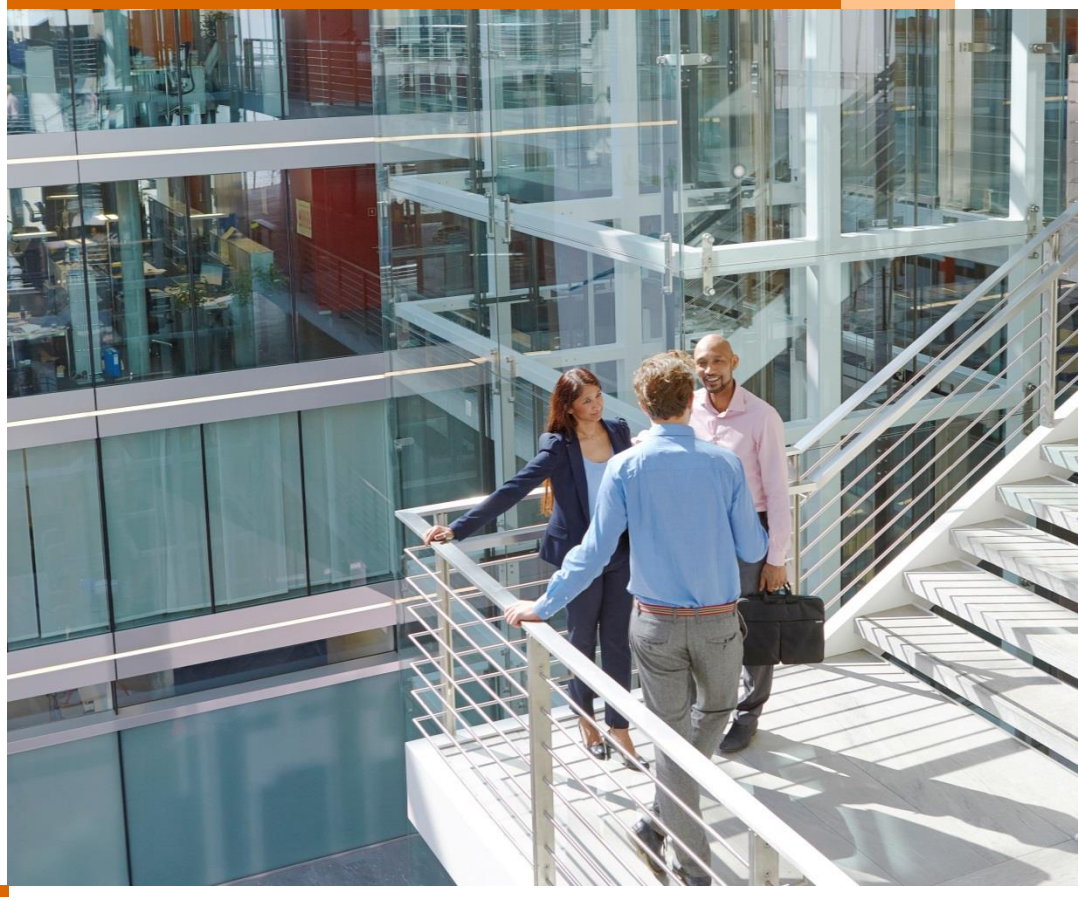
www.pwc.pl/bezpieczenstwo-biznesu

Zarządzanie ryzykiem w cyberprzestrzeni

Kluczowe obserwacje z wyników ankiety „Globalny stan bezpieczeństwa informacji 2015”

(The Global State of Information Security® Survey 2015)

Grudzień 2014



pwc

Spis treści

Wstęp

Piotr Urban
Partner,
Lider PwC Risk Assurance

Rafał Jaczyński
Lider zespołu PwC Cyber Security w Polsce i Europie Centralnej

Szanowni Państwo,

Mamy przyjemność oddać w Państwa ręce raport, który stanowi nasz wkład w debatę na temat aktualnego stanu bezpieczeństwa informacji w Polsce i na świecie. Jest to druga polska edycja raportu, prezentujemy w niej wyniki dla Polski na tle rezultatów globalnych.

Cyberprzestępczość to realne zagrożenie na świecie. W tym roku przekonaliśmy się, że Polska nie jest zieloną wyspą i że temat w Polsce jest równie ważny, realny, a co więcej nasila się. Ataki na sektor finansowy, energetyczny czy ochrony zdrowia wskazują na rosnącą skalę tego zjawiska.

Zarządzenie bezpieczeństwem w cyberprzestrzeni to temat istotny dla działów informatyki, ale nie jest to zagadnienie tylko IT. Ryzyka związane z prowadzeniem biznesu w cyberprzestrzeni, takie jak ryzyko utraty reputacji, straty finansowe, przerwa w sprzedaży, skutki dla innowacji, badań i rozwoju, czy kary regulacyjne to tematy ważne dla CEO, CFO, COO, Dyrektora Sprzedaży, PR oraz pracowników firmy. Dlatego też powinny znaleźć się na mapie kluczowych ryzyk do monitorowania przez Rady Nadzorcze i Audyt Wewnętrzny – nie bez powodu w 2014 r. Światowe Forum Gospodarcze zaliczyło cyber-ataki do pięciu najważniejszych rodzajów ryzyka pod względem prawdopodobieństwa wystąpienia.

Mamy nadzieję, że informacje zawarte w naszym raporcie będą inspiracją i wsparciem przy kształtowaniu strategii bezpieczeństwa w Państwa firmach.

01

Cyber-ryzyka: groźne i rzeczywiste

Cyberbezpieczeństwo – nierozłącznie związane z biznesem

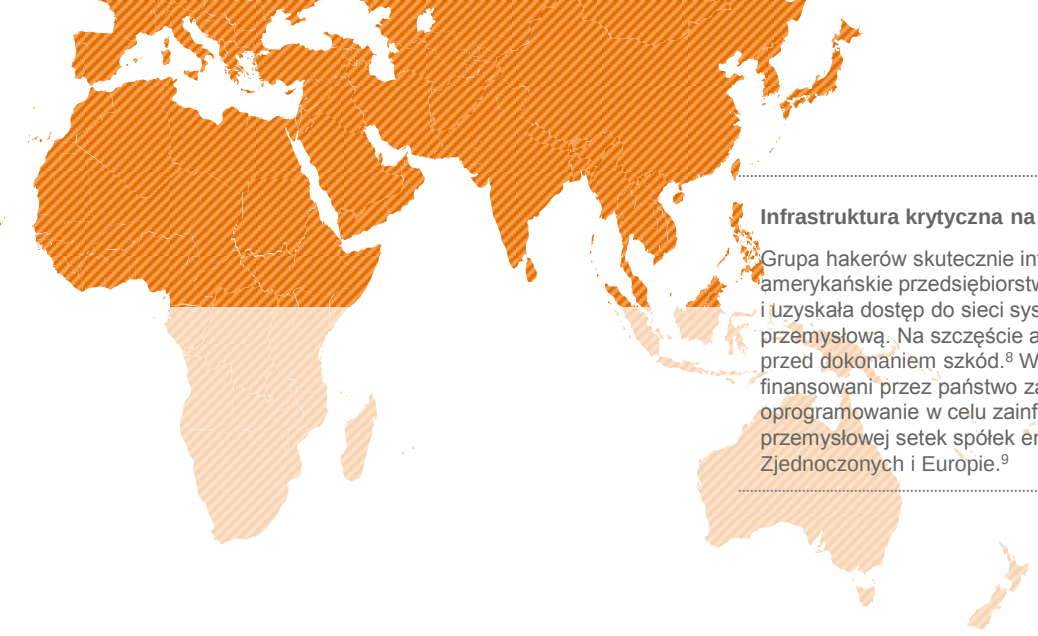
Ataki na systemy informatyczne, telekomunikacyjne i produkcyjne nie są już przedmiotem zainteresowania wyłącznie specjalistów ds. bezpieczeństwa informacji i IT. Ich konsekwencje są odczuwalne dla zarządów firm i innych interesariuszy, w tym klientów.

- Media często podają wypadki związane z przełamaniem zabezpieczeń, a przez ponad 12 ostatnich miesięcy prawie każda branża musiała stawić czoła zagrożeniom cybernetycznym.
- Ze względu na wzrastającą świadomość konsumentów, obywateli i wnikliwość mediów coraz rzadziej poważne włamanie pozostaje niezauważone i coraz częściej wymaga od firm i instytucji rzeczywistej, a nie tylko słownej, reakcji.[1]

Spółki świadczące usługi finansowe nadal są głównym celem ataków, coraz częściej atakowane są giełdy papierów wartościowych

Przestępcy spowodowali straty na rachunkach kart kredytowych dwóch bliskowschodnich banków na całym świecie na ponad 45 mln USD.[2] Amerykańskie banki straciły dane dziesiątek mln klientów w wyniku włamań. Polskie banki były przedmiotem kampanii DDoS powodujących wielogodzinne wyłączenia ich internetowych kanałów obsługi klientów.[3]

Badanie 46 światowych giełd przeprowadzone przez Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO) i Światową Federację Giełd wykazało ponadto, że ponad połowa z nich (53%) padła ofiarą cyberataku.[4] Warszawska Giełda Papierów Wartościowych była również przedmiotem ataków w ciągu mijającego roku.



Infrastruktura krytyczna na celowniku

Grupa hakerów skutecznie infiltrowała przez Internet amerykańskie przedsiębiorstwo usług komunalnych i uzyskała dostęp do sieci systemu sterującego automatyką przemysłową. Na szczęście atak udało się powstrzymać przed dokonaniem szkód.[8] Wyrafinowani cyber-szpiedzy finansowani przez państwo zastosowali specjalne złośliwe oprogramowanie w celu zainfekowania systemów kontroli przemysłowej setek spółek energetycznych w Stanach Zjednoczonych i Europie.[9]

Również w Polsce mijający rok upłynął pod znakiem ataków na istotne systemy infrastruktury krytycznej – w połowie roku media donosiły o akcji grupy hakerskiej wymierzonej w sektor energetyczny.[5]

Zanotowano również wzrost ataków na urządzenia konsumenckie podłączone do globalnej sieci – takie jak urządzenia do monitorowania małych dzieci, termostaty czy telewizory – które składają się na Internet Rzeczy (ang. Internet of Things), powstający ekosystem urządzeń, który wymienia między sobą informacje. Te urządzenia podłączone do Internetu są narażone na ataki, ponieważ nie mają podstawowych zabezpieczeń, co ostatnio potwierdziło badanie HP „Fortify on Demand".

Firma HP dokonała przeglądu 10 najczęściej używanych urządzeń i odkryła, że 70% z nich zawiera poważne podatności mechanizmów ochrony.[6]

Ryzyko dotyczy nie tylko urządzeń

Pojawiły się informacje, że samochody zawierające dziesiątki komputerów często połączonych ze sobą, a w niektórych przypadkach komunikujących się bezprzewodowo z otoczeniem zewnętrznym mogą być celem ataku pozwalającego na przejęcie kontroli nad systemami hamowania, sterowania, a nawet silnika. Firma IOActive opublikowała badanie, które szczegółowo wykazuje, w jaki sposób hakerzy mogą kontrolować Elektroniczne Jednostki Kontroli (Electronic Control Units) konkretnych samochodów i zaproponowali mechanizmy umożliwiające wykrycie ataku.[7]

Warto wspomnieć również spektakularną kradzież danych prawie 4,5 mln pacjentów z amerykańskiej sieci szpitali.

W Polsce w zeszłym roku odnotowano ataki na systemy firm świadczących usługi medyczne. Przyczyną włamania był jeden z najpoważniejszych problemów z bezpieczeństwem Internetu ujawniony w 2014 roku.

Skutki błędu nazwanego *Heartbleed dotknęły* prawie dwie trzecie serwerów sieciowych na całym świecie, w tym niektóre najbardziej popularne usługi poczty elektronicznej, witryny WWW i społecznościowe. Uważa się, że awaria ta zagroziła milionom serwisów, sklepów internetowych i aplikacji, a także komunikatorom internetowym, narzędziom zdalnego dostępu i urządzeniom sieciowym.[10]

Narastające napięcia polityczne i konflikty międzypaństwowe, szczególnie między Rosją i Ukrainą, wywołały serię cyberataków, co doprowadziło do zniknięcia z Internetu stron rządowych tych państw i do zainfekowania złośliwym oprogramowaniem witryn ich ambasad. *Nie dziwi więc uwzględnienie aspektów cyberbezpieczeństwa w podpisanej przez Prezydenta RP w listopadzie 2014 „Strategii Bezpieczeństwa Narodowego RP".* Medialne doniesienia dotyczące ujawnienia kodów źródłowych oraz danych użytkowników systemu wspierającego wybory samorządowe potwierdzają tylko potrzebę przeznaczenia na te zagadnienia zwiększonej uwagi, czasu i środków.

