CYBERBEZPIECZEŃSTWO FIRM

Raport z badania

ORGANIZATORZY PROJEKTU:

CHUBB

cuberesearch

EY
Building a better working world

PARTNERZY PROJEKTU:

BIGRAM
search • career • HR

Helion

Dlaczego zbadaliśmy temat cyberbezpieczeństwa firm?

Fakt, że do sieci podłączone są miliardy ludzi, firm i urządzeń rodzi zagrożenia na nieznaną dotąd skalę.

W rozwój technologii wpisany jest rozwój zagrożeń. Każdego dnia powstają nowe rozwiązania, nowe zabezpieczenia, ale także pojawiają się nieznane dotąd ryzyka. Technologie i zagrożenia te sprzed jeszcze kilku lat, od obecnych dzieli przepaść. Fakt, że do sieci podłączone są miliardy ludzi, firm i urządzeń rodzi zagrożenia na nieznaną dotąd skalę.

Wiedza w dziedzinie cyberzagrożeń i sposobów zabezpieczania się przed nimi dezaktualizuje się codziennie, w związku z tym skazani jesteśmy na codzienne szukanie skuteczniejszych działań prewencyjnych, właściwszych metod identyfikacji zagrożeń oraz lepszych procedur postępowania w sytuacji wystąpienia incydentu.

Czy firmy zdają sobie sprawę ze stojących przed nimi wyzwań w zakresie zapewnienia cyberbezpieczeństwa? Czy metody i procedury, które stosują pozwalają im spać spokojnie? Czy wreszcie, pracownicy firm, o których specjaliści od zabezpieczeń mówią, że stanowią najsłabsze ogniowo łańcucha, rzeczywiście są największym zagrożeniem dla cyberbezpieczeństwa i co zrobić, żeby ich negatywną rolę zminimalizować?

Postanowiliśmy poszukać odpowiedzi na te pytania wśród właścicieli firm oraz osób, które są w tych przedsiębiorstwach odpowiedzialne za bezpieczeństwo cybernetyczne. Mamy nadzieję, że niniejszy raport choć w niewielkim stopniu przyczyni się do zwiększenia cyberbezpieczeństwa Państwa firm.

Zapraszamy do lektury.

Dr Michał Pastuszka
Prezes Zarządu CubeReseach

O badaniu

O badaniu

Zasadniczym celem badania było uzyskanie aktualnych danych związanych z tematem cyberbezpieczeństwa firm. Czy firmy zdają sobie sprawę ze stojących przed nimi wyzwań w zakresie zapewnienia cyberbezpieczeństwa? Czy metody i procedury, które stosują pozwalają im spać spokojnie? Czy pracownicy rzeczywiście stanowią największe zagrożenie dla cyberbezpieczeństwa i co zrobić, żeby zminimalizować ich negatywną rolę?

Badanie składało się z dwóch części – badania zasadniczego, gdzie na zadane pytania odpowiadały osoby na co dzień zajmujące się problematyką cyberbezpieczeństwa firm oraz badania dodatkowego zrealizowanego na pracownikach firm.

W niniejszym raporcie przedstawiamy głównie wyniki badania zasadniczego, w niektórych miejscach konfrontując je z wynikami badania dodatkowego – wtedy każdy z wykresów opatrzony jest stosowną informacją. Autorami badania są konsultanci Cube Research we współpracy z firmą EY oraz Chubb.

Metodyka i próba

Obie części badania zrealizowane zostały za pomocą metody łączonej: wywiady telefoniczne CATI (Computer Assisted Telephone Interview) oraz wywiady online CAWI (Computer Assisted Web Interview).

Badanie było przeprowadzane w zależności od preferencji respondenta telefonicznie lub za pośrednictwem internetu.

Badanie zasadnicze zrealizowano w listopadzie 2016 na próbie 350 firm.

Badanie dodatkowe zrealizowano na próbie 500 pracowników zatrudnionych w polskich firmach. Struktura próby badania dodatkowego odpowiadała strukturze próby badania zasadniczego.

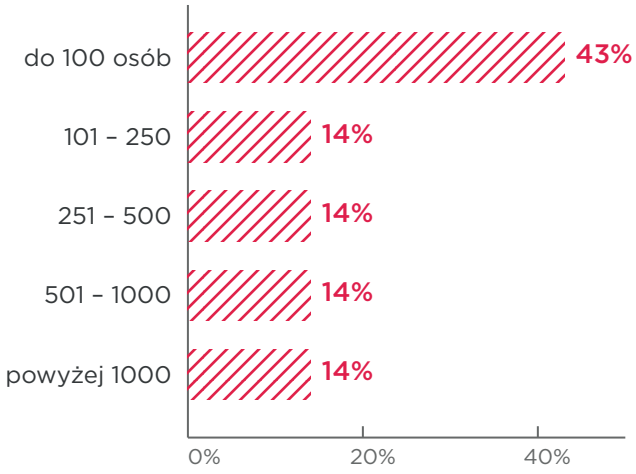
Zatrudnienie

Największą grupę wśród badanych – ponad dwie piąte (43%) stanowiły firmy zatrudniające do 100 pracowników.

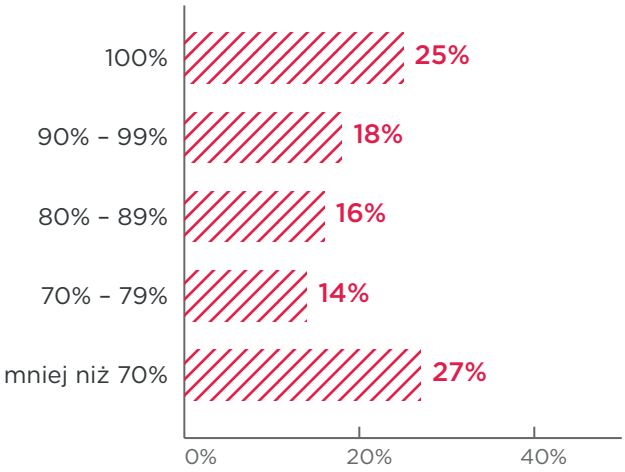
Firmy zatrudniające od 101 do 250 osób stanowiły 14% próby, również 14% firmy zatrudniające od 251 do 500 osób. Taki sam odsetek (14%) stanowiły firmy zatrudniające od 501 do 1000 osób i firmy zatrudniające powyżej 1000 pracowników.

Tylko w nieco ponad jednej czwartej firm (27%) pracownicy mający dostęp do infrastruktury IT (poprzez komputer) lub smartfon stanowią mniej niż 70% pracowników. Czyli zdecydowana większość, bo ponad 70% firm daje dostęp do swojego systemu IT przynajmniej 70% pracowników. W przypadku jednej czwartej badanych firm (25%) wszyscy pracownicy mają dostęp do infrastruktury IT.

Ile osób zatrudnia Państwa firma?



Jaki procent pracowników Państwa firmy posiada dostęp do infrastruktury IT – komputer, smartfon etc.?



Wyniki badania

Wstęp

Od kilkunastu lat zajmuję się walką z nadużyciami i przestępczością. Widzę wyraźny trend przenoszenia ciężaru popełnianych nadużyć, w tym kradzieży pieniędzy i danych, w obszarach cyfrowej rzeczywistości. Hakerzy już dawno przestali być romantykami, przełamującymi zabezpieczenia komputerowe w szczytnym celu. Teraz zarabiają na kradzieży danych lub wymuszaniu okupów za zaszyfrowane dane, często działając w zorganizowanych, międzynarodowych grupach przestępczych.

Jest to pokłosiem naszego uzależnienia od systemów IT, które występują wszędzie. Nosimy je ze sobą (smartfony, inteligentne zegarki), korzystamy z nich w domu i biurze, coraz częściej mamy je wbudowane w urządzenia ułatwiające życie. Im więcej codziennych czynności bazuje na IT, tym większe prawdopodobieństwo intensyfikacji działań przestępczych.

Ponieważ przestępcy pojawiają się tam, gdzie są pieniądze, widzimy niesłabnące ataki na sektor finansowy. Z drugiej strony banki, posiadające historycznie najlepsze zabezpieczenia, wymagają od cyberprzestępców poświęcenia większej ilości czasu i nakładów. Ale może prościej jest atakować firmy z branż tradycyjnie uważanych za mniej atrakcyjne i w związku z tym słabiej zabezpieczone przed atakami cyberprzestępców? Tym pytaniem chciałbym otworzyć dyskusję nad poniższym raportem.

Tomasz Dyrda
Dyrektor w Zespole
Zarządzania Ryzykiem Nadużyć, EY

Powszechność zagrożeń związanych z cyberatakami

Badanie cyberbezpieczeństwa firm rozpoczęliśmy od podstawowego pytania o to, jak nasi respondenci oceniają swoje bezpieczeństwo cyfrowe.

Zdajemy sobie sprawę, że dokonanie takiej oceny w sposób rzetelny nie jest łatwe, bo tak naprawdę nie istnieją dobre mierniki, które w sposób pełny i odpowiedzialny informowałyby o tym, czy firma jest bezpieczna czy nie. Otrzymane wyniki to potwierdzają i stanowią obraz subiektywnego poczucia bezpieczeństwa wyrażonego przez respondentów. Średnia ocen respondentów w skali od 1 do 7 mieści się nieco powyżej polowy skali. Najbardziej bezpiecznie badani czują się w obszarach, które ich zdaniem lepiej kontrolują w sposób fizyczny – czyli za pomocą sprzętu i oprogramowania, wewnętrznej infrastruktury czy stacji roboczych. Zdecydowanie mniej bezpiecznie czują się w obszarach ataków na swoich klientów, ataków socjotechnicznych, wrogich działań związanych z publicznie dostępnymi usługami (np. strony www) czy też w obszarze „cloud".

Firmy powoli zaczynają przyzwyczajać się do tego, że coraz częściej są zmuszone do mierzenia się z atakami cybernetycznymi. Najczęstszymi incydentami bezpieczeństwa wymienianymi przez naszych badanych były ogólne ataki malwarowe (68% badanych firm), przypadkowe (najczęściej) działania pracowników (44% badanych) oraz utrata danych z powodu awarii sprzętu (39%). Wymienione wyżej incydenty są również zdaniem respondentów największymi zagrożeniami dla ich firm.

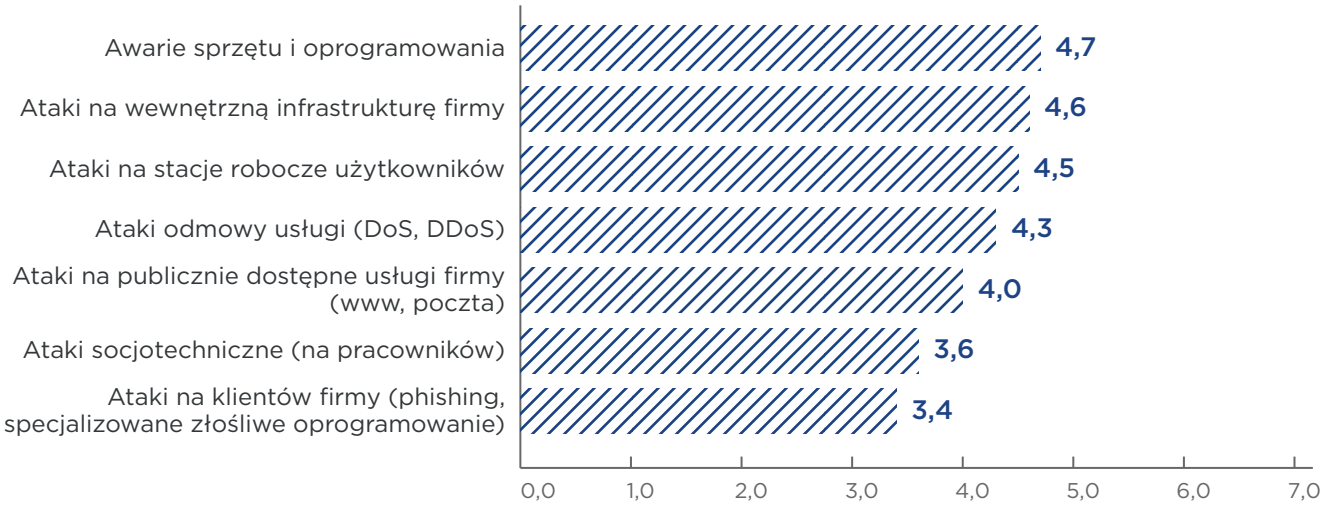
Ocena bezpieczeństwa IT

Największe obawy budzi atak (phishing, wyspecjalizowane złośliwe oprogramowanie) na klientów firmy, gdzie ocena bezpieczeństwa wyniosła 3,4 – czyli minimalnie poniżej połowy skali.

Zagrożenie atakami socjotechnicznymi na pracowników jest oceniane na odrobinę mniejsze – 3,6, czyli minimalnie powyżej środka skali. Przedsiębiorcy nieco mniej boją się ataków na publicznie dostępne usługi firmy (www, poczta) – średnia ocena 4. Jeszcze mniej obawiają się ataków odmowy usługi (DoS, DDoS) – średnia 4,4.

Na kolejnych pozycjach, budzących mniej obaw znalazły się kolejno: ataki na stacje robocze użytkowników (4,5), ataki na wewnętrzną infrastrukturę firmy (4,6), awarie sprzętu i oprogramowania (4,7).

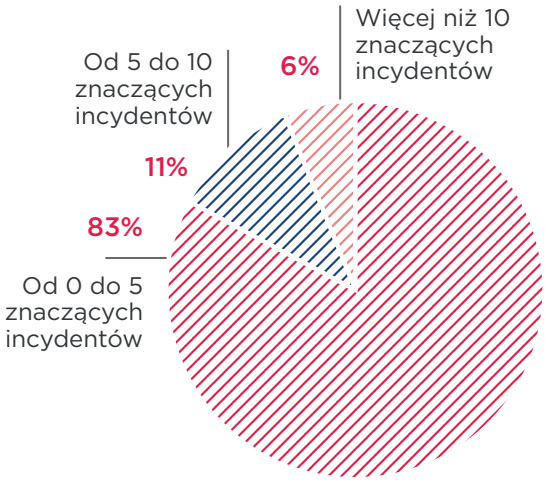
Jak na skali od 1 do 7 (1 oznacza ogromne zagrożenie, a 7 pełne bezpieczeństwo) ocenia Pan(i) stan bezpieczeństwa Państwa firmy w kontekście cyberbezpieczeństwa?



Liczba incydentów w minionym roku

Dominująca większość firm, w ciągu ostatnich 12 miesięcy, zanotowała od 0 do 5 znaczących incydentów naruszenia bezpieczeństwa (83%). Tylko jedna na dziewięć firm padła ofiarą od 5 do 10 incydentów, a 6% – więcej niż 10 incydentów.

Ile incydentów bezpieczeństwa odnotowali Państwo w ciągu ostatnich 12 miesięcy?



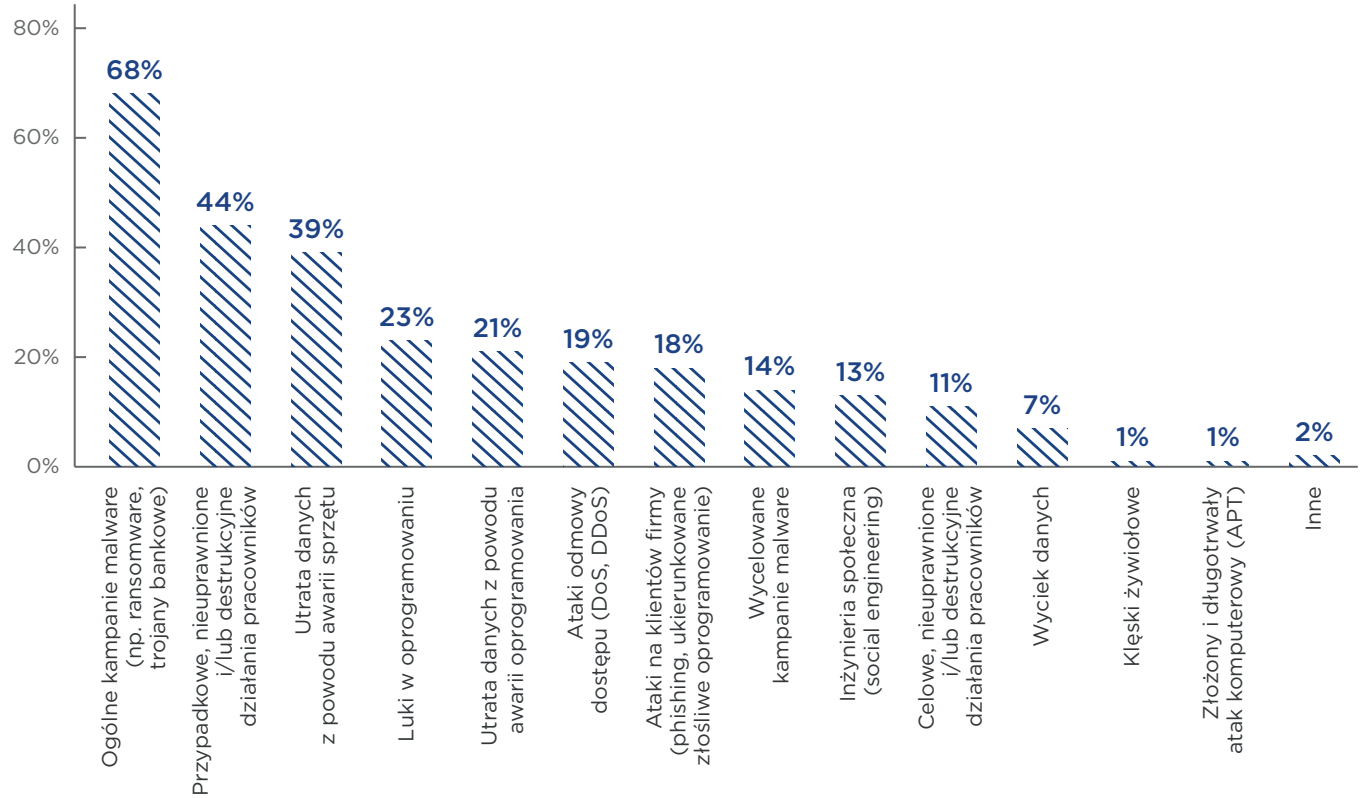
Typy incydentów

Wśród incydentów naruszania bezpieczeństwa, większości firmom zdarzyła się styczność z ogólną kampanią malware (randomware, trojany bankowe) – 68%. Około dwie piąte doświadczyło przypadkowych, nieuprawnionych i/lub destrukcyjnych działań pracowników (44%) oraz utraty danych z powodu awarii sprzętu (39%).

