Minister
Klimatu i Środowiska

DEL-WRD.050.4.2024.AG
3438806.13608952.11343890
Warszawa, 31-12-2024

Pan
Szymon Hołownia
Marszałek Sejmu RP

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedź na interpelację posłanki Małgorzaty Gromadzkiej w sprawie bezpieczeństwa liczników zdalnego odczytu, nr K10INT5388.

Odnosząc się do wyrażonej w interpelacji troski o przebieg procesu cyfryzacji sektora energii w Polsce, uprzejmie informuję, że Rząd dokłada wszelkich starań, aby zapewnić bezpieczeństwo jego realizacji na każdym etapie.

Ramy prawne dla wprowadzenia inteligentnego opomiarowania w Polsce przygotowano w Ministerstwie Klimatu i Środowiska i wprowadzono ustawą z dnia 20 maja 2021 r. *o zmianie ustawy – Prawo energetyczne i niektórych innych ustaw*, tzw. „ustawa licznikową". W Ministerstwie Klimatu i Środowiska przygotowano także akty wykonawcze do tej ustawy, m.in. rozporządzenie Ministra Klimatu i Środowiska z dnia 10 stycznia 2022 r. *w sprawie procesów rynku energii*, rozporządzenie Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. *w sprawie systemu pomiarowego* oraz rozporządzenie Ministra Klimatu i Środowiska z dnia 30 maja 2023 r. *w sprawie wymagań dla standardów komunikacji pomiędzy licznikiem zdalnego odczytu a urządzeniami odbiorcy energii elektrycznej w gospodarstwie domowym oraz dla tych urządzeń na potrzeby komunikacji z licznikiem zdalnego odczytu*. Rozporządzenia te określają m.in. wymagania, jakie muszą spełniać liczniki zdalnego odczytu oraz urządzenia z nimi współpracujące.

W procesie opracowywania aktów prawnych Minister Klimatu i Środowiska prowadził szerokie konsultacje z uczestnikami rynku energii. Przy Ministrze Klimatu i Środowiska działa *Zespół ds. wprowadzenia w Polsce inteligentnego opomiarowania*, w którego skład wchodzą przedstawiciele wszystkich gałęzi sektora energetycznego: Prezesa Urzędu Regulacji Energetyki, Prezesa Głównego Urzędu Miar, Polskich Sieci Energetycznych S.A., Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej, Ogólnopolskiego Stowarzyszenia Dystrybutorów Niezależnych Energii Elektrycznej, Towarzystwa Obrotu Energią, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji oraz Federacji Konsumentów. Postulaty poszczególnych podmiotów stanowiły istotny wkład w prace legislacyjne. Zespół jest nadal aktywny, na obecnym etapie zajmuje się monitorowaniem i wsparciem procesu wdrażania inteligentnego opomiarowania i uruchomienia Centralnego Systemu Informacji Rynku Energii. Zgodnie z ustawą – *Prawo energetyczne* na operatorze systemu elektroenergetycznego spoczywa obowiązek zapewnienia jego bezpiecznego funkcjonowania. Rolą prawodawcy jest wyważyć precyzyjność regulacji i ich zakres w kontekście ich efektywności i zachowania elastyczności funkcjonowania uczestników rynku.

1. Czy ministerstwo planuje wprowadzenie schematów oraz określenie podmiotów certyfikujących dla komponentów AMI (Advanced Metering Infrastructure), w tym w szczególności liczników inteligentnych?

Aktualnie w Polsce już istnieją dobrowolne programy certyfikacji umożliwiające producentom wnioskowanie o certyfikację produktów w oparciu o normy międzynarodowe. W obszarze certyfikacji produktów teleinformatycznych mających znaczenie dla sektora energii, w tym tzw. „liczników inteligentnych" (smart metering), tj. komponentów AMI, stosowane są następujące normy:

a. normy horyzontalne (dla produktów teleinformatycznych) np. PN-EN ISO/IEC 15408, tj. Common Criteria, opcjonalnie uzupełnione o specyficzne profile zabezpieczeń (protection profile) w ramach krajowych lub europejskich programów certyfikacji,
b. normy horyzontalne dla produktów Internetu Rzeczy (IoT) np. PN-ETSI 303 654 CYBER - *Cyberbezpieczeństwo Konsumentów Internetu Rzeczy – Wymagania podstawowe*,
c. normy sektorowe np. mających znaczenie dla przemysłu, tj. PN-EN IEC 62443-4-2 „Bezpieczeństwo w systemach sterowania i automatyki przemysłowej - Część 4-2: Wymagania techniczne bezpieczeństwa dla komponentów IACS (International Association of Classification Societies)",
d. dokumenty normatywne i specyfikacje techniczne opracowywane przez urzędy, grupy producenckie i stowarzyszenia branżowe.

