Grant Thornton

Zamek z papieru, czyli zarządzanie ryzykiem cyfrowym w polskich firmach

Wyniki badania poziomu cyberbezpieczeństwa firm w Polsce

Luty 2020

Wstęp

Cyberbezpieczeństwo zajmuje wysoką pozycję w agendach zarządów firm, które do rozwoju podchodzą odpowiedzialnie. Po produkcji mechanicznej napędzanej siłą pary, produkcji masowej z zastosowaniem energii elektrycznej oraz sterowanej komputerowo zautomatyzowanej linii produkcyjnej, nadszedł czas jednorodnego systemu cyber-fizycznego (ang. cyber-physical system). Jesteśmy świadkami czwartej rewolucji przemysłowej, której istotą jest integracja systemów cyber-fizycznych, Internetu rzeczy i przetwarzania chmurowego. Lawinowy wzrost efektywności przedsiębiorstw, które decydują się na aktywny udział w tych rewolucyjnych zmianach gospodarczych, obarczony jest jednak ryzykiem związanym z cyberzagrożeniami.

Dynamika zagrożeń dla cyberbezpieczeństwa w ostatnich latach przekroczyła poziom, który jest akceptowalny nawet dla amatorów wysokiego ryzyka. Jak można szacować na bazie danych CERT Polska, w minionym roku w polskiej cyberprzestrzeni zarejestrowano ponad 40 tysięcy zdarzeń, które stanowiły potencjalne zagrożenie dla bezpieczeństwa informacji. Blisko 10% z tych zdarzeń to faktyczne incydenty, które naruszyły bezpieczeństwo funkcjonowania organizacji. Przeciętnie więc każdego dnia w Polsce około 10 podmiotów zderza się z realnym zagrożeniem związanym z wyciekiem danych. Dla porównania liczba wszystkich zarejestrowanych incydentów w 2010 wynosiła 60 razy mniej.

Mamy do czynienia z bezprecedensowym wzrostem zagrożeń dla cyberbezpieczeństwa, które awansowały do pierwszej trójki zagrożeń globalnych, obok kataklizmów naturalnych i zmian klimatycznych. Jednocześnie polskie firmy wyraźnie są nieświadome realnych zagrożeń i funkcjonują w iluzji poczucia bezpieczeństwa, nie realizując podstawowych działań, które pozwalałyby uchronić się przed dotkliwymi stratami związanymi z incydentami.

Życzymy przyjemnej lektury.

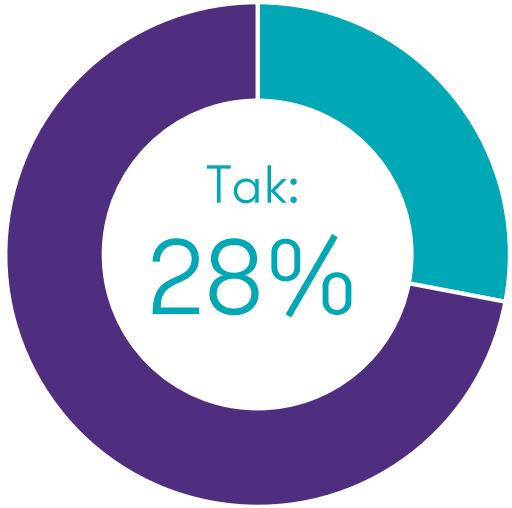
Radosław Kaczorek
Partner
Digital Drive
Cyberbezpieczeństwo

Firmy na cyfrowym celowniku

28% ankietowanych przedsiębiorstw w Polsce przyznało, że w ciągu ostatnich 12 miesięcy były celem cyberataku

O tym, że cyberbezpieczeństwo nie powinno już być traktowane jako priorytet tylko przez banki czy inne potężne instytucje wrażliwe dla funkcjonowania państwa, może świadczyć też fakt, że aż 28% z ankietowanych przez nas średnich i dużych firm twierdzi, że w ostatnim roku padło celem ataku cybernetycznego – np. wycieku lub kradzieży danych wewnętrznych przedsiębiorstwa. Cyberprzestępczość i konieczność chronienia się przed nią staje się powoli chlebem powszednim przedsiębiorstw działających w Polsce i na świecie.