Około jedna piąta firm doświadczyła utraty danych z powodu awarii oprogramowania (21%), ataków odmowy dostępu (19%) lub ataków na klientów firmy (18%). Co siódma firma stała się celem specjalnie ukierunkowanych kampanii malware (14%), co ósma – inżynierii społecznej (13%), co siódma – celowych działań pracowników (11%).

7% badanych ucierpiało z powodu wycieku danych, a pozostałe typy incydentów występowały jedynie w minimalnej liczbie firm.

Z jakiego typu incydentami mieli Państwo do czynienia?



Największe zagrożenia

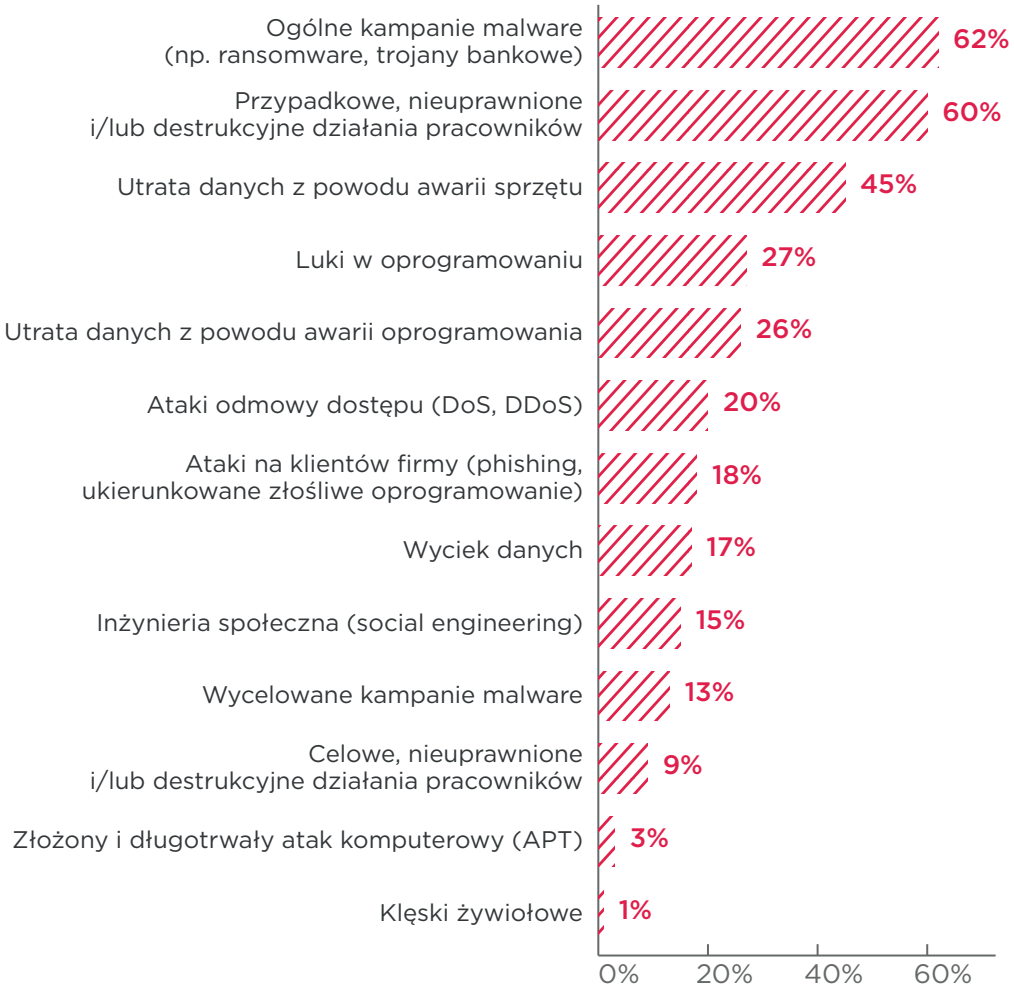
Wśród najbardziej istotnych zagrożeń znaczna większość (62%) wymieniła: ogólne kampanie malware oraz (60%) przypadkowe, nieuprawnione i/lub destrukcyjne działania pracowników. Nieco mniej niż połowa (45%) – utratę danych z powodu awarii sprzętu. Pozostałe zagrożenia jako najistotniejsze widzi znacznie mniejszy odsetek firm.

Około jedna trzecia firm wymienia luki w oprogramowaniu (27%) i utratę danych z powodu awarii oprogramowania (26%). Blisko jedna piąta firm postrzega jako największe zagrożenie: ataki odmowy dostępu (20%), ataki na klientów (18%) oraz wyciek danych (17%).

Co siódma firma najbardziej boi się inżynierii społecznej (15%), co ósma wycelowanych kampanii malware (13%), a mniej niż co dziesiąta celowych, nieuprawnionych i/lub destru-kcyjnych działań pracowników.

Pozostałe zagrożenia, o które pytano – złożone ataki (APT) i klęski żywiołowe zostały wymienione przez mniej niż co dwudziestą firmę.

Które z wymienionych niżej zagrożeń ocenia Pan(i) jako najbardziej istotne z punktu widzenia Państwa firmy?



Komentarz:
Powszechność ataków

Często pytamy naszych klientów o to, czy wydarzył się w ich firmie incydent lub atak hakerski. Zdarza się, że nie dostajemy odpowiedzi na to pytanie, choć podejrzewamy jak ta odpowiedź może brzmieć. Jak widzimy w przeprowadzonym badaniu, zdecydowana większość organizacji miała do czynienia z cyberatakami.

Natomiast wciąż zdarza nam się słyszeć, że danej firmy „cyberataki nie dotyczą". Warto się wtedy zastanowić – czy tak faktycznie jest, czy też może dana firma jest już ofiarą cyberprzestępców, ale jeszcze o tym nie wie.

Bez względu na to, czy jesteśmy dużą lub małą firmą, instytucją publiczną czy osobą fizyczną – cyberprzestępczość też nas dotyczy: środowiska IT firmy, naszych prywatnych danych, ale też danych naszych klientów. Żeby lepiej się chronić i szybciej reagować na ataki, musimy zaakceptować fakt, że jesteśmy na celowniku cyberprzestępców.

Tomasz Dyrda
EY

Komentarz:
Wykrywanie incydentów (detekcja), fałszywe poczucie bezpieczenstwa

Wyniki tego, ale i wielu innych badań wskazują, że firmy nie radzą sobie z wykrywaniem incydentów bezpieczeństwa. Firmy identyfikują bardzo mało incydentów, a wśród tych wykrytych dominują łatwe do zaobserwowania incydenty, takie jak infekcja ransomware czy utrata danych w wyniku awarii. Pojawia się obawa czy brak poczucia zagrożenia nie wynika właśnie z braku możliwości zaobserwowania samych incydentów. Byłoby to zatem fałszywe poczucie bezpieczeństwa, które może prowadzić do zaniedbań w tym obszarze.

Aleksander Ludynia
Starszy Menedżer
w Zespole Zarządzania Ryzykiem
Informatycznym, EY

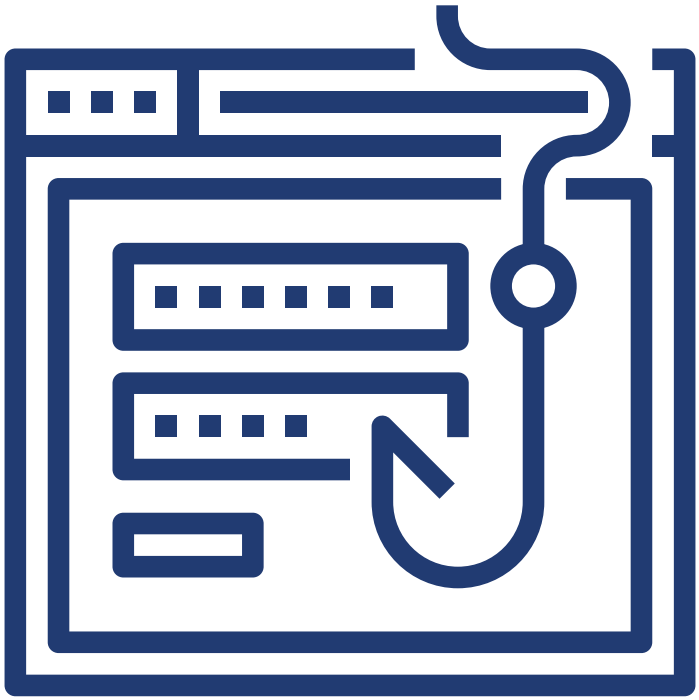
Czy człowiek jest rzeczywiście najsłabszym ogniwem?

Firma jest tak bezpieczna jak bezpieczne jest jej najsłabsze ogniowo. Nie jest zaskoczeniem, że większość badanych za najsłabsze ogniowo uważa nie sprzęt, oprogramowanie czy procedury, ale człowieka, pracownika firmy. Dane te doskonale korespondują z wynikami badań publikowanymi zarówno w Polsce, jak i innych krajach. Na całym świecie eksperci uważają, że człowiek stanowi najsłabszy punkt w systemie zabezpieczeń.

Tyle, że taka konstatacja nie tylko nie rozwiązuje problemu firm, ale wręcz nakłada na nie większe obowiązki w zakresie uświadomienia pracownikom istnienia cyberzagrożeń i sposobów radzenia sobie z nimi.

Tymczasem badanie, które przeprowadzono w ramach niniejszego projektu na pracownikach firm wykazuje, że w tym zakresie sytuacja daleka jest od ideału. Aż 41% badanych pracowników firm twierdzi, że nigdy nie przeszło w tym zakresie żadnego szkolenia. Gdy dodamy do tego 11%, które szkolenie przeszło w ciągu ostatnich 2 lat lub dawniej, widać wyraźnie, że firmy mają w tym zakresie duże zaległości.

Nasze badanie pokazuje, że 40% badanych pracowników ocenia cyberbepieczeństwo firm, w których pracują na 4 lub mniej w skali 7-stopniowej. Trudno się temu dziwić, skoro 30% badanych twierdzi, że w firmie nie istnieją żadne procedury dotyczące bezpieczeństwa.



Przyczyny incydentów

Nieznaczna większość respondentów wskazuje pracowników jako sprawców incydentów (64%). Nieco więcej niż połowa przyczyny upatruje w przestępcach komputerowych (57%).

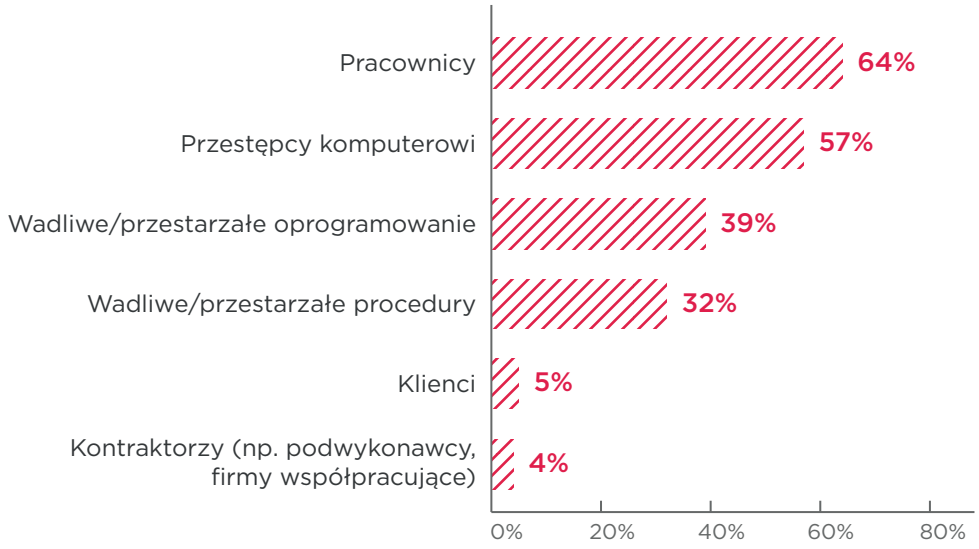
Dwie piąte badanych wini wadliwe bądź przestarzałe oprogramowanie (39%), zaś jedna trzecia przestarzałe lub wadliwe procedury (32%). Znikomy odsetek jako sprawców incydentów wymienia klientów (5%).

Szkolenia w zakresie cyberbezpieczeństwa

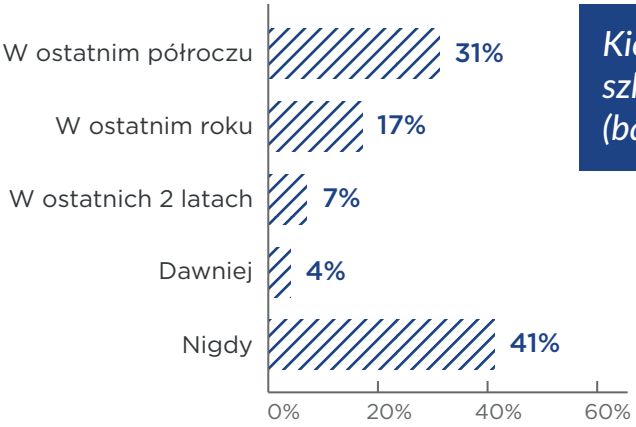
Aż 41% badanych pracowników firm stwierdziło, że w ich firmach nigdy nie odbyło się szkolenie w zakresie cyberbezpieczeństwa. W 17% przypadków badani deklarują, że szkolenie odbyło się w ciągu ostatniego roku, a 11%, że takie szkolenie odbyło się w ciągu ostatnich 2 lat lub nawet dawniej.

Tylko około jedna trzecia (31%) to pracownicy firm, w których szkolenie odbyło się w ciągu ostatniego pół roku.

Kto/co jest najczęstszą przyczyną incydentów?



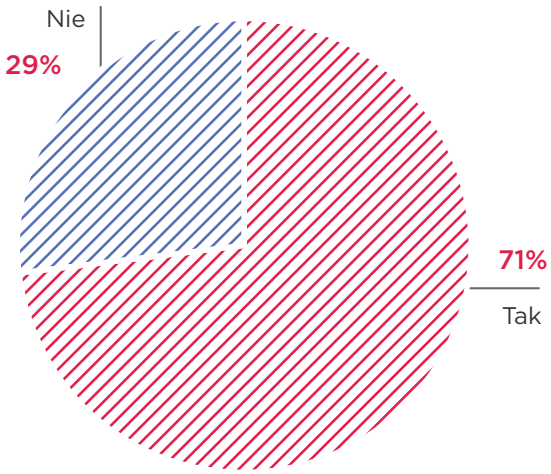
Kiedy ostatnio w Pana(i) firmie miał(a) Pan(i) szkolenie w zakresie cyberbezpieczeństwa? (badanie na pracownikach firm)

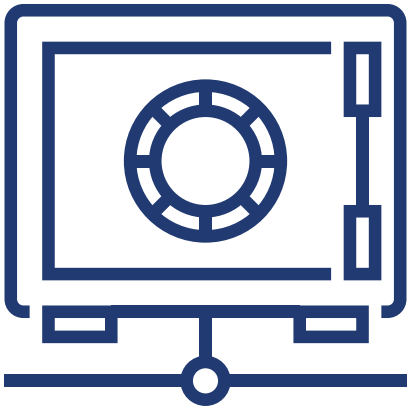


Procedura opisująca zasady bezpieczeństwa IT

Ponad dwie trzecie badanych (71%) deklaruje, że w ich firmach istnieje znana im procedura opisująca zasady bezpieczeństwa. 29% respondentów twierdzi, że w ich firmach takiej procedury nie ma.

