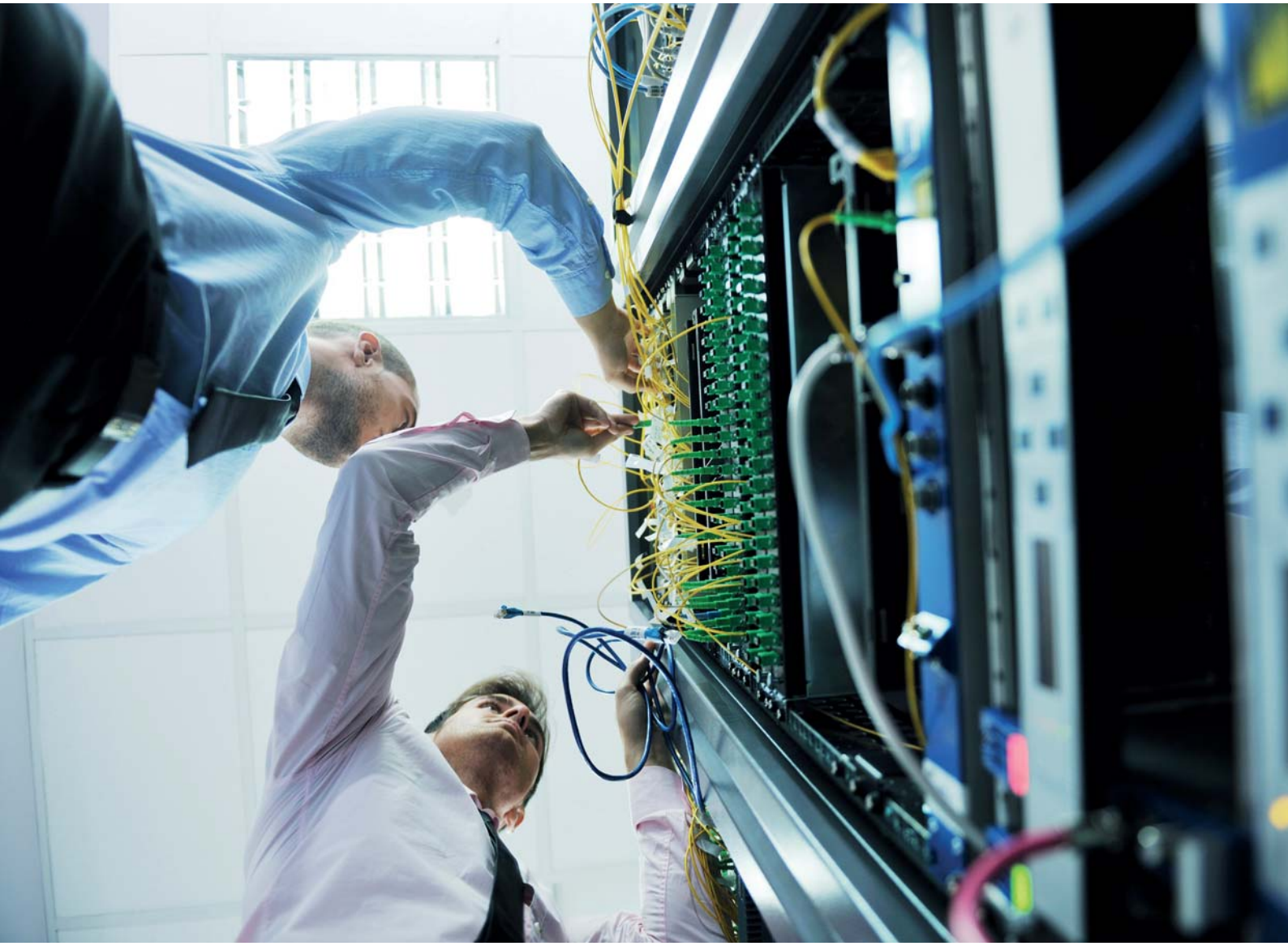
Styczeń 2016

W obronie cyfrowych granic

czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem



pwc

www.pwc.pl/badaniebezpieczenstwa


Plentzia
Kabiczes
Etxebarri
Basauri

Szanowni Państwo

Zmieniające się otoczenie biznesowe i rozwój technologii wymagają od liderów organizacji podejmowania właściwych decyzji, dających przewagę na konkurencyjnym rynku. Jednak czy pamiętają, że pozycja lidera jest powiązana z zaufaniem do sposobu zarządzania bezpieczeństwem informacji oraz skutecznością ochrony danych klientów?

Żyjemy w erze cyberataków i kryzysu zaufania. Liczy się szybka i sprawna reakcja na incydenty. Taka, która synchronizuje technologię, działania prawne i zarządzanie komunikacją. Cyberbezpieczeństwo przestało być trendem i stało się strategiczną koniecznością.

Jakie obawy mają polskie firmy i czego dotyczyły cyberataki i incydenty bezpieczeństwa? 31% ankietowanych naszego badania wskazało, że incydenty były związane z ujawnieniem lub modyfikacją danych. W 33% przełożyły się na straty finansowe, utratę klientów lub spór sądowy z tytułu naruszenia bezpieczeństwa informacji. Często wskazywaną konsekwencją cyberataku była także utrata reputacji – problem taki dotknął 16% polskich firm.

Firmy wchodzące w transformację cyfrową budują swoje modele biznesowe w oparciu o technologie i rozwiązania, otwierając nowe źródła przychodów. Często takie, które wychodzą poza ich dotychczasowe pole działania czy nawet sektor. To wymaga kompleksowego podejścia, które będzie obejmować nie tylko strategię, ale także jej skuteczne wdrożenie oraz monitoring ryzyk.

Porównując działania polskich i globalnych firm oraz analizując trendy, przygotowaliśmy pięć rad dla firm, wspomagających skuteczne przeciwdziałanie cyberzagrożeniom. Jesteśmy pewni, że będą one inspiracją i wsparciem przy kształtowaniu strategii bezpieczeństwa w Państwa organizacjach.

Piotr Urban
Partner, Zespół Zarządzania Ryzykiem

Adam Krasoń
Prezes PwC w Polsce

Spis treści:

Rozwój nowych technologii jest jednym z pięciu globalnych megatrendów kształtujących otaczającą nas rzeczywistość. Szczególnie dynamicznie ewoluują systemy komputerowe wspomagające zarządzanie wieloma dziedzinami. Rozwój ten przyniósł jednak za sobą także nowe zagrożenia. Liczba wykrytych incydentów naruszających bezpieczeństwo informacji wzrosła na świecie w stosunku do zeszłego roku o 38%. Wskazują na to globalne badania PwC „Światowy Stan Bezpieczeństwa Informacji 2016". Polskie badania, przeprowadzone na potrzeby tego raportu wykazały, że w naszym kraju odsetek ten był jeszcze wyższy i wyniósł aż 46%.

