Warszawa, dnia 18 stycznia 2024 r.

Szanowny Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów,
Minister Cyfryzacji

Szanowny Panie Premierze,

w imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców, która zrzesza branżę nowoczesnych technologii, chciałbym przedstawić kluczowe kwestie i rekomendacje w obszarze cyberbezpieczeństwa, w kontekście spodziewanych prac nad nowelizacją Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC).

Na wstępie chciałbym podkreślić że, popieramy wszelkie formy współpracy pomiędzy administracją publiczną, a branżą technologiczną (m.in. doceniamy inicjatywę PWCyber) i apelujemy o aktywne tworzenie programów szkoleniowych zwiększających świadomość zagrożeń i promujących cyber-higienę. Rekomendujemy również opracowanie planów ewakuacji infrastruktury krytycznej do chmury, zgodnie z Narodowym Programem Ochrony Infrastruktury Krytycznej. W tym kontekście niezwykle ważne jest ustanowienie trwałych i skutecznych prawnych ram wymiany danych pomiędzy UE i USA oraz przygotowanie do wdrożenia europejskiej i krajowej legislacji w zakresie cyberbezpieczeństwa (w tym: NIS 2, CER, CRA).

Szczególnie należy mieć na uwadze Dyrektywę NIS2, która weszła w życie 16 stycznia 2023 r. zaś do dnia 17 października 2024 r. państwa członkowskie mają czas na jej implementację do krajowych porządków prawnych.

Najistotniejsze kwestie regulowane Dyrektywą polegają na zwiększeniu odporności i zmniejszeniu podatności podmiotów świadczących usługi kluczowe w zakresie cyberbezpieczeństwa. Polega także na poszerzeniu katalogu podmiotów, które należy uznać za dostawców usług kluczowych o m.in. dostawców usług chmury obliczeniowej, przedsiębiorstwa związane z przemysłem kosmicznym; administrację publiczną działającą na szczeblu centralnym i regionalnym.

Wprowadzeniu kryterium wielkości – zgodnie z nowymi przepisami, każdy średni lub duży podmiot działający w sektorach uregulowanych w NIS2 będzie podlegał przepisom Dyrektywy, a w podziale na dostawców usług kluczowych na niezbędnych - listę 11 sektorów zawiera załącznik nr I do Dyrektywy (np. banki, administracja publiczna, infrastruktura cyfrowa czy dostawcy żywności) oraz ważnych – załącznik nr II do Dyrektywy (np. dostawcy usług cyfrowych, firmy kurierskie).

Odnosząc się już bezpośrednio do UKSC, jako Związek wyrażamy poparcie dla jak najszybszej nowelizacji 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 wdrażana jest sieć 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, która przełoży się na bezpieczeństwo i konkurencyjność polskiej gospodarki.

Postulujemy by projekt UKSC uwzględniał unijne narzędzia 5G Toolbox[1], które mają za zadanie ograniczenie cyber-ryzyk dla europejskich sieci 5G. Uważamy także, że dla utrzymania cyberbezpieczeństwa dla tynku telekomunikacyjnego i komunikacji elektronicznej, Ustawa musi dawać instrumenty, które pozwalają państwu na eliminowanie z obrotu rozwiązań - zarówno sprzętowych jak i oprogramowania - stanowiące zagrożenia dla bezpieczeństwa państwa, przedsiębiorców, jak i obywateli.

Uważamy, że metoda regulacji oparta na analizie ryzyk i wykorzystująca wspólne instrumenty Unii Europejskiej z tzw. Toolbox 5G jest właściwa. Należy bazować na podmiotowej ocenie ryzyka, która odbywa się przez pryzmat dostawcy sprzętu lub oprogramowania. Jest to podejście trafne, jeśli chodzi ryzyko opisane jak *„R.5 State interference through 5G supply chain"*, zgodnie z analizą ryzyk, opracowaną na poziomie EU w dokumencie 5G Toolbox.