Nawet ci, którzy opisują włamania do systemów IT nie uchronili się przed atakiem. Niektóre najbardziej renomowane gazety takie jak „The New York Times", „The Financial Times", CNN czy Reuters, uległy hakerom – ich konta na Twitterze zostały przejęte lub strony zablokowane. Wiele najpoważniejszych ataków przeprowadzili hakerzy powiązani z rządami państw z Bliskiego Wschodu.

Każda istniejąca lista incydentów jest z pewnością niekompletna. Trudno z całą pewnością stwierdzić, które organizacje są infiltrowane, ponieważ wiele z nich nie wie, że zostały zaatakowane. Inne niechętnie ujawniają informacje o włamaniach z uwagi na obawę przed utratą reputacji, sprawami sądowymi czy śledztwem regulatorów.

Regulatorzy na całym świecie prowadzą coraz aktywniejsze działania w sprawie cyber-ryzyka

W wyniku wzrostu ilości incydentów rządy coraz aktywniej pomagają organizacjom w zwalczaniu cyberprzestępstw.

„Moim zdaniem DOJ i FBI będą nadal stosować agresywną strategię wobec państw, które starają się wyrządzić szkodę gospodarce amerykańskiej."

Sean Joyce, dyrektor PwC i były zastępca dyrektora FBI

Przykładowo, amerykańskie Federalne Biuro Śledcze (FBI) ujawniło, że w 2013 roku zawiadomiło 3000 spółek (m.in. banki, sklepy i spółki z branży produkcji wojskowej), że stały się ofiarami ataków hakerskich. W następstwie tego zdarzenia amerykańskie Ministerstwo Sprawiedliwości (DOJ) oskarżyło pięciu chińskich hakerów o cyberszpiegostwo gospodarcze wobec spółek amerykańskich działających w sektorze energii atomowej, metalurgii i energii słonecznej. Był to pierwszy przypadek, kiedy USA oficjalnie oskarżyły urzędników państwowych o szpiegostwo gospodarcze przy użyciu ataków sieciowych.

Przykładem planowanych zmian w otoczeniu regulacyjnym jest ogłoszony niedawno plan Biura ds. Kontroli Zgodności Komisji Papierów Wartościowych i Giełd USA (SEC Office of Compliance Inspections and Examinations – OCIE) dotyczący sprawdzenia przygotowania ponad 50 zarejestrowanych maklerów/brokerów i doradców inwestycyjnych na ewentualny atak cybernetyczny.

W Azji Ustawa o bezpieczeństwie danych osobowych Singapuru (Singapore Personal Data Protection Act) określa nowe standardy zbierania, wykorzystania i ujawniania danych osobowych.

Nowe wytyczne podkreślają kilka wyjątkowych wymogów, między innymi sugerują, że organizacje powinny zapewnić sobie ubezpieczenie cybernetyczne i być w stanie sporządzić kompleksową inwentaryzację wszystkich incydentów naruszenia bezpieczeństwa. Wytyczne SEC wymagają również wprowadzenia przez przedsiębiorstwa procesów oceny ryzyka oraz skuteczniejszej oceny ryzyka sprzedawcy i zapewnienia właściwej staranności.

W Polsce Komisja Nadzoru Finansowego regulująca rynek bankowy wydała w 2013 roku Rekomendację D, która wyznacza nowe standardy w zakresie wymagań dla zarządzania systemami IT i bezpieczeństwem informacji w bankach. Banki powinny się do niej dostosować do 1 stycznia 2015 roku, a kolejni uczestnicy rynku finansowego w Polsce są także sukcesywnie nią obejmowani.

Zarządy firm przyglądają się nowemu unijnemu rozporządzeniu w sprawie ochrony danych, które ma być opracowane do 2015 roku. Oczekuje się, że Rozporządzenie doda nowe wymogi dotyczące zawiadamiania osób fizycznych o naruszeniach, wprowadzi wymogi prowadzenia ocen ryzyka i audytów dla organizacji administrujących danymi osobowymi i zwiększy znacząco kary dla przedsiębiorstw niewystarczająco je chroniących.[11]

„Przedsiębiorcy zobowiązani do ujawniania organom ochrony danych osobowych i osobom fizycznym incydentów dotyczących ochrony danych osobowych, będą baczniej analizować podejmowane działania i zwracać większą uwagę na przypadki ujawnienia danych osobowych. Zakładam, że po wejściu w życie nowych przepisów, liczba zgłoszeń takich incydentów będzie rosła lawinowo, co przełoży się na większą świadomość ryzyka zaistnienia cyberprzestępstw. Przedsiębiorcy, którzy dziś myślą kategoriami „mnie to nie dotyczy", będą musieli przygotować się na zmiany i podjąć działania zabezpieczające dane osobowe lub ryzykować zapłatę wysokich kar pieniężnych."

Anna Kobylańska, adwokat prowadząca praktykę ochrony praw własności intelektualnej, nowych technologii i danych osobowych w kancelarii PwC Legal

Rząd USA wspiera także firmy w podnoszeniu poziomu cyberbezpieczeństwa

W Stanach Zjednoczonych Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST) opracował wytyczne do stosowania przez firmy prywatne. Poszczególne organizacje korzystają z wersji 1.0 dobrowolnego standardu, by ocenić i poprawić swoje bezpieczeństwo cybernetyczne oraz stworzyć wspólny język do dyskusji i współpracy w zakresie wymiany informacji o atakach i zagrożeniach oraz sposobach reagowania na nie.

W obszarze sektora prywatnego firma Google uruchomiła inicjatywę Project Zero, która ma na celu poprawę stanu bezpieczeństwa przez identyfikację i zapobieganie zagrożeniom typu „zero-day" (nieznane wcześniej i „niezałatane" błędy oprogramowania), zanim hakerzy będą mogli je wykorzystać. Google twierdzi, że w ramach Project Zero badacze będą pracować nad poprawą bezpieczeństwa szeroko używanego oprogramowania, studiować motywacje i techniki atakujących oraz prowadzić badania nad skutecznym monitorowaniem i ograniczaniem zagrożeń w cyberprzestrzeni.[12]

02

Liczba incydentów i ich skutki finansowe nadal rosną

Dalszy wzrost liczby incydentów nie jest niespodzianką

Z uwagi na charakter i liczbę istotnych naruszeń bezpieczeństwa w ciągu ostatniego roku nie jest niespodzianką, że liczba incydentów, o których informowali respondenci w naszym badaniu, ponownie wzrosła w porównaniu do minionych lat.

Badanie to, przeprowadzone wśród ponad 9700 członków zarządów spółek odpowiedzialnych za sprawy. bezpieczeństwa, IT i operacji, wykazało, że łączna liczba incydentów związanych z naruszeniem bezpieczeństwa wykryta przez respondentów wzrosła w tym roku do 42,8 mln, co odpowiada wzrostowi o 48% w ciągu 2013 roku. Stanowi to równowartość 117 339 dokonanych codziennie ataków.

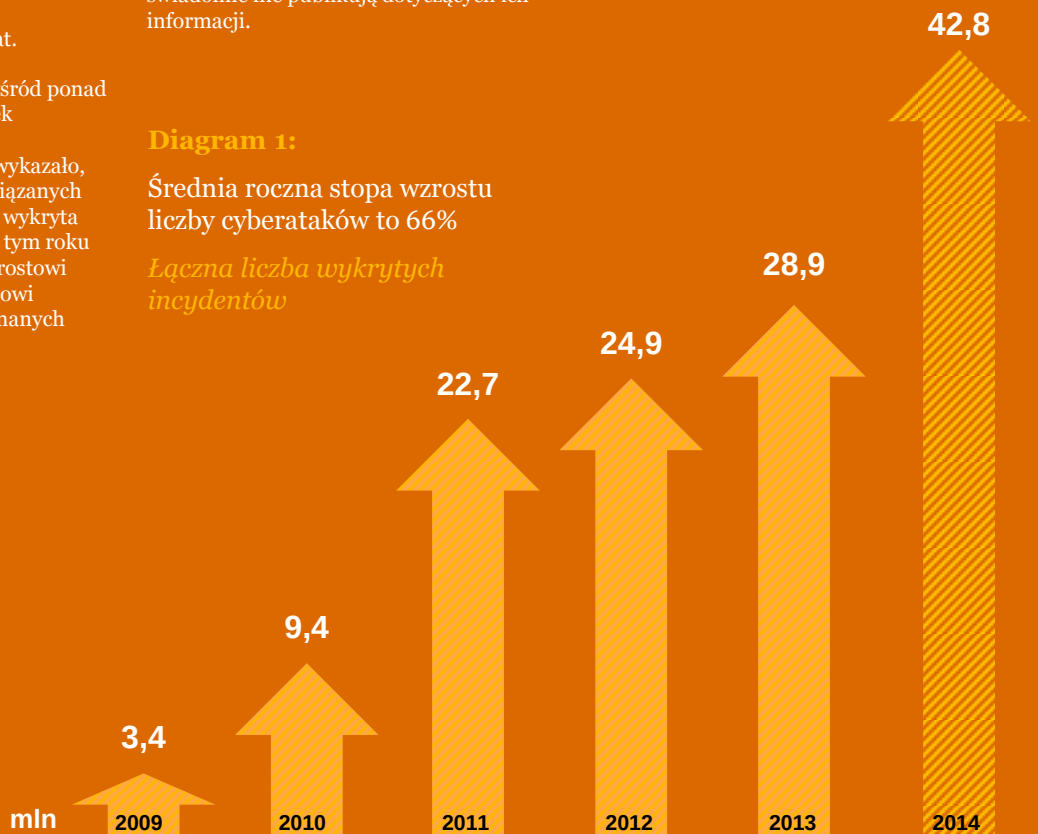
W dłuższej perspektywie nasze dane pokazują, że średnia roczna stopa wzrostu wykrytych incydentów naruszenia bezpieczeństwa wyniosła 66% rok do roku od 2009 roku.

Te liczby nie są jednak w żadnej mierze ostateczne, reprezentują jedynie łączną liczbę wykrytych i zgłoszonych incydentów. Jak pisaliśmy wcześniej, wiele organizacji nie zdaje sobie sprawy z ataków, inne świadomie nie publikują dotyczących ich informacji.

Diagram 1:

Średnia roczna stopa wzrostu liczby cyberataków to 66%

Łączna liczba wykrytych incydentów



Wydaje się pewne, biorąc pod uwagę zaawansowanie dzisiejszych ataków, że znaczna liczba incydentów pozostaje niewykryta. Jedna z firm ochrony cybernetycznej oszacowała ostatnio, że nawet 71% zagrożeń bezpieczeństwa może pozostać niewykrytych.[13]

W zakresie wykrywania incydentów duże spółki mają przewagę nad małymi

W naszej ankiecie duże organizacje (z rocznymi przychodami w wysokości 1 mld USD lub więcej) wykryły o 44% więcej incydentów niż w poprzednim roku. Fakt, że duże spółki wykrywają więcej incydentów, nie jest zaskakujący.

Autorzy zagrożeń zazwyczaj kierują swoje działania przeciwko dużym organizacjom, gdyż przeważnie oferują one bogate zbiory informacji – łącznie z dokumentami dotyczącymi strategii handlowej, własności intelektualnej związanej z projektami produktów i dużymi ilościami danych konsumenckich, które można wykorzystać, sprzedać albo użyć do celów gospodarczych lub wojskowych. Większe spółki zazwyczaj mają również bardziej rozwinięte procesy i technologie bezpieczeństwa, co pozwala im na wykrywanie większej liczby incydentów.

Z powodu wdrażania przez większe firmy bardziej efektywnych zabezpieczeń autorzy zagrożeń coraz częściej atakują spółki średniej wielkości, z których wiele nie wprowadziło równie zaawansowanych rozwiązań. To w części wyjaśnia 64-proc. skok liczby incydentów wykrytych przez organizacje średniej wielkości (o przychodach w wysokości od 100 mln USD do 1 mld USD).

