Cyberbezpieczeństwo – wyzwanie współczesnego prezesa

Marzec 2016

KPMG.pl

Prezesi firm na całym świecie stąpają po cienkiej linie

Członek zarządu pewnej spółki naftowo-gazowej kliknął wiadomość e-mail ze zdjęciem swojej córki strzelającej bramkę w czasie niedawno rozegranego meczu. Dwa lata później ten sam członek zarządu dowiedział się, że w zdjęciu wbudowane było złośliwe oprogramowanie, które pozwoliło atakującemu odtworzyć każde naciśnięcie klawisza komputera na jego biurku, w tym każdy wysłany przez niego e-mail. Cyberszpiedzy okresowo wykonywali zrzuty ekranu, a ponadto uruchamiali kamerę i mikrofon w kontrolowanym komputerze, dzięki czemu mogli podglądać i podsłuchiwać, co dzieje się w gabinecie zarządu. Firma startowała w wielu zamkniętych przetargach na prawa do wydobycia ropy naftowej, ale jakoś zawsze z ceną trafiała tuż powyżej zwycięskiej oferty.

Pewien producent inteligentnych rozwiązań domowych reklamował wspaniałą nową funkcjonalność dla klientów: sterowanie termostatem, światłami i systemem zabezpieczeń domu za pomocą smartfona! Jednak technologia ta okazała się na tyle „wygodna dla użytkowników", że grupa lokalnych złodziei złamała zabezpieczenia systemu i zorganizowała serię włamań. Prosta zmiana ustawień bezpieczeństwa rozwiązania oraz poprawne logowania i monitoring mogła zapobiec włamaniom.

Pewna sieć detaliczna przekonała się na własnej skórze, co się dzieje, kiedy międzynarodowa sieć hakerów po cichu wysysa dane o każdej płatności kartą kredytową i debetową realizowaną w sklepach tej sieci przez wiele miesięcy. Najwyższe kierownictwo i zarząd dowiedziały się o tym naruszeniu od śledczych, a wiadomość została opublikowana zanim firma miała szansę wyeliminować to naruszenie czy poradzić sobie z jego skutkami. Sprzedaż drastycznie spadła, został złożony pozew zbiorowy, a prezes złożył rezygnację.

We wszystkich tych przypadkach mogły pomóc lepsze działania zapobiegawcze, jednak sama prewencja nie okazałaby się wystarczająca. Wbudowywanie lepszych zabezpieczeń w produkty i procesy biznesowe jest wprawdzie istotne, jednak równie ważne jest zrozumienie kto nas atakuje i stworzenie planu radzenia sobie z zagrożeniami tuż po ich wykryciu.

Technologia umożliwia firmom kontaktowanie się z klientami w sposób, którego nikt nie mógł sobie wyobrazić jeszcze dekadę temu – inteligentne urządzenia, zindywidualizowany marketing i produkty, a także zautomatyzowane usługi. Wszystko to usprawniło funkcjonowanie zaplecza firm, a także umożliwiło im zaoferowanie klientom bardziej bezpośrednich i spersonalizowanych usług. Obecnie możemy zrealizować większość transakcji bankowych za pośrednictwem komputera, który mieści się w kieszeni.

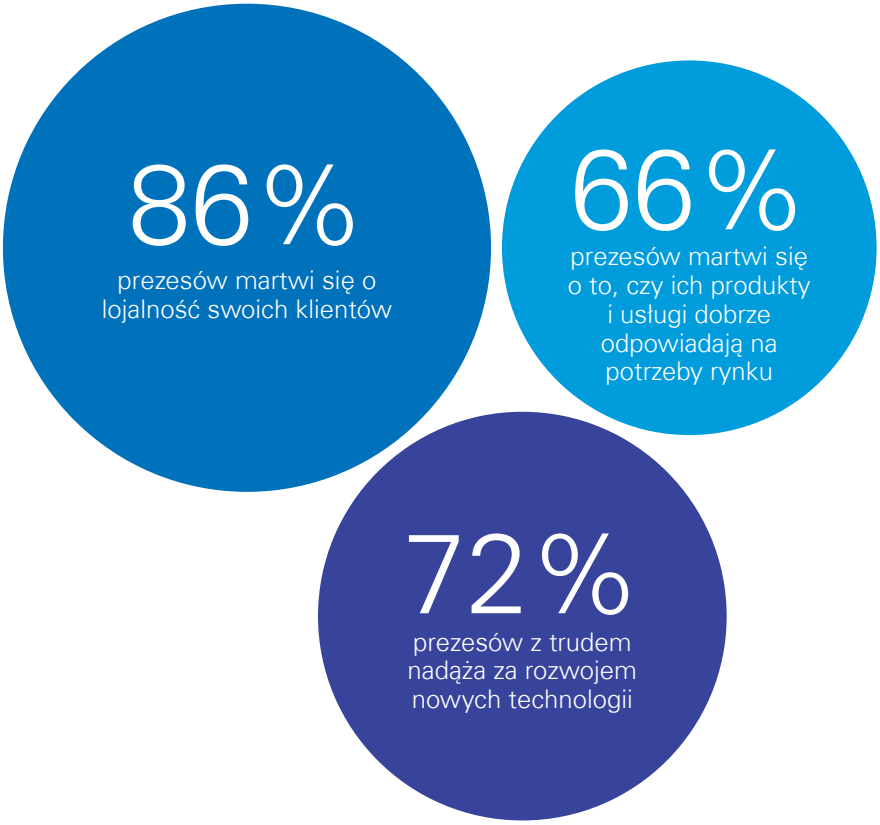
Prawie zawsze jednak innowacje wyprzedzają bezpieczeństwo. A przecież cyberprzestępcy również są innowacyjni. Jednym z najbardziej innowacyjnych rynków na świecie jest dark net, czyli sieć, która obsługuje zarówno przestępczość zorganizowaną, jak i pojedynczych domorosłych hakerów. Każdego dnia pojawiają się tam i są udostępniane nowe narzędzia, nowe usługi do realizowania ataków i nowe strategie spieniężenia ich skutków. Wszystko ulega ciągłej zmianie: słabe punkty, rodzaje ryzyka i konsekwencje ataków.