Czy w Pana(i) firmie istnieje znana Panu(i) procedura opisująca zasady bezpieczeństwa IT? (badanie na pracownikach firm)





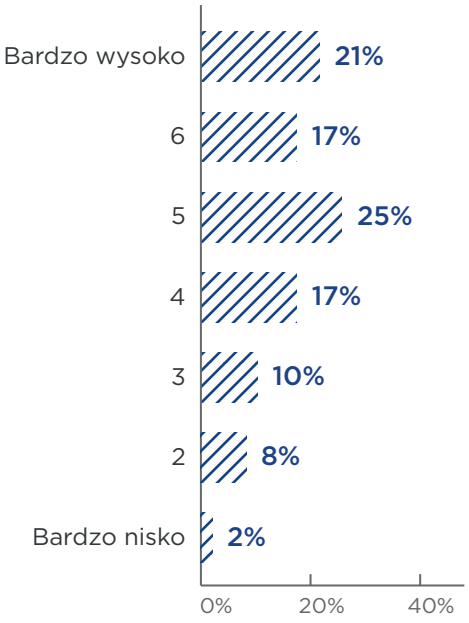
Poziom bezpieczeństwa IT

Prawie co piąty badany (21%) ocenia poziom bezpieczeństwa IT w jego firmie na bardzo wysoki – 7 punktów w skali od 1 do 7.

W przypadku 17% ocena wynosi - 6 punktów, 25% - 5 punktów, 17% - 4 punkty.

Poniżej wartości środkowej znajduje się co piąty badany. I tak 10% oceniło bezpieczeństwo IT na 3 punkty, 8% na 2 punkty, a 2% na 1 punkt.

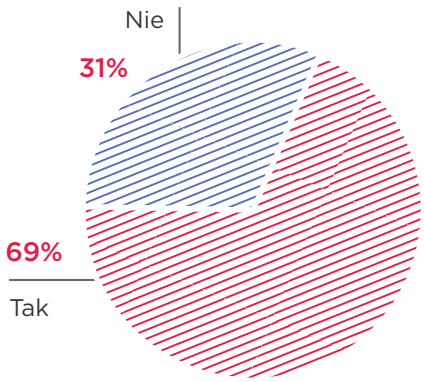
Jak ocenia Pan(i) poziom bezpieczeństwa IT w Pana(i) firmie? (badanie na pracownikach firm)



Okresowe informacje na temat IT

Ponad dwie trzecie respondentów (69%) otrzymuje okresowe informacje dotyczące bezpieczeństwa IT. W 31% tego typu informacji nie ma.

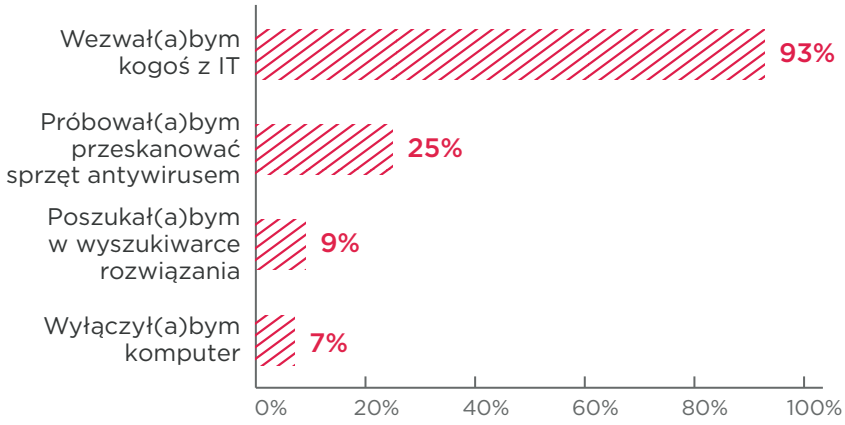
Czy dostaje Pan(i) okresowe informacje dotyczące bezpieczeństwa IT (maile, biuletyny)? (badanie na pracownikach firm)



Reakcja na atak złośliwego oprogramowania

Typową reakcją na atak złośliwego oprogramowania jest wezwanie kogoś z działu IT. Tak postąpiłoby aż 93% badanych. Jedna czwarta (25%) starałaby się we własnym zakresie przeskanować sprzęt programem antywirusowym, co dziesiąty (9%) szukałby pomocy w wyszukiwarce internetowej, a 7% badanych wyłączyłoby komputer.

Co zrobił(a)by Pan(i) w przypadku ataku złośliwego oprogramowania w miejscu pracy? (badanie na pracownikach firm)



Komentarz: Element ludzki

Nie można badać problematyki cyberprzestępczości bez próby identyfikacji najsłabszego ogniwa w kontekście technologia vs człowiek.

Niestety, człowiek jest najsłabszym ogniwem, a popełniane przez nas błędy ułatwiają lub umożliwiają skuteczne ataki cyberprzestępców. Jest to w znacznej mierze efekt tego, jak poważnie traktujemy kwestię bezpieczeństwa IT i cyberprzestępczości, bez względu na to, czy jesteśmy „zwykłym" użytkownikiem czy też ekspertem od IT.

Badanie pokazuje, że fakt przeszkolenia z zakresu bezpieczeństwa IT, złożenia deklaracji przestrzegania zasad, sporadycznego odświeżania wiedzy, działanie według zasady: „przecież podpisaliśmy procedurę.... " nie wystarcza.

Firmy i organizacje regularnie notują incydenty bezpieczeństwa. Listy trywialnych haseł, pokazujące ignorowanie podstawowych zasad ich tworzenia, lekceważenie zaleceń i procedur szyfrowania danych, otwieranie maili phishingowych – to tylko część błędów, które popełniają ludzie, a jednocześnie użytkownicy urządzeń i systemów IT. Powinniśmy w końcu uświadomić sobie, że nawet nie będąc z IT, musimy poważnie traktować świat IT, choćby dlatego, że tam są nasze sekrety i pieniądze.

Tomasz Dyrda
EY

Traktujemy kwestię bezpieczeństwa poważnie, ale bez pomysłu

Informacje na temat cyberzagrożeń goszczą od dłuższego czasu na stałe w mediach i w rozmowach biznesowych. Badani deklarują, że z ich punktu widzenia to ważny temat i że podejmują działania zmierzające do poprawy bezpieczeństwa ich firm. Do takich działań należą audyty, testy bezpieczeństwa czy szkolenia.

Jak wynika z naszych badań tylko 25% respondentów stwierdziło, że nigdy nie przeprowadziło audytu bezpieczeństwa infrastruktury IT. Podobny odsetek deklaruje, że nie prowadzi w firmach żadnych szkoleń w zakresie cyberbezpieczeństwa (o tym więcej w kolejnych rozdziałach raportu). Oznacza to, że około 3/4 traktuje temat bezpieczeństwa firm poważnie. Można się zastanawiać nad tym, czy to rzeczywiście dużo czy mało oraz czy te liczby świadczą o wystarczającym zainteresowaniu kwestiami bezpieczeństwa. Jednak prawdopodobnie o wiele ważniejsze wnioski możemy wyciągnąć po przeanalizowaniu kolejnych kroków podejmowanych przez firmy. A te wskazują, że badani są w swoich działaniach niekonsekwentni.

Samo wykonanie audytu czy szkolenia jest inwestycją, która może służyć bezpieczeństwu, ale jest to tylko pierwszy etap. Aby rzeczywiście zadbać o bezpieczeństwo firmy, poza informacją, co poprawić, potrzebne są kolejne kroki takie jak: zdobycie wiedzy, w jaki sposób wprowadzić zmiany, implementacja konkretnych procedur oraz monitorowanie efektów wprowadzonych zmian.

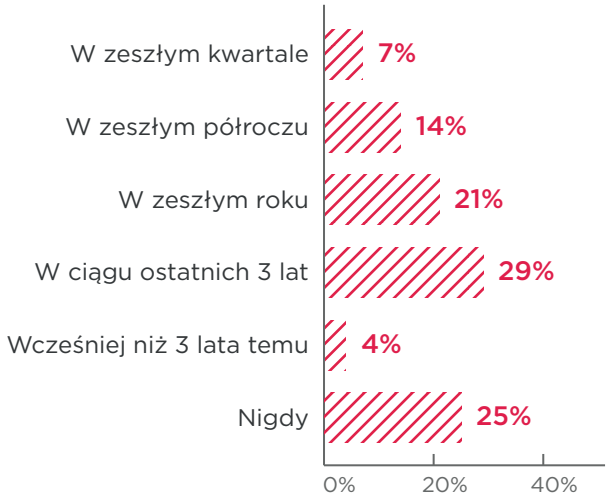
Niestety wygląda na to, że badani wykonują pierwszy krok i przestają działać - ostatecznie jedynie 15% firm wprowadziło wnioski z audytu. Natomiast, aż połowa firm, które prowadzą szkolenia w zakresie cyberbezpieczeństwa nie ma narzędzi pozwalających na weryfikację ich skuteczności.

Audyt bezpieczeństwa infrastruktury IT

W jednej czwartej badanych przedsiębiorstw nigdy nie przeprowadzono audytu bezpieczeństwa infrastruktury IT.

Największą, choć nie dominującą, grupę stanowią firmy, które przeszły taki audyt w ciągu ostatnich 3 lat (29%), dwie piąte firm prowadziło audyt w zeszłym roku (21%), co siódma firma w zeszłym półroczu, a co czternasta w ubiegłym kwartale (7%). Marginalny odsetek ankietowanych przyznał, że audyt infrastruktury IT odbył się u nich więcej niż 3 lata temu (4%).

Kiedy był przeprowadzony ostatni audyt bezpieczeństwa infrastruktury IT?

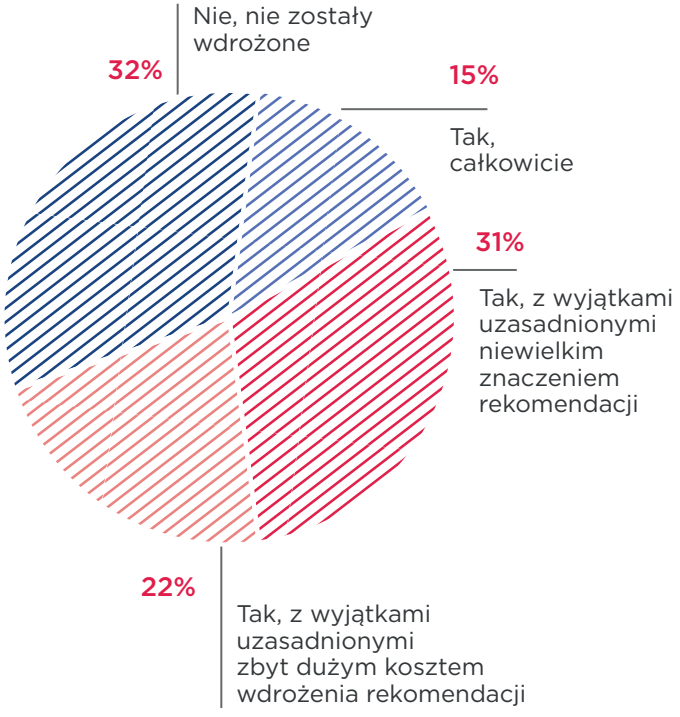


Wnioski z audytu

Ponad jedna trzecia firm przyznała, że nie wdrożyła wniosków z przeprowadzonego audytu (32%). Ponad połowa wdrożyła audyt częściowo: około jedna trzecia z niewielkim wyjątkiem uzasadnionym niewielkim znaczeniem rekomendacji (31%), prawie jedna czwarta z wyjątkiem uzasadnionym zbyt dużym kosztem wdrożenia rekomendacji (22%).

Tylko niespełna jedna siódma firm wdrożyła w pełni wnioski z audytu (15%).

Czy wnioski z audytu zostały wdrożone?



Testy bezpieczeństwa przed wdrożeniem zmian w systemach teleinformatycznych

Dwie piąte badanych firm nie realizuje testów bezpieczeństwa swojej infrastruktury teleinformatycznej (40%). Prawie tyle samo firm realizuje je, ale nieregularnie – w przypadkach uzasadnionych bieżącą potrzebą (36%).

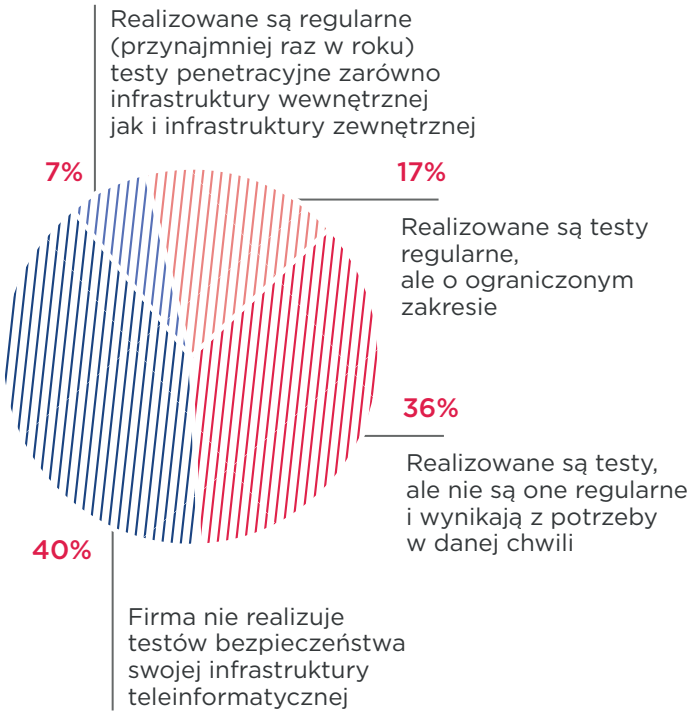
Prawie jedna piąta firm realizuje testy regularnie, ale w ograniczonym zakresie (17%).

Jedynie co czternasta badana firma realizuje regularnie, przynajmniej raz w roku testy penetracyjne zarówno struktury wewnętrznej, jak i zewnętrznej (7%).

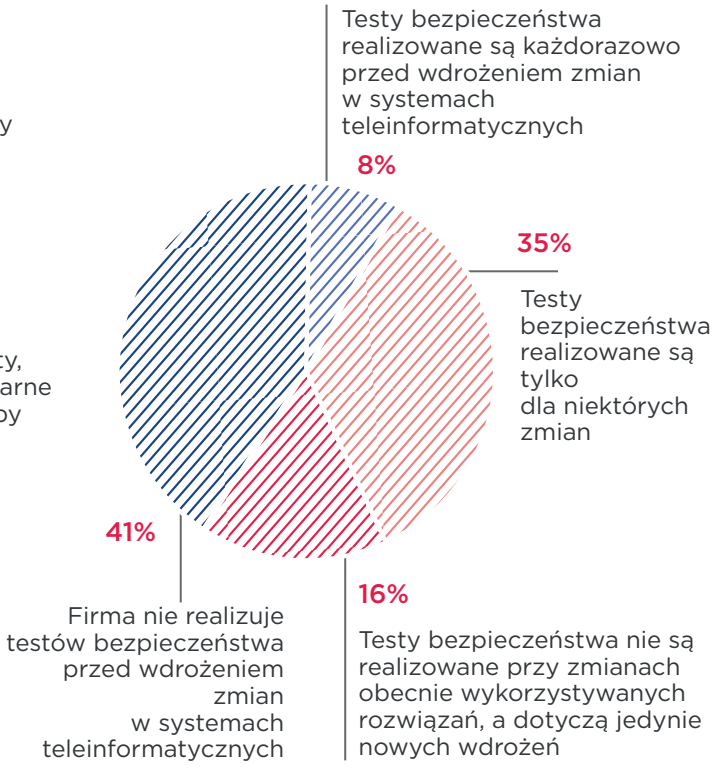
Ponad dwie piąte firm objętych badaniem nie realizuje testów bezpieczeństwa przed wdrożeniem zmian w systemach teleinformatycznych (41%). W przypadku ponad jednej trzeciej – testy bezpieczeństwa realizowane są tylko dla niektórych zmian (35%). W mniej niż jednej piątej firm testy są realizowane jedynie przy zmianach dotyczących nowych wdrożeń (16%).

Tylko co trzynasta firma realizuje testy bezpieczeństwa każdorazowo przed wdrożeniem zmian w systemach informatycznych.

Czy firma realizuje testy bezpieczeństwa swojej infrastruktury?



