Warszawa, dnia 21 sierpnia 2014 r.

RZECZPOSPOLITA POLSKA
MINISTERSTWO
ADMINISTRACJI I CYFRYZACJI

PODSEKRETARZ STANU
Roman Dmowski

BM-WP.072.400.2014

Pan
Bogdan Borusewicz
Marszałek Senatu RP

Szanowny Panie Marszałku ,

Zgodnie z pismem z dnia 30 lipca br., przekazującym oświadczenie złożone przez Senatora RP Pana Jarosława Obremskiego podczas 59. posiedzenia Senatu RP w dniu 24 lipca br. (BPS/043-59-2564/14), przedstawiam odpowiedź na pytania Pana Senatora.

1. **Jak wygląda współpraca pomiędzy MAC a innymi instytucjami państwa w zakresie zabezpieczania obywateli w obszarze cyberprzestrzeni?**

Zgodnie z pkt. 1.5 dokumentu rządowego *Polityka ochrony cyberprzestrzeni RP* Minister Administracji i Cyfryzacji jest podmiotem koordynującym realizację *Polityki* w imieniu Rady Ministrów. Przy pomocy Zespołu ds. ochrony cyberprzestrzeni zapewnia on koordynację i spójność działań, podejmowanych przez poszczególne urzędy państwowe w celu zapewnienia bezpieczeństwa cyberprzestrzeni RP. W Krajowym Systemie Reagowania na Incydenty Komputerowe w CRP (pkt. 4.2 Polityki) Minister także znajduje się na poziomie I – poziomie koordynacji.

Rolą MAC w systemie jest wobec powyższego przede wszystkim podejmowanie działań organizacyjnych, zmierzających do poprawy funkcjonowania systemu ochrony cyberprzestrzeni RP jako spójnej całości, poprzez usprawnienie obiegu informacji, wypracowanie wspólnych standardów i procedur czy też upowszechnienie dobrych praktyk.

Zmierzając do realizacji swej roli, Ministerstwo Administracji i Cyfryzacji od początku 2014 r. zorganizowało w swojej siedzibie szereg spotkań konsultacyjnych z administracją rządową i przedsiębiorcami. Spotkania miały na celu rozpoczęcie współpracy w obszarze bezpieczeństwa cyberprzestrzeni i zebranie opinii interesariuszy, co do optymalnego kształtu dalszej współpracy. Obok spotkań bilateralnych, należy przede wszystkim wskazać na opisane poniżej spotkania w szerokiej formule, obejmujące także podmioty spoza

administracji rządowej, które służą budowaniu szerokiego forum współpracy w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni Polski.

W dniu 14 marca 2014 roku odbyło się spotkanie z administracją państwową, dotyczące organizacji w Polsce prac w związku z ochroną cyberprzestrzeni, w tym przede wszystkim dotyczących projektu dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii Europejskiej (dyrektywa NIS). Spotkaniu przewodniczył Minister Administracji i Cyfryzacji – Pan Rafał Trzaskowski. Uczestniczyli w nim zaproszeni goście z instytucji realizujących w Polsce zadania z zakresu bezpieczeństwa sieci i informacji (MS, MSZ, MON, MSW, MF, KPRM, ABW, GIODO, UKE, KGP, NCK, RCB, NASK). Instytucje uczestniczące w spotkaniu zostały poproszone o przesłanie do Ministerstwa Administracji i Cyfryzacji oficjalnego stanowiska w kwestiach fundamentalnych i systemowych, związanych z dyrektywą NIS, czyli objęcia regulacją administracji publicznej oraz koncepcją „właściwego organu" ds. bezpieczeństwa sieci i informacji. Dodatkowo instytucje zobowiązano do przedstawienia mapy posiadanych kompetencji, osób odpowiedzialnych w zakresie cyberbezpieczeństwa i cyberprzestępczości oraz realizowanej współpracy. Podkreślona została waga bieżącej wymiany informacji pomiędzy odpowiednimi urzędami – np. przekazywanie instrukcji i sprawozdań z wyjazdów i realizowanej współpracy międzynarodowej. Jednocześnie Rządowe Centrum Bezpieczeństwa zobowiązało się do organizacji spotkania roboczego z MAC, celem przedyskutowania kwestii powiązań między dyrektywą NIS a ochroną infrastruktury krytycznej.

