Cyberbezpieczeństwo – problem nas wszystkich?

Strategie państw UE wobec wyzwań związanych z dostępem do danych w sieci

Raporty i analizy 1 [5]/2015 www.csm.org.pl

CENTRUM STOSUNKÓW MIĘDZYNARODOWYCH

Raporty i analizy

EFNI
EUROPEJSKIE FORUM
NOWYCH IDEI

Tekst powstał jako materiał do dyskusji „Cyberbezpieczeństwo – problem nas wszystkich?
Strategie państw UE wobec wyzwań związanych z dostępem do danych w sieci”,
przeprowadzonej podczas Europejskiego Forum Nowych Idei w Sopocie 1 października 2015 r.

WSTĘP

1

Cyberprzestrzeń jest jednym z najszybciej rozwijających się obszarów zagrożeń współczesnego świata. Dotyczy nie tylko organów administracji państwowej, ale także biznesu i zwykłych użytkowników Internetu. Dynamika zmian zachodzących w środowisku bezpieczeństwa międzynarodowego oraz szybki rozwój technologii informatycznych zmuszają do zwrócenia szczególnej uwagi na bezpieczeństwo cyfrowe państwa i jego strategicznych zasobów.

Polska jest na początku tej drogi. Obecnie polski system bezpieczeństwa w cyberprzestrzeni nie jest przystosowany do narastających zagrożeń. W działaniach na rzecz poprawy sytuacji warto wykorzystać zarówno dyskusję na forum Unii Europejskiej, jak i doświadczenia poszczególnych państw członkowskich, zwłaszcza Wielkiej Brytanii i Estonii.

Często o cyberbezpieczeństwie rozmawia się w kategoriach skandalizujących wydarzeń, które dotyczą innych państw lub prywatnych osób bądź firm. Nierzadko postrzega się to zagadnienie jako temat zarezerwowany dla informatyków. Tymczasem bezpieczeństwo w cyberprzestrzeni nie jest problemem, którym powinni zajmować się jedynie informatycy. Nie jest także domeną wyłącznie administracji publicznej, lecz również administratorów sieci, prywatnych firm oraz zwykłych obywateli.

Cyberbezpieczeństwo to klasyczny przykład sprawy, która nie może być analizowana ani rozwiązana w ramach jednego sektora. Aby zapewnić państwu, instytucjom i obywatelom bezpieczeństwo cyfrowe, konieczne są dialog i partnerstwo wielu podmiotów. Dotyczy to zarówno strategii – która powinna być wypracowana dzięki współpracy między przedstawicielami administracji, tworzącymi plany działania, a biznesem, dysponującym doświadczeniem i wypracowanymi procesami eliminacji zagrożeń wynikających z bycia w sieci – jak i działań operacyjnych, podejmowanych przez administratorów sieci urzędów administracji publicznej i ich odpowiedników w firmach prywatnych. I nie może to być dialog pozorowany. UE i państwa członkowskie potrzebują spójnego systemu ochrony, opartego na standardach obowiązujących podmioty, których dotyczy tematyka cyberbezpieczeństwa (czyli *de facto* nas wszystkich). Ochrony w cyberprzestrzeni nie można zapewnić w izolacji od świata zewnętrznego.

Dlatego pozytywne wnioski dla stworzenia spójnego i efektywnego systemu ochrony może przynieść zarówno otwarcie się administracji na doświadczenia i sugestie podmiotów zewnętrznych dostarczających usługi, np. w zakresie przechowywania danych w chmurze, jak też czerpanie z doświadczeń i dobrych praktyk państw lepiej przygotowanych na zagrożenia w wymiarze cybernetycznym.

DZIAŁANIA NA RZECZ CYBERBEZPIECZEŃSTWA NA FORUM UE

W ostatnich latach na forum Unii Europejskiej podejmowane są inicjatywy na rzecz dostosowania regulacji z dziedziny cyberbezpieczeństwa do nowej rzeczywistości. W wielu państwach członkowskich i na poziomie UE brakowało do tej pory rozwiązań prawnych i instytucjonalnych w tej dziedzinie. Zmieni to przyjęcie dokumentu znanego jako *NIS Directive* (*Network and Information Security Directive*, dyrektywa o bezpieczeństwie sieci i informacji).

NIS Directive ma skupiać się na ochronie infrastruktury krytycznej państw, co pomoże administracji publicznej w skuteczniejszej ochronie wrażliwych systemów (postuluje to Parlament Europejski, w Polsce podobne stanowisko mają m.in. Polska Izba Informatyki i Telekomunikacji oraz Konfederacja Lewiatan). Ponadto, w mniejszym zakresie, dyrektywa ma zdefiniować obowiązki przedsiębiorców z branży cyfrowej dotyczące m.in. ochrony danych osobowych. Nowy dokument będzie najprawdopodobniej obowiązywał zarówno instytucje z sektora publicznego, jak też prywatnego.

Przygotowywanie nowej regulacji przyspieszono po ujawnieniu afery PRISM przez Edwarda Snowdena w 2013 r. (pozyskiwania w Internecie danych osobowych przez amerykańskie służby specjalne, powołujące się na zagrożenie terroryzmem). W marcu 2014 r. projekt dyrektywy został przyjęty przez głosowanie w Parlamencie Europejskim. Wciąż jednak trwają prace nad ostatecznym kształtem *NIS Directive*, ponieważ zakres jej stosowania jest przedmiotem sporu pomiędzy krajami członkowskimi. Opóźnia to przyjęcie unijnego dokumentu, co w konsekwencji oznacza tymczasowy brak regulacji w tym zakresie na poziomie wspólnotowym.

Wejście uregulowania w życie zapewni państwom możliwość skuteczniejszej ochrony infrastruktury krytycznej (m.in. systemów energetycznych, transportowych i ochrony zdrowia), a także wzmocni współpracę pomiędzy krajami UE oraz sektorem prywatnym i publicznym. Przyjęcie dyrektywy zapewni także szereg korzyści użytkownikom sieci. Dzięki harmonizacji przepisów prawnych w ramach UE i stworzeniu jednolitego rynku cyfrowego (traktowanego przez Komisję Europejską jako jeden z priorytetowych celów), przedsiębiorcy uzyskają możliwość łatwiejszego podejmowania pracy za granicą, a firmy w całej Unii zaoszczędzą – według szacunków Komisji – nawet do 2,3 mld euro w skali roku. W szerszym wymiarze, przyjęcie nowej regulacji przyczyni się do stworzenia bardziej równych i przejrzystych warunków konkurencji na europejskim rynku.

Wokół założeń dokumentu trwa dyskusja wynikająca z rozbieżnych stanowisk państw odnośnie do niektórych jego zapisów. Kontrowersje budzi m.in. objęcie nowymi regulacjami wszystkich przedsiębiorstw oferujących towary lub usługi użytkownikom z UE, niezależnie od siedziby firmy (czyli także wiodących amerykańskich spółek internetowych). Od momentu wejścia w życie *NIS Directive* zagraniczne spółki, chcące ujawnić państwom trzecim informacje na temat obywateli UE, będą musiały uzyskać zgodę krajowych organów odpowiedzialnych za ochronę danych osobowych. Rozbieżności dotyczą też m.in.: wysokości kar administracyjnych, objęcia zakresem regulacji operatorów telekomunikacyjnych oraz listy podmiotów zaliczanych do infrastruktury krytycznej państwa.

W dyskusji na temat zakresu dyrektywy, Polska Izba Informatyki i Telekomunikacji oraz Konfederacja Lewiatan opowiadają się m.in. za skróceniem listy podmiotów i zasobów zaliczanych do infrastruktury krytycznej oraz ich precyzyjnym zdefiniowaniem (stworzeniem wyczerpującego, kompletnego zestawienia), a także wyłączeniem spod działania regulacji operatorów telekomunikacyjnych. Obie instytucje uważają ponadto, iż należy przyjąć zasadę harmonizacji maksymalnej, czyli tożsamego rozumienia dyrektywy we wszystkich krajach UE zarówno jeśli chodzi o wymagania skierowane do operatorów rynku, jak i zakres dokumentu. Argumentem na rzecz takiego podejścia jest dążenie do zapewnienia jednakowych zasad działalności i konkurencji. Ponadto, polskie instytucje podkreślają znaczenie dobrowolnego i dwustronnego charakteru wymiany informacji pomiędzy różnymi podmiotami (szczególnie z sektora publicznego i prywatnego).