Czy w ciągu ostatnich 12 miesięcy Państwa firma była **celem cyberataku**, w tym wycieku lub kradzieży danych wewnętrznych?



Polskie firmy czują się bezpiecznie...

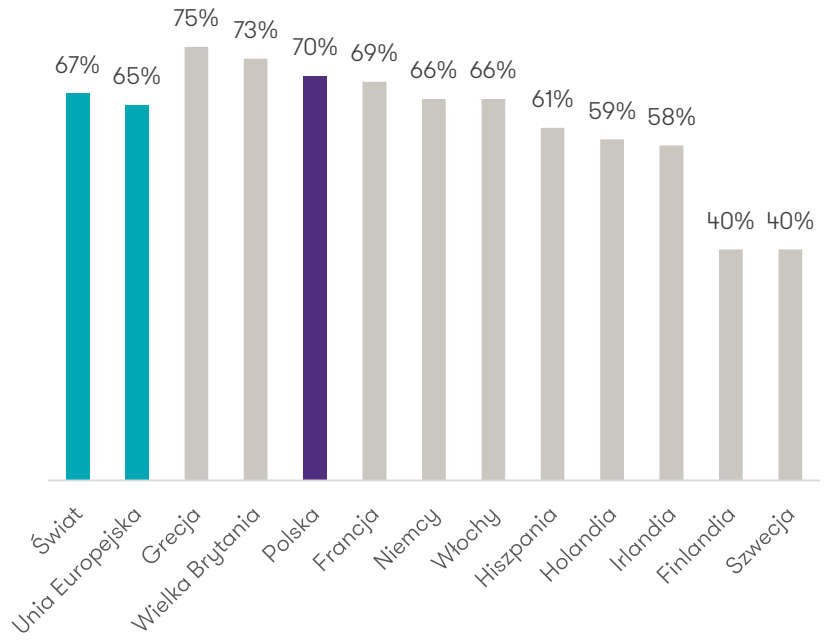
Przedsiębiorcy w naszym kraju w zdecydowanej większości (70% badanych) są zadowoleni z przygotowania swoich firm na ryzyko cyfrowe

W ramach badania zapytaliśmy średnie i duże przedsiębiorstwa w wybranych krajach Unii i na świecie, czy są zadowolone ze swojego przygotowania na ryzyko cyfrowe, tzn. czy ich zdaniem, mają wdrożone odpowiednie procesy wykrywania zagrożenia i reagowania na ataki.

Okazuje się, że polskie firmy – podobnie zresztą jak przedsiębiorstwa w większości badanych krajów – mają bardzo wysoką samoocenę. Aż 70% firm w Polsce odpowiedziało na to pytanie twierdząco. Największy odsetek zanotowano w Grecji (75%) oraz Wielkiej Brytanii (73%). Natomiast najmniejsze zadowolenie z przygotowania na ryzyko cyfrowe wyraziły firmy w Finlandii i Szwecji (40%) oraz Japonii (38%) i Rosji (31%). Średnia dla całego badania to 67%.

Czy to możliwe, że polskie czy greckie firmy są lepiej przygotowane na cyberataki i mają lepsze zabezpieczenia przed nimi niż przedsiębiorstwa w krajach rozwiniętych, jak Szwecja czy Japonia?

Wykres 1. Odsetek firm, które deklarują, że są zadowolone ze swojego przygotowania na cyberataki – wyniki dla krajów Unii Europejskiej



...ale to złudne poczucie

Zapytani o wykonywanie konkretnych czynności związanych z ryzykiem cyfrowym w firmie, przedsiębiorcy w Polsce nie byli już tak optymistyczni

Wykres 2. Czy jesteś zadowolony z gotowości firmy do wykonywania poszczególnych czynności związanych z ryzykiem cyfrowym?

