KOMENTARZ DO PROJEKTU
„POLITYKA OCHRONY CYBERPRZESTRZENI RP”

Warszawa, grudzień 2012

WSTĘP

Do konsultacji publicznej przekazany został dokument „Polityka ochrony Cyberprzestrzeni RP”[1] jest to kolejna w ostatnich latach próba przedstawienia spójnego podejścia instytucji państwa do zagrożeń związanych z używaniem technologii informacyjnych. Przygotowały go wspólnie dwa konstytucyjnie niezależne, ale kluczowe w sprawach bezpieczeństwa informacyjnego organy: Ministerstwo Administracji i Cyfryzacji oraz Agencja Bezpieczeństwa Wewnętrznego. Projekt określa przede wszystkim instytucjonalne ramy informacyjnego bezpieczeństwa państwa w zakresie, który nazwano bezpieczeństwem cyberprzestrzeni RP.
Fundacja Bezpieczna Cyberprzestrzeń wraz ze Stowarzyszeniem Euro-Atlantyckim oraz Fundacją „Instytut Mikromakro” zajęła w tej sprawie wspólne stanowisko.
Poniżej opisujemy w skrócie główne uwagi jakie zawiera oficjalny komentarz do projektu „Polityka Ochrony Cyberprzestrzeni RP” jaki przedstawiliśmy w tej sprawie w Ministerstwie Administracji i Cyfryzacji[2].

1. BŁĄD FUNDAMENTALNY – OGRANICZENIE OBSZARU OBOWIĄZYWANIA POLITYKI

Fundamentalnym brakiem dokumentu jest ograniczenie do organizacji działań w ramach administracji rządowej, ewentualnie zalecanie wymagań innym organom administracji publicznej. Kompetencje ABW w sprawie zagrożeń terrorystycznych są oczywiste, podobnie jak doświadczenie gromadzone w ramach CERT-u rządowego, czy RCB, ale wiedza na temat zagrożeń, środków zaradczych, nie mówiąc o technologiach sieciowych lub organizacji systemów informacyjnych jest w ogromnej części poza instytucjami administracji. Podobnie, istotne z punktu widzenia strategicznych interesów państwa i obywateli współczesne zagrożenia z cyberprzestrzeni, dotyczą systemów zarządzanych bez udziału organów administracji, w dużej części będących własnością prywatną.

Polityka państwa powinna się skupić na strategii komunikacji w sprawach zagrożeń z cyberprzestrzeni wszystkich interesariuszy, tworzeniu warunków dla wypracowywania standardów i procedur.

---

[1] Strona MAiC dotycząca konsultacji dokumentu znajduje się pod adresem: http://mac.bip.gov.pl/prawo-i-prace-legislacyjne/polityka-ochrony-cyberprzestrzeni-rp-resortowe-zglaszanie-uwag-do12-10-2012.html

[2] Dokument zawierający wszystkie uwagi i komentarze znajduje się pod adresem:
http://mac.bip.gov.pl/fobjects/download/3614/fbc_uwagidopolitykiochronycrp_v13-pdf

2. BRAK SYSTEMOWEJ ANALIZY ZAGROŻEŃ

Znaczącą wadą przedstawionej do konsultacji Polityki jest również brak ogólnej systemowej analizy rodzaju i charakteru zagrożeń, które powinny angażować działania służb rządowych, w tym powodów dla których takie zagrożenia mogą wystąpić. Atakującymi przecież niekoniecznie kierują pobudki o podłożu kryminalnym lub terrorystycznym. Zagrożenia powinny być analizowane pod kątem znaczenia jakie mogą mieć dla gospodarki, bezpieczeństwa obywateli i stabilności państwa. Zdolność reagowania, oznacza nie tylko zastosowanie technicznych środków ochrony przed atakami, ale też umiejętność przeciwdziałania sytuacjom, które atak prowokują.

3. BRAK RZECZYWISTEGO PLANU DZIAŁANIA

Za niezbędne uważamy dołączenie do Polityki w formie załącznika planu działań ze wskazaniem podmiotu odpowiedzialnego i czasu realizacji tego zadania. Bez tego Polityka nie będzie miała żadnej realnej mocy sprawczej, zwłaszcza w kontekście kolegialnej odpowiedzialności za bezpieczeństwo cyberprzestrzeni.

