Warszawa, 31 stycznia 2023 r.

Szanowny Pan
Jacek Oko
Prezes Urzędu Komunikacji Elektronicznej

Szanowny Panie Prezesie,

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, przesyłam naszą opinie w ramach trwających konsultacji aukcji na cztery rezerwacje częstotliwości z pasma 3,6 GHz.

W naszym stanowisku chcielibyśmy zaakcentować kwestię cyberbezpieczeństwa, jako kluczową dla wdrożenia i właściwego funkcjonowania sieci piątej generacji.

W tym celu niezbędne jest zastosowanie zestawu narzędzi UE w zakresie cyberbezpieczeństwa 5G jako skoordynowanego podejścia europejskiego w oparciu o wspólny zestaw środków, aby ograniczyć główne zagrożenia dla cyberbezpieczeństwa sieci 5G (szczególnie w zakresie SMO3 i SMO4).

W oparciu o EU toolbox on 5G Cybersecurity oraz nasze doświadczenie, rekomendujemy kilka poniższych działań.

Jeżeli sprzedawca/producent zostanie uznany za Dostawcę Wysokiego Ryzyka:

- Należy go niezwłocznie wykluczyć z dalszych zakupów zarówno sprzętu jak i usług
- W oparciu o nasze doświadczenie rynkowe, w tym znajomość zmiany procesów technologicznych, rekomendujemy wykluczyć taki sprzęt z dalszego użytkowania w ciągu nie dłuższym niż 3 lata oraz opracować kompleksowe plany corocznego, proporcjonalnego wykluczenia takiego sprzętu w okresie 3-letnim

- Natomiast w oparciu o obecny kształt projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa należy całkowicie wykluczyć taki sprzęt z dalszego użytkowania w ciągu nie dłuższym niż 5 lat oraz opracować kompleksowe plany corocznego, proporcjonalnego wykluczenia takiego sprzętu w okresie 5-letnim

Ogólne rekomendacje jakie powinny być wzięte pod uwagę przy ocenie ryzyk:

- Należy pamiętać, że operator, który przeprowadzi ocenę ryzyka, może to zrobić wyłącznie z perspektywy własnej sieci. Bezpieczeństwo sieci telekomunikacyjnych dotyka interesów bezpieczeństwa narodowego, które mogą być oceniane jedynie przez właściwe niezależne organy.
- Ponadto operator dokonujący samooceny ryzyka, może być narażony na konflikt interesów ze względu na swój interes komercyjny i relacje handlowe. Pojawia się więc pytanie o obiektywność takiej samooceny. Dlatego postulujemy przeniesienie oceny ryzyka na niezależny podmiot zewnętrzny.
- Dodatkowo podmiot dokonując oceny ryzyka, musi wziąć pod uwagę regulacje prawne kraju, z którego pochodzi dostawca. Na świecie istnieją kraje, w których miejscowe prawo bezwarunkowo obliguje podmioty fizyczne oraz przedsiębiorstwa, do przekazywania na żądanie danych użytkowników, co w sposób oczywisty zagraża bezpieczeństwu narodowemu oraz jego obywateli, a także przedsiębiorców. Ocena uwarunkowań prawnych kraju pochodzenia sprzętu nie powinna być zadaniem prywatnych firm czy operatorów. Oceny ryzyka powinien dokonywać kompetentny i niezależny organ odpowiedzialny za bezpieczeństwo, np. Agencja Bezpieczeństwa Wewnętrznego

Podsumowując, z naszego punktu widzenia, ale także mając na względzie obiektywne bezpieczeństwo infrastruktury, niezwykle istotne jest uszczelnienie systemu wobec podmiotów, które mogłyby w sposób nieuprawniony administrować danymi lub w inny sposób negatywnie oddziaływać na bezpieczeństwo i stabilność sieci. Co więcej, dokonując analizy potencjalnego ryzyka, należy mieć na uwadze, by podmiot dokonujący analizy był

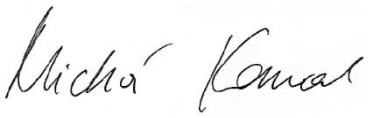
www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

maksymalnie bezstronny i kompetentny oraz nie miał powiązań biznesowo-handlowych z ocenianym podmiotem, co zapewne wpływałoby na wynik oceny.

Pozostajemy do dyspozycji na dalszym etapie wdrożenia sieci piątej generacji.

Z wyrazami szacunku,

Michał Kanownik



Prezes Zarządu

Związek Cyfrowa Polska