Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.105.2025
Warszawa, 07 lipca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 13 czerwca br. Posła na Sejm RP Pana Dariusza Mateckiego w sprawie procedury uznawania dostawców ICT za wysokiego ryzyka (HRV) jako formy nadregulacji w projekcie ustawy o krajowym systemie cyberbezpieczeństwa (UC 32) (interpelacja nr 10187)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Czy projekt UC32, zawierający przepisy o HRV, został ujęty na liście ustaw deregulacyjnych przygotowywanych przez rząd?

Nie. Projekt stanowi wdrożenie dyrektywy NIS 2 do krajowego porządku prawnego.

Ad 2) Czy planowane jest wycofanie lub ograniczenie procedury HRV do faktycznie krytycznych elementów sieci 5G, zgodnie z pierwotnym zakresem EU 5G Toolbox?

Nie ma w planach ograniczania procedury HRV do wybranych sektorów. W ocenie Ministerstwa Cyfryzacji zasadne i niezbędne dla zapewnienia bezpieczeństwa państwa i podmiotów krajowego systemu cyberbezpieczeństwa, w tym łańcuchów dostaw, jest objęcie skutkami uznania dostawcy za dostawcę wysokiego ryzyka wszystkie sektory wymienione w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Projekt ustawy i sama dyrektywa NIS 2 obejmuje swoim zakresem wiele istotnych z punktu widzenia funkcjonowania państwa i jego gospodarki sektorów, które nie powinny być różnicowane pod kątem zapewnienia bezpieczeństwa związanego z koniecznością wycofania sprzętu, oprogramowania czy usług ICT dostarczanych przez dostawcę wysokiego ryzyka. Stałoby to w sprzeczności z nadrzędnym celem dyrektywy.

Zgodnie z NIS2 wszystkie podmioty kluczowe i podmioty ważne mają obowiązek wdrożyć środki zapewniające bezpieczeństwo łańcuchów dostaw - tak więc obowiązek ten nie dotyczy tylko sektora telekomunikacyjnego. Ponadto podmioty kluczowe i podmioty ważne mają uwzględnić wyniki skoordynowanego szacowania ryzyka przeprowadzone wobec konkretnego dostawcy przez Grupę Współpracy NIS - pierwowzorem tego postępowania był unijna ocena cyberbezpieczeństwa sieci 5G, na podstawie której powstał Toolbox 5G. Tak więc aspekt bezpieczeństwa łańcuchów dostaw już jest w dyrektywie NIS 2.

Ryzykowni dostawcy mogą występować nie tylko w sektorze telekomunikacyjnym ale także i w innych. W jednym ze swoich raportów Grupa współpracy NIS wskazała, że czynnikiem sprzyjającym atakom w łańcuchu dostaw w sektorze energetycznym mogą być zależności przedsiębiorstw energetycznych od dostawców sprzętu lub oprogramowania, którzy mogą być uznawani za stwarzający wysokie ryzyko[1]. Dlatego cyberzagrożenia

[1] *A closely related issue and potentially enabling factor for supply chain attacks is the growing material dependencies on third country suppliers, as many suppliers of the often highly specific software and hardware in the electricity sector*

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

w obszarze łańcuchów dostaw należy ujmować holistycznie i uwzględnić zagrożenia potencjalnie występujące nie tylko w jednym z sektorów, ale również w pozostałych. Stąd postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka może dotyczyć dostawcy sprzętu lub oprogramowania dla różnych sektorów.

Za niezasadne należy uznać twierdzenie, że w jednym z sektorów mogą występować dostawcy wysokiego ryzyka, a w innym sektorze z pewnością nie. Prawna niemożliwość identyfikacji zagrożeń oraz ich mitygacji negatywnie wpływa na bezpieczeństwo państwa. Polska będzie wtedy państwem bezbronnym w jednym z obszarów. Oczywiście, każdy przypadek należy rozpatrywać z osobna i decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka obowiązkowo musi być poprzedzona szczegółową analizą ryzyka stwarzanego przez tego dostawcę.

Zwrócić należy uwagę również na fakt, że Komisja Europejska podkreśla konieczność zapewnienia odporności łańcuchów dostaw w Europie. Kwestia ta nie dotyczy wyłącznie jednego sektora gospodarki. Wyraźnie wskazano to w *Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego o Komitetu Regionów w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego (COM/2025/148 final)*[2].