[1] 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

Podejście to choć wyjściowo słuszne, ma jednak jedną zasadniczą wadę - w dzisiejszym zglobalizowanym świecie przynależność geograficzna dostawców nie jest stała, więc również oparcie się wyłącznie na kryterium kraju pochodzenia może okazać się nieskuteczne już w perspektywie kilku lat. Przykładowo niedawno jeszcze nikt nie przypuszczał, że cały brytyjski przemysł samochodowy znajdzie się w rękach inwestorów poza UE i NATO. Tak samo niewielu spodziewało się, że największy grecki port w Pireusie będzie własnością chińskich inwestorów. **Tak więc kryterium geopolityczne, jakkolwiek ważne dla bezpieczeństwa (w tym także cyberbezpieczeństwa), powinno zostać wzmocnione dodatkowymi mechanizmami.**

Jednocześnie należy wskazać, ze ryzyka opisane w diagnozie 5G Toolbox są znacznie szersze i bardziej różnorodne. Jednym z najbardziej jaskrawych jest „*R4. Dependency on a single supplier"*. Stan obecny w Polsce wskazuje, ze sprzęt i oprogramowanie od jednego dostawcy stanowią dziś ok. 65 proc. całej infrastruktury LTE i 5G na terenie kraju, a w przypadku niektórych operatorów jest to ponad 80 proc. ich zasobów sieciowych. Jest to zjawisko głęboko niepożądane, gdyż problem z jednym tylko dostawcą stawia pod znakiem zapytania cyberbezpieczeństwo około 2/3 sieci LTE/5G w kraju, a pozostała część sieci nie ma szans obsłużyć nawet najbardziej niezbędnego ruchu. Z punktu widzenia bezpieczeństwa sieci, a także bezpieczeństwa państwa, należałoby w UKSC wprowadzić środki zaradcze, które adresują to właśnie zjawisko.

Zgodnie z przyjętym również przez Polskę na szczeblu europejskim dokumentem 5G Toolbox rozwiązaniami adresującymi to ryzyko są:

- dywersyfikacja dostawców,
- zrównoważony i zróżnicowany łańcuch dostaw i wartości 5G.

Ich skuteczność w opracowanym 5G Toolbox określono jako „bardzo wysoką" (Very High) i one jako jedyne adresują to właśnie ryzyko. W naszej opinii UKSC jest odpowiednim aktem prawnym, aby stosowanie tych środków zaradczych wprowadzić – zawarcie tych rozwiązań w przyszłych aktach wykonawczych, a więc w aktach niższego szczebla (np. rozporządzeń Ministerstwa Cyfryzacji) może w przyszłości wzbudzać wątpliwości legislacyjne.

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

Wdrożenie dywersyfikacji oraz zrównoważonego łańcucha dostaw i wartości do projektu ustawy jest możliwe, ale wymaga spojrzenia przez pryzmat podmiotów budujących sieć, a nie dostawców sprzętu i oprogramowania. Oczywistym adresatem będą operatorzy sieci (obecni oraz przyszli), ale także podmioty budujące sieci lokalne w modelu Private Networks, Smart City i podobnych. Kluczowym elementem takiej oceny będzie więc nie tyle kraj pochodzenia danego sprzętu lub oprogramowania, co parytet sprzętu i oprogramowania pochodzącego od jednego dostawcy w całej sieci krajowej (danego operatora/ operatora lokalnego). Oczywiście inne ryzyka także muszą być mitygowane. Wydaje się, że obowiązek dywersyfikacji powinien zostać wprowadzony przede wszystkim dla sieci o zasięgu krajowym, a także dla sieci o znaczeniu strategicznym dla bezpieczeństwa państwa. Przykładem mogą być sieci prywatne 5G, które powstaną w kluczowych zakładach i obiektach (typu rafinerie, gazoporty, lotniska).

Podejście do tego tematu powinno uwzględniać zarówno dywersyfikacje horyzontalną (ilościową, geograficzną), jak i wertykalną (zróżnicowanie na poziomie różnych elementów sieci).

Dywersyfikacja horyzontalna oznacza, że żaden podmiot posiadający sieć lub ją budujący nie opiera się na jednym dostawcy, a więc np. maksymalnie połowa infrastruktury może pochodzić od jednego dostawcy. Rozwiązanie zbliżone do tego podejścia wdraża Wielka Brytania. W tym modelu wystąpienie incydentu poważnie zagrażającego cyberbezpieczeństwu państwa jest siłą rzeczy ograniczone terytorialnie oraz podmiotowo (ponieważ działa kilka konkurujących sieci).