Kolejne pytania w naszym badaniu sugerują, że wysoki poziom zadowolenia polskich firm z przygotowania na cyberataki wynika raczej z niskiej świadomości tego, czym są procedury zarzadzania cyberbezpieczeństwem niż z faktycznego dobrego przygotowania na zagrożenia. Poziom zadowolenia przedsiębiorców znacznie bowiem spada, jeśli pytamy ich o przygotowanie firmy w konkretnych obszarach związanych z ryzykiem cyfrowym. A to właśnie te poszczególne obszary budują wspólnie faktyczny system odporności na cyberataki.

Według badania, tylko 29% firm w Polsce jest zadowolonych ze swoich możliwości wykrywania przypadków naruszenia prywatności danych, a tylko 41% dobrze ocenia swoje zdolności do reagowania na ataki. Tylko 30% firm twierdzi, że po wykryciu incydentu są w stanie odpowiednio ocenić sytuację i zaistniałe szkody. Pokazuje to bardzo niską skuteczność wykrywania incydentów wśród polskich firm oraz długi czas, który upływa od wystąpienia incydentu do jego wykrycia. Mierzony jest on nie w godzinach, czy dniach, ale… w miesiącach. Tworzy to złudne poczucie bezpieczeństwa, które samo w sobie jest zagrożeniem.

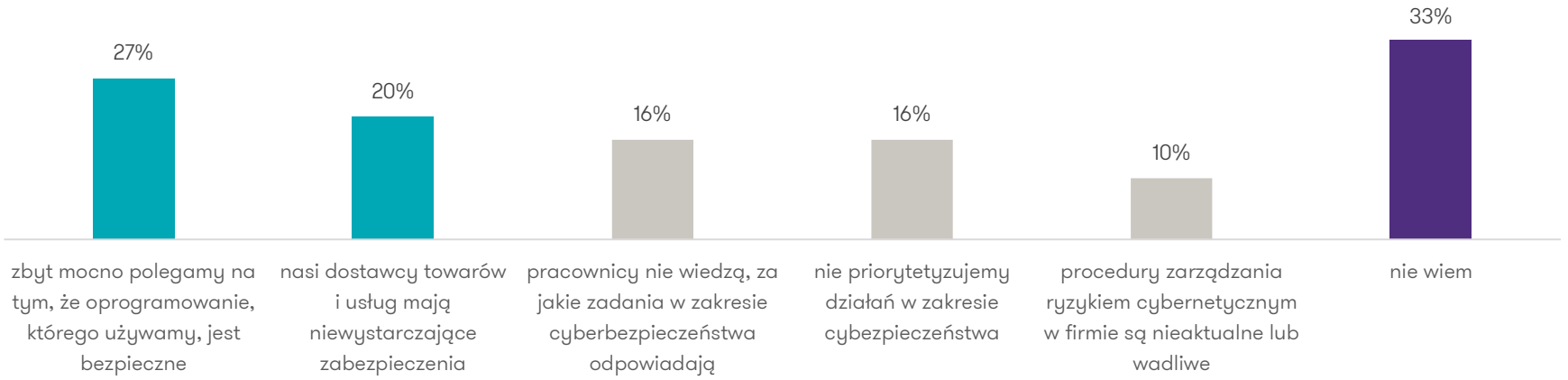
Upadek modelu zaufania

Niewiedza, zbyt mocne poleganie na oprogramowaniu komputerowym i niezabezpieczeni dostawcy to najsłabsze punkty zarządzania ryzykiem w firmie

Przedsiębiorcy zapytani o słabe strony firmy w zarządzaniu cyberbezpieczeństwem najczęściej odpowiadają „nie wiem". Oznacza to, że aż co trzeci przedsiębiorca w Polsce nawet nie zna kondycji swojej firmy w zakresie odporności na cyberzagrożenia.

