aut. Andrzej Kozłowski 30.11.2017

ZNACZENIE BEZPIECZEŃSTWA DANYCH W FIRMIE - WYNIKI BADANIA RYNKU CYBERBEZPIECZEŃSTWA W POLSCE 2017 [ANALIZA]

Co czwarta firma w Polsce nadal nie wie, jakie zmiany będzie musiała wdrożyć w związku z wejściem Rozporządzenia o Ochronie Danych Osobowych (GDPR) w maju 2018 roku. Blisko połowa przedsiębiorstw nie zarejestrowało żadnego cyberataku na swoje zasoby. W przypadku odnotowanych zdarzeń firmy najczęściej wskazywały na cyberataki z wykorzystaniem złośliwego oprogramowania. Wynika z raportu podsumowującego Badanie Rynku Cyberbezpieczeństwa w Polsce w dużych i średnich firmach przygotowanego na zlecenie T-Mobile.

Stan przygotowań do GDPR

Raport „Badanie rynku cyberbezpieczeństwa w Polsce 2017" powstał w newralgicznym dla przedsiębiorców momencie. W maju 2018 roku zacznie obowiązywać Rozporządzenie o Ochronie Danych Osobowych (GDPR), które będzie dotyczyło wszystkich firm działających na obszarze Unii Europejskiej. Nowe przepisy znacznie rozszerzają odpowiedzialność i obowiązki związane z ochroną danych osobowych oraz raportowaniem związanych z nimi incydentów. To ogromna zmiana w stosunku do dotychczasowych przepisów. Do tej pory takie restrykcyjne podejście obejmowało jedynie wybrane branże, m.in. banki oraz operatorów telekomunikacyjnych. Teraz uchybienia w systemach IT będą musiały zlikwidować wszystkie przedsiębiorstwa, niezależnie od prowadzonej działalności.

Czasu pozostało bardzo mało. Mimo to, ponad połowa firm biorących udział w badaniu nie podjęła jeszcze albo kroków, które oceniłyby wpływ RODO na ich działalność albo działań w celu dostosowania się do regulacji. Przedstawiciel co piątej dużej i średniej firmy działającej w Polsce uważa, że rozporządzenie RODO nie ma wpływu na jego firmę i nie będzie trzeba się do niego dostosowywać. Warto również zaznaczyć, że co czwarta badana firma nie spotkała się nigdy wcześniej z określeniem RODO/GDPR.

> *Postanowiliśmy, jeszcze przed wejściem RODO w życie, sprawdzić podejście do zagadnień związanych z cyberbezpieczeństwem w polskich firmach. Badanie obejmowało przeprowadzenie niemal 700 wywiadów zarówno w dużych spółkach, jak i średnich firmach. Położyliśmy w nich nacisk na zagrożenia cyberatakami, rozwiązania zapewniające bezpieczeństwo IT, wydatki ponoszone na budowę i utrzymanie infrastruktury ICT oraz znaczenie firm zewnętrznych i własnych*

> *specjalistów w zakresie ochrony zasobów przedsiębiorstwa. Wyniki przeprowadzonego badania stanowią swoistą diagnozę potrzeb firm w obszarze outsourcingu usług cyberbezpieczeństwa. Jako firma od lat specjalizująca się w monitorowaniu ataków i ochronie danych partnerów biznesowych, zwracamy na to szczególną uwagę, przygotowując produkty i usługi dla przedsiębiorców. Obraz, który udało nam się uchwycić, mówi wiele o postrzeganiu cyberbezpieczeństwa przez polskie firmy*
>
> *Artur Ostrowski - Członek Zarządu, Dyrektor ds. Rynku Biznesowego w T- Mobile Polska S.A.*

Poziom cyberbezpieczeństwa musi wejść na wyższy poziom

Obserwacje prowadzone na całym świecie wskazują, że praktycznie każda infrastruktura dostępna w Internecie poddawana jest atakom. Szerokim echem odbiły się ostatnio dwie duże kampanie malware – WannaCry i NotPetya. Ta druga dotknęła polskie firmy współpracujące z Ukrainą i została dobrze zapamiętana przez przedsiębiorców. W wynikach badań potwierdza to wysoki procent ataków na firmy związane z transportem i logistyką. W sumie 48% firm (w tym 51% respondentów z sektora średnich przedsiębiorstw i 45% dużych spółek) zadeklarowało, że nie padło ofiarą cyberataku. Taki wynik może świadczyć o niskiej kondycji cyberbezpieczeństwa w Polsce. Przyjmuje się, że praktycznie każda infrastruktura dostępna w Internecie poddawana jest atakom. Czas wykrycia poważnego incydentu często zajmuje miesiące, a nawet lata. Dane te odzwierciedlają zatem niską jakość stosowanych metod monitorowania i rejestracji incydentów w polskich firmach, które ignorują nadzorowanie stanu bezpieczeństwa swoich zasobów i opóźniają wykrycie udanych ataków cybernetycznych.