4. BRAK WSKAZANIA NAJWAŻNIEJSZYCH OBSZARÓW OCHRONY

Należy rozważyć czy istnieją „systemy strategiczne z punktu widzenia bezpieczeństwa Państwa" inne niż eksploatowane przez wymienione w dokumencie instytucje i podmioty. […] Rządowy dokument rangi politycznej powinien określać, co jest interesem państwa, w tym jakiego typu systemy mają znaczenie strategiczne, a nie postulować rozważania.

Polityka nie jest konsekwentna jeżeli chodzi o odnoszenie się do obszarów, których dotyczy. W akapicie szóstym nacisk położono na gospodarkę RP, podczas gdy wcześniej koncentrowano się na zadaniach administracji publicznej. Celowym wydaje się jednoznaczne określenie obszarów, których dotyczy Polityka.

Nie wiadomo na jakiej zasadzie zalecenia Polityki mają być „rekomendowane również przedsiębiorcom" i co z tego wynika. Kwestia partnerstwa publiczno-prywatnego w budowaniu systemu bezpieczeństwa informacyjnego państwa nie powinna być kwitowana tak lakonicznymi stwierdzeniami.

5. ZAMIESZANIE TERMINOLOGICZNE

Wprowadzenie sformalizowanych definicji odwołujących się do pojęć definiowanych w ustawach, normach jest błędem w dokumencie rangi politycznej opisującym działania w nowym obszarze, wymagającym dużej elastyczności. Tego typu uściślający zbiór definicji nie jest konieczny. Jeżeli natomiast miałby pozostać, to należy zastosować definicje opisowe, które pozwolą lepiej rozumieć Politykę.

Wiele pojęć zdefiniowanych w „Terminach" nie jest stosowanych w dalszej treści Polityki, np. Sektorowy Punkt Kontaktowy bądź dla znaczenia odpowiadającego zdefiniowanemu pojęciu stosuje się inne pojęcie niż to zdefiniowane. Należy dokonać przeglądu Polityki pod względem ujednolicenia pojęć.

Ponadto w Polityce pojawia się bezosobowy styl „proponuje się". Kto proponuje i w jakim trybie?

6. DYSONANS W STANDARDACH BEZPIECZEŃSTWA DLA RÓŻNYCH PODMIOTÓW

Teoretycznie Polityka adresowana jest do wszystkich użytkowników CRP, jednak administrację rządową ona obowiązuje, dla administracji samorządowej i innych urzędów jest rekomendowana, a dla pozostałych użytkowników CRP jest jedynie wskazówką. Ten dysonans odczuwalny jest w całym tekście Polityki, której najwięcej rozwiązań opisanych bardziej szczegółowo odnosi się tylko do administracji np. pełnomocnik ds. bezpieczeństwa cyberprzestrzeni, czy przeprowadzanie oceny ryzyka. Wydaje się, że tak skonstruowana Polityka nie będzie skuteczna dla ochrony CRP, gdyż zastosowanie niższych standardów dla wprowadzania Polityki, tzn. tylko rekomendacji a nie obowiązku, dla tak istotnych podmiotów jak Kancelarii Prezydenta Rzeczypospolitej Polskiej, Kancelarii Sejmu Rzeczypospolitej Polskiej, czy Kancelarii Senatu Rzeczypospolitej Polskiej, może mieć bardzo istotny wpływ na poziom bezpieczeństwa CRP.

7. BŁĘDNE WSKAZANIE ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO CRP

Wskazanie na Radę Ministrów jako odpowiedzialnej za bezpieczeństwo CRP może wpłynąć na mniejszą skuteczność podejmowanych działań w przypadku wystąpienia incydentu lub zagrożenia bezpieczeństwa

państwa z cyberprzestrzeni. Lepsze byłoby przyznanie odpowiedzialności za bezpieczeństwo cyberprzestrzeni Prezesowi Rady Ministrów, co znajduje uzasadnienie w innych zapisach Polityki.

8. BRAK STRATEGII ZAPEWNIENIA KOMPLEKSOWEGO BEZPIECZEŃSTWA

Określenie, że „Infrastruktura teleinformatyczna CRP musi być chroniona przed atakami z cyberprzestrzeni, zniszczeniem, uszkodzeniem i dostępem osób nieuprawnionych" nie odwołuje się do podstawowych cech zapewnienia bezpieczeństwa, czyli poufności, integralności i dostępności, a zatem jest błędnym wskazaniem priorytetów ochrony.

