Warszawa, 23 maja 2024 r.

Szanowny Pan
Dariusz Standerski
Sekretarz Stanu,
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców, która zrzesza branżę nowoczesnych technologii, przesyłam nasze stanowisko do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).*

Na wstępie chciałbym podkreślić, że oceniamy bardzo pozytywnie ogólny cel projektu (m.in. implementację dyrektywy, tzw. NIS2) i większość zaproponowanych rozwiązań, w tym odwołania do 5G toolbox w zakresie Dostawców Wysokiego Ryzyka, zwłaszcza w zakresie kryteriów technicznych jak i nietechnicznych ich oceny. W tym miejscu polecamy uwadze raport Strand Consult[1] dotyczący dostawców do europejskich operatorów.

Co więcej uważamy, że niezwłoczne przyjęcie proponowanych przepisów jest niezbędne ze względu na skalę cyberzagrożeń, zwłaszcza w kontekście geopolitycznej sytuacji Polski. Postulujemy więc o jak najszybsze procedowanie przedmiotowego projektu.

Pragniemy jednak zwrócić uwagę na fakt, że niektóre przepisy wymagają doprecyzowania, bowiem w wersji poddanej konsultacjom - w wielu przypadkach - wykraczają poza intencje unijnych prawodawców tworząc nadregulację. Pozostawienie ustawy w aktualnym brzmieniu może pociągnąć za sobą szereg negatywnych konsekwencji dla systemu cyberbezpieczeństwa

[1] https://strandconsult.dk/there-are-many-myths-about-china-and-its-technology-suppliers-the-eu-published-a-report-you-should-read/

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

oraz otoczenia gospodarczego, a także rodzi ryzyko stworzenia aktu niezgodnego z prawem Unii Europejskiej. Poniżej chcielibyśmy się odnieść do kilku kluczowych zagadnień.

Dyrektywa NIS2 nie definiuje terminu „organu zarządzającego", a jedynie wykorzystuje go w ramach trzech odniesień, które dotyczą wymagań w zakresie zarządzania. Tymczasem w projekcie przedstawionym przez Ministerstwo Cyfryzacji (art. 2 pkt 8a) określenie "organ zarządzający" zostało zastąpione terminem "kierownik jednostki" z bezpośrednim odwołaniem interpretacyjnym do art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), co sprawia, że przepisy interpretacji mają swoje zastosowanie nie tylko wobec członków zarządu danego podmiotu, ale także osób odpowiedzialnych (w danym momencie) za zarządzanie tym podmiotem.

Państwa członkowskie zapewniają w NIS2, że organy zarządzające podmiotów kluczowych i ważnych zatwierdzają środki zarządzania ryzykiem cyberbezpieczeństwa podjęte przez te podmioty w celu przestrzegania artykułu 21, nadzorują ich wdrażanie oraz mogą ponosić odpowiedzialność za naruszenia tego artykułu przez te podmioty. Polski projekt implementacji określa obowiązki szefów podmiotów kluczowych i ważnych (art. 8c do 8e) oraz zasady związane z karami finansowymi, które mogą być na nich nałożone (art. 73a). Kara może być nałożona w dwóch przypadkach:

a. jeśli szef jednostki nie wypełnił swoich obowiązków wynikających z polskiej implementacji NIS2, wymienionych w art. 73a projektu, lub
b. jeśli podmiot kluczowy ub ważny nie wypełnił swoich obowiązków wynikających z projektu implementacji NIS2, wymienionych w art. 73 krajowego projektu implementacji.

Kwota kary nie może przekroczyć 600% wynagrodzenia otrzymanego przez ukaraną osobę, obliczonego zgodnie z zasadami dotyczącymi ustalania ekwiwalentu pieniężnego za urlop. Takie uszczegółowienie w sposób istotny odbiega od zasad określonych w dyrektywie. Kara taka powinna uwzględniać zdolność finansową szefa jednostki.

Projekt wykracza poza założenia dyrektywy, przyznając władzom szersze uprawnienia egzekucyjne zarówno wobec podmiotów kluczowych, jak i ważnych. Organ właściwy do spraw cyberbezpieczeństwa w myśl projektu może bowiem:

- żądać zawieszenia, ograniczenia zakresu lub cofnięcia licencji lub autoryzacji przyznanej jednostce, lub usunięcie jednostki z rejestru działalności regulowanej,

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

- żądać tymczasowego zakazu pełnienia funkcji przez szefa podmiotu kluczowego lub ważnego,
- powołać decyzją na określony czas spośród osób zatrudnionych w biurze obsługującym organ inspektora monitorującego wykonywanie obowiązków wymienionych w rozdziale 3,
- wymagać od podmiotów kluczowych i ważnych przeprowadzenia audytów bezpieczeństwa oraz oceny bezpieczeństwa systemów informacyjnych.