Ci którzy znają kondycję swojej firmy, przyznają, że zbyt mocno polegają na oprogramowaniu komputerowym. Wychodzą z założenia, że skoro kupili oprogramowanie, to na pewno jego twórcy zadbali o jego bezpieczeństwo. Ponadto, firmy twierdzą, że zagrożeniem są ich dostawcy – mój system bezpieczeństwa na niewiele się zda, jeśli moi dostawcy będą mieli luki w swoich systemach. To bardzo mocny trend pokazujący upadek modelu zaufania do partnerów biznesowych.

Wykres 3. Jakie są słabe punkty w zarządzaniu zagrożeniami związanymi z cyberbezpieczeństwem i prywatnością danych w Twojej firmie?



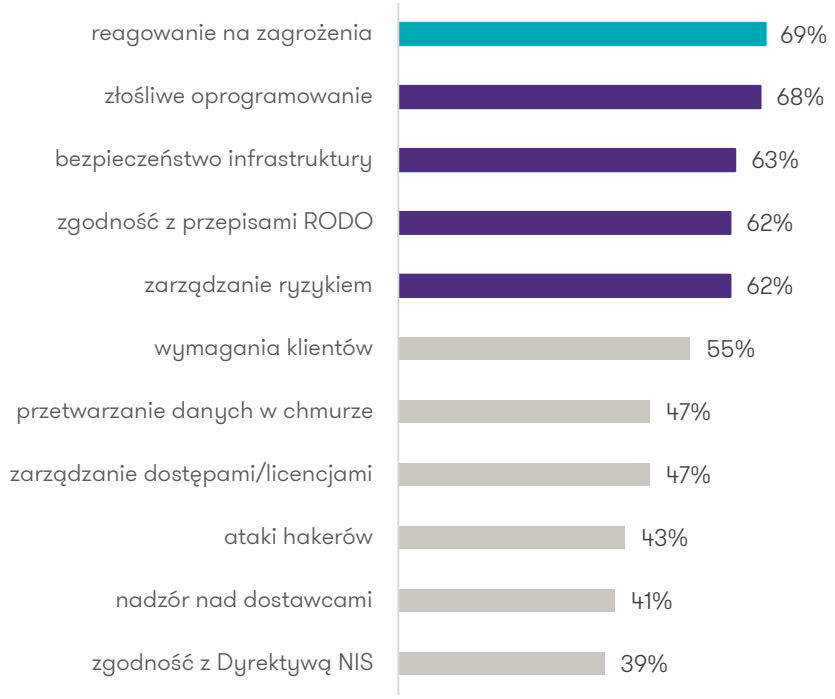
Najtrudniejsza jest odpowiednia reakcja

Największym wyzwaniem w obszarze bezpieczeństwa IT w firmach w Polsce jest reagowanie na zagrożenia oraz złośliwe oprogramowanie

Zapytaliśmy przedsiębiorców w Polsce również o to, z jakimi największymi wyzwaniami w obszarze bezpieczeństwa informatycznego mierzą się ich firmy. Najwięcej (69%) wskazań otrzymało odpowiednie reagowanie na zagrożenia. Drugim równie silnym problemem, z jakim mierzą się działy firmy, jest złośliwe oprogramowanie – odpowiedź tę wskazało 68% respondentów. Przedsiębiorcy jako wyzwanie dla bezpieczeństwa IT wskazywali również bezpieczeństwo infrastruktury (63%), zgodność z przepisami RODO oraz zarządzanie ryzykiem (po 62% odpowiedzi).