Co spędza prezesom sen z powiek

Myślenie o bezpieczeństwie danych nie jest już w większości organizacji aspektem bycia „mądrym po szkodzie", bez względu na to, czy chodzi o dane klientów, numery IP czy bardziej prozaiczne dane niezbędne do prowadzenia działalności firmy. KPMG International niedawno przeprowadziło badanie wśród ponad 1200 menedżerów wyższego stopnia z wielu największych firm o najbardziej złożonej strukturze na świecie. Badanie to wykazało, co spędza im sen z powiek. Dwie trzecie z nich jest zaniepokojonych tym, czy ich produkty i usługi właściwie odpowiadają na potrzeby rynku, trzy czwarte z trudem nadąża za nowymi technologiami, a prawie wszyscy martwią się o lojalność swoich klientów[1]. Cyberbezpieczeństwo jest ściśle związane z lojalnością klientów, ich zaufaniem, a także z innowacyjnością. Naruszenie bezpieczeństwa może poważnie osłabić zaufanie konsumentów i zniszczyć reputację marki.

A przecież wbudowanie funkcjonalności związanych z cyberbezpieczeństwem w produkty i procesy może stać się przewagą konkurencyjną – stwierdza Malcolm Marshall, Globalny Dyrektor ds. Cyberbezpieczeństwa w KPMG. *Niektóre organizacje przekształcają problem związany z bezpieczeństwem w funkcjonalność produktu, stosując np. identyfikację dotykową (ang. touch ID)* – wyjaśnia Marshall. Przykładowo, banki zaczynają zastępować niedoskonałe procedury uwierzytelniania identyfikacją dotykową. *Jeśli ktoś jest w stanie uwierzytelnić pracowników i klientów z bardzo wysokim poziomem pewności, oznacza to, że jest też w stanie zapewnić znacznie bardziej zindywidualizowany poziom usług.*

[1] Patrz: metodologia badania opisana na końcu niniejszego raportu.



Źródło: Raport 2015 KPMG CEO Outlook, maj 2015

Każda firma jest cyberfirmą

Jednym z największych błędów, jakie może popełnić organizacja, jest uznanie cyberbezpieczeństwa za sprawę, która jest wyłącznie domeną dyrektora ds. informatycznych (CIO). *Dyrektor ds. informatycznych pełni bardzo ważną rolę, jednak choć coraz więcej firm wykorzystuje media cyfrowe jako sposób dotarcia do klienta, nie zawsze konsultują się one z ekspertami do spraw bezpieczeństwa cyberprzestrzeni* – zwraca uwagę Malcolm Marshall. *Wielu członków najwyższej kadry kierowniczej nie wie, jaki poziom technologiczny reprezentują produkty oferowane przez ich firmy. Podobnie też niewiele osób z najwyższego kierownictwa firm ma za sobą refleksję nad tym, że cyberprzestępcy mogą wykorzystać ich produkty czy usługi w bardzo twórczy i przebiegły sposób.* Cyberprzestępczość nie jest rozumiana równie dobrze jak wiedza o przestępczości konwencjonalnej.

W ostatecznym rachunku chodzi o integralność produktu i reputację, a są to sprawy będące przedmiotem troski zarządów. Przykładowo inwestorzy instytucjonalni są mniej skłonni zainwestować w firmę, która doznała poważnego naruszenia cyberbezpieczeństwa, które przedostało się do wiadomości publicznej. Fakt ten może mieć wpływ na cenę akcji, jak również na zdolność firm do pozyskiwania kapitału.

> “Wspólnie wędrujemy po omacku i dochodzimy do sytuacji, w której stoimy na przegranej pozycji nie wbudowując w nasze produkty elementów bezpieczeństwa od początku ich tworzenia.”
>
> – Malcolm Marshall, *Global Head of Cyber Security at KPMG*

Wniosek: Cyberbezpieczeństwo to sprawa, która dotyczy obecnie każdej firmy, a więc każda firma musi zwracać baczną uwagę na kwestie bezpieczeństwa.

Cyberbezpieczeństwo – ryzyko strategiczne

Członkowie najwyższego kierownictwa i zarządów tradycyjnie uznawali cyberbezpieczeństwo za problem taktyczny, a nie zagadnienie strategiczne. Jednak w ciągu ostatnich dziesięciu lat pojawiła się już świadomość, że cyberbezpieczeństwo może być źródłem ryzyka w skali całego przedsiębiorstwa.

W omawianym tu badaniu prawie jedna trzecia prezesów wymieniła cyberbezpieczeństwo jako problem, który ma obecnie największy wpływ na sytuację ich firm. Jeden na pięciu wskazał, że bezpieczeństwo informacji to ryzyko, które budzi ich największe obawy. Wśród najistotniejszych typów zagrożeń wymieniono ryzyko operacyjne i ryzyko związane z przestrzeganiem przepisów i regulacji. Należy jednak pamiętać, że cyberryzyko – jeśli nie ma nad nim kontroli – bardzo szybko staje się problemem zarówno operacyjnym, jak i regulacyjnym.

