5. edycja Badania Stanu Bezpieczeństwa Informacji

Cyber-ruletka po polsku

Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście

pwc

pwc.pl/badaniebezpieczenstwa

Rok 2017 był niezwykle obfity w wydarzenia o charakterze cyberprzestępczym. *WannaCry, Petya,* ponowne ataki na infrastrukturę krytyczną Ukrainy, ciągłe informacje o zagrożeniu przez niezidentyfikowanych hackerów, w końcu niedawna kradzież bitcoinów. Ataki nie ominęły również polskich przedsiębiorstw, przyczyniając się do przestojów, ale także do utraty zaufania i wiarygodności.

Część firm rozumie, że cyber aktywność świata przestępczego wystawia ich własne działanie na niespotykane do tej pory ryzyko. 80% prezesów największych światowych organizacji uznaje digitalizację i nowe technologie za pierwszy czynnik zapewniający zwiększenie ich innowacyjności, a przez to konkurencyjności na rynku[1]. Z kolei 80% zdaje sobie sprawę, że cyberataki są jednym z największych zagrożeń dla rozwoju ich biznesu (w regionie Europy Środkowo-Wschodniej odsetek przekonanych o tym prezesów wynosi 77%)[2].

Coraz trudniej nadążyć za rozwojem technologii – technologii, która ma wspierać efektywność biznesu, ułatwiać pracę i przyczyniać się do większej integracji przedsiębiorstw, konsumentów i międzynarodowych rynków. Z drugiej strony ta sama technologia otwiera wrota do świata biznesu dla osób o nieuczciwych zamiarach, mogąc być źródłem istotnych strat. Firmy biorące udział w naszym badaniu deklarują, że na cyberbezpieczeństwo przeznaczają średnio zaledwie 3% swojego całkowitego budżetu IT.

Balansując pomiędzy koniecznością zapewnienia wzrostu i utrzymania bezpieczeństwa, przedsiębiorstwa często nie doceniają skali zagrożenia, z jaką się mierzą. Znanych jest wiele przykładów ataków i związanych z nimi incydentów, skutkujących zatrzymaniem głównych procesów biznesowych, jednak informacje o ich faktycznych kosztach nie są zbierane.

Jednocześnie trudno jest dokonać wyceny utraty wiarygodności i zaufania partnerów biznesowych oraz klientów. 85% konsumentów twierdzi, że nie zamierza współpracować z firmą, która nie będzie w stanie przekonać ich, że powierzone jej dane są odpowiednio zabezpieczone[3]. Każdy z nas chce być bezpieczny i oczekuje, że bezpieczeństwo zostanie mu bezwzględnie zapewnione. Czy zatem firmy znają sposoby na zagwarantowanie bezpieczeństwa, czy też wykazują wysoki apetyt na ryzyko i liczą na szczęście?

Już po raz piąty zapytaliśmy polskie firmy o stan ich przygotowania do zapewnienia bezpieczeństwa informacji i danych, jakie są w ich posiadaniu. Jest to niezwykle istotne właśnie teraz, ponieważ w połowie 2018 roku wejdą w życie dwa ważne akty regulujące zasady cyberbezpieczeństwa: rozporządzenie o ochronie danych osobowych (RODO) i dyrektywa NIS. Tymczasem połowa przebadanych przez nas firm ocenia swój stan gotowości do nowych wymagań RODO jedynie na 30% lub mniej. Unijne wymogi zapisane w dyrektywie NIS nakładają obowiązek monitorowania i zgłaszania incydentów przez firmy odpowiedznialne za świadczenie usług kluczowych. Wśród wszystkich uczestników naszego badania SOC posiada jedynie 14% firm, natomiast 34% ma systemy klasy SIEM. Liczby te nie napawają optymizmem, szczególnie w zestawieniu z informacją, że dla 30% spółek główną przyczyną wystąpienia incydentu były przeoczenia czy wręcz błędy ich własnych pracowników, które często prowadziły do wycieku danych, zaś dla 44% organizacji zakończyły się poniesieniem strat finansowych.

Prezentujemy raport o praktykach polskich firm w zakresie bezpieczeństwa teleinformatycznego, dodając kilka wskazówek, w jaki sposób wzmocnić działania obronne i uodpornić organizację, przygotowując ją do stabilnego funkcjonowania w przyszłości.

Piotr Urban

Partner, Lider usług cyberbezpieczeństwa
w regionie Europy Środkowo-Wschodniej

Anna Sieńko

Partner, Lider ds. technologii
w regionie Europy Środkowo-Wschodniej

[1] *PwC, 2017 Global Digital IQ® Survey: 10th anniversary edition*
[2] *PwC, 21th CEO Survey*
[3] *PwC US, Protect.me Survey, 2017*

Jaki jest stan przygotowania polskich firm,
by stawić czoło “wirtualnym” zagrożeniom?

Czy posiadają one odpowiednią strategię,
całościowe spojrzenie i plan, zapewniający
bezpieczeństwo będących w ich posiadaniu danych?

Czy też górę bierze cyber-ruletka:
działanie w pojedynkę, w sytuacji niepełnej
informacji i jedynie obstawianie możliwych zdarzeń?

Trudna rozgrywka

44%
firm poniosło straty finansowe na skutek ataków

62%
spółek odnotowało zakłócenia i przestoje funkcjonowania

21%
padło ofiarą zaszyfrowania dysku (ransomware)

Ryzykowny blef

20%
średnich i dużych firm nie posiada nikogo od cyberbezpieczeństwa

46%
spółek nie posiada operacyjnych procedur reakcji na incydenty

3%
budżetu IT stanowią średnio wydatki na bezpieczeństwo – to co najmniej trzy razy za mało

Gra o wysoką stawkę

Firmy dalej nie są gotowe do RODO:

20%
respondentów nie zaczęło jeszcze przygotowań

50%
spółek ocenia swoją gotowość na **30%** lub mniej

3%
firm osiągnęło pełną gotowość

Indeks Cyberbezpieczeństwa

8% **przebadanych firm jest dojrzałych pod względem bezpieczeństwa informacji**

Spis treści

1.

Ryzykowna defensywa

Dobre przygotowanie do odpierania cyberataków nie jest prostym zadaniem. Wymaga zaangażowania wielu zasobów: ludzkich, technologicznych i oczywiście finansowych. Jaki jest stan przygotowania polskich firm, by stawić czoło „wirtualnym" zagrożeniom? Czy posiadają one odpowiednią strategię, całościowe spojrzenie i plan zapewniający bezpieczeństwo będących w ich posiadaniu danych? Czy też górę bierze cyber-ruletka: działanie w pojedynkę, w sytuacji niepełnej informacji i jedynie obstawianie możliwych zdarzeń?

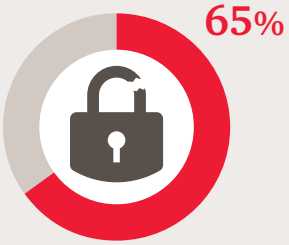
W wielu przedsiębiorstwach dominuje przekonanie, że zagrożenie incydentami cyberbezpieczeństwa ich po prostu nie dotyczy. Zastanawiający jest brak działań prewencyjnych i podejmowanie jedynie akcji obronnych, co gorsza w ograniczonym zakresie. Brakuje konsekwencji w rozwiązywaniu zidentyfikowanych problemów.

Brak jest także otwartości zaatakowanych podmiotów i większej chęci do dzielenia się wiedzą o zaistniałych incydentach, która może pomóc zarówno samym ofiarom jak i potencjalnie poszkodowanym w ochronie ich aktywów. Jest to element prewencji, na który czekamy od lat.

Bezpańskie incydenty

Liczenie na łut szczęścia w obszarze bezpieczeństwa teleinformatycznego to bardzo ryzykowna gra. Aż 65% uczestników naszego badania zadeklarowało, że w ich przedsiębiorstwach w ciągu ostatnich 12 miesięcy wykryto incydenty związane z naruszeniem bezpieczeństwa informacji lub systemów IT. Biorąc pod uwagę, że nie wszystkie zostały zidentyfikowane i uwzględnione w raportach, można przyjąć, że ich liczba była jeszcze większa. Warto zasygnalizować, że w wielu firmach incydenty są tematem tabu. Informacja o ich wystąpieniu (jeżeli mają one ograniczony charakter) dociera jedynie do wąskiej grupy pracowników, skutkiem czego duża część zatrudnionych pozostaje nieświadoma faktycznej skali zagrożenia.

