ZIPSEE
CYFROWA POLSKA

Warszawa, 19 sierpnia 2019r.

**Marek Zagórski**
**Minister cyfryzacji**
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

*Opinia Związku Cyfrowa Polska do projektu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*

Szanowny Panie Ministrze

Projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 to bardzo ważny dokument, który podkreśla potrzebę stworzenia takiego mechanizmu wymiany informacji, który będzie gwarantował ochronę interesów państwa m.in. poprzez ochronę tajemnicy administracji państwowej czy jej wizerunku. Dziś technologie informacyjno-komunikacyjne stanowią podstawę do funkcjonowania w każdym obszarze administracji. Istotne jest to, by działały one bezpiecznie. Niewątpliwie istnieje wyraźna potrzeba wypracowania i wdrożenia przez państwo rekomendacji zarówno w zakresie prawa, jak i zabezpieczeń technicznych.

Niewątpliwym celem, do którego należy wspólnie dążyć w najbliższych latach to zagwarantowanie dostępu do bezpiecznego internetu i usług cyfrowych. Przy czym warto podkreślić, że dotyczy to również bezpiecznego dostępu np. do informacji, które w żaden sposób nie mogą być ograniczane np. ze względów politycznych czy kulturowych.

**Współpraca z sektorem prywatnym**

Zapewnienie cyberbezpieczeństwa to wspólne wyzwanie dla państwa oraz sektora prywatnego. Związek Cyfrowa Polska chętnie włączał się w przeszłości w projekty realizowane przez Ministerstwo Cyfryzacji i deklaruje dalszą współpracę m.in. przy realizacji Strategii. W naszej ocenie zapewnienie cyberbezpieczeństwa będzie efektywne jedynie przy szerokiej współpracy ekspertów z doświadczonych firm działających w tym obszarze. Dobrze byłoby doprecyzować projekt Strategii w zakresie modelu współpracy z samorządami, podmiotami prywatnymi oraz organizacjami pozarządowymi m.in. „w doborze, wdrażaniu i utrzymaniu środków technicznych zwiększających cyberbezpieczeństwo, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych". Warto doprecyzować również punkt Strategii mówiący o współpracy z uczelniami wyższymi w celu stymulowania badań i rozwoju w obszarze cyberbezpieczeństwa tak, by znalazła się tam także kwestia rozwoju sztucznej inteligencji.

**Finansowanie cyberbezpieczeństwa**

W opinii Związku Cyfrowa Polska wyznaczone priorytety w rządowej Strategii Cyberbezpieczeństwa stanowią niezbędną podstawę do rozwoju cyfryzacji w Polsce, w tym sieci 5G przy zachowaniu bezpieczeństwa naszego kraju. Z całą pewnością cyberbezpieczeństwo powinno być zarówno dla administracji publicznej, jak również dla przedsiębiorców i wszystkich obywateli kwestią nadrzędną, dlatego należy zainwestować wszelkie, możliwe środki z budżetu państwa, które są niezbędne do osiągnięcia tego celu. Dlatego warto doprecyzowań w Strategii, jakie środki finansowe należy na cele związane z cyberbezpieczeństwem przeznaczyć. Trudno bowiem założyć – jak jest w Strategii – że „przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego". Warto przypomnieć, że kilka miesięcy temu Komisja Europejska w nowym programie wspierającym cyfryzację w krajach Unii na lata 2021-2027 założyła, że na ochronę gospodarki cyfrowej, społeczeństwa i demokracji w UE poprzez budowanie cyberobrony i unijnego sektora cyberbezpieczeństwa oraz finansowanie najnowocześniejszych urządzeń i infrastruktury cyberbezpieczeństw trzeba będzie przeznaczyć 2 mld euro.

Z całą pewnością są to koszty, które warto ponieść. Bo inwestycje w cyfryzację i cyberbezpieczeństwo są niezbędne do dalszego rozwoju innowacji i nowoczesnej gospodarki konkurencyjnej dla Europy i Świata. Dlatego liczymy, że szczegółowe szacunki finansowe konieczne do wdrażania w życie Strategii oraz ich źródło zostaną doprecyzowane w planie działań na rzecz wdrożenia Strategii.

**Edukacja na temat cyberzagrożeń**

Z danych Cyfrowej Polski wynika, że w Polsce istnieje ogromna skala cyberzagrożeń. W 2017 r. średnio 700 razy na godzinę cyberprzestępcy starali się włamać do naszych prywatnych, firmowych oraz państwowych urządzeń i sieci. A co 4,2 sekundy pojawia się na świecie nowe złośliwe oprogramowanie, które coraz częściej atakuje hardware urządzeń. W przyszłości nowym celem ataków staną się urządzenia typu IoT, których liczba stale rośnie.
Dziś statystyki wskazują, że jedynie 40 proc. pracowników w praktyce myśli o cyberochronie urządzeń końcowych – takich jak komputery, laptopy, drukarki, urządzenia wielofunkcyjne – i w praktyce stosuje odpowiednie mechanizmy. W związku z tym, że tzw. infrastruktura krytyczna – państwowa i prywatna – nieustannie się rozwija, zmienia się również profil i skala cyberzagrożeń. Dlatego tak ważne jest stałe kształcenie i podnoszenie świadomości urzędników administracji publicznej z kwestii związanych z bezpieczeństwem cyberprzestrzeni. Rekomendujemy wprowadzenie specjalnych programów edukacyjnych, które zwiększałyby wiedzę konsumentów o cyberzagrożeniach wynikających ze stosowania urządzeń elektronicznych oraz wskazywały na praktyczne rozwiązania chroniące urządzenia użytkowników przed cyberatakami. Powinny też powstać specjalne wytyczne stosowane przez administrację państwową przy przetargach i zamówieniach publicznych na sprzęt elektroniczny, które dotyczyłyby właśnie cyberbezpieczeństwa. Tak, by docelowo zamawiający urządzenia i usługi, które są narażone na potencjalne cyberataki dokonywali wyborów takich rozwiązań, które gwarantują bezpieczeństwo cyfrowe.



www.zipsee.pl
ZIPSEE Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Zdaniem Cyfrowej Polski wymogiem powinno stać się także to, że administracja publiczna wykorzystuje tylko sprzęt elektroniczny posiadający specjalny krajowy certyfikat bezpieczeństwa, który powinien zostać wprowadzony przez polski rząd. Rekomendacja ta zbieżna jest z zapisami rządowej polityki cyberbezpieczeństwa na lata 2017-2022, w której wskazano, że ważnym elementem zapewnienia tzw. bezpiecznego łańcucha dostaw jest ocena i certyfikacja produktów, a priorytetem jest utworzenie „krajowego systemu oceny". Wprowadzenie odpowiednich zabezpieczeń przed cyberatakami to wspólne wyzwanie dla państwa i sektora prywatnego. Zapewnienie cyberbezpieczeństwa będzie efektywne jedynie wtedy, kiedy będzie istniała szeroka współpraca rządu z ekspertami z doświadczonych firm działających w tym obszarze.

Istotnym krokiem w tym kierunku byłoby również ustalenie zestawu wytycznych dla administracji publicznej dotyczących ochrony przed cyberzagrożeniami w zamówieniach publicznych na urządzenia elektroniczne. Certyfikowany sprzęt i oprogramowanie stanowi podstawę dla bezpieczeństwa cyfrowego. Dlatego warto byłoby, aby na bazie przepisów dotyczących cyberbezpieczeństwa w przetargach premiowano urządzenia, które posiadają odpowiedni certyfikat bezpieczeństwa. W ten sposób poza kryterium ceny brano by pod uwagę to, czy zamawiany sprzęt spełnia wymagane standardy i normy. Tarcza w postaci certyfikowanego sprzętu w połączeniu ze świadomymi użytkownikami znacząco poprawiłaby bezpieczeństwa naszych danych.

**Realizacja celów Strategii**

Choć założenie celów Strategii są słuszne, nie ma jasności, w jaki sposób będzie można ocenić stopień ich realizacji. Proponujemy stworzenie specjalnego harmonogramu, który będzie miernikiem wdrażania Strategii.

Związek Cyfrowa Polska docenia prace jaką Ministerstwo Cyfryzacji pod kierownictwem Pana Ministra wykonało przygotowując projekt Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej. Jednocześnie oferujemy eksperckie wsparcie i jesteśmy do dyspozycji Pan Ministra na dalszych etapach prac nad cyberbezpieczeństwem w Polsce.

Z wyrazami szacunku

Michał Kanownik

Prezes Zarządu
Związek Cyfrowa Polska



www.zipsee.pl
ZIPSEE Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214