Źródło: Raport 2015 KPMG CEO Outlook, maj 2015

W przypadku ataków, które przedostały się do wiadomości publicznej, powstaje problem – firma nie może skupić się na swojej podstawowej działalności operacyjnej, ponieważ musi zajmować się zaistniałym incydentem – zauważa Greg Bell, Cyber Security Leader w KPMG w USA. *Inna sytuacja powstaje wtedy, kiedy firma musi wstrzymać część swojej działalności operacyjnej, ponieważ próbuje naprawić lub wyeliminować problem z cyberbezpieczeństwem, a wtedy pojawia się szereg skomplikowanych skutków prawnych i procesy sądowe* – dodaje Greg Bell.

Opracowanie ram działania w kontekście cyberryzyka

Ryzyko utraty reputacji, a także ryzyko regulacyjne i prawne to problem wszystkich firm. W przypadku organizacji posiadających fizyczną infrastrukturę zagrożenia są wielokrotnie większe. Atak może naruszyć mechanizmy kontrolne, zniszczyć posiadany sprzęt, sparaliżować działalność i stworzyć zagrożenie dla płynności finansowej. Dokonywane w ostatnich latach ataki na państwowe spółki naftowo-gazowe stały się sygnałem alarmowym dla wszystkich organizacji sektora energetycznego i przemysłowego. Bez linii kredytowych i gwarancji rządowych wiele z tych spółek napotkałoby problemy z płynnością finansową w ciągu dosłownie kilku dni, gdyby doszło do podobnych ataków.

Wiele organizacji już posiada system oceny ryzyka dla swoich przedsiębiorstw, ale wciąż jednak cyberryzyko jest traktowane inaczej niż pozostałe zagrożenia, co jest błędem – wyjaśnia Marshall.

Przykładem może być tzw. ryzyko strony trzeciej (*third party risk*). Wiele organizacji, zwłaszcza banków, od dawna uwzględnia tego typu ryzyko. Niektóre banki przestawiły się na współpracę z wieloma dostawcami – jeśli więc jeden z dostawców zawiedzie, będą odporne na taką sytuację. Po głębszym zastanowieniu można jednak dostrzec, że rozproszone ryzyko może zostać skoncentrowane w kolejnym kroku, gdyby na przykład wszyscy zdywersyfikowani dostawcy byli uzależnieni od jednego poddostawcy. Jest to zjawisko znane jako „ryzyko strony czwartej". Takie odkrycia bywają powszechne przy ocenie ryzyka płynności, ale ocena ryzyka może przynieść podobne wnioski w przypadku oceny odporności na cyberzagrożenia. Można się na przykład zastanowić, co by się stało, gdyby wszyscy dostawcy opierali się na współpracy z tym samym poddostawcą usług w chmurze obliczeniowej?

Każda organizacja powinna mieć system analizy cyberbezpieczeństwa, a system ten – w idealnej sytuacji – powinien być zintegrowany z innymi systemami oceny ryzyka istniejącymi w przedsiębiorstwie – zwraca uwagę Marshall. Istnieje kilka takich systemów, z których mogą korzystać organizacje: The Framework for Improving Critical Infrastructure Cybersecurity (System poprawy cyberbezpieczeństwa infrastruktury krytycznej) opublikowane przez NIST w Stanach Zjednoczonych, Cyber Essentials w Wielkiej Brytanii czy międzynarodowa norma ISO27001, która jest najpowszechniej stosowanym systemem na całym świecie. *Sam wybór systemu oceny bezpieczeństwa jest znacznie mniej istotny niż to, jak zostanie on zintegrowany i wdrożony* – zwraca uwagę Marshall. *Chodzi przede wszystkim o to, aby system ten stał się elementem głównego nurtu zarządzania ryzykiem w organizacji.*

Zrozumieć swojego wroga

W pierwszej kolejności należy zastanowić się, kto mógłby zaatakować nasze przedsiębiorstwo, w co by uderzył i dlaczego miałby to zrobić. Mówiąc w skrócie, należy zrozumieć swojego wroga. (Patrz ramka nt. wywiadu w sferze bezpieczeństwa, strona 9). Posiadany system oceny może również pomóc organizacjom zdać sobie sprawę, które składniki majątku najbardziej potrzebują ochrony, a które mogłyby spowodować największe szkody, gdyby zostały naruszone. *Dzięki takiej refleksji można skoncentrować inwestycje i ochronę na sferach, które miałyby najpoważniejsze skutki dla organizacji* – radzi Marshall.

Przykładowo w przypadku większości firm technologicznych „klejnotem w koronie" jest własność intelektualna. Co się jednak stanie, kiedy globalna spółka projektuje swoje produkty w jednym kraju, opracowuje oprogramowanie w innym, a części konstrukcji sprzętu w trzecim, przy czym dostawcy są rozproszeni po całym świecie?

Zarząd jednej z takich spółek zidentyfikował własność intelektualną jako potencjalne zagrożenie dla kontynuowania działalności. Stwierdził on, że gdyby ktoś uzyskał do niej dostęp, poznałby plany spółki w zakresie wprowadzania nowych wersji produktu i był w stanie je skopiować, mogłoby to zagrozić istnieniu firmy.

Słabym punktem firmy okazał się zakład, w którym produkowano najbardziej dochodowy produkt spółki w największych ilościach. Tak zwany „etyczny haker" (white-hat hacker) wynajęty przez konsultanta tej firmy w ciągu zaledwie około 30 sekund uzyskał dostęp do wszystkich systemów działających w hali produkcyjnej. Z punktu widzenia cyberbezpieczeństwa, haker ten posiadał pełną kontrolę nad wszystkim, łącznie z własnością intelektualną. Co więcej, umiarkowanie utalentowany haker mógłby przejąć kontrolę nad każdym serwerem, od programów zapewniania jakości aż do procesu produkcyjnego. Dyrektor ds. informatycznych (CIO) nie był zaskoczony tym odkryciem. Starał się wcześniej uświadamiać to zagrożenie zespołom odpowiedzialnym za produkcję, ale ich członkowie obawiali się, że kontrole bezpieczeństwa mogłyby utrudniać działalność operacyjną.

