UCHWAŁA nr 1
RADY do SPRAW CYFRYZACJI
z dnia 3 listopada 2023 roku
na temat Dostawców Wysokiego Ryzyka.

Na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 17 Ministra Cyfryzacji z dnia 24 czerwca 2020 r. w sprawie ustanowienia regulaminu Rady do Spraw Cyfryzacji (Dz. Urz. z 2020 r. poz. 19), uchwala się, co następuje:

Zarówno przed, jak i po rozpoczęciu inwazji Rosji na Ukrainę Rząd Polski podejmował oraz nadal podejmuje szereg specjalnych działań legislacyjnych i organizacyjnych związanych z cyberbezpieczeństwem. Wśród takich działań można wymienić np. utworzenie Funduszu Cyberbezpieczeństwa, powołanie Centralnego Biura Zwalczania Cyberprzestępczości (CBZC) w strukturach Policji, czy skierowanie do Sejmu projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (KSC), wprowadzającej instytucję Dostawcy Wysokiego Ryzyka (HRV lub DWR).

Tymczasem wiele instytucji państwowych, w tym ministerstw i urzędów centralnych oraz podmiotów korzystających z systemów infrastruktury krytycznej kontynuuje zakupy urządzeń i systemów pochodzących od dostawców, wywodzących się np. z Chin, którzy regularnie stanowią obiekt debaty o DWR. Takie działania mogą wiązać się z ryzykiem, że do podmiotów z ChRL będą trafiać dane dotyczące najważniejszych operacji polskich instytucji publicznych i firm, w tym tych o znaczeniu strategicznym, stwarzając poważne zagrożenie dla obronności, bezpieczeństwa państwa i infrastruktury kluczowej dla jego właściwego funkcjonowania. Potencjalnie rodzi to ryzyko, że krytyczne dla właściwego działania państwa informacje trafią do służb kraju współpracującego na wielu płaszczyznach z Federacją Rosyjską, także po jej inwazji na Ukrainę w 2022 r.

Ponadto, zasadna jest wątpliwość, czy chińskie firmy nie uzyskają w oparciu o gromadzone dane wiedzy dającej im istotną, nieuprawnioną przewagę konkurencyjną na polskim rynku. Należy też zapytać, czy istnieje ryzyko wystąpienia poważnych zakłóceń lub zatrzymania działań kluczowych instytucji publicznych w przypadku zewnętrznych interwencji w obsługę wspomnianych systemów. Szczególne zaniepokojenie przedsiębiorców budzi projekt e-faktur oparty na chińskich sprzęcie, z którego korzystać będzie musiała praktycznie cała polska gospodarka już w 2024 r. Aktualny pozostaje też problem współpracy z Chinami w sferach istotnych dla bezpieczeństwa - z państwem rywalizującym bezpośrednio ze Stanami Zjednoczonymi, kluczowym sojusznikiem i gwarantem bezpieczeństwa Polski, na co wielokrotnie wskazywali przedstawiciele rządu oraz najważniejszych politycznych ugrupowań.

Rada pragnie przypomnieć, że główne chińskie firmy z sektora ICT wywodzą się ze środowiska Armii Ludowo Wyzwoleńczej ChRL. Wskazać należy, że powiązania tych firm z rządem i

rządzącą partią pozostają nieprzejrzyste, a chińska ustawa o bezpieczeństwie narodowym nakazuje, aby każdy chiński obywatel i każde przedsiębiorstwo pomagało ministrowi bezpieczeństwa w działaniach wywiadowczych.

Rada uważa, że instytucja DWR musi znaleźć twarde podstawy ustawowe w polskim systemie prawnym oraz obejmować wszelkie zagrożenia związane nie tylko ze sferą telekomunikacyjną, ale ze wszystkimi rozwiązaniami sprzętowymi, programistycznymi i usługowymi związanymi z ICT. Proces ten powinien jednak uwzględniać ryzyka związane z zerwaniem ciągłości łańcuchów dostaw.

Istotnym elementem analizy zagrożeń ze strony DWR powinno być także uwzględnienie, że produkty od takich dostawców stosowane w kluczowych sektorach rynku (np. telekomunikacja, energia, woda) przekładają się na usługi oferowane dla szerokiego zakresu odbiorców instytucjonalnych i fizycznych, którzy nie mają świadomości, że te usługi oparte są na sprzęcie i oprogramowaniu, które wprowadza wysokie ryzyko dla bezpieczeństwa i ciągłości działania krytycznych usług opartych na technologiach ICT.