Takie odpowiedzi wskazują, że polskie firmy w swojej zdecydowanej większości przyjmują strategię cyberbezpieczeństwa opierającą się na reagowaniu na zaistniałe zagrożenia, niż na zapobieganiu im. Firmy zwykle nie mają opracowanych i funkcjonujących mechanizmów prewencyjnych, które w sposób proaktywny powinny obniżać liczbę incydentów, podnosząc skuteczność i efektywność ochrony przez cyberzagrożeniami. Czas, który firmy obecnie poświęcają na reagowanie na zagrożenia, powinien zostać zainwestowany w zbudowanie systemu odporności.

Wykres 4. Obecnie największym wyzwaniem w obszarze IT i bezpieczeństwa dla Twojej firmy jest:



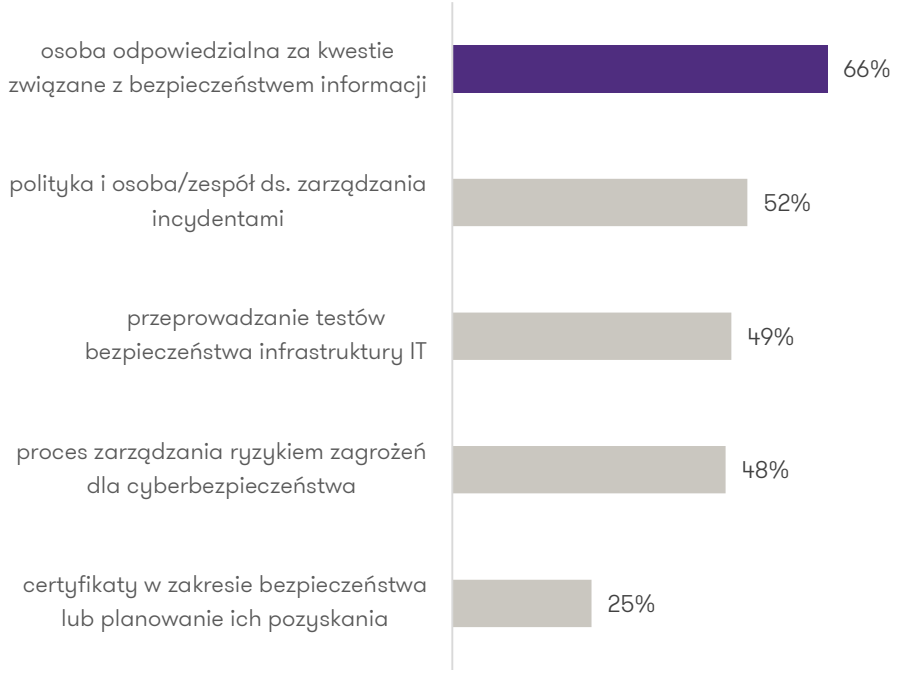
Działania w ramach bezpieczeństwa

W 66% firm w Polsce funkcjonuje osoba odpowiedzialna za bezpieczeństwo informacji. Politykę zarządzania incydentami prowadzi 52% firm

Jak polskie firmy przygotowują się na zagrożenia? Dwie trzecie ankietowanych firm w Polsce zatrudnia osobę odpowiedzialną za kwestie związane z bezpieczeństwem informacji. W 52% przedsiębiorstw wdrożona jest polityka zarządzania incydentami, a także osoba bądź zespół, który za to odpowiada. Ponadto, 49% firm deklaruje, że przynajmniej raz w roku prowadzi testy bezpieczeństwa infrastruktury IT. Tylko 25% posiada lub planuje pozyskanie certyfikatów bezpieczeństwa (np. ISO 27001, ISO 22301, ISAE 3402).

Odpowiedzi respondentów wskazują na to, że w polskich firmach relatywnie często istnieją struktury zarządzania bezpieczeństwem. Jednak, jak wynika z innych odpowiedzi, zakres ich działań jest mocno ograniczony i skoncentrowany na kwestiach technologicznych. Cyberbezpieczeństwo traktowane jest jako element zarządzania informatyką, tymczasem budowanie faktycznej odporności na cyberzagrożenia powinno dotyczyć całej organizacji. Najsłabszym ogniwem organizacji i jej systemu bezpieczeństwa nie jest bowiem sprzęt czy oprogramowanie, ale ludzie i ich słabości.

