Warszawa, dn. 04.08.2023 roku

**Stanowisko**
**Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji**
**dotyczące bezpieczeństwa liczników energii elektrycznej**[1]

W nawiązaniu do opublikowanego rozporządzeniem Ministra Klimatu i Środowiska z dnia 22 marca 2022 roku w sprawie systemu pomiarowego oraz biorąc pod uwagę:

- krytyczność sektora energetycznego i urządzeń pomiarowych instalowanych w publicznych sieciach elektroenergetycznych,
- aktualną sytuację geopolityczną,
- zagrożenia bezpieczeństwa krajowego,

**rekomendujemy aby w publikowanych przez Spółki OSD postępowaniach przetargowych wprowadzić zmiany oraz wymagania mające na celu ograniczenie ryzyka związanego z pozyskaniem w ramach prowadzonych postępowań przetargowych, produktów lub usług pochodzących od niezaufanych dostawców lub producentów, które nie zapewniają wymaganego bezpieczeństwa.**

Rekomendujemy również aby powstała instytucja certyfikująca systemy weryfikacji skuteczności działania procedur produkcji pod kontrolą liczników i innych urządzeń mających znaczenie dla cyberbezpieczeństwa infrastruktury krytycznej (np. w NASK). W okresie przejściowym Ministerstwo Klimatu i Środowiska powinno wydać rekomendacje dotyczące nie zamawiania liczników smart z obszarów geograficznych wysokiego ryzyka (tak jak zrobiono to w innych krajach UE, miękka i szybka rekomendacja ministerstwa "na szybko" zanim powstanie "twarda regulacja" prawna o systemie weryfikacji i dopuszczeń (która jest już wpisana w naszym stanowisku i która oczywiście jest konieczna).

Zgodnie z wymaganiami w/w rozporządzenia infrastruktura pomiarowa powinna być zabezpieczona przed nieuprawnionym dostępem do informacji zawartych w licznikach oraz w systemach odczytowych. Przy czym należy podkreślić, że **zabezpieczania techniczne i teleinformatyczne urządzeń i systemów są tylko częścią całego systemu bezpieczeństwa**, w którym także **ogromne znaczenie ma dobór wykonawców lub dostawców** infrastruktury pomiarowej AMI oraz ich odpowiednia weryfikacja.

Opierając się na doświadczeniach członków KIGEiT oraz analizami z innych rynków europejskich, przedstawiamy kilka istotnych kryteriów, według których powinna zostać przeprowadzona weryfikacja produktów oraz uczestników postępowań zakupowych, aby w przyszłości po zainstalowaniu liczników w sieci zasilającej, uniknąć lub zminimalizować ryzyko związane ze złamaniem bezpieczeństwa:

1. Główna siedziba producenta powinna być położona w kraju będącym sygnatariuszem porozumienia GPA[2] (Government Procurement Ageement), podpisanego w ramach WTO (World Trade Organization) w sprawie zasad realizacji zamówień publicznych.

[1] Stanowisko zostało wypracowane w ramach Sekcji Inteligentnych Sieci - Smart Grids KIGEiT przy udziale pozostałych firm Członków KIGEiT

[2] https://www.uzp.gov.pl/baza-wiedzy/zamowienia-publiczne-na-swiecie/gpa

2. Miejsce produkcji urządzeń nie powinno znajdować się poza obszarem Europejskiego Obszaru Gospodarczego (EOG[3]) lub Europejskiego Stowarzyszenia Wolnego Handlu (EFTA[4]).
3. Takie samo wymaganie jak powyżej powinno dotyczyć także miejsca, gdzie są generowane, przechowywane oraz wgrywane do urządzeń klucze szyfrujące.
4. Dystrybucja kluczy szyfrujących nie powinna odbywać się przez pośredników, agentów lub dystrybutorów, którzy mogą wejść w posiadanie kopii materiałów bezpieczeństwa i uzyskać nieuprawniony dostęp do wszystkich liczników instalowanych w sieci elektroenergetycznej.
5. Wykonawca powinien prowadzić zarejestrowaną działalność handlową na terenie Rzeczpospolitej nie krócej niż 10 lat.
6. Udział komponentów zastosowanych w systemach pomiarowych, pochodzących z Europejskiego Obszaru Gospodarczego lub Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) powinien być zgodny wymaganiami dla EUR-1 i WIP[5] (zgodnie z Protokołem 4 WTO[6] dotyczącym reguł pochodzenia towarów).
7. Zgodnie z art. 393 ust. 1 pkt 4 PZP[7] zamawiający może, w przypadku zamówienia na dostawy, odrzucić ofertę, w której udział produktów, w tym oprogramowania wykorzystywanego w wyposażeniu sieci telekomunikacyjnych pochodzących z państw członkowskich Unii Europejskiej, państw, z którymi Unia Europejska zawarła umowy o równym traktowaniu przedsiębiorców, lub państw, wobec których na mocy decyzji Rady stosuje się przepisy dyrektywy 2014/25/UE[8], nie przekracza 50%, jeżeli przewidział to w ogłoszeniu o zamówieniu, a jeżeli postępowanie nie jest wszczynane za pomocą ogłoszenia o zamówieniu – w SWZ
8. Wyższa waga pozacenowych kryteriów wyboru dostawcy w przetargach publicznych, szczególnie tych związanych z bezpieczeństwem infrastruktury krytycznej i dostawcami z obszarów wysokiego ryzyka.
9. Wprowadzenie standardu (w formie rozporządzenia) obejmującego system weryfikacji i dopuszczania na rynek polski liczników smart pod kątem cyberbezpieczeństwa (w tym procedur aktualizacji i usuwania wad oprogramowania)
10. Wprowadzenie procedury zgłaszania incydentów naruszenia bezpieczeństwa cyfrowego związanych z komunikacją zdalną i jasne określenie instytucji odpowiadającej za reagowanie w sektorze energetycznym.

