Warszawa, dnia 2 listopada 2021 r.

Szanowny Pan
Janusz Cieszyński
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów

Szanowny Panie Ministrze,

W imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców, która zrzesza największe firmy z branży RTV i IT działające w Polsce, a w tym producentów, importerów i dystrybutorów sprzętu elektrycznego i elektronicznego, przekazuję nasze uwagi do *Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne [UD68]* („**Projekt**").

Na wstępie, chciałbym jeszcze raz podkreślić, że Związek Cyfrowa Polska wyraża poparcie dla nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa. Jest ona potrzebna i wyczekiwana przez rynek cyfrowy i nowoczesnych technologii. Cyberbezpieczeństwo musi stać się najważniejszym elementem cyfrowej gospodarki, a bez jednoznacznych, jasno sprecyzowanych regulacji prawnych byłoby to niemożliwe. Niewątpliwie należy pamiętać, że mówiąc o cyberbezpieczeństwie nie wskazujemy interesu jednego czy innego dostawcy usług, ale całościowo określamy bezpieczeństwo narodowe. I właśnie z tej perspektywy należy ocenić narzędzia, jakie daje nowelizacja ustawy dla cyberbezpieczeństwa kraju. Jest to dziś tym bardziej istotne, że w perspektywie czeka nas wdrożenie sieci piątej generacji, która zmieni funkcjonowanie całego rynku nowoczesnych technologii i która da nowe możliwości do rozwoju innowacji. Jednak by w pełni wykorzystać dobrodziejstwa, jakie przyniesie sieć 5G, trzeba przede wszystkim zadbać o jej właściwą cyfrową ochronę, które przełoży się na bezpieczeństwo i konkurencyjność polskiej gospodarki.

Należy również mieć na względzie, że technologie oparte o IT stały się bardzo ważnym elementem infrastruktury krytycznej państwa i są wykorzystywane do zarządzania energetyką, telekomunikacją, transportem, bankowością, służbą zdrowia itd. Ataki na infrastrukturę krytyczną mogą postawić pod znakiem zapytania bezpieczeństwo całego kraju, a nawet regionu. Warto zauważyć, że już w 2016 roku na szczycie Paktu Północnoatlantyckiego w Warszawie, cyberprzestrzeń została uznana za kolejny obszar możliwości prowadzenia przyszłych działań wojennych.

Ataki cybernetyczne

W ostatnim czasie mogliśmy obserwować wiele szczególnie wyrafinowanych ataków na państwa sojusznicze. Przykładowo wagę ryzyka obrazuje niedawny atak cybernetyczny na infrastrukturę Colonial Pipeline – największego operatora rurociągów w Stanach Zjednoczonych. System rurociągów produktów rafinacji ropy naftowej o długości 8850 km w wyniku ataku nie działał przez 5 dni.(Działanie infrastruktury przywrócono po wpłaceniu 5 milionów dolarów okupu).[1]

Na skalę zagrożeń tak w skali państwa jak i dla poszczególnych firm i obywateli wskazuje również przykład oprogramowania złośliwego InvisiMole, które infekuje komputery przejmując nad nimi kontrolę, rejestrując dźwięk oraz wykonując nieautoryzowane zrzuty z ekranów użytkowników. Dopiero po 5 latach wykryto ten atak i sklasyfikowano jako zagrożenie[2]. Również smartfony i tablety narażone są na ataki, w wyniku których uzyskiwany jest zdalny dostęp do urządzenia, jego zasobów, mikrofonu i kamery użytkownika – ofiary ataku.

Pojawiły się również ataki na szczególnie ważne instytucje UE w okresie pandemii, w tym cyberatak na Europejską Agencję Medyczną. O czym poinformowała w komunikacie Komisja Europejska:

„The cyberattack on the European Medicines Agency revealed that unlawfully accessed documents related to COVID-19 medicines and vaccine can have dramatic effects once put on the internet ".[3]

[1] https://www.nbcnews.com/tech/security/colonial-announces-pipeline-restart-says-normal-service-will-take-seve-rcna917
[2] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/
[3] https://op.europa.eu/en/publication-detail/-/publication/e076b7dd-d3ff-11eb-895a-01aa75ed71a1

www.zipsee.pl
Związek 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

W Polsce wg. raportu Computerworld powstałego na zlecenie klastra CyberMadeinPoland:[4]

- **33% wszystkich** i w tym aż 42% dużych przedsiębiorstw zmagało się w ostatnim roku z naruszeniami cyberbezpieczeństwa
- **6% dużych firm** doświadczyło wielokrotnych ataków
- **45% zagrożeń cyberbezpieczeństwa** dotyczyło działania szkodliwego oprogramowania

Ponadto, według danych z corocznych sprawozdań CSIRT, NASK i ABW oraz statystyk policyjnych, stale rośnie liczba postępowań prowadzonych w sprawach z zakresu cyberprzestępczości z art.267 par.1 i 287 par 1 k.k oraz innych przestępstw z wykorzystaniem narzędzi internetowych w tym oszustw internetowych. Za krok w dobrym kierunku uznać należy wzmocnienie służb policyjnych przeznaczonych do walki z cyberprzestępczością i mamy nadzieję, że służyć temu będzie utworzenie Centralnego Biura Zwalczania Cyberprzestępczości (CBZC).