W dniu 16 maja 2014 roku odbyło się spotkanie z podmiotami prywatnymi (sektorem biznesu, przedstawicielami środowisk naukowych, organizacjami pozarządowymi), dotyczące działań związanych z realizacją *„Polityki ochrony cyberprzestrzeni RP"* oraz stanowiska w sprawie dyrektywy NIS. W spotkaniu wzięli udział przedstawiciele m.in.: UKE, PKPP Lewiatan, Polskiej Izby Spedycji i Logistyki, Instytutu Kościuszki, Wojskowego Instytutu Łączności, Fundacji Pułaskiego, Fundacji Bezpieczna Cyberprzestrzeń, Wojskowej Akademii Technicznej, Związku Banków Polskich, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, e-IZBY Gospodarki Elektronicznej. Instytucje uczestniczące w spotkaniu zostały poproszone o przesłanie do Ministerstwa Administracji i Cyfryzacji oficjalnego stanowiska w kwestiach dotyczących cyberbezpieczeństwa, szczególnie w kontekście projektowanych przepisów unijnych. Dyskutowana była głównie kwestia zakresu podmiotowego dyrektywy; większość podmiotów gospodarczych pozytywnie ocenia podejście PL, zakładające wprowadzenie definicji „podstawowych", „krytycznych" usług elektronicznych, wobec których miałyby zastosowanie przepisy dyrektywy oraz wskazanie w dyrektywie sektorów infrastruktury krytycznej, gdzie tego typu usługi są świadczone. Z pozytywną reakcją spotkała się propozycja stworzenia stałej grupy konsultacyjnej ds. cyberbezpieczeństwa – szereg podmiotów zgłosiło już swój udział. Zdaniem MAC grupa ta

(maksymalnie 20 osobowa) powinna objąć także podmioty z administracji i stanowić szybką ścieżkę do roboczych konsultacji. Skład zostanie ogłoszony niebawem, po zakończeniu konsultacji. Prace powinny stanowić uzupełnienie i wkład dla prac *Zespołu zadaniowego KRMC* oraz element realizacji pkt. 4.5 *„Polityki ochrony cyberprzestrzeni RP"* (współpraca z przedsiębiorcami).

Kolejne spotkanie z administracją państwową, poświęcone *„Polityce ochrony cyberprzestrzeni RP"* i projektowi dyrektywy NIS, zorganizowane zostało w dniu 4 czerwca 2014 roku. Głównym celem spotkania było omówienie działań podejmowanych w zakresie cyberbezpieczeństwa przez MAC i zebranie opinii pozostałych uczestników. Poruszono kwestie związane z powołaniem *Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP*. W porozumieniu z Kancelarią Prezesa Rady Ministrów została podjęta decyzja, że *Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni* będzie powołany w ramach Komitetu Rady Ministrów ds. Cyfryzacji. Został także przedstawiony stan prac nad dyrektywą nt. bezpieczeństwa sieci i informacji (NIS), jak również wnioski z zainicjowanej dyskusji z sektorem prywatnym i pozarządowym w Polsce.

Powyższe spotkania organizowane były ad hoc w celu koordynowania polityki działań organów Państwa oraz w celu zebrania przez MAC opinii wszystkich interesariuszy.

Decyzją Przewodniczącego Komitetu Rady Ministrów ds. Cyfryzacji, w celu usprawnienia procesu realizacji celów *„Polityki ochrony cyberprzestrzeni RP"* oraz zapewnienia skuteczności działań organów władzy państwowej w zakresie cyberbezpieczeństwa 13 czerwca 2014 roku, został powołany *Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni RP,*_który przejął centralną rolę w procesie koordynacji jako stałe forum spotkań pomiędzy zaangażowanymi urzędami. Zespół odpowiedzialny jest (zgodnie z pkt. 3.4 *Polityki*) za przygotowywanie rekomendacji działań i rozwiązań, dotyczących zapewnienia bezpieczeństwa w obszarze cyberprzestrzeni oraz za koordynację wszelkich działań z tym związanych. 28 lipca 2014 roku w siedzibie Ministerstwa Administracji i Cyfryzacji, odbyło się I Posiedzenie *Zespołu Zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP*. Spotkaniu przewodniczył Minister Administracji i Cyfryzacji – Pan Rafał Trzaskowski, przy udziale Podsekretarza Stanu – Pana Romana Dmowskiego. Uczestniczyli w nim przedstawiciele członków *Zespołu Zadaniowego KRMC ds. bezpieczeństwa cyberprzestrzeni RP.* Na wstępie został przedstawiony kontekst i cel spotkania, następnie opisano formalne kwestie związane z *Zespołem.* Przedstawiono wyniki audytu zleconego przez Ministerstwo Finansów w 2013 r. Uczestnicy spotkania zostali zobligowani do nadesłania wkładów do Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, przewidzianego w *„Polityce ochrony cyberprzestrzeni RP"* oraz w decyzji powołującej *Zespół zadaniowy,* w zakresie właściwości urzędów. Plan ten powinien zostać przyjęty do października br.