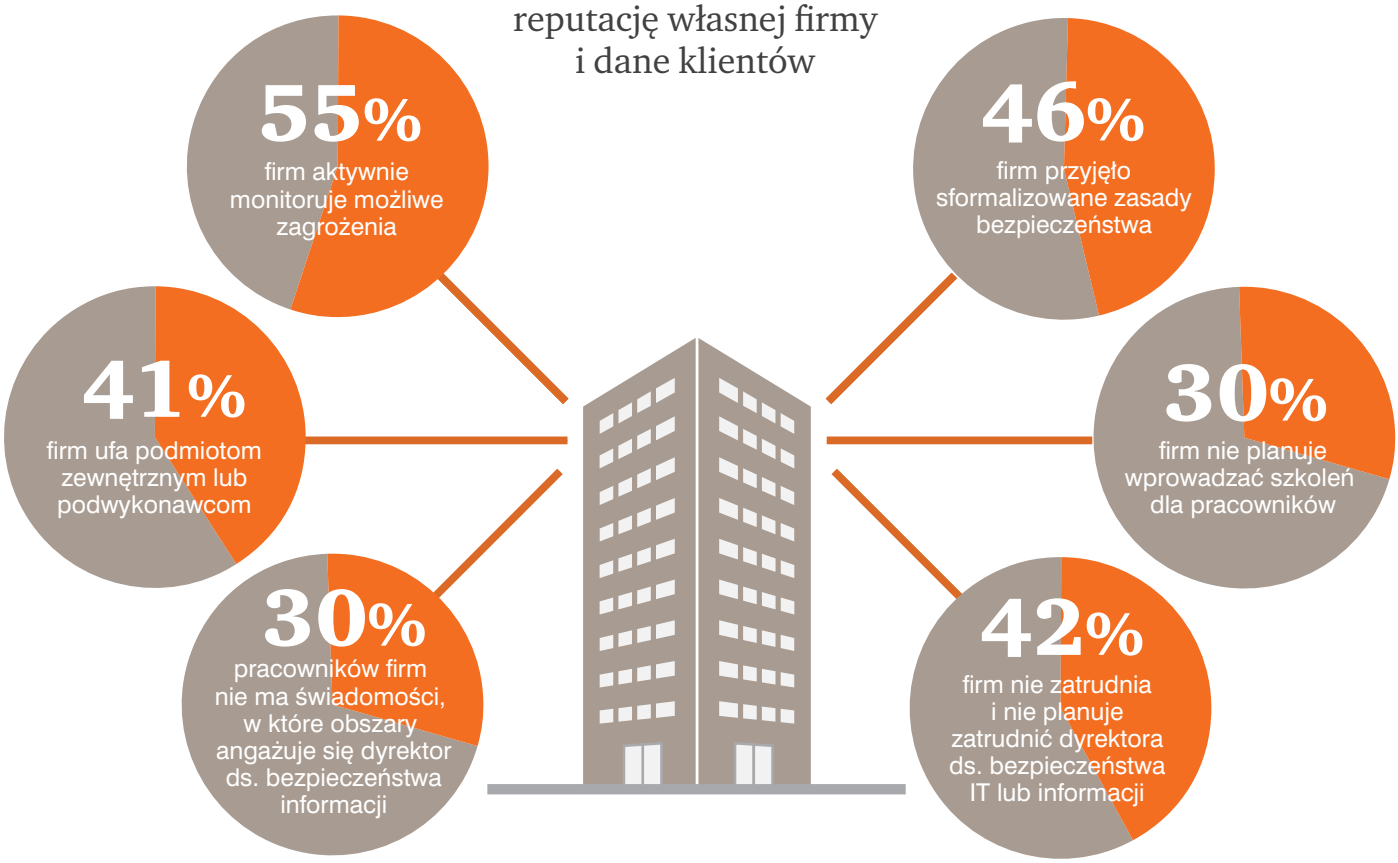
Skalę problemu pokazuje także liczba przeprowadzonych ataków. Średnio na każdą firmę w Polsce przypadało aż 126 cyberataków. A połowa badanych przez nas firm odnotowała więcej niż 6 cyber incydentów.

Jak na te statystyki reagują polskie firmy? Badania pokazały, że 65% respondentów uważa, iż podejmowane przez ich organizacje działania w zakresie cyberbezpieczeństwa są skuteczne. To i tak umiarkowany poziom optymizmu w stosunku do wyników badania „Digital IQ", przeprowadzonego przez PwC w 2015 roku, gdzie 88% ankietowanych stwierdziło, że ich przedsiębiorstwa dokonują dokładnej analizy potencjalnych zagrożeń bezpieczeństwa oraz prywatności w projektach związanych z technologiami cyfrowymi. Wnioski płynące z przeprowadzonej przez nas symulacji scenariuszy ataków dla polskich firm są również niezmienne. Średni czas uzyskania nieautoryzowanego dostępu do systemów i danych to nadal 4 godziny. Ponadto zaledwie jedno na sto poddanych testom przedsiębiorstw zauważyło, że jest obiektem ataku.

Do niedawna na celowniku cyberprzestepców był głównie sektor finansowy. Jednak coraz częściej ich ofiarami stają się firmy z sektora przemysłowego czy energetycznego. Systemy sterowania procesami produkcyjnymi (SCADA/ICS) są łatwym celem, szczególnie, że często nie były projektowane z myślą o integracji ze środowiskiem IT. W czasie napiętej sytuacji geopolitycznej możliwość przejęcia zdalnej kontroli nad infrastrukturą krytyczną przeciwnika staje się jedną z broni w arsenale cyberarmii. Przypadki takich ataków na polskie firmy obserwowaliśmy już w 2014 roku, a w ostatnich dniach 2015 nastąpiła rozległa awaria systemu dystrybucji energii u naszych sąsiadów spowodowana najprawdopodobniej atakiem hakerskim, przypisywanym grupie Energetic Bear, tej samej, która stała za atakami rok wcześniej. Systemy produkcyjne są szczególnie podatne na cyberatak ze względu na długi cykl życia i główny nacisk w eksploatacji na dostępność i wysoką utylizację. Warto zweryfikować, na jakie ryzyka są one wystawione i jak można je ograniczyć.

Poziom dojrzałości polskich firm

Działania skoncentrowane jedynie na osiąganiu zgodności z wymogami ustawowymi nie są obecnie wystarczające by chronić reputację własnej firmy i dane klientów



Rada 1. Działaj proporcjonalnie, czyli minimum już nie wystarcza

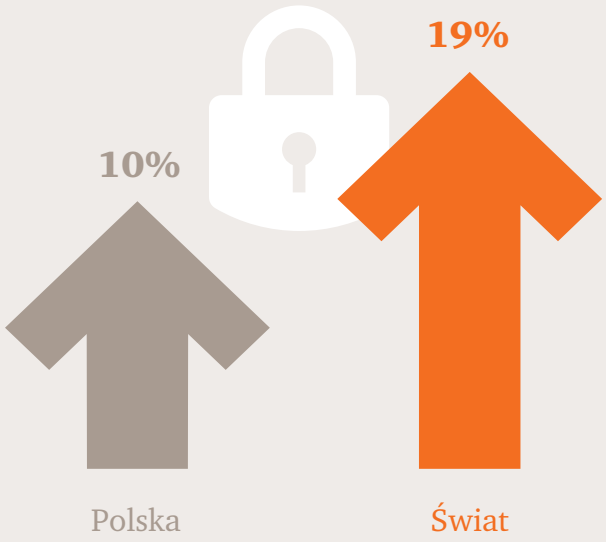
firm nie zatrudnia osoby odpowiedzialnej za bezpieczeństwo informacji

Łatwiej już było. Prognozy poparte danymi z ostatnich lat są jednoznaczne – poziom ryzyka będzie stale wzrastał. Pojawiające się cyberzagrożenia będą pociągać za sobą straty, związane z utratą reputacji, własności intelektualnej, przewagi konkurencyjnej – bądź też z ograniczeniem zdolności świadczenia usług. Będą one narażać organizacje na odpowiedzialność karną lub finansową, a także poważne straty wizerunkowe skutkujące utratą zaufania klientów. W tej sytuacji niezbędne jest wyjście poza podejmowanie tylko podstawowych, wymaganych prawem działań z zakresu cyberbezpieczeństwa.

Jak pokazują wyniki badania, w wielu firmach temat cyberzagrożeń wciąż nie znajduje się odpowiednio wysoko na agendzie zarządów – co dziwi szczególnie w kontekście wyników globalnego badania „PwC CEO Survey 2015" skierowanego do liderów firm. Prezesi światowych przedsiębiorstw wskazali na zagrożenia związane z cyberbezpieczeństwem jako na drugie najważniejsze ryzyko mogące zagrozić prowadzonym interesom. Tymczasem w Polsce często główne działania w tym obszarze wciąż koncentrują się jedynie na osiąganiu zgodności z wymogami ustawowymi, związanymi przede wszystkim z ochroną danych osobowych. Potwierdzają to zebrane przez nas odpowiedzi. 13% respondentów stwierdziło, że w ich firmach nie jest zatrudniona ani jedna osoba odpowiedzialna za bezpieczeństwo informacji, a co trzeci ankietowany zadeklarował, że w jego organizacji odpowiada za to tylko jeden pracownik. W obliczu rosnących zagrożeń warto, aby firmy nieposiadające specjalistów w tym zakresie rozważyły ich zatrudnienie lub skorzystanie ze wsparcia zewnętrznego, a firmy posiadające taki zespół pomyślały nad jego rozbudową w przyszłości. Naszą rekomendację kierujemy w szczególności do 42% ankietowanych, których firmy nie planują zatrudnienia dyrektora do spraw bezpieczeństwa IT lub informacji.

Część organizacji jest jednak świadoma skali zagrożeń. Potwierdza to deklarowany poziom wydatków, przeznaczanych na bezpieczeństwo informatyczne. Prawie połowa ankietowanych poinformowała, że ich firmy przeznaczają rocznie ponad pół miliona złotych na tę sferę. Udział tych wydatków w stosunku do całego budżetu IT zwiększył się z 5,5 do 10% a dalszy wzrost jest bardzo prawdopodobny. Warto zaznaczyć, że na świecie zgodnie z wynikami badania PwC „Światowy Stan Bezpieczeństwa Informacji 2016 ” udział ten wzrósł do 19%. Trend ten obserwujemy już w kolejnym badaniu. Owszem, biorąc pod uwagę światowe tendencje być może wciąż inwestujemy zbyt mało odważnie – ale kształtujący się trend jest jednoznacznie pozytywny.

