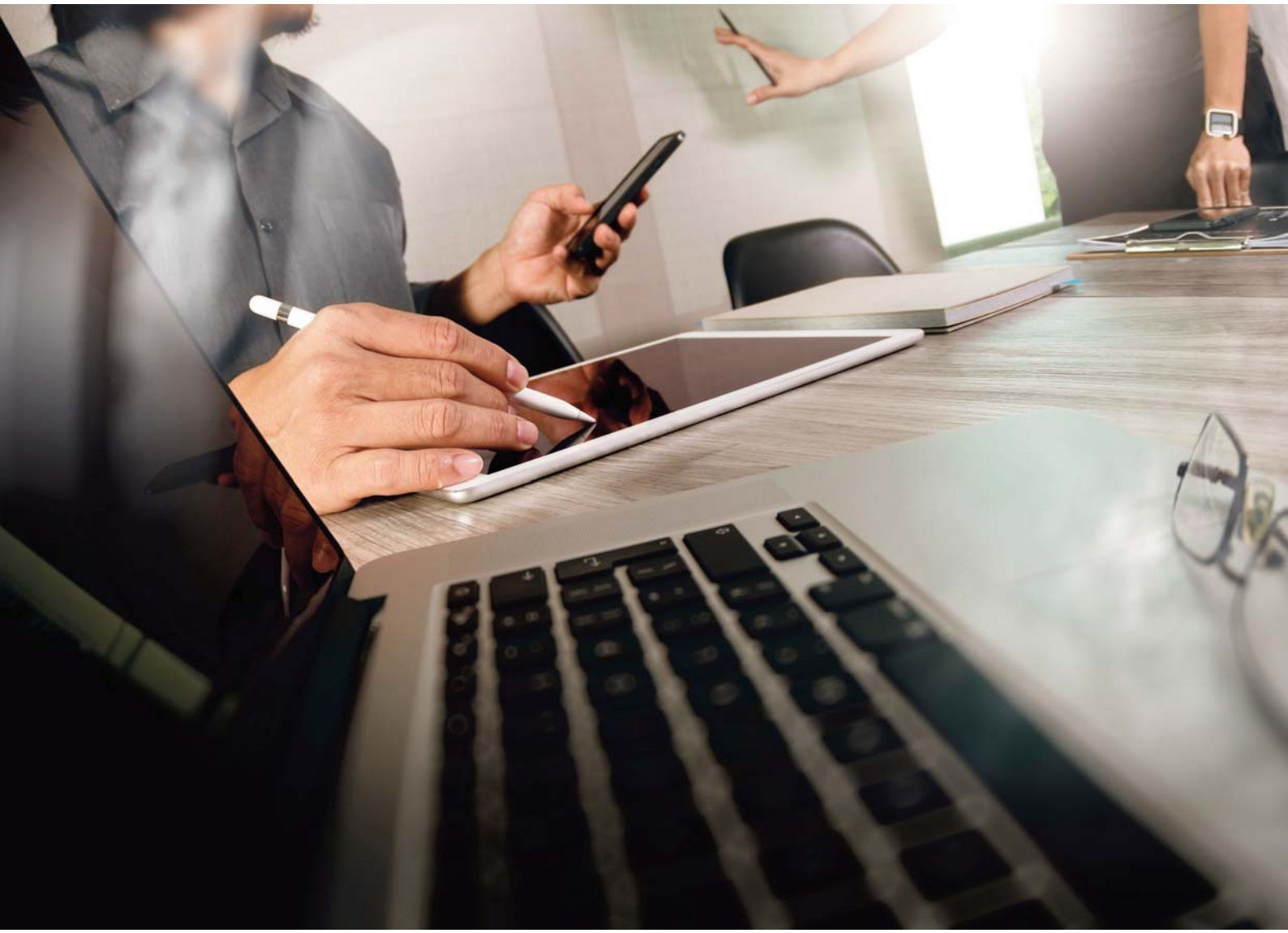
4. edycja badania stanu bezpieczeństwa informacji w Polsce

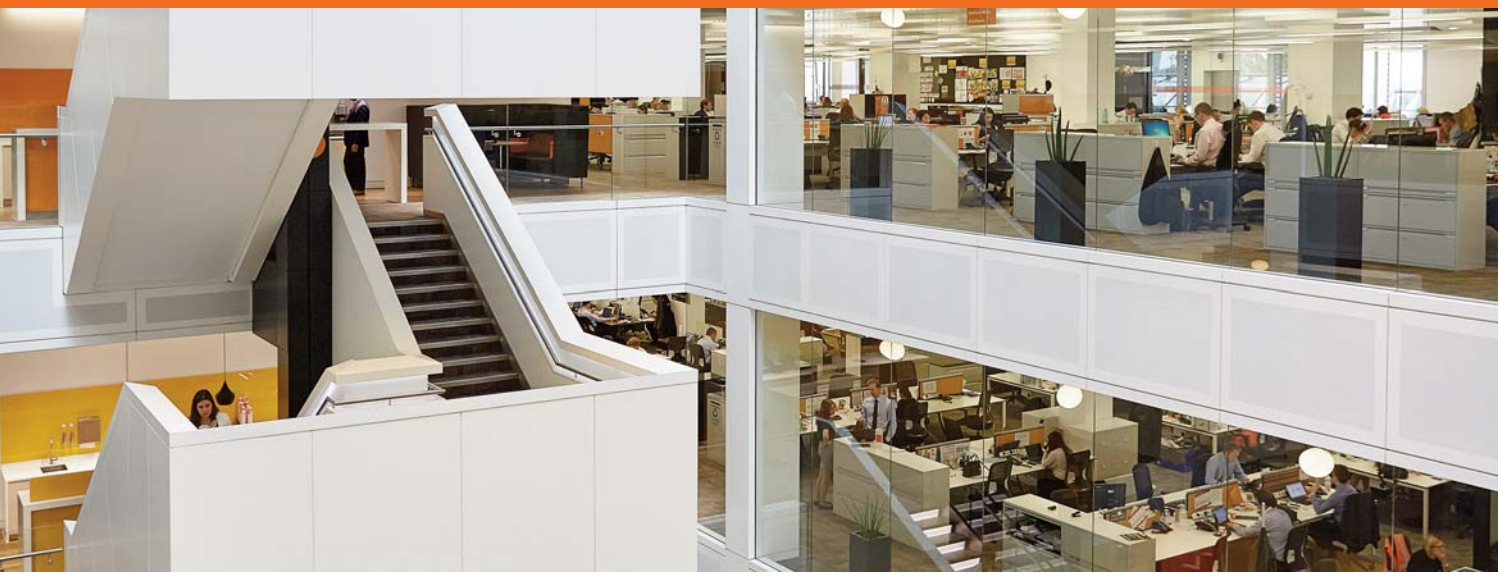
Ochrona biznesu w cyfrowej transformacji

czyli 4 kroki do bezpieczniejszej firmy



pwc

pwc.pl/stanbezpieczenstwa



Szanowni Państwo,

Cyfrowa transformacja wystawia na próbę zaufanie w cyfrowym świecie. Skuteczna ochrona systemów IT, zgromadzonych danych i informacji jest dziś kluczowym elementem dla stabilnego funkcjonowania firmy. 61% prezesów największych światowych organizacji wskazało cyberzagrożenia jako jedno z największych obszarów ryzyka dla ich biznesu.[1] Jedną z najbardziej wrażliwych kwestii jest zaufanie rynku do marki, szczególnie w sytuacji, gdy sieć połączeń zarówno pomiędzy ludźmi jak i urządzeniami stale rośnie.