Udział respondentów, którzy odnotowali incydenty



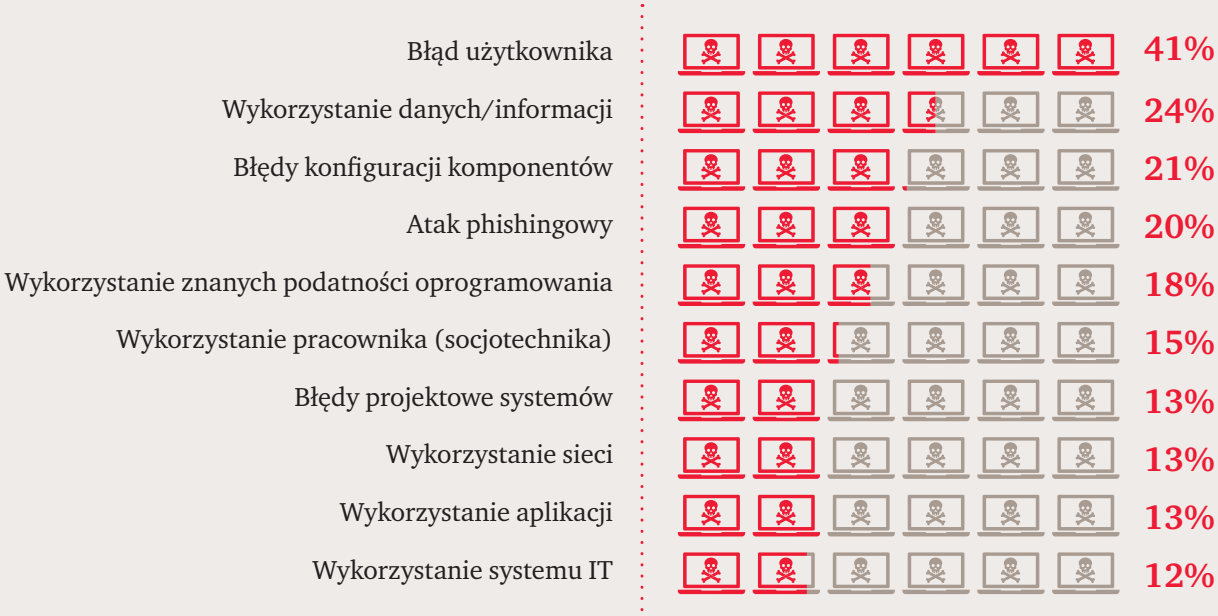
2017

Najbliższe otoczenie dalej najbardziej niebezpieczne

Podobnie jak w latach ubiegłych, głównym źródłem incydentów i zagrożeń pozostaje bezpośrednie otoczenie firmy. Zgodnie z deklaracjami respondentów, aż w 1/3 ich źródłem były osoby obecnie zatrudnione w przedsiębiorstwach. 13% badanych wskazało na byłych pracowników, zaś 6% na aktualnych usługodawców, konsultantów lub wykonawców. 4% za źródło uznało klientów, zaś po 2% wskazało na byłych usługodawców i dostawców. Warto zestawić te wartości z 28% odpowiedzi, że sprawcami ataków byli hakerzy.

33% firm wskazało, iż głównym źródłem incydentów byli obecnie zatrudnieni pracownicy firmy

Przyczyny incydentów bezpieczeństwa



„Nieświadomi pracownicy pozostają nadal jednym z najsłabszych ogniw w strategii zabezpieczeń przedsiębiorstw. Przejęcie stacji roboczej wskutek udanego ataku phishingowego jest często pierwszym krokiem w dalszej udanej propagacji ataku na kluczowe elementy infrastruktury IT przedsiębiorstwa. W zależności od motywacji sprawców celem może być pozyskanie środków finansowych, jak to ma miejsce w incydentach związanych z podszywaniem się pod pracowników tzw. (BEC – Business Email Compromise), gdzie w związku z realizacją fikcyjnych przelewów przez nieświadomych pracowników, straty mogą sięgać kilkudziesięciu milionów euro wskutek jednego ataku. Poważne problemy mogą zacząć się od niepozornej infekcji stacji roboczej zwykłego pracownika. Ataki hybrydowe, których scenariusze łączą podatności technologii i podatności pracowników na ataki socjotechniczne są najtrudniejsze do zapobiegania i wczesnego wykrycia. Strategie rozwoju bezpieczeństwa przedsiębiorstw powinny uwzględniać odpowiedni rozwój mechanizmów zabezpieczających w warstwach organizacjo-technologicznych dostosowanych do potrzeb biznesowych i sytuacji rynkowej".

Tomasz Sawiak
wicedyrektor, Zespół Cyber Security

Oprócz źródeł incydentów należy także przeanalizować okoliczności, w jakich dochodziło do naruszeń bezpieczeństwa teleinformatycznego. Aż 41% respondentów zadeklarowało, że były one następstwem błędów popełnionych przez użytkowników systemów. 24% uczestników badania wskazało na wykorzystanie wcześniej wykradzionych danych lub informacji, zaś 21% na błędy w konfiguracji komponentów. Ataki phishingowe pozostawały w czołówce stosowanych scenariuszy ataków – wciąż co piąty ankietowany deklarował, że jego organizacja padła ofiarą tego prostego mechanizmu.

Liczna grupa organizacji biznesowych realizuje jedynie plan minimum – zapewniający przetrwanie poprzez zgodność z obowiązującymi przepisami w minimalnym zakresie.

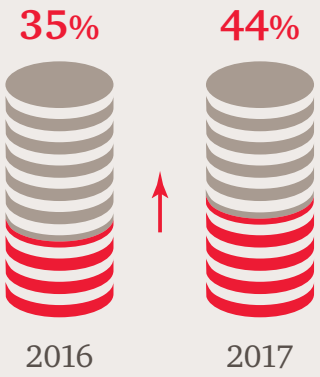
Co istotne, pomimo znajomości źródeł incydentów oraz zidentyfikowania sytuacji, które do nich doprowadziły, firmy na ogół nie podejmują działań mających na celu uszczelnienie funkcjonujących systemów zabezpieczeń. Wielu incydentów można byłoby uniknąć, gdyby wdrożone zostały odpowiednie zabezpieczenia, pracownicy mieli większą świadomość zagrożeń, oraz gdyby istniały odpowiednie polityki i procedury określające sposób postępowania.

Znakomitym przykładem pokazującym, że przedsiębiorstwa nie wyciągają wniosków ze zmieniających się znanych zagrożeń i obserwowanych ataków są spektakularne infekcje dużych firm złośliwym oprogramowaniem typu Ransomware. W 2017 roku świat obiegła informacja o fali infekcji złośliwym oprogramowaniem szyfrującym dyski *(WannaCry)* na niespotykaną dotąd skalę. Pomimo tego, wiele przedsiębiorstw, które nie padły ofiarami ataku i których dane nie zostały zaszyfrowane, nie wyciągnęło wniosków z tego, co się stało. Zapewne dlatego część z nich padła ofiarą podobnego działania zaledwie kilka miesięcy później *(Petya)*. Atak ten wykorzystywał dokładnie taki sam mechanizm infekcji i podatności, jak ten stosowany przez *WannaCry*. Malware Petya zebrał imponujące żniwo – w przypadku niektórych przedsiębiorstw działających na skalę globalną straty sięgnęły dziesiątek milionów dolarów.

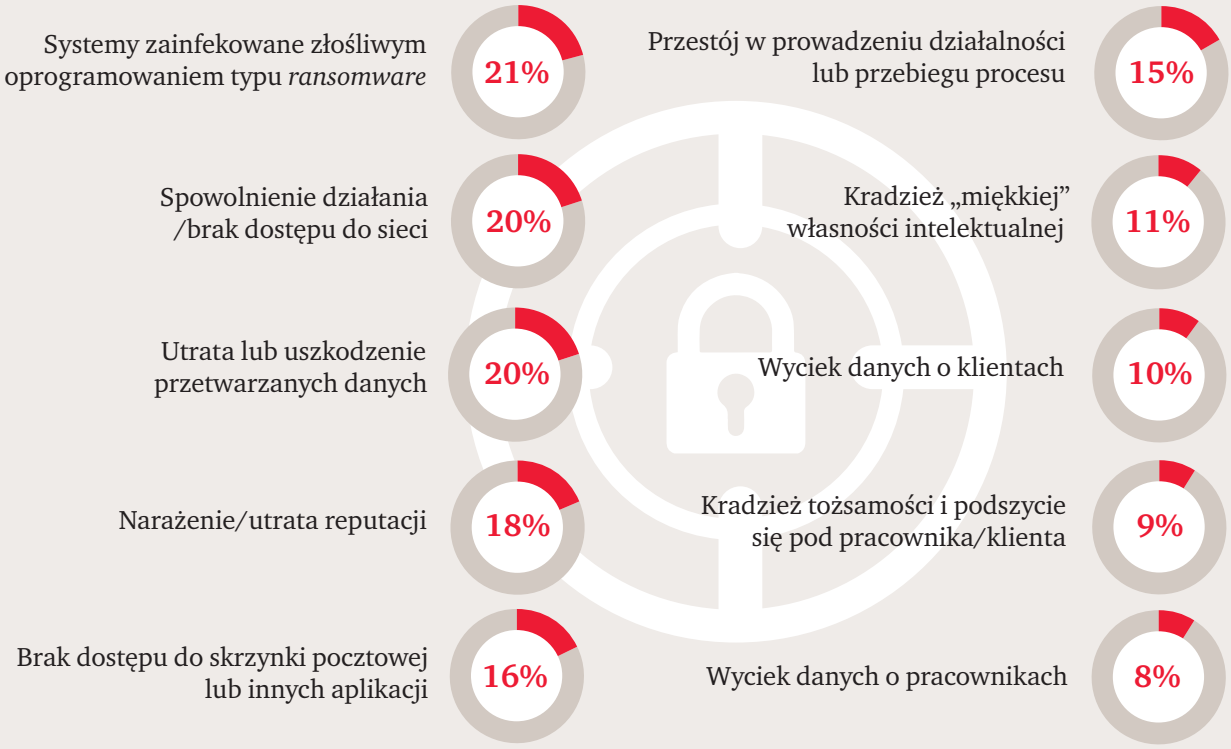
Cyber-ruletka kołem się toczy

Podobnie jak w kasynie, zdając się w dziedzinie bezpieczeństwa na los, można ponieść wymierne straty. Jak pokazują wyniki badania, z tytułu incydentów w obszarze bezpieczeństwa teleinformatycznego straty finansowe odnotowało aż 44% badanych organizacji, co stanowi wzrost o 9 punktów procentowych w stosunku do ubiegłego roku. Często jednak ich wysokość nie jest dokładnie liczona – aż 30% firm nie było w stanie wskazać wymiaru poniesionych szkód, a 26% stwierdziło, że nie odnotowało strat finansowych. W badaniu sprzed dwóch lat wartość ta sięgnęła 53% – wygląda więc na to, że firmy zaczęły dostrzegać związek pomiędzy atakami i stratami finansowymi, jednak jeszcze nie wdrożyły odpowiednich narzędzi do szacowania strat. Tymczasem utrudnienia w działaniu organizacji są rejestrowane: 21% badanych poinformowało o zainfekowaniu systemów złośliwym oprogramowaniem, powodującym zaszyfrowanie dysku. 20% odnotowało spowolnienie działania lub brak dostępu do sieci oraz utratę lub uszkodzenie przetwarzanych danych. 16% utraciło dostęp do skrzynek mailowych lub innych aplikacji, a także odnotowało przestój w prowadzeniu działalności lub przebiegu procesu.