Oprócz możliwości kradzieży własności intelektualnej, zidentyfikowane luki świadczą o tym iż program zapewniania jakości dla najbardziej dochodowego produktu tej firmy nie był wystarczający i spójny. W przypadku pozwu zbiorowego firma, która straciła kontrolę nad systemem zapewnienia jakości, miałaby poważne trudności, żeby znaleźć coś na swoją obronę.

Kolejne, często niedoceniane ryzyko wiąże się z fuzjami i przejęciami. Niektóre organizacje uczą się na własnych błędach, że przejęcie firmy, która nie ma wbudowanych zabezpieczeń w swoich produktach, może okazać się kosztowne. W jednym z ostatnich takich przypadków okazało się, że koszty naprawy luk w cyberzabezpieczeniach sięgnęły 25% ceny zakupu. Proces due diligence przeprowadzony przez firmę przejmującą nie wykrył tej luki, ponieważ firma kupująca nie miała świadomości, jak niezwykle istotne jest cyberbezpieczeństwo w przypadku produktu przeznaczonego do stosowania w pojazdach.

Czy jesteście gotowi?

Połowa ankietowanych prezesów odpowiedziała, że ich firmy są w pełni przygotowane na incydenty związane z cyberbezpieczeństwem, które mogą się zdarzyć w przyszłości. Badanie wykazało jednak, że tylko połowa prezesów mianowała dyrektora ds. cyberbezpieczeństwa lub specjalny zespół zajmujący się tą tematyką, a mniej niż połowa dokonała zmian w procesach wewnętrznych, takich jak procedury udostępniania danych.

Jeszcze bardziej zaskakujące było to, że tylko jedna trzecia organizacji dokonała zmian w procesach zewnętrznych, takich jak procedury udostępniania danych na zewnątrz czy przetwarzanie transakcji. Cyberprzestępcy potrafią obejść solidniejsze zabezpieczenia w dużych organizacjach dzięki przeniknięciu do pomniejszych dostawców czy usługodawców za pomocą złośliwego oprogramowania. W takiej sytuacji złośliwy program może zostać dołączony się do faktury lub dostarczanych podzespołów.

W ostatnich latach część najbardziej spektakularnych i nagłośnionych zagrożeń powstała za sprawą dostawców zewnętrznych. Biorąc pod uwagę rosnącą złożoność zarządzania łańcuchem dostaw oraz tendencję do posiadania coraz większej liczby wzajemnie podłączonych urządzeń i procesów, cyberbezpieczeństwo zaczyna dotyczyć całego łańcucha dostaw, a także łańcucha dostaw naszych dostawców i sprzedawców. Sytuacja taka stwarza również okazję, aby przekształcić kwestię cyberbezpieczeństwa w przewagę konkurencyjną. Solidny i udokumentowany protokół zabezpieczeń może być argumentem sprzedażowym dla każdej firmy, która łączy się z klientami przez otwartą sieć, jak pokazuje przykład w ostatnim podrozdziale.

Badanie wykazało jednak, że w przypadku kilku scenariuszy respondenci albo nie planują, albo opóźnili proces planowania w zakresie ważnych środków bezpieczeństwa.

Plany powołania dyrektora/zespołu ds. cyberbezpieczeństwa

Podjęto kroki zapobiegawcze	50%
Planuje się podjęcie kroków w ciągu najbliższych 3 lat	29%
Nie planuje się działań	21%

Plany dokonania zmian w procesach wewnętrznych (udostępnianie danych, korzystanie z urządzeń)

Podjęto kroki zapobiegawcze	45%
Planuje się podjęcie kroków w ciągu najbliższych 3 lat	44%
Nie planuje się działań	11%

Plany modernizacji obecnej technologii

Zaktualizowano tylko posiadaną technologię/ podjęto kroki zapobiegawcze	37%
Planuje się podjęcie kroków w ciągu najbliższych 3 lat	49%
Nie planuje się działań	14%

Plany zmiany procesów zewnętrznych (zbieranie danych, przetwarzanie transakcji, udostępnianie danych)

Podjęto kroki zapobiegawcze	34%
Planuje się podjęcie kroków w ciągu najbliższych 3 lat	53%
Nie planuje się działań	13%

Źródło: Raport 2015 KPMG CEO Outlook, maj 2015

Znaczące inwestycje w USA

Istnieją poważne różnice danych dotyczących gotowości na cyberataki w zależności od położenia geograficznego. Poziom przygotowania zależy od tego, gdzie znajduje się firma. W Stanach Zjednoczonych 87% prezesów stwierdziło, że ich firmy są w pełni przygotowane na cyberatak. Zasady obowiązkowego ujawniania naruszonych danych konsumenckich, szereg szeroko nagłośnionych naruszeń oraz aktywne działania rządu na rzecz cyberbezpieczeństwa przyczyniły się do podniesienia świadomości zagrożeń, który jest teraz na znacznie wyższym poziomie w USA w porównaniu do innych regionów świata. Stany Zjednoczone są ulubionym celem cyberprzestępców, a w Ameryce Północnej ataki tego typu są zwykle bardziej nagłaśniane w mediach.

