aut. Ireneusz Piecuch 28.08.2019

STRATEGIĄ W CYBERZAGROŻENIA. PERSPEKTYWA BIZNESU [KOMENTARZ]

Rok temu weszły w życie przepisy ustawy ustanawiającej Krajowy System Cyberbezpieczeństwa. Na początku sierpnia ukazał się natomiast, przeznaczony do konsultacji, projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024. Czy dokument ten wniesienie coś nowego z punktu widzenia polskich przedsiębiorstw?

Rok temu weszły w życie przepisy ustawy ustanawiającej Krajowy System Cyberbezpieczeństwa. Po raz pierwszy w polskim ustawodawstwie, doczekaliśmy się kompleksowej regulacji obejmującej całe sektory polskiej gospodarki, w tym również sektor paliwowo-energetyczny, sektor transportu, bankowości, ochrony zdrowia czy też sektor infrastruktury cyfrowej. Regulacje, stanowią implementację dyrektywy NIS z roku 2016 - pierwszego poważnego kroku na drodze do zbudowania jednolitego, europejskiego systemu ochrony przed cyberzagrożeniami.

Od tego czasu pojawiło się kilka rozporządzeń wykonawczych (niektóre wzbudzając mocne kontrowersje). Tempo wdrożenia ustawy wydaje się jednak dalekie od zakładanego. Do maja bieżącego roku, a więc po ponad pół roku od wejścia w życie ustawy, mówiło się o około 70 wydanych decyzjach uznających poszczególne spółki za te świadczące usługi krytyczne (na około 500 przedsiębiorstw, które taką decyzje powinny otrzymać).

Na początku sierpnia ukazał się natomiast, przeznaczony do konsultacji, projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 (dalej przywoływanej jako „Strategia"), który w zamyśle ma zastąpić obowiązujące obecnie Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022. Jako, że dokument ten powstawał w okresie wdrażania ustawy o KSC, powinien on już odzwierciedlać pierwsze doświadczenia wynikające z tego procesu, jak również zmiany w ustawodawstwie europejskim, do których doszło w bieżącym roku. Czy tak jest w istocie?

Wizja i cele

Jak można przeczytać w mądrych książkach dobra Strategia potrzebuje najpierw zdefiniowania wizji. I tu, bez zdziwienia (przynajmniej bez zdziwienia wszystkich związanych z tematem), możemy przeczytać, że pomyślny rozwój naszego kraju jest związany ze „sprawnym i bezpiecznym działaniem systemów informatycznych i środków komunikacji elektronicznej". Stąd już tylko krok od stwierdzenia, że rząd nie poprzestanie jedynie na wdrożeniu ustawy o KSC, ale zamierza systematycznie wzmacniać i rozwijać ów system. To jasny sygnał dla wszystkich tych, którzy ustawili ustawę o KSC w szeregu innych ustaw związanych z zapewnieniem zgodności regulacyjnej i uznali jej wdrożenie za wydarzenie

jednostkowe. Jednak KSC w obecnym kształcie to dopiero początek a rozwój Krajowego Systemu Cyberbezpieczeństwa został wymieniony jako cel szczegółowy Strategii nr 1.

Na kolejnych miejscach znalazło się „stymulowanie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności skutecznego zapobiegania incydentom". I ten cel nie powinien budzić wątpliwości, zwłaszcza jeśli wziąć pod uwagę to, że od wystąpienia incydentu do jego wykrycia, wedle różnych opracować mija od 50 do 90 dni. Cel 3 wiąże się ze zwiększeniem potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni. Cel 4 odwołuje się do jakże istotnej kwestii budowania świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa a cel 5 deklaruje odgrywanie aktywnej roli na arenie międzynarodowej.

Z punktu widzenia przedsiębiorstw, z pewnością warto się bliżej przyjrzeć dwóm pierwszym celom.

Regulacje sektorowe i efektywność KSC na celowniku

Uchwalenie KSC trzeba traktować jako początek a nie koniec prac legislacyjnych w obszarze cyberbezpieczeństwa. Strategia zakłada, że Minister Cyfryzacji, we współpracy z innymi resortami, dokona przeglądu regulacji sektorowych i szczególnych i to nie tylko tych dotyczących cyberbezpieczeństwa lecz również takich które, mogą mieć wpływ na ochronę danych osobowych czy też na infrastrukturę krytyczną. Strategia zapowiada też podjęcie działań legislacyjnych w obszarze wytwarzania, posiadania, pozyskiwania oraz wykorzystywania narzędzi podwójnego zastosowania do prowadzenia działań defensywno-ofensywnych w cyberprzestrzeni. Zmiany szykują się także w obszarze prawa telekomunikacyjnego a dotyczyć będą zapewnienia wymogów bezpieczeństwa, które firmy telekomunikacyjne będą musiały spełniać przy budowie sieci 5G.