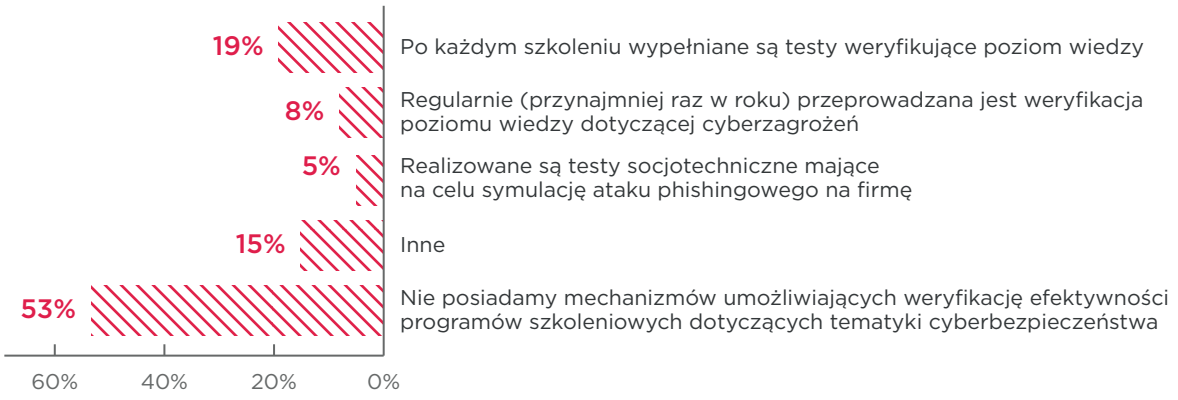
Czy firma realizuje testy bezpieczeństwa przed wdrożeniem zmian w systemach teleinformatycznych?



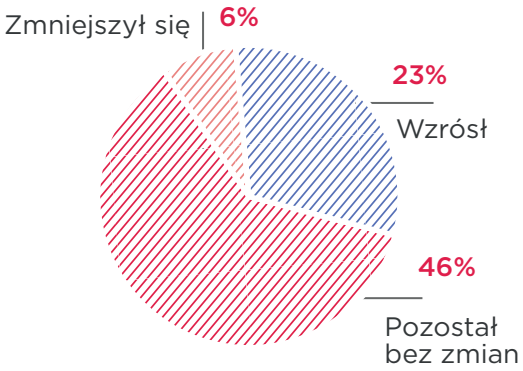
Efektywność szkoleń dotyczących cyberbezpieczeństwa

Ponad połowa badanych firm nie posiada mechanizmów umożliwiających weryfikację efektywności programów szkoleniowych, dotyczących tematyki cyberbezpieczeństwa (53%). W jednej piątej przypadków po każdym szkoleniu wypełniane są testy weryfikujące poziom wiedzy (19%). W 8% przeprowadza się weryfikację poziomu wiedzy dotyczącej cyberzagrożeń regularnie, przynajmniej raz w roku. W jednej dwudziestej badanych firm realizuje się testy socjotechniczne, mające na celu symulację ataku phishingowego na firmę (5%). Odpowiedzi: „inne" udzieliło 15% badanych.

Czy firma posiada zaimplementowane narzędzia umożliwiające zmierzenie efektywności programów szkoleniowych dotyczących tematyki bezpieczeństwa?



Czy w ciągu ostatnich 12 miesięcy w porównaniu z poprzednimi latami budżet przeznaczony na zagadnienia związane z cyberbezpieczeństwem:



Budżet na cyberbezpieczeństwo

W porównaniu z ubiegłym rokiem budżet przeznaczony na cyberbezpieczeństwo wzrósł w przypadku prawie dwóch piątych firm (36%), a zmalał tylko w przypadku niemal jednej piątej (18%). Niemal połowa organizacji utrzymała budżet na identycznym poziomie.

Komentarz: Audyt biezpieczeństwa, brak rekomendacji

Dla audytora bezpieczeństwa IT niepokojący jest fakt, że ciągle 25% firm nie prowadzi audytów bezpieczeństwa swojego środowiska teleinformatycznego. Audyt jest jednym z najbardziej efektywnych sposobów podnoszenia bezpieczeństwa – pozwala na skuteczne podnoszenie poziomu bezpieczeństwa na podstawie analizy zabezpieczeń i oceny ich faktycznej skuteczności. Dzięki audytowi można wdrożyć te mechanizmy bezpieczeństwa, które są faktycznie potrzebne i których wdrożenie realnie wpłynie na bezpieczeństwo firmy. Równie niepokojący jest brak wdrażania rekomendacji audytowych – w wielu przypadkach takie postępowanie może prowadzić do zwiększenia podatności firm na cyberataki.

Aleksander Ludynia
EY

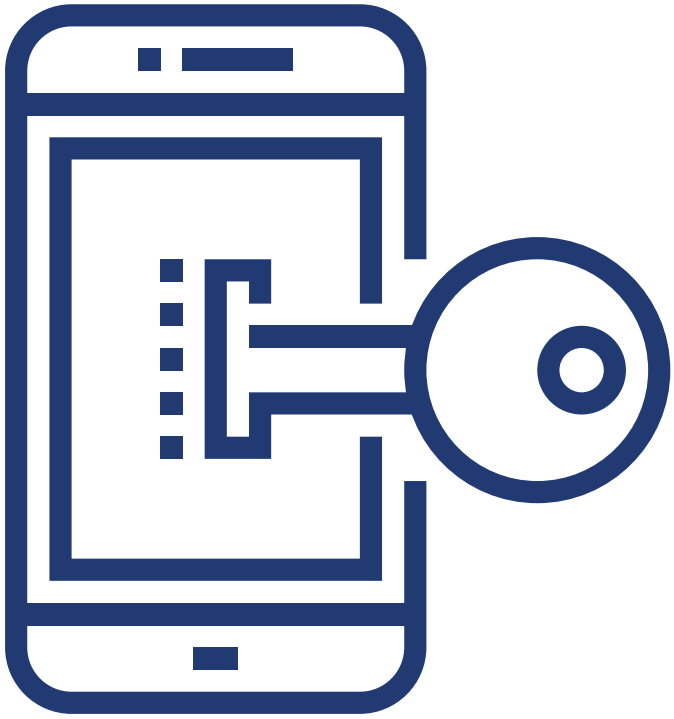
Zabezpieczamy się w większości jedynie na podstawowym poziomie

Kolejnym obszarem badania są sposoby, jakimi firmy zabezpieczają się przed zagrożeniami teleinformatycznymi. Czy rzeczywiście odpowiadają na stawiane przed nimi zadania? Czy można powiedzieć, że firmy są w tym zakresie dobrze zabezpieczone?

Badanie w tym obszarze nie nastraja optymistycznie. Jedynie 7% firm posiada system informowania o incydentach, działający w trybie 24/7/365, do którego podłączone są wszystkie istotne systemy teleinformatyczne. Aż 43% firm wcale nie posiada systemu, który informowałby o wystąpieniu incydentów w sieci teleinformatycznej.

Wprawdzie przedsiębiorstwa deklarują, że korzystają z zabezpieczeń swoich sieci, ale w praktyce okazuje się, że w przeważającej większości przypadków jest to ochrona na poziomie podstawowym tzn. antywirusa (93%) i firewalla (89%). Niestety z reguły takie zabezpieczenia są wszystkim z czego firmy korzystają. Popularność innych sposobów zabezpieczenia sieci w badanych firmach nie przekroczyła 1/3.

Pokazuje to, że zabezpieczenia firm są zdecydowanie doraźne i nie stanowią elementu bardziej kompleksowej strategii. Z wyzwaniami w tym zakresie powinni zmierzyć się przede wszystkim liderzy mniejszych firm, gdyż w ich przypadku poziom zabezpieczeń zazwyczaj można określić jako całkowicie symboliczny.

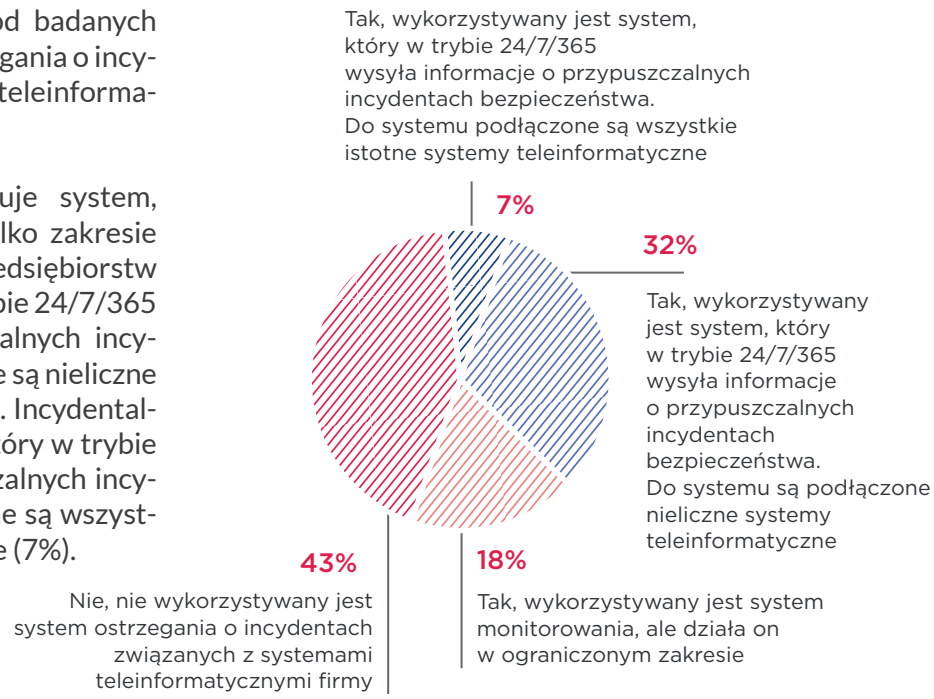


Incydenty związane z systemami teleinformatycznymi

W ponad dwóch piątych spośród badanych firm nie używa się systemu ostrzegania o incydentach związanych z systemami teleinformatycznymi (43%).

Prawie jedna piąta wykorzystuje system, który działa w ograniczonym tylko zakresie (18%). Ponad jedna trzecia przedsiębiorstw wykorzystuje system, który w trybie 24/7/365 wysyła informacje o przypuszczalnych incydentach, a do systemu podłączone są nieliczne systemy teleinformatyczne (32%). Incydentalnie firmy wykorzystują system, który w trybie 24/7/365 informuje o przypuszczalnych incydentach, a do systemu podłączone są wszystkie istotne systemy informatyczne (7%).

Czy w Państwa firmie wykorzystywane są systemy informujące o incydentach związanych z systemami teleinformatycznymi firmy?



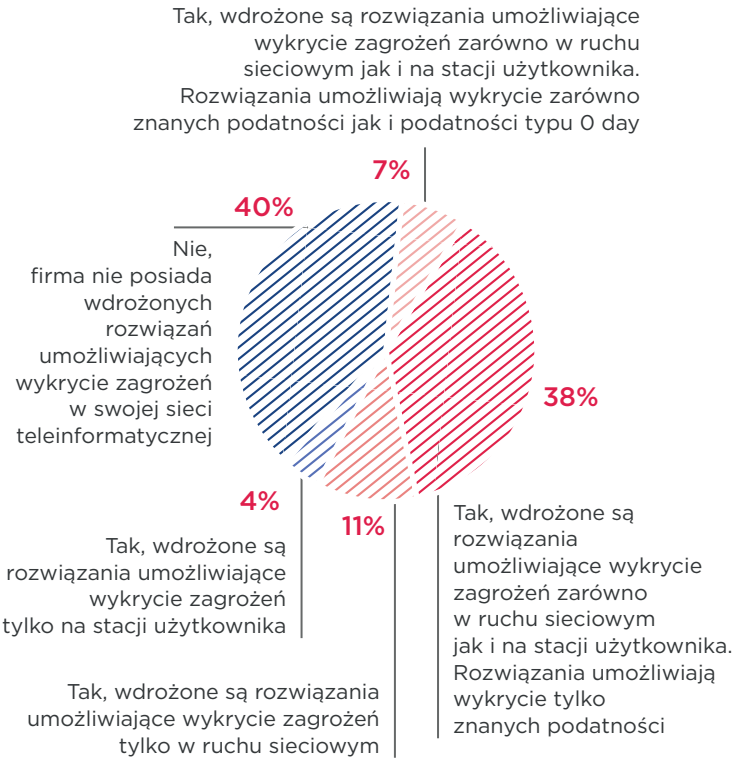
Rozwiązania do wykrywania zagrożeń w infrastrukturze teleinformatycznej

Pośród badanych przedsiębiorstw, dwie piąte nie posiada wdrożonych rozwiązań umożliwiających wykrycie zagrożeń w swojej sieci teleinformatycznej (40%) i prawie taki sam odsetek posiada wdrożone rozwiązania umożliwiające wykrycie zagrożeń zarówno w ruchu sieciowym, jak i na stacji użytkownika. Rozwiązania, które umożliwiają wykrycie tylko znanych podatności (38%).

Co dziewiąta firma posiada takie rozwiązania, ale umożliwiają one wykrycie zagrożeń tylko w ruchu sieciowym (11%). Natomiast jedynie co czternasta firma korzysta z systemu umożliwiającego wykrycie zarówno znanych podatności, jak i podatności typu 0 day (7%).

Niewiele firm posiada rozwiązania wykrywające zagrożenia tylko na stacji użytkownika (4%).

Czy firma posiada rozwiązania umożliwiające wykrycie zagrożeń w swojej infrastrukturze teleinformatycznej?

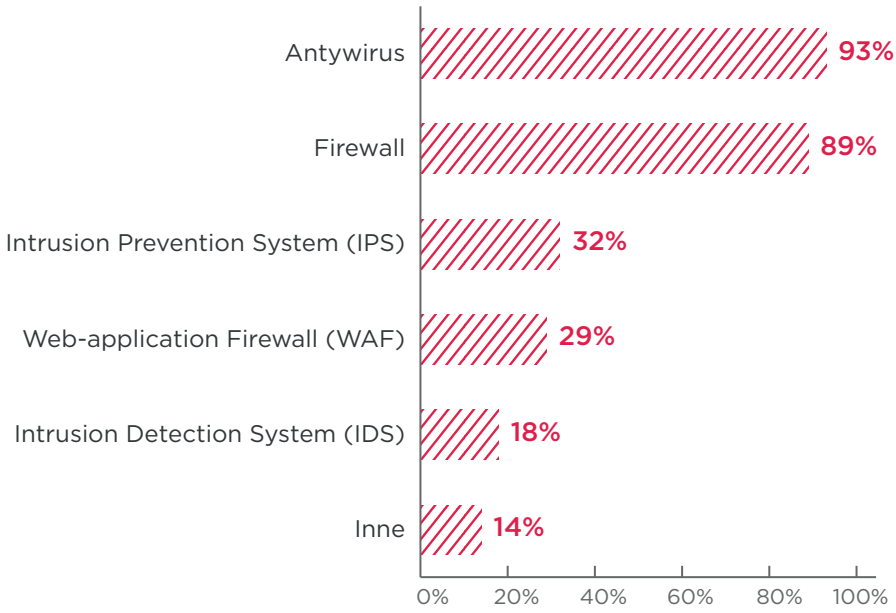


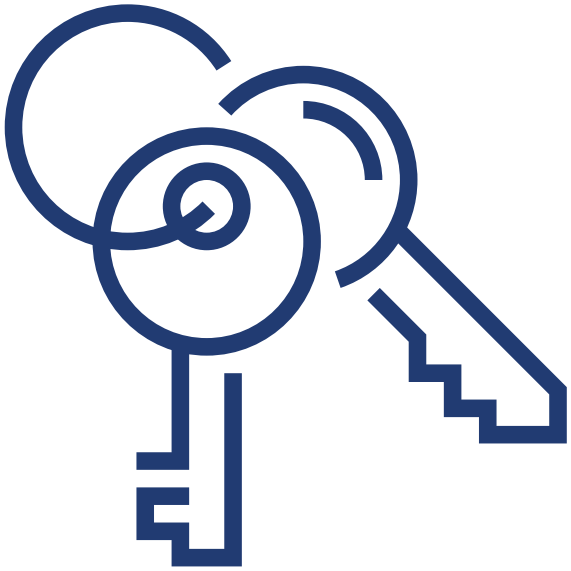
Urządzenia bezpieczeństwa

Jeśli chodzi o rodzaj narzędzi bezpieczeństwa, zdecydowana większość firm korzysta z antywirusa (93%) i firewalla (89%).

Niemal jedna trzecia korzysta z Intrusion Prevention System (IPS), nieco mniejszy odsetek z Web-application Firewall (WAF). Prawie jedna piąta używa Intrusion Detection System (IDS), a co siódma wymienia inne narzędzia/urządzenia (14%).

Z jakich narzędzi/urządzeń bezpieczeństwa korzysta firma? [pytanie wielokrotnego wyboru]





Nie ma odpowiednich planów i możliwości reakcji w przypadku wystąpienia ataku cybernetycznego

Cyberzagrożenia istnieją naprawdę – udawanie, że jest inaczej raczej nie działa na korzyść firmy. W momencie zagrożenia potrzebne jest zdecydowane i sprawne działanie. Aby było ono możliwe, potrzebny jest plan działania i ludzie potrafiący zareagować w sposób adekwatny do sytuacji.