Ile spółek poniosło straty finansowe?



Skutki incydentów bezpieczeństwa

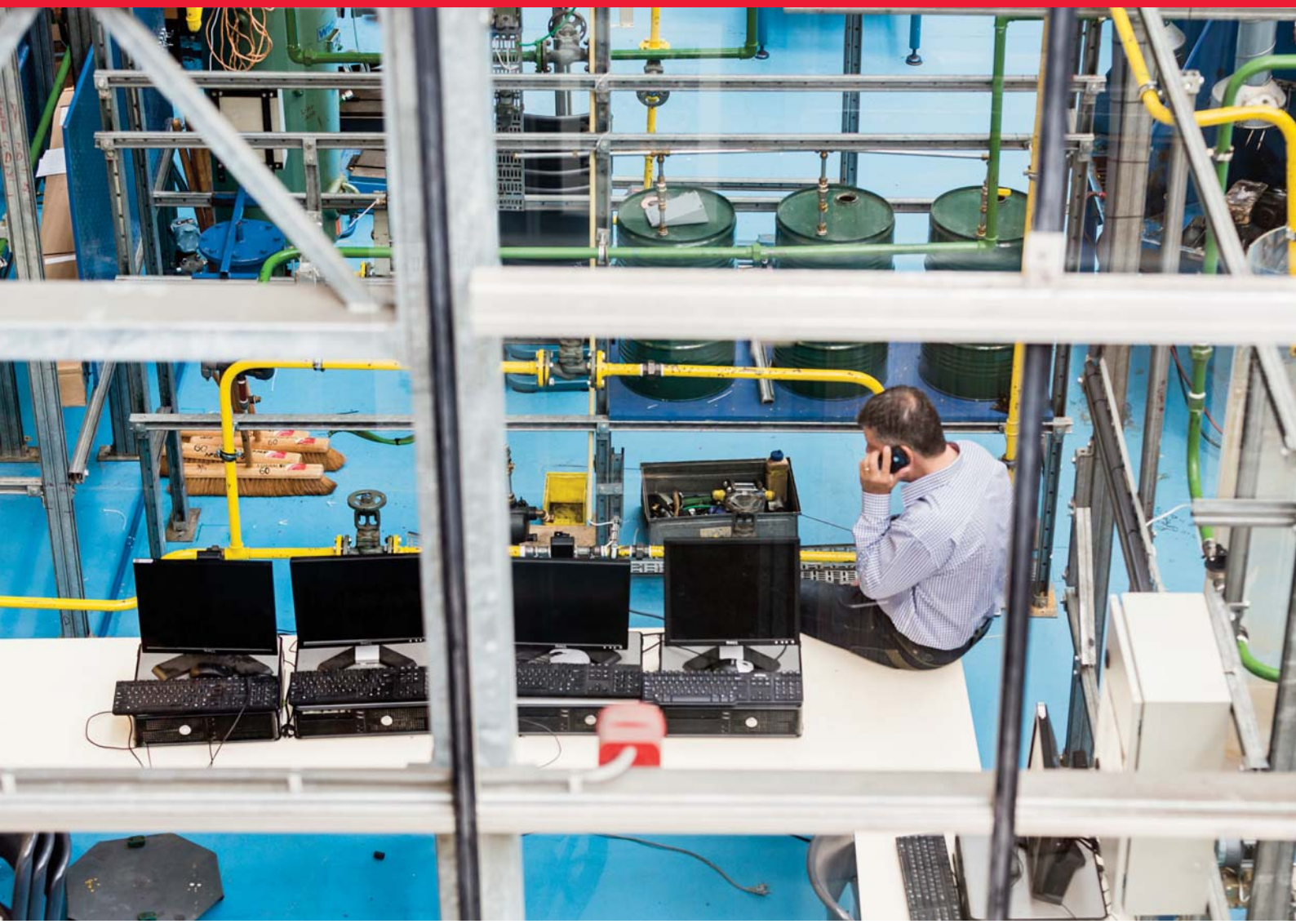


Oczywiście straty poniesione wskutek naruszeń nie mają jedynie charakteru finansowego. Skalę problemów wywoływanych przez cyberataki można też zilustrować za pomocą innego parametru – przestojów w funkcjonowaniu organizacji. W 2017 roku aż 40% wszystkich incydentów wiązało się z dłuższymi niż 3 godziny przestojami w prawidłowym funkcjonowaniu spółek. Jest to sytuacja tym bardziej poważna, iż w czasie przestojów działalność firmy może zostać całkowicie sparaliżowana lub utrudnione może być funkcjonowanie poszczególnych działów: obsługi klientów, sprzedaży czy jednostek odpowiedzialnych za działalność produkcyjną.

Zgodnie z deklaracjami uczestników badania, w 12% przedsiębiorstw przerwy w funkcjonowaniu trwały od 3 do 8 godzin, w takiej samej liczbie spółek – od 9 do 24 godzin. Efektywna praca była czasem niemożliwa przez dłuższy czas – w 15% badanych organizacji przestoje trwały więcej niż jeden dzień, z czego w 5% przypadków było to ponad 5 dni.

W tym obszarze trzeba podkreślić, że poziom gotowości i umiejętność szybkiej reakcji na incydenty nie poprawiły się w czasie. W badaniu przeprowadzonym dwa lata temu przestoje trwające dłużej niż 3 godziny stanowiły 47% wszystkich przypadków.

Dlaczego tak niski jest poziom wiedzy dotyczący poniesionych strat finansowych? Powodów takiego stanu rzeczy może być wiele. W niektórych przypadkach można oczywiście stwierdzić, iż incydenty nie wyrządziły istotnych szkód. Część respondentów może również nie zdawać sobie sprawy ze skutków zaistniałych naruszeń. Ponadto, tak jak przed rokiem, nadal obserwujemy istotne braki w zakresie procesów i ustalania metodyki szacowania skutków naruszeń bezpieczeństwa. Potrzeba rozwoju systemów zarządzania ryzykiem i gromadzenia informacji o incydentach bezpieczeństwa jest nadal niezwykle istotna, gdyż dopiero umiejętność dokładnej oceny kosztów i skutków naruszeń stanowić może podstawę do efektywnego zarządzania bezpieczeństwem firmy i stanowić uzasadnienie zwiększenia nakładów na rozwój zabezpieczeń.



„Przestoje będące wynikiem cyber incydentu szczególnie dotkliwe mogą być dla firm produkcyjnych, gdzie straty z tym związane bardzo łatwo przełożyć na wymiar finansowy. Wspomniany już atak ransomware spowodował wymierne straty m.in. w wielu fabrykach i firmach logistycznych należących do międzynarodowych koncernów. Obszar produkcji jest szczególnie podatny na ataki ze względu na zamknięty charakter systemów sterowania, wykorzystujących przestarzałe technologie informatyczne. Łączenie ich z systemami informacji zarządczej lub ERP otwiera je na współczesne cyberataki. Tym większe znaczenie ma zapewnienie właściwej ochrony systemom sterowania i nadzoru (SCADA/MES/DCS), które często nie są odporne na tego typu zagrożenia".

Patryk Geborys
wicedyrektor, Zespół Cyber Security

Zabezpiecz mnie

Jak kwestię cyberbezpieczeństwa danych postrzegają konsumenci?

konsumentów wierzy, że to właśnie prywatny biznes, a nie rząd, jest w stanie najskuteczniej zadbać o bezpieczeństwo ich danych

konsumentów dostrzega, że firmy są narażone i podatne na cyberataki

konsumentów jest przekonanych, że większość organizacji obchodzi się odpowiedzialnie z powierzonymi im danymi osobowymi

Źródło: PwC US Protect.me Survey, 2017

Poważną sytuację pogarsza dodatkowo fakt, że pomimo niestosowania zaawansowanych metodyk i procesów obsługi skutków incydentów, większość firm nie próbuje się ubezpieczać od ryzyk cyberbezpieczeństwa. Jedynie co dziesiąta badana przez nas spółka posiada polisę ubezpieczeniową od ryzyk cyberbezpieczeństwa. Należy jednak także zauważyć, że oferta tego typu ochrony na rynku polskim nadal jest dosyć ograniczona.

