Stanowisko Rady do Spraw Cyfryzacji w sprawie rządowego projektu ustawy o zmianie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz innych regulacji i instrumentów mających na celu wzmocnienie cyberbezpieczeństwa w Polsce z dnia 15 grudnia 2024 r. skierowane do Prezesa Rady Ministrów.

Polska stanowi obecnie jeden z najczęściej atakowanych cyfrowo krajów, nie tylko w Europie, ale i na świecie. Granica naszego kraju stanowi jednocześnie wschodnią granicę Unii Europejskiej. Tuż za nią toczy się nieprzerwanie już od ponad 1000 dni wojna na Ukrainie, zaś w Polsce coraz intensywniej odczuwamy skutki wojny hybrydowej i cyberataków naszych adwersarzy. W związku z tą wojną, ale także wobec szerszego kontekstu geopolitycznego, Polska staje w obliczu bezprecedensowego wyzwania w sferze bezpieczeństwa narodowego, w tym w obszarze cyberbezpieczeństwa.

Liczba ataków na infrastrukturę krytyczną w Polsce, w tym na naszą infrastrukturę telekomunikacyjną, nieustannie rośnie i nie ma żadnych przesłanek, by sądzić, że ta niepokojąca sytuacja ulegnie zmianie na lepsze.

Ostatnie lata przynoszą stały wzrost liczby ataków cyfrowych i incydentów cyberbezpieczeństwa[1]. Nie ulega zatem wątpliwości, że infrastruktura podmiotów krajowego systemu cyberbezpieczeństwa musi opierać się o bezpieczne rozwiązania pochodzące od zaufanych dostawców, a w jej konstrukcji nie ma miejsca na elementy obarczone wysokim ryzykiem.

W związku z powyższym **Rada do spraw Cyfryzacji wyraża swoje pełne poparcie dla wszelkich rządowych inicjatyw regulacyjnych i dla prawodawstwa w sferze cyberbezpieczeństwa, mającego na celu zapewnienie odpowiedniego poziomu odporności cyfrowej naszego kraju.**

W szczególności opowiadamy się za pilnym przyjęciem nowelizacji ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UC32)[2], stanowiącej implementację Dyrektywy NIS2[3], której termin wdrożenia dla krajów członkowskich upłynął w dniu

[1] Statystyki CSIRT NASK za ostatnie lata przedstawiają się następująco:

Okres	Cyberzagrożenia zgłoszone do CSIRT NASK	Incydenty zgłoszone do CSIRT NASK
2021	115 884	29 442
2022	320 210	39 621
2023	364 848	79 978
01.01.2024-28.11.2024	547 354	97 273

Źródło: https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska?page=1&per_page=50&q=&sort=-data_date&model=resources .

[2] https://legislacja.rcl.gov.pl/projekt/12384504.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, s. 80).

17 października 2024 r. W pełni rozumiemy i zgadzamy się z potrzebą priorytetowego traktowania bezpieczeństwa narodowego Polski. Jesteśmy przekonani, że zapisy zaprojektowanej nowelizacji ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa pozwolą cel ten skutecznie realizować. **Nawołujemy również do pilnego wdrożenia przepisów dyrektywy CER[4], a także apelujemy o dalsze wysiłki w zakresie spełniania przez Polskę Siedmiu bazowych wymogów NATO dotyczących odporności (7 Baseline Requirements)[5] z wykorzystaniem technologii cyfrowych.**

Jesteśmy przekonani, że kluczowe komponenty sieci o znaczeniu krytycznym powinny spełniać możliwie najwyższe standardy bezpieczeństwa i być zgodne z wytycznymi polityki bezpieczeństwa naszego kraju, UE i NATO. Odpowiedź Unii Europejskiej na rosnące zagrożenia w obszarze cyberbezpieczeństwa obejmuje m.in. zestaw narzędzi na rzecz bezpieczeństwa 5G (tzw. 5G Toolbox[6]), Dyrektywę NIS2 i CER oraz Rozporządzenie DORA[7]. Komunikat Komisji Europejskiej dla Państw Członkowskich UE z czerwca 2023 roku[8], stanowi jasno, iż kluczowe jest uwzględnienie w najwyższym możliwym stopniu zaleceń zawartych w sprawozdaniu dotyczącym unijnej skoordynowanej oceny ryzyka związanego z cyberbezpieczeństwem w sieciach piątej generacji (5G)[9].