Wykres 5. Czy w Państwa firmie funkcjonuje:



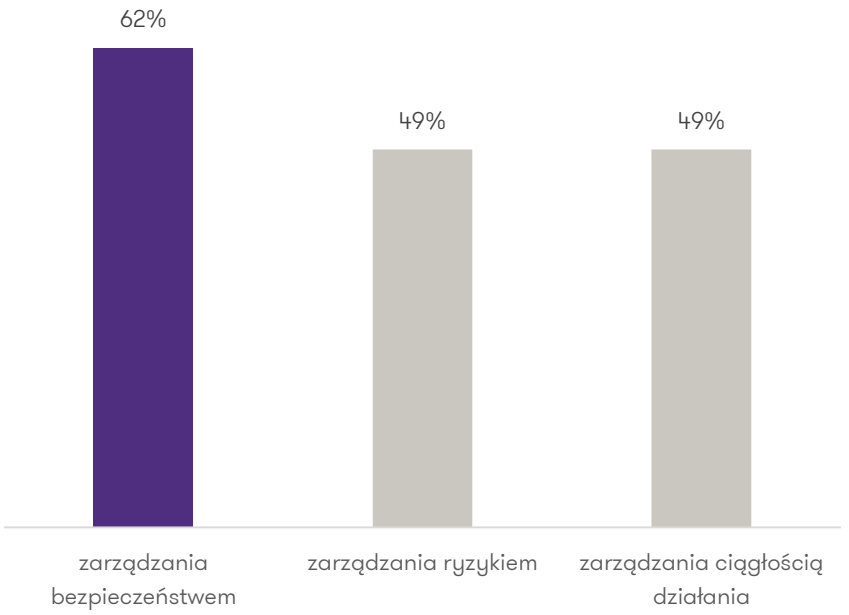
Działania w ramach bezpieczeństwa

Ponad połowa firm w Polsce (62%) wdrożyła formalne procesy zarządzania bezpieczeństwem. 49% ma procesy zarządzania ryzykiem i ciągłością działania

Elementem skutecznego wykrywania incydentów i odpowiedniego na nie reagowania jest także wdrożenie konkretnych procesów w organizacji. Według badania, 62% firm w Polsce ma wdrożone formalne procesy w zakresie zarządzania bezpieczeństwem. Prawie połowa ankietowanych przedsiębiorstw wdrożyła u siebie procesy zarządzania ryzykiem i zarządzania ciągłością działania – w obu przypadkach odnotowano 49% odpowiedzi.

Odsetek firm, które deklarują wdrożenie procesów zarządzania jest, w naszej ocenie, dosyć wysoki. Nie powinno to dziwić w świetle rosnących wymagań regulacyjnych, takich jak europejskie rozporządzenie o ochronie danych osobowych oraz ustawa o krajowym systemie cyberbezpieczeństwa. Rośnie również poziom wymagań ze strony klientów tych firm, co zmusza je do uregulowania obszarów zarządzania bezpieczeństwem, ryzykiem i ciągłością działania. Odpowiedzi udzielone na inne pytania mogą sugerować jednak, że choć firmy mają formalnie wdrożone procedury, to skuteczność działania firm w ramach tych procesów jest niska.