Należy w tym miejscu zauważyć, że przyznanie władzom szerszych uprawnień egzekucyjnych może prowadzić do nadmiernej ingerencji w działalność podmiotów kluczowych i ważnych, a przez to do destabilizacji ich funkcjonowania. Sugerujemy ponowne rozważenie proponowanych przepisów, aby znaleźć bardziej zrównoważone podejście, które zapewni bezpieczeństwo, jednocześnie minimalizując ryzyko nadmiernych obciążeń i zakłóceń dla podmiotów kluczowych i ważnych.

W dyrektywie możemy przeczytać (art. 36 Dyrektywy): “Państwa członkowskie ustanawiają przepisy dotyczące kar stosowanych wobec naruszeń krajowych środków przyjętych zgodnie z niniejszą dyrektywą oraz podejmują wszelkie niezbędne środki, aby zapewnić ich wdrożenie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.” Polski projekt implementacji w art. 73 ust.1 określa kary finansowe, które mogą być nałożone na podmioty kluczowe lub ważne. Maksymalne kwoty kar przewidziane w polskim projekcie ustawy są takie same jak w NIS2, z dwoma wyjątkami, gdzie organ właściwy może nałożyć wyższe kary tj. karę w wysokości do 100 000 000 PLN oraz karę w wysokości od 500 PLN do 100 000 PLN za każdy dzień opóźnienia.

Przewidziane kary mogą być nieproporcjonalne w stosunku do naruszeń. Wysokie kary za nieznaczne uchybienia mogą prowadzić do nadmiernej represji i nieproporcjonalnego obciążenia podmiotów kluczowych lub ważnych. Ponadto przyznanie organom władzy możliwości nakładania wysokich kar oraz decydowania o zawieszeniu lub cofnięciu licencji może prowadzić do ryzyka arbitralności i nadużycia władzy. Proponujemy ponowne przeanalizowanie wysokości kar oraz wprowadzenie mechanizmów zapewniających proporcjonalność i sprawiedliwość w egzekwowaniu przepisów.

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

Dyrektywa NIS2 zakłada, że państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych używania określonych produktów ICT, usług ICT i procesów ICT, opracowanych przez podmiot kluczowy lub ważny, albo pozyskanych od stron trzecich, które są certyfikowane w ramach europejskich schematów certyfikacji cyberbezpieczeństwa przyjętych zgodnie z artykułem 49 rozporządzenia (UE) 2019/881. Tymczasem projekt implementacji nie zobowiązuje podmiotów kluczowych lub ważnych do korzystania z konkretnych produktów ICT. Równocześnie pojawia się upoważnienie dla rządu w zakresie wydawania rozporządzeń określających konkretne wymagania dla systemów zarządzania informacją dla różnych rodzajów działalności prowadzonych przez podmioty ważne lub kluczowe.

W zakresie zasad dotyczących zgłaszania znaczących incydentów, opiniowany projekt implementacji wykracza poza dyrektywę NIS2 w zakresie:

a) Przedsiębiorcy komunikacji elektronicznej są zobowiązani do zgłaszania wczesnego ostrzeżenia o poważnym incydencie bez zbędnej zwłoki, nie później niż 12 godzin od jego wykrycia (art. 11 ust. 1a projektu polskiej ustawy implementującej).
b) Zgodnie z art. 2 pkt 7 projektu, poważny incydent jest opisany między innymi jako incydent, który wpływa na inne podmioty powodując szkodę materialną lub niematerialną (w porównaniu z definicją w art. 23 ust. 3 lit. b dyrektywy NIS2, projekt nie zawiera odniesienia do „znacznej" szkody oraz do incydentu, który nie tylko wpływa, ale również „może wpływać" na osoby).
c) Zgodnie z art. 2 pkt 20 projektu poważne zagrożenie cybernetyczne to zagrożenie cybernetyczne, które ze względu na swoje cechy techniczne może mieć poważny wpływ na bezpieczeństwo systemów informatycznych powodując szkodę materialną lub niematerialną (w porównaniu z definicją w art. 6 (11) dyrektywy NIS2, polski projekt nie zawiera odniesienia do „znacznej" szkody). Projekt jedynie przewiduje, że rząd wyda rozporządzenie określające progi uznania incydentu za poważny incydent, z uwzględnieniem sektorów i podsektorów.