W szczególności chodzi o zalecenia dotyczące zakresu ograniczeń, które powinny obejmować krytyczne, a także wysoce wrażliwe zasoby zidentyfikowane w skoordynowanej ocenie ryzyka UE sieci 5G, takie jak funkcjonalności sieci rdzeniowej, systemy zarzadzania siecią czy funkcjonalności radiowej sieci dostępowej oraz zalecenia dotyczące stosowania okresów przejściowych, które powinny być określone w celu zapewnienia usunięcia istniejącego sprzętu, pochodzącego od dostawcy określonego jako dostawca wysokiego ryzyka. W zależności od wyników szacowania ryzyka, tego typu ograniczenia powinny mieć zastosowanie nie tylko do sieci 5G, ale ogólniej, do technologii informacyjno-komunikacyjnych (ICT), jak usługi sieciowe, rozwiązania komunikacyjne, produkty ICT, w tym rozwiązania do przechowywania danych sieci, rozwiązania Internetu Rzeczy (IoT), rozwiązania branżowe, takie jak ICT dla przemysłu lub służby zdrowia, a także rozwiązania z zakresu monitoringu i analityki, w tym analityki predykcyjnej, oraz zalecenia dotyczące stosowania okresów przejściowych, które powinny być określone w celu zapewnienia usunięcia istniejącego sprzętu, pochodzącego

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. s. 164).
[5] *Resilience, civil preparedness and Article 3* [na:] https://www.nato.int/cps/en/natohq/topics_132722.htm, 13 listopada 2024 r., dostęp 5 grudnia 2024 r.
[6] *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, NIS Coordination Group, 23 stycznia 2020 r., https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1).
[8] *Communication from the Commission: Implementation of the 5G cybersecurity Toolbox*, European Commission, 15.06.2023 r., https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox, s. 3.
[9] NIS Cooperation Group, *Report on EU coordinated risk assessment of 5G*, NIS Coordination Group, 9 października 2019 r., https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

od dostawcy określonego jako dostawca wysokiego ryzyka w najkrótszym możliwym czasie. W swoim opracowaniu z 2024 r. Grupa Współpracy NIS2 potwierdziła, że w dalszym ciągu istnieje duże ryzyko ataków poprzez łańcuchy dostaw. Skomplikowane łańcuchy dostaw powodują, że kupujący sprzęt nie są w stanie przeprowadzić dokładnej analizy zakupionego sprzętu i oprogramowania. Stopień narażenia na te ryzyka jest zależny od zakresu w jakim dostawca sprzętu lub oprogramowania ma dostęp do sieci telekomunikacyjnej oraz profilu ryzyka danego dostawcy. Zagrożeniem dla sieci 5G są również zależności od dostawców w państwach, które wywierają wpływ na dostawców w celu przeprowadzenia cyberataków. Grupa współpracy NIS2 podkreśliła jednak, że to zagrożenie nie dotyczy wyłącznie sieci 5G, ale także całego sektora telekomunikacyjnego[10]. W konsekwencji Grupa Współpracy NIS2 zaleca zwiększenie bezpieczeństwa łańcuchów dostaw, m.in. poprzez ocenę ryzyka stwarzanego przez dostawców wysokiego ryzyka oraz implementację Toolboxa 5G[11].

Ważne dla systemu cyberbezpieczeństwa jest także pilne przyjęcie przez Parlament ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)[12], która także nadal jest na etapie projektu rządowego.

