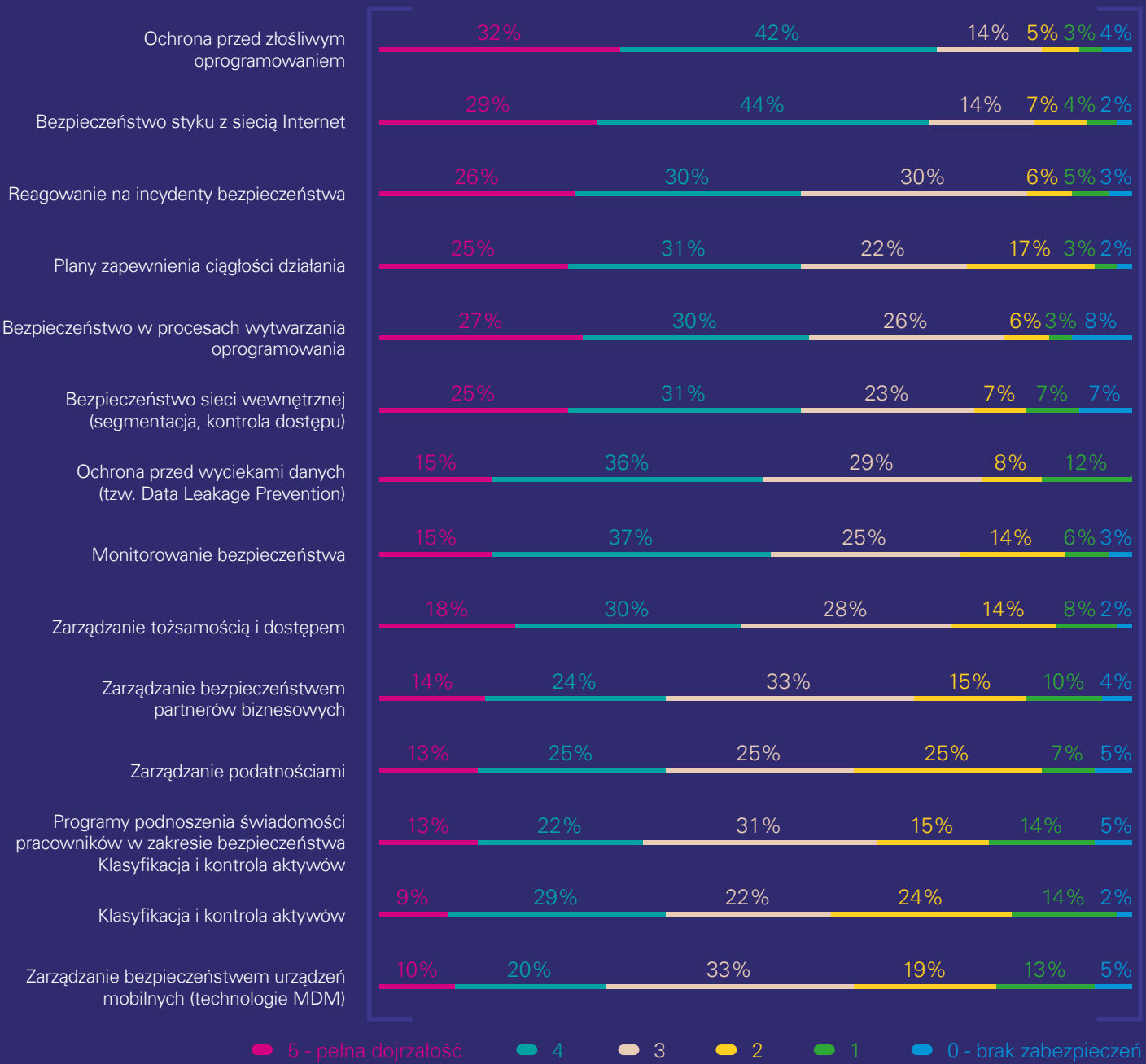


Funkcje/ procesy bezpieczeństwa realizowane przez zewnętrznych dostawców

Dojrzałość obszarów zabezpieczeń w firmach w Polsce

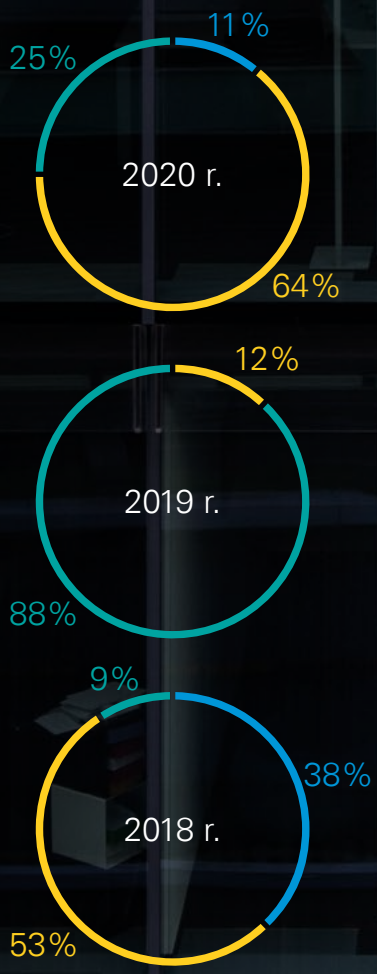
Podobnie jak w poprzedniej edycji badania przedsiębiorstwa najlepiej oceniają swoją ochronę przed złośliwym oprogramowaniem oraz zabezpieczenia styku z siecią internetową. Dodatkowo deklarują, że w dużym stopniu osiągnęły dojrzałość w kwestii reagowania na incydenty bezpieczeństwa oraz planowania zapewnienia ciągłości działania. W najmniejszym stopniu zabezpieczone są działania związane z zarządzeniem bezpieczeństwem urządzeń mobilnych. Firmy o przychodach powyżej 100 mln zł deklarują większą dojrzałość takich procesów, jak: ochrona przed wyciekiem danych, zarządzania bezpieczeństwem partnerów i urządzeń, a także klasyfikacji i kontroli aktywów.

Jak firmy oceniają dojrzałość poszczególnych obszarów zabezpieczeń w swoich organizacjach?



Firmy zdecydowanie lepiej oceniają dojrzałość obszarów swoich zabezpieczeń w porównaniu do ubiegłorocznej edycji badania. 64% respondentów deklaruje dojrzałość zabezpieczeń na poziomie dostatecznym w większości analizowanych obszarów, natomiast 11% w każdym z analizowanych obszarów. W ubiegłorocznej edycji badania blisko 9 na 10 firm zadeklarowało dostateczną dojrzałość obszarów zabezpieczeń najwyżej w połowie analizowanych obszarów.

Odsetek firm deklarujących przynajmniej dostateczną dojrzałość obszarów zabezpieczeń