W 2021 r. została ustanowiona Jednostka Certyfikująca Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) oraz system certyfikacji cyberbezpieczeństwa wyrobów oparty o normę Common Criteria, który jest dostępny dla wszystkich podmiotów zainteresowanych certyfikacją. Jednostka Certyfikująca NASK-PIB jest akredytowana przez Polskie Centrum Akredytacji na zgodność z normą PN-EN ISO/IEC 17065 – *Wymagania dla jednostek certyfikujących wyroby, procesy i usługi*. Jest także uznawana przez międzynarodowe porozumienia Senior Officials Group-Information Systems (SOG-IS) Mutual Recognition Agreement (MRA) i Common Criteria Recognition Arrangement (CCRA). System certyfikacji działa w oparciu o „Program oceny i certyfikacji bezpieczeństwa IT (PC1)", a certyfikacja jest prowadzona na zgodność z normami PN-EN ISO/IEC 15408, tj. Common Criteria oraz PN-EN ISO/IEC 19790 (dla modułów kryptograficznych). Planowane jest rozszerzenie zakresu akredytacji Jednostki Certyfikującej NASK-PIB o normę PN-ETSI 303 654. Jednostka Certyfikująca NASK-PIB działa w ścisłej współpracy z laboratoriami oceny bezpieczeństwa IT funkcjonującymi w Instytucie Łączności – Państwowy Instytut Badawczy oraz Instytucie Technik Innowacyjnych EMAG w sieci Łukasiewicz. Laboratoria te są zarządzane i akredytowane w stosownym zakresie zgodnie z normą PN-EN ISO/IEC 17025 - *Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących*. W najbliższej przyszłości planowany jest pilotaż badania laboratoryjnego i certyfikacji jednego z urządzeń pomiarowych polskiego producenta, który określił swoje wstępne zainteresowanie. Pilotaż, o ile dojdzie do skutku, umożliwi opracowanie wniosków i ew. rekomendacji dla całego sektora. Powyższe działania są monitorowane przez Ministra Cyfryzacji.

2. Czy ministerstwo planuje wprowadzenie przepisów regulujących lub wykluczających dostawców wysokiego ryzyka z rynku liczników inteligentnych?

Instytucja tzw. „czarnej listy dostawców" (z ang. High Risk Vendors, HRV) została wprowadzona w ramach opublikowanego w styczniu 2020 r. zestawu środków dotyczących minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanym jako Toolbox 5G. Toolbox 5G wymaga transponowania przez kraje członkowskie, które mają swobodę co do sposobu jego wdrożenia. Przepisy te powstaną w ramach kompetencji Ministra Cyfryzacji na podstawie aktualnie procedowanych ustaw:

a) projektu ustawy *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32),
b) projektu ustawy *o krajowym systemie certyfikacji cyberbezpieczeństwa* (UC42).

Samo przyjęcie tych przepisów nie będzie jednak oznaczało wykluczenia jakiegokolwiek podmiotu z rynku.

W projekcie UC32 tworzy się procedurę, w ramach której można uznać danego dostawcę produktów ICT (Information and Communications Technology), usług ICT lub procesów ICT za dostawcę wysokiego ryzyka, a decyzja o uznaniu wiąże się z obowiązkiem wycofania produktów/usług/procesów ICT takiego dostawcy z infrastruktury odbiorcy. Termin na wycofanie będzie się pokrywał z cyklem życia takich produktów i będzie wynosił 4 bądź 7 lat w zależności od tego, czy odbiorca jest przedsiębiorcą komunikacji elektronicznej.

Obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu

kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W związku z powyższym, w przepisach nowelizacji została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Szeroka definicja dostawcy pozwala na objęcie ww. procedurą producenta, importera czy dystrybutora. Przez produkty ICT należy rozumieć element lub grupę elementów systemu informacyjnego, przez usługę ICT usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych, a przez proces ICT należy rozumieć zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT.

W ocenie ministra właściwego do spraw informatyzacji taka procedura będzie stanowiła skuteczne narzędzie w zapewnianiu odporności i bezpieczeństwa państwa w kontekście stale rosnących cyberzagrożeń.