Budżety firm przeznaczane na bezpieczeństwo informacji



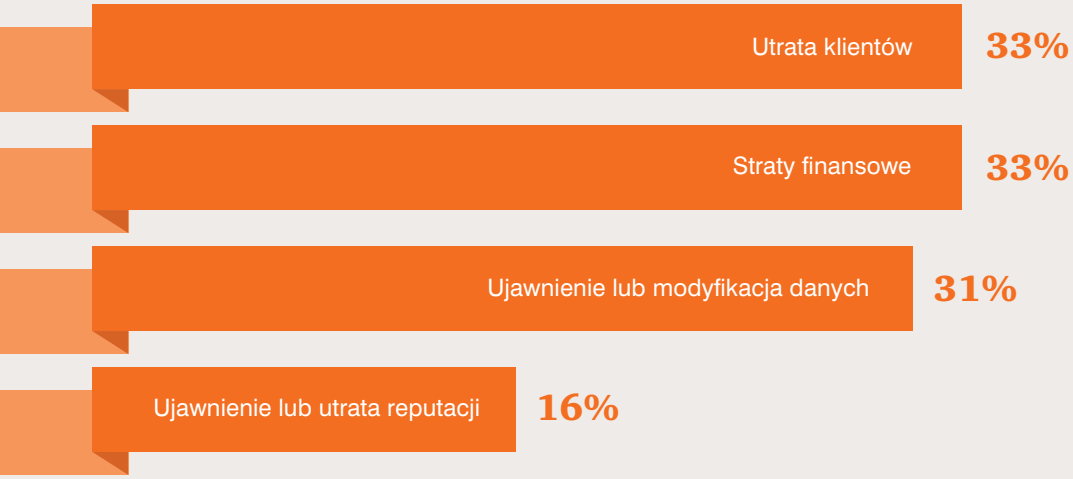
50%

firm wydaje rocznie 0,5 mln zł na bezpieczeństwo informacji

„Wzrost budżetu na cyberbezpieczeństwo to ważny i pozytywny moment w karierze CISO. Niestety, jak uczą przykłady spektakularnych wpadek globalnych organizacji, odpowiedź na pytanie „w co inwestować” jest przynajmniej równie istotna, jak odpowiedź na pytanie „ile”. Należy zawsze pamiętać, że tak naprawdę nie mówimy już o inwestycjach stricte w bezpieczeństwo IT. Wyzwań mogą nam dostarczyć wszystkie obszary działalności, w których wykorzystywane są technologie cyfrowe – sieci telekomunikacyjne, systemy SCADA w energetyce, firmach paliwowych i produkcyjnych, systemy sterowania ruchem, urządzenia medyczne… a wiele z tych obszarów jest bardziej istotnych dla prowadzonej przez firmę działalności biznesowej, a jednocześnie mniej doinwestowanych z punktu widzenia cyberbezpieczeństwa, niż „tradycyjne” IT”.

Rafał Jaczyński – *Dyrektor, Zespół Cyber Security w Polsce i Europie Centralnej*

Konsekwencje wystąpienia cyberataków w firmach



O ile jeszcze niewiele firm raportuje sześciocyfrowe straty, to pojawiają się już przypadki dłuższych, niż 5 dni przestojów w działalności firmy. Warto zauważyć, że taki przestój w działalności dla firm może oznaczać dużo większe straty – a w przypadku infrastruktury krytycznej niepowetowane straty w skali całego kraju.

Niepokojącym jest także fakt, że jedynie 46% firm w Polsce kieruje się jasno zdefiniowanymi formalnymi regułami bezpieczeństwa. Na świecie odsetek ten był niemal dwukrotnie wyższy i wyniósł 91%. Co ciekawe, 70% przedsiębiorstw deklaruje, że dostosowało się do wymogów ustawy o ochronie danych osobowych.

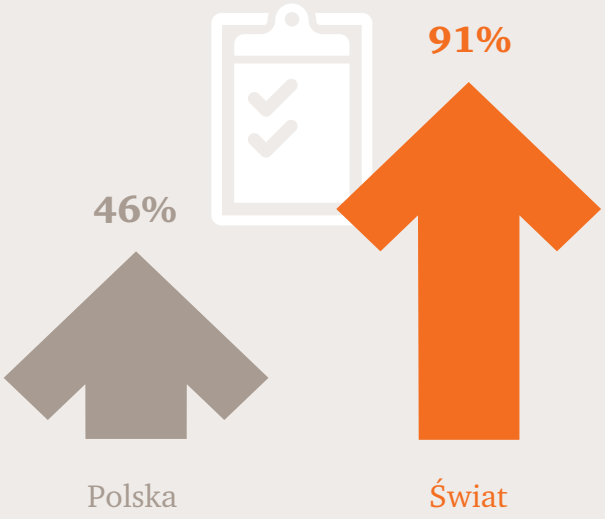
Oznacza to, że po kilkunastu latach obowiązywania w Polsce Ustawy o Ochronie Danych Osobowych wciąż niemal jedna trzecia firm nie osiągnęła z nią zgodności i powinna pilnie przystąpić do działania. Jest to tym bardziej istotne, że UE planuje wdrożyć regulacje, w oparciu o które możliwe byłoby ukaranie firmy karą w wysokości do 4% globalnych obrotów za uchybienia w ochronie danych osobowych. Planowane nowe rozporządzenie UE w zakresie ochrony danych osobowych nałoży jeszcze więcej obowiązków na przedsiębiorców. Ich wykonanie będzie wymagało nie tylko „odtwórczego" zastosowania przepisów, ale dokonania samodzielnej analizy możliwych zagrożeń i dobrania do nich odpowiednich środków zabezpieczających dane osobowe.

„W grudniu 2015 roku organy UE uzgodniły brzmienie dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (dyrektywa NIS). Celem dyrektywy jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji. Państwa członkowskie zobowiązane będą do zagwarantowania minimalnego poziomu krajowych zdolności poprzez ustanowienie właściwych organów ds. bezpieczeństwa sieci i informacji, powołanie zespołów reagowania na incydenty komputerowe (CERT) oraz przyjęcie krajowych strategii i planów współpracy w zakresie bezpieczeństwa sieci i informacji. Nowa regulacja nakłada także obowiązki na firmy. Przedsiębiorstwa w określonych krytycznych sektorach (sektor łączności elektronicznej, dostawcy usług społeczeństwa informacyjnego, np. platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych, sklepy z aplikacjami) oraz administracja publiczna będą zobowiązane do dokonania oceny zagrożeń, na jakie są narażone, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość krytycznych usług i dostaw towarów. Obowiązek zgłaszania incydentów (w zakresie ochrony danych osobowych) będzie nałożony na przedsiębiorców także na podstawie rozporządzenia UE o ochronie danych osobowych. Firmy będą musiały zastosować liczne środki w celu monitorowania incydentów, zapobiegania im oraz reagowania na ujawnione zagrożenia lub naruszenia”.

Anna Kobylańska – *adwokat, counsel w kancelarii prawnej PwC Legal*

firm nie dostosowało się do wymogów ustawy o ochronie danych osobowych

Firmy, które przyjęły sformalizowane zasady bezpieczeństwa



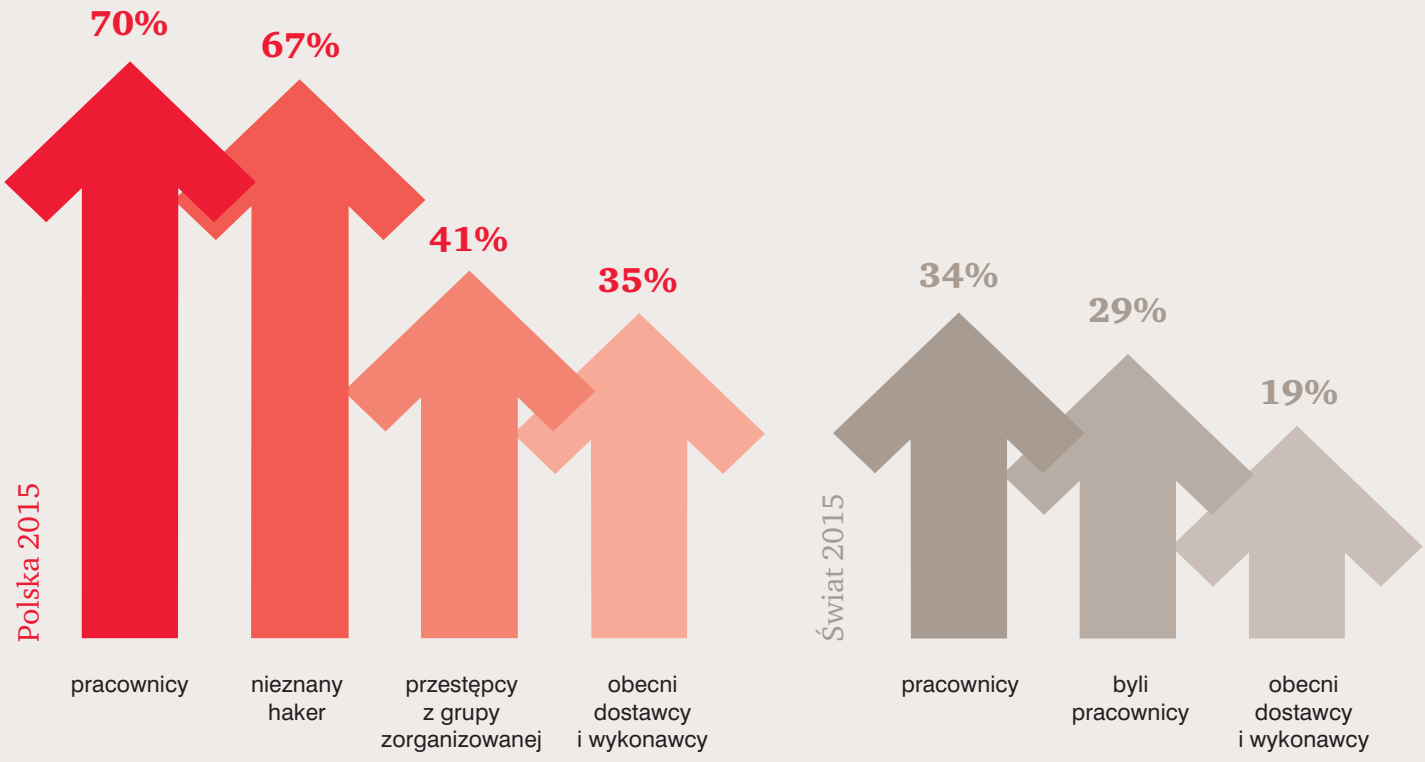
Rada 2. Przyjrzyj się najpierw najbliższemu otoczeniu