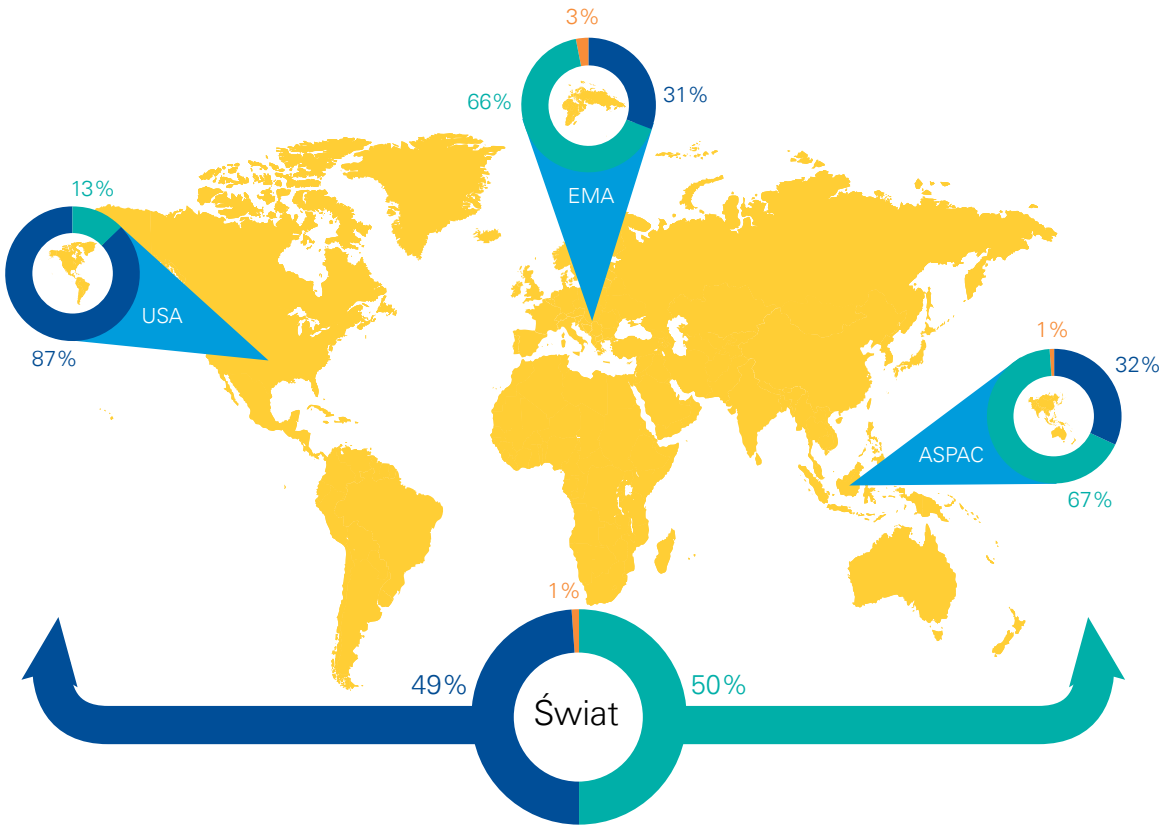
W konsekwencji wiele organizacji dokonało dużych inwestycji w środki służące zapobieganiu atakom – stwierdza Greg Bell. *Do niedawna zbyt wiele uwagi poświęcano zagadnieniom zapobiegania, a zbyt mało sprawom ochrony i reagowania". Obecnie prezesi zaczynają pytać: „Jak możemy szybciej wykryć, że doszło do cyberincydentu i jak możemy skuteczniej reagować?* – mówi Bell. Taki poziom gotowości odróżnia organizacje, które szybko dochodzą do siebie po incydencie od tych, które ponoszą ich skutki przez długi czas.

> „Zasadnicza przyczyna leży często w braku wyobraźni – nieumiejętności wyobrażenia sobie, jak zaawansowani i wytrwali potrafią być hakerzy atakujący daną firmę."
>
> – Malcolm Marshall, *Global Head of Cyber Security at KPMG*

Ostrożność w Europie

W Europie mniej niż jedna trzecia prezesów potwierdza gotowość na cyberincydenty. Wiele organizacji europejskich znajduje się w stanie przejściowym. *Rewelacje Snowdena dały wielu europejskim prezesom materiał do przemyśleń i zmiany cyberstrategii oraz środków bezpieczeństwa* – mówi Uwe Bernd-Striebeck, Cyber Security Leader w KPMG w Niemczech. *Obserwujemy, że bardzo wiele firm europejskich przechodzi na współpracę z krajowymi dostawcami rozwiązań w zakresie bezpieczeństwa i zastępuje amerykańskie narzędzia i aplikacje europejskimi lub planuje to zrobić w najbliższej przyszłości.*

Wiele firm w regionie znajduje się jeszcze na początku lub w trakcie swojej drogi do cyberbezpieczeństwa – mówi Bernd-Striebeck. Poszukują one skutecznych i opłacalnych rozwiązań w zakresie bezpieczeństwa, które zapewniłyby im najlepszą ochronę i umożliwiły odpowiednie reagowanie w przypadku cyberincydentów. *Nawet jeśli firmy europejskie zainwestowały w bezpieczeństwo, ich prezesi rzadziej deklarują, że ich firmy są w pełni przygotowane w zakresie cyberbezpieczeństwa, ponieważ są zwykle bardziej ostrożni niż prezesi firm w USA* – stwierdza Bernd-Striebeck.



Źródło: Raport 2015 KPMG CEO Outlook, maj 2015

Azja – reagowanie na istniejące zagrożenia

W regionie Azji i Pacyfiku te cechy, które spowodowały przyśpieszenie działań w zakresie bezpieczeństwa w USA, nie są ani tak silnie widoczne, ani tak bardzo zaawansowane – zauważa Dani Michaux, Cyber Security Leader w KPMG w Azji. Tylko 32% prezesów stwierdziło, że ich organizacje są w pełni przygotowane na cyberzagrożenia. Władze publiczne zaczynają przyglądać się tym zagadnieniom i aktywniej działają na poziomie poszczególnych krajów, dokonywana jest rewizja przepisów o ochronie prywatności, a przedsiębiorstwa podejmują działania w odpowiedzi na rosnące zagrożenia.