Dyskusja na temat *NIS Directive* wskazuje na dążenie do kompleksowego traktowania cyberbezpieczeństwa na forum UE, a także wypracowania ram europejskiej współpracy w tym zakresie. Niewątpliwym plusem jest położenie nacisku na partnerstwo publiczno-prywatne – kluczowy warunek skutecznego współdziałania na rzecz realizacji nakreślonych celów. Minusem są utrzymujące się rozbieżności, wynikające z ogromnej złożoności problemu. Krokiem w kierunku ich ograniczenia jest analiza dwóch przypadków państw członkowskich UE, które reprezentują odmienne podejście do tego wyzwania, uwarunkowane przez ich specyfikę.

CYBERBEZPIECZEŃSTWO
w ESTONII

Zaledwie 1,5-milionowa Estonia jako jeden z pierwszych krajów przyjęła w 2008 r. strategię bezpieczeństwa cybernetycznego, zaktualizowaną w 2014 r. Kraj ma dobrze rozwinięty zespół CERT, w 2008 r. w Tallinie utworzono Centrum Doskonalenia Obrony Cybernetycznej NATO, a zaktualizowana strategia bezpieczeństwa cybernetycznego na lata 2014-17 uznaje za główny cel wzmocnienie cybernetycznej tarczy.

Szczególna aktywność Estonii w dziedzinie cyberbezpieczeństwa wynika z dwóch czynników. Po pierwsze – dzięki konsekwentnej polityce kolejnych rządów, zawartej w haśle „E-stonia", kraj stał się technologicznym liderem Europy: miejscem, gdzie wybory przeprowadzane są online, narodził się Skype, a ponad 95 proc. transakcji bankowych przeprowadzanych jest przez Internet. Po drugie – w 2007 r., po usunięciu z centrum Tallina radzieckiego pomnika Brązowego Żołnierza, Estonia stała się ofiarą cyberataku na niespotykaną wcześniej skalę. Zostały unieruchomione strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Największe natężenie ataków miało miejsce 9 maja (w rosyjski Dzień Zwycięstwa): celem hakerów stał się wtedy również sektor prywatny, a dwa największe banki, Hansapank i SEB Ühispank, musiały zawiesić usługi on-line i wstrzymać transakcje zagraniczne.

Doświadczenia z cyberataku wykorzystano w tworzeniu systemu ochrony, który nie poszedł w kierunku zwiększenia niedostępności i otoczenia się „wirtualnym murem", lecz przeciwnie – ulokowania maksymalnej ilości zasobów w przestrzeni cyfrowej, tak aby w wypadku ataku państwo mogło dalej działać, nawet pozbawione terytorium. Specyfikę tego rozwiązania oddaje plan utworzenia „wirtualnej ambasady danych" – fizycznego lub wirtualnego centrum danych w sojuszniczym państwie wybranym przez rząd, gdzie przechowywane są dane dotyczące m.in. krytycznych systemów informatycznych. Osiągnięciem polityki bezpieczeństwa cybernetycznego Estonii jest też daleko posunięte partnerstwo publiczno-prywatne. W jego ramach utworzono Ligę Obrony Cybernetycznej zasilaną przez ochotników z sektora prywatnego, którzy w sytuacji zagrożenia bezpieczeństwa kraju mają podlegać dowództwu wojskowemu.

2008 r.
↳ w Tallinie utworzono Centrum Doskonalenia Obrony Cybernetycznej NATO ↵

2013 r.
↳ estoński rząd rozpoczął inicjatywę „wirtualnej ambasady danych" ↵

16 mln euro
↳ to koszt realizacji strategii bezpieczeństwa cybernetycznego na lata 2014-17 ↵

30
↳ tyle minut potrzeba na wyrobienie nowego elektronicznego dowodu osobistego ↵

CYBERBEZPIECZEŃSTWO
w WIELKIEJ BRYTANII

Prawie 60-milionowa Wielka Brytania podeszła do wyzwań związanych z cyberbezpieczeństwem odmiennie niż Estonia, ale traktuje je również w sposób priorytetowy. O wadze zagadnienia dla brytyjskiej administracji świadczy m.in. najlepiej na świecie rozwinięty sektor e-handlu. Wpisuje się on w obraz całej gospodarki, w dużej części opartej na korzystających z Internetu usługach (np. londyńskie City). Doceniając skalę problemu, Strategia Bezpieczeństwa Narodowego z 2010 r. umieściła ataki w cyberprzestrzeni wśród zagrożeń najwyższej kategorii (*Tier 1*). W 2011 r. przyjęta została nowa Strategia Cyberbezpieczeństwa (pierwsza powstała w 2009 r.). Jednym z jej celów jest uczynienie Wielkiej Brytanii jednym z najbardziej bezpiecznych miejsc do prowadzenia biznesu na świecie. Kluczowe znaczenie tego aspektu w największym stopniu odróżnia brytyjski system od estońskiego, ukierunkowanego głównie na zapewnienie bezpieczeństwa struktur państwa w kontekście zagrożeń z zewnątrz (w tym walki w sferze informacyjnej).

W swojej polityce cyberbezpieczeństwa brytyjskie władze dużą wagę poświęcają zabezpieczeniu sektora prywatnego oraz obywateli. W celu zwiększenia świadomości przedsiębiorców, opracowały poradniki skierowane do różnego rozmiaru firm, w których zawarte zostały jasne i zwięzłe informacje na temat zwiększania bezpieczeństwa kluczowych zasobów.

Dużym problemem w zapewnianiu cyberbezpieczeństwa sektora prywatnego jest motywowana względami wizerunkowymi niechęć firm do dzielenia się informacjami o tym, że padły ofiarą cyberataku. Ominięciu tego problemu służy specjalna platforma CISP (*Cyber Security Information Sharing Partnership*), która umożliwia anonimowe dzielenie się w czasie rzeczywistym informacjami na ten temat między biznesem a stroną rządową. Ogółem na realizację celów wyznaczonych przez strategię brytyjski rząd przeznaczył 1,3 mld dolarów.

750
↳ liczba organizacji zrzeszonych w CISP (Cyber Security Information Sharing Partnership) ↵

850 mln funtów
↳ wydatki przeznaczone na wdrożenie założeń Strategii Cyberbezpieczeństwa w ciągu pięciu lat ↵

2 mld funtów
↳ zakładana wartość eksportu związanego z dziedziną cyberbezpieczeństwa w 2016 r. ↵

24 127 osób
↳ zarejestrowani podczas pierwszej rundy internetowych kursów „Introduction to Cyber Security" ↵

CYBERBEZPIECZEŃSTWO W POLSCE

Polska podjęła już pewne kroki wobec wyzwań związanych z dostępem do danych w sieci, wprowadzając do polskiego systemu prawnego m.in. pojęcie cyberprzestrzeni oraz ustanawiając prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia. W czerwcu 2013 r. Rada Ministrów przyjęła dokument „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej". Większość zaleceń tam opisanych jest nadal w trakcie realizacji.

Na poziomie operacyjnym Polska ma dwa zespoły CERT (ang. *Computer Emergency Response Team*) – CERT.GOV.PL i CERT PL. Ten pierwszy pełni rolę głównego zespołu CERT w obszarze administracji rządowej i w obszarze cywilnym. Jego podstawowym zadaniem jest zapewnianie i rozwijanie zdolności administracji publicznej do ochrony przed cyberzagrożeniami. Natomiast CERT.PL, funkcjonujący w Naukowej i Akademickiej Sieci Komputerowej, to pierwszy powstały w Polsce zespół reagowania na incydenty. Współpracuje on z podobnymi jednostkami na całym świecie.

We wspomnianym dokumencie podkreśla się szczególną rolę edukacji. Wskazuje się, że działania edukacyjne powinny być podejmowane nie tylko wobec pracowników administracji rządowej, mających dostęp do cyberprzestrzeni i korzystających z niej, ale też ogółu społeczeństwa. We współczesnym świecie zapewnienie bezpieczeństwa teleinformatycznego w dużej mierze zależy bowiem od wiedzy i codziennych działań każdego użytkownika sieci. Jeśli zapowiedziane tam wprowadzenie bezpieczeństwa teleinformatycznego jako stałego elementu kształcenia na uczelniach wyższych będzie skutecznie zrealizowane, korzyści z tej sytuacji osiągną także prywatne firmy, które notorycznie cierpią na brak specjalistów w tej dziedzinie. To tylko jeden przykład korzyści wynikających ze ściślejszego partnerstwa publiczno-prywatnego.

Z kolei w Doktrynie Cyberbezpieczeństwa RP, opublikowanej przez Biuro Bezpieczeństwa Narodowego w styczniu 2015 r., wskazano, że sektor prywatny powinien współpracować z sektorem publicznym w zakresie przeciwdziałania zagrożeniom cybernetycznym, w tym opracowywać propozycje regulacji prawnych. Wydaje się, że właśnie w tym elemencie Polska może osiągnąć znacznie więcej, niż obecnie. Wymaga to jednak przełamania wielu stereotypów, nieufności i wzajemnego otwarcia się na wspólny cel – bezpieczeństwo wszystkich użytkowników sieci. Jest to szczególnie istotne w odniesieniu do najważniejszej z punktu widzenia bezpieczeństwa państwa infrastruktury krytycznej, coraz bardziej uzależnionej od rozwiązań teleinformatycznych. To właśnie z tego powodu cyberataki stają się coraz poważniejszym zagrożeniem. Ścisłe współdziałanie administracji publicznej z prywatnymi operatorami jest konieczne także ze względu na fakt, że coraz większa część infrastruktury krytycznej znajduje się w prywatnych rękach.

Kolejnymi wyzwaniami dla podmiotów sektora publicznego są: definicja odpowiedzialności oraz koordynacja współpracy między poszczególnymi podmiotami i jednostkami, a także tworzenie standardów i dobrych praktyk w obszarze cyberprzestrzeni, w tym wymiany informacji i współpracy ze środowiskiem biznesu. Raport Najwyższej Izby Kontroli (z czerwca 2015 r.)[1] wskazuje, że działania instytucji państwowych są prowadzone w sposób rozproszony i bez spójnej wizji systemowej. NIK wskazał na brak niezbędnych regulacji prawnych oraz niespójną i nieefektywną politykę najważniejszych podmiotów państwowych odpowiedzialnych za bezpieczeństwo Polski w wymiarze teleinformatycznym. Co szczególnie niepokojące, wskazano na brak procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią.

Podsumowując, w związku z powyższym Polska zrobiła pierwsze kroki w kierunku wzmocnienia bezpieczeństwa cyfrowego państwa, ale nie jest właściwie przygotowana na zagrożenia w tej dziedzinie i nie ma zdefiniowanego strategicznego modelu podejścia do tego zagadnienia. Administracja działa zaś niespójnie i w oderwaniu od innych sektorów. Z drugiej strony, warto odnotować pozytywne przykłady zaangażowania się społeczeństwa w ochronę cyberprzestrzeni. Od połowy września br. rozpoczęła działalność Polska Obywatelska Cyberobrona (POC), a jej członkowie – cywilni eksperci chcą wspierać cyberbezpieczeństwo kraju jako wolontariusze.

[1] *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Najwyższa Izba Kontroli, czerwiec 2015, URL <https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf>.

INTENSYFIKACJA DEBATY

Nie ulega wątpliwości, że cyberbezpieczeństwo należy traktować jako wspólne zadanie dla wszystkich podmiotów, które mają wpływ na stan bezpieczeństwa danych w Internecie. Szczególną rolę odgrywają tu państwa i firmy informatyczne. Kwestią do dalszej debaty pozostają sposoby i formy współpracy między sektorem publicznym i prywatnym w tym obszarze. Odpowiedzi na powyższe zagadnienia nadejdą zapewne wraz z transpozycją dyrektywy *NIS* do prawodawstwa państw członkowskich i lokalnych dyskusji wokół tego tematu.