Wyniki tegorocznej, czwartej już edycji badania stanu bezpieczeństwa informacji w Polsce wskazują, że biznes stoi przed dużym wyzwaniem związanym ze stabilnym zaufaniem w sieci i poczuciem bezpieczeństwa pracowników i klientów.

Przygotowanie polskich przedsiębiorstw do RODO nadal jest na początku drogi. Firmy zaczęły implementację nowych regulacji od rozwiązań najprostszych. Najgorzej wypada gotowość procesowa firm – program umożliwiający identyfikację wrażliwych zasobów wdrożyło zaledwie 11% firm, a 58% w ogóle go nie planuje.

Wyniki badania wskazują, że 96% firm doświadczyło ponad 50 incydentów przestrzeni ostatniego roku. Do ich negatywnych skutków badani najczęściej zaliczali straty finansowe i narażenie na ryzyko prawne czy proces sądowy (35%). Innymi często wskazywanymi odpowiedziami były utrata klientów (30%), jak również wyciek korespondencji firmowej (25%).

Również przenikanie się środowisk IT i automatyki przemysłowej (OT) wymaga zmian związanych z podejściem do bezpieczeństwa i monitorowania produkcji w polskich firmach. Zdaniem przeszło 60% ankietowanych procesy, które wspierają systemy automatyki przemysłowej (OT), związane z zarządzaniem incydentami bezpieczeństwa w przedsiębiorstwie, wymagają zmian.

Analizując trendy, wyzwania oraz kierunki rozwoju globalnych firm prezentujemy cztery kroki, które pozwolą polskim firmom kompleksowo przygotować się do nadchodzących zmian regulacyjnych, wzmocnić lub uzupełnić elementy bezpieczeństwa, w które już zainwestowały oraz budować wartość i przewagę konkurencyjną na rynku.

Piotr Urban
Partner, Zespół Zarządzania Ryzykiem

[1] *Badanie PwC CEO Survey 2017*

Ochrona biznesu w cyfrowej transformacji

Krok 1

Zaufanie w centrum uwagi – przygotuj się do zmian

20 mln euro

kary za naruszenie przepisów RODO

72 godziny

na zgłoszenie cyber ataku do organu regulacyjnego

Przygotowanie do nowego rozporządzania o ochronie danych osobowych (RODO)

Jednym z najważniejszych wydarzeń minionego roku związanych z bezpieczeństwem informacji było przyjęcie przez Unię Europejską ogólnego rozporządzenia o ochronie danych osobowych (RODO), które od maja 2018 ma zastąpić wszystkie krajowe przepisy w tym zakresie i wprowadzić jednolite zasady dla całego wspólnego rynku europejskiego.

W Polsce zmienia ono przepisy ustawy z 29 sierpnia 1997 roku o ochronie danych osobowych. Rozporządzenie jest stosowane wprost, dlatego staje się wiążącym prawem dla wszystkich przedsiębiorców. Obecnie trwa okres ustanowiony dla przedsiębiorców na wdrożenie wymagań rozporządzenia, które w pełni stosowane będzie od 25 maja 2018 roku. Naruszenie przepisów będzie wiązać się z ryzykiem nałożenia na przedsiębiorstwa kary finansowej do 20 mln euro lub 4% wartości rocznego światowego obrotu przedsiębiorstwa.

RODO wprowadza wiele istotnych zmian w podejściu do spełnienia wymagań zabezpieczania danych osobowych. W miejsce szczegółowych, nie zawsze dostosowanych do rozwiązań technicznych zasad, w przepisach RODO zawarte zostało wymaganie, by administratorzy i podmioty przetwarzające dane wdrożyły odpowiednie środki techniczne i organizacyjne, dobrane samodzielnie przez administratora lub podmiot przetwarzający.

Co najważniejsze – incydenty związane z naruszeniem bezpieczeństwa danych osobowych będą musiały być zgłaszane w ciągu 72 godzin do organu regulacyjnego. Dodatkowo każdy rodzaj biznesu przetwarzający takie dane będzie musiał przeprowadzić przynajmniej stosowne analizy ryzyka i wdrożyć adekwatne zabezpieczenia. Może to oznaczać zmianę lub konieczność nowej strategii w zakresie zarządzania danymi i wdrożenia procesów oraz technologii w celu zapewnienia inwentaryzacji i ochrony danych osobowych.

Z tegorocznej edycji badania wynika, że pod względem przygotowania do RODO polskie firmy znajdują się dopiero na początku drogi do zapewnienia zgodności z nowymi przepisami.

Wśród podjętych kroków najskuteczniej zrealizowane zostało uwzględnienie mechanizmów ochrony danych osobowych w fazie projektowania nowych systemów informatycznych (ang. *Privacy by Design*) – 42% respondentów deklaruje, że przy wdrażaniu nowych systemów uwzględnili zagadnienia związane z prawidłową ochroną danych osobowych. Na drugim miejscu uplasowało się zobowiązywanie pracowników do odbywania okresowych szkoleń dotyczących polityki ochrony danych osobowych, takiej odpowiedzi udzieliło 34% badanych, 27% respondentów wskazało na wdrożenie zabezpieczeń w zakresie ochrony danych osobowych oraz audyty zgodności firm zewnętrznych obsługujących dane osobowe (tzw. procesorów).

Obiecująco przedstawia się perspektywa wdrożenia rozwiązań szyfrujących dane. Aż 34% firm deklaruje wysoki priorytet dla wdrożenia tego typu rozwiązań. W pozostałych aspektach związanych z RODO przedsiębiorstwa powinny się pospieszyć. Najbardziej zaniedbanymi obszarami związanym z nowymi przepisami są: utworzenie lub aktualizacja rejestru operacji przetwarzania danych osobowych, ocena skutków operacji przetwarzania oraz ograniczenie liczby operacji przetwarzania danych do minimum koniecznego do osiągnięcia celu, dla którego zostały zebrane. Odpowiednio tylko 12, 15 i 12% firm ma wdrożone właściwe rozwiązania. Może to oznaczać, że jeszcze nie przeprowadziły analiz, które pokazują, z jakimi tak naprawdę zmianami w systemach IT i procesach biznesowych wiąże się implementacja RODO.

Firmy zaczęły implementację nowych regulacji od rozwiązań najprostszych, to stanowi dobrą podstawę do realizacji innych zadań. Należy jednak mieć na uwadze ograniczony czas na wdrożenie przepisów RODO. Najbardziej krytyczne z punktu widzenia ochrony danych osobowych jest podejście firm do tematu Big Data. 80% firm nie rozważa wprowadzenia rozwiązań mających na celu zapewnienie bezpieczeństwa tego obszaru. Ponieważ rozporządzenie RODO dotyczy również operacji masowego przetwarzania, wszystkie procesy zmierzające do zapewnienia bezpieczeństwa danych osobowych powinny również obejmować obszar Big Data.