Jednocześnie, jak wskazano powyżej, MAC stale współpracuje z innymi instytucjami, zaangażowanymi w działania związane z bezpieczeństwem cyberprzestrzeni. Przede

wszystkim należy tu wymienić Rządowe Centrum Bezpieczeństwa (w kwestiach związanych z infrastrukturą krytyczną Państwa) oraz Departamentem Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (pełniącego rolę głównego zespołu CERT w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP w obszarze administracji rządowej). MAC regularnie współpracuje także z NASK (Naukowa i Akademicka Sieć Komputerowa), w ramach którego funkcjonuje zespół CERT Polska.
Ministerstwo uczestniczy także w pracach nad Doktryną cyberbezpieczeństwa RP, tworzoną obecnie przez Biuro Bezpieczeństwa Narodowego.

2. **Na jakim etapie jest wprowadzany od 2013 r. dokument *„Polityka Ochrony Cyberprzestrzeni RP"*?**

Dokument rządowy *„Polityka ochrony cyberprzestrzeni RP"*, przyjęty uchwałą Rady Ministrów w dniu 25 czerwca 2013 r., obecnie znajduje się w fazie realizacji. Stopniowo, mając na uwadze niewielkie środki początkowo przeznaczone na to działanie (*Polityka* przewiduje realizację zadań w ramach już posiadanych przez jednostki środków), wprowadzane są w życie kolejne jej postanowienia. Poniżej opisane są poszczególne realizowane działania, obok wspomnianego powyżej powołania *Zespołu zadaniowego.*
Pierwszym działaniem, wymienionym w *Polityce* (pkt. 3.1) i w dużym stopniu warunkującym kształt dalszych działań, jest przeprowadzenie szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni. W ubiegłym roku przeprowadzony był przez Ministerstwo Finansów audyt zlecony przez KPRM, którego tematem było „Zarządzanie bezpieczeństwem systemów teleinformatycznych w wybranych urzędach administracji rządowej". Celem audytu było zebranie informacji nt. działań jednostek administracji rządowej w zakresie zapewnienia bezpieczeństwa wybranych systemów teleinformatycznych, zidentyfikowanie zagrożeń i słabych punktów w zarządzaniu bezpieczeństwem tych systemów. Objęte audytem były jawne systemy teleinformatyczne jednostek. Obecnie wyniki tego audytu zostały przedstawione do dyskusji na forum *Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni* RP i będą stanowiły materiał pomocniczy w pracach nad planem działań.
Do przeprowadzenia właściwego szacowania ryzyka MAC przystąpiło na początku 2014 roku. Do dnia 31 marca jednostki organizacyjne administracji (głównie rządowej) przekazywały do Ministerstwa wypełnione sprawozdania, podsumowujące wyniki szacowania ryzyka własnych systemów teleinformatycznych za rok 2013, zgodnie z przekazanym wzorcem i metodyką. Obecnie wyniki z ok. 200 otrzymanych ankiet są poddawane analizie i MAC przygotuje na ich podstawie zbiorcze sprawozdanie z szacowania ryzyka. Ma ono przede wszystkim służyć opracowaniu docelowej wersji metodyki sporządzania analizy ryzyka cybernetycznego, która będzie stanowiła z kolei podstawę szacowania ryzyka za rok bieżący. W ten sposób ryzyko ma być szacowane w sposób ciągły

w cyklu rocznym, a zbiorcze opracowanie wyników stanowić będzie podstawę programowania dalszych działań.