Głównym celem cyberataku jest użytkownik. Najczęstszym wektorem ataków jest złośliwe oprogramowanie, któremu uległo łącznie 37% respondentów. Ataków na komputery pracowników doświadczyło ogółem 14% badanych firm

> *Popularność tego typu ataków związana jest z najsłabszym ogniwem w łańcuchu zabezpieczeń, czyli aktywnością człowieka. O wiele łatwiej jest uśpić czujność użytkownika niż przełamać techniczne zabezpieczenia, co potwierdzają dane zgromadzone w badaniu.*
>
> *Arkadiusz Buczek - Główny Specjalista ds. Cyberbezpieczeństwa, T-Mobile Polska S.A.*

Duże firmy, z racji skali swojej działalności, znacznie częściej niż średnie przedsiębiorstwa bywają celem bezpośrednich ataków, takich jak: ataki na serwery firmowe (15%), zasoby WWW (13%) czy bazy danych (8%).

> *Ataki na systemy informatyczne nie są już przedmiotem zainteresowania wyłącznie specjalistów ds. bezpieczeństwa informacji i IT. Ich konsekwencje są odczuwalne zarówno dla zarządów firm i innych interesariuszy, jak również klientów. Przyglądając się opracowanym przez nas materiałom, należy pamiętać, że na funkcjonowanie cyberbezpieczeństwa wpływa także intensywny rozwój cyberzagrożeń, które charakteryzują się coraz wyższym stopniem zaawansowania. Wszyscy możemy więc na co dzień obserwować wpływ tych niebezpiecznych przemian na działalność biznesową wielu firm – 51% firm stało się ofiarami cyberataków, a 93% dużych przedsiębiorstw zostało zaatakowanych tylko w 2016 roku. Straty z tym związane szacowane są łącznie na 200 mld euro w Europie, a w skali świata na 450 mld euro. Cyberbezpieczeństwo stało się zatem koniecznością dla biznesu, a nie jedynie opcją.*
>
> *Włodzimierz Nowak - Członek Zarządu, Dyrektor ds. Prawnych, Bezpieczeństwa i Zarządzania Zgodnością w T-Mobile Polska S.A*

Mimo rozwoju technologii cyberzabezpieczeń, firmy wciąż ufają rozwiązaniom takim jak firewall i antywirus, które od pewnego czasu uznawane są za niewystarczające. Największą popularnością wśród badanych cieszą się produkty firm Cisco Systems, Fortinet i Eset. Niepokojący jest fakt, że choć poziom zaawansowania cyberataków znacznie wzrósł, to sposoby zabezpieczeń mają się nie zmienić – te same rozwiązania znalazły się na liście priorytetów na najbliższe 1-2 lata. Wynika to z niewielkiej wciąż świadomości cyberzagrożeń w przedsiębiorstwach. Większość przedsiębiorstw nie tworzy oddzielnych stanowisk dla osób, których podstawowym obowiązkiem jest dbanie o bezpieczeństwo. Obowiązki te przydzielane są zazwyczaj pracownikom działu IT – administratorom systemów i/lub sieci. Większość firm inwestuje we własny sprzęt i ludzi (80%), natomiast z outsourcingu ekspertów lub zasobów korzysta co szóste przedsiębiorstwo. Jednak poziom zaufania do zewnętrznych dostawców, w szczególności operatorów usług z zakresu bezpieczeństwa, powinien z każdym rokiem rosnąć. Wynika to przede wszystkim z ograniczonej liczby kompetencji w kwestii cyberbezpieczeństwa na rynku oraz wysokich kosztów zatrudnienia specjalistów pokrywających wszystkie obszary zabezpieczeń środowiska IT.

Choć obraz wyłaniający się z przedstawionych danych może wydawać się niepokojący, warto zaznaczyć, że przeszło 71,5% dużych i średnich firm przeprowadza testy penetracyjne sprawdzające poziom ich zabezpieczenia przed atakami. Wystawianie systemu na próbę jest jednak niewystarczające, by zagwarantować ochronę zasobom przedsiębiorstwa. Pentesty powinny być przeprowadzane regularnie, przez wysoko wykwalifikowanych specjalistów, a zalecenia płynące z diagnozy muszą być wdrożone, by testy odniosły pożądany skutek. Wciąż 87% podmiotów deklaruje także, że nie będzie korzystać z usług operatorów zapewniających profesjonalne wsparcie w zakresie cyberbezpieczeństwa. Dopóki więc firmy nie zaczną stawiać na ekspertów, stan bezpieczeństwa IT w Polsce długo może pozostawiać wiele do życzenia.

Tylko jedna trzecia średnich firm przeprowadziła audyt bezpieczeństwa informacji pod kątem zgodności z normą ISO 27001. Częściej na przeprowadzenie audytu wskazywali przedstawiciele dużych firm (43% w stosunku do 33% w grupie średnich przedsiębiorstw).

