Stanowisko Rady do Spraw Cyfryzacji w sprawie zagrożeń ze strony Dostawców Wysokiego Ryzyka.

W związku z zagrożeniami dla bezpieczeństwa państwa, w szczególności - z agresją Federacji Rosyjskiej na Republikę Ukrainy oraz procesem wdrażania w całej Unii Europejskiej nowych aktów prawnych dotyczących cyberbezpieczeństwa, takich jak Dyrektywa NIS 2 oraz CER, które zakładają wzmocnienie środków odporności w najważniejszych sferach działalności państwa i społeczeństwa w oparciu o analizę ryzyka i nawiązując do Uchwały nr 3 Rady do Spraw Cyfryzacji z dnia 14 kwietnia 2022 r. w sprawie wzmocnienia systemu cyberbezpieczeństwa w związku z inwazją Federacji Rosyjskiej na Republikę Ukrainy skutkującą zagrożeniem dla bezpieczeństwa sieci i systemów teleinformatycznych oraz zasobów cyfrowych RP:

Rada ds. Cyfryzacji apeluje o przyspieszenie prac nad nowelizacją ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Rada ds. Cyfryzacji apeluje o modyfikacje projektowanych zapisów w nowelizacji Ustawy o KSC dotyczących Dostawców Wysokiego Ryzyka w taki sposób by, jeżeli sprzedawca lub producent zostanie uznany za Dostawcę Wysokiego Ryzyka, został wykluczony z dalszych zakupów sprzętu oraz usług, a jego sprzęt został usunięty z dalszego użytkowania w ciągu nie dłuższym niż 4 lata.

Rada uważa, że brak ustawowych kryteriów uznawania za Dostawcę Wysokiego Ryzyka powoduje szereg zagrożeń dla bezpieczeństwa państwa - także w związku z założeniami aukcji na częstotliwości 5G, będącej obecnie przedmiotem konsultacji, według których operatorzy telekomunikacyjni mają sami decydować, kogo uznać za DWR. Dokonywanie takich ocen powinno być zadaniem kompetentnego organu państwowego i dokonywać się na podstawie ustawowych kryteriów, z poszanowaniem konstytucyjnych zasad zarówno ochrony własności prywatnej, jak i bezpieczeństwa państwa i obywateli.

Rada widzi pilną potrzebę wprowadzania w procedurę zamówień dla najważniejszych podmiotów i systemów objętych postanowieniami Dyrektyw CER i NIS2, zapisów zapewniających interes bezpieczeństwa państwa tak, by zahamować napływ urządzeń i systemów wygrywających ceną, a nie jakością cyberbezpieczeństwa.

Rada widzi pilną potrzebę dokonania audytu systemów IT, będących w posiadaniu administracji publicznej a zwłaszcza administracji rządowej, pod kątem zagrożeń ze strony dostawców wysokiego ryzyka.

Rada z uwagą przysłuchuje się wypowiedziom Europejskiego Rzecznika Ochrony Danych Osobowych, który 1 marca 2023 r. stwierdził, że nie ma żadnych możliwości weryfikacji poziomu ochrony danych osobowych w Chinach, co jednoznaczne jest z tym, iż nie ma żadnych gwarancji ich ochrony nawet w przypadku legalnego transferu między Polską i Chinami.

Rada ds. Cyfryzacji wyraża zaniepokojenie wykorzystywaniem chińskich technologii do masowego transferu danych do Chin, czego przykładem jest raport litewskiego Ministerstwa Obrony Narodowej.

Należy zauważyć, że zgodnie z obowiązującym w Chińskiej Republice Ludowej prawem, wszystkie podmioty, jak i osoby, są prawnie zobowiązane do pełnej współpracy z instytucjami bezpieczeństwa państwa, w tym do wszelkiej pomocy, asysty i wsparcia dla służb specjalnych poza granicami Chin.

Równocześnie trwa proces odsuwania firm z Chińskiej Republiki Ludowej od dostępu do technologii amerykańskich, w tym oprogramowania i mikroprocesorów najnowszych generacji. Podobne działania podejmują inne państwa Zachodu, jednak rola USA, jako głównego sojusznika Polski i partnera w NATO, jest zasadnicza.

Rada pragnie zwrócić uwagę, że już we wrześniu 2019 r. Rząd RP podpisał z USA porozumienie dotyczące bezpieczeństwa sieci 5G, w którym znajdujemy wymagania względem dostawców, zgodnie z którymi ich wnikliwa ocena powinna obejmować odpowiedzi na poniższe pytania:

- czy dostawca jest kontrolowany przez obcy rząd bez możliwości odwołania się do niezawisłego sądu;
- czy dostawca ma przejrzystą strukturę własności;
- czy dostawca w swojej historii wykazywał się etycznym postępowaniem korporacyjnym oraz, czy podlega on porządkowi prawnemu, który zapewnia przejrzystość działalności firm.

Zdaniem Rady powyższe kryteria eliminują chińskie firmy z kręgu dostawców kluczowych systemów ICT dla instytucji publicznych w Polsce. Kwestie te podejmowało Polskie Towarzystwo Informatyczne m.in. w raporcie Izby Rzeczoznawców PTI i ekspertów Rady ds. Cyfryzacji dotyczącym zagrożeń ze strony Dostawców Wysokiego Ryzyka dla sieci telekomunikacyjnych w Polsce.

Rezolucja Parlamentu Europejskiego podjęta 16 września 2021 roku podkreśla m.in., że przyszła strategia UE wobec Chin powinna zapewnić narzędzia i dane niezbędne do przeciwdziałania zagrożeniom politycznym, gospodarczym, społecznym i technologicznym wywołanym przez Chiny, a w pkt 27 podkreśla, jak ważne jest wzmocnienie zdolności sektora prywatnego i publicznego w zakresie cyberbezpieczeństwa, wzywa do ściślejszej współpracy i ustanowienia systemu mającego na celu uniemożliwienie szkodliwych działań w cyberprzestrzeni ze strony Chin, w tym cyberataków, przymusowych transferów technologii, cyber-szpiegostwa i wykorzystania cyberprzestrzeni do kradzieży własności intelektualnej.

Rada przyjęła stanowisko większością głosów.

Józef Orzeł
Przewodniczący Rady
/podpisano elektronicznie/