Polityka określa także obowiązki ciążące na poszczególnych podmiotach administracji, w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa. Przede wszystkim istnieje obowiązek opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI), którego ważnym komponentem jest m.in. polityka bezpieczeństwa informacji. Dotychczasowe badania (np. wskazany powyżej audyt) pokazują, że w wielu jednostkach organizacyjnych nie funkcjonują wciąż odpowiednie rozwiązania w tym zakresie. Zgodnie z sugestią zawartą w *Polityce,* Minister Administracji i Cyfryzacji przy współpracy *Zespołu zadaniowego*, zamierza umieścić w Planie działań punkt dotyczący opracowania i zapewnienia wdrożenia wytycznych, dotyczących systemów zarządzania bezpieczeństwem informacji. W tym zakresie rozważane jest oparcie się na opracowanej przez Komisję Nadzoru Finansowego Rekomendacji D.

Kolejnym obowiązkiem określonym w *Polityce*, ściśle związanym z wyżej wymienionym SZBI, jest ustanowienie w każdej jednostce pełnomocnika ds. bezpieczeństwa cyberprzestrzeni. Osoba taka odpowiedzialna będzie za całość zagadnień z tym związanych, w tym w szczególności:

a. realizację obowiązków wynikających z przepisów aktów prawnych właściwych dla zapewnienia bezpieczeństwa cyberprzestrzeni;
b. opracowanie i wdrożenie procedur reagowania na incydenty komputerowe, które będą obowiązywały w organizacji;
c. identyfikowanie i prowadzenie cyklicznych analiz ryzyka;
d. przygotowanie planów awaryjnych oraz ich testowanie;
e. opracowanie procedur zapewniających informowanie właściwych zespołów CERT o:
    - wystąpieniu incydentów komputerowych,
    - zmianie lokalizacji jednostki organizacyjnej, danych kontaktowych, itp.

Prośba o ustanowienie pełnomocnika i przekazanie jego danych kontaktowych została przekazana do jednostek wraz z ankietą szacowania ryzyka cyberprzestrzeni. Obecnie ok. 100 jednostek organizacyjnych przekazało do MAC informacje o wyznaczeniu pełnomocnika ds. ochrony cyberprzestrzeni.

Polityka duży nacisk kładzie na działania edukacyjne. Jednym z zadań w zakresie edukacji specjalistycznej jest podnoszenie kwalifikacji wspomnianych pełnomocników ds. ochrony cyberprzestrzeni (pkt. 3.5.1 *Polityki*). MAC przygotowuje obecnie pierwsze dedykowane szkolenie dla pełnomocników, które odbędzie się we wrześniu tego roku. Poza przekazywaniem praktycznej wiedzy, szkolenia tego typu mają także w założeniu służyć nawiązywaniu bezpośrednich kontaktów pomiędzy pełnomocnikami oraz wymianie doświadczeń i dobrych praktyk. Należy wspomnieć, że szkolenia wpisujące się w cele *Polityki,*

prowadzone są także w ramach projektu „Nowoczesne kadry polskiej teleinformatyki administracji publicznej, narzędzia wymiany doświadczeń i podnoszenia kompetencji", który realizowany jest przez MAC. Szkolenia te prowadzone będą cyklicznie we współpracy z ABW i NASK, a być może także z udziałem ekspertów ENISA.

W zakresie edukacji powszechnej (pkt. 3.5.4 *Polityki*), MAC także zleciło przeprowadzenie szeregu kampanii, mających na celu propagowanie bezpiecznego korzystania z Internetu w ramach ogólnych działań, dotyczących promowania społeczeństwa informacyjnego. W szczególności należy wymienić tu realizację zadania publicznego „Upowszechnienie korzystania z internetu i rozwój kompetencji cyfrowych", gdzie cztery projekty, wyłonione w trybie konkursu, wpisywały się w działania związane ze wspieraniem bezpiecznego korzystania z Internetu. MAC zamierza, wykorzystując tu także powołany *Zespół zadaniowy,* zacieśnić współpracę w tym zakresie z Ministerstwem Edukacji Narodowej, w celu przeprowadzenia szerokiej kampanii edukacyjnej, skierowanej do dzieci, młodzieży, nauczycieli i rodziców. Uważa się, że ta tematyka powinna być stale obecna w programach nauczania.