W przypadku organizacji z siedzibą w regionie Azji i Pacyfiku mamy do czynienia z wieloma poziomami zaawansowania i doceniania znaczenia cyberryzyka – niektóre dopiero zaczynają dostrzegać i zrozumieć cyberzagrożenia, a inne są w pełni zaangażowane, a ich zarządy i prezesi mają wysoką świadomość roli cyberbezpieczeństwa dla ochrony i rozwoju działalności biznesowej.

Przyjęty przez Pekin cel polegający na wyeliminowaniu amerykańskich technologii i wprowadzeniu w Chinach surowych przepisów dotyczących produktów i usług związanych z bezpieczeństwem miał niezwykle silny wpływ na ten największy azjatycki rynek cyberbezpieczeństwa.

Wiele australijskich prezesów i członków zarządu rozumie znaczenie cyberbezpieczeństwa, jednak często świadomość ta nie sięga jeszcze poziomu, który skłaniałby ich do podejmowania działań – wyjaśnia Gordon Archibald, Cyber Security Leader w KPMG w Australii. Częściowo wynika to z braku widoczności i orientacji w tym, co należałoby zrobić. *Problem ten spada na kadrę zarządzającą, która czasem nie potrafi jasno określić problemu – Co będziemy chronić? Jakie zagrożenia nas dotyczą? Na ile dobrze chronione są nasze składniki majątkowe?* – wyjaśnia Gordon Archibald. Kadry zarządzające są świadome zagrożeń, ale nie zawsze dostrzegają ich potencjalny wpływ na działalność biznesową czy nowe technologie.

Osoby, które dla nas pracują, są równie ważne jak nasza własna wiedza

Wszystkie te kwestie razem wzięte tworzą ogromny popyt na utalentowanych pracowników, a nasilające się niedobory umiejętności mogą się jeszcze pogorszyć w nadchodzących latach. W omawianym tu badaniu prezesi przyznający, że nie są przygotowani na cyberincydenty w przyszłości, częściej są skłonni do zwiększania zatrudnienia w ciągu najbliższych trzech lat, a połowa z nich spodziewa się, że w tym samym okresie pojawi się niedobór umiejętności po stronie pracowników.

Jednym z największych wyzwań jest ogromna skala niedoboru umiejętności. Według globalnych szacunków ponad 23% stanowisk związanych z zapewnianiem cyberbezpieczeństwa nie może być obsadzonych przez ponad sześć miesięcy, a po tym okresie nadal 10% pozostaje nieobsadzonych. Amerykańskie Biuro Statystyki Rynku Pracy (US Bureau of Labor Statistics) szacuje, że w USA niemal 300 tysięcy miejsc pracy w sektorze cyberbezpieczeństwa pozostaje nieobsadzonych (stan na sierpień 2015 r.). Niedobory personelu i umiejętności są najbardziej dotkliwe w przypadku specjalistów ds. cyberbezpieczeństwa, którzy łączyliby w sobie wiedzę techniczną z umiejętnościami w zakresie szerzej rozumianego biznesu, zarządzania, zagrożeń lub nauk społecznych.

Zdaniem Marshalla znalezienie utalentowanych informatyków jest wyzwaniem w przypadku większości organizacji – jest to szczególne wyzwanie w przypadku każdego projektu, w ramach którego rozwiązania technologiczne stają się elementem tzw. doświadczenia klienta (customer experience). *Każdy rozumie, że na zapleczu potrzebni są świetni specjaliści ds. bezpieczeństwa. Jednak aby projektować nowe produkty, osadzać w nich nowe technologie i śmiało wprowadzać je na nowe rynki, niezbędni są świetni specjaliści ds. bezpieczeństwa, którzy będą odgrywać rolę „frontmenów" współpracujących z projektantami i marketingowcami. Niezbędni są utalentowani pracownicy, dzięki którym doświadczenie klienta w kontakcie z produktem lub usługą będzie przyjemnością, a nie złym snem ze względu na brak odpowiednich zabezpieczeń* – konkluduje Marshall.

Cyberdyrektor z wyczuciem biznesowym

Powstaje również pytanie, kto ponosi ostateczną odpowiedzialność za cyberbezpieczeństwo w organizacji. W badaniu KPMG czterech na dziesięciu prezesów stwierdziło, że w nadchodzących latach zwiększy się rola dyrektora ds. informatycznych (CIO), jednak wielu z tych dyrektorów ani nie należy do ścisłego kręgu kierownictwa, ani nie cieszy się poważaniem jako partnerzy do rozmów o biznesie. Istnieje również niebezpieczeństwo, że jeśli dyrektor ds. informatycznych jest jedynym członkiem najwyższego kierownictwa odpowiadającym za kwestie bezpieczeństwa, to reszta organizacji przekaże odpowiedzialność działowi informatycznemu, nie dbając o to, aby kwestie bezpieczeństwa były wplecione w zachowania i procesy w całej organizacji.

Bezpieczeństwo musi być kwestią o szerszym zasięgu – zauważa Marshall. *Rekomendujemy, aby jednej osobie na poziomie zarządu oraz jednemu z głównych dyrektorów, niepełniącemu funkcji dyrektora ds. bezpieczeństwa, powierzyć ogólne zadanie dbania o to, aby kwestie cyberbezpieczeństwa były zintegrowane z procesami biznesowymi – zarówno w kontekście unikania ryzyka, jak i poszukiwania szans biznesowych.*

Takie podejście będzie również dla wszystkich ważnym sygnałem, że bezpieczeństwo to nie tylko sprawa informatyków.