Mamy również przekonanie, że **Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, wspólnie z Urzędem Zamówień Publicznych, powinien wydać (jako pomoc dla zamawiających) jednolite rekomendacje w sprawie uwzględniania w kryteriach zamawiania sprzętu, oprogramowania i usług cyfrowych – określonych wymogów i kryteriów cyberbezpieczeństwa.** Jest niezbędnym, aby w każdym postępowaniu zakupowym dotyczącym technologii informacyjno-komunikacyjnych (ICT), aspekt cyberbezpieczeństwa był brany pod uwagę, ze względu na to, iż ataki takie, jak np. ransomware, są kierowane na podmioty różnej wielkości z wielu sektorów, np. z administracji publicznej, instytucji zdrowia, uczelni wyższych i szkół, czy też biznesu – powodując często dotkliwe skutki dla zaatakowanych podmiotów. Zamawiający powinni zatem mieć świadomość zagrożeń cyberbezpieczeństwa, a także móc skorzystać z określonych rekomendacji i wzorców postępowania przy dokonywaniu zakupów ICT, tak aby kryterium najniższej ceny, które jest bardzo często stosowane, przestało dominować. Takie rekomendacje i wzorce powinny być, zdaniem Rady, przygotowane wspólnie, z inicjatywy Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Prezesa Urzędu Zamówień Publicznych. Punktem wyjścia dla opracowania tych rekomendacji powinny być Vademecum bezpiecznych zakupów oprogramowania i rozwiązań IT[13], opracowane na

[10] NIS Cooperation Group, *EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors*, 2024 r., https://ec.europa.eu/newsroom/dae/redirection/document/107357, s. 4.
[11] Ibid., s. 34–35.
[12] https://legislacja.rcl.gov.pl/projekt/12385350.
[13] R. Stefanowski, M. Konopka, Vademecum bezpiecznych zakupów oprogramowania i rozwiązań IT, https://www.gov.pl/attachment/d13e446b-42cd-4d30-b280-4ad930a485b8.

potrzeby projektu Cyberbezpieczny Samorząd oraz wytyczne dotyczące cyberbezpieczeństwa zawarte w Polityce Zakupowej Państwa[14].

Jesteśmy przekonani, że priorytetem wprowadzenia projektowanych przepisów jest bezpieczeństwo kraju, które powinno stanowić wartość nadrzędną w dyskusji nie tylko na temat projektu nowelizacji ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ale w szerszej debacie społecznej dotyczącej cyberbezpieczeństwa. Stoimy na stanowisku, że Polska musi niezwłocznie dokonać oceny dostawców działających na krajowym rynku, a następnie zaprzestać dalszych instalacji rozwiązań pochodzących od podmiotów, które uznane zostaną w ramach obiektywnego postępowania za dostawców wysokiego ryzyka, jednocześnie sukcesywnie usuwając zainstalowane wcześniej komponenty z infrastruktury w kraju. Uważamy, że w celu zachowania najwyższego bezpieczeństwa narodowego, proces usuwania rozwiązań od dostawców wysokiego ryzyka powinien rozpocząć się na obszarach kraju szczególnie narażonych na ryzyko ze względu na ich położenie geograficzne.

Rada do Spraw Cyfryzacji stoi na stanowisku, że w celu wzmocnienia bezpieczeństwa narodowego Polski, jej obywateli, przedsiębiorstw i instytucji, konieczne jest **pilne uchwalenie nowelizacji ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wdrożenie przepisów dyrektywy CER, podjęcie wysiłków w zakresie spełniania przez Polskę Siedmiu bazowych wymogów NATO dotyczących odporności z wykorzystaniem technologii cyfrowych oraz przyjęcie jednolitych rekomendacji w sprawie uwzględniania w kryteriach zamówień publicznych określonych wymogów i kryteriów cyberbezpieczeństwa.**

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji

[14] Rozdział IX Narzędzia, pkt 7 Cyberbezpieczeństwo, Polityka Zakupowa Państwa, [w:] załącznik do uchwały nr 6 Rady Ministrów z dnia 11 stycznia 2022 r. w sprawie przyjęcia Polityki zakupowej państwa (M.P. poz. 125).