Grant Thornton

Zamek z papieru

Cyberbezpieczeństwo w polskich firmach

Wyniki 2. edycji badania Grant Thornton na temat zarządzania cyberbezpieczeństwem w przedsiębiorstwach

Listopad 2024

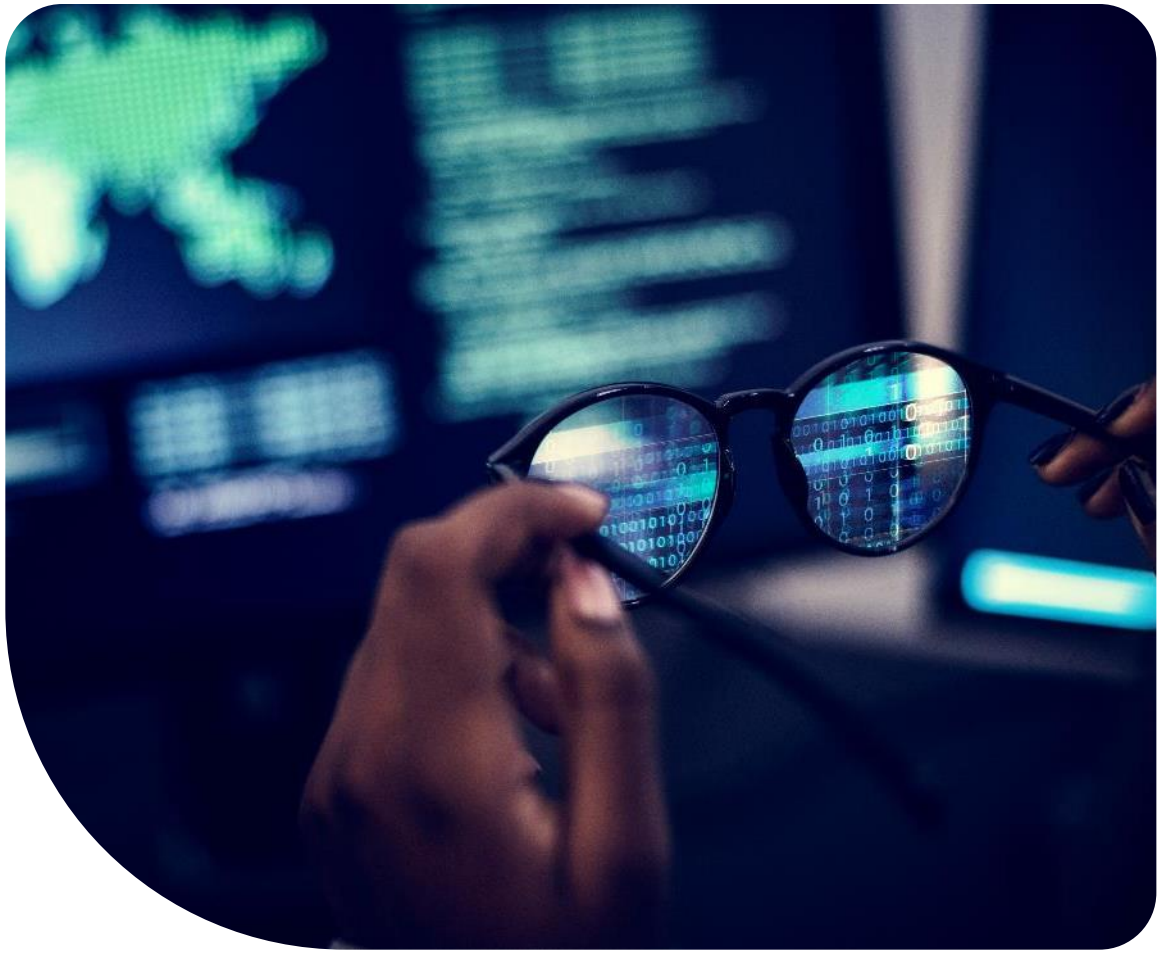
Wprowadzenie

Zagrożenie wyparte ze świadomości

W firmach, które do rozwoju podchodzą odpowiedzialnie, cyberbezpieczeństwo zawsze zajmuje wysoką pozycję na liście priorytetów. 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.

Liczba zagrożeń dla cyberbezpieczeństwa w ostatnich latach rośnie w lawinowym tempie. Są one w ścisłej czołówce zagrożeń globalnych, obok kataklizmów naturalnych i zmian klimatycznych. Jednocześnie polskie firmy pozostają nieświadome realnych zagrożeń i funkcjonują w iluzji poczucia bezpieczeństwa, nie realizując podstawowych działań, które pozwalałyby uchronić się przed dotkliwymi stratami związanymi z incydentami. Nasz raport powinien skłonić zarządy przedsiębiorstw do refleksji – czy na pewno moja firma jest odporna na zagrożenia?