Mając powyższe na uwadze, procedura dostawcy wysokiego ryzyka powinna odnosić się do wszystkich sektorów objętych zakresem ustawy.

Ad 3) Czy przeprowadzono ocenę kosztów wdrożenia tej procedury dla przedsiębiorców objętych obowiązkiem, w tym kosztów wymiany sprzętu ICT i reorganizacji systemów?

Nie przeprowadzono oceny kosztów wdrożenia tej procedury dla przedsiębiorców, w tym kosztów wymiany sprzętu ICT i reorganizacji systemów. Wynika to z faktu braku rzetelnych danych. Jest to zupełnie nowa instytucja w związku z czym nie zostały do tej pory wydane żadne decyzje. Na obecnym etapie nie jest nawet wiadome, czy kiedykolwiek decyzja o uznaniu jakiegoś dostawcy za dostawcę wysokiego ryzyka zostanie wydana. Procedura ta będzie stosowana w razie zaistnienia takiej potrzeby. Jakakolwiek próba ustalenia potencjalnych kosztów wdrożenia procedury dostawcy wysokiego ryzyka musiałaby odbyć się ze z góry założoną tezą, że jakiś dostawca, za dostawcę wysokiego ryzyka, może zostać uznany. Stałoby to w sprzeczności z wieloaspektową, szczegółową procedurą przewidzianą w projekcie.

Jednocześnie, w projektowanych przepisach nie przewidziano mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty kluczowe i podmioty ważne zostaną zobowiązane do wycofania sprzętu bądź oprogramowania w określonym czasie, który najczęściej równy jest cyklowi życia tego sprzętu i oprogramowania.

---

are not EU-based and may be judged high risk. The number of dependencies for the electricity sector is rising sharply, driven by the increasing digitalisation of existing electricity infrastructures and the rapid growth of renewable energy plants. This requires novel and increasingly complex constellations of technologies developed and/or manufactured outside of the EU, making security controls difficult. Such suppliers may be susceptible to interference by the government of a non-EU country without adequate legal or judicial constraints. This includes states that may be able to exert enough influence over their private sector to force them into implementing backdoors or malicious components or code into their products at a large scale. Following similar dynamics, critical electricity infrastructures dependencies on foreign cloud-hosted services can be exploited by countries hosting those cloud infrastructure.
NIS Cooperation Group, EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors, 2024, str. 18 https://ec.europa.eu/newsroom/dae/redirection/document/107357 .

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52025DC0148

Ad 4) Czy rząd przewiduje wprowadzenie pełnych gwarancji proceduralnych (np. stosowanie KPA, prawo do odwołania), które umożliwią przedsiębiorcom skuteczne kwestionowanie decyzji Ministra Cyfryzacji?

W projekcie ustawy przewidziana została szczegółowa procedura uznawania dostawcę za dostawcę wysokiego ryzyka. Zapewnione zostały przy tym wszelkie niezbędne gwarancje dla przedsiębiorców, w tym m.in. możliwość wniesienia skargi na decyzję o uznaniu za dostawcę wysokiego ryzyka. W związku z tym nie przewiduje się zmian w procedurze uznawania dostawcy za dostawcę wysokiego ryzyka.

Ad. 5) Czy rząd przeanalizował wpływ tak skonstruowanej regulacji na konkurencyjność polskiego rynku w relacji do innych państw członkowskich UE?

Przedmiotowa regulacja wynika z obowiązku wdrożenia zaleceń z tzw. 5G toolbox. Projektodawca dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów w innych państwach UE. Wyniki analizy zostały zaprezentowane w załączniku nr 1 do OSR Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie.

W większości państw Unii Europejskiej wprowadzone zostały przepisy umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie dla bezpieczeństwa narodowego. Obowiązujące regulacje przewidują dokonanie takiego wyłączenia w drodze władczego rozstrzygnięcia dokonywanego przez jeden z organów władzy wykonawczej np. w drodze decyzji administracyjnej. W wielu państwach w tego rodzaju postępowaniach istotną rolę odgrywa również organ doradczy składający się z przedstawicieli administracji, wojska oraz służb specjalnych.

Polska jest jednym z ostatnich państw UE, która nie wdrożyła do tej pory podobnych regulacji.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

Kancelaria Sejmu

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa