Rozmawiamy z Karolem Okońskim, Sekretarzem Stanu, Pełnomocnikiem Rządu do spraw Cyberbezpieczeństwa w Ministerstwie Cyfryzacji

W jakim zakresie partnerstwo publiczno-prywatne może być szansą na realizację zadań z zakresu cyberbezpieczeństwa? Czy strategie rządowe w zakresie PPP i cyberbezpieczeństwa mają jakieś wspólne zakresy? Jak mogłaby wyglądać współpraca między sektorem publicznym i prywatnym?

Pojęcie partnerstwa publiczno-prywatnym w kontekście cyberbezpieczeństwa ma znaczenie szersze, niż zdefiniowane w ustawie o partnerstwie publiczno-prywatnym. Chodzi raczej o długotrwałą współpracę między podmiotami publicznymi i komercyjnymi, zarówno w wymiarze kraju, jak i międzynarodowym. Współpraca ta nie musi być skupiona na realizacji konkretnego przedsięwzięcia, ale może być nastawiona na wymianę informacji, ponieważ wiedza na temat zaistniałych incydentów jest kluczem do działań na rzecz zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Wymiana informacji na temat tego, co dzieje się w firmach, czy określonym sektorze gospodarki, pozwala na zdiagnozowanie potencjalnych zagrożeń i podjęcie odpowiednich środków zaradczych.

Inicjatywa „Partnerstwo dla cyberbezpieczeństwa" rozwijana przez Instytut NASK, której patronuje Ministerstwo Cyfryzacji, sprowadza się do dobrowolnego zawierania porozumień zarówno przez podmioty publiczne, jak i komercyjne pogrupowane sektorowo, które zobowiązują się do wzajemnego informowania o wykrytych zagrożeniach, czy ryzykach zdiagnozowanych w trakcie własnej działalności, otrzymując w zamian informacje o potencjalnych zagrożeniach wykrytych u innych podmiotów działających w tym samym obszarze rynku. Współpraca ma charakter barterowy, zawarcie

umowy nie jest związane z kosztami. NASK ma w tej współpracy rolę szczególną pełniąc funkcje edukacyjne, i jako lider partnerstwa dodatkowo organizuje stosowne sesje szkoleniowe oraz prowadzi działalność wydawniczą.

Ministerstwo, w kontekście obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], do podobnej współpracy zachęca samorządy wskazując, że nie zawsze sensowne jest samodzielne tworzenie w każdym samorządzie osobnych zespołów reagujących na naruszenia cyberbezpieczeństwa. Celowe jest powoływanie wspólnych struktur tego rodzaju, które mogłyby działać na rzecz kilku powiatów czy gmin. Współpraca taka jest bardziej efektywna, ponieważ możliwe jest działanie zdalne, a najważniejsza jest szybkość wymiany informacji.

Jaka jest skala współpracy między podmiotami zaangażowanymi w system cyberbezpieczeństwa?

Ustawa o krajowym systemie cyberbezpieczeństwa jest implementacją Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Obowiązuje od końca sierpnia 2018 r. i porządkuje jednocześnie wiele kwestii dodatkowych. W praktyce, trwają właśnie działania mające na celu wdrożenie przewidzianych w niej rozwiązań. Ustawa opisuje między innymi obowiązki operatorów usług kluczowych, spośród których część to przedsiębiorstwa komunalne lub Szpitalne Oddziały Ratunkowe. Status operatora usług kluczowych zyskuje się na mocy decyzji wydawanej przez tzw. organ właściwy, wskazany w ustawie zgodnie ze specyfiką branży, np. dla sektora finansowego jest to Komisja Nadzoru Finansowego. Rozporządzenie wykonawcze do ustawy wskazuje jednocześnie określone progi regulujące zakres obowiązków, proporcjonalny do znaczenia usług krytycznych, i ich powiązania z systemem informatycznym. Status operatora usług kluczowych, nadany w drodze decyzji administracyjnej, łączy się z koniecznością spełnienia obowiązków adekwatnych do natury świadczonych usług. Proces spełnienia wymogów ustawy jest dynamiczny, a sama decyzja określa również harmonogram wykonania określonych zadań wynikających z uzyskania statusu operatora usług kluczowych. W ocenie Ministerstwa Cyfryzacji, w skali całego kraju status operatorów usług kluczowych posiadać może około 500 podmiotów, z czego w toku jest około 400 postępowań, a wobec 150 wydano już stosowne decyzje. Jest to grupa przedsiębiorców prywatnych, spółek Skarbu Państwa, z czego część to jednostki zależne od samorządu. Poza grupą operatorów usług kluczowych obowiązki zgłaszania incydentów do CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, jak np. NASK) mają wszystkie podmioty publiczne. Pozwala to na uprzedzenie innych przed ryzykiem poniesienia konsekwencji podobnych, zaistniałych już incydentów naruszenia cyberbezpieczeństwa.

Jakie zadania, w obszarze regulowanym ustawą o cyberbezpieczeństwie, obciążają bezpośrednio samorząd?

Samorząd, jako organ administracji, nie jest adresatem decyzji przyznającej mu status operatora usług kluczowych. Jednak administracja samorządowa musi stworzyć warunki dla wywiązywania się z ciążących na niej obowiązków, np. wskazać osobę odpowiedzialną za dokonywanie odpowiednich zgłoszeń, a od wielkości gminy zależy skala spoczywających na niej zadań. Ministerstwo Cyfryzacji wspiera samorządy edukacyjnie, ponieważ przed wieloma niebezpieczeństwami uchronić można się za sprawą przestrzegania elementarnych zasad bezpieczeństwa w cyberprzestrzeni, co nie wymaga zaangażowania środków finansowych. Należy pamiętać, że cyberbezpieczeństwo wiąże się też z zapobieganiem naruszeń w obszarze ochrony danych osobowych, co może być bardzo dotkliwe dla samorządów. Należy pamiętać, że każdy operator usług kluczowych, w okresie dwóch lat po uzyskaniu swego statusu, powinien wykonać odpowiednie działania kontrolne, z których wynika zakres koniecznych działań wdrażających cyberbezpieczeństwo.

Czy wszystkie usługi i elementy infrastruktury, koniecznej do wywiązania się z ciążących na adresatach ustawy obowiązków (np. w zakresie centrum operacyjnego), muszą znajdować się w zasobach podmiotów publicznych?

Nie. Możliwe jest zlecanie tych zadań na zewnątrz. Jest to spójne z intencją ustawodawcy do wytworzenia rynku usług w tym zakresie, choć należy pamiętać, że zlecając realizację owych zadań przedsiębiorcy prywatnemu podmiot publiczny zachowuje odpowiedzialność za wywiązania się ze swych zadań. Ów podmiot zewnętrzny musi spełnić odpowiednie kryteria określone w ustawie. W wielu przypadkach outsourcing jest optymalnym rozwiązaniem.

Jest to logika wpisująca się w założenia partnerstwa publiczno-prywatnego. Czy Pana zdaniem możliwe jest, aby po stronie zamawiającego tego typu usługi występowało kilka podmiotów publicznych?

Jak to zasadne rozwiązanie. Jeśli znalazłoby się kilka podmiotów publicznych, które po przeanalizowaniu zasadności takiego podejścia chciałyby wspólnie udzielić zamówienia we wspomnianym zakresie, to Ministerstwo Cyfryzacji mogłoby

[1] Dz.U. 2018 poz. 1560

wesprzeć merytorycznie działania tej pilotażowej grupy. Wypracowane w ramach pilotażu rozwiązania mogłyby posłużyć za dobrą praktykę dla kolejnych chętnych.

Czy sektor prywatny jest przygotowany na podjęcie współpracy?

Wydaje się, że duże firmy działające w skali globalnej byłyby gotowe działać na naszym rynku tworząc lokalne oddziały. Problemem jest jednak obecnie mała skala polskiego rynku, która na razie nie uzasadnia stworzenia lokalnego ***data center***, z którego można byłoby świadczyć usługi chmurowe lub uruchomić oddział świadczący usługi specjalistyczne. Mam jednak nadzieję, że dynamika tego rynku wzrośnie i sytuacja w niedługiej perspektywie się zmieni - także za sprawą podejmowanych przez nas działań. W każdym przypadku zakładamy jednak, że serwery muszą znajdować się na terenie UE, a w pewnych przypadkach dodatkowe wymagania co do sprzętu i organizacji usług ze względu na wymogi bezpieczeństwa narodowego określić może np. ABW.

Jakie obszary współpracy są możliwe z punktu widzenia Ministerstwa Cyfryzacji?