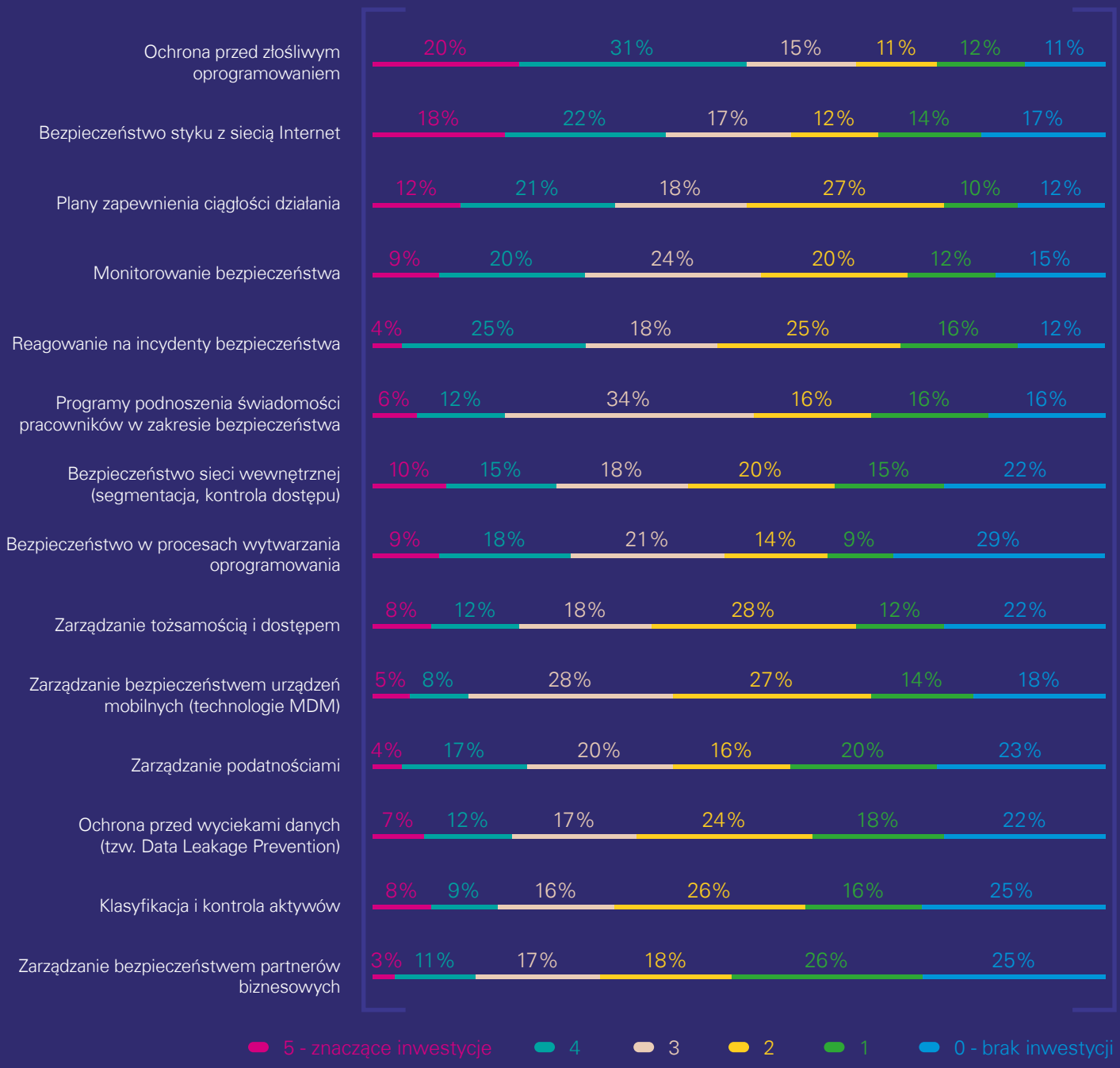


Na wykresie zaprezentowano odsetek firm deklarujących dojrzałość obszarów zabezpieczeń na poziomie 3-5 w skali 0-5.