3. Czy będą wspólne porozumienia OSD w zakresie bezpieczeństwa komponentów AMI?

Operatorzy systemów dystrybucyjnych elektroenergetycznych przy określaniu warunków zamówienia w postępowaniu zakupowym są zobowiązani uwzględniać wytyczne dotyczące wymagań funkcjonalnych oraz wymagań w zakresie bezpieczeństwa systemu pomiarowego określone w rozporządzeniu Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. *w sprawie systemu pomiarowego*. W związku z tym dodatkowe porozumienia między operatorami systemu dystrybucyjnego w tym zakresie nie wydają się uzasadnione

4. Czy ministerstwo planuje wprowadzenie zasady obligatoryjnego podziału dostarczanych w ramach przetargów urządzeń?

Stroną zamawiającą i odpowiedzialną za przeprowadzenie całego procesu w postępowaniu o udzielenie zamówienia na liczniki zdalnego odczytu są operatorzy systemu dystrybucyjnego elektroenergetycznego. Prawo nie przewiduje możliwości ingerowania Ministra Klimatu i Środowiska w proces zakupowy poszczególnych podmiotów działających na rynku energii.

5. Czy ministerstwo planuje opracowanie metodyki i narzędzi testowania wymagań bezpieczeństwa?

W Ministerstwie nie ma planów opracowania metodyki i narzędzi testowania wymagań bezpieczeństwa. Szczegółowych informacji w odniesieniu do pytania 5 dostarcza odpowiedź na pytanie 2.

6. Czy ministerstwo planuje wprowadzenie ścisłych regulacji prawnych określających odpowiedzialność dostawców za zabezpieczenie łańcucha dostaw?

Ministerstwo nie planuje wprowadzenia regulacji określających odpowiedzialność za zabezpieczenie łańcucha dostaw. Opisany w odpowiedzi na pytanie 9 przygotowywany w Ministerstwie Cyfryzacji projekt ustawy *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* wdraża dyrektywę Network and Information Systems Directive 2 (NIS 2) określającą wytyczne sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, m.in. liczników zdalnego odczytu. Jak można przeczytać w uzasadnieniu do projektu ustawy: *należy wprowadzić politykę łańcucha dostaw obejmującą relację z bezpośrednimi dostawcami. (…)"*. Działania te wydają się wystarczające dla zapewnienia bezpieczeństwa korzystania z liczników zdalnego odczytu.

7. Czy jest w planach Nowelizacja Prawa Zamówień Publicznych w zakresie pochodzenia produktu?

Ustawa z dnia 11 września 2019 r. - *Prawo zamówień publicznych* (dalej: ustawa Pzp) zawiera regulacje, które już obecnie dają zamawiającemu narzędzia do tego, aby nie dopuszczać do procedowania w postępowaniu o udzielenie zamówienia ofert wykonawców, w sytuacji gdy obejmują one produkty niespełniające wymagań w zakresie cyberbezpieczeństwa określonych przez prawo.

Przepis art. 226 ust. 1 pkt 17 ustawy Pzp daje zamawiającemu podstawę do odrzucenia oferty wykonawcy, jeżeli obejmuje ona urządzenia informatyczne lub oprogramowanie

wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe. Oznacza to, że jeżeli urządzenia informatyczne lub oprogramowanie zostaną zamieszczone w rekomendacji, oferta je obejmująca podlega obligatoryjnemu odrzuceniu. Rekomendacja, o której mowa w art. 33 ust. 4 ustawy *o krajowym systemie cyberbezpieczeństwa* jest wydawana, gdy uprawnione organy po przeprowadzeniu badania urządzenia informatycznego lub oprogramowania zidentyfikują podatność (urządzenia lub oprogramowania), której wykorzystanie może zagrozić, w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa (art. 33 ust. 1 tej ustawy). Rekomendacja nie ma charakteru decyzji administracyjnej, niemniej jednak informacje w niej zawarte są wiążące przy ocenie ofert.

Jednocześnie, warto zaznaczyć, że co do zasady wykonawca, który decyduje się złożyć ofertę w postępowaniu o udzielenie zamówienia potwierdza przez sam fakt złożenia oferty, że działa zgodnie z przepisami prawa, w tym poświadcza zgodność oferowanego produktu ze standardami w zakresie bezpieczeństwa (bez względu na to czy jest on producentem czy dostawcą danego produktu).

Dodatkowo, opisana w odpowiedzi na pyt. 9 projektowana ustawa *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32), w art. 10, przewiduje nadanie nowego brzmienie art. 226 ust. 1 pkt 17 ustawy Pzp, zgodnie z którym odrzuceniu będzie podlegała oferta obejmująca produkt ICT, usługę ICT lub proces ICT (w rozumieniu art. 2 pkt 12 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. *w sprawie ENISA (European Union Agency for Cybersecurity - Agencji Unii Europejskiej ds. Cyberbezpieczeństwa*) *oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013)*, wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ww. *ustawy o krajowym systemie cyberbezpieczeństwa*, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe.

Ponadto, istotnym nowym rozwiązaniem dodawanym projektowaną ustawą jest wprowadzenie zakazu nabywania, przez podmioty biorące udział w procesie udzielania zamówień publicznych, produktów ICT, usług ICT lub procesów ICT, które zostały określone w decyzji regulowanej projektowanym art. 67b ust. 15 (art. 67c ust. 4 projektu ustawy). W myśl projektowanego art. 67b ust. 15, minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje bowiem dostawcę sprzętu lub oprogramowania oraz podmioty wchodzące w skład grupy kapitałowej, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. *o rachunkowości*, w ramach której funkcjonuje dostawca, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.

Z rozwiązaniem tym skorelowana jest podstawa odrzucenia oferty, której dodanie przewiduje projekt ustawy. Zgodnie z dodawanym pkt 19 w art. 226 ust. 1 ustawy Pzp, odrzuceniu będzie podlegać również oferta obejmująca produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy *o krajowym systemie cyberbezpieczeństwa*, lub usługę ICT, lub proces ICT, określone w tej decyzji.

8. Czy są rekomendacje pełnomocnika ds. Cyberbezpieczeństwa dotyczące dostawców wysokiego ryzyka w obszarze inteligentnych liczników energii?

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa nie wydał do tej pory rekomendacji dotyczących dostawców wysokiego ryzyka w obszarze inteligentnych liczników energii.

9. Czy jest brane pod uwagę wprowadzenie zmiany ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), obejmującej m.in.:

- ***wymaganie wdrożenia przez dostawców rozwiązań pomiarowych dla energetyki Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);***
- ***realizację ściśle określonych wymagań bezpieczeństwa przez dostawców rozwiązań pomiarowych dla energetyki;***

- ***wymóg audytów zgodności z UKSC w akredytowanych jednostkach certyfikujących lub upoważnionych podmiotach?***

Przygotowywany w Ministerstwie Cyfryzacji projekt ustawy *o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* wdraża dyrektywę Parlamentu Europejskiej i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) i tym samym przewiduje zmiany w zakresie sporządzania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, rozbudowuje obowiązki podmiotów krajowego systemu cyberbezpieczeństwa, a także wprowadza instytucję audytów doraźnych mających charakter audytu zewnętrznego.

Obowiązkami tymi zostaną objęte podmioty kluczowe i podmioty ważne. Podmioty te będą, co do zasady, podlegać samoidentyfikacji na podstawie wskazanych w ustawie kryteriów – wymienionych w szczególności w projektowanym art. 5 oraz w załączniku nr 1 i 2 do projektu ustawy. Poza audytami doraźnymi podmioty kluczowe obowiązane będą do przeprowadzania audytu co najmniej raz na 3 lata. Audyt ten może mieć charakter wewnętrzny.

Należy podkreślić, że zgodnie z załącznikiem 1 do projektu ustawy do podmiotów kluczowych, które będą realizowały obowiązki z zakresu cyberbezpieczeństwa należą operatorzy systemu dystrybucyjnego elektroenergetycznego. To te podmioty są odpowiedzialne za umożliwienie komunikacji licznika zdalnego odczytu z urządzeniami odbiorcy końcowego, a także są uprawnione do wysyłania poleceń do liczników zdalnego odczytu na obszarze swojego działania. W związku z tym, przedsiębiorstwa kluczowe dla działania liczników będą objęte ww. obowiązkami z zakresu cyberbezpieczeństwa, w tym obowiązkowymi audytami.

10. Czy planowane jest zarekomendowanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa, aby w krajowym systemie energetycznym nie stosować urządzeń lub oprogramowania pochodzących spoza Europejskiego Obszaru Gospodarczego?

Zgodnie z ustawą *o krajowym systemie cyberbezpieczeństwa* wydanie przez Pełnomocnika rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania zależy od przedstawienia w tej sprawie wniosków ze strony zespołów CSIRT (The Computer Security Incident Response Team - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) oraz opinii Kolegium do Spraw Cyberbezpieczeństwa. Przedstawienie Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa takiej rekomendacji musi zostać poprzedzone odpowiednimi pracami oraz analizą zagrożeń. Obecnie trwają prace nad taką analizą, prowadzone przez Ministerstwo Cyfryzacji, w które zaangażowane jest Ministerstwo Klimatu i Środowiska oraz Instytut Łączności – Państwowy Instytut Badawczy.

Z wyrazami szacunku

Z up. Ministra

Miłosz Motyka
Podsekretarz Stanu
Ministerstwo Klimatu i Środowiska
/ – podpisany cyfrowo/