Zapraszamy do lektury!



Kluczowe wnioski

40%

Taki odsetek firm w Polsce doświadcza rocznie incydentów (np. ataków na systemy czy bazy danych), które mogły zagrozić ich funkcjonowaniu.

48%

Taki odsetek firm nie rejestruje zmian w systemach informatycznych, co w razie incydentu utrudnia im odpowiednią reakcję.

48%

Taki odsetek firm nie poddaje swoich systemów skanom podatności.

23%

Tylko tyle firm posiada wykupioną polisę ubezpieczeniową na wypadek ataku cybernetycznego.

O badaniu:
Dane prezentowane w raporcie pochodzą z badania dojrzałości cybernetycznej, przeprowadzonego przez Grant Thornton metodą CAWI na losowej grupie 210 przedstawicieli zespołów IT firm (średnich i dużych) w czerwcu-październiku 2024 roku.

Incydentów przybywa lawinowo

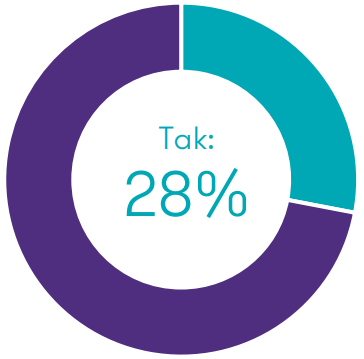
Aż 40% firm w Polsce doświadczyło w ostatnim roku ataku cybernetycznego. W ciągu kilku najbliższych lat będzie tego doświadczało regularnie niemal każde przedsiębiorstwo.

Jeszcze dekadę temu konieczność budowania systemu ochrony cybernetycznej kojarzona była z obszarem, który dotyczy niewielkiej grupy organizacji w kraju – banków, potężnych platform internetowych czy instytucji rządowych. Powszechna opinia była taka, że tylko tego rodzaju instytucje są celem internetowych ataków, więc „zwykłe" firmy nie muszą się tym przejmować, a tego rodzaju działania przez wiele osób traktowane było jako element przesadnej korporacyjnej biurokracji.

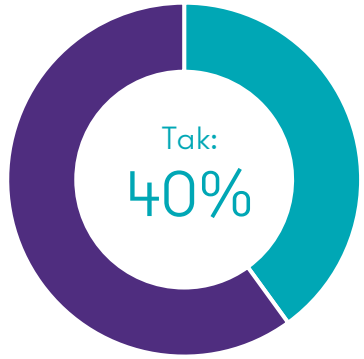
Sytuacja szybko zaczęła się jednak zmieniać. Kiedy pięć lat temu ankietowaliśmy firmy w Polsce, 28% z nich przyznało, że w ostatnich 12 miesiącach padło ofiarą próby ataku. Obecnie to już 40%, co oznacza, że niemal co druga firma w Polsce doświadcza raz w roku próby włamania do swoich systemów, np. wycieku lub kradzieży danych. W okresie 3-letnim ten odsetek sięgałby zatem obecnie prawdopodobnie 60%, a może nawet 70%, a w kolejnych latach należy się spodziewać dalszego wzrostu. Oznacza to, że cyberprzestępczość i konieczność ochrony stała się już chlebem powszednim przedsiębiorstw działających w Polsce i na świecie.

Czy w ciągu ostatnich 12 miesięcy w Państwa firmie wydarzył się **incydent cybernetyczny** (np. wyciek lub kradzież danych), który wpłynął lub mógł wpłynąć na ciągłość jej działania?

2019:



2024:



Firmowe systemy z wieloma lukami

Najczęstsze błędy wśród przedsiębiorstw, które narażają je na ataki, to przede wszystkim brak rejestrowania zmian w systemach i brak kontroli nad uprawnieniami.

Jak wynika z naszego badania, działy IT w polskich firmach mają dość wysoką świadomość tego, jak zarządzać firmowym środowiskiem, aby zadbać o ich bezpieczeństwo, ale nadal w swoim działaniu pozostawiają pewne luki. Jedynie 52% badanych firm przyznało, że każdorazowo rejestruje zmiany dokonywane w systemach IT czy bazach danych, co oznacza, że prawie połowa firm tego nie robi. Brak rejestracji zmian uniemożliwia natychmiastowe przywrócenie działania w przypadku poważnego incydentu, a także utrudnia identyfikację nieautoryzowanych zmian w systemach.