Małe organizacje okazały się wyjątkiem w liczbie wykrywanych zagrożeń. Spółki o przychodach niższych niż 100 mln USD wykryły w tym roku o 5% mniej incydentów. Przyczyny nie są oczywiste, ale jednym z możliwych wyjaśnień jest to, że małe spółki inwestują mniej w bezpieczeństwo informacji, co może sprawiać, że są niezdolne do wykrywania incydentów i że są lepszym celem dla cyberprzestępców.

Małe firmy często uważają, że nie są łakomym kąskiem – to duży błąd. Należy również zauważyć, że zaawansowani przeciwnicy często koncentrują się na małych i średnich spółkach, które mają pełnić rolę „przyczółka" do wejścia do powiązanych z nimi przedsiębiorstw partnerskich. Dodatkowo duże spółki często nie dokładają starań, by monitorować bezpieczeństwo swoich partnerów, dostawców czy łańcuchów dostaw.

Brak właściwej staranności w kontroli stron trzecich jest tak powszechny, że rosnąca liczba regulatorów wymaga teraz oceny możliwości partnerów i całego łańcucha dostaw firm w newralgicznych sektorach rynkowych.

Aby poprawić swoją sytuację w zakresie bezpieczeństwa, jedną z możliwości dla małych i średnich spółek jest rozważenie korzystania z outsourcingu. To pozwoli im na zastosowanie nowoczesnych technologii i procesów do wykrycia incydentów zagrożenia bezpieczeństwa w oszczędny sposób.

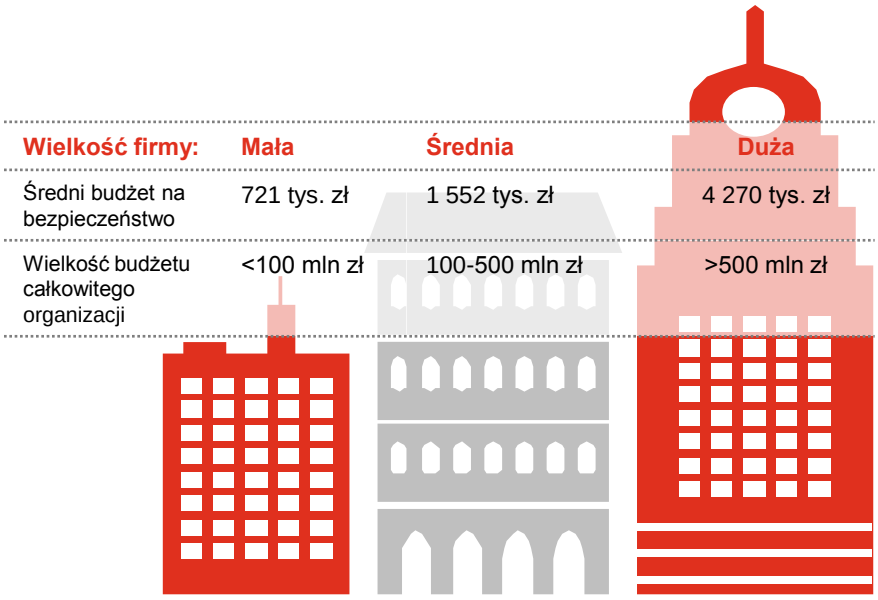
Należy jednak zwrócić uwagę, że Polska, w porównaniu do liderów, ma jeszcze sporo do nadrobienia w zakresie szerokości oferty outsourcingu usług zarządzania bezpieczeństwem. Usługi tego typu są często oferowane przez małe podmioty, z definicji nie posiadające możliwości ludzkich i kapitałowych, pozwalających na spełnienie wymagań ciągłości działania i kontraktowej odpowiedzialności.

Przyglądając się incydentom dotyczącym bezpieczeństwa w różnych regionach geograficznych, widać, że cyberprzestępczość rośnie w istotny sposób w Europie, gdzie zanotowano **41% skok** liczby wykrytych incydentów.

W Ameryce Północnej w tym roku respondenci wykryli o 11% więcej incydentów. Respondenci z Dalekiego Wschodu deklarują mniejsze osiągnięcia w zakresie wykrywania incydentów i zgłaszają 5% wzrost wykrytych przypadków.

Jedynym rejonem, gdzie odnotowano spadek wykrytych zagrożeń, jest Ameryka Południowa: liczba incydentów spadła tam o 9%. Warto zauważyć, że wydatki na bezpieczeństwo informacji spadły w Ameryce Południowej o 24%, znacznie bardziej niż w innych regionach.

Diagram 2:
Budżet na zapewnienie bezpieczeństwa informacji
według wielkości spółki (przychody) w 2014 r. (Polska)



Straty finansowe szybko rosną

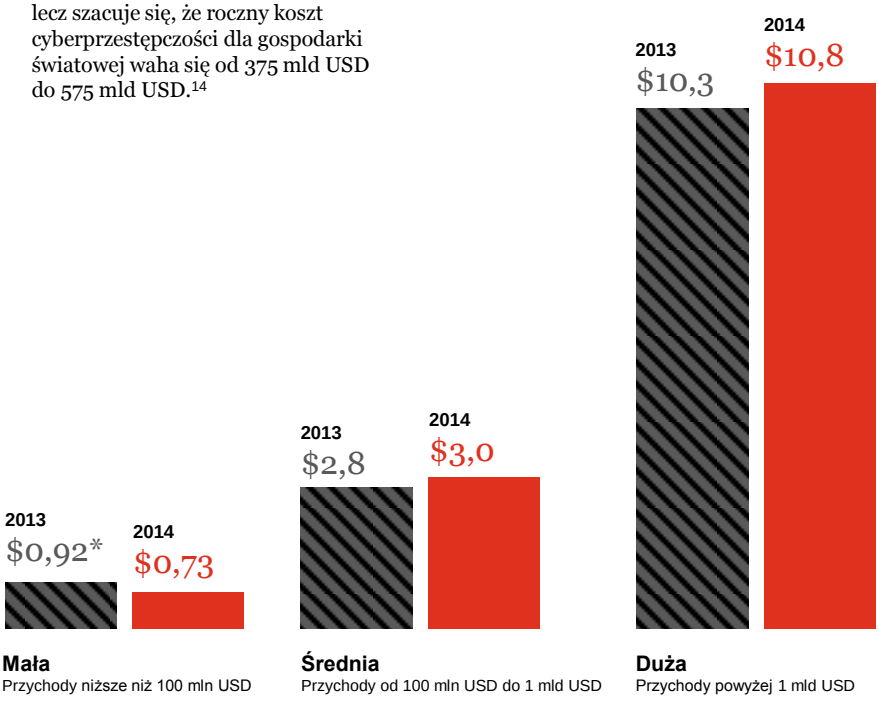
W miarę wzrostu liczby cyberataków rosną koszty zarządzania i ograniczania skutków incydentów.

Na świecie roczne szacowane średnie straty finansowe przypisywane incydentom naruszania cyberbezpieczeństwa wyniosły 2,7 mln USD, co stanowi znaczny, bo 34% wzrost w porównaniu z 2013 rokiem.

Podobnie jak łączna liczba incydentów, światowy koszt cyberprzestępczości jest niestety niemożliwy do zweryfikowania, gdyż wiele ataków pozostaje niezgłoszonych, a wartość niektórych informacji, takich jak własność intelektualna, jest trudna do wyliczenia. Ostatnio prowadzone przez Center for Strategic and International Studies badanie wykazało, że są trudności w oszacowaniu skutków finansowych, lecz szacuje się, że roczny koszt cyberprzestępczości dla gospodarki światowej waha się od 375 mld USD do 575 mld USD.[14]

Ta kwota wydaje się wysoka, jednak nawet w przybliżeniu jest niższa od strat, jakie mogą wyniknąć z kradzieży tajemnic handlowych i własności intelektualnej. Wpływ tego rodzaju utraty informacji można mierzyć wskaźnikami finansowymi i niefinansowymi.

Diagram 3:
Incydenty są bardziej kosztowne dla większych organizacji
Średnie straty finansowe wynikające z incydentów bezpieczeństwa, lata 2013–2014 (globalnie)



* miliony USD

Skutki finansowe mogą obejmować spadek przychodów, zakłócenia w działalności gospodarczej, kary od organów nadzoru i odpływ klientów.

Skutki niefinansowe mogą obejmować utratę reputacji, piractwo produktów, zmianę kierunku informacji dotyczących badań i rozwoju, skutki dla innowacji, kradzież projektów lub prototypów produktów, kradzież procesów gospodarczych lub produkcyjnych, a także utratę wrażliwych informacji, takich jak plany fuzji lub połączeń oraz strategii przedsiębiorstwa. Należy wspomnieć również o coraz częstszych konsekwencjach personalnych dla zarządów firm.

Korzystając z danych Banku Światowego, który podaje szacowane roczne światowe PKB za 2013 rok na poziomie **74,9 bln USD**, straty z tytułu tajemnicy handlowej mogą się wahać od **749 mld USD** do nawet **2,2 bln USD** rocznie.[15]

Centrum odpowiedzialnej przedsiębiorczości i handlu (Center for Responsible Enterprise And Trade – CREATe.org) wspólnie z PwC oszacowały wpływ kradzieży tajemnicy handlowej na 1% do 3% rocznego produktu krajowego brutto danego kraju (PKB).[16] Potencjalne straty wydają się jeszcze groźniejsze, gdy wliczy się prawdopodobieństwo działań hakerskich.

W 2014 roku w globalnym raporcie na temat ryzyka Światowe Forum Gospodarcze zaliczyło cyber-ataki do **pięciu najpoważniejszych rodzajów ryzyka** pod względem prawdopodobieństwa wystąpienia.[17] Możliwość naruszenia bezpieczeństwa stanowi zagrożenie, z którego coraz więcej członków wyższego kierownictwa zdaje sobie sprawę.

Prawie **połowa (48%)** respondentów sondażu „Global Economic Crime Survey 2014" przeprowadzonego przez PwC stwierdziła, że postrzeganie ryzyka cyberprzestępczości dla ich organizacji w ciągu ubiegłego roku wzrosło, podczas gdy w 2011 roku było to 39% badanych.[18] Członkowie kierownictwa wyraźnie widzą, że zagrożenia cybernetyczne stały się istotnym problemem w zarządzaniu ryzykiem przedsiębiorstwa.

Choć ryzyko stało się powszechne, nasze badanie dotyczące bezpieczeństwa wykazało, że straty z tytułu incydentów naruszenia bezpieczeństwa różnią się znacznie w zależności od wielkości przedsiębiorstwa. Aby zrozumieć te rozbieżności, przyjrzeliśmy się sposobom pomiaru skutków finansowych incydentów dotyczących bezpieczeństwa dla przedsiębiorstw.

Analiza z punktu widzenia wielkości przedsiębiorstw nie przyniosła zaskakujących wyników – duże światowe spółki zazwyczaj wydają więcej na bezpieczeństwo informacji, wdrażają bardziej dojrzałe programy i w związku z tym bardziej prawdopodobne jest posiadanie przez nie procesów i wiedzy wystarczających do dokładnego wyliczenia strat finansowych. Dzięki temu mogą rozważyć pełny zakres możliwych skutków, łącznie z kosztami związanymi z utratą klientów, opłatami za obronę sądową, ugodami sądowymi, badaniami kryminalistycznymi i utratą reputacji.

Większe organizacje mają również bardziej strategiczne podejście do bezpieczeństwa dzięki określeniu wrażliwych aktywów i przeznaczeniu wydatków na najbardziej wartościowe dane; zazwyczaj rozumieją one również ryzyko ze strony stron trzecich, dzięki zastosowaniu linii odniesienia do bezpieczeństwa dotyczącego partnerów gospodarczych.

Duże spółki zazwyczaj również wdrożyły procesy i technologie pozwalające na aktywne monitorowanie i analizowanie informacji wywiadowczych dotyczących bezpieczeństwa; w przypadku wykrycia anomalii są lepiej przygotowane do szybkiego zareagowania na incydent.

Duże organizacje częściej kultywują kulturę bezpieczeństwa dzięki uświadamianiu pracowników i programom szkoleniowym, a także dzięki temu, że wyższa kadra kierownicza rozpowszechnia wiedzę o znaczeniu cyberbezpieczeństwa w przedsiębiorstwie.