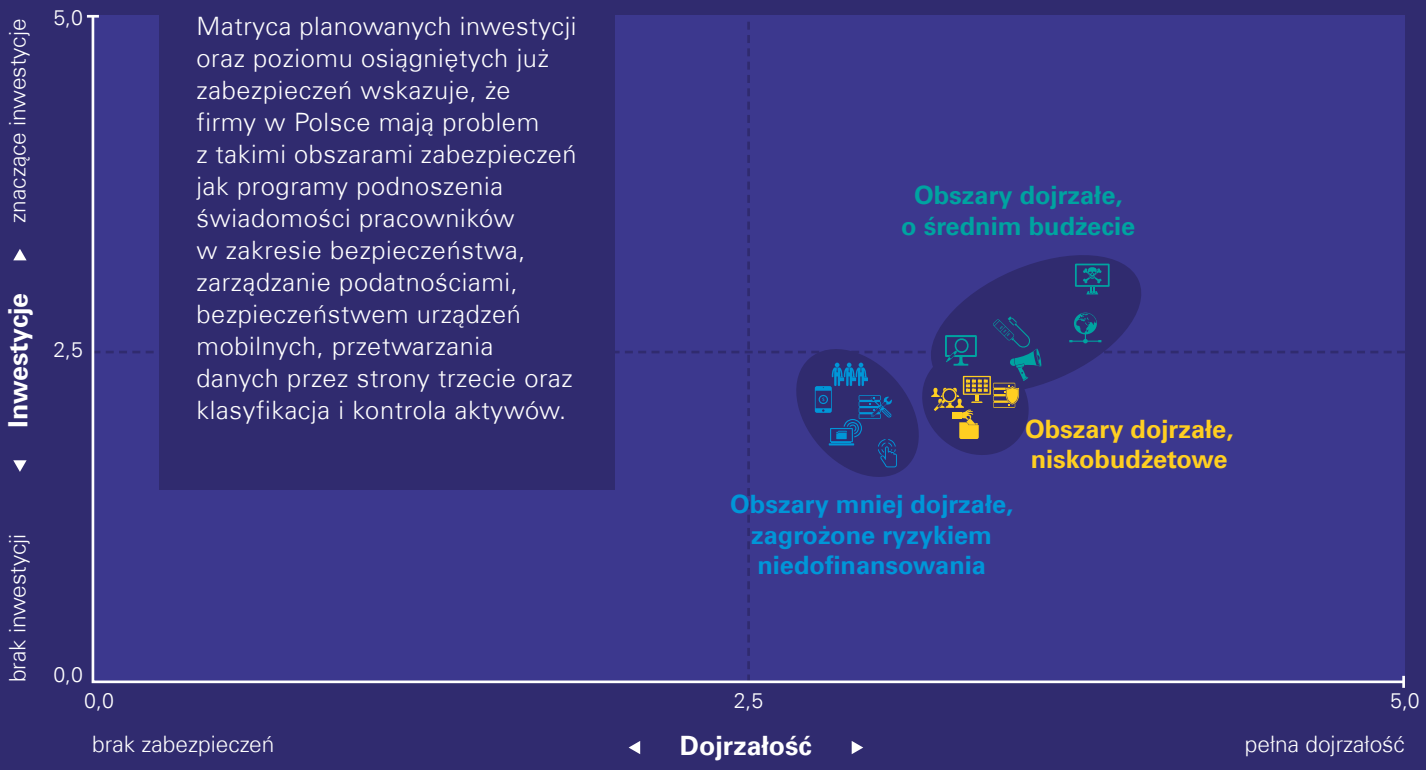
Planowane inwestycje w zabezpieczenia

Ochrona danych przed złośliwym oprogramowaniem, ochrona danych na styku z siecią internetową oraz zaplanowanie zapewnienia ciągłości działania oraz monitorowanie bezpieczeństwa są priorytetowymi inwestycjami planowanymi w przedsiębiorstwach w najbliższym czasie. Firmy o przychodzie do 100 mln zł częściej planują inwestycje przeciwdziałające złośliwemu oprogramowaniu, zapewnieniu bezpieczeństwa na styku z internetem oraz reagowaniu na incydenty bezpieczeństwa.

W jakie obszary zabezpieczeń planują inwestować firmy?



Obszary zabezpieczeń - obecna dojrzałość a planowane inwestycje



Obszary dojrzałe, o średnim budżecie

- Ochrona przed złośliwym oprogramowaniem
- Bezpieczeństwo styku z siecią Internet
- Plany zapewnienia ciągłości działania
- Monitorowanie bezpieczeństwa
- Reagowanie na incydenty bezpieczeństwa

Obszary dojrzałe, niskobudżetowe

- Bezpieczeństwo w procesach wytwarzania oprogramowania
- Bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu)
- Zarządzanie tożsamością i dostępem
- Ochrona przed wyciekami danych (tzw. Data Leakage Prevention)