Aby lepiej chronić się przed zagrożeniami, a przede wszystkim skutecznie ich unikać, ważne jest prawidłowe zidentyfikowanie ich źródeł. Tylko dokładna analiza może przyczynić się do skutecznej eliminacji negatywnych zjawisk. Zdaniem 48% ankietowanych głównym źródłem zagrożeń w ubiegłorocznym badaniu byli pracownicy. W tym roku odpowiedź taką wybrało aż 70% respondentów. W ubiegłym roku na atak nieznanych hakerów wskazało 35% pytanych, w tym roku liczba takich odpowiedzi niemal się podwoiła: wskazało tak aż 67% ankietowanych.

Podobnie było z przestępczością zorganizowaną – liczba takich wskazań wzrosła w ujęciu rok do roku z 26 do 41%. Tendencja wzrostowa objęła również zagrożenia ze strony usługodawców – tutaj także widoczny jest wzrost z 17 do 35%.

Na świecie obecni pracownicy firm zostali wskazani jako źródło zagrożeń przez 34% ankietowanych, 29% wskazało na byłych pracowników, obecni usługodawcy zostali wymienieni przez 19% respondentów, zaś partnerzy biznesowi przez 16% ankietowanych.

Główne źródła cyberataków



70%

firm nie prowadzi monitoringu zachowań pracowników

Wielu zarządzających organizacjami zdaje sobie sprawę, że znaczna część zagrożeń pochodzi ze strony pracowników firmy. Mimo to, nie prowadzą monitoringu ich zachowań w celu eliminacji potencjalnie najbardziej ryzykownych działań – odpowiedzi takiej udzieliło 70% ankietowanych w naszym kraju. 60% ankietowanych zadeklarowało, że przeprowadza szkolenia dla swoich pracowników, zaś 6 na 10 respondentów z tej grupy stwierdziło, że ich firma wymaga, aby podmioty zewnętrzne przestrzegały zasad polityki bezpieczeństwa.

Chociaż 78% firm deklaruje, że posiada ogólną strategię bezpieczeństwa, to wciąż niemal 30% firm nie planuje żadnych szkoleń związanych z cyber-bezpieczeństwem. To ważne, gdyż do większości naruszeń bezpieczeństwa informacji dochodzi w środowisku biurowym oraz w związku z mediami społecznościowych, na co wskazało aż 64% respondentów. Często monitorowanie zachowań pracowników mylnie postrzegane jako inwigilacja.

Tymczasem zdarza się, że pracownicy mimowolnie stają się narzędziem ataku. Może się tak stać w sytuacji, gdy złośliwe oprogramowanie wykradnie ich dane dostępowe, i za ich pośrednictwem umożliwi nieuprawnione działania w systemie firmy. Sprawne monitorowanie pozwala wykryć nieprawidłowości i niestandardowe zachowania, które mogą być następstwem cyberataku.

„Skuteczne monitorowanie środowiska teleinformatycznego pod kątem bezpieczeństwa wymaga dobrej znajomości charakterystyki zagrożeń i ataków. Są one specyficzne i różnią się między sobą w zależności od typu przedsiębiorstwa. Podobnie jak formy ataków, które rozwijają się razem z pomysłowością atakujących i nowych podatności, tak odpowiednie scenariusze monitorowania powinny również ulegać ciągłemu rozwojowi. Wymyślenie i wstępne wdrożenie strategii monitorowania, to połowa sukcesu. Ważne jest umiejętnie rozwijanie w czasie przyjętych mechanizmów, należy stale je doskonalić, dostosowywać je do profilu ryzyka danej infrastruktury teleinformatycznej i zmieniających się zagrożeń. Monitorowanie i zapewnianie bezpieczeństwa to proces, a nie jednorazowa inwestycja. W przypadku dużych przedsiębiorstw często kluczowym staje się posiadanie odpowiedniego zespołu – Centrum Monitorowania Bezpieczeństwa, który odpowiadając za bieżące monitorowanie, odpowiednio reaguje i doskonali zabezpieczenia, w tym mechanizmy monitorowania, które ulegają dewaluacji wraz z postępem technologicznym i wymagają ciągłego rozwoju. Zakup nawet najlepszych technologii wspierających monitorowanie bezpieczeństwa bez odpowiedniej konfiguracji i jej stałego rozwoju, a także odpowiednich prezesów i kadry jest ślepą uliczką dającą fałszywe poczucie bezpieczeństwa, o czym należy szczególnie pamiętać”.

Tomasz Sawiak – *Wicedyrektor, Zespół Cyber Security Technology Services*

Rada 3.
Przygotuj się na nowe

30%

firm w Polsce korzysta z chmury obliczeniowej

69%

firm na świecie korzysta z chmury obliczeniowej

Firmy chętnie korzystają z szans, jakie oferują im nowe technologie. Niestety oprócz wielu zalet, pociągają one za sobą niewystępujące wcześniej zagrożenia, które niezidentyfikowane i nieuświadomione w porę mogą stanowić ryzyka dla organizacji.

Jednym z coraz częściej stosowanych w wielu obszarach biznesowych rozwiązań staje się chmura obliczeniowa. Rozwiązanie to jest różnie oceniane również wśród specjalistów od bezpieczeństwa i ochrony danych osobowych. Warto zwrócić natomiast uwagę na zalety *cloud computingu* w zastosowaniach związanych z bezpieczeństwem. Coraz częściej rozwiązania dostarczane jako usługa dają mniejszym organizacjom możliwość skorzystania z niedostępnych wcześniej dla nich ze względów kosztowych narzędzi bezpieczeństwa, takich jak analityka danych, zarządzanie dostępem czy zaawansowane uwierzytelnianie. Duża moc obliczeniowa jest nie do przecenienia w sytuacji, kiedy zachodzi potrzeba przetwarzania dużych zbiorów danych.
W tym kontekście trzeba zauważyć dystans, jaki dzieli polskie firmy od przedsiębiorstw światowych – w badaniu globalnym 69% ankietowanych poinformowało, że korzysta z usług cyberbezpieczeństwa w chmurze. W Polsce chmura obliczeniowa jest wykorzystywana przez 30% firm.

„Chmura jest w porządku. W PwC stworzyliśmy narzędzia wykorzystujące moc analityczną chmury Google do analizy dużych zbiorów danych, koniecznej przy prowadzeniu dochodzeń związanych z incydentami bezpieczeństwa. Zbudowaliśmy też, wykorzystującą tę samą technologię, platformę do analizy zbieranych przez nas na całym świecie informacji klasy threat intelligence – danych zarówno wpisywanych przez naszych pracowników i partnerów, jak i pochodzących z naszych źródeł sieciowych. Nasze doświadczenia wskazują jasno, że w przypadku największych projektów analitycznych, jak i oczekiwań związanych z dostarczaniem informacji o zagrożeniach przekraczamy już możliwości tradycyjnych platform analitycznych".

