Rekomendacje Stowarzyszenia Euro-Atlantyckiego dotyczące cyberprzestrzeni RP

Stowarzyszenie Euro-Atlantyckie, którego statutowym celem jest inicjowanie publicznej dyskusji oraz rozwijanie dialogu z instytucjami odpowiedzialnymi za bezpieczeństwo i obronność, z troską obserwuje działania rządu w sprawach związanych z bezpieczeństwem cyberprzestrzeni.

Mieliśmy okazję dyskutować na ten temat 19 grudnia 2012 roku w SEA przy okazji prezentacji wyników ćwiczeń ochrony cyberprzestrzeni „Cyber-Exe Polska 2012" zorganizowanych we wrześniu ub.r. we Wrocławiu. W naszej debacie wzięło udział szerokie grono ekspertów i praktyków bezpieczeństwa teleinformatycznego. Byli to członkowie SEA oraz zaproszeni goście, w tym reprezentanci firm i instytucji, które zaangażowały się w wielomiesięczne przygotowania, a następnie przeprowadziły z powodzeniem pierwsze w Polsce ćwiczenia, dające okazję do przetestowania procedur współdziałania w sytuacji ataku cyberterrorystycznego na operatorów infrastruktury krytycznej.

Minister Administracji i Cyfryzacji zakończył publiczne konsultacje projektu rządowego dokumentu zatytułowanego „Polityka ochrony cyberprzestrzeni RP". SEA prosi MAiC o stanowisko do zgłoszonych opinii, publikowanych na stronie BIP, oraz informacje o kolejnej wersji projektu prezentowanego na forum Komitetu Rady Ministrów ds. Cyfryzacji.

SEA skłania się ku stanowisku, że działania w zakresie ochrony cyberprzestrzeni muszą być w Polsce uzgadniane w szerokim gronie zainteresowanych podmiotów i instytucji oraz organizacji pozarządowych, bowiem chodzi przecież o bezpieczeństwo wszystkich obywateli. Tym bardziej dla przedsiębiorców, którzy zarządzają w różnych sektorach infrastrukturą

o istotnym znaczeniu dla bezpieczeństwa obywateli i gospodarki. Powszechność zastosowań technologii informacyjnych, rozwój konkurencyjnego rynku usług i sieci telekomunikacyjnych, swoboda wprowadzania do Internetu nowych zastosowań, coraz większe uzależnienie infrastruktury od systemów informacyjnych spowodowały, że państwo straciło najprawdopodobniej na zawsze monopol na wiedzę o bezpieczeństwie i rozwoju metod przekazywania, przetwarzania i przechowywania informacji.

Polityka ochrony cyberprzestrzeni, której oczekujemy od rządu, musi organizować działania w ramach administracji rządowej, ewentualnie określić wytyczne lub delegować zadania innym organom administracji publicznej. **Bezpieczeństwo państwa w zakresie systemów przetwarzania, przechowywania i przesyłania informacji wymaga spójnej i zorganizowanej komunikacji pomiędzy wszystkimi interesariuszami.**

W następstwie dotychczasowych dyskusji nasuwa się spostrzeżenie, że kwestie polityki bezpieczeństwa cyberprzestrzeni nie są na razie w Polsce prawidłowo umocowane instytucjonalnie. Kompetencje ABW w sprawie zagrożeń terrorystycznych są oczywiste, podobnie jak doświadczenie gromadzone w ramach Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, RCB, czy MON, ale ogrom wiedzy na temat zagrożeń, środków zaradczych, nie mówiąc o technologiach sieciowych lub organizacji systemów informacyjnych znajduje się poza instytucjami administracji publicznej. Większość rozwiązań technicznych w sprawach bezpieczeństwa to dziś produkty prywatnego przemysłu.

Przedsiębiorcy to również grupa podmiotów, które są narażone na współczesne zagrożenia z cyberprzestrzeni. Zagrożenia te, w pewnej skali, mogą mieć znaczenie dla strategicznych interesów państwa i obywateli, funkcjonowanie gospodarki, systemu bankowego, transportu, energetyki.