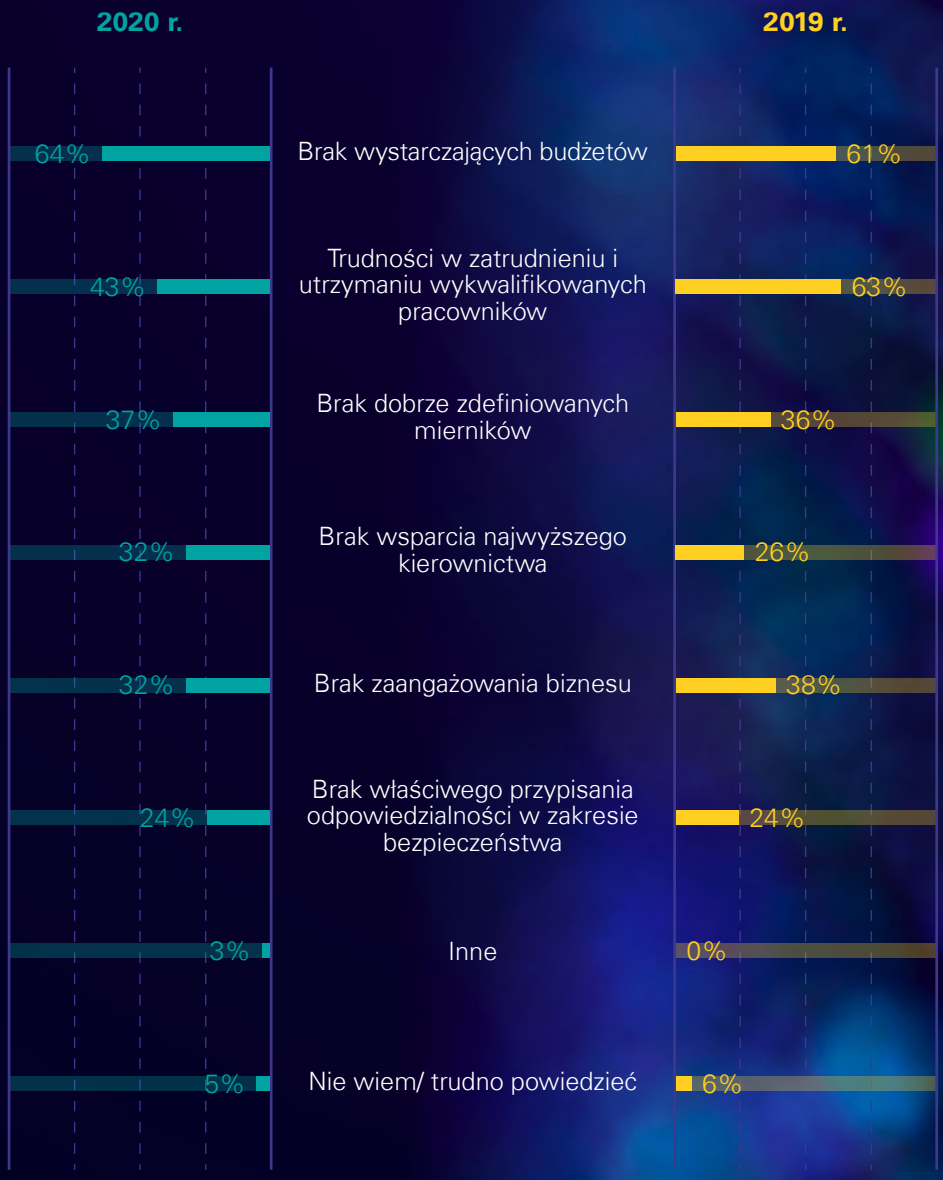
Obszary mniej dojrzałe, zagrożone ryzykiem niedofinansowania

- Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa
- Klasyfikacja i kontrola aktywów
- Zarządzanie bezpieczeństwem partnerów biznesowych
- Zarządzanie bezpieczeństwem urządzeń mobilnych (MDM)
- Zarządzanie podatnościami

Ograniczenia w budowaniu cyberbezpieczeństwa w firmach

Brak wystarczającego budżetu jest największym ograniczeniem dla 64% firm w osiągnięciu oczekiwanego poziomu bezpieczeństwa. W tym roku na znaczeniu stracił czynnik ludzki – mniej niż połowa przedsiębiorstw wskazuje, że ma trudność w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. Brak dobrze określonych mierników bezpieczeństwa informacji lub brak zaangażowania kierownictwa czy przypisania odpowiedzialności w zakresie bezpieczeństwa zdają się być mniejszymi barierami.