Polskie firmy są na początku drogi w przygotowaniu do nowych przepisów. Gotowość dużych i średnich firm można określić jako słabą. Pewne najprostsze do wdrożenia przepisy zostały zrealizowane, zatrudnieni zostali specjaliści od ochrony danych osobowych i planowane są wdrożenia technicznych rozwiązań mających na celu zapewnienie bezpieczeństwa danych. Najgorzej wypada gotowość procesowa firm – program umożliwiający identyfikację wrażliwych zasobów wdrożyło zaledwie 11% firm, a 58% w ogóle go nie planuje.

Stopień przygotowania polskich firm do RODO

Odsetek firm, które wdrożyły odpowiednie rozwiązania.

Przygotowanie do RODO wymaga analizy

„Należy pamiętać, że sposób spełnienia wymagań RODO dla każdego administratora lub podmiotu przetwarzającego może być inny. Możliwa jest także sytuacja, gdy w ramach jednego podmiotu konieczne będzie zastosowanie różnych sposobów spełnienia tego wymagania. Każda decyzja o stosowanych środkach ochrony danych osobowych powinna być poprzedzona pogłębioną analizą, która pozwoli na wybranie najlepszego rozwiązania. Wymagania zawarte w Ogólnym rozporządzeniu o ochronie danych mają wpływ na bardzo wiele obszarów działalności firmy. Dotyczą nie tylko działu prawnego, ale również marketingu, HR-u czy obsługi klienta. W związku z tym, aby zapewnić adekwatne wdrożenie wymagań wynikających z przepisów RODO zalecanym jest powołanie interdyscyplinarnego zespołu ekspertów, w szczególności z obszaru prawnego, biznesu oraz IT i bezpieczeństwa informacji”.

Anna Kobylańska – *adwokat, counsel w kancelarii prawnej PwC Legal*
Łukasz Ślęzak – *menadżer, Zespół Cyber Security*

Współpraca na rzecz cyber bezpieczeństwa

Cyberzagrożenia dotyczą wszystkich firm bez wyjątku. Postanowiliśmy sprawdzić, czy przedsiębiorstwa decydują się na podjęcie współpracy, aby wspólnie działać na rzecz zwiększenia cyberbezpieczeństwa. Temat jest ważny, ponieważ, jak ukazały wyniki badania, większość respondentów nie jest przekonanych, że podejmowane przez ich partnerów czy dostawców działania są wystarczające dla zapewnienia bezpieczeństwa informatycznego. Raczej lub stanowczo przekonanych, że tak się dzieje jest zaledwie jedna czwarta ankietowanych.

Także na poziomie administracji publicznej kwestia współpracy i koordynacji działań jest wysoko na agendzie. W opublikowanym pod koniec 2016 roku projekcie dokumentu *„Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”* Ministerstwo Cyfryzacji za jeden z głównych celów stawia „Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa”.[2] Nie przekłada się to na chęć zacieśnienia więzów pomiędzy różnymi podmiotami. Podobnie jak w poprzednim roku, respondenci wyrazili sceptycyzm w zakresie kooperacji i wymiany informacji z innymi podmiotami. Tylko 31% uczestników naszego badania potwierdziło, że firma, którą reprezentują, prowadzi współpracę z innymi podmiotami na rzecz poprawy bezpieczeństwa i ograniczenia ryzyka w przyszłości. O tym, że ich firmy tego nie robią, wie 27% respondentów, 42% nie było w stanie udzielić odpowiedzi na to pytanie. Dlaczego współpraca tego rodzaju jest mało popularna?

Podstawową przeszkodą jest nieufność wobec zewnętrznych źródeł informacji. Na dalszych miejscach pojawiła się też niechęć do odkrywania słabych stron swojego przedsiębiorstwa. Odpowiedzi wskazują, że ankietowanym trudno jest dostrzec pozytywne aspekty kooperacji, raczej widzą w niej zagrożenie.

Pewnym zaskoczeniem jest fakt, że pomimo braku zaufania, większość ankietowanych jest przekonanych, że ich firma nie planuje wdrażać programów monitorujących lub audytów zewnętrznych partnerów i dostawców usług, dla zyskania pewności, że przestrzegają oni polityk bezpieczeństwa i ochrony danych obowiązujących w ich firmach. Jedynie 8% organizacji wdrożyło takie działania.

Warto też zwrócić uwagę, że są sfery, w których wymiana informacji jest praktykowana – branża bankowa, czy telekomunikacyjna. Królują jednak nieformalne kanały wymiany informacji. Czy promowane przez Ministerstwo Cyfryzacji tzw. Sektorowe zespoły CERT (*Computer Emergency Response Team*) będą panaceum na tą nieufność?

[2] *Ministerstwo Cyfryzacji „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”*

Powody braku współpracy firm z innymi podmiotami na rzecz poprawy bezpieczeństwa

Konsumenci w sieci

Kwestia zaufania wiąże się nie tylko z relacjami z partnerami biznesowymi, ale także z klientami indywidualnymi. Jak wynika z badania *PwC Total Retail 2017* firmy nie chcą nadużywać zaufania konsumentów. Ponad połowa firm zadeklarowała, że ich organizacje nie planują prosić klientów o udostępnienie dodatkowych danych osobowych (takich jak dane demograficzne czy kontaktowe) w ciągu najbliższego roku, w celu personalizacji świadczonych usług.

Biorąc pod uwagę nastroje wśród klientów, to dobra decyzja. Ludzie niechętnie dzielą się informacjami na swój temat, głównie w obawie przed oszustwem. Konsumenci w sieci korzystają przede wszystkim z usług firm, którym ufają – tak robi 52% respondentów w Polsce i 59% globalnie. Podobnie, 54% konsumentów w Polsce i 63% na świecie deklaruje, że korzysta jedynie z zaufanych stron internetowych. Co czwarty uczestnik badania w Polsce stwierdził, że zapoznaje się z politykami ochrony danych, na świecie odsetek ten jest tylko nieznacznie niższy.

Coraz częściej polscy klienci kupują za pośrednictwem mediów społecznościowych – tak zadeklarowało 21% respondentów. To ważna informacja, firmy muszą podjąć działania mające na celu ochronę danych dostarczanych im tą drogą. Aktywność w sieci jest związana z decyzjami, które pociągają za sobą konieczność pozostawiania danych umożliwiających identyfikację lub płatność – zwiększenie sprzedaży tą drogą wymaga więc odpowiedniego zabezpieczenia przetwarzanych danych w cyberprzestrzeni. Obawy konsumentów dotyczą także korzystania z urządzeń mobilnych. 71% respondentów boi się ataku hackerskiego na swoje smartfony czy tablety, tylko 29% uważa płatności mobilne za bezpieczne.

Poziom zaufania klientów w przywołanych obszarach jest w dalszym ciągu stosunkowo niski. To istotna informacja dla firm. Jeżeli chcą, aby klienci chętniej powierzali im swoje dane lub korzystali z zakupów on-line konieczne jest zwiększenie bezpieczeństwa i poprawa komunikacji z klientami na temat podejmowanych przez firmę działań. To cenna informacja dla firm chcących się wyróżnić – podejmowanie działań na rzecz bezpieczeństwa i dbałość o nie – to duży atut.