Dywersyfikacja wertykalna oznacza, że łańcuch wartości w sieci jest zróżnicowany, a więc różne elementy sieci kompatybilne ze sobą nawzajem pochodzą od różnych dostawców. Dzięki temu podejściu możliwe jest budowanie sieci z uwzględnieniem obszarów infrastruktury krytycznej (tylko bezpieczni dostawcy) oraz pozostałych (większa swoboda zakupowa, bo mniejsze ryzyko). Podejście to również jest stosowane w kilku krajach budujących swoje sieci 5G. Dzięki temu podejściu sieci budowane w modelu *non-stand-alone* łatwiej jest dostosować do nowych wymagań cyberbezpieczeństwa, ponieważ urządzenia peryferyjne nie generujące ryzyka, mogą pozostać na swoim miejscu, a właściciele sieci zbudowanej na komponentach od jednego, ryzykownego dostawcy, muszą zadbać o wymianę infrastruktury krytycznej, a nie całej sieci. Oczywiście jest to możliwe przy założeniu, że dostawcy Ci udostępnią interfejsy swoich urządzeń i oprogramowania w taki sposób, aby była możliwa konfiguracja całego zestawu ze sprzętu i oprogramowania różnych dostawców.

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

Rozwiązaniem najlepiej adresującym problem dywersyfikacji wertykalnej są otwarte (z definicji) interfejsy, oparte o powszechnie przyjęte międzynarodowe standardy. Przykładem takiego rozwiązania jest model Open RAN, w którym poszczególne elementy infrastruktury aktywnej mogą pochodzić od różnych dostawców i żaden dostawca nie ma kontroli nad całością sieci.

Podsumowując, wdrożenie do porządku prawnego dywersyfikacji horyzontalnej i jednocześnie wertykalnej daje szanse na uodpornienie infrastruktury na zależność od jednego dostawcy i jest to znakomite rozwiązanie zabezpieczające o charakterze geopolitycznym.

Dla wdrożenia dywersyfikacji w projekcie legislacyjnym UKSC należy zaproponować przepisy, przyznające Ministrowi właściwemu do spraw informatyzacji, po zasięgnięciu opinii właściwego kolegium, kompetencji do określania w drodze rozporządzenia, maksymalnego parytetu udziału jednego dostawcy w sieci publicznej (czyli w skali sieci jednego), przynajmniej w zakresie infrastruktury krytycznej.

Należałoby również wprost wymagać stosowania otwartych interfejsów dla poszczególnych elementów infrastruktury sieciowej, jako środka pozytywnie wpływającego na ocenę ryzyka.

Należy też podkreślić, że dziś zagrożenie w cyberprzestrzeni jest dużo bardziej prawdopodobne niż zagrożenia czysto militarne-siłowe. Dlatego, choć niektórzy zdają sobie to lekceważyć, cyberbezpieczeństwo jest absolutnym priorytetem dla funkcjonowania państwa. Dziś cyberzagrożenia coraz częściej dotyczą np. infrastruktury krytycznej. Zaś nieustanny rozwój sztucznej inteligencji czy Internetu Rzeczy oznacza, że w najbliższej przyszłości będą one dotyczyły np. całych miast (smart cities). Dlatego ustawa musi być ogólna, dawać szerokie i narzędzia, by zapewnić cyberbezpieczeństwo w stale zmieniających się warunkach. Z tego punktu widzenia ustawa musi obejmować całość rynku i operatorów telekomunikacyjnych. W kontekście cyberbezpieczeństwa mówimy nie tylko o ochronie czy przesyłaniu danych, ale również o stabilności funkcjonowania państwa. Nie możemy pozwolić sobie na cień ryzyka odnośnie stabilności i funkcjonowania sieci.

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

Dostawcy wysokiego ryzyka

Pierwotny projekt UKSC procedowany w poprzedniej kadencji Sejmu zakładał, 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 4 lat oraz do 12 miesięcy w przypadku infrastruktury krytycznej – analogicznie do rekomendacji przedłożonych przez Radę do Spraw Cyfryzacji. [2] Postulujemy również bezwzględnie i niezwłocznie wykluczyć takie podmioty z dalszych zakupów sprzętu oraz usług. 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.

Konkludując, mamy nadzieję, że znowelizowana 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.

Jako organizacja branżowa pozostajemy do dyspozycji Rady Ministrów w procesach konsultacyjnych oraz mamy nadzieję na owocną współpracę w zakresie dyskusji o cyfrowych politykach publicznych.

Z wyrazami szacunku,

Michał Kanownik

Prezes Zarządu

Związek Cyfrowa Polska

[2] https://www.gov.pl/attachment/0896ec46-0a30-4b13-bbaf-a9640e0404b6

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