W wielu firmach występuje też niedostateczna kontrola nad nadawaniem i odbieraniem uprawnień. Tylko 55% ankietowanych firm deklaruje, że rejestruje wnioski o zmianę w uprawnieniach, a 62% kontroluje konta o podwyższonych uprawnieniach. To oznacza, że prawie połowa firm nie posiada właściwej kontroli nad dostępem do krytycznych aktywów swoich organizacji.

Procedury nadal stosunkową rzadkością

Choć w firmach stopniowo przybywa procedur związanych z cyberbezpieczeństwem, to nadal nie wszystkie obszary są w ten sposób odpowiednio zabezpieczone.

Z procedur, które funkcjonują obecnie w polskich firmach, najczęstszą jest polityka haseł – wdrożyło ją 79% ankietowanych przedsiębiorstw. 64% firm, posiada też zabezpieczone odpowiednie struktury (wewnętrzne lub zewnętrzne) delegowane do szybkiego, profesjonalnego reagowania na incydenty.

Jednocześnie jedynie 41% badanych firm twierdzi, że wdrożono proces stałego zarządzania ryzykiem i podatności systemów na ewentualne ataki, a 48% deklaruje, że posiada opracowany plan ciągłości działania (tzw. business continuity plan), czyli plan awaryjny pozwalający organizacji sprawnie działać mimo sytuacji kryzysowej. Biorąc pod uwagę, jak istotne są to procedury (decydujące często o być albo nie być firmy) poziom świadomości i wdrożenia zasad ładu i nadzoru jest zdecydowanie zbyt niski.

Firewall i Antywirus to podstawa bezpieczeństwa

Znaczny odsetek firm wykazuje się brakiem świadomości, jak ważne dla bezpieczeństwa infrastruktury logicznej prócz oprogramowania antywirusowego jest zabezpieczenie sieci firmowej.

Najczęściej stosowanym przez firmy rozwiązaniem zabezpieczającym przed złośliwym oprogramowaniem są systemy antywirusowe. Niestety, sam zabieg ochrony przed wirusami nie wystarczy. Zapory sieciowe (ang. firewall) to kolejne obowiązkowe narzędzie służące do ochrony sieci przed nieautoryzowanym dostępem, atakami lub zainfekowanym oprogramowaniem. Spośród ankietowanych przez nas firm, 77% wykorzystuje to rozwiązanie w celu zapewnienia bezpieczeństwa organizacji, co oznacza, że prawie co czwarta firma nie stosuje tego rozwiązania.

Antywirus i firewall nie są jednak jedynymi rozwiązaniami pozwalającymi zagwarantować bezpieczeństwo firmy. W naszej ankiecie zapytaliśmy czy firmy posiadają wdrożone inne rozwiązania mające na celu ochronę sieci i systemów informatycznych tj. systemy klasy UTM, XDR, PAM, MDM i SIEM. Wyniki badania wskazują, że zdarza się to obecnie rzadko, tylko w przypadku 10-15% firm, a to oznacza że większość firm opiera swoją linię obrony wyłącznie na podstawowych mechanizmach.

Naszym zdaniem

Obecne otoczenie regulacyjne oraz wzrastające wymagania wśród naszych Klientów inspirują nas do poszukiwania coraz to nowych metod działania w odpowiedzi na identyfikowane ryzyka. Próba weryfikacji, jak w praktyce wyglądają zabezpieczenia polskich przedsiębiorstw, pozwoliła nam odnieść rzeczywiste braki do najwyższych rynkowych standardów.

Aktywnie pomagamy firmom w reagowaniu na incydenty i nasze obserwacje na przestrzeni ostatnich kilku lat wyraźnie wskazują na poważne braki zabezpieczeń wśród polskich firm. Zainspirowało nas to do przeprowadzenia badania rynkowego i oceny czy nasz rynek jest w stanie obronić się przed zagrożeniami dla cyberbezpieczeństwa. Raport z badania powinien skłonić do refleksji właścicieli i zarządów polskich przedsiębiorstw i odpowiedzi na ważne pytania. Czy moja firma jest gotowa na cyberatak? Czy spełniamy wymagania regulacji europejskich takich jak np. NIS-2 czy DORA? Czy firma jest przygotowana na wyciek kluczowych danych, w tym danych osobowych. Jak długo firma wytrwa w sytuacji unieruchomienia systemów informatycznych po ataku cybernetycznym. Czy konkurencja robi to lepiej niż moja firma.