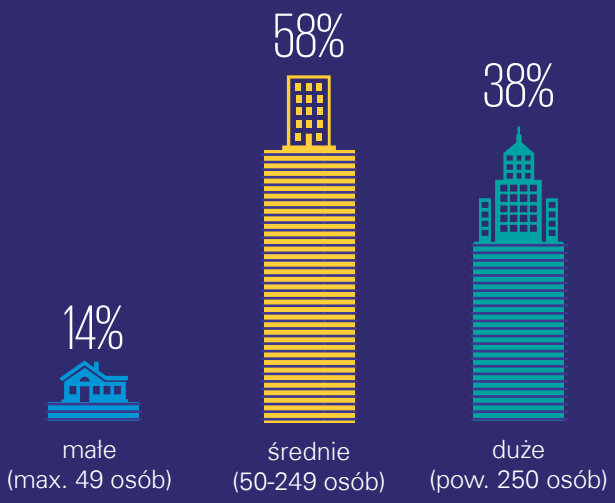
Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji



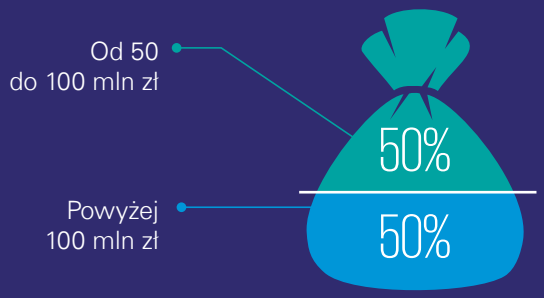
Informacje o badaniu

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 przeprowadzono na próbie 100 organizacji w styczniu 2020 roku przez firmę Norstat Polska.