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

Art. 8 projektu zawiera przepis dotyczący systemu zarządzania bezpieczeństwem informacji oraz enumeratywne wyliczenie funkcji, które ma ten system zapewnić. Przepisy ustawy z oczywistych przyczyn zawierają sformułowania ogólne, a jednocześnie liczba podmiotów objętych nowymi przepisami i różnorodność sektorów, z których się wywodzą jest znaczna. Pojawia się tutaj problem polegający na skierowaniu konkretnych wymogów do przedsiębiorców bez jednoczesnego wskazania na to, czy kierunek, wg którego podejmują oni działania i wprowadzają do swoich systemów zmiany – jest wg organu właściwego słuszny i wypełnia oczekiwania, a przede wszystkim jest zgodny z przepisami. Ma to szczególne znaczenie w kontekście ust. 4 omawianego przepisu, w której podmioty objęte ustawą mają uwzględniać podatności danego dostawcy oraz „ogólną jakość produktów ICT (…)". W ustawie jest to rozwiązane na dwa sposoby: przede wszystkim art. 67a przewiduje fakultatywne działanie Pełnomocnika ds. cyberbezpieczeństwa w postaci wydania stosownych rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa – jest to formuła aktów prawa miękkiego – stosunkowo elastyczna dla przedsiębiorców. Warto byłoby zastanowić się, czy przepis nie powinien zmierzać w kierunku obligatoryjnego działania Pełnomocnika ds. cyberbezpieczeństwa, który uzupełnia przepisy stosownymi rekomendacjami/przewodnikami dla przedsiębiorców.

W art. 8a wskazano fakultatywną możliwość działania Rady Ministrów w drodze rozporządzenia – o ile to działanie będzie miało charakter wiążący dla przedsiębiorcy, to wyznaczenie Rady Ministrów jako organu właściwego może okazać się nieefektywne dla całego procesu zapewnienia zgodności systemów zarządzania bezpieczeństwem informacji.

Przepisy różnicują termin na zgłoszenie wczesnego ostrzeżenia o incydencie poważnym – dla podmiotów ważnych i kluczowych 24 godziny zgodnie z przepisami NIS2, a dla przedsiębiorcy komunikacji elektronicznej – 12 godzin od momentu jego wykrycia. Sugerujemy, żeby zgodnie z przepisami dyrektywy NIS2, ustawodawca trzymał się terminu 24 godziny na zgłaszanie takich incydentów. Termin 12 godzin jest ekstremalnie krótki, przy uwzględnieniu warunków pracy przedsiębiorcy.

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 zakresie Dostawców Wysokiego Ryzyka:

1) w Art. 67c ust 1 pkt 1) – chcielibyśby wnioskować o **wprowadzenie zasady proporcjonalnego wycofania** z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15.
w Art. 67c ust 2 – chcielibyśmy wnioskować o **skrócenie terminu i rozróżnienie warunków dla infrastruktury krytycznej. Wnioskujemy o wycofanie sprzętu HRV w ciągu: (i) 1 roku dla infrastruktury krytycznej w geograficznie wrażliwych obszarach (np. bazy wojskowe, instalacja militarne/ NATO, budynki administracji publicznej)i (ii) w ciągu 3 lat dla pozostałej infrastruktury krytycznej proporcjonalnie w każdym roku, z uwzględnieniem pierwszeństwa obszarów o największej gęstości zaludnienia**
Uzasadnienie:

   Aby zapewnić stopniowe wycofywanie w celu ograniczenia zidentyfikowanych ryzyk z wyznaczonymi dostawcami wysokiego ryzyka, a tym samym stale wzmacniać cyberbezpieczeństwo kraju, zaleca się stopniową, ale proporcjonalną fazę wycofania sprzętu HRV.

2) Załącznik nr 3 pkt 3 – proponujemy, by temu punktowi nadać brzmienie: **“5G, 3GPP release 15 and onwards, Radio Base Station Baseband Unit and other features such as Radio Units and antennas”** - zamiast istniejącego “5G Radio Base Station Baseband Unit and other features”. Pozwoli to uniknąć wątpliwości interpretacyjnych.

   Uzasadnienie:
   Zmiana brzmienia Punktu 3 Załącznika nr 3 poprzez odniesienie się do 3GPP release 15 i późniejszych, a także rozróżnienia elementów stacji bazowej na Baseband, Radio Unit oraz anteny pozwoli na jednoznaczne odniesienie się do międzynarodowych standardów 3GPP, w których po raz pierwszy pojawiła się technologia 5G (i jego kolejnych iteracji), a także wskazuje wprost elementy, z jakich składa się stacja bazowa i pozwoli na uniknięcie naditerpretacji zapisu w jego pierwotnej formie.

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

3) Art. 67b ust 9 – postulujemy o poszerzenie katalogu podmiotów, które *mogą przedstawić ministrowi właściwemu do spraw informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT,* również o Związki Pracodawców, działających na postawie Ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców.

Pozostajemy do dyspozycji Pana Ministra.

Z wyrazami szacunku,

Michał Kanownik

Prezes Zarządu

Związek Cyfrowa Polska