Podczas gdy na forum UE toczą się intensywne spory o ostateczny kształt zapisów *NIS Directive*, w Polsce o cyberbezpieczeństwie dyskutują nieliczni eksperci. Kraj pozostaje poza głównym nurtem unijnej debaty, a cyberbezpieczeństwo nie jest postrzegane przez rząd priorytetowo. Najwyższy czas, aby polska administracja aktywnie włączyła się w szukanie optymalnych rozwiązać systemowych m.in. poprzez zainicjowanie szerokiej dyskusji publicznej. Temat bezpieczeństwa w cyberprzestrzeni powinien zaangażować większą liczbę środowisk i podmiotów – zarówno ze sfery publicznej, jak i prywatnej.

Elementami systemu powinny być m.in.:

- edukacja i działania prewencyjne w celu uświadamiania ryzyka oraz wskazywania pożądanych praktyk, by unikać zagrożeń pochodzących z Internetu,
- zbudowanie platformy ściślejszej współpracy administracji ze środowiskiem biznesu w ochronie cyberprzestrzeni,
- jasne zdefiniowanie kompetencji (doradczych, konsultacyjnych i przede wszystkim koordynacyjnych) ponadresortowego organu pomocniczego Rady Ministrów w sprawach cyberbezpieczeństwa,
- przedstawienie katalogu zasad przy tworzeniu nowych rozwiązań prawnych w zakresie bezpiecznego dostępu do danych w sieci.

Porównując strategie Wielkiej Brytanii i Estonii do polskiej strategii obrony w cyberprzestrzeni, można zauważyć, jak ważne jest przyspieszenie działań w celu stworzenia całościowej, strategicznej i przede wszystkim spójnej polityki Polski w tej dziedzinie. Warto zastanowić się w tym kontekście, jakie doświadczenia Wielkiej Brytanii i Estonii mogłyby być zastosowane w Polsce, a jakie działania i mechanizmy mogłyby być z kolei polską specjalnością.

W kwestii wyzwań związanych z bezpieczeństwem cyfrowym klasyczny podział między sektorem państwowym a prywatnym nie ma racji bytu, ponieważ uniemożliwia wypracowanie skutecznych rozwiązań ochronnych. W tym kontekście kluczowa jest szeroka współpraca tych sektorów – tym bardziej, że kwestia cyberbezpieczeństwa nabiera coraz większego znaczenia ze względu na szybki rozwój technologii informacyjnych i komunikacyjnych oraz wciąż nowe rozwiązania i możliwości dostarczane przez rynek.

AUTORZY:

dr Małgorzata Bonikowska

prezes Centrum Stosunków Międzynarodowych i partner w ośrodku THINKTANK

Michał Szczygielski

analityk Centrum Stosunków Międzynarodowych

Antoni Wierzejski

analityk Centrum Stosunków Międzynarodowych

CENTRUM STOSUNKÓW MIĘDZYNARODOWYCH

CSM jest niezależnym, pozarządowym ośrodkiem analitycznym zajmującym się polską polityką zagraniczną i najważniejszymi problemami polityki międzynarodowej. Fundacja została zarejestrowana w 1996 r. CSM prowadzi działalność badawczą i edukacyjną, wydaje publikacje, organizuje konferencje i spotkania, uczestniczy w międzynarodowych projektach we współpracy z podobnymi instytucjami w wielu krajach. Tworzy forum debaty i wymiany idei w sprawach polityki zagranicznej, relacji między państwami oraz wyzwań globalnego świata. Działalność CSM jest adresowana przede wszystkim do samorządowców i przedsiębiorców, a także administracji centralnej, polityków, dyplomatów, politologów i mediów. W 2009 r. CSM został uznany za jeden z najlepszych think tanków Europy Środkowo-Wschodniej w badaniu „The Leading Public Policy Research Organizations In The World" przeprowadzonym przez Uniwersytet Pensylwanii.

CENTRUM STOSUNKÓW MIĘDZYNARODOWYCH, ul. Mińska 25, 03-808 Warszawa, tel.: +48 22 646 52 67