Tymczasem tak jak pokazują liczne przypadki, paraliż systemów, lub wyciek poufnych informacji może oznaczać w skrajnych przypadkach wielomilionowe straty, spowodowane na przykład niemożnością obsługi klientów, czy znaczącym spadkiem zaufania do marki.

Jak wynika z globalnego badania *PwC Protect.Me*, krytycznym jest, by firmy zrozumiały i odpowiednio reagowały na obawy swoich konsumentów związane z ich cyberbezpieczeństwem. Aby zdobyć zaufanie konsumentów, należy skrupulatnie i proaktywnie chronić ich dane, a w procesie komunikacji i korzystania ze zgromadzonych informacji – szanować ich prywatność.

Jedynie co dziesiąta spółka posiada polisę ubezpieczeniową od ryzyk cyberbezpieczeństwa

Jak odzyskać zaufanie klientów po wycieku danych?

Źródło: PwC US Protect.me Survey, 2017

Konsumenci mają bardzo określone oczekiwania względem firm, które to zaufanie zawiodły. Aż 18% badanych w tym roku firm w Polsce przyznało, że incydent bezpieczeństwa zagroził reputacji ich marki. Około 10%, że wyciekły dane ich klientów, pracowników lub informacje umożliwiające identyfikację ich partnerów biznesowych. Jak prawidłowo zareagować na zdarzenie tego rodzaju? Po wycieku danych konsumenci oczekują od organizacji konkretnych działań naprawczych. 22% oczekuje jasnej komunikacji o sytuacji, a 27% rekompensaty za utratę danych. Przygotowanie firmy do reagowania na incydenty związane z wyciekiem danych zapewne zostaną poprawione przez wewnętrzne inicjatywy przedsiębiorstw związane z wdrożeniem RODO. Jednym z jego wymogów jest bowiem analiza incydentu związanego z wyciekiem danych klientów i implementacja odpowiednich mechanizmów zabezpieczających, w tym planu reakcji na incydent zagrażający bezpieczeństwu, czyli tzw. *Breach Response Plan*.

2.

Odporność na przyszłość

Technologie tak, ale punktowo

Porównując powszechnie stosowane rozwiązania zabezpieczające przed incydentami, należy uznać, że polskie firmy nie są jeszcze w pełni przygotowane na przeciwdziałanie współczesnym zagrożeniom i metodom ataków, chociaż widoczny jest pewien postęp w deklarowanym poziomie gotowości.

Posiadanie ogólnej strategii bezpieczeństwa deklaruje 65% badanych, natomiast opracowane procesy reagowania na incydenty 54% firm. Nakreślenie ram i ogólnych kierunków działania jest bardzo ważne, bo pozwala stworzyć usystematyzowane podejście i plan działania, oraz skaskadować cele. Ważne jest jednak, aby założenia były faktycznie realizowane, co jak wskazuje badanie, nie zawsze ma miejsce.

Jeżeli chodzi o stosowane zabezpieczenia punktowe, do najbardziej popularnych należą rozwiązania klasy *web application firewall*, wykorzystywane w połowie przedsiębiorstw. Również w nieco ponad połowie spółek działają systemy detekcji włamań (IPS/IDS). Obydwa te tradycyjne już zabezpieczenia okazują się nieskuteczne w obecnej sytuacji wysokiego rozwoju systemów informatycznych i dostępności aplikacji w środowisku sieciowym, a także w obliczu zaawansowanych ataków klasy APT (ang. *Advanced Persistent Threat*), czy nawet zwykłych ataków phishingowych, które bazują na interakcji z użytkownikiem końcowym. Trzecim najczęściej stosowanym zabezpieczeniem są mechanizmy filtrowania ruchu www (ang. *web proxy*) – wykorzystuje je 51% badanych organizacji biznesowych, zaś dalszych 15% chce je implementować w ciągu najbliższego roku.

Specjalistyczne rozwiązania chroniące przed zaawansowanymi atakami (tzw. *anty APT*) stosowane są przez 46% ankietowanych firm, co stanowi istotny wzrost w stosunku do roku poprzedniego – wówczas jedynie 26% respondentów deklarowało ich posiadanie. Większą popularność rozwiązań z tego zakresu można uznać za przyczynę spadku incydentów phishingowych jako deklarowanego sposobu naruszeń – z 39% w roku poprzednim do 18% obecnie.

65% badanych deklaruje posiadanie ogólnej strategii bezpieczeństwa, a 54% firm opracowane procesy reagowania na incydenty

Zabezpieczenia technologii wdrożone w firmach:

SIEM i SOC dla wybranych

Efektywne zarządzanie bezpieczeństwem informatycznym firmy wymaga całościowego spojrzenia na infrastrukturę teleinformatyczną i wiedzy na temat działania mechanizmów zabezpieczających, dostosowanych do mnogości rozwiązań i systemów. Co cieszy, w tym zakresie widać pewną poprawę. Obecnie 34% ankietowanych posiada system klasy SIEM, co stanowi istotny wzrost w porównaniu do 21% firm w roku ubiegłym.

34% ankietowanych posiada system klasy SIEM

Jednocześnie jednak, aż 63% respondentów stwierdziło, że ich firma nie posiada i nie planuje uruchomienia *Security Operations Center* (SOC). 15% ankietowanych zadeklarowało, że w ich spółce nie funkcjonuje takie rozwiązanie, ale planowane jest jego wdrożenie w przyszłości. Obecnie SOC działa w 14% badanych firm. Ogółem upowszechnienie tego typu rozwiązań jest więc wciąż niewielkie. Warto jednak podkreślić, że w niektórych sektorach, na przykład energetycznym i finansowym w większości badanych spółek SOC już funkcjonuje.

14% badanych firm uruchomiło Security Operations Center (SOC)

„Mechanizmy zabezpieczające, tworzące architekturę bezpieczeństwa, w które inwestują firmy, można podzielić na 3 typy: prewencyjne, detekcyjne i reakcyjne. Technologia SIEM zalicza się do mechanizmów detekcyjnych, z kolei SOC (Security Operation Center) do mechanizmów reakcyjnych związanych z monitorowaniem i reagowaniem na identyfikowane incydenty bezpieczeństwa. Odpowiednio zaplanowana i wdrożona architektura bezpieczeństwa to zestaw wzajemnie połączonych ze sobą mechanizmów, stanowiących jednolity system obronny, które powinny działać jak sprawny system immunologiczny. W przypadku infrastruktury IT jest podobnie – wnioski z incydentów należy odpowiednio sformułować i wdrożyć doskonaląc zabezpieczenia. Implementowane mechanizmy zabezpieczające ulegają dewaluacji w czasie z uwagi na stale zmieniające się zagrożenia i metody ataków. Powoduje to, że konfiguracje funkcjonujących systemów wymagają ciągłego doskonalenia. SOC jest tutaj kluczowym rozwiązaniem, które dzięki sprawnym reakcjom na incydenty i wyciąganym wnioskom z ich obsługi, pozwala na doskonalenie systemów”.

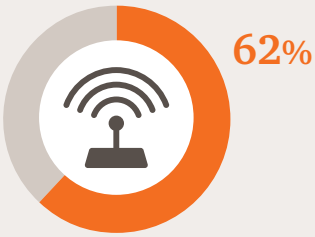
Tomasz Sawiak
wicedyrektor, Zespół Cyber Security

„W ostatnich latach obserwujemy dynamiczny wzrost zainteresowania zatrudnianiem specjalistów z obszaru monitorowania bezpieczeństwa. Mimo, że procentowo liczba zespołów SOC funkcjonujących w przedsiębiorstwach nie wygląda imponująco, to jednak czołowe firmy z sektora finansów, energetyki, czy telekomunikacji stawiają na rozwój tych kompetencji. Dla mniejszych spółek przeszkodą do stworzenia własnej funkcji monitorowania bezpieczeństwa są koszty – technologii, ludzi i pozyskania kompetencji. Alternatywę mogą stanowić usługi klasy MSSP (Managed Security Service Provider), czy outsourcing do wyspecjalizowanych dostawców. W Polsce ciągle jest to nisza, ale oferta z roku na rok się poszerza. Decydując się na taki model współpracy warto jednak pamiętać o wyzwaniach z nim związanych – jak w każdym outsourcingu, i tu zamawiający powinien mieć ludzi i kompetencje umożliwiające zdefiniowanie zakresu i weryfikację jakości dostarczanych usług”.

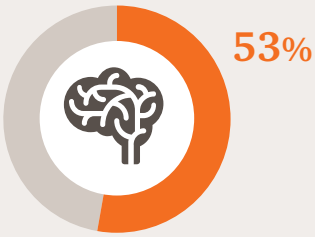
Piotr Urban
partner,
lider ds. cyberbezpieczeństwa w regionie Europy Środkowo-Wschodniej

Niebezpieczna luka technologiczna

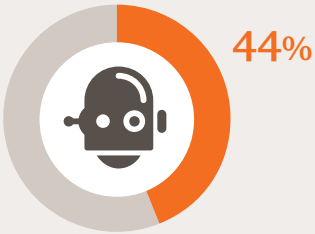
Jakie technologie staną się priorytetem inwestycyjnym polskich firm za 3 lata?