Adam Woźniak
Executive Director
Cybersecurity
Grant Thornton

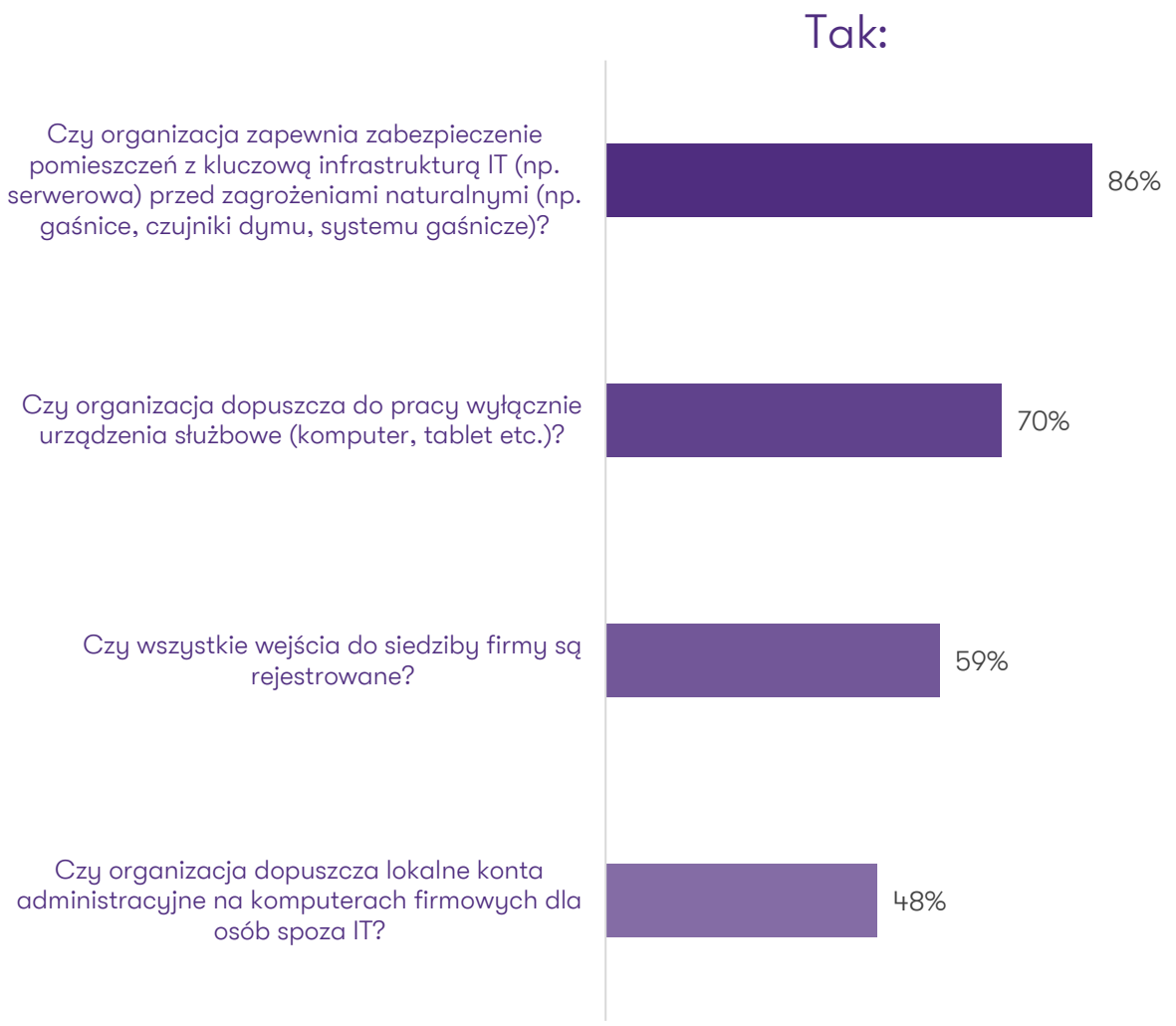
Infrastruktura podatna na kryzysy

Ważnym źródłem potencjalnych incydentów jest infrastruktura fizyczna, a więc budynki, systemy kontroli dostępu czy sprzęt IT. Jak pod tym względem chronione są polskie firmy?

Niestety, również w tym obszarze stosunkowo łatwo przestępcom znaleźć luki bezpieczeństwa. Blisko połowa firm w Polsce nadaje uprawnienia administracyjne osobom spoza zespołu IT. Podwyższone uprawnienia powinny być ściśle kontrolowane a jednak tak się nie dzieje. Niewłaściwe wykorzystanie podwyższonych uprawnień często ułatwia instalację złośliwego oprogramowania lub dokonanie nieautoryzowanych zmian w systemach.