W Polsce respondenci w większości wskazują, że nie znają kosztu związanego z incydentem bezpieczeństwa albo pozostaje on w granicach 50 000 PLN. Może to wskazywać na fakt, że firmy nie zaczęły jeszcze analizować kosztów incydentów, a co za tym idzie, nie są w stanie stwierdzić jak skuteczne są ich nakłady na obszar bezpieczeństwa – wniosek taki jest uzasadniony szczególnie w świetle wyników innego badania PwC „Badanie przestępczości gospodarczej Polska 2014", w którym 43% respondentów zadeklarowało brak wiedzy w zakresie strat i kosztów związanych z incydentami cyberbezpieczeństwa. Takie podejście ma niestety swoje konsekwencje – funkcja bezpieczeństwa jest często postrzegana przez polskie zarządy jako niepotrzebny kosztogenny narzut na organizację, a nie element budujący przewagę konkurencyjną firmy bądź ograniczający wymierne i reputacyjne straty.

Globalne firmy mają często możliwość ograniczenia strat w przypadku udanego cyberataku dzięki ubezpieczeniu od następstw incydentów cyberbezpieczeństwa. Skorzystanie z tej możliwości nie zwalnia jednak od zapewnienia należytego bezpieczeństwa informacji i systemów – przeciwnie, ograniczenie ryzyka jest koniecznym warunkiem wykupienia polisy.

W Polsce wiedza o istnieniu takich możliwości nie jest jeszcze powszechna – w naszej ankiecie tylko 3% respondentów zadeklarowało korzystanie z tej formy transferu ryzyka – a znalezienie firmy oferującej cyberubezpieczenia, działającej na lokalnym rynku nie jest proste.

Analiza rynku ubezpieczeń w Stanach Zjednoczonych i Europie Zachodniej (w szczególności Wielkiej Brytanii) wskazuje jednak, że jest to najszybciej rosnący segment wśród ubezpieczeń specjalizowanych, dlatego przewidujemy, że tego typu produkty będą wkrótce dostępne także na polskim rynku.

Małe spółki zgłosiły **spadek** kosztów incydentów o **37%** w porównaniu z poprzednim rokiem, a duże spółki zanotowały **53% wzrost** szkód finansowych. Średniej wielkości przedsiębiorstwa znajdują się gdzieś w połowie stawki, zgłaszając **wzrost** kosztów incydentów o **25%** w porównaniu z rokiem ubiegłym.

03

Pracownicy wskazywani jako najczęstsze źródło incydentów

Szpiedzy, hakerzy i zorganizowane grupy przestępcze – to czarne charaktery, na które wszyscy chętnie wskazują

Po raz kolejny obecni i byli pracownicy okazali się głównymi podejrzanymi o cyberprzestępstwa.
Co ciekawe, w polskim badaniu – w odróżnieniu od wyników globalnych – w tym roku respondenci rzadziej wskazywali pracowników i byłych pracowników jako źródła incydentów. Sądzimy, że jest to skutkiem rosnącego zrozumienia, że pracownicy w wielu przypadkach mogą nieświadomie powodować zagrożenie dla bezpieczeństwa danych, np. będąc ofiarami phishingu – stając się w ten sposób narzędziem w ręku rzeczywistych sprawców.

Polscy respondenci co prawdą rzadziej, ale wciąż w większości wskazują jako główne źródła incydentów pracowników, hakerów i byłych pracowników…
Co ciekawe, znacząca liczba respondentów przyznaje, ze nie jest w stanie zidentyfikować źródeł ataków. Jak widać pogląd, że źródłem wszelkiego zła są pracownicy, ma się nadal dobrze. Należy jednak zwrócić uwagę, że w dobie ataków hybrydowych na organizacje, pracownik zazwyczaj jest tylko medium dla przenoszenia złośliwego oprogramowania, obiektem ataku phishingowego, czy też innego wykorzystującego socjotechnikę.

Rozpatrując dane w tym kontekście należy zwrócić większą uwagę na kwestie podnoszenia świadomości pracowników, praktyki w zakresie bezpieczeństwa partnerów biznesowych oraz własną zdolność do wykrywania i reakcji na incydenty bezpieczeństwa. *W tych obszarach niestety podobnie, jak w roku poprzednim polskie firmy na tle globalnych wyników prezentują się słabiej.*

Ujawnione ataki na polski sektor energetyczny pokazują, że już nie tylko nasze firmy powinny się obawiać ataków oportunistycznych, ale także celowanych w konkretne branże. Warto zauważyć, że na świecie tylko 9% odpowiedzi wskazywało na to zagrożenie (wzrost o 2 punkty procentowe w stosunku do zeszłego roku).

Inne zagrożenie dotyczy tego, że firmy często same zajmują się naprawianiem skutków cyberprzestępczości pracowników. Okazuje się, że 75% respondentów w sondażu dotyczącym cyberprzestępczości w USA stwierdziło, że nie angażują organów ścigania i nie wnoszą oskarżeń w związku z przestępstwami popełnianymi przez osoby z wewnątrz firmy.[19] Takie podejście niesie ze sobą niestety poważne konsekwencje dla całego ekosystemu biznesowego– warto pamiętać, że brak naszej reakcji powoduje narażenie na ryzyko innych organizacji, być może będących w przyszłości naszymi partnerami z uprzywilejowanym dostępem do zasobów.

Jesteśmy przekonani, że jakość reakcji również polskich przedsiębiorstw na cyberprzestępstwa może i powinna ulec znacznej poprawie.

Właściwa reakcja obejmuje konieczność zaangażowania nie tylko ekspertów technicznych, ale również prawników, specjalistów PR i osoby doświadczone we współpracy z organami ścigania. Nasze dotychczasowe obserwacje wskazują, że wiele polskich firm nie posiada jeszcze opracowanych zawczasu procedur reakcji na cyberprzestępstwa i nie dysponuje własnymi bądź współpracującymi ekspertami w każdej z powyższych, kluczowych dziedzin. W sytuacji kryzysu wywołanego włamaniem do systemów, kiedy istotna jest zarówno trafność podejmowanych decyzji, jak i ich czas, takie nieprzygotowane firmy zwiększają ryzyko poniesienia niepowetowanych szkód reputacyjnych i utraty informacji istotnych do przeprowadzenia pełnego dochodzenia.

Z wewnątrz

50% 48%

Obecni pracownicy

25% 22%

Byli pracownicy

Brak danych 22%

Partnerzy biznesowi

15% 17%

Obecni dostawcy usług/konsultanci/wykonawcy

10% 9%

Klienci

5% 4%

Byli dostawcy usług/konsultanci/wykonawcy

Z zewnątrz

43% 39%

Nie wiem

25% 35%

Hakerzy

Brak danych 17%

Podmioty i organizacje zagraniczne

5% 9%

Aktywiści/organizacje aktywistów/aktywiści-hakerzy

10% 9%

Konkurenci

5% 4%

Terroryści

10% 4%

Przestępczość zorganizowana

3% 4%

Brokerzy informacji

Diagram 4
Osoby z wewnątrz a osoby z zewnątrz organizacji
Źródła incydentów dotyczących bezpieczeństwa, 2013–2014 (Polska)

Zagrożenie ze strony tych, którym ufamy narasta – i nie mówimy tu o pracownikach

Procent incydentów przypisywanych w polskim badaniu partnerom biznesowym i obecnym usługodawcom, konsultantom i wykonawcom wzrósł odpowiednio do 22% i 17% w 2014 roku. Jest to zgodne z trendem zaobserwowanym w wynikach globalnych.

To zagrożenie szczególnie wyraźnie pokazały liczne ataki na sklepy w USA w ubiegłym roku. Część ataków przeprowadzili przestępcy, którzy zdobyli dostęp do sieci i systemów sklepów detalicznych przez infiltrację ze strony obcych dostawców i wykonawców – w tym tak wydawałoby się nieprawdopodobnych, jak dostawcy systemów klimatyzacyjnych.

Firma Verizon określiła w swoim dorocznym raporcie „Data Breach Investigations Report" rok 2013 jako „rok naruszenia bezpieczeństwa handlu detalicznego", gdyż incydenty w tym obszarze miały miejsce w 467 miejscach na świecie. Verizon zauważył, że głównym celem ataków były dane z kart płatniczych, których dotyczyło 95% wszystkich incydentów w firmach handlu detalicznego.[20]

Wygląda na to, że rok 2014 będzie kolejnym złym rokiem dla tego sektora. W chwili sporządzania przez nas tego raportu ujawniono informację o kolejnym wycieku informacji ze sklepów w Stanach Zjednoczonych, który spowodował utratę 56 mln danych z kart płatniczych.[21]

W Polsce testy, które PwC przeprowadza u swoich klientów z wykorzystaniem autorskiej metodyki STRIKE, także pokazują, że przełamanie pierwszej linii obrony firm zajmuje niepokojąco mało czasu, a jeśli tylko atakujący znajdzie się w sieci wewnętrznej, organizacje są praktycznie bezbronne. Na kilkadziesiąt wykonanych do tej pory symulacji, wszystkie zakończyły się sukcesem (a raczej porażką zabezpieczeń), czyli uzyskaniem nieautoryzowanego dostępu do istotnych informacji biznesowych, a dodatkowo żadne z aktywności nie były zazwyczaj wykrywane.

Szybki wzrost spektakularnych przestępstw

Cyberprzestępstwa, które przyciągają najwięcej uwagi – infiltracja przez terrorystów, przestępczość zorganizowaną i konkurencję – są najrzadsze.

Nie jest to jednak pocieszające – wyniki naszego sondażu pokazują, że te zagrożenia rosną najszybciej.

„Polska przestała być anonimowym punktem na mapie celowanych ataków. Obserwujemy coraz większą aktywność hakerów i państw w obszarach infrastruktury krytycznej, także polskiej. Liczba ataków ze strony zorganizowanych grup przestępczych również wydaje się najwyższa w historii, a stopień ich zorganizowania i infrastruktury są bezprecedensowe."

Patryk Gęborys, menedżer w zespole PwC Cyber Security w Polsce

Państwa prowadzące agresywną politykę w cyberprzestrzeni często celują w głównych dostawców infrastruktury w celu kradzieży własności intelektualnej i tajemnic handlowych, co jest środkiem do uzyskania przewagi politycznej i gospodarczej. W związku z tym nie jest niespodzianką, że patrząc na wyniki globalne incydenty ze strony obcych państw są najczęstsze w takich sektorach jak sektor **ropy naftowej i gazu (11%), lotniczy i technologii kosmicznych, obronny (9%), technologiczny (9%),** a także **telekomunikacyjny (8%).**

Przyczyną tego wzrostu może być to, że spółki odkrywają, iż w związku z rozpowszechnieniem przechowywania informacji w formie cyfrowej coraz łatwiej, taniej i szybciej jest wykraść własność intelektualną i tajemnice handlowe, zamiast samemu opracowywać odpowiednie rozwiązania. Prowadząc podobne ataki, konkurenci często łączą zaawansowane techniki z innymi metodami, takimi jak rekrutacja pracowników spółki będącej przedmiotem ataku, przekupstwo, wymuszenie czy obietnica nowej pracy. Zwiększenie liczby cyberprzestępstw przypisywanych służbom państwowym i konkurentom jest skorelowane ze wzrostem kradzieży własności intelektualnej i innych rodzajów informacji wrażliwych.

W tym roku kradzież własności intelektualnej wzrosła o 19% w porównaniu z rokiem 2013. Prawie jedna czwarta (24%) respondentów zgłosiła kradzież „miękkiej" własności intelektualnej, która obejmuje informacje na temat procesów i wiedzy instytucjonalnej. Mniej (15%) twierdzi, że ukradziono im „twardą" własność intelektualną, taką jak strategiczne biznesplany, dokumenty z transakcji kapitałowych oraz wrażliwe dokumenty finansowe.

W tym roku 15% respondentów twierdziło, że źródłem incydentów jest przestępczość zorganizowana, w zeszłym roku było to 12%. W podziale na regiony liczba kradzieży spowodowanych przez przestępczość zorganizowaną była szczególnie wysoka w **Malezji (35%), Indiach (22%),** i **Brazylii (18%).**

Kradzież własności intelektualnej jest najwyższa wśród respondentów z branży lotniczej i technologii kosmicznych oraz obronnej – ich tajemnice handlowe mogą zawierać informacje krytyczne dla bezpieczeństwa narodowego danego kraju.

W tym roku respondenci z branży lotniczej i kosmonautycznej oraz obronnej zgłosili **97% wzrost** kradzieży twardej własności intelektualnej i **66% wzrost** kradzieży „miękkiej" własności intelektualnej – są to wzrosty o wiele wyższe niż w innych sektorach.

Służby specjalne: nowe źródło zagrożeń

Informacje ujawnione przez Edwarda J. Snowdena dotyczące inwigilacji ze strony rządów USA i Wielkiej Brytanii dodały do listy zagrożeń nowego gracza: krajowe służby wywiadowcze.

W wyniku przecieków Snowdena rośnie sceptycyzm przedsiębiorstw i całego społeczeństwa w związku z inwigilacją ze strony służb; rośnie też obawa o potencjalne skutki dla poufności zebranych danych i możliwości ich nieuprawnionego wykorzystania.

Rewelacje Snowdena, które trafiły na pierwsze strony gazet, spowodowały uświadomienie i znaczne obawy wśród członków kadry kierowniczej przedsiębiorstw. Nie tylko wywołują pytania o inwigilację ze strony rządów USA i Wielkiej Brytanii, ale również o spółki telekomunikacyjne i technologiczne, które musiały dać rządowi dostęp do danych oraz rządy innych państw, które przy tym współpracowały.

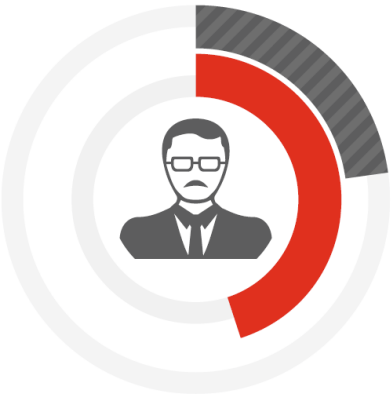
59% respondentów na całym świecie twierdzi, że członkowie ich zarządów martwią się inwigilacją ze strony rządu. Obawy są znacznie wyższe w **Chinach (93%), Indiach (83%)** i **Brazylii (77%).**

Te obawy wiążą się z potencjalnie rozległymi skutkami dla niektórych spółek telekomunikacyjnych i zaawansowanych technologii. Firmy, zwłaszcza ze Stanów Zjednoczonych, ale także z Europy, tradycyjnie dominowały na rynku telekomunikacji i sprzętu sieci komunikacyjnych dla przedsiębiorstw. Jednak perspektywy spółek azjatyckich są jaśniejsze od chwili odkrycia, że rząd amerykański zbierał wrażliwe informacje o niektórych krajowych firmach technologicznych i telekomunikacyjnych.

W rezultacie organizacje w niektórych krajach donoszą, że ponownie rozważą zaopatrzenie w sprzęt u producentów uznawanych dotychczas za zaufanych. Faktycznie, globalnie 42% respondentów twierdzi, że nabywanie produktów i usług z zaufanych krajów jest weryfikowane, a 29% twierdzi, że obecnie kupują mniej produktów i usług z tych krajów.

„Efekt Snowdena", który pomógł klientom zrozumieć koncepcję analizy dużych zbiorów danych (ang. Big Data analytics) wywołał również czujność wśród społeczeństw. Przecieki Snowdena i rozpowszechnienie Big Data spowodowały konieczność poddania pod debatę publiczną kwestii poufności danych osobowych. Unia Europejska zapowiedziała wzmocnienie wymagań i kontroli w tym obszarze, a duże zmiany są przewidywane najdalej w 2016 roku.

Kwestie, które najbardziej martwią zarządy? Poufność danych osobowych, potencjalne **ryzyko** prawne i **utrata** własności intelektualnej.



04

Wzrost liczby incydentów, spadek wydatków na bezpieczeństwo

Organizacje są zaniepokojone wzrostem cyberprzestępczości

Prawie połowa (48%) respondentów badania „Global Economic Crime Survey 2014" przeprowadzonego przez PwC stwierdziła, że świadomość ryzyka cyberprzestępczości w ich organizacji w ciągu ubiegłego roku wzrosła, w roku 2011 twierdziło tak 39%.[22]

W Polsce ostatnich dwóch lat cyber-przestępstw doświadczyło 19% organizacji w Polsce (wg tego samego badania), natomiast aż 35% organizacji wierzy, że stanie się ofiara cyber-ataków w najbliższej przyszłości. Jest to poziom zbliżony do wyników Badania z 2011 roku – zagrożenie w przyszłości ze strony cyber-przestępczości zadeklarowało 1/3 organizacji w Polsce.

Jednocześnie coroczne badanie przeprowadzone przez PwC wśród prezesów firm wykazało, że 48% światowych członków zarządów ma obawy związane z zagrożeniami cybernetycznymi dotyczącymi ich spółek, łącznie z utratą bezpieczeństwa informacji.[23]

Mimo zwiększonych obaw nasze badanie wykazało, że światowe budżety na zapewnienie bezpieczeństwa informacji w rzeczywistości spadły o 4% w porównaniu z 2013 rokiem. Wydatki na bezpieczeństwo przez ostatnie pięć lat nie przekroczyły 4% całego budżetu przeznaczonego na informatykę.

Co ciekawe, w tegorocznym badaniu w Polsce powiało w tym obszarze optymizmem – deklarowany budżet na bezpieczeństwo w stosunku do budżetu IT wyniósł średnio 5,5%, co zbliża polskie firmy do firm zagranicznych. Panuje przekonanie, że wydatki na bezpieczeństwo wzrosną w ciągu 12 miesiecy (43% respondentów) lub pozostaną na tym samym poziomie (28% badanych). Polscy respondenci nie przewidują odkładania zaplanowanych już inicjatyw.

Tendencja ta wydaje się być spowodowana przytoczonymi już spektakularnymi doniesieniami medialnymi z incydentów mających miejsce w naszym kraju, co spowodowało znaczący wzrost świadomości wśród decydentów. *Polscy szefowie bezpieczeństwa coraz lepiej negocjują budżet, przechodząc z pozycji FUD (fear-uncertainity-doubt – strach-niepewność-zwątpienie) do partnerskiej rozmowy z zarządami i biznesem o ryzyku prowadzenia biznesu.*

Daleko jednak jeszcze wszystkim polskim firmom do osiągnięcia wyników z prognozy Gartnera, przewidującej wzrost wydatków na bezpieczeństwo o prawie 17% na przestrzeni lat 2014-2015. Cieszy na razie, że przynajmniej liderzy w Polsce wzięli sobie do serca obecne zagrożenia dla informacji i systemów IT.

Patrząc na wyniki globalne, jedynym wyjaśnieniem ograniczenia wydatków na świecie, może być wielkość inwestycji odnotowanych w zeszłorocznym badaniu. W 2013 roku spółki globalnie zwiększyły w porównaniu do 2012 roku inwestycje informatyczne o 40%, a wydatki na bezpieczeństwo o 51%. Być może respondentom w tym roku trudno było utrzymać takie tempo wzrostu inwestycji. *W polskich firmach i urzędach z kolei mamy do czynienia w większości z wieloletnim niedoinwestowaniem – dlatego tegoroczny wzrost wydatków cieszy, ale nie doprowadzi w krótkim czasie do zniwelowania dystansu do najlepszych światowych praktyk.*

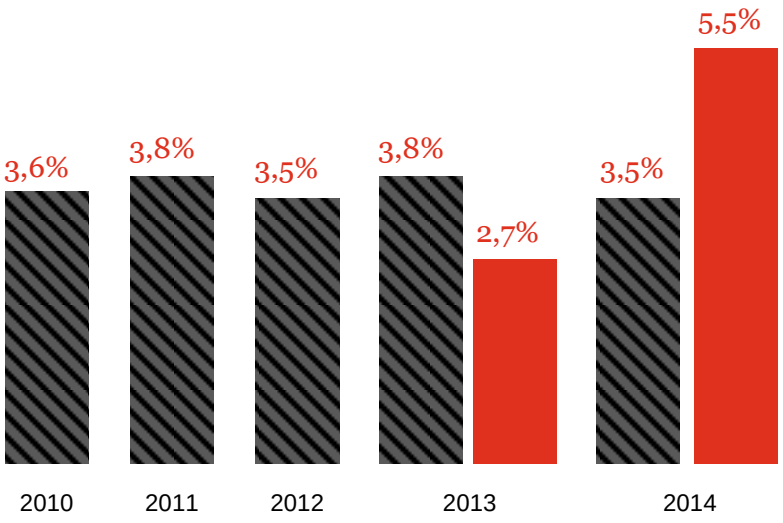


Diagram 5
Na świecie przeciętne budżety na zapewnienie bezpieczeństwa nieco spadły, co zmienia dotychczasowy trzyletni trend,
W Polsce – odwrotnie: zanotowano zwiększenie udziału bezpieczeństwa w budżecie IT

Na świecie najwyższe wzrosty w wydatkach na bezpieczeństwo wykazuje branża ochrony zdrowia i ubezpieczeń medycznych (66%), branża ropy naftowej i gazu (15%) oraz usług komunalnych (9%). Wzrost wydatków w ochronie zdrowia jest szczególnie widoczny, ale z pewnością uzasadniony, biorąc pod uwagę obecne ryzyko i utrzymujące się trendy. W tym roku branża ochrony zdrowia i ubezpieczeń medycznych wykazała 60% wzrost wykrytych incydentów, co doprowadziło do niesłychanego wzrostu strat finansowych o 282% w porównaniu z rokiem 2013.

Wyjaśnieniem tej lawiny incydentów i strat finansowych może być fakt, że hakerzy celują w służbę zdrowia i ubezpieczycieli z racji coraz wyższej wartości, jaką stanowią dane na temat zdrowia pacjentów. Ewidencja zdrowotna często zawiera pełne informacje – finansowe, medyczne, rodzinne i osobowe – które można wykorzystać do stworzenia pełnej tożsamości.

Pełen zestaw wykradzionych danych medycznych jest wart na czarnym rynku setki dolarów, osiąga nawet 1000 USD za każdą tożsamość, a same dane z ubezpieczenia zdrowotnego dają dochody rzędu 20 USD za sztukę. Dla porównania, skradzione karty płatnicze zazwyczaj sprzedawane są po 1 USD każda.[24]

Czarny rynek kradzionych danych rośnie zarówno pod względem rozmiarów, jak i stopnia skomplikowania

Choć nie wiadomo, ile jest witryn sprzedających dane, liczba przestępców uczestniczących w tym handlu prawdopodobnie wzrośnie, gdyż według RAND Corp42 coraz łatwiej jest uzyskać do niego dostęp. Częściowo dlatego, że dzisiejszy czarny rynek składa się z coraz większej liczby witryn, forów oraz kanałów czatowych, na których można nabywać i sprzedawać towary.