25%

co czwarty polski konsument czyta politykę prywatności zostawiając swoje dane w sieci

Krok 2

Świadomość przede wszystkim – miej pewność

Fundamentalne znaczenie ma wyasygnowanie budżetu umożliwiającego podjęcie działań obronnych. W naszym badaniu ponad połowa przedstawicieli firm zadeklarowała, że budżet przeznaczony na bezpieczeństwo IT i bezpieczeństwo informacji na 2016 rok mieścił się w przedziale od 500 tys. do 1 mln. złotych. Wydaje się jednak, że w kontekście przygotowań do RODO średnich i dużych firm, to dopiero początek inwestycji w tym obszarze. Zmieniła się także dynamika wydatków – inwestycje realizowane są punktowo, w wyselekcjonowane obszary. Choć w ujęciu globalnym, wydatki na bezpieczeństwo nie uległy zmianie, to zmienił się ich rozkład pomiędzy poszczególnymi sektorami gospodarki.

W kontekście budżetu większość badanych deklaruje posiadanie ogólnej strategii bezpieczeństwa teleinformatycznego, jednak aż 72% z tych firm nie prowadzi obecnie działań zmierzających do identyfikacji wrażliwych zasobów, a większość nie posiada szczegółowych strategii np. w obszarach mediów społecznościowych, urządzeń mobilnych czy chmury obliczeniowej (odpowiednio 63%, 86%, 63%). To zastanawiające, ponieważ trendem na rynku jest pozwalanie pracownikom na używanie ich prywatnych urządzeń elektronicznych (smartfonów czy tabletów) do korzystania z aplikacji firmowych. Już dziś jest to możliwe w 46% badanych firm, kolejnych 14% planuje umożliwić takie działania w przyszłości. „Nie" tego rodzaju praktykom mówi zaledwie 17% organizacji. Jednocześnie, tylko 16% firm wymaga zainstalowania na tych urządzenia chrozwiązań klasy MDM (ang. *Mobile Device Management*), aby użytkownicy mogli korzystać z firmowych aplikacji.

firm wydaje mniej niż 1 milion PLN rocznie na bezpieczeństwo IT

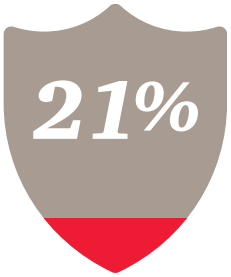
46%

firm pozwala pracownikom korzystać z aplikacji firmowych na prywatnych smartfonach i tabletach

Skuteczne bezpieczeństwo wymaga kompleksowego podejścia

„Posiadanie ogólnej strategii bezpieczeństwa nie gwarantuje jeszcze optymalnego wydatkowania środków i wyboru adekwatnych technologiczno-organizacyjnych mechanizmów zabezpieczających. Dopiero wiedza o otoczeniu i zagrożeniach, o tym, co jest najistotniejsze dla organizacji, i jakie zasoby powinny być chronione, pozwala na skierowanie inwestycji we właściwą stronę. Wynik badań i obserwacje rynku wskazują jednak, że nadal wydatki są kierowane punktowo i raczej na technologię, niż podniesienie poziomu dojrzałości bezpieczeństwa całej organizacji. Często w ślad za nowymi rozwiązaniami technicznymi nie idą inwestycje w ludzi, którzy mogliby skutecznie je wykorzystać, i w procesy, które zapewnią, że technologia i ludzie będą efektywnie pracować. Takie podejście oraz brak odpowiednich procedur zarządzania ryzykiem oznacza konieczność uczenia się na błędach, a to może być bardzo kosztowne".

Tomasz Sawiak – *wicedyrektor, Zespół Cyber Security*



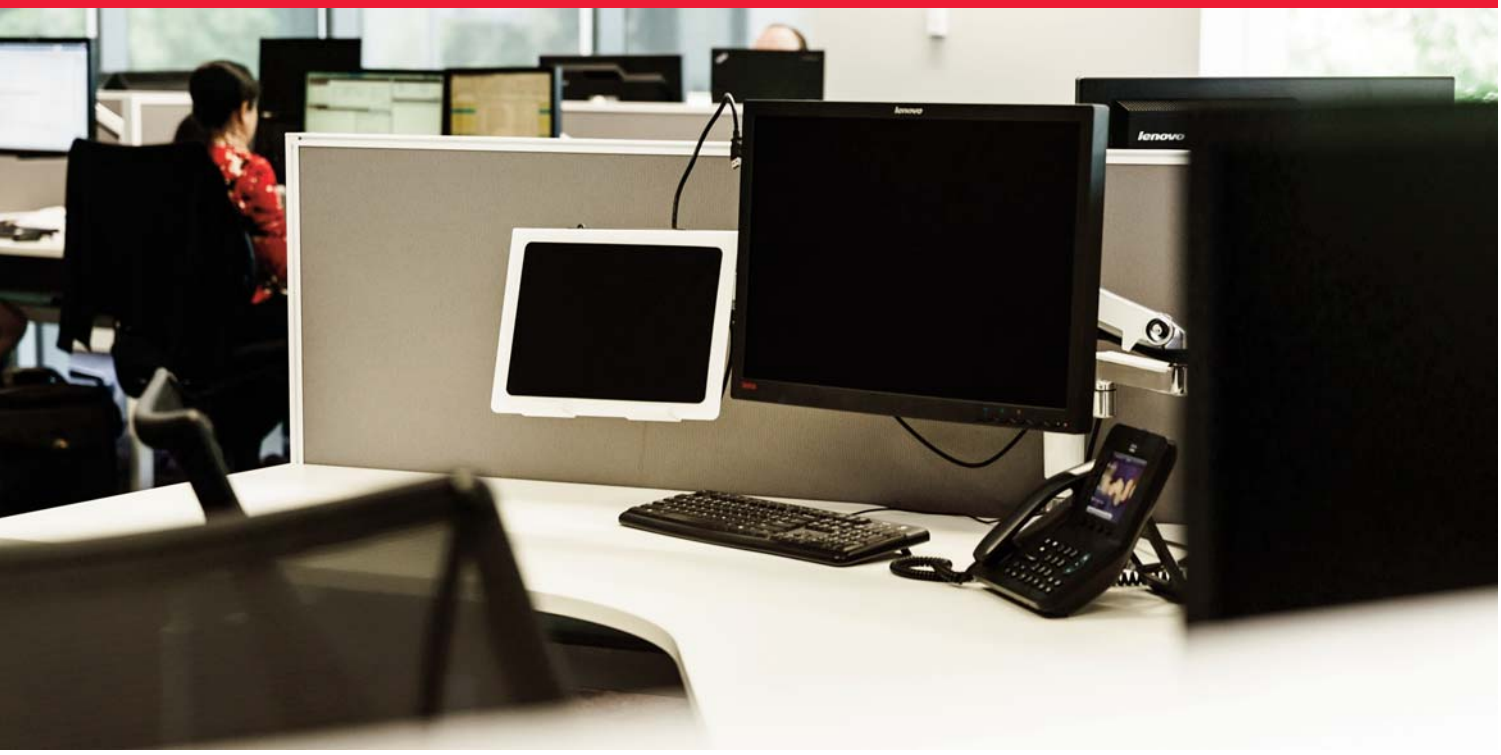
firm posiada SIEM

(Security Information Event Management)