Internet rzeczy



Sztuczna inteligencja



Robotyka

Źródło: Digital IQ, PwC PL, 2017

Patrząc na rozwój firmy w długiej perspektywie, utrzymanie odpowiedniego poziomu bezpieczeństwa to sztuka umiejętnego dopasowania się do specyfiki biznesu, towarzyszących mu zagrożeń i technologii koniecznych dla uzyskania przewagi konkurencyjnej.

Co ciekawe, jak wynika z naszego badania, deklarowanemu wzrostowi zainteresowania nowymi technologiami nie towarzyszy wzrost zapotrzebowania na zabezpieczenia w danym zakresie. Jak ukazało badanie *Digital IQ 2017*, polskie firmy zaczynają już planować działania w obszarze Internet of Things (60%) czy Sztucznej Inteligencji (36%). Tymczasem zapytani o priorytety bezpieczeństwa, respondenci wskazują przede wszystkim na zagadnienia związane z bieżącą ochroną i wykonywaniem swoich obowiązków. Zdecydowanie mniejszym zainteresowaniem cieszy się działanie ukierunkowane na zapewnienie spójności między procesami technologicznymi, a bezpieczeństwem funkcji organizacji. Tym samym można stwierdzić, iż cyberbezpieczeństwo w polskiej firmie nie jest elementem integralnym w procesie wdrażania technologii.

Jeżeli dodatkowo weźmiemy pod uwagę, że nakłady na bezpieczeństwo w badanych spółkach wynoszą średnio zaledwie ~3% wartości całego budżetu IT, można śmiało stwierdzić, iż będziemy w dalszym ciągu obserwować powiększanie się luki pomiędzy błyskawicznie rozwijającą się technologią wspierającą biznes, a powolnie zmieniającym się lub, w ekstremalnych przypadkach, stojącym w miejscu cyberbezpieczeństwem firmy. Postęp technologiczny przyśpiesza i wykorzystywanie metod pochodzących z ubiegłego dziesięciolecia, do walki z wyzwaniami jakie niesie za sobą obecne, poważnie zagraża bezpieczeństwu teleinformatycznemu spółek.

3% nakłady na bezpieczeństwo stanowią średnio tylko 3% wartości całego budżetu IT

Najważniejsze wyzwania dla bezpieczeństwa firmy

„Technologie mobilne, Internet rzeczy (IoT) czy cloud computing to już dobrze znane rozwiązania. Dzięki nim pojawiły się zupełnie nowe możliwości zarówno dla organizacji biznesowych, jak i dla klientów. Ich wykorzystywanie łączy się jednak z konkretnymi wyzwaniami. Lawinowo rosnąca liczba urządzeń podłączonych do sieci to oprócz nowych szans, olbrzymia liczba potencjalnych punktów dostępu dla przestępców. Co więcej, wchodzące niebawem w życie regulacje dotyczące ochrony danych osobowych bardziej wyczulają firmy na możliwe następstwa naruszeń w sferze ochrony zgromadzonych informacji.

Obecnie obserwujemy intensywny rozwój technologii, które stanowią pewnego rodzaju odpowiedź na przywołane wyzwania. Jedną z nich jest tzw. edge computing, czyli architektura rozproszonych zasobów IT, w ramach których dane przetwarzane są na peryferiach sieci, tj. blisko źródła pochodzenia. Dzięki temu rozwiązaniu dane kluczowe dla firmy mogą być analizowane niemal w czasie rzeczywistym, zaś informacje mniej wrażliwe lub o niższym priorytecie – magazynowane w chmurach obliczeniowych.

Kolejnym rozwiązaniem technologicznym, które umożliwia skuteczniejsze zabezpieczanie danych są rejestry rozproszone (ang. blockchain). W ich przypadku, mamy do czynienia ze zdecentralizowaną bazą danych, której poszczególne bloki są połączone i „przechowywane" przez samych użytkowników. Trzeba jednocześnie podkreślić, że nie są to rozwiązania idealne. Jak pokazują wydarzenia 2017 roku, przeprowadzono już z sukcesem ataki, np. na kryptowaluty. Przejrzystość i ogólnodostępność rozwiązań blockchain umożliwia jednak poddawanie ich stałej weryfikacji i testom. To właśnie stanowić będzie klucz do sukcesu rejestrów rozproszonych w przyszłości i podstawę jego rozwoju poza sektor finansowy, m.in. do sektorów energetycznego, ochrony zdrowia czy motoryzacji".

Anna Sieńko
Lider ds. technologii w regionie
Europy Środkowo-Wschodniej

Jak dokładnie wygląda sytuacja? Nie napawa optymizmem, że w grupie działań priorytetowych nie występują zabezpieczenia związane z najdynamiczniej rozwijającymi się technologiami. Przykładowo, choć media społecznościowe stały się jednym z elementów codzienności, tylko 23% przedsiębiorstw zadeklarowało, że posiada związaną z nimi strategię bezpieczeństwa. Dobrą wiadomością jest to, że 19% ankietowanych stwierdziło, że w ich spółkach taki dokument ma powstać w ciągu najbliższego roku.

Sytuacja przedstawia się podobnie w przypadku zabezpieczeń Big Data. W przypadku chmury obliczeniowej strategię bezpieczeństwa posiada 27% badanych spółek, 17% ma w planach jej stworzenie w ciągu najbliższego roku. Mimo szerokiego dostępu społeczeństwa do smartfonów czy tabletów, zwiększonej mobilności i zmian w preferowanym trybie pracy, większość spółek nie stara się wykorzystać możliwości podniesienia efektywności poprzez nadanie swoim pracownikom dostępu do firmowych danych i aplikacji na prywatnych urządzeniach. Pozwala na to jedynie 38% badanych organizacji, podczas gdy 54% deklaruje brak takich możliwości. Tylko 3% badanych stwierdziło, że takie rozwiązanie zostanie udostępnione w ich spółce w przeciągu najbliższego roku.

Jednocześnie warto odnotować, że tylko w 13% firm warunkiem koniecznym by móc korzystać z zasobów firmowych na prywatnym urządzeniu, jest zainstalowanie oprogramowania klasy MDM (ang. *Mobile Device Management*). Dodatkowe aplikacje pozwalają na ustanowienie bezpiecznego połączenia oraz identyfikację urządzenia w sieci firmowej.

Strategie bezpieczeństwa

Wdrożenie nie jest planowane		Wdrożone / zlecane na zewnątrz
58%	Big Data	25%
58%	Media społecznościowe	23%
55%	Chmura obliczeniowa	27%
41%	Urządzenia prywatne wykorzystywane w celach służbowych	39%
39%	Urządzenia mobilne	36%

Niegotowi na RODO

Bez wątpienia jednym z istotniejszych wyzwań dla polskich firm w nadchodzących miesiącach będzie osiągnięcie zgodności z Rozporządzeniem o Ochronie Danych Osobowych (RODO). Niewywiązanie się z wynikających z tego dokumentu obowiązków może skutkować karami finansowymi do 20.000.000 euro lub 4% wartości rocznego światowego obrotu przedsiębiorstwa. Tu liczenie na łut szczęścia jest obarczone potężnym ryzykiem. Mówiąc bardziej obrazowo: wygrać może tylko kasyno, czyli regulator. Gracze niestosujący się do wytycznych będą zmuszeni płacić za niespełnianie wymogów.

Jak ankietowani oceniają stan przygotowań swoich przedsiębiorstw? Odpowiedzi nie napawają entuzjazmem. W czasie gdy nasi respondenci wypełniali ankiety,