W ciągu najbliższych 2 lat badane firmy z sektora dużych i średnich przedsiębiorstw nie planują

większych zmian w działaniach związanych z cyberbezpieczeństwem. Podstawowe zabezpieczenia będą oparte na oprogramowaniu antywirusowym oraz zaporach sieciowych. Ponadto nadal dużą uwagę będą przywiązywać do rozwiązań, mających na celu zapewnienie bezpieczeństwa baz danych.

Wydatki dużych i średnich przedsiębiorstw poniesione z tytułu działań w obszarze cyberbezpieczeństwa kształtują się na relatywnie niskim poziomie. Trzy czwarte badanych firm zadeklarowało, że na ten cel w 2016 r. przeznaczyło mniej niż 50 tys. zł. Warto też zwrócić uwagę na fakt, że ok. 7% dużych firm działających w Polsce przeznaczyło w ubiegłym roku ponad 1 mln zł na działania w obszarze cyberbezpieczeństwa.

Nie jest zaskakujące, że duże firmy przeznaczały w 2016 r. większe kwoty na cyberbezpieczeństwo niż średnie przedsiębiorstwa. Wyższe koszty były związane z większymi przychodami, które na ogół wypracowują duże podmioty, oraz z większymi zasobami IT do zabezpieczenia. Struktura wydatków na działania w obszarze cyberbezpieczeństwa w dużych i średnich firmach nieznacznie się różni. O ile średnie firmy wydają mniej więcej tyle samo na sprzęt oraz oprogramowanie, to duże firmy nieco większe kwoty przeznaczają na sprzęt. Zwiększenie budżetu na działania w obszarze cyberbezpieczeństwa w 2017 r. rozważa jedynie co piąta średnia i co trzecia duża firma.

> *Zgodnie z najlepszymi praktykami budżet przeznaczany na cyberbezpieczeństwo powinien stanowić nie mniej niż 10% budżetu IT. Dlatego wydatki do 50 tys. odnotowane u 84% średnich przedsiębiorstw mogą odzwierciedlać racjonalny poziom kosztów ponoszonych przez firmy, choć wydają się one nieproporcjonalnie małe w stosunku do kar, które będą obowiązywały w ramach RODO/GDPR. Większość respondentów nie planuje podniesienia wydatków na bezpieczeństwo – dynamika zmian na poziomie 6–7% wskazuje raczej na wzrost inflacyjny niż inwestycję w nowe rozwiązania. Stagnacja w obszarze zabezpieczeń jest niepokojąca i wynika z braku świadomości zagrożeń. W przypadku, gdy firmy nie widzą skutków ataków, konsekwencją jest zaniechanie inwestycji w dodatkowe zabezpieczenia. Równocześnie korzystanie z usług pentestów wzmacnia przeświadczenie o byciu twierdzą nie do zdobycia, co powoduje, że w rezultacie przedsiębiorstwa pozostają w tym samym miejscu – z zabezpieczeniami w postaci firewalla, antywirusa, bez procedur zarządzania bezpieczeństwem*
>
> *Arkadiusz Buczek - Główny Specjalista ds. Cyberbezpieczeństwa, T-Mobile Polska S.A.*

Przedstawiciele 80% badanych firm z sektora dużych i średnich przedsiębiorstw zadeklarowali, że sami kupują, wdrażają oraz zarządzają rozwiązaniami z zakresu cyberbezpieczeństwa. Obawy o wyższe koszty są szczególnie widocznie wśród średnich firm, co jest zrozumiałe, gdyż generują one niższe przychody niż duże firmy. Dwie piąte dużych i tylko co piąta średnia firma zatrudnia specjalistę odpowiedzialnego za obszar bezpieczeństwa cyfrowego. Większe firmy częściej decydują się na zatrudnienie specjalnej osoby odpowiedzialnej za cyberbezpieczeństwo, ponieważ – jak wynika z

deklaracji badanych – częściej borykają się z problemem cyberataków.

Najważniejszy wniosek to rosnące znaczenie cyberbezpieczeństwa, które znajduje się na liście priorytetów polskich firm, jeśli chodzi o wydatki na IT. Nie powinno to specjalnie dziwić, bo temat jest wielowymiarowy. Zapewnienie bezpieczeństwa ważne jest w każdym przypadku: chmury, dostępu zdalnego, utrzymania infrastruktury własnej, wykorzystania bardziej zaawansowanych narzędzi analitycznych, Internetu Rzeczy itp. Można się spierać, na ile jest to teoria i tylko deklaracje, że bezpieczeństwo ma priorytet, ale faktem jest, że presja rośnie. Najmocniej oczywiście działają bezpośrednie, negatywne doświadczenia i straty własne, ale swoje robi też stale rosnący poziom zagrożeń cyberatakami, malware i ransomware. Dodatkowo pojawienie się nowych regulacji unijnych w obszarze danych osobowych (RODO) tylko wymusza dostosowanie się firm i potencjalne inwestycje.