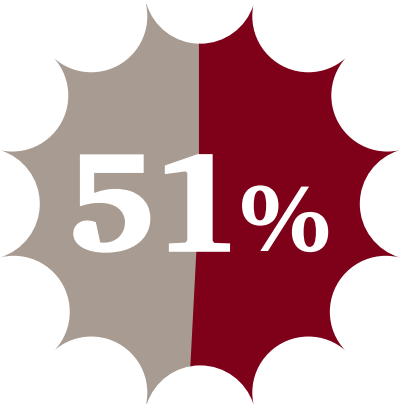
Rafał Jaczyński – *Dyrektor, Zespół Cyber Security w Polsce i Europie Centralnej*

Do modelowania i monitorowania cyberzagrożeń używane są także technologie *Big Data*. Podejście do bezpieczeństwa w oparciu o dane może doprowadzić do rewolucji w sposobie ich ochrony. Ponieważ do analityki danych potrzebne są znaczne moce obliczeniowe, dlatego bardzo często jest ona łączona z chmurą obliczeniową. Dane mogą służyć również do podniesienia poziomu zabezpieczeń – przykładowo zarządzania dostępem. Według raportu PwC „Światowy Stan Bezpieczeństwa Informacji 2016", technologię *Big Data* wykorzystuje 59% firm, w Polsce 67% ankietowanych stwierdziło, że jej nie używa i nie zamierza stosować w przyszłości.

Dziś wśród polskich badanych 50% zadeklarowało jednak, że ich firmy nie planują wprowadzenia oddzielnej strategii bezpieczeństwa dla chmury obliczeniowej, a 63% dla *Big Data*.

Większe zaskoczenie budzi fakt, że 51% respondentów stwierdziło, że ich organizacje nie planują implementacji strategii poświęconej bezpieczeństwu informacji w kontekście funkcjonowania mediów społecznościowych.

Warto w tym miejscu odwołać się do fraszki Andrzeja Waligórskiego – tej o pani Strusiowej. Nie wnikając w szczegóły, chodzi o to, że strategia strusia w odniesieniu do czyhających na nas zagrożeń działa niezwykle rzadko, a każda z nowych technologii teleinformatycznych musi być postrzegana zarówno jako szansa, jak i zagrożenie. Nie wypada więc chować głowy w piasek w obliczu zmian technologicznych, z których takie, jak chmura obliczeniowa, *Big Data* i media społecznościowe już dotykają każdej bez mała polskiej firmy.

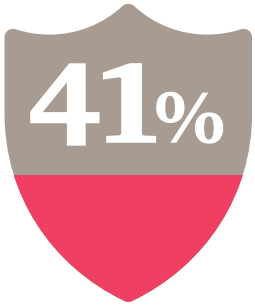


firm nie planuje wprowadzać strategii mediów społecznościowych

„Podczas audytów bezpieczeństwa oraz zarządzania środowiskiem informatycznym, w wielu organizacjach widać obszary, w których zarządzanie ryzykiem i bezpieczeństwem IT jest niewystarczające lub oparte wyłącznie na zakazach opisanych w procedurach. Brakuje kontroli nad działaniami administratorów, właściwego ograniczenia dostępu i rozdziału obowiązków w systemach IT, często słaba jest konfiguracja bezpieczeństwa platform. Często procesy zarządzania różnymi aplikacjami nie są ze sobą spójne i mają różne wymagania, pogłębiając zamieszanie i brak realnego nadzoru nad stanem całości środowiska IT. Jeśli firmy chcą zapewnić sobie bezpieczeństwo, konieczne jest całościowe podejście do tematu. Procesy muszą w sposób kompleksowy i spójny objąć kwestię zarządzania zmianą oraz projektami, z zapewnieniem zarówno jakości jak i bezpieczeństwa, już na poziomie architektury i projektowania rozwiązania IT".

Jacek Masny – *Wicedyrektor, Zespół Zarządzania Ryzykiem IT*

Rada 4.
Zaangażuj najwyższe szczeble



firm uważa, że zarząd powinien bezpośrednio finansować programy bezpieczeństwa informacji

Sprawne i bezpieczne funkcjonowanie organizacji jest możliwe wyłącznie w sytuacji, gdy obszar bezpieczeństwa jest traktowany z wystarczającym priorytetem i jest wspierany przez zarząd. Nie oszukujmy się – tzw. *„tone at the top”* ma fundamentalne znaczenie dla każdej dziedziny działalności firmy, której istotności nie będą w stanie obronić bezpośrednio dane sprzedażowe.

Fundamentalna rola zarządu w zapewnieniu cyberbezpieczeństwa jest oczywista. Wśród respondentów 41% stwierdziło, że to właśnie zarząd powinien bezpośrednio finansować programy bezpieczeństwa informacji. Zaangażowanie zarządu powinno obejmować również operacyjne zagadnienia bezpieczeństwa, w szczególności zarządzanie kryzysowe. W przypadku incydentów związanych z wyciekiem szczególnie wrażliwych informacji lub przestojem firmy wsparcie i działanie zarządu będzie niezbędne zarówno w celu ograniczenia strat finansowych, jak i konsekwencji prawnych.

„Zarządy firm coraz częściej rozumieją, że projektów bezpieczeństwa nie można traktować jako wyizolowanych i oderwanych od kontekstu działania całej firmy. Nie można także opierać uruchomienia tego typu projektów jedynie na wyniku wyliczanego prognozowanego zwrotu z inwestycji, ponieważ przy takim traktowaniu po prostu nie sposób zidentyfikować go w krótkim okresie. Zmienia się myślenie o bezpieczeństwie. Dlatego w inicjatywach, gdzie bezpieczeństwo stanowi istotny aspekt biznesowy – jest istotną wartością dodaną dla celu biznesowego, w analizach zaczyna być traktowany jako część zwrotu z inwestycji całego projektu. Przykładem może być uruchomienie nowej bankowości mobilnej, gdzie niezbędną częścią projektu jest właściwe zabezpieczenie świadczonej przez bank usługi. W tym przypadku wdrażane mechanizmy podnoszą bezpieczeństwo i wartość nowego rozwiązania. Zainwestowanie odpowiednich środków finansowych w budowę mechanizmów bezpieczeństwa jest konieczne. W przeciwnym razie usługa może okazać się bezwartościowa, przynosząc przedsiębiorstwu poważne straty lub poważne naruszenie wizerunku, co szybko doprowadzi do utraty klientów. Zupełnie innym przypadkiem są inwestycje związane z podwyższeniem poziomu bezpieczeństwa infrastruktury informatycznej (wynikające np. z przyjętej strategii firmy) lub spełnieniem regulacji. Oba przypadki nie mają bezpośredniego przełożenia na projekty biznesowe, a stanowią podwaliny pod bezpieczeństwo usług już funkcjonujących w organizacji. Wyliczanie zwrotu z inwestycji tego typu prac jest niezwykle trudne”.

Jacek Sygutowski – *Dyrektor, Zespół Cyber Security Technology Services*
Marcin Makusak – *Wicedyrektor, Zespół Zarządzania Ryzykiem*

30%

firm nie ma świadomości, w które obszary angażuje się dyrektor ds. bezpieczeństwa informacji w ich firmie

Skuteczną metodą podnoszenia poziomu cyberbezpieczeństwa jest osobiste zaangażowanie prezesa firmy w działania na rzecz bezpieczeństwa. Częstym rozwiązaniem usprawniających przepływ informacji o istniejących lub potencjalnych zagrożeniach, a także o możliwościach przeciwdziałania, jest skracanie ścieżki raportowania od osoby odpowiedzialnej za zarządzanie cyberbezpieczeństwem. Już w tej chwili w wielu firmach dyrektor do spraw bezpieczeństwa informacji podlega bezpośrednio prezesowi zarządu. Tak dzieje się w 50% badanych organizacji. Samo optymalne umiejscowienie w strukturze organizacyjnej nie zwalnia jednak szefa bezpieczeństwa z konieczności wykazywania inicjatywy. Zwraca uwagę fakt, że 30% ankietowanych nie ma świadomości, w które obszary angażuje się dyrektor do spraw bezpieczeństwa informacji, nie znając ani zakresu odpowiedzialności, ani rodzaju wykonywanych przez niego zadań.

Oprócz kwestii strategicznych i finansowych, jednym z istotnych zadań zarządów firm jest wsparcie kultury bezpieczeństwa informacji. Wiele zagrożeń można wyeliminować działając prewencyjnie i uzmysławiając pracownikom, że istnieje grupa zachowań narażających firmę na utratę posiadanych danych czy wykorzystanie jej infrastruktury do ataku na inny podmiot.

O potrzebie funkcjonowania w organizacji tego rodzaju wsparcia jest przekonanych 38% ankietowanych. Dodatkowo, w 72% firm cyberbezpieczeństwo wciąż postrzegane jest bardzo wąsko i traktowane tylko jako część – a nawet problem – działu IT. Często brakuje zrozumienia wpływu ryzyk związanych z cyberbezpieczeństwem na poziom ryzyka w całej organizacji i jej finanse.