Technologia w służbie bezpieczeństwa

Utrzymanie poziomu bezpieczeństwa teleinformatycznego, adekwatnego do specyfiki prowadzonego biznesu i obserwowanych w otoczeniu zagrożeń, wymaga zastosowania odpowiedniego zestawu mechanizmów zabezpieczających. Poza zasobami organizacyjnymi wymagane są także odpowiednie rozwiązania technologiczne, odpowiadające na określone problemy i zagrożenia. Firmy, chcąc uzyskać jak największa przewagę konkurencyjną rozwijają i doskonalą swoje procesy biznesowe oraz związane z nimi systemy i środowiska teleinformatyczne. Coraz większe uzależnienie przedsiębiorstw od technologii stanowiącej o ich przewadze konkurencyjnej sprawia, że ryzyko i skutki ataków na środowiska IT rosną. Zwiększa to potrzebę rozważnego doboru odpowiedniego zestawu zabezpieczeń technologicznych. Biorąc pod uwagę dostępne na rynku rozwiązania zabezpieczające oraz specyfikę ataków, można powiedzieć, że przedsiębiorstwa nie są jeszcze w pełni przygotowane na przeciwdziałanie współczesnym zagrożeniom i metodom ataków. Firmy w Polsce czeka jeszcze wiele pracy w obszarze rozwoju technologicznej architektury bezpieczeństwa firmy. Współczesne metody ataków na środowiska IT przedsiębiorstw często skupiają się na uzyskaniu zdalnego dostępu do stacji roboczej uprzywilejowanych użytkowników poprzez infekcje odpowiednio przygotowanym złośliwym oprogramowaniem (tzw. RAT – *Remote Access Trojan*). Stosowane są różne metody ataków, między innymi wykorzystujące niewiedzę użytkowników i nakłaniające ich do nieświadomej infekcji stacji roboczych poprzez odwiedzenie odpowiednio przygotowanych serwisów WWW, otwieranie odpowiednio spreparowanych plików (dokumentów, arkuszy kalkulacyjnych itp.). Specjalistyczne rozwiązania chroniące przed tego typu atakami (tzw. anty APT – *Advanced Persistent Threat*) stosowane są jedynie przez 26% ankietowanych firm.

Duża ilość systemów i zabezpieczeń technologicznych wymaga kompleksowego spojrzenia na całą infrastrukturę teleinformatyczną i wiedzy na temat efektów działań mechanizmów zabezpieczających. Tylko to umożliwi adekwatne reagowanie i prowadzenie analiz identyfikowanych incydentów. Tylko 21% ankietowanych deklaruje, że posiada system klasy SIEM (*Security Information Event Management*), który adresuje wspomnianą potrzebę. W procesie ataku wykorzystywane są często znane podatności komponentów informatycznych.

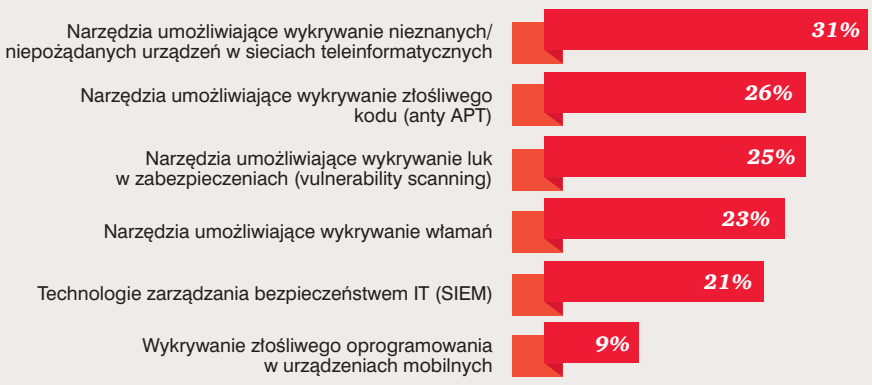


Kluczowe jest usuwanie krytycznych podatności pozwalających na zdalny nieautoryzowany dostęp do komponentów najważniejszych systemów. Niestety tylko 25% ankietowanych deklaruje, że posiada narzędzia wspierające ten proces. Rozwiązania umożliwiające wykrywanie włamań tzw. IDS (*Intrusion Detection Systems*) stanowią rozwiązania oparte o sygnatury znanych ataków i prób wykorzystywania znanych podatności. Systemy te uzupełniają niedoskonałości procesu identyfikacji i zarządzania podatnościami w komponentach infrastruktury i są stosowane przez 23% przedsiębiorstw.

Co raz więcej informacji jest przetwarzane na urządzeniach mobilnych, współczesne aplikacje są projektowane z myślą o użytkownikach mobilnych i łatwym zdalnym dostępie do danych. Niestety, tylko 9% przedsiębiorstw stosuje oprogramowanie wykrywające złośliwe oprogramowanie na urządzeniach mobilnych. Firmy skupiają się na zabezpieczeniu stacji roboczych i zapominają o analogicznym zabezpieczeniu urządzeń przenośnych. Brak zabezpieczeń tego typu skutkować może niekontrolowanym wyciekiem danych, co w kontekście nowych regulacji RODO wymaga zwrócenia szczególnej uwagi.

Poza wdrożeniem odpowiednich zabezpieczeń technologicznych, zasadnicze znaczenie dla bezpieczeństwa IT stanowi odpowiednio wykwalifikowany personel. Nawet najlepsze zabezpieczenia bez właściwych ludzi i odpowiedniej warstwy proceduralno-organizacyjnej, nie zostaną w pełni wykorzystane i nie będą rozwijane. Ważnym elementem jest też stałe doskonalenie konfiguracji wdrożonych systemów, oparte o wiedzę zdobywaną z rejestrowanych incydentów i zagrożeń obserwowanych w otoczeniu przedsiębiorstwa.

Technologie zabezpieczeń wdrożone w firmie



Organizacja bezpieczeństwa informacji i IT w firmach

Działanie na rzecz bezpieczeństwa teleinformatycznego powinno być wspierane na każdym szczeblu i dobrze umocowane na poziomie zarządczym w firmie. Zapytaliśmy naszych respondentów o to, w jaki sposób organizują bezpieczeństwo informacji i IT. Dobrą wiadomością jest, że w badanej grupie nie było żadnego przypadku braku osoby odpowiedzialnej za te obszary. W większości, duże firmy zatrudniają do 10 osób w działach IT i bezpieczeństwa informacji. Osoba w randze dyrektora odpowiedzialna za bezpieczeństwo teleinformatyczne spółki (o ile w firmie istnieje takie stanowisko) najczęściej podlega bezpośrednio dyrektorowi generalnemu, tak odpowiedziało 27% ankietowanych.

Bardzo dużą rolę w zapewnieniu firmie bezpieczeństwa teleinformatycznego może odegrać zarząd firmy. We wszystkich badanych firmach uczestniczy on w kształtowaniu budżetu przeznaczonego na kwestie związane z bezpieczeństwem. 98% respondentów wskazało, że gremium to współtworzy ogólną strategię bezpieczeństwa, a 86% stwierdziło, że aktywnie kształtuje politykę bezpieczeństwa. Tylko niewielka liczba zarządów zajmuje się przeglądem ról i obowiązków związanych z bezpieczeństwem w organizacji. Dzieje się tak tylko w 13% badanych firm. Zaangażowanie zarządów w omawiane w raporcie kwestie cieszy, jednak niska pozycja w hierarchii firmowej menedżerów ds. bezpieczeństwa wskazuje, że nadal tematy ochrony danych, prywatności i bezpieczeństwa nie są wystarczająco wysoko na agendzie dużych i średnich firm.