Wykres 6. Czy w Twojej firmie wdrożono formalne procesy w zakresie:

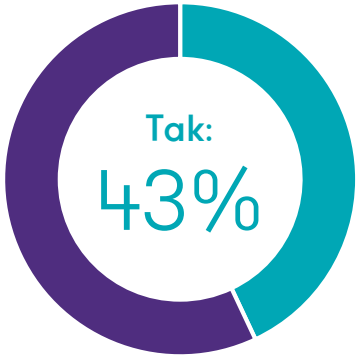


Klienci wymagają cyberbezpieczeństwa

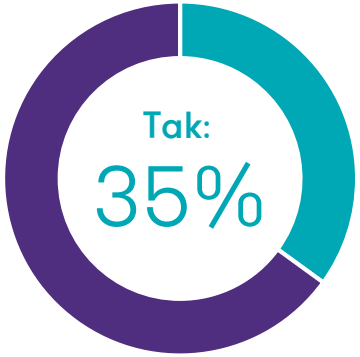
Klienci 43% badanych przedsiębiorstw w Polsce oczekują od nich spełnienia wymagań bezpieczeństwa informacji

Wykres 7. Czy w przypadku Twojej firmy prawdziwe są poniższe twierdzenia?

Klienci oczekują od mojej firmy spełnienia wymagań bezpieczeństwa informacji i/lub certyfikacji?



Klienci mają prawo przeprowadzania audytu bezpieczeństwa w mojej firmie?



Coraz częściej motywacją przedsiębiorstw do inwestowania we własne cyberbezpieczeństwo jest nie tylko poczucie zagrożenia czy wymogi regulacyjne, ale też presja ze strony klientów. Coraz więcej firm przy zakupie usług od zewnętrznych dostawców stawia przed nimi wyśrubowane wymagania dotyczące bezpieczeństwa danych. Przedsiębiorstwa bez wdrożonych odpowiednich procedur często nie mają nawet co brać udziału w pewnych przetargach.

Na pytanie o oczekiwania i zakres działalności klientów firm, 43% ankietowanych przedsiębiorstw zadeklarowało, że ich klienci oczekują od firmy spełnienia wymagań bezpieczeństwa informacji i/lub certyfikacji. Prawo klientów do przeprowadzania audytu bezpieczeństwa w danej firmie mają klienci 35% przedsiębiorstw objętych badaniem.

Wyniki badania wskazują na rosnącą rolę wymagań rynkowych w uzasadnianiu inwestycji w bezpieczeństwo. Niniejszym cyberbezpieczeństwo staje się trwałym elementem budowania przewagi konkurencyjnej i wartości firmy.

Brak specjalistów główną barierą

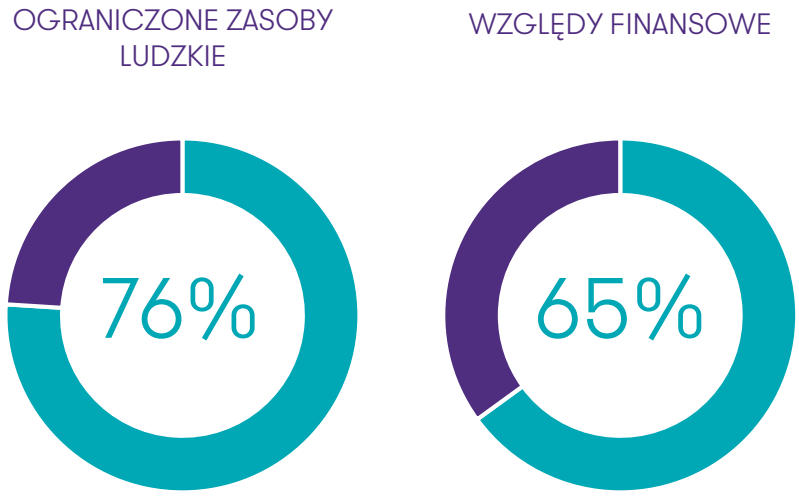
Ograniczone zasoby ludzkie są czynnikiem decydującym o częstotliwości przeprowadzania audytu bezpieczeństwa w 76% firm w Polsce

Ankietowani zostali zapytani również o to, co najbardziej utrudnia im regularne monitorowanie stanu bezpieczeństwa w ich firmach – czy są to raczej ograniczenia finansowe, czy kadrowe.