9. BRAK REALNYCH WYMAGAŃ

Dla urzędów posiadających serwisy transakcyjne (np.: ePUAP, PUE ZUS) powinny być przygotowane co najmniej przybliżone minimalne wymagania dotyczące badania skuteczności zabezpieczeń - na przykład test penetracyjny i skan kodu źródłowego. Kluczową wartością dodaną Polityki byłyby w takim przypadku na przykład zalecenia dotyczące poprawnego zamawiania tego typu usług.

10. BRAK WSPÓŁPRACY PUBLICZNO-PRYWATNEJ

Polityka całkowicie pomija możliwość udziału instytucji pozarządowych w tworzeniu zaleceń oraz dobrych praktyk z zakresu bezpieczeństwa. Biorąc pod uwagę, iż strony internetowe stanowią według Polityki „główne miejsce wymiany informacji pomiędzy jednostkami administracji a obywatelem, w e-społeczeństwie", pominięcie czynnika obywatelskiego oraz profesjonalnego nie znajduje uzasadnienia.

11. BRAK REALNEGO PODEJŚCIA

W Polityce proponuje się to, że zespół, który jeszcze nie jest powołany przygotuje rekomendacje dla ministra w ciągu 30 dni. W dokumencie rangi Polityka taka deklaracja gotowości nie wydaje się

potrzebna, ale jeżeli jest to założenie ekspresowej skutecznej pracy wymagałoby wyjaśnienia. Jeżeli zaryzykować stwierdzenie, że być może projekt tego rodzaju rekomendacji już wstępnie przygotowano, to dlaczego nie zawarto ich w Polityce?

12. NIEJASNE I NIEUZASADNIONE WSKAZANIE WYBRANEGO PRZEDSIĘBIORCY

Polityka stanowi dokument rządowy, stąd wskazywanie w akapicie pierwszym na projekt prowadzony na zasadach komercyjnych wspólnie z przedsiębiorcą, tj. Naukową i Akademicką Siecią Komputerową, wydaje się nieuzasadnionym preferowaniem przez polski rząd tego przedsiębiorcy. Dodatkowo projekt ma charakter szczegółowy i brak podstaw, aby tylko ten projekt oraz zapowiedź jego rozbudowy były wskazywane w treści dokumentu rządowego o charakterze ogólnym, z pominięciem innych projektów, które są lub mogą być realizowane przez instytucje rządowe we współpracy z przedsiębiorcami. Celowość kontynuowania tego projektu powinna zostać nadto zweryfikowana przy pomocy zewnętrznych podmiotów wobec stron tego projektu.

Wskazywanie konkretnych CERT-ów, np. TP CERT w treści dokumentu rządowego powoduje nieuzasadnione preferowanie danego przedsiębiorcy i nie znajduje podstawy w przepisach prawa, szczególnie, iż dalej mowa już o pozostałych przedsiębiorcach telekomunikacyjnych i usługodawcach świadczących usługi drogą elektroniczną. Wyróżnienie tylko niektórych przedsiębiorców z pominięciem pozostałych wydaje się niedopuszczalne.

13. BŁĘDY MERYTORYCZNE

W Polityce witryny internetowe dotyczące bezpieczeństwa, określa się je jako “wewnętrzne”. Z drugiej strony jest mowa o tym, że “witryny będą pełnić rolę punktów zgłaszania incydentów bezpieczeństwa teleinformatycznego”. Wydaje się, że zapisy te leżą w sprzeczności ze sobą, ponieważ możliwość zgłaszania incydentów zazwyczaj wiąże się z dostępnością z zewnątrz serwisu przyjmującego tego typu zgłoszenia.

Wskazana w Polityce lista istniejących CERT-ów, w tym ich nazewnictwa, jest listą dynamiczną. Dlatego podawanie konkretnych nazw zespołów jest niepotrzebne. Już obecnie lista ta jest nieaktualna.

Nie jest jasne dlaczego Polityka odwołuje się do wymiany informacji niejawnych skoro wcześniej w dokumencie znajduje się zastrzeżenie, że Polityka nie obejmuje strategii ochrony takich informacji.