Oprócz kryteriów wymienionych powyżej, mając na uwadze szersze znaczenie bezpieczeństwa, producenci powinni zapewnić bezpieczeństwo samej produkcji, stosowanych materiałów oraz ochronę środowiska dbając o zrównoważony rozwój i społeczną odpowiedzialność związaną z prowadzeniem działalności gospodarczej. Powinni spełniać następujące wymagania dla procesu produkcyjnego:

- Zarządzanie bezpieczeństwem informacji na etapie projektowania (R&D) oraz produkcji urządzeń zgodnie z normą ISO 27001,
- Zarządzanie jakością wg ISO 9001,
- Ograniczenie stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym - Dyrektywa RoHS,
- Zarządzanie środowiskowe zgodnie z normą ISO 14001,

[3] https://www.europarl.europa.eu/factsheets/pl/sheet/169/the-european-economic-area-eea-switzerland-and-the-north
[4] https://www.efta.int/about-efta
[5] Wiążąca informacja o pochodzeniu: https://www.podatki.gov.pl/clo/informacje-dla-przedsiebiorcow/pochodzenie-towarow/wiazaca-informacja-o-pochodzeniu-wip-wytyczne/
[6] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22005D0136
[7] https://www.uzp.gov.pl/__data/assets/pdf_file/0019/42184/ustawa_PZP_z_11_wrzesnia_2019.pdf
[8] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014L0025

- Bezpieczeństwo i higiena pracy wg ISO 45001,
- Zarządzanie ciągłością produkcji wg normy ISO 22301,
- Audyty zgodności z wyżej wymienionymi normami ISO przeprowadzane przez instytucje certyfikujące zlokalizowane na terenie UE,
- Wymagania dotyczące zrównoważonego rozwoju i odpowiedzialności społecznej zawarte w UN Global Compact oraz związana z tym konieczność wykonywania audytów i publikowania raportów opisujących stosowanie przez przedsiębiorców praktyk obejmujących kwestie środowiskowe, ekonomiczne, społeczne oraz ekologiczne.

Warto także podkreślić, że na początkowym etapie procesu zakupowego, a więc na etapie składania ofert ostatecznych, każdy z producentów lub dostawców powinien dostarczyć próbki urządzeń łącznie z odpowiednimi, wymaganymi dokumentami, co pozwoliłyby na zweryfikowanie wszystkich istotnych elementów bezpieczeństwa. Spotykane w postępowaniach przetargowych odstąpienie od tego wymogu i opieranie się jedynie na oświadczeniach dołączonych do oferty, może prowadzić do wyboru produktów, które w praktyce mimo oświadczenia producentów mają luki bezpieczeństwa, które będą w dalszej kolejności usuwane na zasadach gwarancji, a więc już po zainstalowaniu w sieci elektroenergetycznej. Wymaganie dostarczenia wraz z ofertą próbki („wzorca") daje pewność, że oferowany produkt jest dostępny, gotowy do produkcji i można zweryfikować jego należyty stopień ochrony przed nieuprawnionym dostępem do informacji oraz dostępem do funkcji sterujących licznika. Ten ostatni element jest szczególnie ważny ze względu na możliwość zdalnego nieautoryzowanego wyłączenia odbiorcy energii.

**Przedstawiając w naszym stanowisku kwestie dotyczące bezpieczeństwa chcieliśmy wskazać, nie tylko na sam produkt – licznik, który jest głównym elementem infrastruktury pomiarowej, ale także na wiele innych aspektów, które będą miały zdecydowany wpływ na bezpieczne użytkowanie systemu pomiarowego jako całości**.

Signature Not Verified
Dokument podpisany przez Stefan Kamiński
Data: 2023.08.04 12:58:20 CEST
Powód: Złożenie podpisu

Prezes Zarządu
Stefan Kamiński

Dokument podpisany przez JAROSŁAW ANDRZEJ TWORÓG
Data: 2023.08.04 13:28:25 CEST