Równolegle do intensywnych prac legislacyjnych, Strategia przewiduje uruchomienie w roku 2021 systemu teleinformatycznego (zapowiedzianego już w przepisach ustawy) wspierającego zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym oraz ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Specjalną uwagę należałoby jednak poświęcić kolejnemu ustępowi Strategii, który co prawda odnosi się do samorządów, ale z uwagi na swoją istotę, jest adekwatny także dla przedsiębiorstw (zarówno publicznych jak i prywatnych). Chodzi tu mianowicie o rekomendację korzystania z „nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych". Temat przetwarzania w chmurze pojawia się od czasu do czasu, głównie w kontekście zagrożeń – w tym zagrożeń cyberbezpieczeństwa systemów IT. Mimo, że polityka Unii Europejskiej w tej kwestii jest oczywista i przetwarzanie w chmurze jest jednym z filarów budowy cyfrowej Europy, Polska w tej mierze wlecze się w końcówce państw europejskich razem z Bułgarią i Rumunią. Rekomendacja korzystania z chmury w połączeniu z planami opracowania zbioru wymagań organizacyjnych i technicznych dotyczących jej bezpieczeństwa, może pomóc w przełamaniu niechęci do korzystania z tego narzędzia.

Szacowanie ryzyka oraz Narodowe Standardy Cyberbezpieczeństwa

Praktycznym elementem Strategii może okazać się przygotowanie i wdrożenie wspólnej

metodyki statycznego i dynamicznego szacowania ryzyka, uwzględniającego specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, usług kluczowych i dostawców usług cyfrowych. Należy się zgodzić z autorami Strategii, że udostępnienie takiego narzędzia doprowadzi do porównywalności szacowań co z kolei umożliwi lepsze zobrazowanie poziomu ryzyka – także w skali całego kraju. Mankamentem jest harmonogram przewidujący wprowadzenie tego narzędzia dopiero pod koniec 2020 roku.

Narodowe Standardy Cyberbezpieczeństwa mają być w zamierzeniu twórców Strategii zbiorem wymagań organizacyjnych i technicznych dotyczących bezpieczeństwa aplikacji, urządzeń mobilnych, stacji roboczych, serwerów i sieci oraz modeli chmur obliczeniowych. Wspierane przez Polskie Normy oraz aktywne włączenie się Polski w realizację planu ustanowienia europejskich programów certyfikacji zgodni z nowym unijnym rozporządzeniem z 17 kwietnia 2019 roku w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych, mają stworzyć ekosystem, który pozwoli polskim przedsiębiorcą na uzyskiwanie niezbędnych certyfikatów uznawanych w UE a w konsekwencji na skuteczne konkurowanie na jednolitym rynku cyfrowym unii.

Finansowanie, czyli pięta achillesowa Strategii

Kiedy rok temu pisałem o wyzwaniach wdrożeniach KSC wskazywałem na źródła finansowania, wyjątkowo mętnie wpisane w samą ustawę i jej uzasadnienie. Przywoływałem wtedy druzgocący w swojej wymowie raport NIK dotyczący cyberbezpieczeństwa z 2015 roku, który wskazywał, że braki w skoordynowanym podejściu do problemu to jedno, ale zupełny brak systemu finansowania wspierającego działania mające zwiększy poziom cyberbezpieczeństwa to absolutny skandal. Raport ten przypomniał mi się przy lekturze ostatniego, obejmującego trzy krótkie paragrafy rozdziału 11 zatytułowanego „Finansowanie". Warto zacytować tu ostatni paragraf: „Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażaniu Strategii Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej, w miarę zaistnienia takich możliwości".

Jak to jest z tymi cyberzagrożeniami?