Podczas dyskusji w SEA zwracano również uwagę, że większość aspektów ochrony cyberprzestrzeni ma kontekst międzynarodowy, co narzucałoby specjalne zadania również na MSZ. Państwo powinno komunikować się w sprawach zagrożeń z cyberprzestrzeni ze wszystkimi interesariuszami oraz tworzyć warunki dla wypracowywania standardów i procedur.

Podsumowując naszą dyskusję chcielibyśmy przedstawić następujące rekomendacje, nie szeregując ich w kolejności priorytetów:

i. Klasyfikowanie wszelkiego rodzaju zagrożeń z cyberprzestrzeni trzeba prowadzić w duchu partnerstwa publiczno – prywatnego. Państwo powinno odpowiednią polityką tworzyć warunki dla wzmacniania bezpieczeństwa, pełnić rolę animatora

standaryzacji i dobrych praktyk. Proces legislacyjny, który stanowi fundament funkcjonowania państwa, jest dziś za wolny, by nadążać za dynamiką pojawiania się nowych typów zagrożeń, związanych z wykorzystywaniem technologii informacyjnych, usług lub aplikacji.

ii. Polityka ochrony cyberprzestrzeni, w rozumieniu zabezpieczenia ciągłości zarządzania państwem w ramach zadań administracji rządowej powinna być wypadkową ogólniejszej strategii ochrony interesów gospodarczych państwa i obywateli. Dlatego niezbędnym elementem tej polityki musi być skomunikowanie się z interesariuszami i zorganizowanie mechanizmów współdziałania i transferu doświadczeń, które będą przez nich akceptowane i wspierane.

iii. W komunikacji w sprawach bezpieczeństwa, pozwalającej doskonalić rozwiązania organizacyjne, prawne, polityczne, celem jest budowanie mechanizmów zaufania pomiędzy podmiotami, które się ze sobą na co dzień do tej pory nie komunikowały, wspólne rozwiązywanie problemów i zażegnywanie konfliktów.

iv. Niezbędna jest ogólna systemowa analiza zagrożeń, które uzasadniają aktywne zaangażowanie służb rządowych, w tym analiza przyczyn, dla których takie zagrożenia mogą wystąpić. Atakującymi nie muszą kierować pobudki o podłożu kryminalnym, terrorystycznym, hackerskim lub skrajne poglądy polityczne. Zagrożenia powinny być analizowane także pod kątem znaczenia, jakie mogą mieć dla celów gospodarczych poszczególnych przedsiębiorstw, sektorów, całej gospodarki, bezpieczeństwa obywateli i stabilności państwa. Zdolność reagowania oznacza nie tylko zastosowanie technicznych i organizacyjnych środków ochrony przed atakami i wykrywanie podatności, ale w ogromnym stopniu umiejętność rozpoznawania zagrożeń i przeciwdziałania sytuacjom, które atak mogą prowokować.

v. Zadania analityczne powinny dotyczyć również korelacji pomiędzy skutkami zagrożeń. Zastosowanie środków zaradczych wymaga wtedy skomunikowania się i współpracy podmiotów działających w różnych sektorach, służb państwowych i komunalnych, organów administracji.

vi. Penalizowanie zagrożeń z cyberprzestrzeni powinno się opierać przede wszystkim o sprawdzone klauzule generalne. Tendencja wymiaru sprawiedliwości do uszczegóławiania norm prawa karnego nie nadąża za inwencją cyberprzestępców, cyberterrorystów.

vii. Należy dążyć do wypracowania i wdrożenia mechanizmów współpracy i reagowania przedsiębiorców na zagrożenia z cyberprzestrzeni. Poważniejsze zagrożenia z cyberprzestrzeni mają zwykle charakter horyzontalny, więc współpraca powinna dotyczyć również firm z różnych sektorów, które na co dzień nie mają potrzeby komunikowania się. Trzeba się liczyć z tym, że przeciwdziałanie ryzyku zagrożeń z cyberprzestrzeni i utrzymanie zdolności stosowania skutecznych środków zaradczych bywa kosztowne i nie zawsze mieści się w zwykłej taktyce działalności gospodarczej. Pomocne w tej sytuacji jest promowanie wiedzy o ryzykach zagrożeń i wdrażanie przepisów, motywujących funkcjonowanie technicznych grup roboczych, forów wymiany doświadczeń o zagrożeniach, organizacji pozarządowych. Trzeba promować pogląd, że przedsiębiorca, który nie dba o bezpieczeństwo teleinformatyczne naraża na szkodę swoich klientów, akcjonariuszy, kontrahentów.