Tymczasem badanie pokazują, że respondenci nie traktują możliwości ataku na ich firmy w sposób całkowicie poważny (przynajmniej do momentu wystąpienia takiego ataku). Firmy nie tylko nie monitorują czyhających na nie zagrożeń w sieci (o czym pisaliśmy już we wcześniejszych rozdziałach), ale także nie tworzą planów reakcji na wypadek wystąpienia incydentu bezpieczeństwa – dotyczy to 38% firm. Kolejne 40% posiada taki plan, w którym obsługa incydentów jest wyłącznie w kompetencji zespołów technologicznych, co po pierwsze może być niewystarczające, a po drugie (przy pogłębionej analizie wypowiedzi badanych) – zazwyczaj okazuje się planem bardzo ogólnikowym, istniejącym raczej w głowie osoby odpowiedzialnej za IT, a nie w formie spisanego dokumentu.

Również w tym przypadku wielkość firmy ma znaczenie – najlepiej przygotowane są firmy duże, a odsetek przedsiębiorstw mających rzeczywisty plan w przypadku ataku jest tym mniejszy, im mniejsza jest firma.

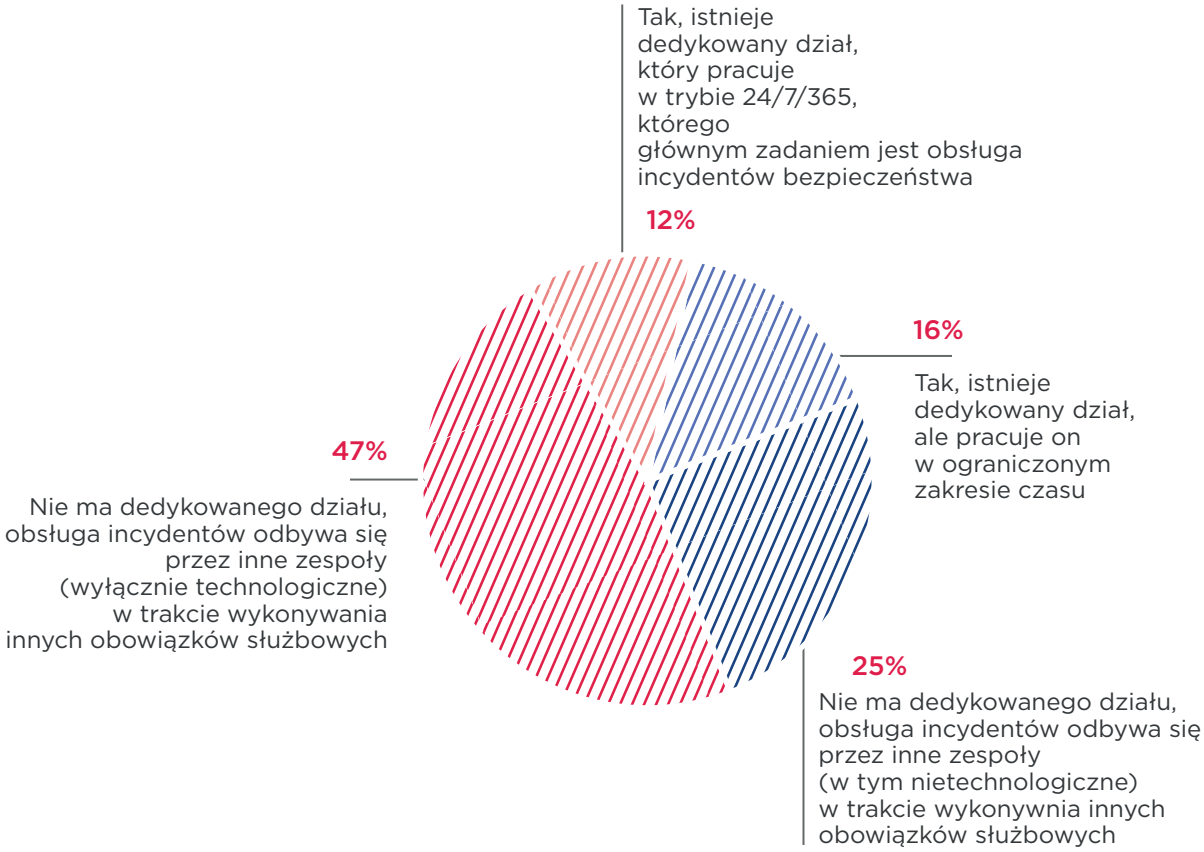
Odpowiedzialny za cyberbezpieczeństwo

Prawie połowa firm przyznaje, że nie ma dedykowanego działu do incydentów bezpieczeństwa, a ich obsługą zajmują się inne zespoły technologiczne (47%).

Jedna czwarta powierza to zadanie innym zespołom, także tym, które nie są technologiczne (25%).

Jedynie w co szóstej firmie istnieje dedykowany dział pracujący w ograniczonym zakresie czasu (16%), a tylko w co ósmej dział, który zajmuje się obsługą bezpieczeństwa w trybie 24/7/365 – (12%).

Czy w firmie istnieje dedykowany dział, którego zadaniem jest obsługa incydentów bezpieczeństwa?



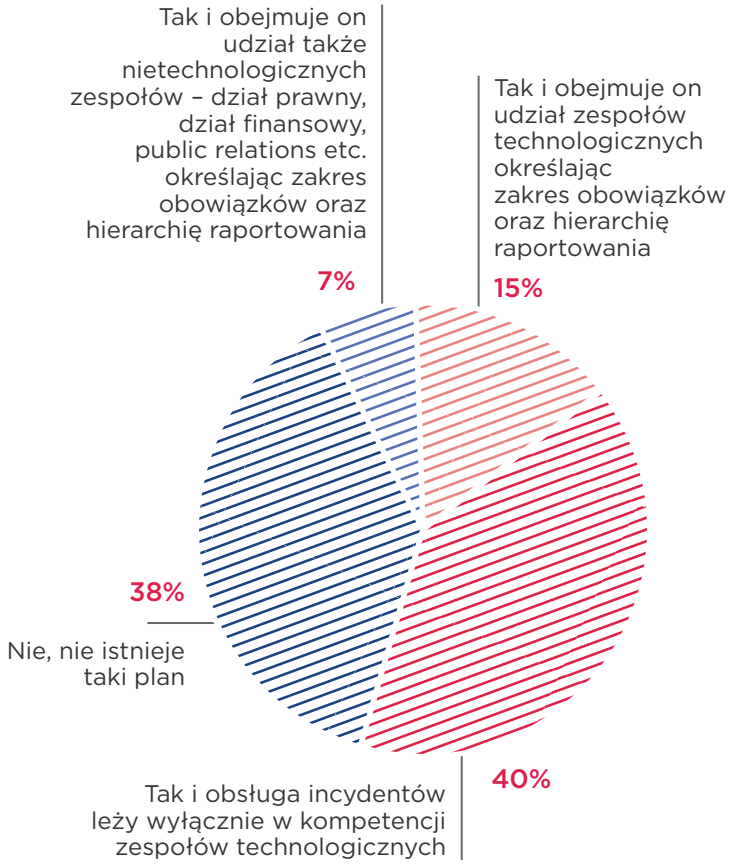
Plan reakcji na incydenty bezpieczeństwa

Dwie piąte firm przyznaje, że nie posiada planu reakcji na incydent bezpieczeństwa (38%). Prawie tyle samo firm posiada taki plan i powierza obsługę incydentów wyłącznie zespołowi technologicznemu (40%).

Co siódmy respondent posiada plan reakcji, obejmujący udział zespołów technologicznych, określający zakres obowiązków oraz hierarchie raportowania (15%).

Tylko co 14 firma posiada plan, który przewiduje udział także nietechnologicznych zespołów (np. działu prawnego, finansowego, PR) z określeniem zakresu obowiązków oraz hierarchii raportowania (7%).

Czy w Państwa firmie istnieje plan reakcji na incydent bezpieczeństwa?



Komentarz: Mądry po szkodzie

Z naszego doświadczenia wynika, że często bodźcem do bardziej energicznych działań w zakresie bezpieczeństwa IT jest incydent, przypadek ataku hakerskiego. W sytuacji kryzysowej, zarząd firmy widzi na bieżąco, jak skuteczne są plany reakcji i struktury odpowiedzialne za bezpieczeństwo IT.

Niestety, w wielu przypadkach ataki są skuteczne – czy to działania socjotechniczne (ostatnio popularna fala ataków „na prezesa"), wymuszenia okupu (ransomware, itp.) czy też ukierunkowane działania hakerów. Firmy ponoszą realne straty i po takim „zimnym prysznicu" następuje refleksja i próba zrozumienia jak i z kim/czym działać w kontekście bezpieczeństwa IT.

W naszym rozumieniu jedynie kompleksowe podejście do bezpieczeństwa IT i konsekwentne, aktywne działania w zakresie prewencji, detekcji i reakcji są w stanie realnie chronić organizację przed cyberzagrożeniami.

Grzegorz Idzikowski
Menedżer w Zespole Zarządzania Ryzykiem Nadużyć, EY

Nie korzystamy z własnych doświadczeń

Aby dobrze zrozumieć kontekst, w jakim budowane jest cyberbezpieczeństwo firm, warto przyjrzeć się umiejętności wyciągania wniosków z zaistniałych sytuacji. O dojrzałości możemy mówić wtedy, gdy firma potrafi wykryć zagrożenie, zareagować na nie, ale także wyciągnąć z niego wnioski na przyszłość.

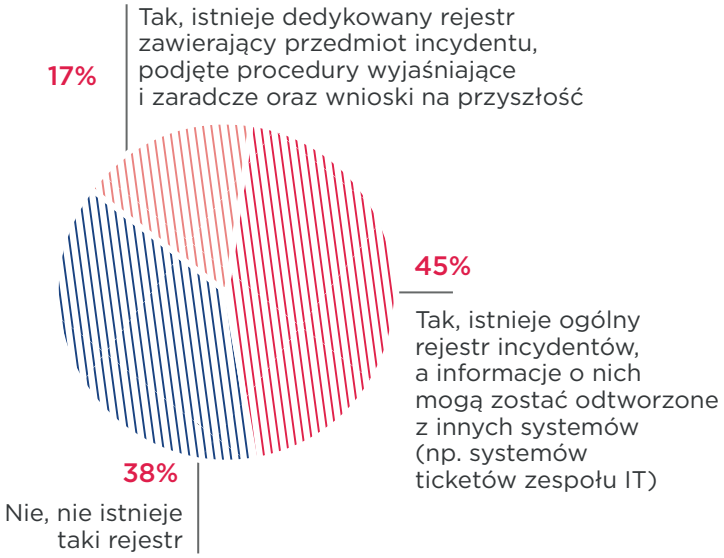
Jedynie 17% spośród badanych przez nas firm posiada dedykowany rejestr incydentów IT. Niewiele więcej, bo jedynie 19% prowadzi badania dotyczące trendów w zidentyfikowanych atakach.

Wniosek nasuwa się sam – większość badanych przedsiębiorstw nie ma szansy skorzystać z własnych doświadczeń. Firmy nie uczą się na nich i wcale nie są lepiej przygotowane do następnych ataków. Ma to również kontekst istotny dla całej gospodarki – firmy nie dzielą się informacjami z innymi, co nie przyczynia się do zwiększenia ogólnego cyberbezpieczeństwa.

Rejestr incydentów w firmie

Prawie połowa badanych firm posiada ogólny rejestr incydentów, a informacje o nich mogą zostać odtworzone z innych systemów (tickety, zespoły IT) – 45%. Blisko dwie piąte firm w ogóle nie posiada takiego rejestru. Prawie jedna piąta posiada rejestr zawierający przedmiot incydentu, wszczęte procedury oraz wnioski (17%).

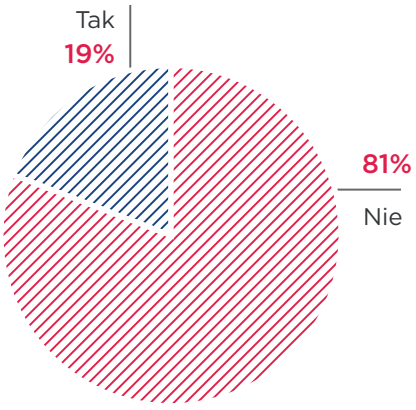
Czy w firmie prowadzony jest rejestr incydentów?



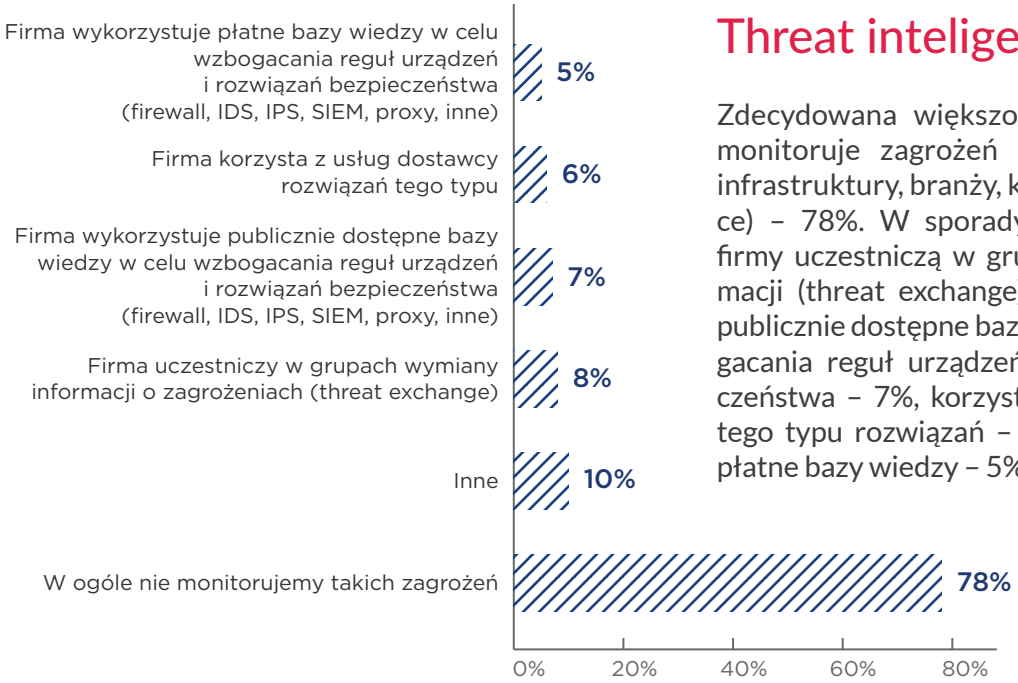
Analiza incydentów pod kątem trendów

Zdecydowana większość badanych przedsiębiorstw nie prowadzi analizy incydentów pod kątem trendów (81%), robi to niespełna jedna piąta firm (19%).

Czy w Państwa firmie przeprowadza się analizę incydentów pod kątem trendów?



Jak firma monitoruje zagrożenia dot. własnej infrastruktury, branży, kraju? (threat inteligence)



Threat inteligence

Zdecydowana większość firm w ogóle nie monitoruje zagrożeń dotyczących własnej infrastruktury, branży, kraju (threat inteligence) – 78%. W sporadycznych przypadkach firmy uczestniczą w grupach wymiany informacji (threat exchange) – 8%, wykorzystują publicznie dostępne bazy wiedzy w celu wzbogacania reguł urządzeń i rozwiązań bezpieczeństwa – 7%, korzystają z usług dostawcy tego typu rozwiązań – 6% czy wykorzystują płatne bazy wiedzy – 5%.

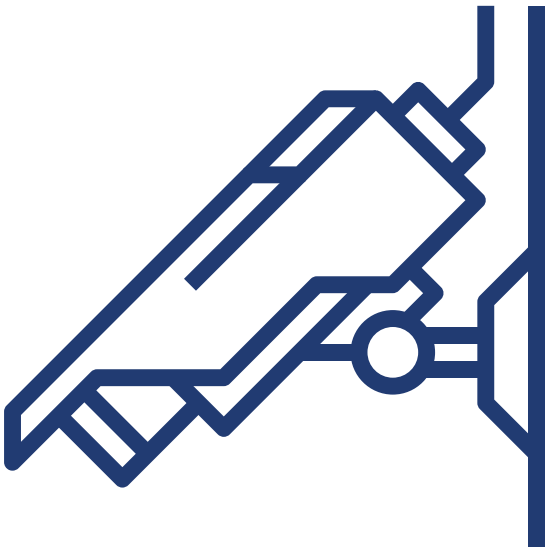
Strukturalnie kwestia bezpieczeństwa jest uważana za sprawę IT

Kwestie cyberbezpieczeństwa mają bez wątpienia kluczowe znaczenie dla funkcjonowania firm i w związku z tym pojawia się pytanie: kto wobec tego powinien wziąć odpowiedzialność za ten obszar i komu powinni podlegać specjaliści od bezpieczeństwa w sieci.