Ponadto, jedynie 59% firm rejestruje wejścia osób do siedziby firmy, co sugeruje, że około jedna trzecia przedsiębiorstw naraża się na możliwość nieuprawnionego wejścia i dokonania kradzieży lub szpiegostwa gospodarczego.

Znacząca grupa firm, bo około 30%, prowadzi dość liberalną politykę korzystania ze sprzętu prywatnego do celów pracowniczych. Tego typu polityka może doprowadzić do niekontrolowanego wycieku danych lub instalacji złośliwego oprogramowania.

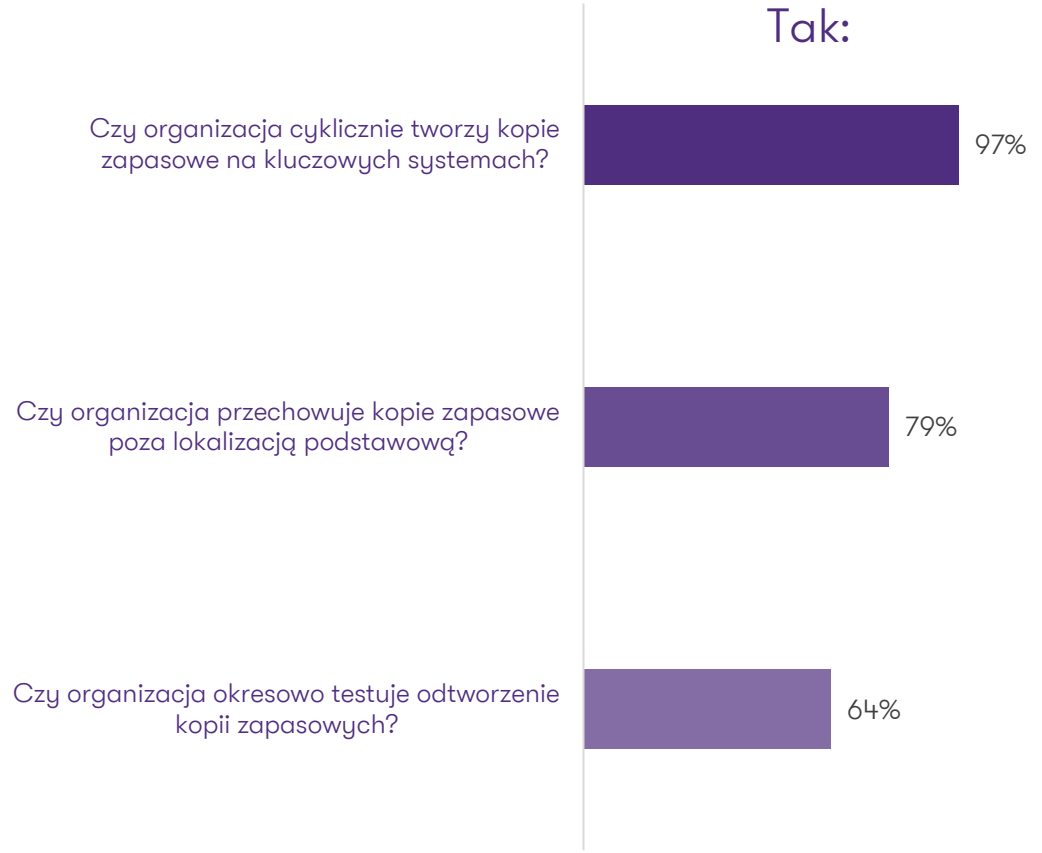


Większość firm dba o kopie zapasowe

Kluczem do opanowania sytuacji kryzysowej jest w wielu przypadkach posiadanie dobrze zabezpieczonej kopii zapasowej. Większość firm je posiada, choć pewne ryzyka pozostają niezarządzone.

Według badania, aż 97% ankietowanych firm regularnie tworzy kopie zapasowe kluczowych danych i systemów. To wysoki wynik – pokazuje, że firmy mają świadomość tego, jak ważna jest ochrona danych. Warto jednak zwrócić uwagę, że 21% przedsiębiorstw tworzy kopie zapasowe w ten samej lokalizacji, w której przechowywane są dane podstawowe. Oznacza to, że w przypadku incydentu mającego wpływ na fizyczną lokalizację, jedna piąta przedsiębiorstw nie będzie miała możliwości skutecznego odtworzenia danych.