Rada z zadowoleniem przyjęła informację o skierowaniu nowelizacji ustawy o KSC do parlamentu i wyraża rozczarowanie, iż ta bardzo potrzebna nowelizacja, nie została przyjęta w obecnej kadencji Parlamentu. Pragniemy jednocześnie wyrazić nadzieję, że nowelizacja zostanie pilnie uchwalona w następnej kadencji oraz że jej ostateczny kształt uwzględni wszystkie istotne wnioski zgłoszone w toku publicznych dyskusji. Rada wyraża przekonanie, że kwestia bezpieczeństwa Polski, jej obywateli i firm będzie podstawą dalszych działań legislacyjnych. Rada będzie te procesy monitorować. Z niepokojem przyjęliśmy do wiadomości fakt, że w ostatniej fazie prac rządowych zmodyfikowane zostały przepisy dot. DWR, osłabiające funkcję ochrony aparatu administracyjnego państwa. W ramach tych zmian zrezygnowano z instytucji „polecenia zabezpieczającego” i wydłużono czas na wymianę sprzętu (innego niż telekomunikacyjny) pochodzącego od DWR z 5 do 7 lat, czyli do czasu ich naturalnego wyeksploatowania.

Rada ds. Cyfryzacji potwierdza, że opowiada się za rozwiązaniem, które wyraziła już Rada poprzedniej kadencji 30 marca br. Proponujemy zmodyfikować projektowane przepisy dotyczące DWR w taki sposób, by, jeżeli sprzedawca lub producent zostanie uznany za DWR:

- bezwzględnie i niezwłocznie wykluczyć go z dalszych zakupów sprzętu oraz usług,
- w oparciu o przepisy ustawy o KSC wykluczyć taki sprzęt z dalszego użytkowania w okresie maksymalnie 4 lat, ale
- do 12 miesięcy w odniesieniu do elementów infrastruktury krytycznej.

Ponadto zwracamy uwagę, że brak podstaw ustawowych dla instytucji DWR poważnie opóźniło aukcję częstotliwości 5G. Podkreślić należy ryzyko uzależnienia największych polskich operatorów telekomunikacyjnych od chińskiej technologii, szczególnie w przypadku zakłócenia łańcuchów dostaw, groźby eskalacji napięć, czy nawet wojny. Doświadczenia ostatnich lat pokazały, że takie sytuacje mogą mieć miejsce i należy uwzględniać je w procesie

stanowienia prawa. Wspierane przez państwo chińskie ataki cybernetyczne APT (Advanced Persistent Threat) oznaczają, że wybór chińskiego sprzętu do sieci 5G w Polsce stanowi poważne zagrożenie dla obronności i bezpieczeństwa polskiego państwa i polskich firm.

Coraz więcej państw zachodnich, na czele ze Stanami Zjednoczonymi, wprowadza ograniczenia dotyczące działalności chińskich dostawców w kluczowych obszarach. Niedawno Amerykańska Izba Handlowa w Polsce zwróciła uwagę na problem własności infrastruktury krytycznej w Polsce i zagrożeń ze strony państw nie będących członkami NATO lub EOG.

W ostatnim czasie także Komisja Europejska, po analizie raportu na temat Toolbox 5G[1], stwierdziła jednoznacznie, że istnieją podstawy do uznania Huawei i ZTE za DWR. Komisja uważa, że decyzje przyjęte przez państwa członkowskie o ograniczeniu lub wykluczeniu Huawei i ZTE z sieci 5G są uzasadnione i zgodne z EU 5G Toolbox. Komisja wprowadziła zakaz zakupów sprzętu tych firm na potrzeby własne. Wiele państw europejskich wprowadziło regulacje zapewniające zwiększenie bezpieczeństwa oraz mitygujące ryzyka związane z zagrożeniami ze strony DWR. Przegląd tych rozwiązań zawierał m.in. załącznik nr 1 do OSR „DWR" do projektu nowelizacji ustawy o KSC.

Rada widzi pilną potrzebę wprowadzania i powszechnego stosowania kryteriów zamówień urządzeń i oprogramowania, w których znajdą się zapisy zabezpieczające państwo i jego instytucje, wymienione w zał. nr 8 do Dyrektywy NIS, w tym dotyczące telekomunikacji i apeluje o wprowadzanie ich do ustaw, takich jak np. Ustawa - Prawo Zamówień Publicznych. Rada podkreśla że kryterium najniższej ceny nie może stać w jawnej kolizji z potrzebami bezpieczeństwa państwa i kluczowych jego instytucji, zgodnie z postanowieniami Dyrektywy NIS 2. Rada apeluje do Prezesa Urzędu Zamówień Publicznych o pilne podjęcie działań zapewniających należyty poziom ochrony bezpieczeństwa narodowego w procesie zamówień publicznych z wykorzystaniem istniejących instrumentów prawnych oraz o podjęcie prac nad nowymi rozwiązaniami legislacyjnymi.

1 Communication from the Commission: Implementation of the 5G cybersecurity Toolbox | Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone w trybie obiegowym. Projekt uchwały nr 1 został przesłany członkom Rady 27 października 2023 r. z terminem głosowania do 3 listopada 2023 r. W głosowaniu wzięło udział 9 członków Rady, z czego oddano:

- 7 głosów „za” przyjęciem uchwały,
- 0 głosów „przeciw” oraz
- 2 głosy „wstrzymuję się”.

Uchwała nr 1 Rady do Spraw Cyfryzacji została przyjęta 3 listopada 2023 roku w głosowaniu tajnym w trybie obiegowym zwykłą większością głosów.

Przewodniczący Rady
Józef Orzeł
/-podpisano elektronicznie/