Różne rozwiązania strukturalne mają pewne plusy i minusy np. związane z komunikacją, ryzykiem rozproszenia odpowiedzialności czy możliwością pojawiania się konfliktów, a to z kolei może mieć realne konsekwencje w sytuacji zagrożenia.

Poszukując optymalnych rozwiązań w obszarze cyberbezpieczeństwa, warto zatrzymać się na chwilę przy strukturze organizacji i sprawdzić kto obecnie odpowiada w firmach za ten obszar.

Z zebranych przez nas danych wynika, że aż w 75% za ocenę cyberzagrożeń i za zabezpieczenie przed nimi odpowiada dział IT. Powszechność tego rozwiązania jest silnie powiązana z wielkością firmy – im mniejsza, tym rzadziej bezpieczeństwem zajmują się specjalnie dedykowane do tego obszaru osoby. Historycznie to, co dotyczy obszarów informatycznych należało do kompetencji IT. Dodatkowo zatrudnienie kolejnej osoby, często przekracza możliwości finansowe wielu firm.



Komentarz: Reakcja – jak to robić (skoro niewielu robi)?

Przy różnych okazjach często słyszymy pytanie – co robić, kiedy zostaniemy zaatakowani?

Reakcja na cyberatak będzie skuteczna, gdy spełnione zostaną następujące warunki:

1) Szybkie działania według planu – należy działać możliwie od razu po wykryciu ataku.
2) Odpowiedni ludzie – dedykowany zespół posiadający odpowiednie narzędzia i kwalifikacje lub zaufana pomoc z zewnątrz.
3) Współpraca między zespołami – w przypadku ataku ważna jest właściwa koordynacja działań – zarządu, działu bezpieczeństwa, działu IT, działu prawnego i dyrektorów operacyjnych.

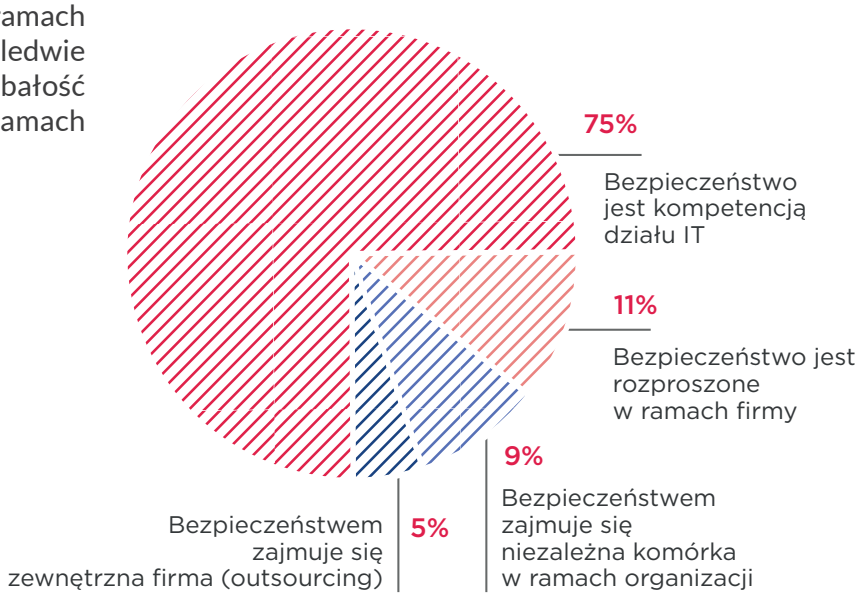
Zadając Państwu pytanie o dedykowane zespoły do reakcji chcieliśmy dowiedzieć się, ilu z Was rzeczywiście jest w stanie reagować na cyberatak. Powyższe warunki spełnia tylko co ósma firma.

Grzegorz Idzikowski
EY

Odpowiedzialność za cyberbezpieczeństwo

Trzy czwarte badanych firm powierza ocenę cyberzagrożeń i zabezpieczenie przed nimi swoim działom IT (75%). W przypadku co dziewiątej firmy, odpowiedzialność za bezpieczeństwo jest rozproszona w ramach firmy. W co jedenastej firmie bezpieczeństwem zajmują się niezależne komórki w ramach organizacji (9%). Znikomy odsetek – zaledwie 5%, czyli co 20 badana firma zleca dbałość o bezpieczeństwo na zewnątrz, w ramach outsourcingu.

Kto w Państwa firmie odpowiedzialny jest za ocenę cyberzagrożeń i zabezpieczenie przed nimi?

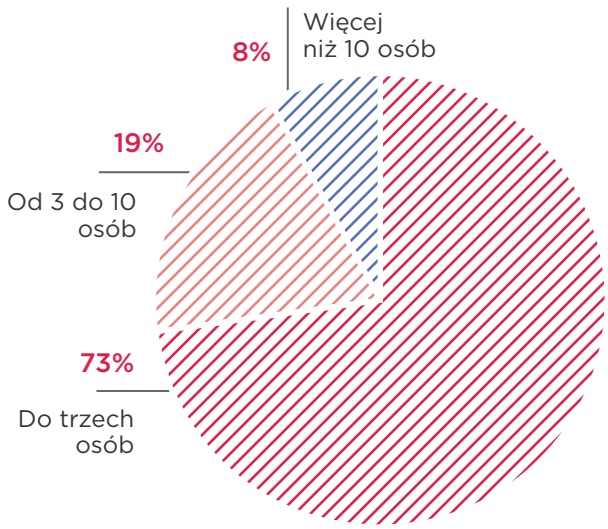


Liczba osób odpowiedzialnych za cyberbezpieczeństwo

W trzech czwartych spośród badanych firm obowiązek zajmowania się wyłącznie bezpieczeństwem IT ma w swoim zakresie do trzech pracowników (75%).

W prawie jednej piątej przypadków, zagadnieniami tymi zajmuje się od 3 do 10 osób (19%). W 8% firm ponad 10 osób jest wyznaczonych do dbania wyłącznie o bezpieczeństwo IT.

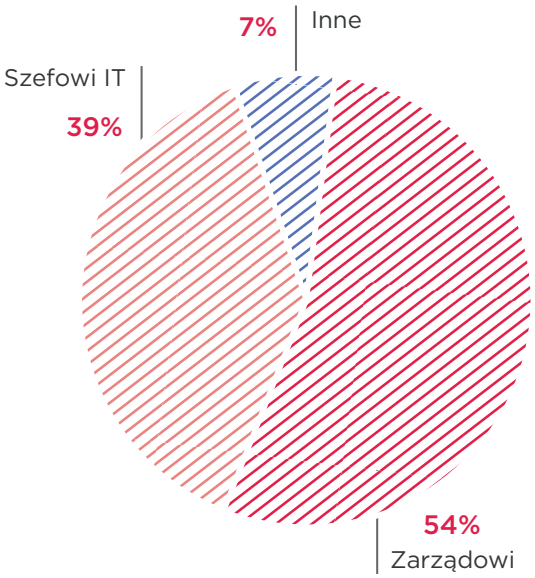
Ile osób w swoich obowiązkach służbowych ma zajmowanie się wyłącznie bezpieczeństwem IT?



Cyberbezpieczeństwo w strukturze firmy

W ponad połowie badanych firm osoba lub osoby odpowiedzialne za bezpieczeństwo IT podlegają zarządowi (54%). W prawie dwóch czwartych – szefowi IT (39%), a w pozostałych przypadkach: (7%) zastosowanie mają inne rozwiązania.

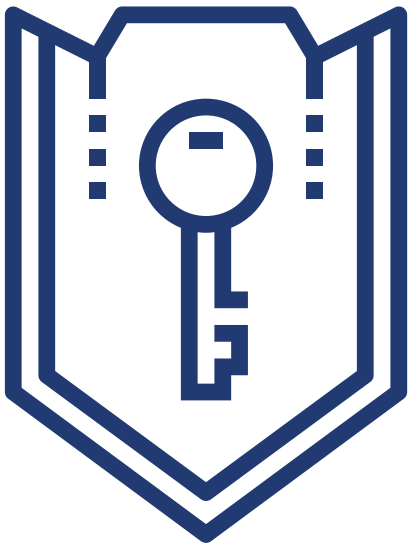
Komu jest podległa osoba(y) odpowiedzialna(e) w firmie za bezpieczeństwo IT?



Komentarz:
Struktura, odpowiedzialność za bezpieczeństwo a IT

W przypadku zdecydowanej większości firm za bezpieczeństwo odpowiada zespół IT. W wielu miejscach takie postępowanie może być uzasadnione, ale należy zwrócić uwagę, że bardzo często priorytety bezpieczeństwa nie są tożsame z priorytetami zespołów IT. Najczęściej celem zespołów IT jest zapewnienie poprawnego funkcjonowania systemów informatycznych, natomiast zapewnienie bezpieczeństwa może przynosić efekt odwrotny i utrudniać efektywne wykorzystanie systemów informatycznych. Zatem konieczne wydaje się oddzielenie odpowiedzialności za bezpieczeństwo systemów informatycznych od odpowiedzialności za ich utrzymanie.

Aleksander Ludynia
EY



Na jak dużo pozwalamy pracownikom?

Trudno oczekiwać, aby każdy z pracowników przychodził do firmy z wiedzą specjalistów z IT. Wielokrotnie w tym raporcie przewija się wątek człowieka jako największego zagrożenia dla bezpieczeństwa firmy. Na jak dużo badane przedsiębiorstwa pozwalają swoim pracownikom? W tym miejscu trudno powiedzieć jaki jest złoty środek. Czy ograniczyć swobodę pracownikom i dzięki temu zabezpieczyć lepiej firmę, czy bardziej ufać wiedzy pracowników i wdrożonym w firmie procedurom?

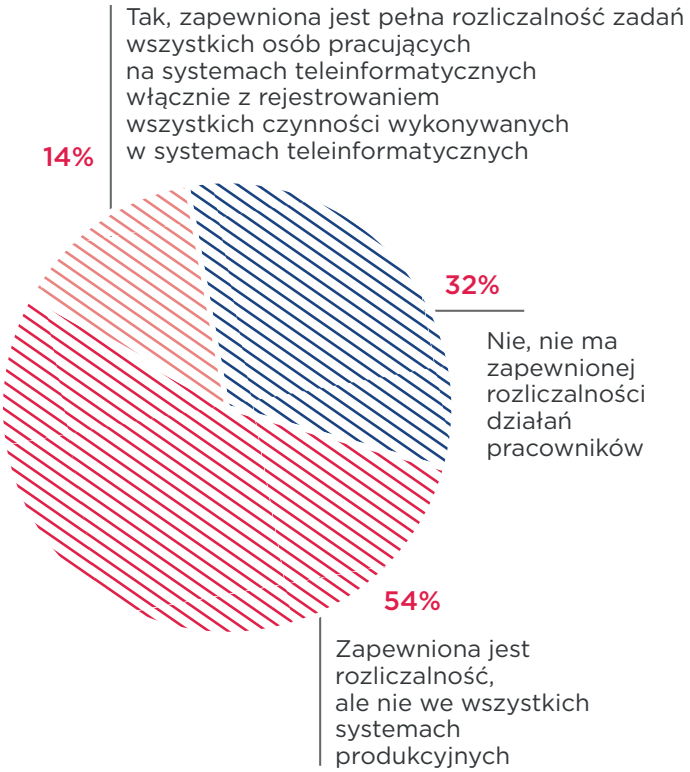
Z badań wynika, że prawie dwie trzecie organizacji nie blokuje pracownikom dostępu do żadnych serwisów internetowych. Spośród badanych firm 36% pozwala pracownikom na korzystanie z własnych urządzeń.

Monitoring czynności wykonywanych przez pracowników

Ponad połowa firm monitoruje czynności wykonywane przez pracowników w systemach teleinformatycznych firmy, ale „rozliczalność" zapewniona jest nie we wszystkich systemach produkcyjnych (54%).

Co siódma firma zapewnia pełną rozliczalność zadań wszystkich pracujących na systemach, włącznie z rejestrowaniem wszystkich czynności. Prawie jedna trzecia firm natomiast nie ma zapewnionej rozliczalności działań pracowników.

Czy firma monitoruje czynności wykonywane przez pracowników w systemach teleinformatycznych firmy?

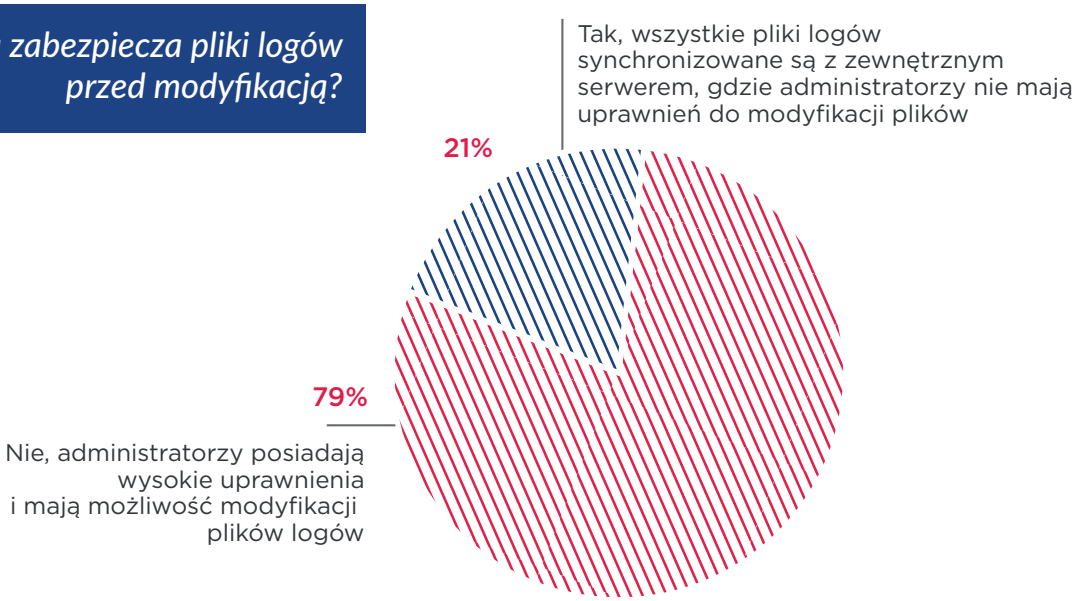


Zabezpieczenie plików logów

Tylko w przypadku jednej piątej badanych firm wszystkie pliki logów zsynchronizowane są z wewnętrznym serwerem, gdzie administratorzy nie mają uprawnień do modyfikacji plików (21%).

W zdecydowanej większości przedsiębiorstw natomiast administratorzy posiadają wysokie uprawnienia i mają możliwość modyfikacji plików logów (79%).

Czy firma zabezpiecza pliki logów przed modyfikacją?



Ograniczenia dostępu do serwisów umożliwiających przesyłanie danych

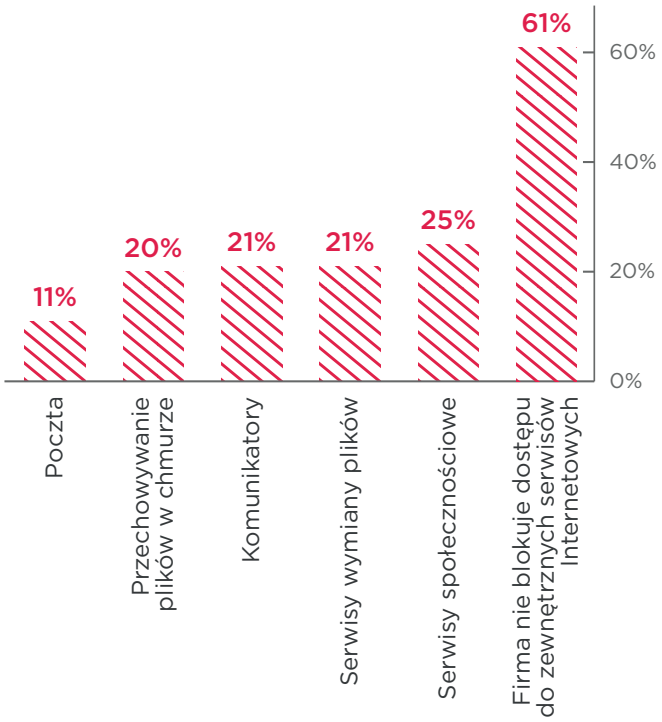
Ponad dwie trzecie badanych firm nie blokuje dostępu do zewnętrznych serwisów internetowych (61%). Jedna czwarta blokuje serwisy społecznościowe (25%), ponad jedna piąta – serwisy wymiany plików (21%). Taki sam odsetek blokuje komunikatory (21%), jedna piąta – przechowywanie plików w chmurze (20%), więcej niż co dziesiąta stosuje blokadę poczty (11%).

