Warszawa, dnia 26 lipca 2017 r.

**RZECZPOSPOLITA POLSKA**
MINISTER CYFRYZACJI

***Anna Streżyńska***

BM-WOP.072.97.2017

**Pan**
**Marek Kuchciński**
**Marszałek Sejmu RP**

Dot. pisma z dnia 12 lipca 2017 r. Posłów na Sejm RP Panów Pawła Pudłowskiego i Pawła Kobylińskiego w sprawie *wykorzystania potencjału Polski dla potrzeb cyberbezpieczeństwa* (interpelacja nr 13915)

Szanowny Panie Marszałku,

Ministerstwo Cyfryzacji dostrzega potencjał, jakim dysponuje Polska w dziedzinie cyberbezpieczeństwa. Wspieranie rozbudowy zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa jest jednym z celów Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022[1], które stanowią podstawę prowadzenia polityki państwa w tym zakresie. Projektowane są więc rozwiązania mające rozwijać potencjał Polski zarówno w dziedzinie przemysłu, jak i kompetencji naukowych.

Polska ma szansę stać ważnym graczem w sferze cyberbezpieczeństwa na arenie międzynarodowej. Jednak aby to osiągnąć, kluczowe jest zbudowanie odpowiednich kompetencji i możliwości. W tym celu m.in. planowane jest powstanie Cyberparku Enigma. Zgodnie z projektem, program ten ma na celu odtworzenie i rozbudowę kompetencji do wytwarzania urządzeń i oprogramowania wykorzystywanych w przemyśle. Nowe technologie będą pozyskiwane także poprzez udział w inicjatywach europejskich takich jak Horyzont 2020 w ramach obszaru „*Secure societies - protecting freedom and security of Europe and its citizens*". Zadanie to zrealizowane będzie we współpracy z Ministerstwem Obrony Narodowej i Ministerstwem Rozwoju.

Aby wyrównać szanse polskich przedsiębiorców na międzynarodowych rynkach planuje się powstawanie hubów innowacyjności. Będą one oferować obsługę dla firm i start-up'ów, polegającą m. in. na testowaniu nowych rozwiązań, badaniu rynku, pomocy w ubieganiu się o środki na rozwój innowacyjnych rozwiązań. To również jest planowane jako przedsięwzięcie prowadzone wspólnie z MON i MR.

[1] Uchwała Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. *w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022*.

W celu wspierania rozwoju ośrodków naukowych w interesującym nas obszarze, MC wspólnie z Ministerstwem Nauki i Szkolnictwa Wyższego oraz Państwową Akademią Nauk utworzy Naukowy Klaster Cyberbezpieczeństwa. Będzie to platforma współpracy dla uczelni wyższych oraz ośrodków naukowo-badawczych specjalizujących się w technologiach cyberbezpieczeństwa.

Działaniami, które przyczynią się do wzmocnienia potencjału Polski w zakresie cyberbezpieczeństwa będą również: budowa systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa (we współpracy z MON i MR), opracowanie programów studiów dla szkół wyższych w specjalnościach z zakresu cyberbezpieczeństwa (odpowiedzialne za to będą uczelnie), uruchomienie programu pozyskania specjalistów o unikatowych umiejętnościach przez ośrodki analityczne na potrzeby rozwiązywania skomplikowanych problemów z zakresu cyberbezpieczeństwa (MON, MSWiA, ABW).

Ministerstwo aktywnie działa również na arenie międzynarodowej. Polska jest członkiem *European Cyber Security Organization* (ECSO)[2]. Głównym celem organizacji jest wsparcie wszystkich typów inicjatyw lub projektów, których celem jest promocja rozwoju cyberbezpieczeństwa w Europie. ECSO współpracuje w celu realizacji swoich zamierzeń z Komisją Europejską. Ponadto Polska buduje własny krajowy system oceny i certyfikacji – dołączyliśmy do grona państw zrzeszonych w SOGIS[3]. Porozumienie SOGIS reguluje współpracę państw UE i EFTA w obszarze koordynowania polityk certyfikacji wyrobów sektora technologii informatyczno-komunikacyjnych. Dzięki uczestnictwu w porozumieniu Polska będzie mogła samodzielnie wystawiać certyfikaty, zgodnie z normą ISO/IEC 15408 Polska (jest to norma pozwalająca weryfikować bezpieczeństwo systemów teleinformatycznych).

Podkreślić należy, że Polska może się pochwalić jednymi z najlepszych specjalistów w dziedzinie cyberbezpieczeństwa. Potwierdzają to liczne konkursy, olimpiady czy też zawody, w których drużyny polskie zdobywają nagrody, zajmując wysokie miejsca. W roku 2014 Polacy zwyciężyli w zawodach „Capture the Flag", w 2015 w tych samych zawodach zajęli drugie miejsce (zaraz za drużyną z USA). Polski zespół składający się z przedstawicieli MIL-CERT, SKW, CERT-GOV, WAT-u oraz CERT Polska wygrał także międzynarodowe ćwiczenia Locked SHIELDS 2014[4] w zakresie ochrony cyberprzestrzeni.

Trzeba mieć też na uwadze, że jednym z czynników, które wpłyną na sytuację na rynku cyberbezpieczeństwa, będzie zmieniające się otoczenie prawne. Rozporządzenie o ochronie

[2] Więcej informacji na stronie ECSO oraz na stronie Komisji Europejskiej o wspieraniu przemysłu cyberbezpieczeństwa .

[3] Senior Official Group Information Security Systems – więcej informacji na www.sogis.org.

[4] Ćwiczenia organizowane przez NATO Cooperative Cyber Defence Centre of Excellence wraz z estońskimi instytucjami rządowymi i koordynowane z terenów Estonii

danych osobowych[5] i towarzyszące mu ustawy, dyrektywa NIS[6] i implementująca ją ustawa o krajowym systemie cyberbezpieczeństwa oraz dyrektywa PSD2[7], wdrażana obecnie przez Ministerstwo Finansów[8], znacząco zmieniają krajobraz polskich regulacji w zakresie cyberbezpieczeństwa. Pojawią się przepisy regulujące postępowanie z incydentami, wymogi dla zespołów reagowania na incydenty komputerowe jak również dodatkowe wytyczne dla przedsiębiorców świadczących niektóre usługi.

Powyższe działania, w opinii Ministerstwa Cyfryzacji, pozwolą stworzyć silne podstawy organizacyjne i prawne, aby Polska zaistniała jako istotny gracz na arenie międzynarodowej. Polscy specjaliści zyskali uznanie w świecie swoimi umiejętnościami i w naszej opinii, zbudowanie odpowiednich struktur i kompetencji pozwoli nam wykorzystać tą szansę i wzmocnić pozycję naszego kraju w tym obszarze.

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
*/podpisano elektronicznie/*

**Do wiadomości:**
Kancelaria Prezesa Rady Ministrów

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*.

[6] Dyrektywa 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*.

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. *w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE*.

[8] Projekt ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, nr z wykazu UC81.