„Ryzyka związane z bezpieczeństwem informacji coraz częściej pojawiają się na mapach ryzyk zarządów polskich spółek, co jest pozytywnym trendem. Niestety, ich ocena nadal nie jest oparta na rzetelnych danych, na przykład analizie incydentów. Brakuje również wiarygodnych informacji dotyczących efektywności mechanizmów zarządzania bezpieczeństwem informacji, uzyskanych na przykład w wyniku kompleksowych audytów. Bardzo istotna jest rola audytu wewnętrznego, który coraz częściej ujmuje w swoich planach aspekty cyberbezpieczeństwa. Audytorzy wewnętrzni zazwyczaj zlecają takie zadania podmiotom zewnętrznym wiedząc, jakie ograniczenia stoją przed nimi. Gorsze od braku informacji na temat przygotowania organizacji na ryzyka związane z bezpieczeństwem informacji jest jedynie fałszywe poczucie bezpieczeństwa, uzyskane w wyniku źle przeprowadzonego audytu”.

Piotr Rówiński – *Dyrektor, Zespół Zarządzania Ryzykiem*

firm traktuje cyberbezpieczeństwo jako część zakresu obowiązków działu IT

Tymczasem obecnie CISO lub CIO musi być nie tylko ekspertem w dziedzinie cyberbezpieczeństwa, ale także zarządzania ryzykiem, a także generalnie – zarządzania. Musi mieć dostęp do najważniejszych osób w firmie, aby naświetlać im kwestie związane z cyberbezpieczeństwem. Kluczowe stają się odpowiednie zdolności komunikacyjne, umożliwiające przejrzysty sposób informowania otoczenia, w szczególności w sytuacjach kryzysowych.

Cyberbezpieczeństwo jest także jednym z elementów, który powinien zostać uwzględniony przy fuzjach i przejęciach. Przed transakcją zasadne może być przeprowadzenie due diligence dotyczącego właśnie obszaru cyberbezpieczeństwa w przejmowanej spółce. Przyłożenie niedostatecznej wagi do tych kwestii może narażać firmę na ryzyko. Przestępcy mogą infiltrować mniejsze organizacje i czekać na ich przejęcie przez duże przedsiębiorstwa, gdzie po integracji systemów uzyskają dostęp do interesujących ich informacji. Oceniając ryzyko cyberbezpieczeństwa podczas transakcji, warto wziąć pod uwagę następujące kwestie: kraj, w którym znajduje się siedziba, i rynki, na których działa spółka. Analizy wymagają także: sektor, w którym działa firma i przyjęte praktyki z zakresu cyberbezpieczeństwa oraz liczba i powody występujących w ostatnim czasie incydentów.

„Współczesny CISO ma trudne zadanie. Kluczowymi czynnikami sukcesu w zakresie skuteczności ochrony aktywów informacyjnych firmy są kompetencje związane z umiejętnościami komunikacyjnymi oraz zarządzaniem ryzykiem. Pierwsza pozwala z jednej strony przekonać zarząd i działy biznesowe, że nakłady ponoszone na cyberbezpieczeństwo nie stanowią tylko „zła koniecznego", ale przyczyniają się do budowy wartości firmy i ograniczają ekspozycję na ryzyko. Z drugiej strony komunikacja CISO z ekspertami cyberbezpieczeństwa i IT jest ważna dla efektywnego przekładania celów strategicznych na działania operacyjne. Drugim krytycznym składnikiem kompetencyjnym jest zdolność CISO do właściwej oceny wagi zagrożeń i podatności dla bezpieczeństwa informacji".

Szymon Sobczyk – *Wicedyrektor, Zespół Cyber Security Technology Services*

„Jednym z motywów przejęcia firmy może być przejęcie własności intelektualnej, lub innych zasobów informacyjnych stanowiących o wartości firmy. Warto zastanowić się – i sprawdzić – czy przypadkiem ta unikatowa wartość intelektualna nie znajduje się wskutek ataku w domenie publicznej i jakie jest ryzyko, że celowo lub przypadkowo opuści przejmowaną firmę zanim staniemy się jej właścicielem. Po zrealizowaniu przejęcia, a przed połączeniem zasobów informatycznych warto z kolei przyjąć w pierwszej fazie założenie, że łączymy się z niezaufaną siecią – i sprawdzić, czy nasze mechanizmy kontrolne będą w stanie przy takim założeniu dalej mitygować ryzyko związane z integracją. Dlatego zawsze warto przeprowadzać testy bezpieczeństwa oraz poszukiwania złośliwego oprogramowania klasy APT również w trakcie fuzji i przejęć".

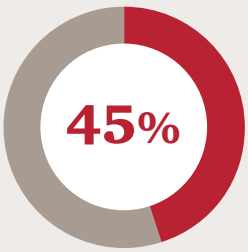
Patryk Gęborys – *Wicedyrektor, Zespół Cyber Security*

Rada 5.
Szukaj wsparcia na zewnątrz

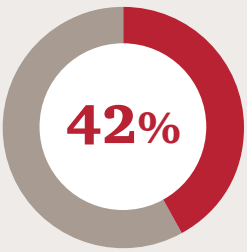
W przypadku cyberbezpieczeństwa duże znaczenie ma dzielenie się wiedzą z innymi podmiotami, które mogą pomóc w zapobieganiu i przeciwdziałaniu zagrożeniom. Tu pojawia się jednak problem, a mianowicie brak zaufania i ograniczona chęć do kooperacji. Tylko 41% ankietowanych stwierdziło, że ufa podmiotom zewnętrznym lub podwykonawcom, co powoduje ograniczoną chęć do nawiązywania współpracy i zawęża obszar, na którym może być ona realizowana. Zgodnie z deklaracjami ankietowanych, współpracę z przedsiębiorstwami z branży na rzecz poprawy bezpieczeństwa informacji nawiązało 45% firm, jednak niemal tyle samo, bo 42% nie współpracuje z partnerami. Przyczyną takiej sytuacji jest właśnie brak zaufania, obawa przed korzystaniem z zewnętrznych źródeł informacji, a także przekonanie, że tego rodzaju współpraca może stanowić zagrożenie dla bezpieczeństwa danych osobowych.

Oczywiście nawet najbardziej rozbudowana kooperacja i wysiłki mające na celu ochronę firmy mogą okazać się nieskuteczne. Jedną z możliwości minimalizacji negatywnych skutków może być zakup polisy ubezpieczeniowej od cyberzagrożeń. W Polsce nie jest to jednak popularne, gdyż jedynie 8% reprezentantów firm zadeklarowało, że ich firmy zdecydowały się na zakup takiego produktu. Na świecie odsetek ubezpieczonych jest znacznie wyższy. Zgodnie z wynikami globalnego badania „Światowy Stan Bezpieczeństwa Informacji 2016", na zakup polisy zdecydowało się 59%.

Współpraca z podmiotami zewnętrznymi

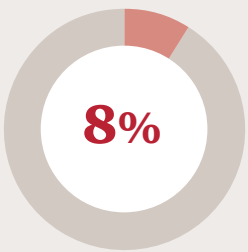


firm nawiązało współpracę z innymi podmiotami z branży na rzecz poprawy bezpieczeństwa informacji

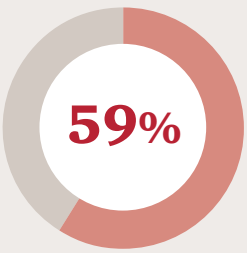


firm nie nawiązało współpracy z innymi podmiotami z branży na rzecz poprawy bezpieczeństwa informacji