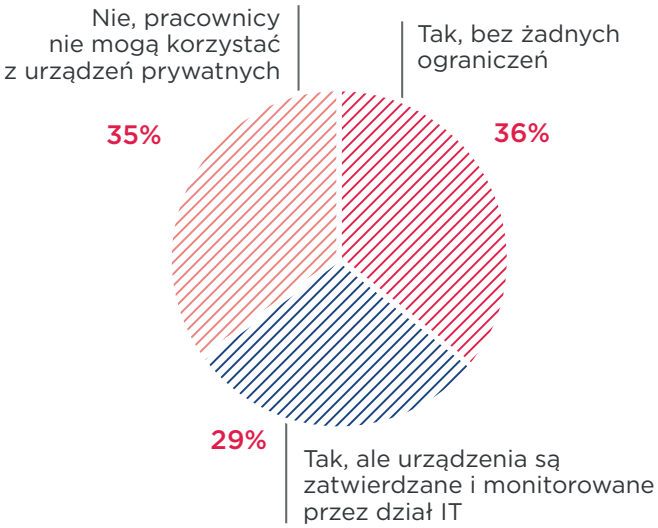
Urządzenia prywatne do celów służbowych

Pod względem zasad korzystania z prywatnych urządzeń informatycznych typu laptopy, telefony w celach służbowych badana próba podzieliła się na trzy proporcjonalne pod względem ilościowym strategie. Ponad jedna trzecia firm nie pozwala pracownikom korzystać z urządzeń prywatnych (35%), mniej niż jedna trzecia pozwala, ale urządzenia te zatwierdza i monitoruje dział IT (29%), ponad jedna trzecia pozwala korzystać z nich bez ograniczeń (36%).

Czy pracownicy mogą korzystać z prywatnych urządzeń informatycznych np. laptopy, telefony etc. w celach służbowych (polityka tzw. bring your own device)?

Czy firma zabezpiecza pliki logów przed modyfikacją?





Komentarz: Zaufanie do pracownika

Pracownicy firm ciągle darzeni są sporym zaufaniem swoich pracodawców. Dotyczy to w szczególności administratorów, których zakres uprawnień w systemach informatycznych w wielu przypadkach wydaje się nieograniczony. Mając na uwadze fakt, że duża część ataków na systemy informatyczne została przeprowadzona przez pracowników firm, wydaje się, że konieczne jest zwiększanie kontroli nad działaniami pracowników. Wiele ataków prowadzonych jest za pomocą przejętych kont administratorów, dlatego ich działania również powinny podlegać szczególnej kontroli i monitorowaniu.

Aleksander Ludynia
EY

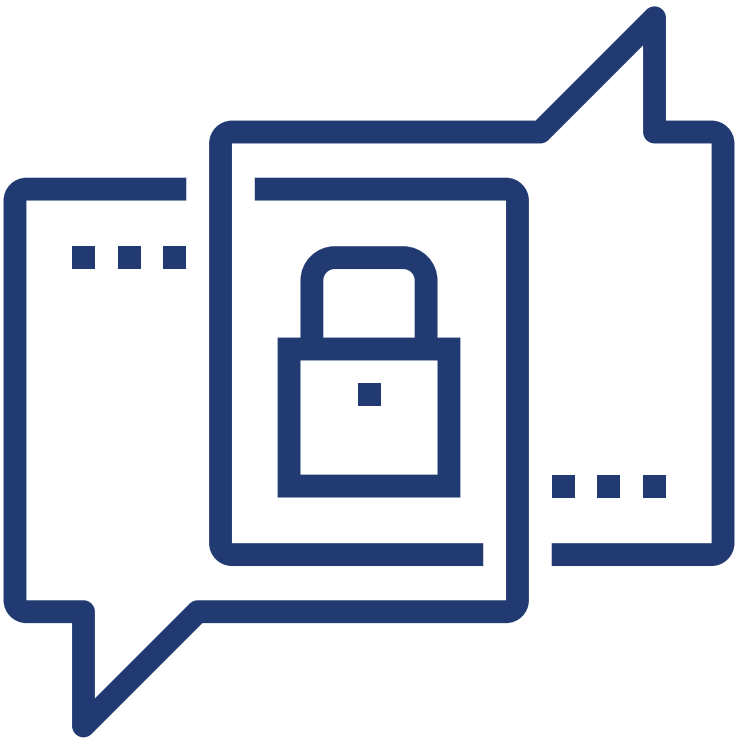
Szkolimy pracowników – czy rzeczywiście?

Wydaje się, że skoro, jak już wcześniej pisaliśmy, człowiek jest najsłabszym ogniwem w strukturze bezpieczeństwa firmy, a problemy naruszenia cyberbezpieczeństwa są najczęściej skutkiem zbyt małej ostrożności pracowników lub/i ich niedostatecznej wiedzy na temat aktualnych niebezpieczeństw – firmy powinny szkolić wszystkich swoich pracowników regularnie i intensywnie. Zwłaszcza, że na rynku jest coraz więcej różnych szkoleń związanych z bezpieczeństwem IT.

W badaniu zapytaliśmy respondentów o to, jakie szkolenia z tematyki cyberbezpieczeństwa prowadzone są w ich firmie, w jaki sposób i kto je prowadzi. Niepokój może budzić fakt, że 30% firm w ogóle nie realizuje szkoleń dotyczących bezpieczeństwa IT, a ponad 60% realizuje takie szkolenia jedynie jako szkolenie wstępne przy przyjmowaniu pracownika do pracy. Znając praktykę w firmach można jedynie wyobrazić sobie, jak takie szkolenia wyglądają i jakie jest ich faktyczne znaczenie dla zapewnienia bezpieczeństwa firmie.

Spośród badanych przedsiębiorstw tylko 18% realizuje takie szkolenia regularnie. Kolejnym zaskakującym faktem w kontekście wiedzy o szybkiej dezaktualizacji informacji w dziedzinie bezpieczeństwa w sieci jest to, że takie szkolenia w większości przypadków prowadzone są wewnątrz firmy przez własnych pracowników i najczęściej w formie wykładu, choć nie od dziś wiadomo, że nie jest to najbardziej efektywna forma przyswajania wiedzy.

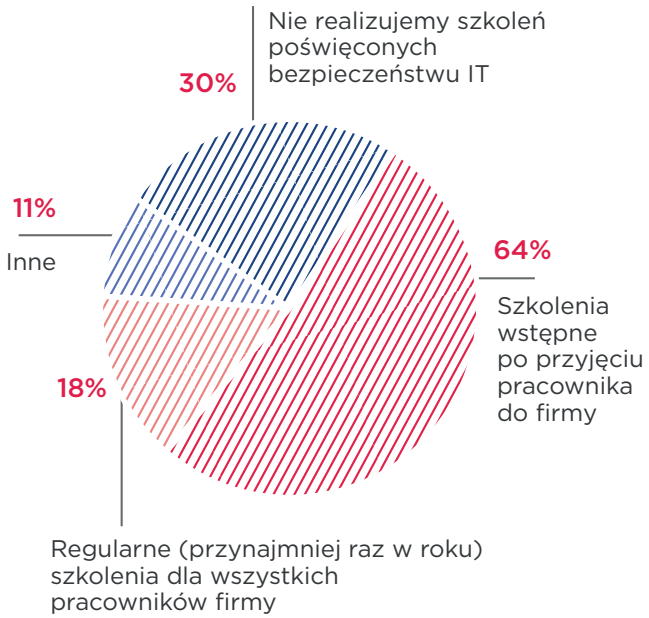
Jednocześnie zauważamy, że im mniejsza firma, tym bardziej spada stopień świadomości pracowników. To kolejne wyzwanie, z którym będą musieli zmierzyć się zarządzający takimi organizacjami zanim nie będzie za późno.



Szkolenia w zakresie cyberbezpieczeństwa

Prawie jedna trzecia badanych firm nie realizuje szkoleń poświęconych bezpieczeństwu IT (30%). W ponad trzech piątych, spośród badanych firm, prowadzi się szkolenia wstępne po przyjęciu pracownika do firmy (64%). Tylko mniej niż jedna piąta prowadzi szkolenia z zakresu bezpieczeństwa IT przynajmniej raz w roku (18%). 11% firm stosuje inne rozwiązania.

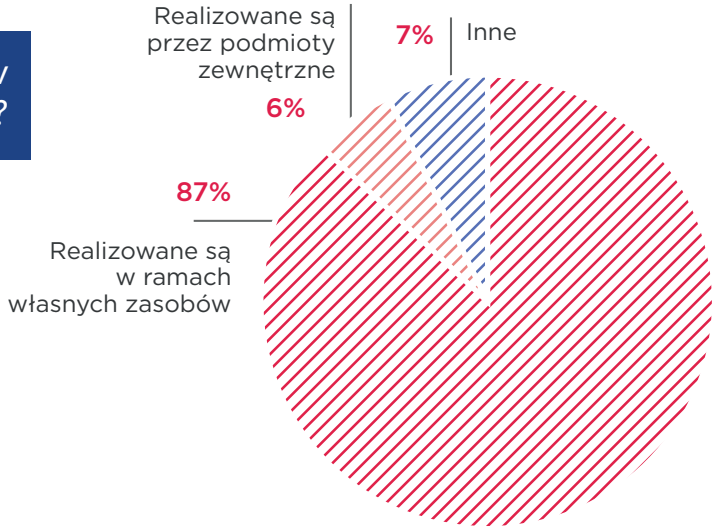
Jakie szkolenia z tematyki dotyczącej bezpieczeństwa IT realizowane są w Państwa firmie dla wszystkich pracowników firmy?



Kto prowadzi szkolenia w zakresie cyberbezpieczeństwa

W przeważającej większości firm szkolenia z zakresu bezpieczeństwa IT prowadzone są przez własnych pracowników. W 6% firm szkoleniami zajmuje się firma zewnętrzna, a w 7% stosuje się inne rozwiązania.

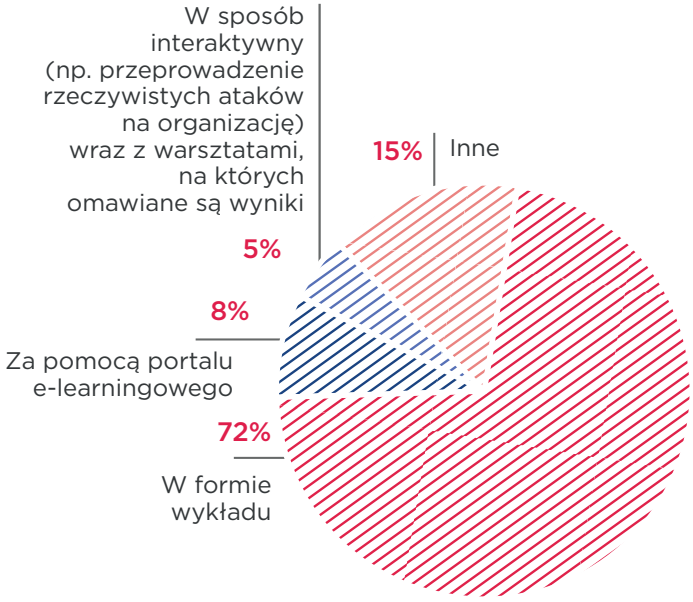
Czy firma zabezpiecza pliki logów przed modyfikacją?



Forma szkoleń

W prawie trzech czwartych badanych firm szkolenia z zakresu bezpieczeństwa IT prowadzi się w formie wykładu. W 8% firm za pomocą portalu e-learningowego. Tylko co dwudziesta firma przeprowadza szkolenia w sposób interaktywny np. przeprowadzając rzeczywiste ataki na organizację – wraz z warsztatami, na których omawiane są wyniki (5%). Inne rozwiązania wskazało 15% badanych.

Jakie szkolenia z tematyki dotyczącej bezpieczeństwa IT realizowane są w Państwa firmie dla wszystkich pracowników firmy?



Komentarz: Szkolenia

Nasze doświadczenie pokazuje, że szkolenia traktowane są jako „dobro konieczne". Pracownicy bądź to na żywo, bądź poprzez narzędzia IT przechodzą przez zestawy pytań, których nie są w stanie odnieść do rzeczywistości. A zatem szkolenia są jedynym bezpośrednim środkiem, aby wzmocnić najsłabsze ogniwo – i nie traktujemy ich wystarczająco poważnie.

Powinniśmy:

a) przeprowadzać różne szkolenia dla konkretnych grup pracowników
b) budować programy szkoleń – zmienić ich jednorazowość w przyzwyczajenie
c) być w stanie zmierzyć skuteczność szkoleń.

Tylko wtedy będziemy w stanie zmienić mentalność naszych pracowników.

Grzegorz Idzikowski
EY

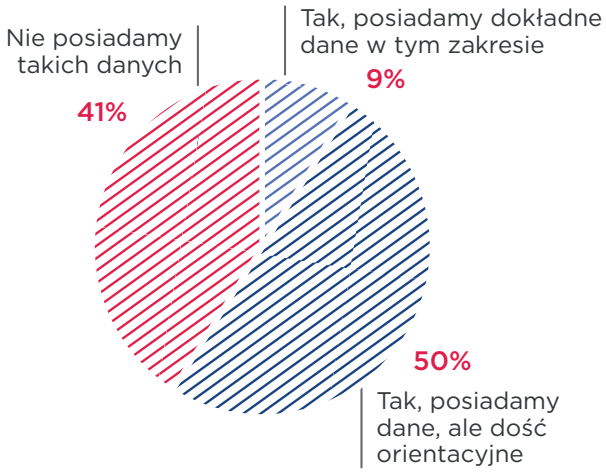
Nadal zbyt mało uwagi poświęcane jest na edukację użytkowników w zakresie bezpieczeństwa. Firmy albo nie prowadzą szkoleń, albo organizują jedno ogólne szkolenie rocznie, co nie może przynieść pozytywnych rezultatów. Aby faktycznie podnieść poziom świadomości bezpieczeństwa pracowników firm, konieczna jest realizacja kompleksowych programów obejmujących zarówno szkolenia jak i cykliczne działania utrwalające wiedzę przekazywaną podczas szkoleń. Zakres wiedzy, która powinna zostać przekazana pracownikom, rośnie wraz z rozwojem technik cyberprzestępców. Nie sposób przekazać i utrwalić wszystkich zagadnień w ciągu jednego godzinnego szkolenia rocznie.

Aleksander Ludynia
EY

Transfer ryzyka na ubezpieczyciela

Wśród polskich przedsiębiorców zauważalne jest poczucie niepewności związanej z cyber-zagrożeniami i ich konsekwencjami. Związane jest to z faktem, że cyberbezpieczeństwo jest ostatnio głośnym i często poruszanym tematem. W badaniu zapytaliśmy przedsiębiorców o to, czy w ich firmach przeprowadzona została analiza potencjalnych strat w wypadku zagrożenia cyberinformatycznego. Wyniki nie nastrajają optymistycznie. Okazuje się, że jedynie co dziesiąta firma (9%) posiada dokładną wiedzę w tym zakresie. Połowa ankietowanych posiada jakieś, ale tylko orientacyjne dane na ten temat, a z kolei 41% badanych przyznało, że nie ma żadnej wiedzy, ponieważ nie były przeprowadzane tego typu analizy.

Czy w Państwa firmie przeprowadzona została analiza, na jakie straty jest narażona firma w związku z zagrożeniami cyberinformatycznymi?



Poczucie niepewności związanej z konsekwencjami cyberzagrożeń jest powiązane z faktem, iż, jak już pisaliśmy w niniejszym raporcie, większość firm odnotowała w ciągu ostatnich 12 miesięcy znaczące incydenty bezpieczeństwa, w tym w co piątej firmie takich incydentów było więcej niż 5. Badane firmy miały do czynienia z różnymi rodzajami zagrożeń: ogólnymi kampaniami malware, działaniem pracowników, utratą danych wskutek awarii systemu czy atakami DDoS. Świadomość ryzyka jest coraz wyższa, bo wynika z zaistniałych incydentów, z którymi firmy musiały się zmierzyć. Wiedza, że zagrożenie jest realne i spowodowane może być wieloma czynnikami (działaniami pracowników, przestępczością komputerową, wadliwym oprogramowaniem czy procedurą) towarzyszy każdemu. Pomimo to sposoby reagowania i podejścia do tej tematyki są odmienne.

Poza atakami hakerskimi, coraz bardziej wyrafinowanymi przykładami przestępczości komputerowej spory odsetek polskich firm (60%) obawia się przypadkowych, nieuprawnionych i destrukcyjnych działań swoich pracowników, wskazuje to jako najbardziej istotne zagrożenie dla bezpieczeństwa firmy. Co dziesiąta firma (9%) obawia się natomiast celowego, nieuprawnionego i destrukcyjnego działania pracowników.

Zróżnicowane jest przygotowanie badanych firm do reagowania na incydenty cybernetyczne, jak też ich higiena informatyczna. Ciekawym i dla niektórych innowacyjnym rozwiązaniem może być transfer części ryzyka cybernetycznego na ubezpieczyciela w ramach zawartej polisy ubezpieczeniowej.