Co więcej, 36% firm nie testuje regularnie procedury odtworzenia kopii zapasowych. Te firmy, pomimo posiadania kopii zapasowych mogą mieć kłopot z procesem odtworzenia danych z tych kopii i szybkiego powrotu do działania w przypadku incydentu związanego z utratą danych np. ataków ransomware.



Dostawcy mogą być źródłem problemu

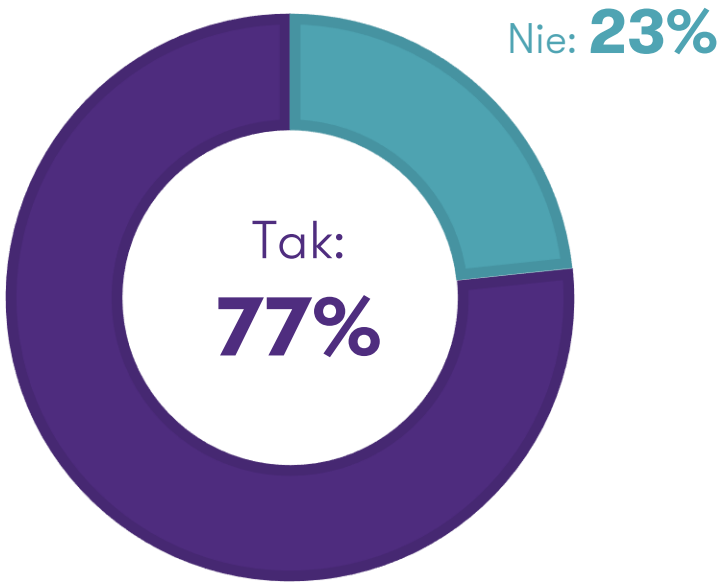
Ponad 50% ataków* w organizacjach dokonywanych jest za pośrednictwem kontrahentów i dostawców.

Warto mieć świadomość, że najwięcej ataków cybernetycznych nie jest prowadzonych bezpośrednio, poprzez ingerencję w systemy ofiary, a pośrednio, poprzez atak na dostawców zewnętrznych i zaufanych partnerów biznesowych. Wiele firm nie zdaje sobie sprawy, że za jednym dostawcą może kryć się sieć współzależnych organizacji i poddostawców.

Poprzez atak na dostawców, wykorzystując relację zaufania, cyberprzestępcy są w stanie przedostać się do naszej firmy i wywołać w niej katastrofalne skutki. Warto podkreślić, że aż 77% ankietowanych przez nas firm posiada usługi zewnętrznych dostawców IT. Spośród nich 16% nie ma podpisanych umów zawierających sprecyzowane parametry realizacji usługi (ang. service level agreement, SLA), a 39% nie ma w umowach zapisu dotyczącego kar przewidzianych w razie błędów po stronie dostawcy. Jednakże 92% firm zawiera w umowach z dostawcami zasady dotyczące przetwarzania danych osobowych i poufności. Jednocześnie rzadko nakładane są na dostawców obowiązki informowania o incydentach bezpieczeństwa, których skutki przecież mogą dotknąć również nas.

*źródło: https://newsroom.trendmicro.com/

Czy organizacja posiada dostawców zewnętrznych w obszarze IT?