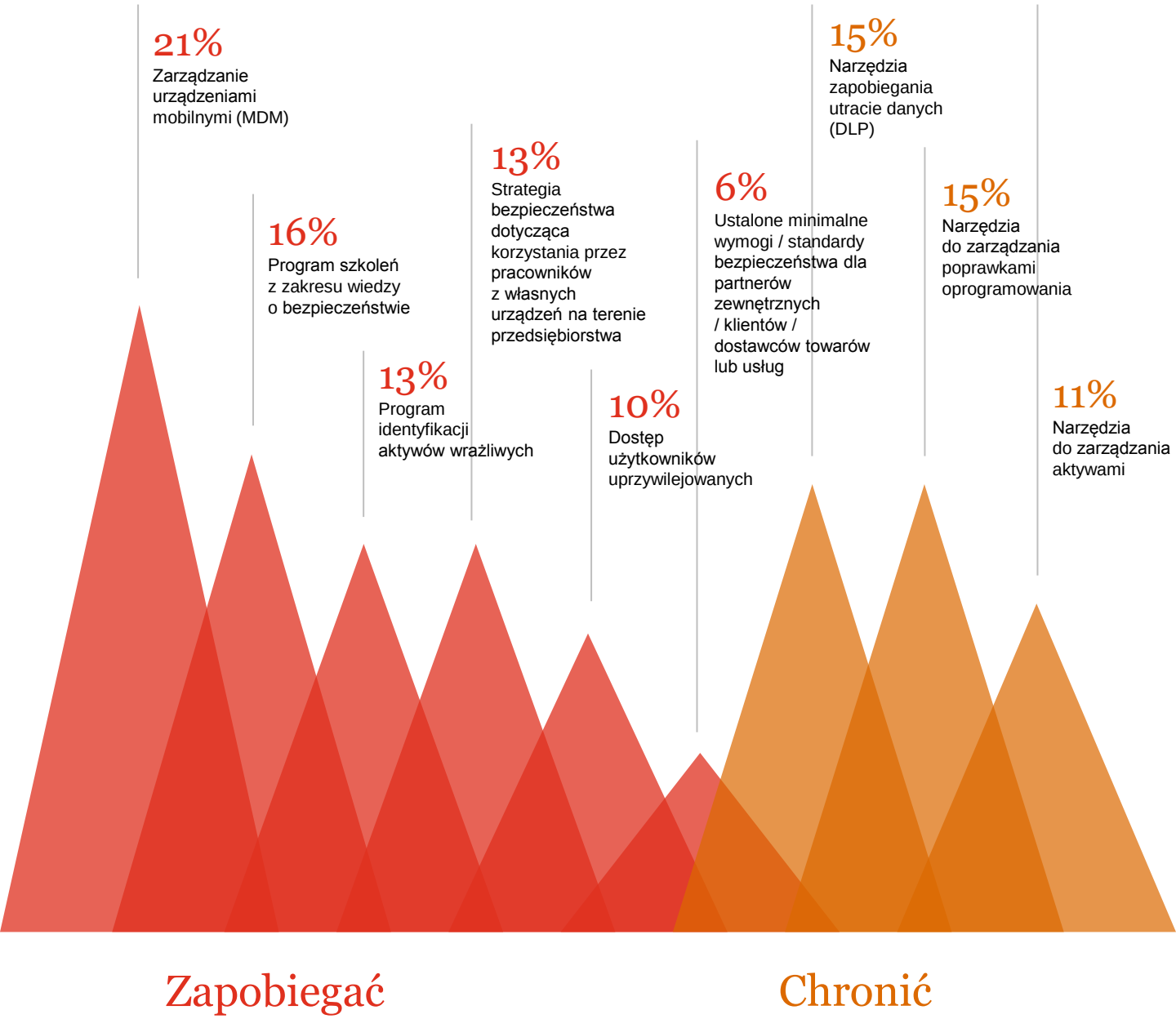
Branża ochrony zdrowia i ubezpieczeń medycznych musi zwiększać nakłady na inwestycje zapewniające bezpieczeństwo, przygotowując się na wprowadzenie połączonych sieciowo urządzeń do monitorowania stanu zdrowia i wzrostu ilości danych – tego, co niesie za sobą Internet Rzeczy (ang. Internet of Things). Dla branży ochrony zdrowia Internet Rzeczy już teraz nie jest futurystycznym wymysłem, a ryzyko z nim związane nie jest teoretyczne.

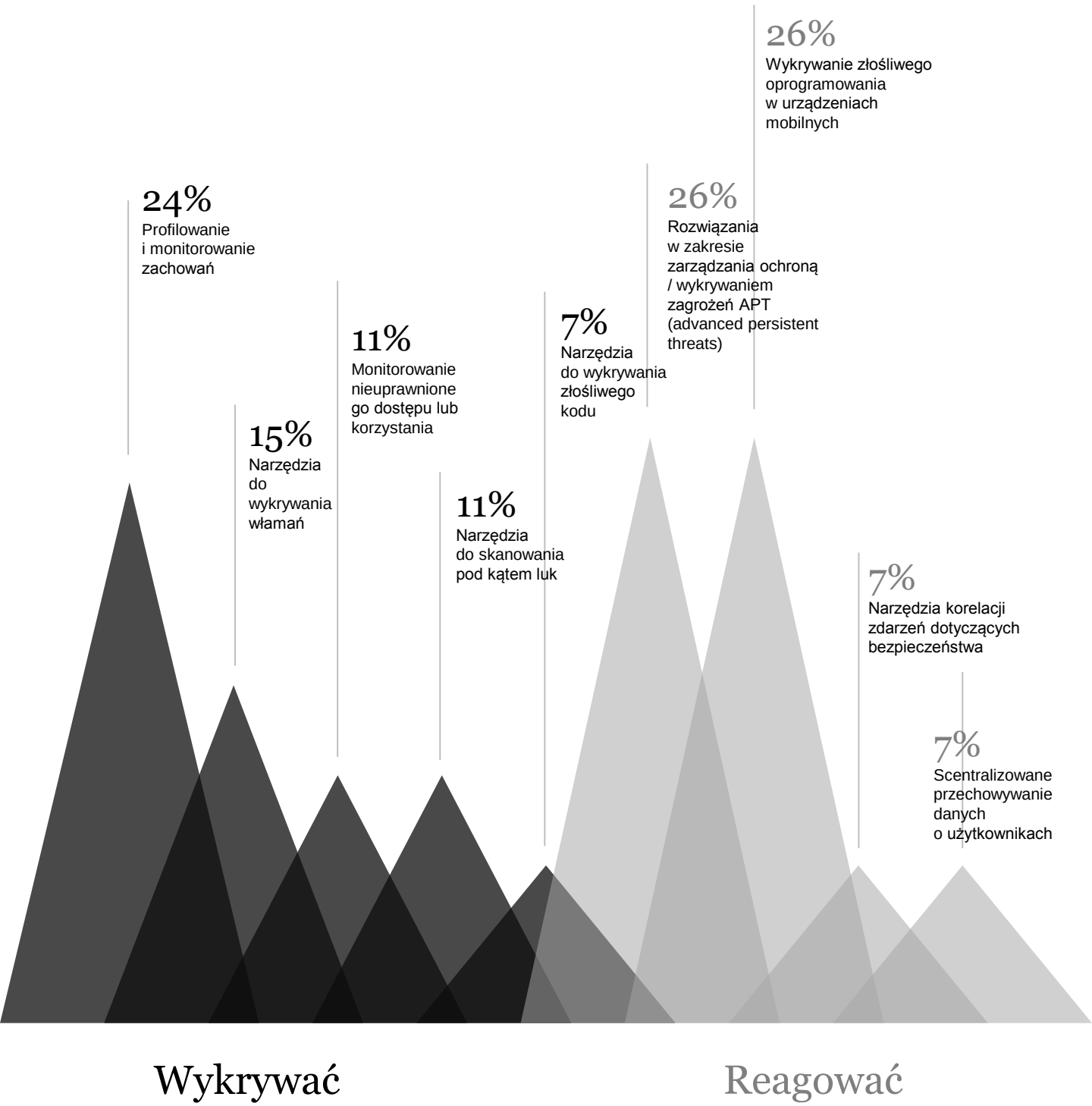
Należy zauważyć, że na świecie prawie połowa (47%) respondentów z branży ochrony zdrowia twierdzi, że wykorzystuje technologie konsumenckie, takie jak przenośne urządzenia do monitorowania stanu zdrowia, czy technologie operacyjne, np. zautomatyzowane systemy wydawania leków.

Jednak nie udało im się wystarczająco szybko zapewnić bezpieczeństwa urządzeń medycznych połączonych z Internetem.

Więcej niż **jedna trzecia (34%)** respondentów z branży ochrony zdrowia skontaktowała się z producentami urządzeń w celu zrozumienia możliwości ochrony i ryzyka związanego ze sprzętem, a 58% dokonało oceny ryzyka urządzeń lub technologii. Tylko 53% wprowadziło mechanizmy kontroli bezpieczeństwa połączonych z Internetem urządzeń.

Diagram 6
Priorytetowe wydatki w polskich firmach w ciągu kolejnych 12 miesięcy
Zapobiegać, chronić, wykrywać, reagować




24%
Profilowanie i monitorowanie zachowań
15%
Narzędzia do wykrywania włamań
11%
Monitorowanie nieuprawnione go dostępu lub korzystania
11%
Narzędzia do skanowania pod kątem luk
7%
Narzędzia do wykrywania złośliwego kodu
26%
Rozwiązania w zakresie zarządzania ochroną / wykrywaniem zagrożeń APT (advanced persistent threats)
26%
Wykrywanie złośliwego oprogramowania w urządzeniach mobilnych
7%
Narzędzia korelacji zdarzeń dotyczących bezpieczeństwa
7%
Scentralizowane przechowywanie danych o użytkownikach
Wykrywać
Reagować

05

Podstawowe praktyki w zakresie bezpieczeństwa informacji

Zabezpieczenia muszą nadążać za stale zmieniającymi się zagrożeniami i wymaganiami biznesu

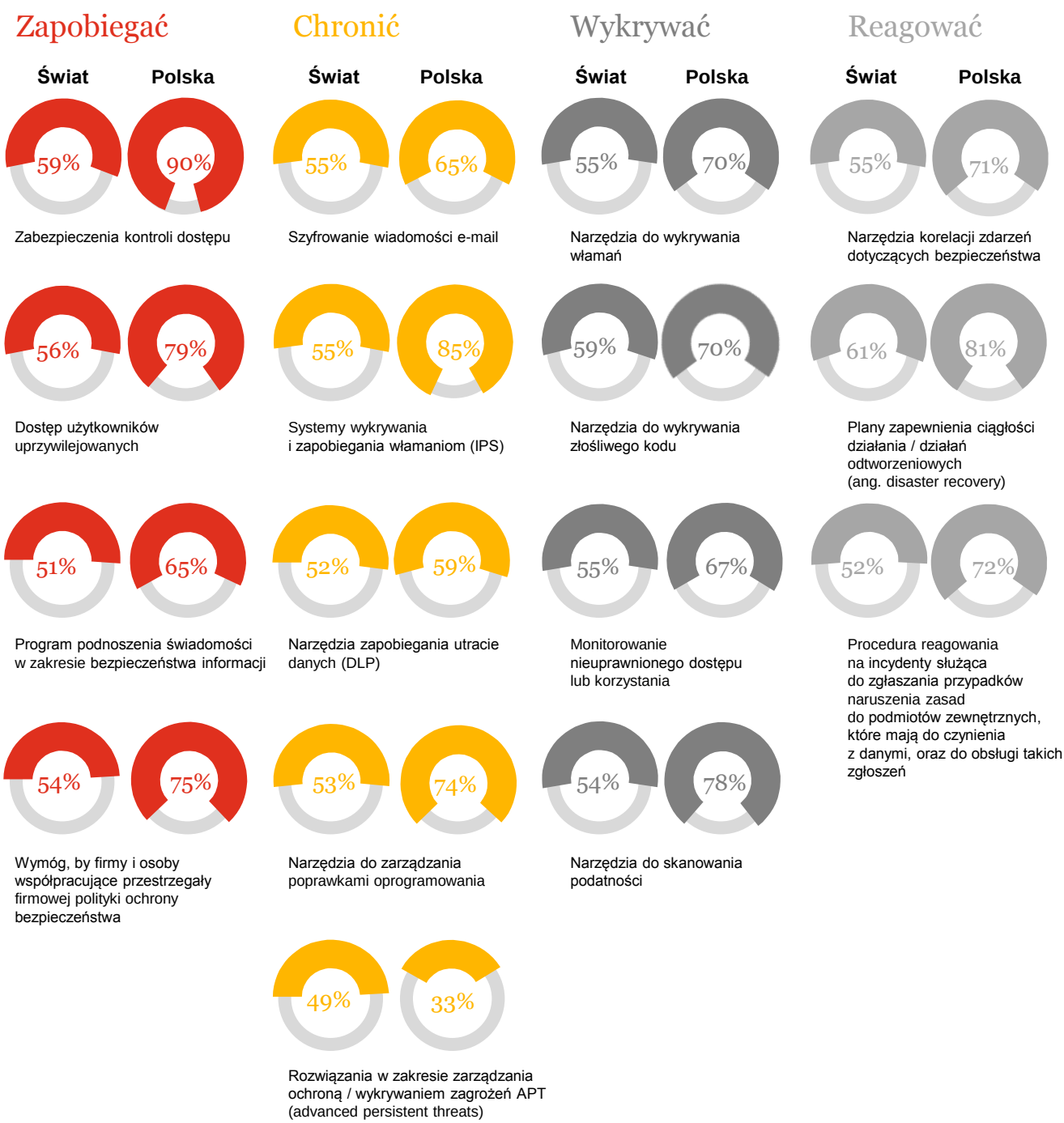
Aby to osiągnąć, należy skoncentrować się na właściwych procesach i technologiach dla zapobiegania, ochrony, wykrywania i reagowania na ryzyka w obszarze bezpieczeństwa informacji. Mówiąc wprost, niepokojąco wiele organizacji na świecie nie radzi sobie z tym wyzwaniem.