Okazuje się, że aż 76% przedsiębiorstw zadeklarowało, że główną przeszkodą w regularnym audycie ich firmy stanowią ograniczone zasoby ludzkie – zespoły albo nie mają czasu, żeby zostawić bieżące zadania i zająć się profilaktyką cyberbezpieczeństwa, albo nie mają odpowiednich kompetencji do prowadzenia takich audytów. Względy finansowe, a więc np. ograniczone budżety IT na dodatkowe narzędzia czy zlecanie audytów na zewnątrz, również stanowią barierę, ale mniejszą – odpowiedź tę wskazuje 65% ankietowanych.

Ograniczony dostęp do specjalistycznej wiedzy w zakresie cyberbezpieczeństwa stanowi ogromne wyzwanie dla większości firm. Nieuchronne zatem jest przesunięcie ciężaru nadzoru nad bezpieczeństwem do wyspecjalizowanych dostawców.

Wykres 8. Które z poniższych czynników mają decydujące znaczenie o tym, jak regularnie przeprowadzają Państwo audyt bezpieczeństwa w firmie?



Naszym zdaniem

Fikcyjne bezpieczeństwo

Wyniki badania wskazują, że kluczowym motywatorem do budowania bezpieczeństwa informatycznego w polskich firmach nie jest realne poczucie zagrożenia i chęć zapobiegania im, ale wymagania prawne, jakie w coraz większym stopniu spoczywają na przedsiębiorstwach. Na znaczeniu zyskuje też fakt, że coraz częściej klienci wymuszają na dostawcach wykazania się procedurami bezpieczeństwa. Nadal jednak zarządzanie bezpieczeństwem oparte jest raczej na modelu reaktywnym, a nie proaktywnym. Wszystko to sprawia, że polskie firmy budują bezpieczeństwo „papierowe". Zarządzanie bezpieczeństwem informacji sprowadzone jest zwykle do zarządzania zgodnością. Taka sytuacja, przy rosnącej dynamice zagrożeń, naraża polskie firmy na istotne ryzyko realnych strat finansowych. Sytuacja jest tym bardziej niepokojąca, że – według badania – polskie przedsiębiorstwa mają poważny problem z dostępem do wykwalifikowanej kadry w dziedzinie cyberbezpieczeństwa. W długim okresie taki model zarządzania nie uchroni firm przed incydentami bezpieczeństwa. Firmy powinny być świadome, na jak poważne ryzyko są narażone, oraz jak w sposób profesjonalny, w oparciu o specjalistyczną wiedzę, budować realny, a nie papierowy, system bezpieczeństwa.

Radosław Kaczorek
Partner
Digital Drive
Cyberbezpieczeństwo

O badaniu:

Raport zawiera wyniki dwóch badań przeprowadzonych w okresie kwiecień-grudzień 2019 roku. Pierwsze badanie przeprowadzone zostało w ramach projektu International Business Report przez firmę Dynata na zlecenie Grant Thornton International metodą CAPI i CAWI na grupie 200 przedstawicieli zarządów średnich i dużych firm działających w Polsce i 35 krajach świata. Drugie zostało przeprowadzone przez Grant Thornton Polska metodą CAWI na losowej grupie 107 przedsiębiorstw działających w Polsce.

Zapraszamy do kontaktu

Kontakt dla klientów:

Radosław Kaczorek
Partner
Digital Drive
Cyberbezpieczeństwo
T +48 501 433 303
E Radoslaw.Kaczorek@pl.gt.com

Kontakt dla mediów:

Jacek Kowalczyk
Dyrektor Marketingu i PR
T +48 505 024 168
E Jacek.Kowalczyk@pl.gt.com

O nas

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie, obecna w 140 krajach i zatrudniająca ponad 56 tys. pracowników. W Polsce działamy od 27 lat. Zespół 700 pracowników wspiera naszych klientów w obszarach takich jak audyt, doradztwo podatkowe, doradztwo transakcyjne czy outsourcing płac i kadr oraz outsourcing księgowości.