Ubezpieczenie od cyberzagrożeń



firm w Polsce posiada polisę ubezpieczeniową od cyberzagrożeń



firm na świecie posiada polisę ubezpieczeniową od cyberzagrożeń

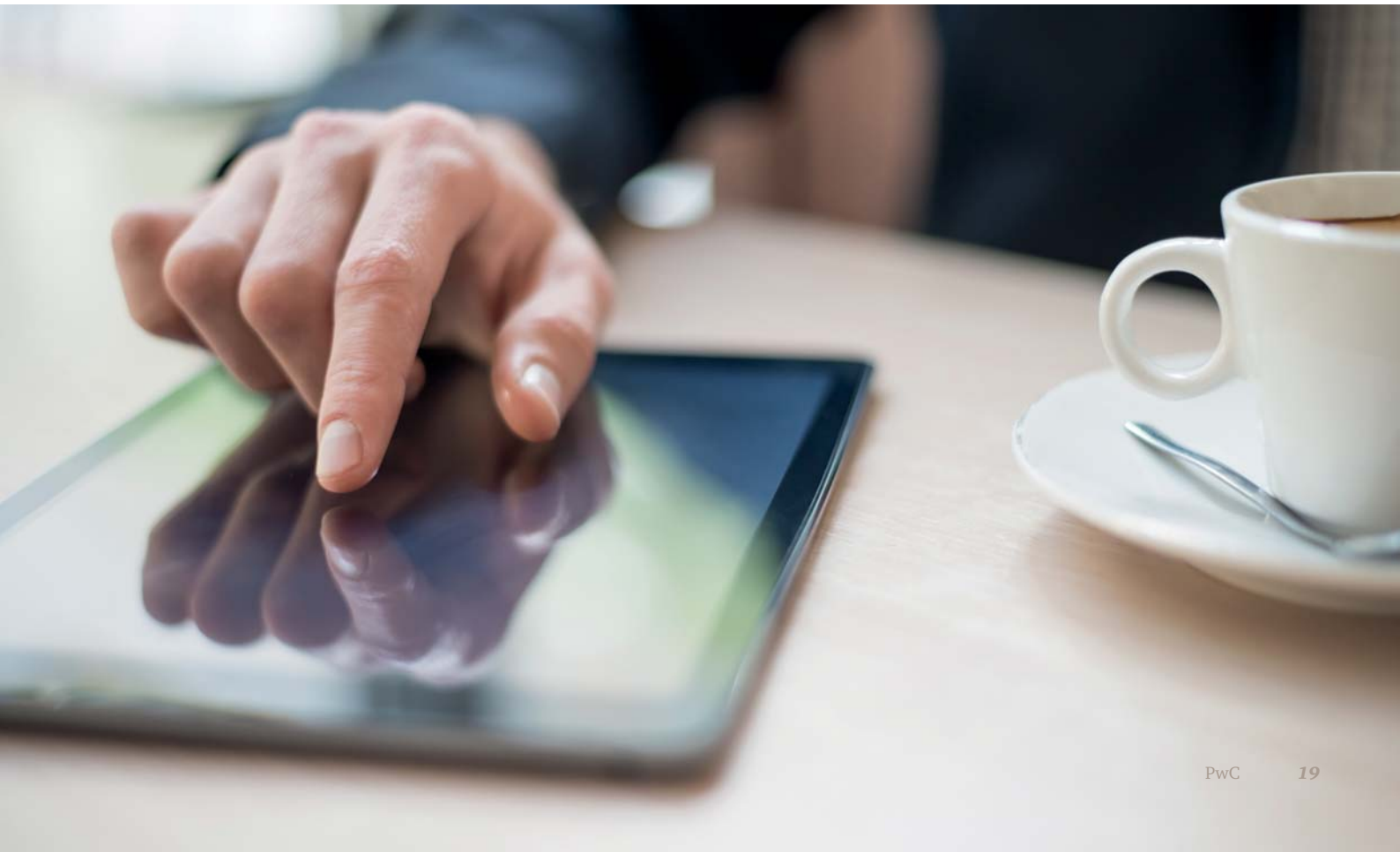
„Polski rynek powoli dojrzewa do kwestii ubezpieczeń od skutków związanych z cyberatakiem. Spoglądając na rynki dojrzalsze widać, że wysyp produktów w tym obszarze jest jeszcze przed nami. Ubezpieczenie z pewnością nie może stanowić alternatywy wobec zabezpieczeń techniczno-logicznych, które chronią informację i dobre imię firmy, ale zdecydowanie może okazać się dobrym uzupełnieniem tych działań. W szczególności warto przemyśleć strategię ubezpieczeniową dla wrażliwych danych klientów firmy. W przypadku ich ujawnienia w sposób niepożądany zabezpieczy to firmę od problemów finansowych wynikających np. z lawiny roszczeń od niezadowolonych klientów. Spoglądając w niedaleką przyszłość widać, że ubezpieczenia od skutków cyberataków będą odgrywały coraz większe znaczenie – z jednej strony na wagę stawiamy inwestycje w zabezpieczenia techniczno-logiczne oraz ubezpieczenie, z drugiej skutki skutecznego ataku".

Marcin Makusak – *Wicedyrektor, Zespół Zarządzania Ryzykiem*

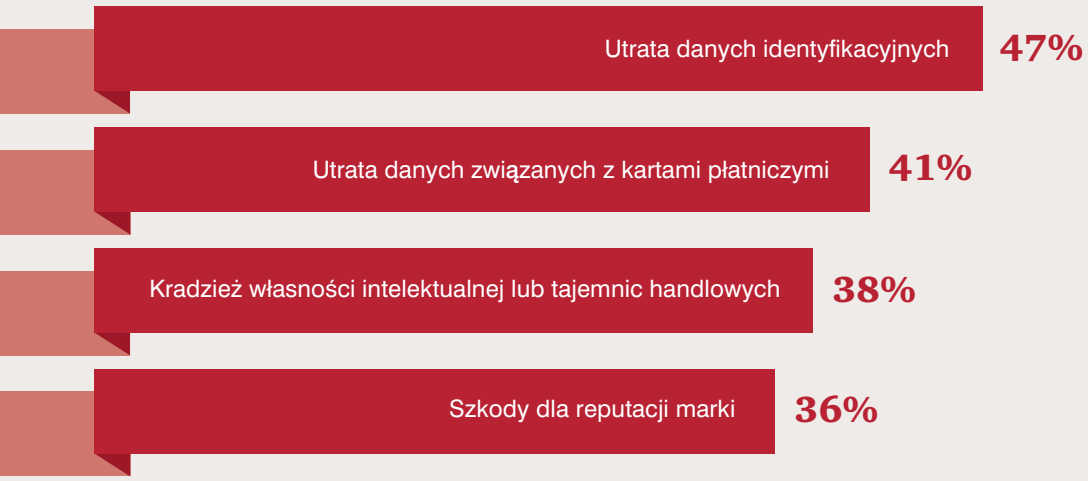
Z tytułu jakich strat firmy ubezpieczeniowe na świecie najczęściej wypłacały odszkodowania? 47% ankietowanych wskazało, że wypłata odszkodowania związana była z utratą danych identyfikacyjnych. 41%, że wiązały się z utratą danych związanych z kartami płatniczymi, 38% wypłat było następstwem kradzieży własności intelektualnej lub tajemnic handlowych, zaś 36% wiązało się ze szkodami dla reputacji marki.

Polisy ubezpieczeniowe mają bardzo wiele wariantów. Mogą obejmować zniszczenie danych, ataki powodujące odmowę obsługi oraz kradzież i wymuszenie. Fakultatywnie także reakcję na incydenty i koszty napraw, a także dochodzenie i koszty audytu cyberbezpieczeństwa. Niektóre firmy ubezpieczeniowe rozszerzają swoją ofertę o polisy umożliwiające pokrycie wartości utraconej własności intelektualnej, reputacji, wizerunku i marki oraz awarie infrastruktury. Trzeba jednak mieć na uwadze, że dużą trudność stanowi oszacowanie, jaką wysokość powinna mieć zakupiona polisa oraz jaka może być skala szkód poniesionych w skutek cyberataku. To bardzo ważne, gdyż z reguły zakup ubezpieczenia wymaga przeznaczenia większej sumy z budżetu, zatem precyzyjne oszacowanie potrzeb firmy odgrywa tutaj duże znaczenie.

Warto w tym miejscu dodać, że na świecie jest to jeden z najszybciej rosnących segmentów ubezpieczeń. Jak pokazuje globalny raport PwC „Światowy Stan Bezpieczeństwa Informacji 2016", jego wartość wzrośnie z 2,5 mld dolarów w 2015 roku do 7,5 mld dolarów w 2020 roku.



Odszkodowania za wystąpienie cyberataków



Dodatkowym efektem zakupu polisy ubezpieczeniowej jest lepsze rozpoznanie istniejących zagrożeń i skuteczniejsze przygotowanie się do nich. To następstwo wymogów ubezpieczycieli, którzy obligują firmy do analizowania swoich możliwości zapobiegania cyberatakom i bieżącego monitorowania poziomu zagrożeń. Pamiętajmy, że ubezpieczyciele nie zaproponują firmie korzystnego ubezpieczenia od zdarzeń, które ocenią jako pewne – bez zachowania podstawowej higieny bezpieczeństwa potwierdzonej najczęściej niezależną weryfikacją nie będziemy mogli liczyć na polisę.