Ktoś powie strategia jak strategia. Dużo ogólnych sformułowań, ale jak to będzie działać w praktyce? Ponad rok obowiązywania ustawy o KSC pokazuje, że z tym bywa różnie. Są przedsiębiorstwa, w których cyberbezpieczeństwo od dawna wpisane jest w DNA firmy z uwagi na olbrzymią rolę jaką przedsiębiorstwa te przywiązują do zaufania klientów. Dobrym przykładem są tu banki. Są też przedsiębiorstwa, gdzie z miejsca zadekretowano, że to temat dla IT, zupełnie ignorując badania pokazujące, iż przyczyną większości problemów (ponad 70%) jest błąd człowieka – i to bardzo rzadko pracownika działu IT. Szefowie spółek z którymi rozmawiam często kiwają ze zrozumieniem głowami, wspominając, że może uda im się zwiększyć nakłady na cyberbezpieczeństwo … w przyszłorocznym budżecie, szybko zastrzegając jednak, że może być różnie, bo projekty nastawione na wzrost przychodu (lub ograniczenie kosztów) mają absolutny priorytet. Słucham tego wszystkiego i myślę, że warto byłoby zacząć od początku.

Więc jeszcze raz. Cyberprzestępczość to nie działalność kilku nawiedzonych hackerów w

wyciągniętych swetrach. To olbrzymi, świetnie zorganizowany przemysł, za którym stoją nie tylko zorganizowane grupy przestępcze, ale całe państwa. Co warte podkreślenia, cyberprzestępcy są w absolutnej czołówce „przedsiębiorców" korzystających z najnowszych rozwiązań cyfrowych. Ba, wydają na rozwój, badania i inwestycje dziesięciokrotnie więcej niż przedsiębiorstwa na zabezpieczenia (specjaliści mówią o nakładach rzędu biliona dolarów).

Przestępczość cyfrowa to biznes z definicji globalny. Nie zna granic czy problemów językowych a jego ofiarą może paść każdy.

Po stronie poszkodowanych mogą być osoby fizyczne, firmy, rządy i całe społeczeństwa. Centralny Bank Bangladeszu stracił ponad 80 milionów dolarów a był o krok od utraty miliarda. Rok przed tym wydarzeniem, bank postanowił dokonać przeglądu zabezpieczeń, ale proces zakupowy nie miał odpowiednio wysokiego priorytetu i trwał zbyt długo (sic!). Aramco – jeden z najbogatszych koncernów świata utracił miliony dolarów, po tym jak większość stacji roboczych koncernu została zainfekowana a zawarte na nich dane utracone. Irański projekt jądrowy został skutecznie opóźniony na lata po ataku wirusa Stuxnet. Equifax stracił miliony dolarów na dodatkowe nakłady IT a jego akcjonariusze dużą część wartości swoich akcji po wycieku 145 miliona danych klientów tej firmy, których można było uniknąć, gdyby firma wystarczająco szybko zareagowała na podatność swoich systemów. Taką listę można by mnożyć w nieskończoność, mimo że jak podają źródła brytyjskie, jedynie 13% incydentów związanych z cyberatakami jest ujawnianych przez zaatakowane firmy.

A mówimy tu tylko o historii. A jutro? Mamy już udokumentowane przykłady możliwości przejęcia kontroli nad urządzeniami wspomagającymi pracę serca (swego czasu, ówczesny wiceprezydent USA, Dick Chenney, przeszedł dodatkowy zabieg mający na celu wyłączenie modułu zdalnego sterowaniu w wszczepionym mu urządzeniu). Mamy przykłady zdalnego przejęcie kontroli nad systemem hamulcowym samochodu (większość produkowanych obecnie samochodów ma możliwość zdalnej współpracy z pokładowym systemem komputerowym). Wiemy o dokonanej z sukcesem penetracji infrastruktury krytycznej i wykorzystania zasobów informatycznych wspomagających jej pracę do …kopania bitcoinów. Internet rzeczy, e-zdrowie, sztuczna inteligencja niosą z sobą nowe obietnice, ale też nowe zagrożenia. Także i w tej mierze, cyberprzestępcy zdają się być o krok przed nami.

John Chambers, wieloletni szef CISCO powiedział, że firmy dzielą się na dwie kategorie. Te, które zostały zahakowane i wiedzą czym to smakuje, i te które zostały zahakowane, ale jeszcze o tym nie wiedzą. Bardzo dobrze, że powstaje nowa Strategia Cyberbezpieczeństwa RP. Świetnie, że osoby kreujące politykę państwa w tym zakresie potrafią zdefiniować klarowną wizję i cele. Konfrontując to jednak z rzeczywistością dnia codziennego oraz tempem wdrażania praktycznych mechanizmów zaszytych w KSC, należy pamiętać o tym, że wizja pozbawiona egzekucji jest niczym innym jak halucynacją.

Ireneusz Piecuch - Partner Zarządzający, Kancelaria IMP