3% badanych spółek osiągnęło pełną gotowość do RODO

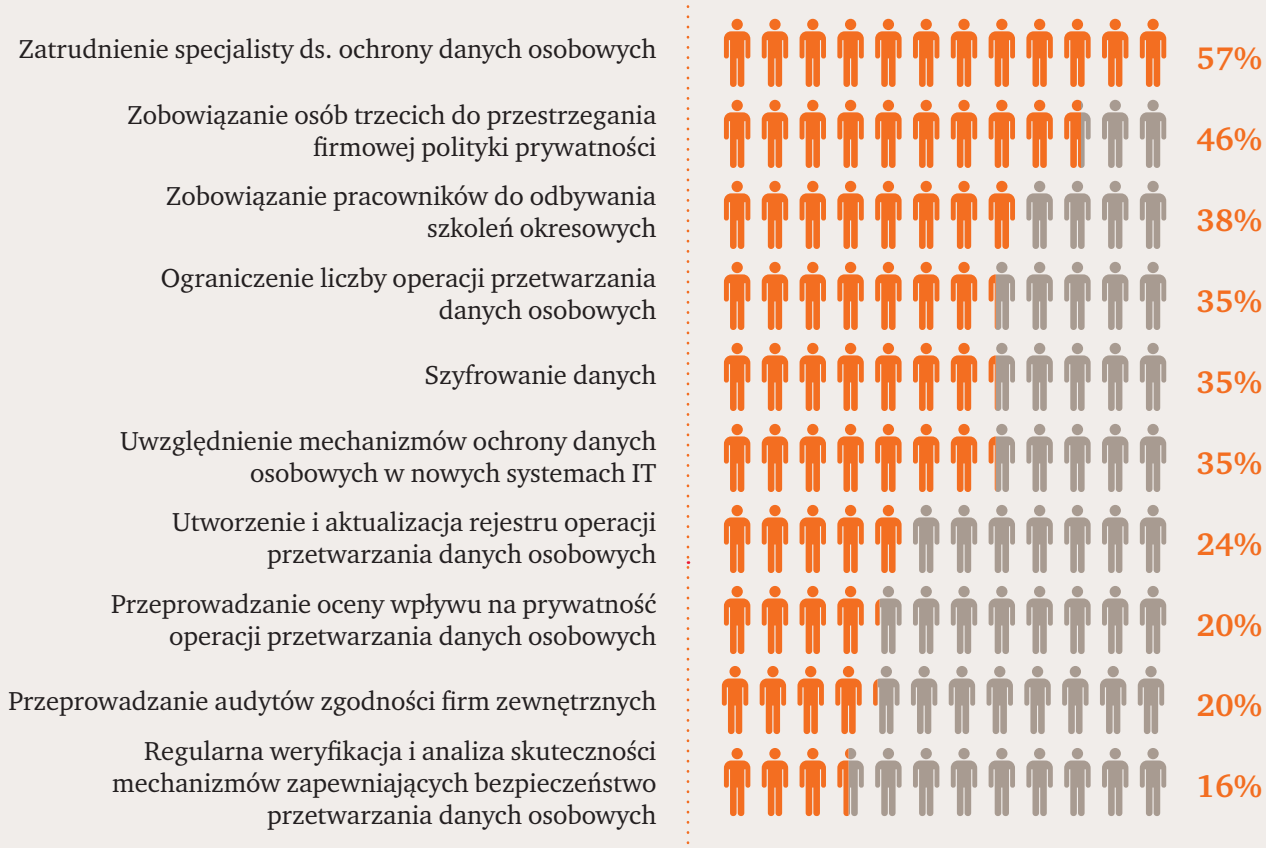
co piąta firma nie zainicjowała jeszcze przygotowań. Pełną gotowość osiągnęło zaledwie 3% badanych spółek, 20% rozpoczęło ocenę RODO. Na różnych etapach operacjonalizacji wypracowanych rozwiązań było 17% przedsiębiorstw. Wreszcie 20% respondentów zadeklarowało, że dostosowywanie organizacji do osiągnięcia zgodności z RODO wciąż trwa.

poniżej
30%

tak swoją gotowość do RODO ocenia połowa badanych firm

Przygotowania dalej są ograniczane do rozwiązań operacyjnie najprostszych. Najpowszechniej deklarowaną przez respondentów praktyką z obszaru ochrony danych osobowych jest zatrudnianie specjalisty do spraw ich ochrony lub pracownika na podobnym stanowisku, odpowiedzialnego za prowadzenie działalności zgodnie z obowiązującymi regulacjami (54% wskazań). W dalszej kolejności, firmy deklarują zobowiązywanie podmiotów trzecich do przestrzegania polityki prywatności (46% odpowiedzi) oraz obligowanie pracowników do odbywania szkoleń (38% wskazań).

Zabezpieczenia danych osobowych wdrożone w firmach



Tak jak przed rokiem, najbardziej zaniedbanymi obszarami są: ocena skutków przetwarzania danych osobowych, o której w badaniu wspomniało jedynie 20% badanych, czyli zaledwie o 5 punktów procentowych więcej niż w roku ubiegłym, oraz regularna weryfikacja i analiza skuteczności mechanizmów zapewniających bezpieczeństwo przetwarzania danych osobowych (16% wskazań). W obliczu niskiego średniego poziomu gotowości do RODO, można przypuszczać, że wiele działań zostanie podjętych na ostatnią chwilę, a sam ich zakres będzie ograniczony do minimum. To grozi powstaniem nieefektywnych rozwiązań tymczasowych, które raz wdrożone, będą funkcjonowały przez długie lata.

Także szansa weryfikacji efektywności obecnie podejmowanych działań nie jest wysoka. Już teraz mniej niż połowa firm wskazała, że przeprowadza lub zamierza przeprowadzać wśród swoich pracowników regularne szkolenia w zakresie ochrony danych osobowych – jednak najczęściej to właśnie pracownicy swoim zachowaniem doprowadzają do sytuacji, w których dane przechowywane w organizacji są zagrożone. Odsetek firm deklarujących chęć przeprowadzania regularnych audytów zgodności również nie jest wysoki. Obecnie rozwiązanie to funkcjonuje w 20% badanych organizacji. Optymizmem napawa jednak fakt, że aż 43% chce je wdrożyć w ciągu najbliższego roku.

„Zapewnienie zgodności z RODO jest złożonym i co istotne ciągłym procesem. Złożoność polega między innymi na tym, że nie ma w nowych przepisach unijnych zdefiniowanej listy czynności, których wykonanie doprowadzi w prosty sposób do spełnienia wymogów Rozporządzenia. Potrzebne jest między innymi zinwentaryzowanie i zrozumienie obiegu danych osobowych w organizacji, ich kategorii, wolumenu, wrażliwości, a także ryzyka związanego z ich przetwarzaniem. Dopiero na tej podstawie możliwe jest podejmowanie odpowiednich (dostosowanych do potrzeb organizacji) działań dostosowawczych w obszarze organizacyjnym, prawnym oraz IT. Samo zatrudnienie specjalisty ds. ochrony danych osobowych odpowiedzialnego za przestrzeganie przepisów (co deklaruje ponad połowa ankietowanych) może być jednym z podjętych kroków, ale na pewno nie jedynym.

Zapewnienie zgodności prowadzonej działalności z RODO w maju 2018 r. nie kończy procesu dostosowawczego – nie jest to bowiem akt jednorazowy. Ochrona danych osobowych i odpowiednie procedury w tym zakresie muszą zostać na stałe zakorzenione w organizacji, aby każde kolejne działania np. akcje marketingowe, wdrożenia IT czy podpisywane umowy były zgodne z nowymi przepisami. Warto już teraz zaplanować jakie działania należy podjąć w tym zakresie (stworzenie odpowiednich procedur, szkolenia, zakup narzędzi do monitorowania ryzyk związanych z przetwarzaniem danych osobowych), aby wymagania RODO były spełnianie zawsze, nie tylko w maju 2018”.

Michał Mastalerz
Partner odpowiedzialny
za portfolio usług RODO

3.

Wywrotna struktura

Cyberbezpieczeństwo na agendzie? Na pewno nie teraz

Już po raz piąty zadajemy pytanie: czy polskie firmy są naprawdę gotowe stawić czoło cyberzagrożeniom, czy też dominuje cyber-ruletka, obstawianie co może się przydarzyć, w miejsce całościowego podejścia i budowy trwałego systemu obrony?

Wyniki naszego badania niezmiennie od lat ukazują główną przyczynę zaistniałych problemów, rozbieżności i niekonsekwencji w zarządzaniu cyberryzykiem: w większości firm temat cyberzagrożeń wciąż nie znajduje się odpowiednio wysoko w agendzie zarządów.

Sytuacja ta dziwi szczególnie w obliczu faktu, że o ile zarządy polskich firm znają już wartość, jaką generuje stosowanie nowych technologii i potrafią z powodzeniem wdrażać je do swojego biznesu, o tyle w dalszym ciągu nie doceniają wyzwań związanych z naruszeniami cyberbezpieczeństwa towarzyszącemu tym technologiom.

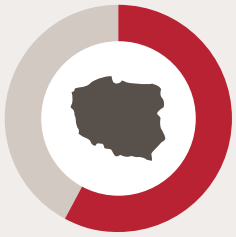
Jak wskazują wyniki badania *Digital IQ 2017*, w czasie, gdy prezesi światowych przedsiębiorstw w ogromnej większości wskazują na cyberbezpieczeństwo jako kompetencję o kluczowym znaczeniu dla funkcjonowania firmy, w Polsce działania w tym zakresie często ograniczają się do formalnego osiągania zgodności z regulacjami, związanymi zwłaszcza z ochroną danych osobowych. Jedynie w 18% firm dyrektor ds. bezpieczeństwa informacji postrzegany jest przez kierownictwo i zarząd, jako jeden z liderów firmy. Co więcej, w 80% przypadków firm brak jest jakichkolwiek procedur regularnego raportowania do zarządu o stanie bezpieczeństwa informacji. Brak jest tym samym fundamentów proceduralnych, aby ulokować cyberbezpieczeństwo w agendzie zarządczej.

Powodów zaistniałej sytuacji można się dopatrywać w braku świadomości ścisłego kierownictwa, jak istotną rolę w organizacji odgrywa cyberbezpieczeństwo i na jakie konkretne wyniki przekłada się aktywność w tym zakresie. Mamy tu do czynienia z zaklętym kręgiem przyczyn i skutków. Firmy nie postrzegają cyberbezpieczeństwa jako stałego wyzwania, a tym samym jego priorytet w agendzie jest niski, przez co spółki nie inwestują w całościowe rozwiązania typu SIEM czy SOC.

Cyberbezpieczeństwo jako kompetencja kluczowa dla firmy:

83%

Firmy na świecie



58%

Firmy w Polsce

Źródło: PwC, 2017 Global Digital IQ(R)

Z drugiej strony właśnie ta bierność i brak całościowego spojrzenia, nie powiązanie mechanizmów zabezpieczających i brak procesów detekcji, oceny i kwantyfikacji skutków incydentów sprawia, że wszelkie niedociągnięcia w tym zakresie wydają się nie mieć wpływu na wyniki firmy, utrzymując zarząd w fałszywym przekonaniu, iż cyberbezpieczeństwo to rynkowy trend, nie mający faktycznego długoterminowego przełożenia na kierowaną przez nich firmę.