Obszary zaangażowania zarządu

Badając poziom strategiczny w organizacjach, postanowiliśmy sprawdzić, jakie priorytety mają organizacje na najbliższych 12 miesięcy. Jak pokazały wyniki naszych badań, największa grupa, bo aż 57% firm będzie prowadziła ciągły monitoring bezpieczeństwa teleinformatycznego. Na drugim miejscu znalazły się szkolenia zwiększające poziom wiedzy o bezpieczeństwie, na trzecim miejscu uplasowała się dbałość o bezpieczeństwo fizyczne. Duże organizacje zaczęły doceniać znaczenie monitorowania bezpieczeństwa oraz poziomu świadomości pracowników. Dziwi jednak bardzo mały nacisk na wdrożenie zmian związanych z RODO. Wydaje się, że będzie się to zmieniać w nadchodzących miesiącach, w miarę, jak świadomość na temat samego rozporządzania oraz jego wpływu na organizację będzie rosnąć.

Priorytety w obszarze bezpieczeństwa firmy na najbliższe 12 miesięcy

Zarządzanie cyberbezpieczeństwem na agendzie CEO

„W Polsce zarządzanie cyber ryzykiem wciąż jest na agendzie niewielu zarządów. Tylko dojrzałe organizacje dostrzegają korzyści z posiadania stałej informacji na ten temat oraz możliwości wykorzystania ich w decyzjach biznesowych. W dużych firmach w Stanach Zjednoczonych czy Europie Zachodniej, cyberbezpieczeństwo jest jednym z kluczowych tematów, systematycznie omawianych i analizowanych na posiedzeniach zarządów. Do tego organizacja musi jednak posiadać właściwe narzędzia umożliwiające pozyskanie, analizę, śledzenie i raportowanie otoczenia i związanych z nim ryzyk. Warto podkreślić, że takie narzędzia istnieją – systemy SIEM czy DLP (ochrona przed wyciekami informacji) często jednak brakuje procesów i wiedzy oraz systemów, które umożliwiłyby ich pełne wykorzystanie. Dobrym przykładem są systemy klasy GRC (Governance-Risk-Complinace), które umożliwiają analizę danych i automatyzację wielu procesów z obszaru bezpieczeństwa, audytu, czy zgodności, dając zarządom przejrzyste informacje o stanie ryzyk w firmie”.

Patryk Gęborys – *wicedyrektor, Zespół Cyber Security*

Krok 3

Monitorowanie efektów – sprawdzaj skuteczność i wyciągaj wnioski

Wdrażane przez firmy zabezpieczenia technologiczno-organizacyjne, składające się na ich architekturę bezpieczeństwa, ograniczają ryzyko ataków i potencjalne straty. Jednak z uwagi na złożoność środowisk IT, nieprzerwaną ewolucję zagrożeń i ataków nie gwarantują 100% skuteczności. Wyciąganie wniosków z obserwowanych incydentów pozwala na planowanie kierunków działań dalszego rozwoju zabezpieczeń, identyfikację potencjalnych luk i ich rozważne adresowanie. Firmy odnotowują rosnącą liczbę incydentów, co wiąże się ze zwiększającą się świadomością problemu i rozwijanymi procesami monitorowania – 96% firm doświadczyło ponad 50 incydentów przestrzeni ostatniego roku.

96%

firm doświadczyło ponad ***50*** incydentów naruszenia bezpieczeństwa w ostatnim roku

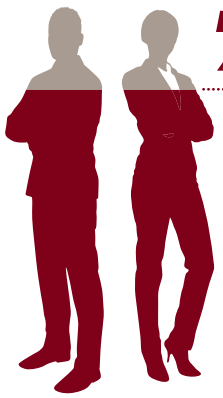
Sposoby, źródła i konsekwencje incydentów naruszenia bezpieczeństwa

Z badania wynika, że najczęściej wykorzystywaną metodą był atak phishingowy (mający na celu zmylenie użytkownika i nakłonienie do wykonania zamierzonej operacji), takiej odpowiedzi udzieliło 39% ankietowanych. Na drugim miejscu respondenci wskazali na wykorzystanie zewnętrznych nośników danych, z czym wiążą się infekcje komponentów infrastruktury oraz możliwość wycieku danych.

Pierwszą trójkę zamyka wykorzystywanie urządzeń mobilnych oraz sieci – tak wskazało po 18% badanych. Wielu z incydentów można byłoby uniknąć, gdyby wdrożone były odpowiednie systemy zabezpieczeń, pracownicy mieli większą świadomość zagrożeń, oraz gdyby istniały odpowiednie polityki i procedury określające sposób postępowania.

atak phishingowy najczęstszym incydentem naruszenia bezpieczeństwa w firmach

Przyczyny incydentów naruszenia bezpieczeństwa



79%

incydentów w firmach powodują aktualni pracownicy

W porównaniu do poprzedniej edycji badania, nie zmieniło się podstawowe źródło zagrożeń – pozostali nim aktualni pracownicy – zadeklarowało tak 79% badanych. Z 67 do 62% zmalała natomiast liczba ankietowanych wskazujących na działania hakerów. Warto odnotować dość wysoki udział przestępczości zorganizowanej, który choć zmalał z 41% w poprzedniej edycji badania, do 38% obecnie, wciąż jest na wysokim poziomie. Tylko o 1 punkt procentowy mniej ankietowanych wskazało na aktualnych usługodawców, konsultantów lub wykonawców. Mówiąc o źródłach i liczbie incydentów nie można zapominać, że każdy z nich może za sobą pociągać poważne następstwa.

Jak pokazały wyniki, 55% respondentów nie ma świadomości, jakie były efekty ataków na dane w ich organizacjach biznesowych. W części zapewne oznacza to, że nie wyrządziły one żadnych szkód, część respondentów może sobie jednak nie zdawać sprawy ze skutków naruszeń, gdyż mogą być one trudne do oszacowania bez odpowiedniej metodyki. Wskazuje to potrzebę rozwoju systemów zarządzania ryzykiem i gromadzenia informacji o zdarzeniach operacyjnych – w tym o incydentach bezpieczeństwa – w sposób zapewniający spójne gromadzenie informacji o kosztach, skutkach i obsłudze incydentów.

Skutki naruszenia bezpieczeństwa

Znacząca grupa badanych (29%) stwierdziła, że efektem cyberataków była utrata lub uszkodzenie przetwarzanych danych, 6% poinformowało o wycieku danych klientów, a 5% o wycieku danych pracowników. O jeszcze poważniejszych skutkach wspomniało 3% – poinformowali oni, że w ich firmie nastąpił wyciek danych i informacji pozwalających na identyfikację klienta lub kontrahenta, a w 2% organizacji taki, który umożliwił kradzież tożsamości. Te ostatnie mogą mieć szczególnie negatywne konsekwencje, od wizerunkowych, aż po poważne straty finansowe.

W stosunku do poprzedniej edycji badania z 13 do 5% spadła liczba odpowiedzi wskazujących na wyciek danych pracowników, większe znaczenie ma jednak fakt ograniczenia wycieków danych klientów (spadek z 18 do 6%). Niestety symultanicznie odnotowaliśmy znaczący wzrost w obszarze utraty lub uszkodzenia danych, z 16% w zeszłorocznej do 29% w tym roku.