Kolejnym działaniem z zakresu podnoszenia kompetencji, które przewidziane jest w *Polityce,* to wprowadzenie tematyki bezpieczeństwa teleinformatycznego, jako stałego elementu kształcenia na uczelniach wyższych. Takie działania już są podejmowane i MAC będzie ściśle współpracowało w tej kwestii z MNiSW.

Kolejnym polem współpracy z MNiSW jest kwestia programów badawczych w zakresie cyberbezpieczeństwa. Przyjmuje się, że podmiotem koordynującym wdrażanie zapisów *Polityki* w tym zakresie będzie MNiSW, jako właściwe w sprawach badań naukowych i prac rozwojowych. Wykaz inicjatyw uwzględniających dynamikę stanu wiedzy określony zostanie na poziomie projektów szczegółowych, opracowanych na podstawie *Polityki* i może być uzupełniany z inicjatywy właściwych podmiotów odpowiedzialnych za jego realizację. Obecnie MAC uczestniczy w projekcie badawczym „System ewaluacji zagrożeń bezpieczeństwa cyberprzestrzeni RP na potrzeby systemu zarządzania bezpieczeństwem narodowym RP (SEZBC)", finansowanym przez NCBiR, a realizowanym przez konsorcjum kierowane przez Wojskowy Instytut Łączności. Celem projektu jest opracowanie systemu zbierania i analizy informacji o bieżących zagrożeniach cyberprzestrzeni RP.

3. **Kiedy możemy się spodziewać pierwszych efektów prowadzonej przez MAC polityki na rzecz bezpieczeństwa w sieci?**

Osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa jest realizowane poprzez stworzenie ram organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy użytkownikami cyberprzestrzeni. Podejmowane działania są wynikiem oszacowań ryzyka, prowadzonych przez poszczególne podmioty, w odniesieniu do zagrożeń występujących w cyberprzestrzeni. Po wykonanym szacowaniu

ryzyka i analizie wyników, otrzymamy ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których poszczególna instytucja działa i za które odpowiada. Na tej podstawie powstanie zbiorcze sprawozdanie i możliwe będzie wystosowanie rekomendacji, zaleceń i sposobów postępowania z istniejącym ryzykiem, co doprowadzi do skutecznej walki z zagrożeniami i osiągnięciem akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa.

Zauważalnymi efektami będą także działania i decyzje podejmowane przez *Zespół ds. bezpieczeństwa cyberprzestrzeni RP,* którego zadaniem jest usprawnienie procesu realizacji *Polityki* oraz zapewnienie skuteczności działań organów władzy państwowej w zakresie bezpieczeństwa cyberprzestrzeni. *Zespół* ten odpowiedzialny jest za przygotowywanie rekomendacji z zakresu wykonania czy koordynacji wszelkich działań związanych z bezpieczeństwem cyberprzestrzeni.

Należy tu zauważyć, że Minister Administracji i Cyfryzacji nie posiada żadnych uprawnień władczych związanych z zapewnieniem bezpieczeństwa cyberprzestrzeni. Koordynacyjna rola MAC w tym systemie polega na miękkim oddziaływaniu, a skuteczność tych działań jest trudna do zmierzenia. Każda z instytucji administracji państwowej, ale także podmioty prywatne (np. operatorzy telekomunikacyjni) ponoszą odpowiedzialność za bezpieczeństwo pewnego wycinka cyberprzestrzeni RP. MAC będzie wspierać działania tych podmiotów poprzez swoje działania, ale nie może zapewnić lub gwarantować pełnego bezpieczeństwa cyberprzestrzeni RP. W naszej ocenie i odbieranych przez MAC opiniach interesariuszy, obecne działania zmierzają w dobrym kierunku i ich intensyfikacja powinna przynieść wymierne efekty już w krótkim horyzoncie czasowym (12-18 miesięcy).

Z poważaniem,

SEKRETARZ STANU
w Ministerstwie Administracji i Cyfryzacji

Roman Dmowski

Do wiadomości:
Kancelaria Prezesa Rady Ministrów