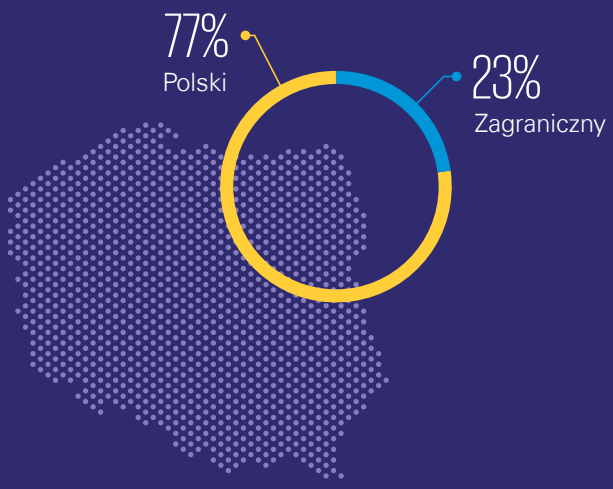
Wielkość Firmy



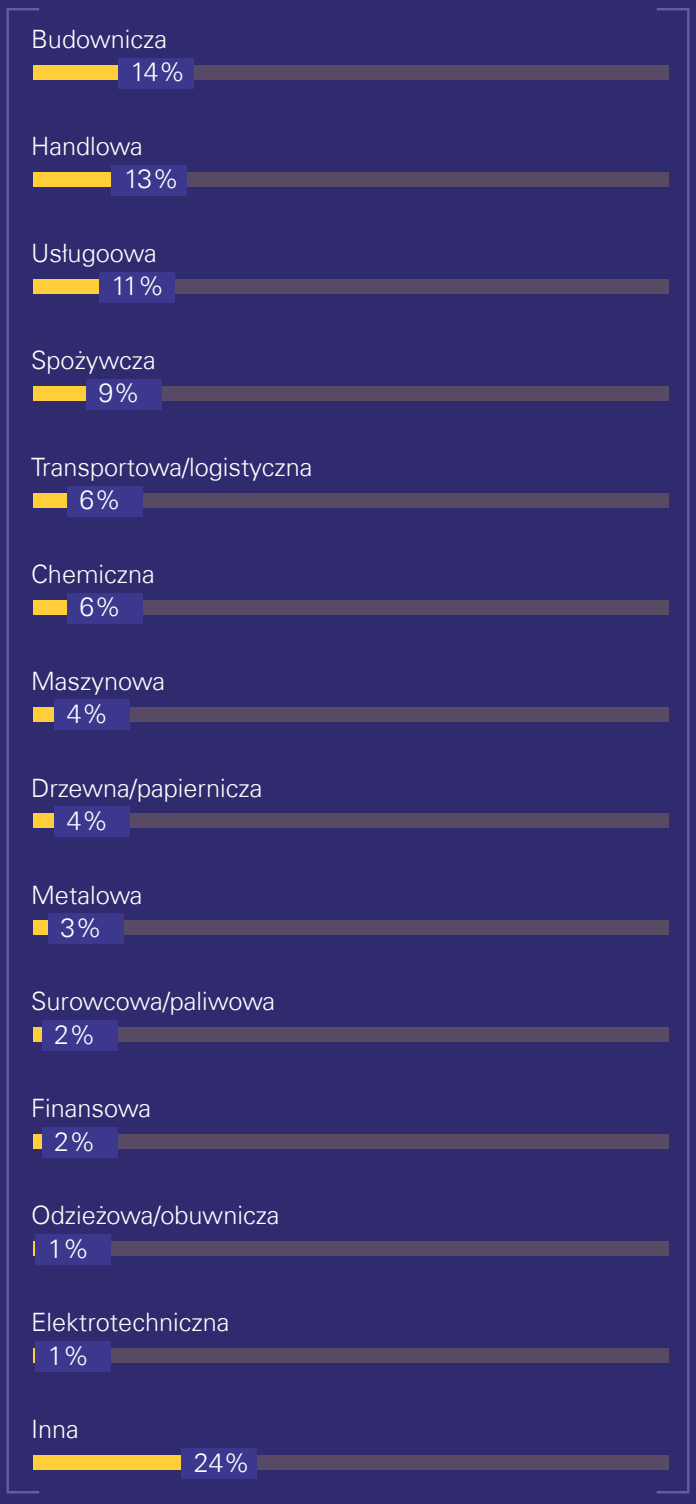
Średnie roczne przychody



Typ kapitału

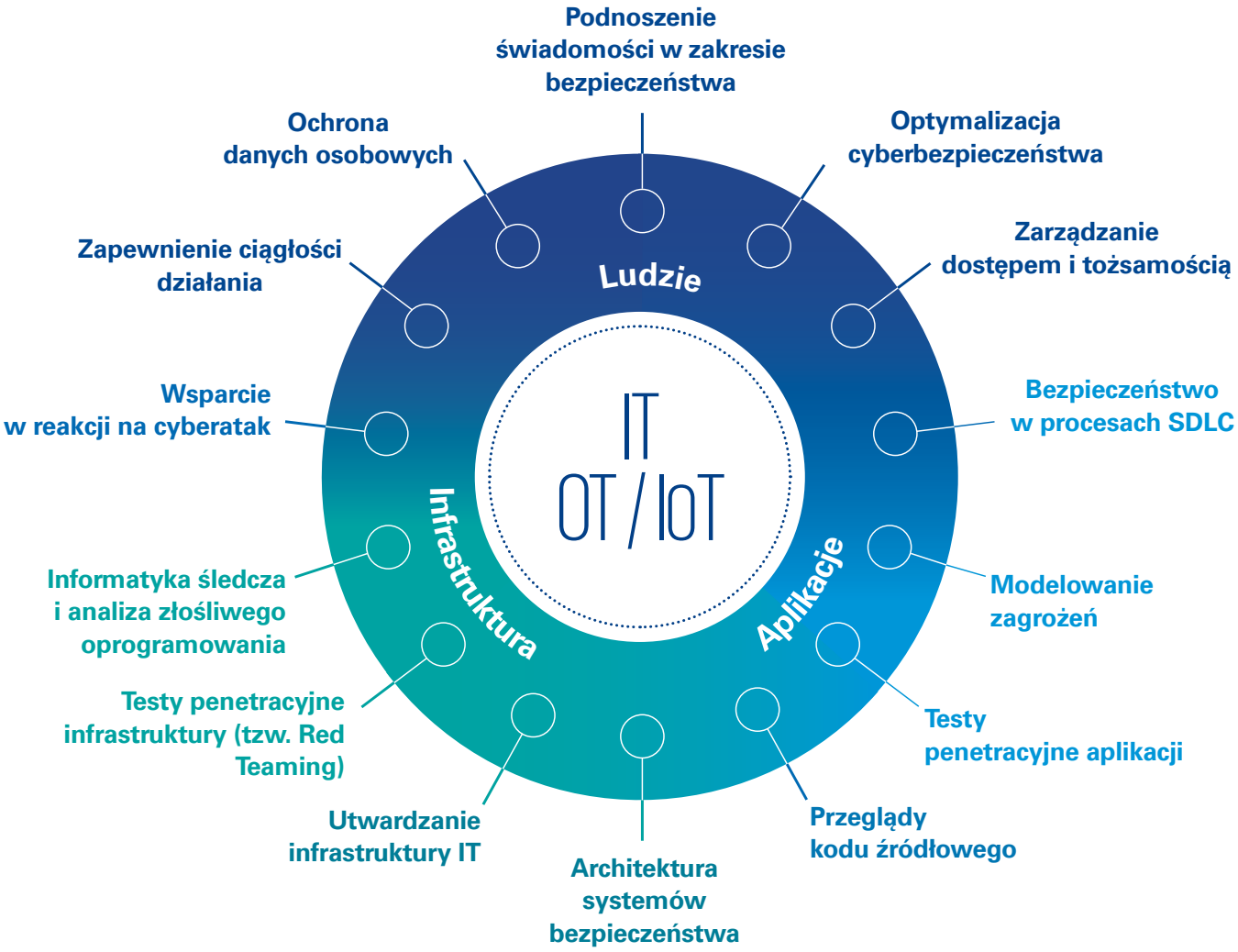


Branża



Usługi KPMG w zakresie cyberbezpieczeństwa

Zespół Cyberbezpieczeństwa KPMG w Polsce świadczy szeroki zakres usług, podchodzący w kompleksowy sposób do ochrony informacji. Wspiera firmy w zabezpieczeniu infrastruktury, aplikacji oraz zadbaniu o czynnik ludzki, czyli właściwą organizację, procesy oraz wiedzę pracowników w zakresie ochrony informacji. Pomaga firmom zarówno w przygotowaniu się na odparcie cyberataku, jak również w podjęciu właściwych działań, gdy cyberatak już nastąpił.



Wybrane publikacje KPMG w Polsce i na świecie