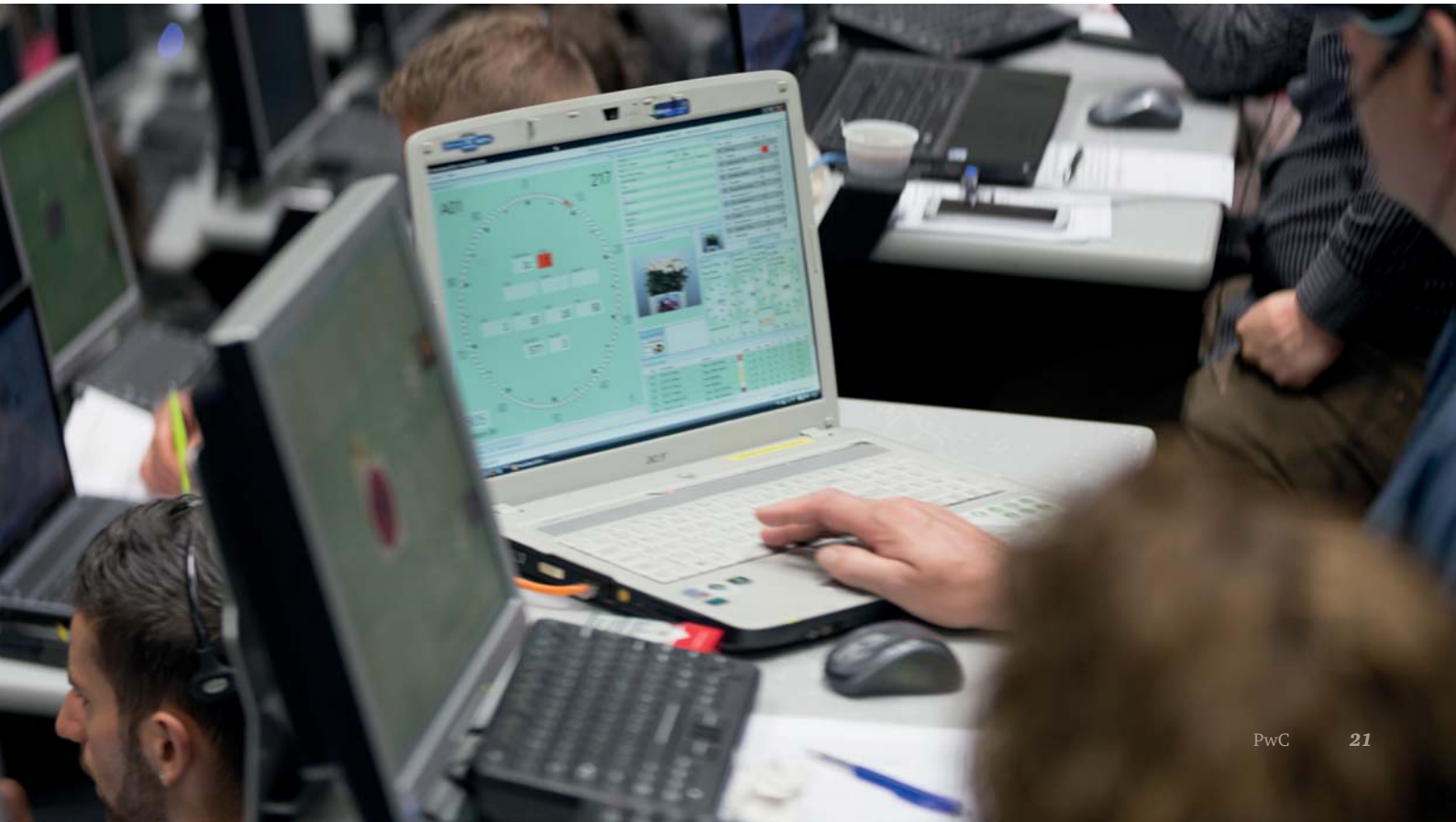
Czynnikiem ułatwiającym współpracę pomiędzy przedsiębiorstwami może być powstawanie agend rządowych zbierających dane na temat przeprowadzonych ataków oraz ułatwiających wymianę informacji. Ważną funkcję mogą pełnić także organizacje branżowe tworzące platformy do wymiany danych o zagrożeniach. Taka wymiana sprzyja również budowaniu świadomości na temat istniejących zagrożeń. Sytuacja może być bardziej skomplikowana, gdy współpracę chcą nawiązać podmioty z różnych krajów. Rozbieżności w ich systemach prawnych mogą powodować utrudnienia na przykład związane z ochroną danych osobowych, a nawet z tym, co w poszczególnych krajach jest uznawane za dane osobowe.

Z bezpieczeństwem jest trochę tak, jak z jazdą po drogach – po pierwsze, przewidujmy rozwój sytuacji i nie dajmy się zaskoczyć. Po drugie, w razie incydentu nie traćmy głowy. Po trzecie, pamiętajmy, że ubezpieczenie nie zapobiegnie wypadkowi, ale może ograniczyć jego konsekwencje dla naszego budżetu.

Nie dajmy się trafić cyberprzestępcom i nie strzelajmy sobie sami w stopę – zbierajmy informacje o tym, co nadchodzi, dbajmy o podstawową higienę w zakresie bezpieczeństwa, o jakość procesów, technologii i personelu odpowiedzialnego za systemy teleinformatyczne. Kiedy wydarzy się incydent pamiętajmy, że potrzebny nam będzie technik, który zajmie się informatyczną stroną zagadnienia, prawnik, który zwróci uwagę na obowiązki i konsekwencje prawne, i rzecznik, który efektywnie będzie komunikował się z rynkiem i udziałowcami. Tak, to wszystko będzie nas słono kosztowało, ale nie tyle, co utrata rynku czy przewagi konkurencyjnej reputacji i zaufania klientów bądź zdolności do prowadzenia działalności.

„Cyberbezpieczeństwo naszego biznesu jest tak samo ważne, jak jakiekolwiek inne bezpieczeństwo. Na zakłócenie jego poziomu czyhają również międzynarodowe zorganizowane grupy przestępcze, szukające finansowania swojej działalności przestępczej za pośrednictwem sieci. Dotyczy to również przestępczości gospodarczej, karuzele i wyłudzenia podatkowe zostają przeniesione do cyberprzestrzeni. Do prowadzenia tego procederu często zatrudniani są wysoko wykwalifikowani eksperci w dziedzinie informatyki, bezpieczeństwa sieci, a także cyberprzestępcy. Zajmują się oni oprócz kamuflowania działań przestępczych, badaniem najnowszych podatności w systemach, budowaniem złośliwego oprogramowania pozwalającego na wykradanie tzw. klejnotów koronnych. Konieczne jest dlatego minimalizowanie skutków zdarzenia, zabezpieczenie dowodów działania sprawców w celu podjęcia postępowania przed sądem karnym lub cywilnym. Wiąże się to również z tym, iż instytucje państwowe dostrzegły konieczność rozwijania cyberbezpieczeństwa kraju (rozbudowa organów ścigania, regulacji prawnych) i że ten proces nie może odbywać się bez współpracy agend rządowych z podmiotami sektora prywatnego”.

Marcin Klimczak – *Partner, Lider Zespołu Usług Śledczych i Zarządzania Ryzykiem Nadużyć*



Metodologia

Raport został przygotowany na bazie badania, w którym wzięło udział 126 polskich ekspertów zajmujących się IT i bezpieczeństwem informacji. Badanie zostało przeprowadzone jesienią 2015 roku metodą ankiety online. Wyniki badania zostały opracowane na podstawie agregacji udzielonych odpowiedzi.

Kontakt

Piotr Urban
Partner, Lider Zespołu Zarzadzania Ryzykiem w Polsce
Tel.: +48 502 184 157
E-mail: piotr.urban@pl.pwc.com

Rafał Jaczyński
Dyrektor, Zespół Cyber Security w Polsce i Europie Centralnej
Tel.: +48 519 507 122
E-mail: rafal.jaczynski@pl.pwc.com

Jacek Sygutowski
Dyrektor, Zespół Cyber Security Technology Services
Tel.: +48 519 504 954
E-mail: jacek.sygutowski@pl.pwc.com

Magda Sarzyńska
Menedżer ds. Rozwoju Biznesu
Tel.: +48 519 507 153
E-mail: magdalena.sarzynska@pl.pwc.com

www.pwc.pl/badaniebezpieczenstwa

Publikacja została przygotowana wyłącznie w celach ogólnoinformacyjnych i nie stanowi porady w rozumieniu polskich przepisów.
Nie powinni Państwo opierać swoich działań/decyzji na treści informacji zawartych w tej publikacji bez uprzedniego uzyskania profesjonalnej porady. Nie gwarantujemy (w sposób wyraźny, ani dorozumiany) prawidłowości, ani dokładności informacji zawartych w naszej prezentacji. Ponadto, w zakresie przewidzianym przez prawo polskie, PricewaterhouseCoopers Sp. z o.o., jej partnerzy, pracownicy, ani przedstawiciele nie podejmują wobec Państwa żadnych zobowiązań oraz nie przyjmują na siebie żadnej odpowiedzialności – ani umownej, ani z żadnego innego tytułu – za jakiejkolwiek straty, szkody ani wydatki, które mogą być pośrednim lub bezpośrednim skutkiem działania podjętego na podstawie informacji zawartych w naszej publikacji lub decyzji podjętych na jej podstawie.

© 2016 PwC Polska Sp. z o.o. Wszystkie prawa zastrzeżone.