Toolbox 5G

Regulacje zawarte w projekcie, powinny m.in. stanowić podstawę prawną dla budowy bezpiecznej sieci, w tym sieci piątej generacji. Mając to na uwadze oraz w celu zapewnienia harmonizacji i standaryzacji kwestii cyberbezpieczeństwa, za szczególnie ważną uznajemy kwestię pełnej implementacji tzw. "Toolbox 5G" do polskiego prawa, czyli zalecanych przez ENISA[5] i Komisję Europejską zestawu narzędzi związanych z tworzeniem sieci telekomunikacyjnych nowych generacji, a w tym:

„5G Toolbox" zaleca (str. 18),[6] aby wszystkie państwa członkowskie zapewniły stosowanie zabezpieczeń (w tym silną rolę regulatorów krajowych) właściwych i proporcjonalnych

[4] Cyberbezpieczeństwo Polskich Firm 2021 - Raport #CyberMadeInPoland
[5] Agencja Unii Europejskiej ds. Cyberbezpieczeństwa
[6] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

www.zipsee.pl
Związek 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

w odpowiedzi do obecnie zidentyfikowanych, jak i przyszłych ryzyk. W szczególności w zakresie:

- wzmocnienia wymagań bezpieczeństwa dla operatorów (np. dokładnego/precyzyjnego zarządzania dostępem, zasad bezpiecznych działań operacyjnych i monitorowania, ograniczenia outsourcingu specyficznych funkcji, itp.)
- oszacowania profilu ryzyka dla dostawców, a jako konsekwencja wdrożenia właściwych restrykcji dla dostawców wysokiego ryzyka włącznie z ich wykluczeniem

Dostawcy wysokiego ryzyka

Aktualnie projekt ustawy zakłada, że podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia, przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym, operatorzy infrastruktury krytycznej będą musiały wycofać z użytkowania dany sprzęt lub oprogramowanie w ciągu 7 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postulujemy o skrócenie tego okresu do 5 lat, tak jak ma to miejsce w przypadku infrastruktury krytycznej. Takie rozwiązanie nie tylko podniesie poziom cyberbezpieczeństwa poprzez przyspieszenie procesu wymiany sprzętu i elimanacji sprzętu pochodzącego od dostawców wysokiego ryzyka, pozwoli również ustandaryzować i ujednolić regulację w tym zakresie.

Uważamy również, że zakres Ustawy o Krajowym Systemie Cyberbezpieczeństwa w obecnym kształcie jest jednak zbyt szeroki i cechuje go brak jasności co do definicji „dostawców" oraz „sprzętu i oprogramowania". Obecne zapisy sugerują, że wszyscy dostawcy IT, a także wszelkie produkty i usługi IT mogą być potencjalnie objęte zakresem oceny. Takie uniwersalne podejście (tzw. *one-size-fits-all*) do wszystkich podmiotów generuje niepewność prawną dla dostawców, w tym lokalnych MŚP, może negatywnie wpłynąć na innowacyjność i zniechęcić dostawców do inwestowania w Polsce. Może to również prowadzić do zerojedynkowej klasyfikacji dostawców, która może wykluczyć technologie istotne dla polskich organizacji i obywateli.

Zgodnie z art. 66a ust. 8 pkt 2) Projektu opinia Kolegium w przypadku wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka z urzędu, zawiera m.in. „*analizę prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą*

www.zipsee.pl
Związek 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

państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem m.in. przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie […]"

Wskazany przepis, pomimo, że wskazuje konkretne regulacje, które mają być wzięte pod uwagę, rodzi ryzyko uznaniowości. Uprawdopodobnienie jest środkiem zastępczym w stosunku do dowodu, nie dającym pewności, lecz tylko prawdopodobieństwo pewnego faktu. O ile ten zakres analizy ma stanowić tylko część opinii Kolegium, nie stanowi on definitywnej podstawy do uznania dostawcy za dostawcę wysokiego ryzyka. Niemniej warunki do wydania takiej decyzji przez Ministra, również nie są precyzyjne, bowiem w art. 66a ust. 11 Projektu wskazuje jako podstawę „poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi". Zatem należy wskazać, że procedura o uznaniu podmiotu za dostawcę wysokiego ryzyka jest naznaczona nieprecyzyjnością, co może stanowić tym większe zagrożenie dla podmiotów, wobec których może zostać wszczęte postępowanie w przedmiocie uznania za dostawcę wysokiego ryzyka. Jest to w szczególności istotne mając na uwadze ograniczenie środków zaskarżenia w toku procedury uznania za dostawcę wysokiego ryzyka.