viii. Procedury ustalania obiektów infrastruktury krytycznej, w obowiązującej ustawie o zarządzaniu kryzysowym, mogą nie nadążać za zagrożeniami z cyberprzestrzeni. Należy promować podejście, w którym posiadacze różnego rodzaju infrastruktury, szczególnie z sektora prywatnego, zostaliby zmotywowani do gromadzenia i wymiany doświadczeń w kwestiach bezpieczeństwa, a także analizowania korelacji mogących wpływać na bezpieczeństwo zarządzanej infrastruktury i obsługujących ją systemów teleinformatycznych.

ix. Należy przedyskutować czy i w jakim stopniu reagowanie w stanach nadzwyczajnych może uzasadnić użycie środków, naruszających prywatność, prawa własności intelektualnej, bezpieczeństwo obrotu gospodarczego, ujawnienie zbiorów danych osobowych. Wzrost znaczenia technologii informacyjnych i zagrożeń z cyberprzestrzeni spotęguje ryzyko tego rodzaju naruszeń. Trzeba te kwestie rozstrzygnąć pod kątem prawnym, a także wprowadzić procedury niwelowania negatywnych skutków naruszenia cyberbezpieczeństwa osób prywatnych i podmiotów gospodarczych w następstwie zastosowania przez służby państwowe środków nadzwyczajnych.

x. Dokument definiujący zadania dla poszczególnych organów administracji w związku z ochroną cyberprzestrzeni, powinien określać ramy działań i wskazywać podmioty odpowiedzialne za te działania i czas realizacji każdego celu. To szczególnie istotne ze względu na horyzontalny charakter zagrożeń i środków zaradczych.

xi. Należałoby sugerować aktywne podejście do monitorowania cyberbezpieczeństwa infrastruktury istotnej dla obywateli i gospodarki. Procedury reagowania na wykryte zagrożenia wymagają ciągłej bieżącej weryfikacji.

xii. Działania, jakie należy podjąć w ramach „Polityki ochrony cyberprzestrzeni RP" powinny obejmować analizę ustawodawstwa innych państw i prawa międzynarodowego / UE. Pozwoli to, z jednej strony, sięgnąć do sprawdzonych wzorców, z drugiej zaś, uzyskać zgodność z obowiązującymi lub zapowiadanymi normami, w tym przede wszystkim UE. W tym kontekście istotne znaczenie będą miały działania legislacyjne ws. oczekiwanego projektu ***Strategii UE w zakresie bezpieczeństwa cybernetycznego***, tj. inicjatywy Komisji Europejskiej kompleksowego podejścia do wyzwań związanych z możliwościami cyber ataków przez opracowania kompleksowej strategii bezpieczeństwa cybernetycznego. Warto przy tym pamiętać o aktywnej roli, jaką pełni Parlament Europejski w debacie nt. cyberprzestrzeni, który m.in. apeluje do Państw Członkowskich o niezwłoczne opracowanie (w przypadku braku) i uzupełnienie ich krajowych strategii bezpieczeństwa cybernetycznego i cyber obrony oraz opracowanie solidnej polityki i zapewnienie procedur zarzadzania ryzykiem i odpowiednich środków i mechanizmów przygotowawczych.

xiii. Zaleca się monitorowanie rozwoju i włączenie w prace Europejskiego Centrum ds. Cyberprzestępczości, które rozpoczęło działalność od początku 2013r., jako struktura EUROPOL. Centrum jest punktem kontaktowym ds. zwalczania cyberprzestępczości w UE i realizuje następujące funkcje: centrum wymiany informacji, tworzenie zasobów eksperckich dla wsparcia PCz oraz wsparcie dochodzeń w zakresie cyberprzestępczości. Na obecnym etapie trudno określić, jaką wartość dodaną będzie miało Centrum dla działań w zakresie ochrony cyberprzestrzeni na poziomie narodowym w Państwach Członkowskich. W tym kontekście włączenie w prace Centrum powinno, w pierwszej kolejności, obejmować informowanie właściwych podmiotów / służb o rozwoju, możliwościach a także potrzebach Centrum.