W wielu dobrze zarządzanych firmach istnieje stanowisko dyrektora ds. bezpieczeństwa informacji (Chief Information Security Officer). Obecnie osoby na tym stanowisku podlegają zwykle dyrektorowi ds. informatycznych. Sytuacja ta zaczyna się jednak zmieniać, ponieważ przedsiębiorstwa w coraz większym stopniu rozumieją, że cyberbezpieczeństwo jest powiązane z ryzykiem biznesowym, które ma wpływ na funkcjonowanie całego przedsiębiorstwa. Istnieją już przypadki, że osoby na stanowisku CISO podlegają innym dyrektorom z najwyższego szczebla, np. dyrektorowi operacyjnemu, dyrektorowi finansowemu, głównemu radcy prawnemu, a w paru przypadkach nawet bezpośrednio prezesowi firmy. Każda firma, która rozumie cyberzagrożenia wiążące się z fuzjami i przejęciami czy projektowaniem produktów, będzie również skłonna uznać, że odpowiedzialność powinny przejąć wszystkie osoby z najwyższego szczebla zarządzania.

Oczywiście struktura podległości służbowej to tylko jeden element profilu bezpieczeństwa w firmie. Bardzo wiele zależy od osób, które pełnią te role. *Niezwykle ważne jest, aby mieć tu eksperta merytorycznego* – zauważa Marshall. *Jeśli w firmie jest silny lider – czyli ktoś, kto potrafi inspirować i prowadzić utalentowanych ekspertów merytorycznych – w fotelu dyrektora ds. bezpieczeństwa informacji nie musi zasiadać specjalista w zakresie bezpieczeństwa.*

40%
respondentów twierdzi, że w ciągu najbliższych 3 lat w ich organizacji zwiększy się rola dyrektora ds. informatycznych

Źródło: Raport 2015 KPMG CEO Outlook, maj 2015

Osoba na stanowisku CISO powinna potrafić rozmawiać merytorycznie z przedstawicielami najwyższego szczebla zarządzania oraz członkami zarządu – zauważa Bell. Zbyt często zdarza się, że taka osoba próbuje wyjaśniać niuanse zagrożeń technicznych, podczas gdy biznesowo nastawieni dyrektorzy odbierają to jako „inżynierskie gadanie". *Jeśli w naszej organizacji jest lider, który potrafi rozmawiać o ryzyku biznesowym wynikającym z cyberzagrożeń, to taka rozmowa jest znacznie skuteczniejsza* – konkluduje Bell.

Odpowiednie narzędzia

Organizacje muszą zainwestować w odpowiednie narzędzia, jak również we właściwych ludzi. Przede wszystkim muszą zapewnić sobie widoczność, żeby wiedzieć, czy są atakowane. Bez widoczności niemożliwe jest wykrycie dziur w arsenale bezpieczeństwa ani słabości w infrastrukturze. Istnieją organizacje, które zostały zaatakowane dawno temu, a wykryły straty dopiero po latach.

Jednym ze sposobów na poszerzenie wiedzy jest zastosowanie narzędzi gromadzenia danych wywiadowczych na potrzeby bezpieczeństwa (security intelligence) do wykrywania problemów, wskazywania anomalii i nietypowej lub podejrzanej aktywności. Narzędzia takie mogą wspomóc firmy na dwa sposoby. Po pierwsze, „usługa wczesnego ostrzegania" może zmniejszyć tzw. okno zagrożenia, czyli czas, jaki upływa od wykrycia ataku do poradzenia sobie z nim. Narzędzia te mogą także dać szerszy obraz globalnych zagrożeń niż informacje, które mogłaby zebrać pojedyncza firma na własną rękę. Bezpieczeństwo jest swego rodzaju ekosystemem – organizacje muszą wiedzieć, co się dzieje zarówno na zewnątrz, jak i wewnątrz.

Udostępnianie informacji o zagrożeniach

Organizacje mogą poszerzyć posiadaną przez siebie wiedzę dokonując wymiany informacji o własnych zagrożeniach w zakresie bezpieczeństwa z podobnymi podmiotami i konkurencją. Mimo iż w teorii pomysł ten wydaje się rozsądny, to dzielenie się informacjami z konkurencją nie jest krokiem, który wiele organizacji jest gotowych podjąć – przynajmniej na razie. Większość organizacji niechętnie ujawnia swoje słabe strony, a wiele z nich nigdy publicznie nie ujawnia naruszeń, chyba że zostają do tego zmuszone z mocy prawa. Instytucje finansowe są tu wyjątkiem, ponieważ infrastruktura finansowa jest na tyle wzajemnie powiązana, że takie instytucje są bardziej skłonne do współpracy. Skłonność ta opiera się na założeniu, że w razie ataku albo wszystkie przetrwają, albo wszystkie pójdą na dno. Z drugiej jednak strony w wielu innych branżach nie wykształciła się jeszcze kultura dzielenia się informacjami.

Innym sposobem na radzenie sobie z zagrożeniem jest tworzenie sieci współpracy – na przykład poprzez wspólne finansowanie „etycznych hakerów". Są to tacy hakerzy komputerowi, którzy wykorzystują swoje umiejętności w dobrych, a nie złych celach, pomagając organizacjom w wykrywaniu słabych miejsc w architekturze systemów. Dyrektorzy zatrudniający takich hakerów są często zaskoczeni, jak szybko haker potrafi przeniknąć do systemów firmy – często w ciągu zaledwie kilku minut.

Nie istnieje coś takiego jak zapewnienie całkowitego bezpieczeństwa. Organizacje muszą traktować kwestie cyberbezpieczeństwa proaktywnie i wyprzedzająco, a nie opierać się zbyt mocno na technologiach o charakterze reaktywnym, jak np. firewalle czy systemy zapobiegania włamaniom. Jednym ze sposobów na zapobieganie cyberatakom jest nieustanne badanie słabych punktów we własnych systemach. Inną metodą jest zapoznanie się z krajobrazem zagrożeń i poznanie swojego wroga za pomocą środków wywiadowczych. Należy starać się wykryć to, czego nie da się uniknąć. A jeśli nie możemy czegoś wykryć, powinniśmy być gotowi na szybkie reagowanie.