Ogólnie rzecz biorąc, nie jest jasne, jakie kryteria zostałyby zastosowane do oceny rzeczywistych zagrożeń i określenia środków w celu ich złagodzenia. W rezultacie potrzebna jest większa jasność i szczegółowość zakresu ustawy, która powinna powstrzymać się od zakazywania technologii, a zamiast tego zapewniać ich zgodność z unijnymi przepisami i normami dotyczącymi ochrony danych i cyberbezpieczeństwa.

Ograniczenie środków zaskarżenia w toku procedury uznania za dostawcę wysokiego ryzyka

Projekt znacznie ogranicza grono podmiotów mogących być stroną postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka, co uniemożliwia ochronę ich praw i interesów. Ograniczona ścieżka odwoławcza, a także brak możliwości zawieszenia decyzji o uznaniu za dostawcę wysokiego ryzyka w toku postępowania przed Sądem Administracyjnym, może istotnie, negatywnie wpłynąć na sytuację podmiotu, wobec którego

www.zipsee.pl
Związek 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

toczy się ww. postępowanie.

Zgodnie z art. 66a ust. 3 Projektu procedura oceny ryzyka dostawcy sprzętu lub oprogramowania ma być oparta na przepisach Kodeksu postępowania administracyjnego („**KPA**") z wyłączeniem jednak tych przepisów, które są kluczowe dla strony postępowania. W postępowaniu nie będą stosowane przepisy następujących artykułów KPA:

Art. 28 – wyłącza się zasadę zgodnie z którą stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek;

Art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;

Art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;

Art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;

Art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu.

Niezależnie w art. 66a ust 7 Projektu wyłączono zastosowanie art. 106 § 5 KPA dot. uprawnienia do złożenia zażalenia na stanowisko organu, które następuje w drodze postanowienia. W praktyce oznacza to, że nie przysługuje zażalenie na opinie Kolegium.

W zamian za ograniczenie zastosowania ww. przepisów, zaproponowano treść art. 66a ust. 4 Projektu, w myśl którego stroną postępowania będzie ten, wobec kogo zostanie ono wszczęte. Oznacza to, że wiele podmiotów (np. przedsiębiorcy telekomunikacyjni) korzystających z produktów, usług i procesów objętych zakresem postępowania zostanie pozbawionych przymiotu strony. Podmioty, które na podstawie ogólnych zasad KPA miałyby pełne prawa strony, w myśl projektu zostaną całkowicie pozbawione możliwości udziału i obrony swych praw w toku postępowania administracyjnego.

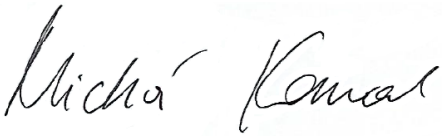
Dodatkowo zgodnie z art. 66a ust. 15 Projektu od decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, nie przysługuje wniosek o ponowne rozpatrzenie sprawy. Zgodnie zaś z art. 16 par. 1 KPA, decyzje, od których nie służy odwołanie w administracyjnym toku instancji lub wniosek o ponowne rozpatrzenie sprawy, są ostateczne.

Uchylenie lub zmiana takich decyzji, stwierdzenie ich nieważności oraz wznowienie postępowania może nastąpić tylko w przypadkach przewidzianych w kodeksie lub ustawach szczególnych. Zatem w tej sytuacji, pozostaje złożenie skargi do Sądu administracyjnego. W tym względzie należy zwrócić uwagę, że zgodnie art. 66d ust. 1 Projektu wyłączono jawność posiedzenia Sądu administracyjnego rozpatrującego skargę na decyzje. Powyższe znajduję uzasadnienie ze względu na wrażliwą materie potencjalnych postępowań. Co jednak może budzić wątpliwości to brzmienie art. 66d ust. 3 Projektu, który stanowi, że Sąd administracyjny nie może wstrzymać wykonalności decyzji, o której mowa w art. 66a ust. 11, po wniesieniu skargi na tę decyzję. Zatem nawet w przypadku wszczęcia postępowania przez Sądem administracyjnym, decyzja o uznaniu za dostawcę wysokiego ryzyka pozostanie wykonywana, przez co zainteresowany podmiot może zostać narażony na znaczne konsekwencje gospodarcze.

Konkludując, mamy nadzieję że nowelizowana ustawa o Krajowym Systemie Cyberbezpieczeństwa stanowić będzie kolejny krok w podniesieniu poziomu cyberbezpieczeństwa Polski, zarówno w sektorze publicznym, jak i prywatnym oraz, że służyć będzie ochronie zarówno państwa jak i obywateli.

Pozostajemy do dyspozycji Pana Ministra na dalszym etapie procedowania projektu ustawy.

Z wyrazami szacunku,
Michał Kanownik



Prezes Zarządu
Związek Cyfrowa Polska

Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego - ZIPSEE Cyfrowa Polska

www.zipsee.pl

Związek 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