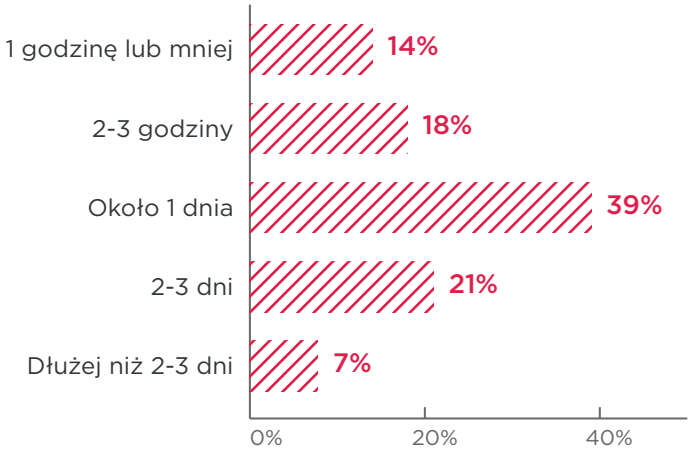
W procesie transferu ryzyka sprawdzane są zasady bezpieczeństwa informatycznego, zarządzania ryzykiem i wspomniana wcześniej higiena informatyczna firmy. Podczas oceny ryzyka przez ubezpieczyciela badane są takie obszary jak: stosowanie przez firmę narzędzi/urządzeń bezpieczeństwa, tj. antywirusa, firewalla, IPS i innych szyfrowanych, przechowywanych przez firmy danych oraz wykonywanie kopii bezpieczeństwa.

Mimo, że polisa ubezpieczeniowa nie jest remedium na wszelkie problemy, ma możliwość zmniejszenia ponoszonych przez firmę konsekwencji. Ubezpieczyciel może bowiem wziąć na siebie część ryzyka poprzez pokrywanie kosztów prawników w przypadku roszczeń

pokrzywdzonych w związku z ujawnieniem ich danych niezgodnie z przepisami prawa wraz z zapłatą kar administracyjnych nałożonych przez organy regulacyjne, kosztów doradców PR i informatyków śledczych. Jest to swego rodzaju assistance, który ma na celu szybką reakcję i skoordynowane działania specjalistów od tego rodzaju sytuacji kryzysowych. Innym sposobem ograniczenia strat finansowych spółek jest ochrona ubezpieczeniowa w przypadku przerwy w działalności wywołanej przez atak hakerski. Jest to ryzyko, które może wywołać dotkliwe skutki, zwłaszcza w każdej firmie, która generuje wysokie przychody, ale też w znacznym stopniu uzależnia swoją działalność od systemów informatycznych.

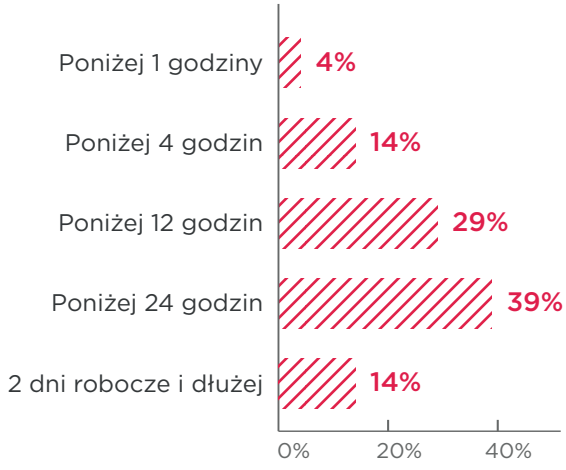
Prawie dwie piąte badanych stwierdziło, że w przypadku braku kluczowych systemów informatycznych firma mogłaby pracować około jednego dnia roboczego bez ponoszenia znaczących strat finansowych (39%), prawie jedna piąta firm mogłaby przetrwać 2-3 dni (18%), taka sama liczba badanych tylko 2-3 godziny. 16% ankietowanych może funkcjonować bez straty maksymalnie 1 godzinę. Natomiast najmniejsza grupa (7%) twierdzi, że może działać bez kluczowych systemów dłużej niż 2-3 dni.

Jak długo Państwa firma mogłaby działać bez kluczowych systemów informatycznych nie ponosząc znacznej straty finansowej?



Z drugiej strony ciekawą kwestią towarzyszącą niedostępności systemów jest szybkość usunięcia ich awarii. Największą grupę w badaniu stanowiły firmy, które jako maksymalny akceptowalny czas usunięcia skutków incydentu przyjęły czas poniżej 24 godzin (39%). Mniej niż jedna trzecia (29%) ankietowanych akceptuje czas poniżej 12 godzin. Co siódma firma wymaga czasu do 4 godzin (14%), tyle samo firm akceptuje nawet 2 dni i dłużej (14%). Niewielki odsetek firm natomiast (4%) akceptuje czas poniżej 1 godziny.

Jaki jest maksymalny akceptowany czas usunięcia awarii (skutków incydentu) systemu IT?



Nawet firmy, które mają satysfakcjonujące procedury, procesy, zabezpieczenia oraz usystematyzowane takie obszary jak zapewnienie ciągłości działania firmy poprzez funkcjonowanie business continuity planu, disaster recovery planu etc., nie jest wykluczone wystąpienie zagrożenia cyberinformatycznego. Możliwe jest zminimalizowanie ryzyka związanego z zakłóceniem nieprzerwanego działania organizacji spowodowanego incydentem, nie jest natomiast możliwe wyeliminowanie takich zagrożeń w 100%.

Nie jest więc zaskoczeniem, że 85% badanych firm uznaje, iż zapewnienie ciągłości działania

firmy będzie w najbliższych latach najistotniejsze z punktu widzenia bezpieczeństwa firmy.

To samo dotyczy ryzyka związanego z działaniami pracowników. Podnoszenie świadomości pracowników i szkolenia są wskazywane przez 86% badanych firm jako najważniejsze w zakresie zapewnienia bezpieczeństwa firmy. Badania wskazują, że to właśnie pracownik jest najsłabszym ogniwem w organizacji – przez naiwność, nieostrożność czy niedbałość pracowników, spółki mogą ponosić znaczne straty.

Przykładem incydentu związanego z przerwą w działalności ataku cybernetycznego może być zdarzenie, które dotknęło jednego z europejskich producentów wykorzystujących zaawansowane technologie do wytwarzania produktów, kiedy to w wyniku przypadkowego wgrania szkodliwego oprogramowania przez pracownika doszło do zakłócenia działania systemu komputerowego. W wyniku tego przestała działać linia do automatycznego sortownia i składania produktów. Producent miał procedury związane z zapewnieniem ciągłości działania i wdrożył już po 2 godzinach business continuity plan. Mimo że wszystkie ekipy zostały wezwane, zakład funkcjonował z dużymi opóźnieniami. Drugiego dnia producent, w ramach umów zawartych z firmami zapewniającymi pracowników, zaangażował dodatkowych pracowników do ręcznego składania produktów. Dopiero ósmego dnia zakład wrócił do normalnego trybu pracy. Szacowana szkoda finansowa związana z przerwą w działalności producenta wynosiła kilka milionów euro.

Marta Paruch (CHUBB),
Adam Gmurczyk (CHUBB)

Tysiące udanych rekrutacji menedżerów i specjalistów.

BIGRAM

search • career • HR

Szukasz dobrych specjalistów do obszaru cyberbezpieczeństwa?

We Love IT

Polujemy na najlepszych specjalistów IT

Skontaktuj się z nami, aby porozmawiać o skutecznej rekrutacji do IT.

Julia Chumakova
Konsultant Działu IT
721 001 684
julia.chumakova@bigram.pl

Marta Tkaczyk
Konsultant Działu IT
605 551 406
marta.tkaczyk@bigram.pl

www.bigram.pl

Polowanie na specjalistów ds. cyberbezpieczeństwa

Cyberbezpieczeństwo staje się coraz głośniejszym tematem w biznesie, również w obszarze rekrutacji. Coraz więcej firm zdaje sobie sprawę, iż mogą paść ofiarą zewnętrznych ataków, jak również ponieść straty finansowe lub utracić ważne dane w wyniku niefrasobliwych działań własnych pracowników.

Wielu pracodawców deklaruje, że ma już w strukturze organizacji dedykowane działy bezpieczeństwa lub zleca takie usługi firmom zewnętrznym. Rosną budżety przeznaczane na podniesienie świadomości użytkowników sieci firmowej i jakości zabezpieczeń. Aby utworzyć strategię bezpieczeństwa oraz zapobiec ewentualnym incydentom zagrażającym systemom danej organizacji niezbędne są osoby wyspecjalizowane w tej dziedzinie.

Specjaliści z obszaru security są poszukiwani w dużej mierze głównie przez sektor finansowo-ubezpieczeniowy oraz telekomunikacyjny. Na specjalistów ds. bezpieczeństwa polują również konsultanci zespołu specjalizującego się w IT w BIGRAM.

„Z naszych rekrutacyjnych doświadczeń wynika, iż najczęściej poszukiwani są kandydaci na stanowiska Pentesterów i Analityków 2 i 3 linii SOC. Bardzo często poszukiwani są także menedżerowie z 3-5 letnim doświadczeniem w zarządzaniu zespołem i dłuższym doświadczeniem w obszarze technologicznym, potwierdzonym certyfikatami dziedzinowymi. – ***deklaruje Julia Chumakova, konsultant BIGRAM, specjalizujący się w rekrutacjach IT*** *– W 2017 roku ten trend będzie się nasilał, co już możemy zaobserwować na podstawie umieszczanych ogłoszeń na internetowych portalach pracy."*

Aby zidentyfikować i pozyskać odpowiedniego kandydata rekruterzy stosują przeróżne metody. W przypadku kandydatów związanych z cyberbezpieczeństwem metoda poszukiwań bezpośrednich, direct search / headhunting na telefon firmowy nie jest najlepsza. Może ona wzbudzić nieufność, a nieraz nawet niechęć wśród kandydatów IT. Dlatego, aby zdobyć przychylność kandydatów lepiej nawiązywać kontakt droga mailową, za pośrednictwem social media lub rekomendacji.

Potencjalni kandydaci na stanowiska w obszarze IT security zazwyczaj niezbyt chętnie wdają się w dłuższe dyskusje, więc trzeba być dobrze przygotowanym do rozmowy by przedstawić taką ofertę, która takiego kandydata zainteresuje. Prezentacja korzyści i mocnych stron oferty powinna odnosić się do realnych bieżących warunków na rynku pracy w tym sektorze. W IT „atrakcyjność" ofert nie jest jednoznaczna, a jej ocena ulega dynamicznym zmianom. *„Najczęściej interesujące dla kandydatów są: nowa technologia, zakres zadań, wyzwań lub np. brak pracy zmianowej. Mniej ważna okazuje się marka pracodawcy. W przypadku stanowisk Pentesterów kandydaci również doceniają możliwość częściowej pracy zdalnej, ale najważniejszym motywatorem wciąż pozostaje oferta finansowa."–* ***doradza Julia Chumakova.***

Julia Chumakova
BIGRAM, Konsultant ds. Rekrutacji IT

CHUBB

Chubb to największa na świecie notowana na giełdzie spółka specjalizująca się w ubezpieczeniach majątkowych i osobowych.

Spółka Chubb prowadzi działalność w 54 krajach i oferuje osobom fizycznym i firmom ubezpieczenia majątkowe, a także ubezpieczenia wypadkowe, dodatkowe ubezpieczenia zdrowotne, reasekurację i ubezpieczenia na życie. Firma kieruje swoją bogatą ofertę produktów i usług do zróżnicowanej grupy klientów. Wyróżniają ją znaczący potencjał w zakresie dystrybucji, wzorowa kondycja finansowa, najwyższa jakość zapewnianej ochrony ubezpieczeniowej, ogromne doświadczenie w zakresie likwidacji szkód i globalna sieć oddziałów lokalnych.

Koncern dysponuje aktywami o wartości 150 mld USD, a wartość orientacyjna składek przypisanych brutto wynosi 37 mld USD. Dzięki temu główne firmy ubezpieczeniowe wchodzące w skład koncernu mogą pochwalić się bardzo wysokimi ocenami kondycji finansowej (ocena AA przyznana przez agencję Standard & Poor's oraz A++ przyznana przez agencję A.M. Best). Spółka macierzysta Chubb notowana jest na Nowojorskiej Giełdzie Papierów Wartościowych (NYSE: CB) i wchodzi w skład indeksu S&P 500.

Więcej informacji:
www2.chubb.com/pl-pl/

Kontakt:
Marta Paruch:
e-mail: Marta.Paruch@Chubb.com

Adam Gmurczyk:
e-mail: Adam.Gmurczyk@Chubb.com

Cube Research

To, co robimy w Cube Research przekłada się na realne zyski firm z którymi pracujemy. Większa sprzedaż wśród nowych klientów, większa sprzedaż i lepsze relacje z klientami dotychczasowymi, zwrócenie uwagi potencjalnych klientów i wyróżnienie się spośród konkurencji.

Pracujemy z różnymi firmami od tych bardzo dużych do całkiem niewielkich startupów. Zazwyczaj udaje nam się znaleźć optymalny model współpracy. Czerpiemy satysfakcję z pracy z naszymi klientami i ich sukcesów. Sukces naszego klienta jest naszym sukcesem. Gdy nasi klienci zarabiają – my także zarabiamy.

Zapraszamy do kontaktu – sprawdźmy czy możemy pomóc w realizacji celów Twojej firmy.

Więcej informacji:
www.cuberesearch.pl

Kontakt:
Michał Berezowski
e-mail: berezowski@cuberesearch.pl

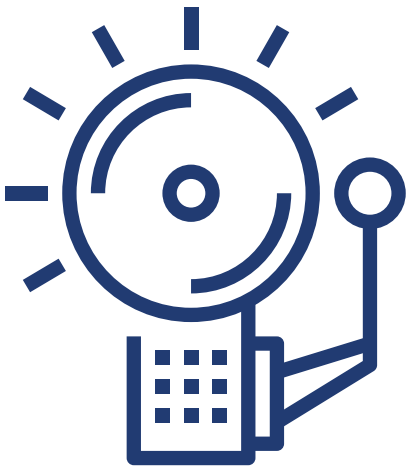
Michał Pastuszka:
e-mail: pastuszka@cuberesearch.pl

Anna Bus:
e-mail: a.bus@cuberesearch.pl

Building a better working world

EY

EY jest światowym liderem rynku usług profesjonalnych obejmujących usługi audytorskie, doradztwo podatkowe, doradztwo biznesowe i doradztwo transakcyjne. Nasza wiedza oraz świadczone przez nas najwyższej jakości usługi przyczyniają się do budowy zaufania na rynkach kapitałowych i w gospodarkach całego świata. W szeregach EY rozwijają się utalentowani liderzy zarządzający zgranymi zespołami, których celem jest spełnianie obietnic składanych przez markę EY. W ten sposób przyczyniamy się do budowy sprawniej funkcjonującego świata. Robimy to dla naszych klientów, społeczności, w których żyjemy i dla nas samych.



Nazwa EY odnosi się do firm członkowskich Ernst & Young Global Limited, z których każda stanowi osobny podmiot prawny. Ernst & Young Global Limited, brytyjska spółka z odpowiedzialnością ograniczoną do wysokości gwarancji (company limited by guarantee) nie świadczy usług na rzecz klientów.

Więcej informacji: www.ey.com/pl
EY, Rondo ONZ 1, 00-124 Warszawa

Kontakt:

Zespół Zarządzania Ryzykiem Nadużyć:
Tomasz Dyrda, Dyrektor
tel.: +48 22 557 8746
e-mail: Tomasz.Dyrda@pl.ey.com

Grzegorz Idzikowski, Menedżer
tel.: +48 22 557 8845
e-mail: Grzegorz.Idzikowski@pl.ey.com

Zespół Zarządzania Ryzykiem Informatycznym:
Kazimierz Klonecki, Partner
tel.: +48 22 557 6356
e-mail: Kazimierz.Klonecki@pl.ey.com

Aleksander Ludynia, Starszy Menedżer
tel.: +48 32 760 7876
e-mail: Aleksander.Ludynia@pl.ey.com

#HACKING #BEZPIECZEŃSTWO
#SIEĆ #PROGRAMOWANIE
#KRYPTOGRAFIA

ebookpoint

CZY WIESZ,
ŻE KTOŚ CIĘ OBSERWUJE?
OCHROŃ SWOJE DANE PRZED HACKERAMI!

KUP EBOOKI HELION 50% TANIEJ!*

WEJDŹ NA *HTTP://EBOOKPOINT.PL/WYDAWCA/HELION*

Wybierz interesujące Cię ebooki i podaj w koszyku KOD:

62B37F

* Promocja jest ważna do dnia 31.03.2017 i obejmuje wyłącznie ebooki dostępne na stronie [http://ebookpoint.pl/wydawca/helion]. Rabat nie łączy się z innymi promocjami.