Biorąc pod uwagę dzisiejszy wzajemnie połączony ekosystem gospodarczy, w którym generuje się dane w postępie geometrycznym i dzieli się je z partnerami biznesowymi i dostawcami, szczególne obawy budzi brak polityki i właściwej staranności wobec stron trzecich. Niepokój budzą wyniki globalnego badania, które wskazują, że w ciągu ostatniego roku osłabł nacisk na bezpieczeństwo stron trzecich, mimo że wzrosła liczba incydentów przypisywanym tej kategorii użytkowników.

Nadzór nad usługodawcami i partnerami biznesowymi staje się jednym z kluczowych aspektów ochrony zasobów – słabo zabezpieczony dostawca mający zaufany dostęp do sieci wewnętrznej firmy może zniweczyć wszelkie wysiłki włożone w oddzielenie organizacji od zagrożeń zewnętrznych. W związku z tym należy zwrócić szczególną uwagę na następujące aspekty: dobra ochrona umowna, stały monitoring i kontrola, do jakich zasobów ma dostęp strona trzecia. Monitoring powinien obejmować zarówno własne systemy, jak i cykliczne audyty w lokalizacjach dostawcy.

Oceniając na podstawie tych kryteriów, stwierdzamy, że wielu respondentów nie stosuje tych zasad. Na przykład tylko 50% twierdzi, że ocenia ryzyko swoich dostawców (spadek z 53% w 2013 roku), a 50% potwierdza przeprowadzenie inwentaryzacji wszystkich stron trzecich, które mają styczność z danymi osobowymi pracowników i klientów. Nieco ponad połowa (54%) respondentów oświadczyła, że ma oficjalną politykę, która wymaga od stron trzecich przestrzegania ich zasad poufności, co stanowi spadek wobec 58% w 2013 roku.

Diagram 7:
Wiodące polskie firmy wyróżniają się pozytywnie na tle średniej globalnej
Zapobiegać, chronić, wykrywać, reagować



W tym roku aż **65%** respondentów z Polski stwierdziło, że mają program uświadamiania zagrożeń i organizowania odpowiednich szkoleń, co wygląda imponująco na tle globalnego poziomu 51%. Niemal tyle samo firm, bo **64%**, twierdzi, że wymaga od pracowników zakończenia szkolenia w zakresie zasad poufności.

Szkolenie i uświadamianie pracowników jest podstawowym elementem każdego programu, ponieważ ludzie są najczęściej najsłabszym ogniwem w łańcuchu bezpieczeństwa. Często łańcuch pęka, ponieważ przedsiębiorstwa zatrudniają niewłaściwych pracowników i nie uświadamiają ich za pomocą programów komunikacyjnych.

Skuteczne uświadamianie kwestii bezpieczeństwa wymaga również zaangażowania na wszystkich szczeblach – od góry do samego dołu – i sprawnej komunikacji, taktyki, która jest często niedoskonała. Tylko 49% respondentów twierdzi, że w ich firmie jest zespół międzydziałowy, który regularnie zbiera się, by omawiać, koordynować i komunikować się w sprawach dotyczących bezpieczeństwa informacji. Wymaga to również bezpośredniego zaangażowania dyrekcji i zarządu.

Na dyrekcji spoczywa odpowiedzialność za ochronę przed cyber-ryzykiem i za zapewnienie, że zarząd rozumie, jak organizacja będzie się bronić przed atakami w sieci i jak będzie na nie reagować.

Grad incydentów, jaki wystąpił w ostatnim czasie i minionym roku, wywołał liczne dyskusje na temat zaangażowania zarządu w sprawy bezpieczeństwa. Jednak mimo wielu rozmów widać, że przedsiębiorstwa nie doprowadziły dyskusji na temat bezpieczeństwa na szczebel zarządów.

06

Poprawa w niektórych obszarach

Mimo zmniejszenia działań związanych z ochroną są dziedziny, w których odnotowujemy wzrost bezpieczeństwa

Ryzyko cybernetyczne, technologie i narażenia na atak ewoluują z prędkością światła, tym samym silny program zapewnienia bezpieczeństwa cybernetycznego wymaga przede wszystkim dzielenia się przez podmioty prywatne i publiczne informacjami na temat cyber-ryzyka i szybkiego reagowania.

Na świecie coraz więcej podmiotów jest skłonnych do współpracy z innymi jednostkami dla poprawy bezpieczeństwa i wymiany informacji dotyczących zagrożeń. Gary Hayes, dyrektor działu informatyki z CenterPoint mówi, ze jego spółka aktywnie współdziała z kilkoma ośrodkami dzielenia się informacjami i prowadzenia analiz (Information Sharing and Analysis Centers – ISAC) i stowarzyszeniami branżowymi, a także z agendami rządowymi. Ta inicjatywa okazała się nieoceniona.

„Jeśli nie bierzesz udziału w konwersacjach, tracisz wątek. W obecnym otoczeniu czyhających zagrożeń nie ma powodów do unikania współpracy."

Gary Hayes, dyrektor działu informatyki z CenterPoint

Respondenci globalnego badania zaczynają doceniać znaczenie współdziałania.

W tym roku 55% respondentów twierdzi, że współpracuje z innymi w celu zapewnienia bezpieczeństwa; stanowi to wzrost o 12% w porównaniu z 2013 rokiem. Im większa spółka, tym bardziej prawdopodobne jest nawiązywanie współpracy z innymi: robi tak 66% dużych przedsiębiorstw w porównaniu z 49% małych firm. Współpraca jest częściej podejmowana w regionach, w których rozwój infrastruktury informatycznej w ciągu ostatniej dekady następował szybko. Na przykład respondenci z Ameryki Południowej i Dalekiego Wschodu chętniej nawiązują współpracę z innymi w celu zwiększenia zakresu informacji wywiadowczych dotyczących bezpieczeństwa.

Niestety w Polsce obserwujemy trend wręcz odwrotny. Tylko 48% odpowiedzi wskazywało, że organizacja oficjalnie współpracuje z innymi podmiotami w branży – jest to 7-proc. spadek w stosunku do 2013 roku. Wzrosła nieufność – aż połowa z grupy nie współpracującej w zakresie bezpieczeństwa wskazuje, że przyczyną jest brak zaufania do konkurentów – w zeszłym roku nikt nie wskazał takiej odpowiedzi. Brak zainteresowania współpracą wynika także z poglądu, że konkurencja nie jest bardziej zaawansowana od pozostałych (75% odpowiedzi w tej grupie). Trudno wytłumaczyć taki stan rzeczy, jednak należy się spodziewać, że zwiekszająca się liczba ataków spowoduje zmianę nastawienia polskich firm.

Smartfony i tablety stały się wszechobecne, mimo to spółki nie spieszyły się z wprowadzaniem zabezpieczeń mających przeciwdziałać zagrożeniom ze strony urządzeń przenośnych. W tym roku jednak zauważyliśmy zdecydowany postęp.
60% respondentów z Polski (54% globalnie) twierdzi, że wdrożyło strategię bezpieczeństwa dla urządzeń przenośnych. Z uwagi na ryzyko związane z mobilnością nadal nie jest to wiele, ale i tak więcej niż 44%, co było wynikiem za 2013 rok.

Zarządzanie urządzeniami przenośnymi (Mobile Device Management – MDM) i zarządzanie aplikacjami przenośnymi (Mobile Application Management – MAM) to rozwiązania niezbędne do zabezpieczenia floty urządzeń danej firmy.

W tym roku 59% respondentów z Polski twierdzi, że stosuje rozwiązania MDM/ MAM, co jest poprawą w stosunku do 48% w poprzednim roku. Wynik ten jednak można i należy jeszcze znacznie poprawić.

Nie dziwi fakt, że zaawansowanie w dziedzinie bezpieczeństwa urządzeń mobilnych jest wyższe w większych firmach, które generalnie mają bardziej rozwinięte systemy bezpieczeństwa. Z punktu widzenia sektorów gospodarki, największe postępy w tej dziedzinie odnotowały firmy z sektora finansowego, telekomunikacyjne i produktów przemysłowych.

Kolejną dziedziną, którą można poprawić, jest podejście do ubezpieczeń od następstw cyber-ataków

W Stanach Zjednoczonych wytyczne SEC OCIE sugerują, aby firmy z sektora usług finansowych zawierały umowy ubezpieczenia przed cyber-ryzykiem w ramach skutecznej strategii zarządzania nim.

W Polsce takie rozwiązanie także dopuszcza Komisja Nadzoru Finansowego w Rekomendacji D dot. zarządzania IT i bezpieczeństwem.

Z racji wyższego ryzyka dzisiejszego otoczenia i rosnących kosztów cyberprzestępczości uważamy, że ochrona przed stratami finansowymi spowodowanymi przez ryzyko w sieci powinna być traktowana równie poważnie jak inne rodzaje ubezpieczenia.

Jest to podejście, które wiele firm na świecie zdaje się doskonale rozumieć. Globalnie ponad połowa (51%) respondentów twierdzi, że nabyła ubezpieczenie zapewniające bezpieczeństwo w sieci, co stanowi wzrost w porównaniu z 45% w poprzednim roku. Być może ważniejsze jest odkrycie, że niektóre spółki wykorzystują ubezpieczenie w sieci jako sposób poprawy swoich programów bezpieczeństwa. Ponad jedna trzecia (36%) twierdzi, że podjęła kroki mające na celu poprawę sytuacji w zakresie bezpieczeństwa, aby obniżyć składkę ubezpieczeniową. Ubezpieczenie w sieci zapewne najchętniej będą kupować spółki lotnicze, przemysłu technologii kosmicznych, obronnego, samochodowego, rozrywki i mediów, a także firmy świadczące usługi finansowe.
Z niecierpliwością czekamy na ofertę ubezpieczycieli dla polskich przedsiębiorstw.

Pod względem zawartych umów ubezpieczenia informacji w sieci przoduje Ameryka Południowa, gdzie polisy wykupiło **58%** respondentów. W Stanach Zjednoczonych zainteresowanie tym ubezpieczeniem jest najmniejsze i wykupiło je **44%** respondentów. W Polsce jest to rozwiązanie rzadko spotykane w ofercie ubezpieczycieli i raczej niestosowane przez firmy. Należy się jednak spodziewać wprowadzenia takiej oferty w kolejnych latach.

Wydatki strategiczne na bezpieczeństwo wymagają od firm ustalenia i inwestowania w te rozwiązania bezpieczeństwa (technologie i procesy), które są najistotniejsze z punktu widzenia nowoczesnych zaawansowanych ataków. Ważne jest stworzenie i wdrożenie procesów, które w pełni integrują możliwości w zakresie przewidywania, zapobiegania, wykrywania i reagowania na incydenty w celu minimalizowania ich skutków.

Ważne jest również inwestowanie środków w kwalifikacje ludzi, co pozwala spółkom na szybkie reagowanie na incydenty i ograniczanie ich skutków.

Należy też zapewnić wystarczające fundusze na kompleksowe, stałe szkolenie pracowników i programy uświadamiania zagrożeń.

Spółki, które mają programy budowania świadomości w obszarze bezpieczeństwa, zgłaszają znacznie niższe straty finansowe z tytułu incydentów w sieci

Oszczędności mogą być znaczne: spółki, które nie przewidują szkoleń w dziedzinie bezpieczeństwa dla nowych pracowników, wykazały roczne straty finansowe czterokrotnie wyższe od tych, które mają takie szkolenia.

Skuteczne zabezpieczenia wymagają również wiedzy na temat obecnych i przyszłych wrogów, łącznie z motywami, zasobami i metodami ataku. Nie jest to możliwe bez budżetu na analizę i monitorowanie zagrożeń oraz poświęcenia czasu i środków na współpracę z innymi firmami, organami porządku publicznego i innymi podmiotami.

Obecnie, w obliczu zmieniających się ciągle zagrożeń, praktyki zapewniania bezpieczeństwa oparte na ryzyku powinny być podstawowym elementem ogólnego modelu zarządzania ryzykiem przez firmę.

Choć dobrze zaprojektowany program zarządzania ryzykiem bezpieczeństwa w sieci nie eliminuje ryzyka całkowicie, może ułatwić firmom przeciwdziałanie zagrożeniom dzięki procesowi pozyskiwania informacji i podejmowania decyzji, zwiększyć sprawność funkcji zapewniania bezpieczeństwa i zbudować bardziej odporną na zagrożenia organizację.