Do negatywnych skutków incydentów naruszenia bezpieczeństwa badani najczęściej zaliczali straty finansowe i narażenie na ryzyko prawne czy proces sądowy (35%). Innymi często wskazywanymi odpowiedziami były utrata klientów (30%), jak również wyciek korespondencji firmowej (25%). W ocenie badanych takie incydenty rzadko dotyczą nadużyć o charakterze finansowym, utraty partnerów biznesowych lub dostawców, czy kradzieży „miękkiej" własności intelektualnej (5%).

Ubezpieczenia od cyber ryzyk

Świadomość zagrożeń, jakie niosą za sobą cyber ryzyka, wpływa na podjęcie przez część firm decyzji o zakupie polisy ubezpieczeniowej od ich wystąpienia. Jak ukazały wyniki naszego badania, taką decyzję podjęło 7% firm. 40% firm, które posiadają ubezpieczenia od cyber ryzyk uważa, że ich firma poczyniła kroki w kierunku poprawy stanu bezpieczeństwa w organizacji, aby obniżyć składkę ubezpieczeniową.

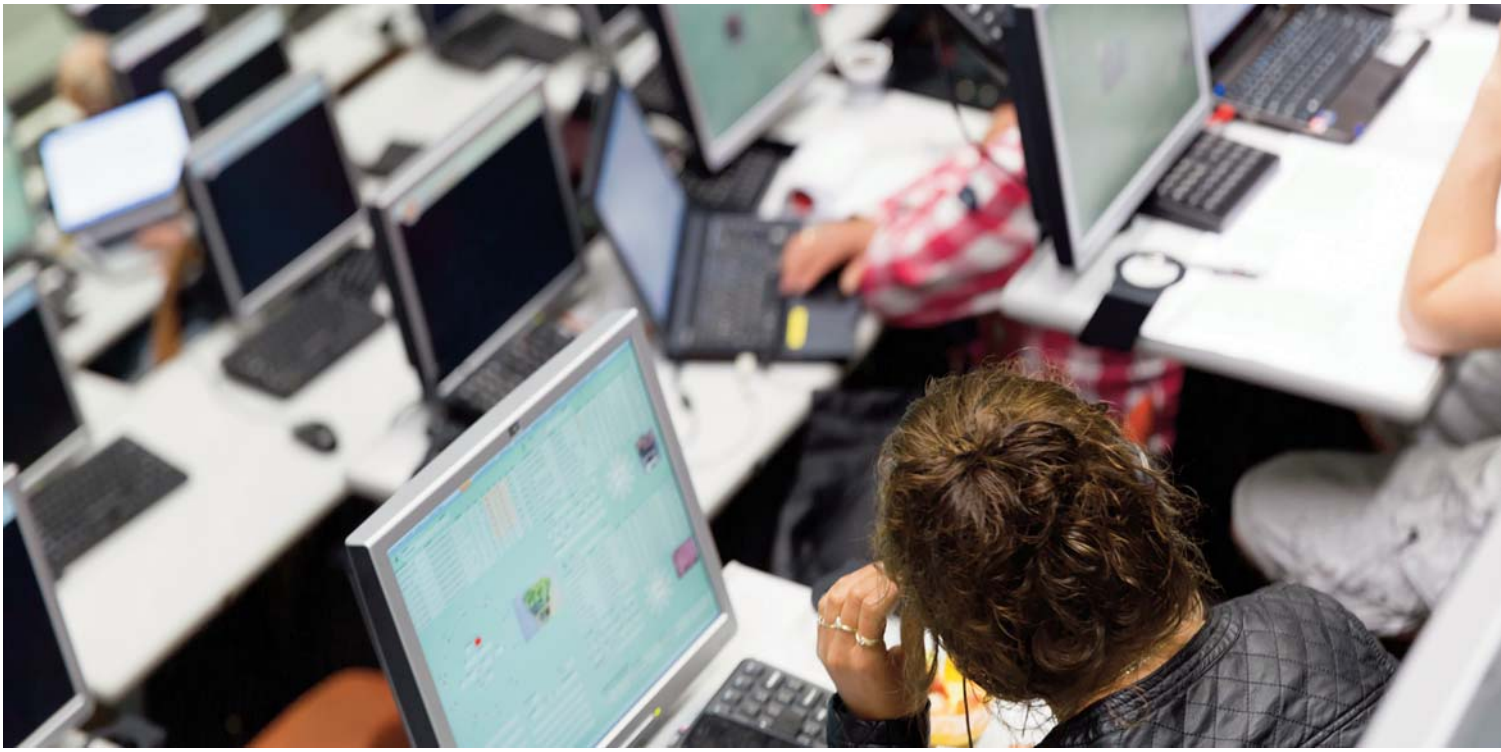
Krok 4

Analityka, automatyka, internet rzeczy – patrz szerzej

58%

respondentów na świecie korzysta z prywatnych chmur

Prawie połowa zbadanych organizacji organizacji używa jakiejś formy chmury obliczeniowej. Najbardziej rozpowszechnione jest wykorzystywanie publicznych chmur, na takie rozwiązanie wskazało 54% badanych. Na dalszej pozycji znalazł się model prywatny i hybrydowy. Na świecie z prywatnych chmur korzysta 58% respondentów, z publicznych 33%, zaś z hybrydowych 30%. Co więcej, na świecie 47% respondentów wskazało, że ich firmy opracowały strategię ochrony danych w chmurze, opracowanie takiego dokumentu podmiotom zewnętrznym zleciło 29% przedsiębiorstw. Korzystanie z rozwiązań chmurowych na świecie stało się już dosyć powszechne. Pozostaje jednak ciągle pytanie o stabilność takich usług. Spektakularne awarie chmur Amazon i Microsoftu w ciągu 2016 i 2017 roku pokazują, że pomimo wielkich nakładów, nie są to rozwiązania całkowicie niezawodne.



Analityka dużych zbiorów danych

Z własnych lub zewnętrznych narzędzi do analizy dużych zbiorów danych korzysta w Polsce 13% badanych organizacji, zaś 7% deklaruje, że jest to ich priorytet na nadchodzące 12 miesięcy. Ogółem warto podkreślić niewielką liczbę takich firm i fakt, że 41% spółek w ogóle nie planuje wdrażać tego typu rozwiązań. Na tle wyników globalnych nasz kraj wypada raczej mizernie. Na świecie z tego rodzaju rozwiązań korzysta 43% badanych spółek, zaś w ciągu najbliższych 12 miesięcy zamierza je wdrożyć kolejnych 24% organizacji. Jedynie nieco ponad 11% firm nie zamierza implementować takich narzędzi.

Podobnie jak w przypadku dużych zbiorów danych, również w przypadku internetu rzeczy (IoT) polskie firmy nie są bardzo zaawansowane. 53% respondentów wskazało, że w ich firmach to rozwiązanie nie jest wykorzystywane, jedynie 5% zadeklarowało, że ich firmy wykorzystują tę technologię. W tej sytuacji nie powinno dziwić, że większość firm nie ma opracowanej strategii bezpieczeństwa w zakresie internetu rzeczy. Taki rozkład odpowiedzi pozwala postawić tezę, że dla polskich przedsiębiorstw temat bezpieczeństwa IoT w zasadzie nie istnieje.