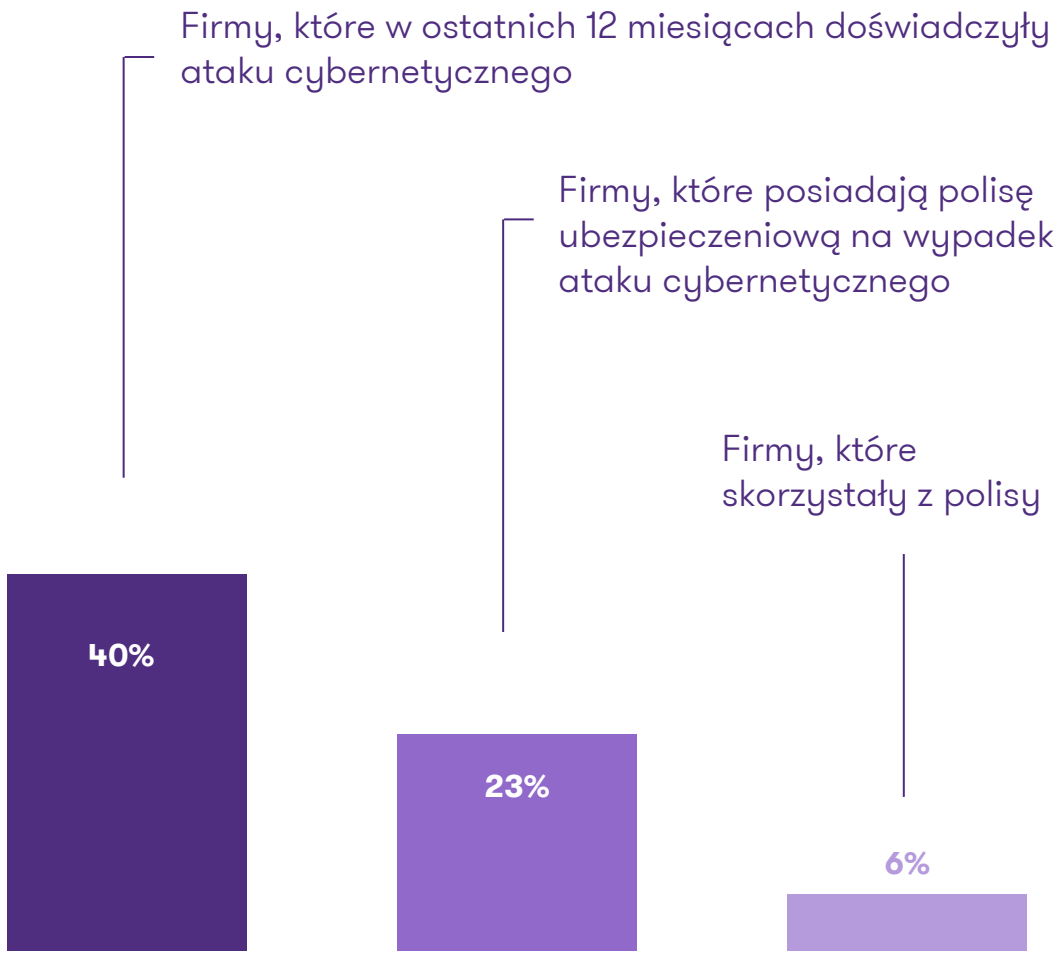


Cyberpolisy to wśród firm nadal rzadkość

Mniej niż 23% badanych przedsiębiorstw deklaruje, że posiada wykupioną polisę na wypadek incydentu cybernetycznego, a tylko 6% z niej skorzystało.

Choć polskie firmy – jak same przyznają – często padają ofiarami ataków cybernetycznych, to nadal stosunkowo rzadko ubezpieczają się na taką okoliczność. Tylko 23% ankietowanych przez nas firm przyznało, że posiada aktywną polisę ubezpieczeniową od ataków cybernetycznych i ich skutków.

Co więcej, tylko 6% skorzystało z tej polisy. Tak niewielki odsetek może częściowo wynikać z faktu, że część incydentów nie przyniosła istotnych negatywnych skutków dla firmy, ale częściowo może wynikać z faktu, że firma nie dopełniła zobowiązań wynikających z zapisów polisy, czyli nie utrzymywała określonych w polisie procedur bezpieczeństwa, np. dotyczących wymagań w zakresie zabezpieczeń czy nie wykonywała czynności wynikających z danej procedury. W efekcie spotkała się z odmową wypłaty odszkodowania.



Firmy nadal niegotowe na dyrektywę NIS-2

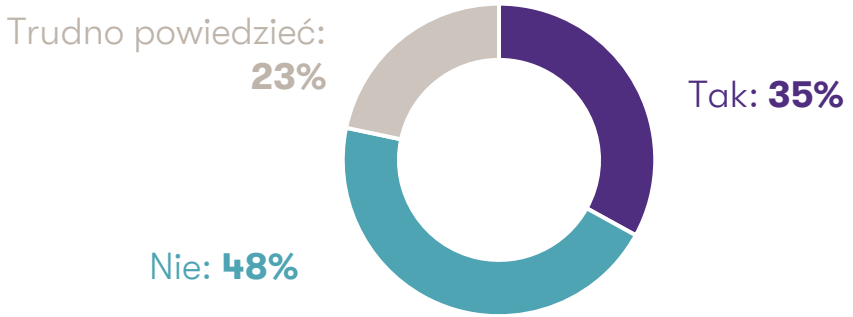
Aż 48% przedsiębiorstw jeszcze nie zweryfikowało, czy podlega pod dyrektywę NIS2. A firmy, które podjęły taki wysiłek uznały, że to dla nich zbyt skomplikowane.