„Audyt wewnętrzny w zakresie cyberbezpieczeństwa ma do odegrania ważną rolę, szczególnie obecnie. Teoretycznie jej zakres jest prosty do określenia – upewnienie się, że ryzyka związane z cyberbezpieczeństwem są odpowiednio wysoko na agendzie zarządu, doradztwo w zakresie prewencji i detekcji, audyty sprawdzające, czy organizacja odpowiednio zarządza ryzykami, ale... Audytorzy zazwyczaj nie mają świadomości i wiedzy w tym obszarze, nie czują się komfortowo w rozmowach o cyberbezpieczeństwie. Tematy cyberbezpieczeństwa występują rzadko w planach audytu, zwłaszcza w sektorze niefinansowym. W praktyce pojawiają się audyty zlecane przez kierownictwo, ale nie są koordynowane przez audyt wewnętrzny. Mają często charakter wycinkowy, na przykład ograniczają się do testów penetracyjnych. Co gorsze, takie działania dają zarządowi fałszywe poczucie bezpieczeństwa, a audytowi wewnętrznemu wymówkę, że za audyty w zakresie cyberbezpieczeństwa odpowiada kto inny".

Piotr Rówiński
Partner odpowiedzialny
za usługi zarządzania ryzykiem
i audytu wewnętrznego

Bezpiecznik to wciąż samotna wyspa

W obliczu niskiego umocowania cyberbezpieczeństwa w agendzie polskiej firmy, nie dziwi fakt, że w blisko 20% średnich i dużych firm nie ma żadnej osoby odpowiedzialnej za bezpieczeństwo informacji. Kolejne 21% respondentów zadeklarowało, że w ich organizacji za ten obszar odpowiada tylko jeden pracownik. Jedynie w 10% firm funkcjonują rozbudowane zespoły bezpieczeństwa informacji złożone z 20 lub więcej specjalistów.

W przypadku bezpieczeństwa IT sytuacja wygląda podobnie. 19% średnich i dużych firm nie zatrudnia żadnego specjalisty z tego zakresu. Natomiast 41% respondentów zadeklarowało, że o ten obszar troszczy się w ich spółce od 2 do 10 osób.

Porównując tę sytuację do wyników sprzed 2 lat można śmiało stwierdzić, że ten problem dodatkowo się nasila. W 2015 roku 86% firm zatrudniało przynajmniej jednego specjalistę z obszaru bezpieczeństwa informacji. Tak jak dwa lata temu, tak i obecnie, specjaliści ci zatrudnieni są w oddzielnych zespołach czy komórkach organizacyjnych, pozostając głównie osadzeni w ramach istniejących departamentów IT.

Szukając przyczyn zjawiska stale słabego poziomu obsadzenia stanowisk specjalistów bezpieczeństwa informacji w firmach, należy zastanowić się nie tylko nad wspomnianą już kwestią nie powiązania priorytetów strategicznych firmy z agendą cyberbezpieczeństwa, ale również nad sytuacją na rynku pracy. Tylko w Polsce deficyt specjalistów IT szacowany jest na około 40-50 tysięcy etatów. Specjaliści z zakresu cyberbezpieczeństwa są z tej grupy najbardziej poszukiwanymi ekspertami.

W obliczu tego niedoboru tym bardziej zaskakuje fakt, że umocowanie tych, bardzo często, pojedynczych specjalistów w ramach struktury organizacji nie jest dostatecznie wysokie. Kierownika lub dyrektora do spraw bezpieczeństwa zatrudnia jedynie 41% badanych przez nas przedsiębiorstw. Zaledwie 9% badanych deklaruje, że pozyskanie takiego pracownika jest priorytetem na najbliższy rok. Niestety zjawisko to wpisuje się w szeroko obserwowane zaniedbywanie bezpieczeństwa teleinformatycznego na poziomie strategicznym.

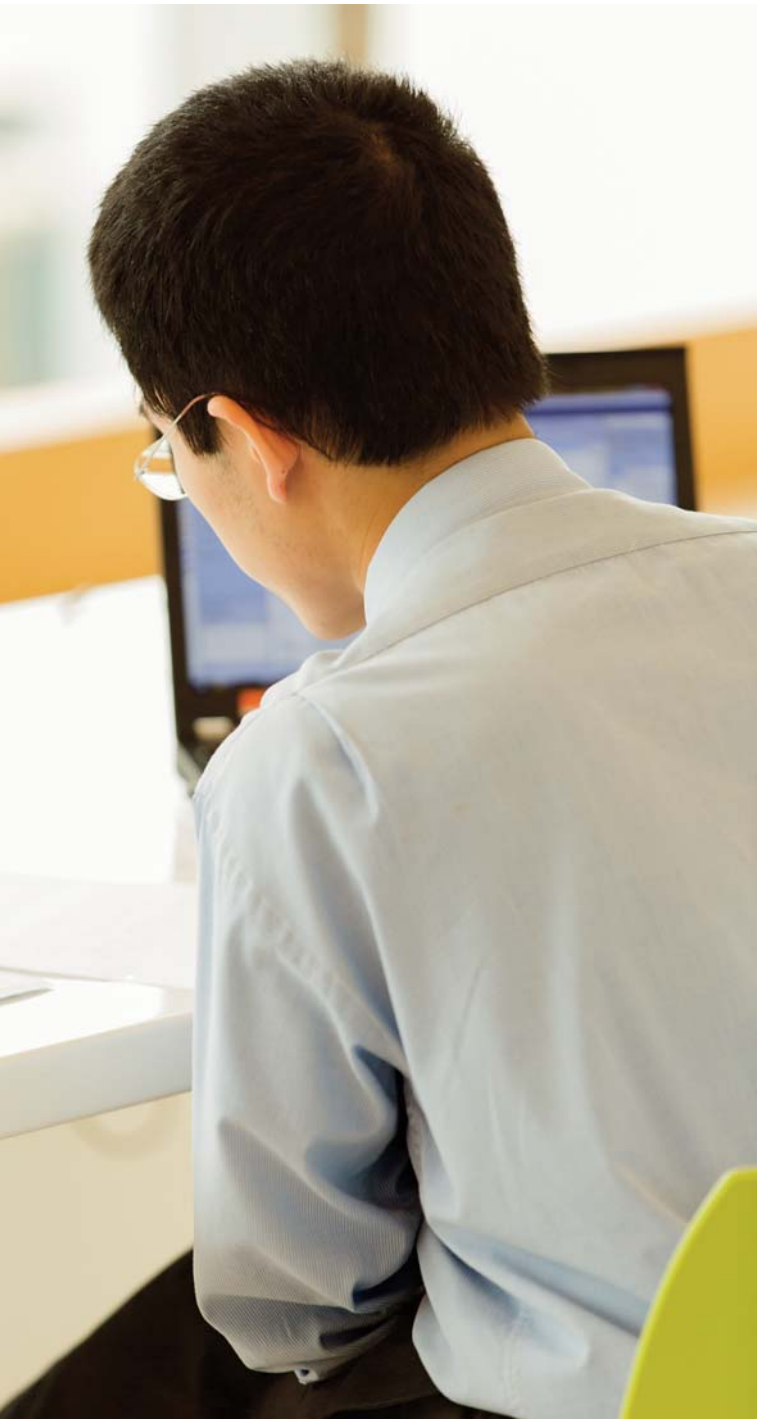
20%

średnich i dużych firm nie posiada żadnej osoby odpowiedzialnej za bezpieczeństwo informacji

59%

przedsiębiorstw nie zatrudnia kierownika lub dyrektora do spraw bezpieczeństwa

Stawka wysoka, a budżety niskie



Analiza wysokości budżetów przeznaczanych na bezpieczeństwo informacji jedynie potwierdza poprzednie tezy. Aż 28% respondentów ze średnich i dużych firm deklaruje, że przeznacza na bezpieczeństwo informacji mniej niż 50 000 złotych rocznie. Jedynie 12% uczestników badania wskazuje na budżety wyższe niż 1 milion złotych. Należy jednak podkreślić, że deklarowane wartości dotyczą wszystkich związanych z bezpieczeństwem informacji wydatków – od etatów po narzędzia i szkolenia.

Efektywna infrastruktura teleinformatyczna, która podnosi poziom dojrzałości całej organizacji opiera się na synergii trzech elementów – narzędzi i rozwiązań technicznych, ludzi, którzy mogliby z tych narzędzi korzystać oraz procesów, które stanowią fundament funkcjonowania tych elementów w organizacji. W tym kontekście widać, jak rażąco małe są budżety na cyberbezpieczeństwo. W wielu przypadkach niższe niż wysokość rocznego wynagrodzenia pełnoetatowego pracownika.

Przy takiej wysokości wydatków, ciężko jest mówić o jakiejkolwiek koordynacji inwestycji na cyberbezpieczeństwo – koordynacji, która jest podstawą efektywnego zarządzania bezpieczeństwem informacji firmy.

28%

respondentów ze średnich i dużych firm deklaruje, że przeznacza na bezpieczeństwo informacji mniej niż 50 000 złotych rocznie

4.

Karty na stół

Karty na stół, czyli kto wygrywa

Wnioski z tegorocznego badania są pesymistyczne, gdyż po raz kolejny prowadzą do podobnej jak w ubiegłych latach konkluzji. W opinii przeciętnej polskiej firmy, cyberbezpieczeństwo jest trendem, nie zaś realnym wyzwaniem, które powinno stać się jednym z priorytetów zarządu.

Na szczęściu można polegać jedynie do momentu, kiedy się je posiada, czyli nie z absolutną pewnością i nigdy na długo. Dopiero w momencie, kiedy firma padnie ofiarą ataku, cyberbezpieczeństwo objawia się jako jeden z filarów funkcjonowania firmy.

Przewiduje się, że takich okazji do nauki firmy będą miały coraz więcej. Według globalnego badania *PwC Risk in Review 2017* – ponad 62% zarządów firm uważa, że cyberzagrożenia będą w jeszcze większym stopniu wpływać na globalny rynek w przeciągu 3 najbliższych lat. Ten sam raport wskazuje, że w obliczu rosnącego zagrożenia jedynie około 9% wszystkich firm posiada wysoko rozwinięte kompetencje w zakresie zarządzania cyber ryzykiem firmy, natomiast kolejne 17% ma je opanowane na poziomie średnim.

Patrząc na rynek globalny, najlepiej radzą sobie firmy z branż transportu i logistyki oraz bankowości. Posiadają one nie tylko wysoko rozwinięte systemy SIEM, DLP czy SOC, ale również procesy, zespoły, oraz rozwiązania, które umożliwiają pełne ich wykorzystanie. Dotyczy to m.in. systemów klasy *Governance-Risk-Compliance*, które umożliwiają analizę szeregu danych i procesów z obszaru audytu, bezpieczeństwa oraz zgodności.

62% zarządów firm uważa, że cyberzagrożenia będą w jeszcze większym stopniu wpływać na globalny rynek

Indeks cyberbezpieczeństwa firm w Polsce

W ramach tegorocznego Badania Stanu Bezpieczeństwa Informacji podsumowaliśmy stan przygotowania zbadanych firm i zestawiliśmy jego elementy ze składowymi „wzorowej" infrastruktury teleinformatycznej w trzech wymiarach tj:

- odpowiednie narzędzia i systemy (m.in. SIEM, Anty APT, IPS/IDS, SOC)
- posiadanie oraz regularna weryfikacja procedur, inwestycja w zabezpieczenia na równi z technologiami
- proceduralne umocowanie kompetencji cyberbezpieczeństwa w firmie, zbudowany zespół ds. bezpieczeństwa informacji

Jak wynika z analizy, jedynie 8% ze wszystkich badanych przez nas firm posiada wysokie kompetencje w zakresie cyberbezpieczeństwa. Kolejne 7% to przedsiębiorstwa, które nie posiadają wszystkich kluczowych zabezpieczeń i elementów infrastruktury, lecz planują ich wdrożenie w okresie najbliższych 12 miesięcy.

Najbardziej dojrzałe firmy pochodzą z branż sektora finansowego, telekomunikacji energetyki oraz produkcji przemysłowej.

Sprawne i bezpieczne funkcjonowanie zapewniają im zrównoważone inwestycje w narzędzia i systemy (wszystkie posiadają wdrożone SOC, SIEM, Anty APT) oraz kompetencje zespołów. Co istotne, wszystkie firmy cechujące się wyższą dojrzałością w zakresie cyberbezpieczeństwa odznaczają się również odpowiednio wysokim umiejscowieniem tej funkcji w organizacji, oraz kulturą firmy, która to bezpieczeństwo wspiera. Mamy w ich przypadku do czynienia z pełną integracją funkcji cyberbezpieczeństwa z innymi funkcjami organizacji, a Dyrektorzy działów bezpieczeństwa informacji pełnią kluczowe role w firmowej hierarchii (80% wskazań).

Co więcej, w grupie firm najbardziej dojrzałych, nakłady ponoszone na rozwój cyberbezpieczeństwa nie stanowią tylko „zła koniecznego", tj. obowiązku sprostania regulacjom, ale przyczyniają się do budowy wartości firmy, jednocześnie ograniczając ekspozycję na ryzyko. Decyzje o uruchamianiu kolejnych projektów z tego obszaru nie opierają się jedynie o wynik prognozowanego zwrotu z inwestycji, lecz podejmowane są w szerszym kontekście z uwzględnieniem trudno kwantyfikowalnych długookresowych korzyści, takich jak zapewnienie stabilności operacyjnej firmy czy utrzymanie zaufania konsumentów do marki.

Indeks Cyberbezpieczeństwa

8% firm jest dojrzałych pod względem cyberbezpieczeństwa

Wdrożone systemy: SIEM, Anty APT, IPS/IDS, SOC

Budżet bezpieczeństwa równy min. 10% wydatków na IT

Zespół cybersecurity min. 2 osoby

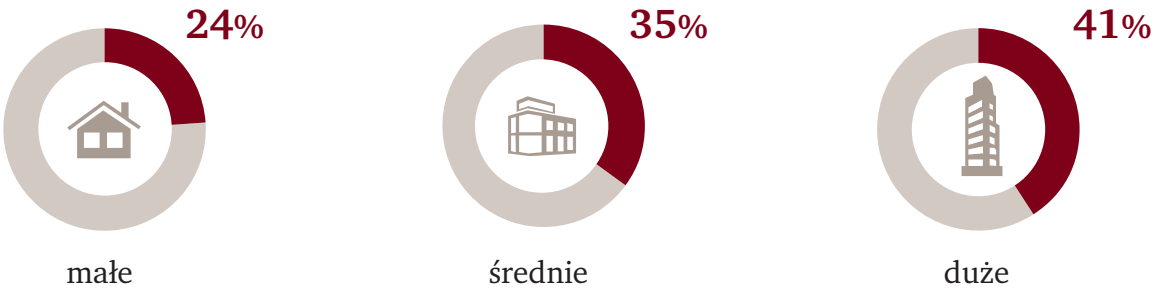
Raportowanie o stanie bezpieczeństwa bezpośrednio do zarządu

Utworzone stanowisko Dyrektora /Kierownika ds. cyberbezpieczeństwa

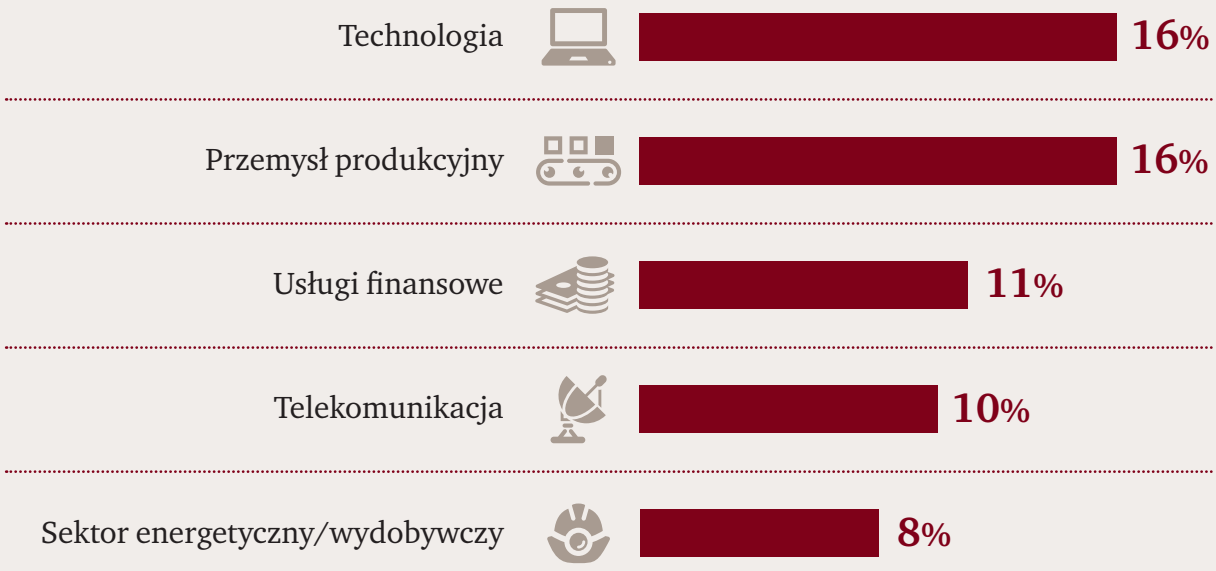
Metodyka

Raport został przygotowany na podstawie badania, w którym wzięło udział 127 polskich ekspertów zajmujących się IT i bezpieczeństwem informacji. Badanie zostało przeprowadzone jesienią 2017 roku metodą ankiety online.

Wielkość badanych firm:



Sektory działania badanych firm (Top 5):



pwc.pl/badaniebezpieczenstwa

Kontakt

Piotr Urban
Partner, Lider ds. cyberbezpieczeństwa
w regionie Europy Środkowo-Wschodniej
Tel.: +48 502 184 157
E-mail: piotr.urban@pwc.com

Anna Sieńko
Partner, Lider ds. technologii
w regionie Europy Środkowo-Wschodniej
Tel.: +48 601 455 845
E-mail: anna.sienko@pwc.com

Tomasz Sawiak
Wicedyrektor, Zespół Cyber Security
Tel.: +48 519 504 234
E-mail: tomasz.sawiak@pwc.com

Patryk Gęborys
Wicedyrektor, Zespół Cyber Security
Tel.: +48 519 506 760
E-mail: patryk.geborys@pwc.com