Bezpieczeństwo systemów przemysłowych (OT – operational technology)

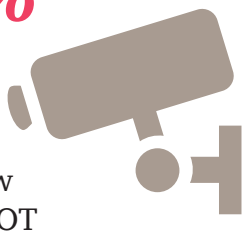
Systemy OT odpowiadają za podtrzymanie kluczowych procesów technologicznych w firmach. Cyberataki na to środowisko mogą mieć poważne i daleko idące konsekwencje. Poza stratami finansowymi, możliwe są przedłużające się przerwy w dostawie usług krytycznych, szkody wyrządzone środowisku naturalnemu, a nawet zagrożenie zdrowia i życia ludzkiego.

Wysoko wykwalifikowani i zmotywowani przestępcy aktywnie starają się wykorzystać słabości zabezpieczeń w sieciach OT, systemach sterowania procesami i infrastrukturze krytycznej. Ich motywacje wahają się od korzyści ekonomicznych i szpiegostwa, przez chęć złośliwego zakłócenia pracy.

Jak ukazały wyniki pogłębionych wywiadów w dużych firmach, respondenci doskonale zdają sobie sprawę z tego, jak poważne następstwa mogą za sobą pociągać incydenty w obszarze bezpieczeństwa OT. 64% ankietowanych wskazało, że ich efektem może być przerwanie procesów technologicznych w firmach. 43% wyraziło przekonanie, że incydenty mogą spowodować wyciek wrażliwych informacji, 41% obawia się, że może dojść do uszkodzeń infrastruktury, co pociągnie za sobą znaczące koszty.

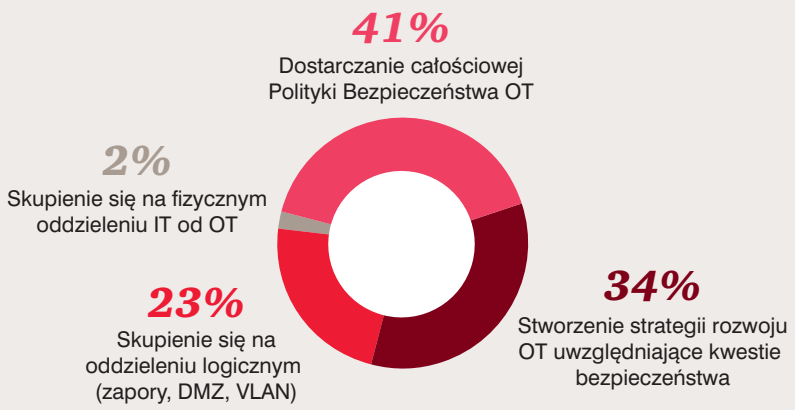
Jako źródła incydentów 68% respondentów wskazało na nieautoryzowany dostęp z wnętrza organizacji. To oznacza, że podobnie jak w przypadku IT największe zagrożenie (choć warto podkreślić, że często nieświadomie) stanowią sami pracownicy.

68%



incydentów systemów OT to nieautoryzowany dostęp

Najważniejsze elementy zapobiegania incydentom bezpieczeństwa OT



Zdaniem przeszło 60% ankietowanych procesy, które wspierają systemy automatyki przemysłowej (OT), związane z zarządzaniem incydentami bezpieczeństwa w przedsiębiorstwie, wymagają zmian. Wynika to z niskiej dojrzałości środowisk OT w kontekście monitorowania zdarzeń bezpieczeństwa i często nieprzygotowania architektury oraz służb do obsługi takich zdarzeń. Systemy OT były projektowane często w celu podtrzymania procesu technologicznego, głównie koncertując się na kwestii dostępności. Obecne służby utrzymania stoją przed ryzykiem wystąpienia zagrożeń, które w świecie IT są już uwzględniane systemowo w myśl zasady *„Security by design”*. Bezpieczeństwo systemów OT było zapewnione głównie poprzez galwaniczne rozłączenie od innych sieci komputerowych. Obecnie wymagania biznesowe oraz przenikanie się środowisk uniemożliwiają zachowanie tego stanu rzeczy. Panaceum na tą sytuację jest spojrzenie na systemy OT w kontekście rozdzielenia logicznego i monitorowania zdarzeń bezpieczeństwa, co wymaga zmian w podejściu.

Nadal w firmach spotyka się lokalne zarządzanie dostępem do systemów IT/OT i brak jednolitych standardów stacji dyspozytorskich. To podejście, co do zasady miało sens w skali pojedynczego zakładu, a nie obecnie, gdy systemy poszczególnych jednostek stanowią całość, lub wymieniają się informacjami. Aktualnie wskazane jest wprowadzenie centralnego zarządzania uprawnieniami i monitorowanie zdarzeń, co wymaga znaczących zmian w architekturze systemów OT. Brak globalnego podejścia w skali przedsiębiorstwa powoduje, że polityki zarządzania dostępem nie są spójne i wielokrotnie nieweryfikowane (monitorowane). Każda taka zmiana wymaga nakładów finansowych i – co ważniejsze – umiejętnego zaprojektowania, aby nie przerwać procesu technologicznego (niektóre z tego typu procesów wymagają nadzoru i sterowania 24h na dobę).

Również wąska grupa specjalistów rozumiejących OT i jednocześnie znających świat IT w kontekście bezpieczeństwa wpływa na to, że zmiany zachodzą powoli.

Dla 53% respondentów czynnikiem napędowym zmian w ramach środowiska OT w ich firmie są względy bezpieczeństwa. Bezpieczeństwo w OT wymaga holistycznego podejścia w skali przedsiębiorstwa i stworzenia mapy drogowej zmian, jednak nie jak w IT na kilka lat, ale na dekadę lub nawet więcej. Jest to związane z tym, że w niektórych przypadkach prace mogą być wykonane tylko w momencie przerwy technologicznej i w połączeniu z innymi pracami. Koszty wyłączenia i ponowny rozruch urządzeń są ogromne, a wielokrotnie nie jest to możliwe.

72% respondentów stwierdziło, że wdrożeniami związanymi z bezpieczeństwem OT zajmie się zespół do spraw OT, 51% wskazało na dział IT, zaś 44% na doradców merytorycznych lub konsultantów (możliwy był wybór kilku odpowiedzi).

Aspekty bezpieczeństwa OT, na których będą koncentrować się polskie firmy w przyszłości to monitoring i narzędzia analizy informacji (takie jak SIEM), tak uznało 76% ankietowanych. Na drugim miejscu, wskazana przez 42% respondentów znalazła się konieczność poprawy świadomości i kompetencji pracowników. Bardzo ważna jest również ściślejsza współpraca z IT oraz tworzenie interdyscyplinarnych zespołów.

Ochrona biznesu w cyfrowej transformacji

Metodyka Badania

Raport został przygotowany na bazie badania, w którym wzięło udział 100 dużych i średnich polskich firm. Badanie zostało przeprowadzone jesienią 2016 roku metodą ankiety online. Aspekty bezpieczeństwa automatyki przemysłowej (OT) zostały zbadane w ramach wywiadów pogłębionych. Wyniki badania zostały opracowane na podstawie agregacji udzielonych odpowiedzi.

Polskie badanie jest częścią międzynarodowego projektu *The Global State of Information Security® Survey 2017*, który bada 133 kraje pod kątem stanu bezpieczeństwa informacji.

Kontakt

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

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

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

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

pwc.pl/stanbezpieczenstwa