Oprócz wspomnianej już wymiany informacji możliwe jest wdrażanie wspólnych projektów z zakresu badań i rozwoju technologii. Projekty takie mogą być finansowane albo ze środków UE, np. HORIZON 2020 czy HORIZON EUROPE. Jak praktyka pokazuje, są to środki dość trudno dostępne. Wymagają nawiązania współpracy między przedstawicielami przynajmniej paru podmiotów z różnych sektorów, w tym np. instytucji naukowych i przedsiębiorców oraz z różnych krajów, jednak ich zaletą jest możliwość uzyskania wsparcia na rozwiązania, które po wdrożeniu stanowią własność beneficjentów dotacji, w tym firm prywatnych, które mogą oferować na rynku wytworzone w ramach projektu usługi już na zasadach komercyjnych. W obszarze współpracy dotyczącej B+R dostępne są również środki Narodowego Centrum Badań i Rozwoju, który udziela wsparcia w ramach dwóch programów dedykowanych cyberbezpieczeństwu. Jeden z programów nazywa się CyberSecIdent i aktualnie trwa trzeci nabór wniosków w tym programie na ponad 200 mln zł dotacji. Kolejny program CertiSecPl jest skupiony na działaniach związanych z powołaniem polskiej jednostki certyfikacji i laboratoriów pozwalających oceniać zgodność urządzeń ze standardami Common Criteria (dotyczy to na przykład urządzeń kryptograficznych). Do tej pory polskie instytucje publiczne jak i firmy musiały uzyskiwać stosowne certyfikacje za granicą. Celem projektów jest stworzenie krajowych jednostek certyfikujących. Głównym celem tego projektu, jest wzrost konkurencyjności polskich rozwiązań w zakresie bezpieczeństwa teleinformatycznego przez stworzenie polskiego, nowoczesnego systemu oceny i certyfikacji bezpieczeństwa produktów i usług ICT (technologie informacyjno-komunikacyjne), funkcjonującego w europejskich ramach certyfikacji. Polską

jednostką certyfikacji będzie NASK. Co istotne dla współpracy między sektorami, w konkursach NCBiR mogą startować również podmioty komercyjne w partnerstwie z instytucjami badawczymi, przy czym często warunkiem uzyskania dotacji jest komercjalizacja wyników projektu, co powinno budować polski rynek wykonawców i ostatecznie wpłynąć na pobudzenie gospodarki. W zakresie rozwoju usług związanych z zastosowaniem chmury rozliczeniowej Ministerstwo Cyfryzacji spodziewa się, że mogą być one cenne dla samorządów, które zamiast budować własną serwerownię czy zatrudniać własnych ekspertów mogą wykupić kompleksową usługę. Natomiast, barierą w kontraktacji kompleksowych usług jest kompetentne przygotowanie dokumentacji przetargowej na tak skomplikowane usługi. Dlatego Ministerstwo Cyfryzacji planuje zorganizować przetarg ramowy, w którym planuje być liderem współpracując z chętnymi podmiotami administracji publicznej, które będą mogły zamówić u wyłonionych przez Ministerstwo dostawców potrzebne im usługi. Dzięki współpracy z Ministerstwem, zamawiający z administracji publicznej otrzymają stosowny katalog usług oferowany przez „sprawdzonych" dostawców oraz wzór umowy wykonawczej, która umożliwi im zakup bez konieczności samodzielnego organizowania skomplikowanego przetargu. Ministerstwo wzoruje się na modelu G-Cloud sprawdzonym w Wielkiej Brytanii.

Reasumując. Nie jest wykluczone, że jeśli odpowiednio duża grupa samorządów zdecydowałaby się na zakontraktowanie kompleksowych usług z zakresu cyberbezpieczeństwa w jednym przetargu, zastosowanie mógłby znaleźć również model PPP. Obecnie jednak kluczowe jest zachęcenie administracji publicznej do podejmowania wspólnych działań, np. w zakresie tworzenia wspólnych centrów operacyjnych we współpracy z sektorem prywatnym, szczególnie jeśli działałyby w jednym obszarze usług kluczowych. Ministerstwo Cyfryzacji chętnie zaangażuje się w merytoryczne wsparcie takiej inicjatywy.

Dziękuję za rozmowę.

Rozmawiał Bartosz Korbus