Cztery złote zasady cyberbezpieczeństwa

Zadbaj o podstawy

W ponad 75% przypadkach ataków wykorzystuje się nieumiejętność zadbania o podstawowe mechanizmy kontroli

Dbaj o najważniejsze aktywa firmy

W przypadku wydatków na własną obronę trzeba ustalić priorytety, a więc warto zbudować twierdzę wokół najważniejszych aktywów.

Prześwietl swoich wrogów

Należy zainwestować w pozyskanie wiedzy o tym, kto mógłby nas zaatakować, dlaczego i w jaki sposób – pozwoli to przewidzieć najbardziej prawdopodobne scenariusze i bronić tych aktywów, które są najbardziej narażone na ataki.

Potraktuj cyberzagrożenia jako szansę bacznego przyjrzenia się swojej firmie

Kwestie bezpieczeństwa i odporności na ataki mogą mieć wpływ na niemal każdy element funkcjonowania organizacji. Strategie bezpieczeństwa informatycznego i budowania odporności biznesu na ataki powinny być uspójnione z szerszymi celami organizacji – począwszy od ochrony własności intelektualnej poprzez maksymalizację wydajności aż do poszukiwania nowych sposobów na wywołanie entuzjazmu klientów.

Najbardziej innowacyjne firmy zrozumiały już, że kwestie dotyczące cyberbezpieczeństwa są nie tylko zagrożeniem, którym należy się zająć, lecz stanowią także szansę podjęcia działań w zakresie tzw. doświadczeń klienta (customer experience) oraz generowania przychodów. Firmy te poszukują sposobów, dzięki którym gotowość na cyberataki stanie się przewagą konkurencyjną, a nie po prostu kosztem. Wbudowują one elementy bezpieczeństwa w swoje nowe produkty i usługi jeszcze na etapie tworzenia ich koncepcji i zdają sobie sprawę, że cyberbezpieczeństwo nie jest problemem informatycznym – musi ono zostać uwzględnione w całej organizacji oraz jej ekosystemie.

Metodologia

Dane z badania opublikowane w niniejszym raporcie są oparte na badaniu ankietowym przeprowadzonym wśród 1276 prezesów firm z Australii, Chin, Francji, Niemiec, Indii, Włoch, Japonii, Hiszpanii, Wielkiej Brytanii i USA. Respondenci reprezentowali dziewięć kluczowych branż: motoryzacja, bankowość, ubezpieczenia, zarządzanie inwestycjami, opieka zdrowotna, technologia, handel detaliczny/ rynki konsumenckie oraz energetyka/usługi komunalne. Łącznie 347 prezesów pochodziło z firm osiągających przychody od 500 mln do 999 mln USD, 626 z firm osiągających przychody 1–9,9 mld USD, a 303 osób reprezentowało firmy, których przychody wynosiły minimum 10 mld USD. Badanie zostało przeprowadzone w okresie od 22 kwietnia do 26 maja 2015 r.

Współautorzy:

Malcolm Marshall
Global Cyber Security Leader

Greg Bell
Cyber Security Leader in the USA

Dani Michaux
Cyber Security Leader in the AsPaC region

Uwe Bernd-Striebeck
Cyber Security Leader in Germany

Gordon Archibald
Cyber Security Leader in Australia

Kontakt:

Krzysztof Radziwon
Partner
Szef zespołu doradczego
w zakresie bezpieczeństwa IT
w KPMG w Polsce
T: +48 22 528 1137
E: kradziwon@kpmg.pl

Paweł Skowroński
Starszy menedżer
w zespole doradczym
w zakresie bezpieczeństwa IT
w KPMG w Polsce
T: +48 22 528 1350
E: pskowronski@kpmg.pl

Znajdź nas:
kpmg.pl
youtube.com/kpmgpoland
facebook.com/kpmgpoland
twitter.com/kpmgpoland
linkedin.com/company/kpmg_poland
instagram.com/kpmgpoland
pinterest.com/kpmgpoland
kpmg.com/pl/app
itunes.com/apps/KPMGThoughtLeadership
itunes.com/apps/KPMGGlobalTax
itunes.com/apps/KPMGPolandCareer

Zeskanuj kod, aby przejść do strony kpmg.pl

Dostępne w App Store

KPMG Poland

Biura KPMG w Polsce

Warszawa
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Kraków
al. Armii Krajowej 18
30-150 Kraków
T: +48 12 424 94 00
F: +48 12 424 94 01
E: krakow@kpmg.pl

Poznań
ul. Roosevelta 18
60-829 Poznań
T: +48 61 845 46 00
F: +48 61 845 46 01
E: poznan@kpmg.pl

Wrocław
ul. Bema 2
50-265 Wrocław
T: +48 71 370 49 00
F: +48 71 370 49 01
E: wroclaw@kpmg.pl

Gdańsk
al. Zwycięstwa 13a
80-219 Gdańsk
T: +48 58 772 95 00
F: +48 58 772 95 01
E: gdansk@kpmg.pl

Katowice
ul. Francuska 34
40-028 Katowice
T: +48 32 778 88 00
F: +48 32 778 88 10
E: katowice@kpmg.pl

Łódź
al. Piłsudskiego 22
90-051 Łódź
T: +48 42 232 77 00
F: +48 42 232 77 01
E: lodz@kpmg.pl

Przygotowano na podstawie raportu KPMG International pt. „Cyber security: a failure of imagination by CEOs", 2015