Dyrektywa NIS2 (Network and Information System Directive 2) to unijna regulacja mająca zapewnić bezpieczeństwo cybernetyczne we wszystkich krajach Unii Europejskiej. Nakłada na organizacje, w tym firmy prywatne, rygorystyczne obowiązki dotyczące zarządzania ryzykiem i raportowania incydentów. Dyrektywa weszła w życie 16 stycznia 2023 roku, a w 2025 zostanie wprowadzona do polskiego systemu prawnego.

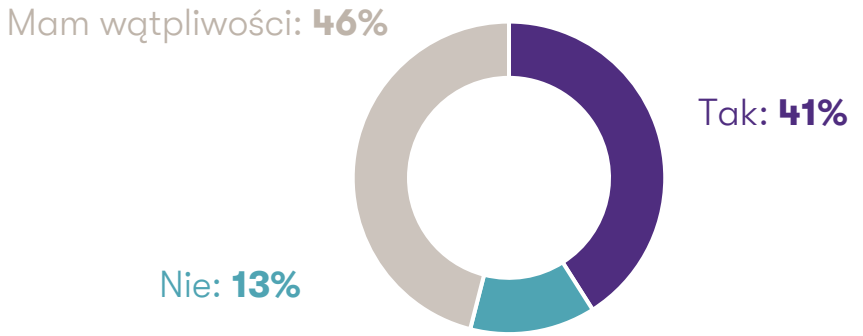
Według naszego badania, aż 48% firm nadal nie ustaliło, czy podlega pod obowiązki wprowadzane przez NIS2. Zrobiło to tylko 35% ankietowanych firm. Prawie połowa (48%) jeszcze tego nie zrobiła, a 23% ankietowanych nie potrafiło udzielić odpowiedzi.

Spośród firm, które przeprowadziły weryfikację podlegania pod dyrektywę, aż 46% twierdzi, że mają wątpliwości, czy pod nią podlegają i w jakim zakresie, a 41% firm ustaliło, że dyrektywa ich obowiązuje. Tylko w 13% weryfikacja przyniosła odpowiedź negatywną i dyrektywa ich nie dotyczy. Płynie z tego wniosek, że niepewność jest duża i wynika z braku zrozumienia wymagań.

Czy weryfikowałeś już, czy podlegasz pod obowiązki wynikające z implementacji NIS2 w Polsce?



Czy w wyniku tej weryfikacji okazało się, że firma podlega pod NIS2?



Naszym zdaniem

Istnieje duża rozbieżność w poziomie dojrzałości i podejściu do cyberbezpieczeństwa pomiędzy dużymi a mniejszymi firmami. Większe przedsiębiorstwa od lat z różnych powodów zmuszone są do stałego podnoszenia poziomu zabezpieczeń, podczas gdy u tych mniejszych można zauważyć skutki zaciągniętego długu technologicznego. Jednak i dużym graczom zdarza się przeoczyć wdrożenie niezbędnych zabezpieczeń, procedur albo też takie firmy bezgranicznie ufają zespołom IT, nie weryfikując w sposób niezależny stanu faktycznego. Wniosek, który płynie z naszego Raportu dla polskich firm jest jeden: w obliczu nadchodzących zmian regulacyjnych oraz krajobrazu zagrożeń, należy jak najszybciej wykonać niezbędne działania w kontekście zmian środowiska IT i przygotować się na najgorsze. Wiara, że nas to nie dotyczy nie tylko nie pomoże, ale może wprost doprowadzić do bardzo dotkliwych skutków, które w przypadku pojedynczego incydentu sięgają setek tysięcy a nawet milionów złotych.

Hubert Bekasiewicz
Specialist
Cybersecurity
Grant Thornton

Szukasz nowych rozwiązań biznesowych?

Skontaktuj się z nami!

Adam Woźniak
Executive Director
Cybersecurity
Grant Thornton
T +48 600 805 785
E Adam.Wozniak@pl.gt.com

Hubert Bekasiewicz
Specialist
Cybersecurity
Grant Thornton
T +48 531 507 437
E Hubert.Bekasiewicz@pl.gt.com

Kontakt dla mediów:

Jacek Kowalczyk
Dyrektor Marketingu i PR
Grant Thornton
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 62 tys. pracowników.

W Polsce działamy od 1993 roku. Zespół 1100 pracowników wspiera naszych klientów w obszarach takich jak doradztwo podatkowe, finansowe, prawne i transakcyjne, audyt, czy outsourcing kadr i płac oraz outsourcing księgowości.

W skład grupy wchodzi m.in. **Grant Thornton Technology**, spółka specjalizująca się w doradztwie dla firm w zakresie outsourcingu IT i cyberbezpieczeństwa, obsługująca kilkaset przedsiębiorstw rocznie w całej Polsce.