Barometr cyberbezpieczeństwa. W obronie przed cyberatakami (2019)

Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym (2018)

Sektor life sciences – innowacje i cyberbezpieczeństwo to ierozłączne elementy

Bezpieczeństwo technologii mobilnych

Cyberbezpieczeństwo – wyzwanie współczesnego prezesa

Clarity on Cyber Security

Kontakt

KPMG Poland

KPMG w Polsce
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Michał Kurek
Doradztwo biznesowe,
Cyberbezpieczeństwo
Partner
E: michalkurek@kpmg.pl

Łukasz Staniak
Doradztwo biznesowe,
Cyberbezpieczeństwo
Starszy Menedżer
E: lstaniak@kpmg.pl

Marcin Strzałek
Doradztwo biznesowe,
Cyberbezpieczeństwo
Menedżer
E: mstrzalek@kpmg.pl

dr Magdalena Maruszczak
Marketing i Komunikacja
Dyrektor
E: mmaruszczak@kpmg.pl

KPMG.pl

Biura KPMG w Polsce

Warszawa
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Kraków
ul. Opolska 114
31-323 Kraków
T: +48 12 424 94 00
F: +48 12 424 94 01
E: krakow@kpmg.pl

Poznań
ul. Roosevelta 22
60-829 Poznań
T: +48 61 845 46 00
F: +48 61 845 46 01
E: poznan@kpmg.pl

Wrocław
ul. Szczytnicka 11
50-382 Wrocław
T: +48 71 370 49 00
F: +48 71 370 49 01
E: wroclaw@kpmg.pl

Gdańsk
al. Zwycięstwa 13a
80-219 Gdańsk
T: +48 58 772 95 00
F: +48 58 772 95 01
E: gdansk@kpmg.pl

Katowice
ul. Francuska 36
40-028 Katowice
T: +48 32 778 88 00
F: +48 32 778 88 10
E: katowice@kpmg.pl

Łódź
ul. Składowa 35
90-127 Łódź
T: +48 42 232 77 00
F: +48 42 232 77 01
E: lodz@kpmg.pl