Naszym zdaniem w nadchodzących latach pojawią się coraz bardziej zaawansowane rozwiązania wspierające firmy w lepszym zarządzaniu ryzykiem i minimalizowaniu skutków zagrożeń bezpieczeństwa w sieci. Zmiany w technologii prawdopodobnie pomogą spółkom zmniejszyć złożoność procesów zarządzania bezpieczeństwem, szybciej wykrywać i reagować na incydenty oraz zwiększać możliwości monitorowania i analizowania zagrożeń. Do tego czasu organizacje – duże i małe – muszą zrozumieć, że zarządzanie ryzykiem cyberbezpieczeństwa jest kluczowe dla przetrwania w cyfrowym, połączonym świecie. I jest to jedno z głównych wyzwań dla prezesów, zarządów i rad nadzorczych i organów administracji państwowej.

07

Ewolucja: od zapewnienia bezpieczeństwa do zarządzania cyber-ryzykiem

Coraz większa liczba naruszeń bezpieczeństwa sprawia, że cyber-ryzyko nie zostanie całkowicie wyeliminowane.

Obecny ekosystem wzajemnych powiązań wymaga przejścia od bezpieczeństwa koncentrującego się na zapobieganiu do podejścia opartego na ryzyku, w którym priorytetem jest koncentracja na najbardziej wartościowych aktywach przedsiębiorstwa oraz największych dla nich zagrożeniach.

Krytyczną kwestią stało się szybkie wykrywanie przypadków przełamania zabezpieczeń lub nawet już samego faktu wypływu danych oraz błyskawiczne i skuteczne reakcje. Aby to osiągnąć, przedsiębiorstwa muszą przeorganizować swoje strategie bezpieczeństwa poprzez ściślejsze połączenie technologii, procesów i kwalifikacji pracowników z szerszymi działaniami w zakresie zarządzania ryzykiem.

„Firmy zazwyczaj nie mają środków, ani wiedzy, aby skutecznie wykryć i zareagować na incydenty. Nadal zbyt często bezpieczeństwo informacji jest traktowane jako problem w zasadzie techniczny i możliwy do rozwiązania przez zakup właściwego oprogramowania lub kolejnego „zunifikowanego" lub „nowej generacji" urządzenia. Bezpieczeństwo informacji dotyczy tymczasem współpracy ludzi, procesów i technologii – a sztuką jest skierowanie inwestycji we właściwe miejsca i dobranie właściwych proporcji pomiędzy prewencją, a detekcją zagrożeń i reakcją na nie."

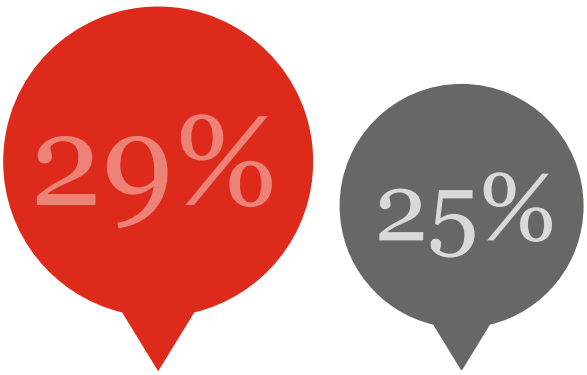
Rafał Jaczyński, lider zespołu PwC Cyber Security w Polsce i Europie Centralnej

Przedsiębiorstwa, które starają się zapewnić właściwe proporcje inwestycji ludzi, procesy i technologię, powinny zapoznać się ze schematem *NIST Cybersecurity Framework*. Choć schemat ten jest kierowany do dostawców infrastruktury krytycznej w Stanach Zjednoczonych, przedstawia skuteczny model bezpieczeństwa opartego na ryzyku dla spółek różnych branż na całym świecie.

Przyjęcie tych wytycznych może również zapewnić dodatkowe korzyści obejmujące lepszą współpracę i komunikowanie postawy sprzyjającej bezpieczeństwu wśród dyrekcji i przedsiębiorstw z branży oraz potencjalne zmniejszenie narażenia na sprawy sądowe w przyszłości, a nawet pomoc w przestrzeganiu przepisów.[25]

„Schemat NIST Framework to doskonały przykład współpracy sektora prywatnego i państwowego zapewniający doskonałe ramy dla bezpieczeństwa w sieci."

Sean Joyce, dyrektor PwC, uczestniczył w przygotowaniu regulacji umożliwiających wprowadzenie tych wytycznych



Firmy w USA już zaczynają wprowadzać zasady *NIST Framework*. Zauważyliśmy, że **29%** respondentów z Ameryki twierdzi, że przyjęło wytyczne, a kolejne **25%**, że ich przyjęcie jest dla nich priorytetem na przyszłość.

Wśród pierwszych kroków proponowanych przez NIST jest określenie i sklasyfikowanie najbardziej wartościowych aktywów informacyjnych oraz ustalenie, gdzie zlokalizowane są najbardziej wartościowe dane w ekosystemie i kto ma do nich dostęp.

Dla spółki górniczej Vale ten wstępny proces stworzył solidny fundament dla programu bezpieczeństwa informacji. Spółka zaczęła od ustalenia, które posiadane przez nią informacje są poufne i gdzie się je przechowuje. To pozwoliło zrozumieć stronę biznesową bezpieczeństwa informacji i sposób korzystania z nich przez pracowników. Pozwoliło także ustalić poszczególne szczeble ochrony i zrozumieć dziedziny, w których spółka może sobie pozwolić na większą pobłażliwość, oraz te, w których powinna postępować z całą stanowczością.

Jednak wielu respondentów badania takich kroków nie podjęło. Tylko 54% ma program pozwalający na ustalenie aktywów wrażliwych, a tylko 56% podjęło wysiłek inwentaryzacji zbierania, przekazywania i przechowywania wrażliwych danych dla pracowników i klientów.

W Polsce klasyfikację wartości biznesowej danych dokonuje tylko 36% badanych, ale już 60% przeprowadziło jakąś formę zarządzania aktywami.

Pod względem regionalnym respondenci z Ameryki Południowej i Dalekiego Wschodu chętniej przeznaczają wydatki na najbardziej wartościowe dane. Ważne jest też dostosowanie strategii bezpieczeństwa do konkretnych potrzeb biznesowych – to krok, z którego 40% respondentów na świecie rezygnuje. Wśród branż, które najprawdopodobniej połączą strategie bezpieczeństwa i biznesu, są: sektor produktów przemysłowych, usługodawcy i płatnicy z branży ochrony zdrowia oraz sektor usług finansowych. Pod względem geograficznym w tym podejściu przodują respondenci z dalekiego Wschodu i Ameryki Północnej.

Warto zauważyć, że w Polsce aż ponad 80% respondentów deklaruje, że polityka bezpieczeństwa spółki jest dobrze dostosowana do jej celów biznesowych.

Kolejnym podstawowym krokiem jest dostosowanie wydatków inwestycyjnych do aktywów strategicznych firmy. Jednak globalnie **34%** respondentów nie kieruje wydatków na bezpieczeństwo do najbardziej zyskownych pionów działalności.

Metodyka

Ankieta Globalny Stan Bezpieczeństwa Informacji 2015 jest światowym przedsięwzięciem PwC, CIO Magazine i CSO Magazine. Została ona przeprowadzona poprzez badanie on-line w dniach od 27 marca 2014 do 25 maja 2014 roku.

Czytelnicy magazynów CIO i CSO oraz klienci PwC zostali zaproszeni poprzez wiadomości elektroniczne do wzięcia udziału w ankiecie. Światowe wyniki omawiane w niniejszym raporcie opierają się na odpowiedziach od ponad 9700 respondentów, wśród których znaleźli się prezesi, członkowie zarządów firm i organizacji, dyrektorzy i osoby odpowiedzialne za finanse, informatykę, bezpieczeństwo, czy też prywatność ze 154 krajów. 35% respondentów pochodziło z regionu Ameryki Północnej, 34% z Europy, 14% z Dalekiego Wschodu, 13% z Ameryki Południowej i 4% z Bliskiego Wschodu i Afryki. Margines błędu wynosi mniej niż 1 %.

W tym raporcie, dane z globalnego badania zostały porównane z wynikami z ankiety polskiej – na zaproszenie skierowane do klientów PwC Polska odpowiedziało dodatkowo 77 firm i organizacji działających w Polsce. Ze względu na ograniczoną liczbę odpowiedzi, obserwacje wynikające z polskiej części mają charakter jakościowy. Głównie reprezentowane wśród polskich respondentów branże to sektor finansowy (bankowość i ubezpieczenia), telekomunikacyjny, wytwarzania oprogramowania oraz usług doradczych.

Podziękowania

Polska edycja raportu „Global State of Information Security 2015" powstała dzięki zaangażowaniu i pomocy następujących osób:

Część merytoryczna:

- *Piotr Urban*
- *Rafał Jaczyński*
- *Patryk Gęborys*
- *Edyta Ziajowska*
- *Mateusz Nalewajski*
- *Marcin Kowalczyk*
- *Wojciech Kubiak*

Projekt graficzny:

- *Aneta Zielińska*
- *Marta Olkowicz-Abaied*

Przypisy

Cyber-ryzyka: groźne i rzeczywiste

1. http://www.cbsnews.com/news/data-breach-costs-take-toll-on-target-profit/
2. Cnet.com, U.S. charges 8 in $45M global cybercrime scheme, 9 maja 2013
3. JP Morgan źródło: http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003
4. IOSCO and the World Federation of Exchanges Office, Cyber-crime, securities markets and systemic risk, lipiec 2013
5. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat
6. HP Fortify on Demand, Internet of Things State of the Union Study, lipiec 2014
7. IOActive, Adventures in Automotive Networks and Control Units, sierpień 2013
8. Department of Homeland Security, ICS-CERT Monitor, January-April 2014, maj 2014
9. Financial Times, Energy companies hit by cyber attack from Russia-linked group, 30 czerwca 2014
10. CHS: http://www.foxnews.com/tech/2014/08/18/community-health-systems-hacked-records-nearly-45-million-patients-stolen
11. Vormetric Data Security, Security measures to go under spotlight as new Data Protection Directive approaches, 8 lipca 2014
12. Google Online Security Blog, Announcing Project Zero, 15 lipca 2014

Liczba incydentów i ich skutki finansowe nadal rosną

13. Trustwave Holdings, 2014 Trustwave Global Security Report, maj 2014
14. Center for Strategic and international Studies, Net Losses: Estimating the Global Cost of Cybercrime, czerwiec 2014
15. Bank Światowy, World Development Indicators Database, lipiec 2014; obliczenia PwC
16. Create.org i PwC, Economic Impact of Trade Secret Theft, luty 2014
17. World Economic Form, Global Risks 2014, Ninth Edition, grudzień 2013
18. PwC, Economic Crime: A threat to business globally, luty 2014

Pracownicy wskazywani jako najczęstsze źródło incydentów

19. US State of Cybercrime Survey, współsponsorowane przez magazyn CSO, Dział CERT Software Engineering Institute w Carnegie Mellon University, PwC, i US Secret Service, marzec–kwiecień 2014
20. Verizon, 2014 Data Breach Investigations Report, kwiecień 2014
21. The Financial Times, Home Depot attack bigger than Target's, 19 września 2014

Wzrost liczby incydentów, spadek wydatków na bezpieczeństwo

22. PwC, Economic Crime: A threat to business globally, luty 2014
23. PwC, Fit for the future: Capitalizing on global trends, kwiecień 2014
24. Dell SecureWorks, Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents, for over $1,000 Per Dossier, 15 lipca 2013

Ewolucja: od zapewnienia bezpieczeństwa do zarządzania cyber-ryzykiem

25. PwC, Why you should adopt the NIST Cybersecurity Framework, maj 2014

Nasi eksperci są do Państwa dyspozycji, zarówno w kwestiach dotyczących tego raportu, jak i wszelkich pytań związanych z bezpieczeństwem informacji i systemów teleinformatycznych.

Osoby kontaktowe – PwC Cyber Security

Piotr Urban
Partner
Lider PwC Risk Assurance
K: +48 502 184 157
E: piotr.urban@pl.pwc.com

Rafał Jaczyński
Lider PwC Cyber Security
K: +48 519 507 122
E: rafal.jaczynski@pl.pwc.com

Patryk Gęborys
K: +48 519 506 760
E: patryk.geborys@pl.pwc.com

Rafał Skoczylas
K: +48 519 506 661
E: rafal.skoczylas@pl.pwc.com

www.pwc.pl/bezpieczenstwo-biznesu